

Introdução à **Segurança de Redes**

Ivo Peixinho

A RNP – Rede Nacional de Ensino e Pesquisa – é qualificada como uma Organização Social (OS), sendo ligada ao Ministério da Ciência, Tecnologia e Inovação (MCTI) e responsável pelo Programa Interministerial RNP, que conta com a participação dos ministérios da Educação (MEC), da Saúde (MS) e da Cultura (MinC). Pioneira no acesso à Internet no Brasil, a RNP planeja e mantém a rede Ipê, a rede óptica nacional acadêmica de alto desempenho. Com Pontos de Presença nas 27 unidades da federação, a rede tem mais de 800 instituições conectadas. São aproximadamente 3,5 milhões de usuários usufruindo de uma infraestrutura de redes avançadas para comunicação, computação e experimentação, que contribui para a integração entre o sistema de Ciência e Tecnologia, Educação Superior, Saúde e Cultura.

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**



Introdução à **Segurança de Redes**

Ivo Peixinho



Introdução à **Segurança de Redes**

Ivo Peixinho

Rio de Janeiro
Escola Superior de Redes
2013

Copyright © 2013 – Rede Nacional de Ensino e Pesquisa – RNP
Rua Lauro Müller, 116 sala 1103
22290-906 Rio de Janeiro, RJ

Diretor Geral
Nelson Simões

Diretor de Serviços e Soluções
José Luiz Ribeiro Filho

Escola Superior de Redes

Coordenação
Luiz Coelho

Edição
Pedro Sangirardi

Revisão Técnica
Fernando Amatte

Coordenação Acadêmica de Segurança e Governança de TI
Edson Kowask Bezerra

Equipe ESR (em ordem alfabética)
Celia Maciel, Cristiane Oliveira, Derlinéa Miranda, Elimária Barbosa, Evellyn Feitosa, Felipe Nascimento, Lourdes Soncin, Luciana Batista, Luiz Carlos Lobato, Renato Duarte, Sergio Ricardo de Souza e Yve Abel Marcial.

Capa, projeto visual e diagramação
Tecnodesign

Versão
2.2.0

Este material didático foi elaborado com fins educacionais. Solicitamos que qualquer erro encontrado ou dúvida com relação ao material ou seu uso seja enviado para a equipe de elaboração de conteúdo da Escola Superior de Redes, no e-mail info@esr.rnp.br. A Rede Nacional de Ensino e Pesquisa e os autores não assumem qualquer responsabilidade por eventuais danos ou perdas, a pessoas ou bens, originados do uso deste material.
As marcas registradas mencionadas neste material pertencem aos respectivos titulares.

Distribuição
Escola Superior de Redes
Rua Lauro Müller, 116 – sala 1103
22290-906 Rio de Janeiro, RJ
http://esr.rnp.br
info@esr.rnp.br

Dados Internacionais de Catalogação na Publicação (CIP)

P380i Peixinho, Ivo de Carvalho.
Introdução à Segurança de Redes / Ivo de Carvalho Peixinho, Fernando Pompeo Amatte. – Rio de Janeiro: RNP/ESR, 2013.
204 p. : il. ; 28 cm.

Bibliografia: p. 183-185.
ISBN 978-85-63630-23-0

1. Redes de Computadores – Segurança. 2. Segurança da informação – Ameaças, Vulnerabilidades, Risco. 3. Segurança lógica. 4. Fundamentos de segurança. 5. Política de segurança. I. Amatte, Fernando Pompeo. II. Título

CDD 004.66

Sumário

Escola Superior de Redes

A metodologia da ESR **xiii**

Sobre o curso **xiv**

A quem se destina **xiv**

Convenções utilizadas neste livro **xiv**

Permissões de uso **xv**

Sobre os autores **xvi**

1. Introdução, histórico e princípios básicos de segurança

Introdução **1**

Exercício de nivelamento 1 – Informação **1**

Segurança da informação **1**

Segurança de redes **2**

Exercício de fixação 1 – Segurança de redes **3**

Anos 50 e 60 **3**

Anos 70 **3**

Anos 80 **4**

Ano de 1988 **6**

Ano de 2001 **6**

Ano de 2003 **7**

Ano de 2009 **7**

Segurança no Brasil **7**

Ano de 2011 **8**

Ano de 2012 **8**

CSIRTs no Brasil **8**

Decreto n° 3505, de 13 de junho de 2000 **9**

DSIC **10**

Princípios básicos de segurança **10**

Exercício de fixação 2 – Princípios básicos de segurança **10**

Princípios básicos de segurança **11**

Roteiro de Atividades 1 13

Atividade 1.1 – Listas e informações complementares de segurança **13**

2. Conceitos de segurança física e segurança lógica

Introdução **15**

Exercício de nivelamento 1 – Conceitos de segurança física e segurança lógica **15**

Segurança física **15**

Segurança externa e de entrada **16**

Segurança da sala de equipamentos **17**

Supressão de incêndio **17**

Exercício de fixação 1 – Segurança em perímetro **19**

Segurança dos equipamentos **19**

Redundância **20**

Exercício de fixação 2 – Redundância **25**

Segurança no fornecimento de energia **25**

Salvaguarda (backup) **26**

Descarte da informação **27**

Segurança lógica **28**

Firewall **28**

Necessidades em um firewall **29**

Packet filtering (filtro de pacotes) **30**

Stateless **30**

Stateful packet filter **30**

Application proxy **30**

Deep packet inspection **31**

Exercício de fixação 3 – Firewall **32**

Uma visão a partir do datagrama **32**

Exemplos de firewalls **33**

Detectores de intrusos **33**

IDS Snort **34**

Fluxo de funcionamento do Snort **34**

Hids **35**

Kids **36**

IPS **36**

Redes virtuais privadas **36**

Autenticação, autorização e auditoria **37**

Autenticação, autorização e auditoria **37**

Roteiro de Atividades 2 **39**

Atividade 2.1 – Segurança física e lógica **39**

3. Panorama atual da área de segurança

Introdução **41**

Panorama atual da internet **41**

Exercício de nivelamento 1 – Panorama atual da área de segurança **42**

Acesso em banda larga modem bridge **42**

Acesso banda larga modem router **42**

Principais erros **43**

Ameaças frequentes **44**

Vírus **44**

Tipos de vírus **45**

Worms **46**

Cavalo de troia **46**

Spyware **48**

Malware **49**

Mobile Malware **49**

Exercício de fixação 1 – Malwares **50**

Prevenção **50**

Vulnerabilidades **50**

Estatísticas **51**

Hacker, cracker e outros personagens **52**

Motivação 54

Roteiro de Atividades 3 55

Atividade 3.1 – Controles de informática 55

Atividade 3.2 – Serviços e ameaças 55

4. Arquitetura TCP/IP – conceitos básicos

Exercício de nivelamento 1 – Arquitetura TCP/IP 57

Introdução 57

Família de protocolos TCP/IP 58

Camada física 58

Hub (Ethernet) 59

Bridge (Ethernet) 59

Switch (Ethernet) 60

Endereçamento físico 61

Camada de rede 61

Protocolo IP (Internet Protocol) 62

Endereçamento IP 63

Subnetting (endereçamento por sub-rede) 64

Protocolos auxiliares (ARP, RARP e ICMP) 64

ICMP 65

Endereçamento dinâmico 66

Exercício de fixação 1 – Endereçamento dinâmico 66

Roteamento 66

Exercício de fixação 2 – Roteamento 67

Camada de transporte 67

TCP 67

Cabeçalho TCP 68

UDP 69

Camada de aplicação 70

Camada OSI 71

Packet Filter (filtro de pacotes) 71

Stateful (Filtragem com Estado de Conexão) 72

Bridge Statefull 73

Soluções de firewall 73

Sniffers 74

Roteiro de Atividades 4 **75**

Atividade 4.1 – Sniffers para captura de dados **75**

Atividade 4.2 – Estados de firewall **75**

5. Arquitetura TCP/IP e segurança

Exercício de nivelamento 1 – Arquitetura TCP/IP e segurança **77**

Introdução **77**

Sniffers (farejadores) **78**

Source routing (roteando pela fonte) **79**

DoS (Denial of Service) **80**

Exercício de fixação 1 – Negação de serviço **81**

Spoofing **81**

E-mail spoofing **82**

IP spoofing **82**

SYN flood **84**

Smurf **85**

Modelo de ataque fraggle **85**

Modelo de ataque DRDOS **86**

Portscan (varredura de portas) **87**

Distributed Denial of Service (DDoS) **88**

DDoS (DoS distribuído) **90**

Exercício de fixação 2 – DDoS **90**

Modelo de ataque DDoS em duas camadas **90**

Modelo de ataque DDoS em três camadas **91**

Modelo de ataque DDoS/Worm **92**

Vulnerabilidades em implementações específicas **92**

Ping da morte **92**

Teardrop **92**

Land **92**

Roteiro de Atividades 5 **95**

Atividade 5.1 – Conceito de varreduras **95**

Atividade 5.2 – Simulando ataques com Hping **95**

Atividade 5.3 – Simulando um ataque DoS Land **96**

6. **Criptografia I – Fundamentos**

Introdução **97**

Exercício de nivelamento 1 – Fundamentos de criptografia **98**

Criptografia – algoritmos e chaves **98**

Tipos de criptografia **100**

Criptografia simétrica **101**

Eletronic Code Book **102**

Cipher Block Chaining **103**

Cipher Feed Back **103**

Output Feedback **104**

Data Encryption Standard (DES) **105**

3DES, RC-4, IDEA e AES **106**

Algoritmo Diffie-Hellman **107**

Criptografia assimétrica **108**

Funções de hash **109**

Exercício de fixação 1 – Criptografia assimétrica **110**

Assinatura digital **110**

Certificação digital **111**

Public Key Infrastructure (PKI) **112**

Exemplo completo **113**

Roteiro de Atividades 6 **115**

Atividade 6.1 – Conhecendo mais sobre certificação digital **115**

Atividade 6.2 – Uso de criptografia em e-mails **115**

Atividade 6.3 – Uso de criptografia em arquivos **115**

Atividade 6.4 – Criando um contêiner seguro **116**

7. **Criptografia II – Aplicações**

Introdução **119**

Exercício de nivelamento 1 – Criptografia **120**

Assinatura digital **120**

Blind signature (assinatura cega) **120**

Votação eletrônica **121**

Dinheiro eletrônico **122**

PayPal **123**

Criptografia de servidor (SSL/TLS) **124**

Criptografia de servidor **125**

Redes virtuais privadas (VPN) **127**

Redes virtuais privadas **128**

Exercício de fixação 1 – Redes Virtuais Privadas (VPNs) **128**

Segurança na www **128**

Seleção de um navegador **129**

Recursos de um navegador **129**

Tipos de certificados **131**

Cookies **131**

Exercício de fixação 2 – Cookies **132**

Segurança no navegador **133**

Pagamentos na internet **133**

Roteiro de Atividades 7 **135**

Atividade 7.1 – Recurso do SSH **135**

Atividade 7.2 – Uso de criptografia em arquivos **135**

Atividade 7.3 – Criptografando arquivos no Linux **135**

8. Política de segurança da informação

Introdução **137**

Exercício de nivelamento 1 – Políticas de segurança da informação **138**

Análise de risco **138**

Identificação, classificação, valoração e criticidade **138**

Vulnerabilidades e ameaças **140**

Risco **140**

Impacto **141**

Exercício de fixação 1 – Risco, ameaças e vulnerabilidades **141**

Metodologias para análise de risco **142**

Construindo uma política de segurança **142**

Orientações da norma ISO 27001 **142**

Norma ISO 27002 **143**

Orientações do NBSO **143**

Orientações do CERT.BR **144**

Acceptable Use Police (AUP) **145**

Exemplo de política de segurança **145**

Mensurando **145**

Calculando **146**

Valor final **147**

Roteiro de Atividades 8 149

Atividade 8.1 – Elaboração de políticas **149**

Atividade 8.2 – Auditoria em Microsoft Windows **149**

Atividade 8.3 – Aumentando a segurança da sua estação de trabalho **149**

Atividade 8.4 – Calculando o impacto do mau uso da web **150**

9. Ameaças recentes

Exercício de nivelamento 1 – Ameaças recentes **151**

Introdução **151**

Phishing **152**

Formas atuais de phishing **153**

Exercício de fixação 1 – Phishing **153**

Programa malicioso **154**

Link para programa malicioso **154**

Página falsificada de comércio eletrônico ou internet banking **155**

E-mail contendo formulário **155**

Uso de computador alheio **156**

Roubo de identidade **156**

Golpes em sites de comércio eletrônico e compras coletivas **157**

Cuidados ao usar comércio eletrônico e internet banking **157**

Proteção antiphishing **157**

Pharming **158**

Prevenção **158**

Exercício de fixação 2 – Pharming **159**

Bot **159**

Rootkit **159**

Tecnologia rootkit em DRM da Sony **160**

Kernel malware **160**

Mailbot aka Costrat **160**

Spear phishing **161**

Páginas contaminadas **161**

Redes sociais **162**

Como se proteger **163**

Exercício de fixação 3 – Redes sociais **163**

SANS Top 20 Internet Security Attack Targets **163**

Como se manter atualizado, quando o assunto é segurança? **164**

Roteiro de Atividades 9 167

Atividade 9.1 – Conceitos de malware **167**

Atividade 9.2 – Antirootkit **167**

10. Fundamentos de segurança da informação

Introdução **169**

Fundamentos **170**

Conceitos básicos **171**

Padrões existentes de segurança **172**

RFC 2196: Site Security Handbook **172**

RFC 3227 **173**

ISO 27001 **174**

Cobit **177**

Outras normas, padrões e leis **178**

Família 27000 **178**

Sarbanes Oxley (SOX) **179**

PCI-DSS **179**

Documentação GSI/DSIC **180**

Roteiro de Atividades 10 181

Atividade 10.1 – Segurança da informação **181**

Atividade 10.2 – Vulnerabilidades **181**

Atividade 10.3 – Descartes **181**

Bibliografia 183

Escola Superior de Redes

A Escola Superior de Redes (ESR) é a unidade da Rede Nacional de Ensino e Pesquisa (RNP) responsável pela disseminação do conhecimento em Tecnologias da Informação e Comunicação (TIC). A ESR nasce com a proposta de ser a formadora e disseminadora de competências em TIC para o corpo técnico-administrativo das universidades federais, escolas técnicas e unidades federais de pesquisa. Sua missão fundamental é realizar a capacitação técnica do corpo funcional das organizações usuárias da RNP, para o exercício de competências aplicáveis ao uso eficaz e eficiente das TIC.

A ESR oferece dezenas de cursos distribuídos nas áreas temáticas: Administração e Projeto de Redes, Administração de Sistemas, Segurança, Mídias de Suporte à Colaboração Digital e Governança de TI.

A ESR também participa de diversos projetos de interesse público, como a elaboração e execução de planos de capacitação para formação de multiplicadores para projetos educacionais como: formação no uso da conferência web para a Universidade Aberta do Brasil (UAB), formação do suporte técnico de laboratórios do Proinfo e criação de um conjunto de cartilhas sobre redes sem fio para o programa Um Computador por Aluno (UCA).

A metodologia da ESR

A filosofia pedagógica e a metodologia que orientam os cursos da ESR são baseadas na aprendizagem como construção do conhecimento por meio da resolução de problemas típicos da realidade do profissional em formação. Os resultados obtidos nos cursos de natureza teórico-prática são otimizados, pois o instrutor, auxiliado pelo material didático, atua não apenas como expositor de conceitos e informações, mas principalmente como orientador do aluno na execução de atividades contextualizadas nas situações do cotidiano profissional.

A aprendizagem é entendida como a resposta do aluno ao desafio de situações-problema semelhantes às encontradas na prática profissional, que são superadas por meio de análise, síntese, julgamento, pensamento crítico e construção de hipóteses para a resolução do problema, em abordagem orientada ao desenvolvimento de competências.

Dessa forma, o instrutor tem participação ativa e dialógica como orientador do aluno para as atividades em laboratório. Até mesmo a apresentação da teoria no início da sessão de aprendizagem não é considerada uma simples exposição de conceitos e informações. O instrutor busca incentivar a participação dos alunos continuamente.

As sessões de aprendizagem onde se dão a apresentação dos conteúdos e a realização das atividades práticas têm formato presencial e essencialmente prático, utilizando técnicas de estudo dirigido individual, trabalho em equipe e práticas orientadas para o contexto de atuação do futuro especialista que se pretende formar.

As sessões de aprendizagem desenvolvem-se em três etapas, com predominância de tempo para as atividades práticas, conforme descrição a seguir:

Primeira etapa: apresentação da teoria e esclarecimento de dúvidas (de 60 a 90 minutos).
O instrutor apresenta, de maneira sintética, os conceitos teóricos correspondentes ao tema da sessão de aprendizagem, com auxílio de slides em formato PowerPoint. O instrutor levanta questões sobre o conteúdo dos slides em vez de apenas apresentá-los, convidando a turma à reflexão e participação. Isso evita que as apresentações sejam monótonas e que o aluno se coloque em posição de passividade, o que reduziria a aprendizagem.

Segunda etapa: atividades práticas de aprendizagem (de 120 a 150 minutos).
Esta etapa é a essência dos cursos da ESR. A maioria das atividades dos cursos é assíncrona e realizada em duplas de alunos, que acompanham o ritmo do roteiro de atividades proposto no livro de apoio. Instrutor e monitor circulam entre as duplas para solucionar dúvidas e oferecer explicações complementares.

Terceira etapa: discussão das atividades realizadas (30 minutos).
O instrutor comenta cada atividade, apresentando uma das soluções possíveis para resolvê-la, devendo ater-se àquelas que geram maior dificuldade e polêmica. Os alunos são convidados a comentar as soluções encontradas e o instrutor retoma tópicos que tenham gerado dúvidas, estimulando a participação dos alunos. O instrutor sempre estimula os alunos a encontrarem soluções alternativas às sugeridas por ele e pelos colegas e, caso existam, a comentá-las.

Sobre o curso

O curso fornece conhecimentos introdutórios da área de segurança, através da apresentação dos conceitos básicos sobre segurança de redes, apoiados por atividades práticas em laboratório. Aborda a história da segurança física e lógica, apresenta um panorama atual da área (vulnerabilidades, tipos de ataque mais comuns, estatísticas), arquitetura TCP/IP (endereçamento, serviços TCP/IP, protocolos, DNS, roteamento), criptografia, políticas, padrões e normas de segurança da informação.

A quem se destina

Profissionais de qualquer instância da área de TI que queiram adquirir os conhecimentos básicos sobre segurança de redes. Como se trata de um curso introdutório, profissionais de outras áreas com interesse no tema também podem participar, desde que possuam como pré-requisitos conhecimentos básicos de computação.

Convenções utilizadas neste livro

As seguintes convenções tipográficas são usadas neste livro:

Itálico
Indica nomes de arquivos e referências bibliográficas relacionadas ao longo do texto.

`Largura constante`

Indica comandos e suas opções, variáveis e atributos, conteúdo de arquivos e resultado da saída de comandos. Comandos que serão digitados pelo usuário são grifados em negrito e possuem o prefixo do ambiente em uso (no Linux é normalmente # ou $, enquanto no Windows é C:\).

Conteúdo de slide 
Indica o conteúdo dos slides referentes ao curso apresentados em sala de aula.

Símbolo 
Indica referência complementar disponível em site ou página na internet.

Símbolo 
Indica um documento como referência complementar.

Símbolo 
Indica um vídeo como referência complementar.

Símbolo 
Indica um arquivo de aúdio como referência complementar.

Símbolo 
Indica um aviso ou precaução a ser considerada.

Símbolo 
Indica questionamentos que estimulam a reflexão ou apresenta conteúdo de apoio ao entendimento do tema em questão.

Símbolo 
Indica notas e informações complementares como dicas, sugestões de leitura adicional ou mesmo uma observação.

Permissões de uso

Todos os direitos reservados à RNP.
Agradecemos sempre citar esta fonte quando incluir parte deste livro em outra obra.
Exemplo de citação: PEIXINHO, Ivo de Carvalho; AMATTE, Fernando Pompeo. *Introdução à Segurança de Redes*. Rio de Janeiro: Escola Superior de Redes, RNP, 2013.

Comentários e perguntas

Para enviar comentários e perguntas sobre esta publicação:
Escola Superior de Redes RNP
Endereço: Av. Lauro Müller 116 sala 1103 – Botafogo
Rio de Janeiro – RJ – 22290-906
E-mail: info@esr.rnp.br

Sobre os autores

Ivo de Carvalho Peixinho é Bacharel em Ciência da Computação pela UFBA e Especialista em Gestão de Segurança da Informação pela UnB. Possui mais de 15 anos de experiência na área de Segurança da Informação. Foi Diretor Técnico na XSite Consultoria e Tecnologia e Analista de Suporte na Universidade Federal da Bahia. Em 2004 atuou como Analista de Segurança Sênior no CAIS/RNP por dois anos, e atualmente é Perito Criminal Federal do Departamento de Polícia Federal desde 2007, lotado atualmente no Serviço de Repressão a Crimes Cibernéticos - SRCC/CGPFAZ/DICOR/DPF. É professor de pós-graduação nas disciplinas de Análise Forense em Sistemas Unix e Análise de Malware, e é palestrante em diversos eventos nacionais e internacionais como GTS, Seginfo, CNASI, ICCyber e FIRST.

Fernando Pompeo Amatte tem mais de 20 anos de experiência na área de segurança da informação e possui as mais respeitadas certificações do mercado da segurança, como CISSP, GCIH e MCSO. Com experiência em provedores de acesso de grande porte, trabalhou em empresas multinacionais de telecomunicações e setor financeiro. Atua como consultor de segurança da informação e como professor nos cursos de pós-graduação de instituições na região de Campinas. Pesquisador nas áreas de análise de malware e análise forense, é também perito de informática para o Tribunal Regional do Trabalho de Campinas.

Edson Kowask Bezerra é profissional da área de segurança da informação e governança há mais de quinze anos, atuando como auditor líder, pesquisador, gerente de projeto e gerente técnico, em inúmeros projetos de gestão de riscos, gestão de segurança da informação, continuidade de negócios, PCI, auditoria e recuperação de desastres em empresas de grande porte do setor de telecomunicações, financeiro, energia, indústria e governo. Com vasta experiência nos temas de segurança e governança, tem atuado também como palestrante nos principais eventos do Brasil e ainda como instrutor de treinamentos focados em segurança e governança. É professor e coordenador de cursos de pós-graduação na área de segurança da informação, gestão integrada, de inovação e tecnologias web. Hoje atua como Coordenador Acadêmico de Segurança e Governança de TI da Escola Superior de Redes.

1

Introdução, histórico e princípios básicos de segurança

objetivos

Apresentar os conceitos básicos de segurança, seu histórico de evolução e os princípios que devem nortear a conduta de um profissional nessa área; indicar ao aluno fontes de estudo, treinamento multimídia e listas de discussão sobre o tema.

conceitos

Segurança, listas de discussão de segurança e ameaças digitais.

Introdução

Este capítulo é uma introdução que apresenta um breve histórico da segurança da informação, mostrando os marcos que impulsionaram esse desenvolvimento até os dias atuais. Apresenta também os princípios básicos que devemos exercitar para alcançar as três características fundamentais da segurança:

- Confidencialidade;
- Integridade;
- Disponibilidade.

Exercício de nivelamento 1
Informação

O que é informação?

Segurança da informação

O que é informação?

- Ativo que tem valor para a organização.
- É o bem ativo mais valioso da organização?

Onde está a informação?

- Papel.
- Banco de dados etc.



Por que proporcionar segurança para a informação?

O que é segurança da informação?

- É o conjunto de dados, imagens, textos e outras formas de representação usadas para os valores da instituição, associados ao seu funcionamento e/ou manutenção das suas vantagens competitivas.

Características básicas da segurança da informação:

- Confidencialidade:
  - A informação é acessada somente por pessoas autorizadas?
- Integridade:
  - Há garantia de que a informação acessada não foi alterada?
- Disponibilidade:
  - A informação está acessível no momento necessário?

Ainda de acordo com a norma NBR ISO/IEC 17799:2001, a segurança da informação consiste na preservação de três características básicas:

- **Confidencialidade**: garantia de que a informação seja acessada somente por pessoas autorizadas.
- **Integridade**: certeza de que a informação é exata e completa e os métodos de processamento, seguros.
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

O conceito inicial de confidencialidade, integridade e disponibilidade deve ser expandido para incluir mais alguns termos:

- **Autenticidade**: há garantia da identidade dos participantes da comunicação? Quem gerou a informação é mesmo quem nós pensamos ser?
- **Legalidade**: a informação ou sua posse está em conformidade com as legislações institucionais, nacionais e internacionais vigentes? Copiar mídia que contém informação é legal? A posse da informação é legal?
- **Não repúdio**: conseguimos a garantia de que um agente não consiga negar uma ação que criou ou modificou uma informação?
- **Auditoria**: existe a possibilidade de rastreamento do histórico dos fatos de um evento assim como a identificação dos envolvidos?

Segurança de redes



Áreas da segurança da informação:

- Segurança física.
- Segurança lógica.
- Segurança de pessoas.
- Segurança de computadores.
- Segurança de redes.
- Segurança de aplicativos etc.

Exercício de fixação 1
Segurança de redes

Quais as áreas da segurança de rede?

Quais são as três características básicas da segurança da informação?

Anos 50 e 60

1950: surge o primeiro padrão de segurança: Transient Electromagnetic Pulse Surveillance Technology (Tempest), criado pelo governo dos EUA.

- Estudo da escuta de sinais eletromagnéticos que emanam dos computadores.
- Vulnerabilidade: obtenção de dados por radiação eletromagnética.

1967: criação da força-tarefa do DoD (Department of Defense – o Departamento de Defesa americano).

- Realizou estudos sobre potenciais ameaças a computadores, identificou vulnerabilidades, introduziu métodos de controle de acesso para computadores, sistemas de rede e informações.

O DoD é o órgão do governo americano que mais contribuiu para o desenvolvimento de vários projetos, não só na área de segurança, mas também em outras áreas, como, por exemplo, o próprio projeto que deu origem à internet, conhecido como Arpanet.

Em segurança, além do Security Controls for Computer Systems (SCCS), o DoD contribuiu para o surgimento do Trusted Computer System Evaluation Criteria (TCSEC), que ficou conhecido mundialmente como Orange Book (Livro Laranja), referência mundial para sistemas seguros de computação.

1969: surge a Arpanet (futura internet), rede de computadores descentralizada ligando:

- Stanford Research Institute.
- University of Utah.
- University of California (Los Angeles).
- University of California (Santa Barbara).

Nesse ano surge ainda a primeira versão do Unix, desenvolvido por Ken Thompson nos Laboratórios Bell. Derivado do Multics, foi chamado primeiramente de Unics; Brian Kernighan, parodiando, finalmente chamou-o de Unix.

Anos 70

1970: publicação pelo DoD do Security Controls for Computer Systems (SCCS).

- SCCS: documento importante na história da segurança de computadores.
- Em 1976, deixou de ser confidencial.

1970: iniciativas patrocinadas pelo DoD em conjunto com a indústria:



- Tiger teams.
- Estudos sobre segurança e desenvolvimento de sistemas operacionais seguros.
- Surgiram conceitos de segurança, como:
  - Política de segurança.
  - Modelos de segurança.
  - Modelos matemáticos de segurança.

Subproduto da guerra fria, o Data Encryption Standard (DES), um algoritmo para cifrar dados, foi adotado pelo governo dos EUA como método oficial de proteção a dados não confidenciais em computadores das agências do governo. Foi muito utilizado nas implementações dos sistemas de autenticação Unix, como Linux, FreeBSD, Solaris etc. Hoje o DES não é mais usado, pois se tornou vulnerável com o grande avanço do poder computacional, tendo sido substituído atualmente pelo MD5 e pelo SHA (algoritmos de hash criptográfico).

O *Computer Fraudand Abuse Act,* criado em 1986, proibia o acesso não autorizado a computadores do governo, prevendo uma pena de cinco mil dólares ou o dobro do valor obtido pelo acesso, além de cinco anos de prisão. Uma medida importante, porque introduziu a punição judicial.

O *Computer Security Act,* criado em 1988, obrigava qualquer computador do governo que processasse dados confidenciais a ter um plano de segurança para a administração e uso do sistema. Além disso, exigia que todo o pessoal envolvido recebesse treinamento periódico de segurança. Sua importância: os órgãos governamentais agora eram obrigados a possuírem uma política de segurança.

1975: Arpanet completamente funcional; o Unix torna-se o sistema operacional oficial.



1977: adotado o *Data Encryption Standard* (DES), padrão de criptografia que durou 20 anos.

Anos 80

1982: adotado o protocolo TCP/IP como padrão da Arpanet.



1983: lançado o Trusted Computer System Evaluation Criteria (TCSEC):

- Cognominado *Orange Book*, bíblia do desenvolvimento de sistemas de computação seguros.
- Classificação feita em níveis D, C, B e A, na ordem crescente de segurança.

Sumary of "Orange Book" security features

Criterion	C1	C2	B1	CMW	B2	B3	A1
Identification and Authentication (IAA)							
Discretionary Access Control (DAC)							
System Architecture (Least Privilege)							
Security Testing							
Auditing							
Object Reuse							
Labeling							
Label Integrity and Label Export							
Multilevel Export							
Single-Level Export							
Printout Labeling							
Mandatory Access Control (MAC)							
Sensitivity Labels							
Device Labeling							
Trusted Path							
Covert Channel Analysis							
Trusted Facility Management							
Configuration Management							
Trusted Recovery							
Trusted Distribuition							
Information Labels							
Authorizations							

Figura 1.1
Os assuntos abordados no Orange Book.

1985: primeira vez em que o nome "internet" foi usado para definir a Arpanet.

Subprodutos da guerra fria.

1986: Computer Fraud and Abuse Act:

- Proibia acesso não autorizado a computadores do governo.
- Pena pecuniária de cinco mil dólares ou o dobro do valor obtido pelo acesso.
- Pena de cinco anos de prisão.

1988: Computer Security Act:

- Computador do governo que guardasse dados confidenciais deveria ter plano de segurança para administração e uso do sistema.
- Exigia que pessoal envolvido recebesse treinamento periódico sobre segurança.

Ano de 1988

O estudante da Universidade de Cornell escreveu um programa capaz de:

- Autorreplicar-se e se autopropagar, chamado de "*worm*", pois rastejava pela rede.
- Explorar vulnerabilidades conhecidas dos servidores:
  - Sendmail.
  - Fingerd.
- Infectou e indisponibilizou milhares de servidores.



Figura 1.2
Robert T. Morris, criador do "Morris Worm", primeiro worm de computador da internet.

Em 2 de novembro de 1988, Robert T. Morris, um estudante de pós-graduação da Universidade de Cornell, escreveu um programa capaz de se autorreplicar e de se autopropagar, que foi chamado de worm, por sua capacidade de rastejar pela rede. Ele lançou o programa dentro do MIT, mas logo se deu conta de que o programa estava se replicando e reinfectando as máquinas numa proporção muito maior do que ele havia imaginado.

Diversos computadores foram afetados, incluindo os de universidades, *sites* militares e instalações de pesquisas médicas. O worm de Morris chamou a atenção sobre a necessidade de proteger os computadores que faziam parte da internet. Robert T. Morris foi condenado por violação do *Computer Fraudand Abuse Act*: três anos de prisão, 400 horas de serviços comunitários e multa de US$ 10.050,00.

Uma das consequências mais importantes foi a criação do Computer Emergency Response Team (CERT), pela Defense Advanced Research Projects Agency (DARPA). O CERT até hoje é uma das entidades mais importantes na coordenação e informação sobre problemas de segurança.

Saiba mais sobre o CERT acessando o endereço http://www.cert.org.

Ano de 2001

- Worm Code Red.
- Explorava uma falha de "Buffer Overflow" nos servidores web da Microsoft.
- Correção para o problema havia saído um mês antes.

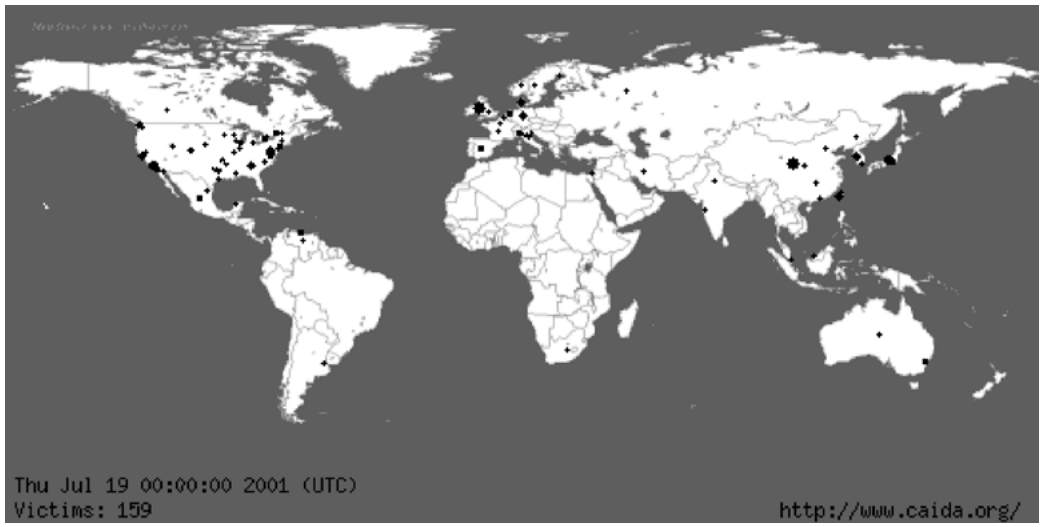


Figura 1.3
Infecção pelo worm Code Red.

Era explorada uma vulnerabilidade conhecida do IIS, servidor web da Microsoft. Estima-se que tenha infectado cerca de 300 mil computadores por dia.

Ano de 2003

SQL Slammer Worm:

- Infectou 75 mil computadores em dez minutos.
- Causou negação de serviço em algumas máquinas, deixando outras muito lentas.
- Explorava uma falha de "Buffer Overflow" nos servidores SQL Server da Microsoft.
- Correção para a falha havia saído seis meses antes (MS02-039).

Ano de 2009

Confiker:

- Infectou entre 9 e 15 milhões de máquinas.
- Utilizava falha em diversas versões do sistema operacional da Microsoft.
- Tentava descobrir senhas utilizando força bruta (tentativa e erro).
- Utilizava várias técnicas para infectar máquinas.
- Varias versões do malware (com possibilidade de atualização).
- Pico das infecções em janeiro de 2009.
- A correção para a falha havia saído em outubro de 2008 (MS08-067).

Segurança no Brasil

1988: The Academic Network at São Paulo (ANSP), via Fapesp, conectou-se com a internet em Chicago (Fermi National Laboratory), nos EUA.

1989: o Ministério da Ciência e Tecnologia criou a Rede Nacional de Ensino e Pesquisa (RNP – http://www.rnp.br), com o objetivo de construir uma infraestrutura de rede internet nacional de âmbito acadêmico.

1995: a internet comercial teve início no Brasil. Na mesma época foi criado o Comitê Gestor da Internet no Brasil (http://www.cgi.br).

O NIC.BR é responsável por registros de domínios e associação de endereços IP. O NIC. BR Security Office (antigo NBSO, atualmente CERT.BR) é responsável por receber, revisar e responder a relatos de incidentes de segurança envolvendo a internet brasileira.

O Centro de Atendimento a Incidentes de Segurança (CAIS – http://www.rnp.br/cais) atua na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes.

Atividades do CAIS:

- Atendimento a incidentes de segurança;
- Coordenação com grupos de segurança já existentes;
- Fomento à criação de novos grupos de segurança no país;
- Disseminação de informações na área de segurança em redes;
- Divulgação de recomendações e alertas;
- Testes e recomendação de ferramentas de segurança;
- Recomendação de políticas para a RNP;
- Recomendação de políticas para os Pontos de Presença (PoPs);
- Recomendação de políticas para o *backbone* da RNP.

Ano de 2011

Junho de 2011: sites da Presidência e do governo brasileiro sofreram ataques de negação de serviço.

- Grupo chamado "LulzSecBrazil" assumiu a autoria dos ataques.
- Mais de dois bilhões de tentativas de acesso em um curto período.

Conheça o ataque que ficou conhecido como # OPWEEKPAYMENT part 2, em http://oglobo.globo.com/tecnologia: "Hackers fazem a terceira vítima e tiram site do Banco do Brasil do ar".

Ano de 2012

- **Janeiro de 2012**: operação #OPWEEKPAYMENT (Operação Semana de Pagamento), realizada por um grupo de pessoas que se denominam AnonymousBR, causou lentidão e indisponibilidade em alguns sites de bancos brasileiros.
- **Outubro de 2012**: os sites da Caixa Econômica Federal, Banco do Brasil, Nota fiscal Eletrônica de São Paulo e da Febraban ficaram fora do ar.

CSIRTs no Brasil

- Gradualmente e com muita relevância, grupos de Resposta a Incidentes de Segurança se organizam e prestam direta ou indiretamente serviços aos usuários da internet, seja através de documentos, notificações de problemas ou mesmo de lista de segurança.
- No site do CAIS encontramos uma lista dos principais CSIRTs atuantes no Brasil:
  - http://www.rnp.br/cais/csirts.html

O Centro de Atendimento a Incidentes de Segurança da RNP (CAIS) reconhece e apoia alguns grupos de segurança brasileiros (CSIRTs, do inglês *Computer Security Incident Response Teams*).

Grupos e seus endereços na internet:

CTIR/GOV
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal
http://www.ctir.gov.br

CCTIR/EB

Centro de Coordenação para Tratamento de Incidentes de Rede do Exército
http://stir.citex.eb.mil.br

TRI-UFRGS

Time de Resposta a Incidentes de Segurança da UFRGS
http://www.ufrgs.br/tri/

Cert-RS

Centro de Emergência em Segurança da Rede Tchê
http://www.cert-rs.tche.br/

CEO/Rede Rio

Coordenação de Engenharia Operacional da Rede Rio
http://www.rederio.br/site/node/8

CSIRT PoP-SE

Grupo de Resposta a Incidentes de Segurança do PoP-SE
http://www.csirt.pop-se.rnp.br/

GRC/Unesp

Grupo de Redes de Computadores
http://grc.unesp.br/

GSR/Inpe

Grupo de Segurança de Sistemas e Redes do Inpe
http://www.inpe.br/

Naris

Núcleo de Atendimento e Resposta a Incidentes de Segurança (UFRN)
http://naris.info.ufrn.br/

NOE

Núcleo de Operações Especiais de Segurança (PoP-RN)
http://www.pop-rn.rnp.br/noe/

Unicamp CSIRT

http://www.security.unicamp.br/

USP CSIRT

http://www.security.usp.br/

Informações extraídas da página do CAIS.

Decreto nº 3505, de 13 de junho de 2000

Instituiu a política de segurança da informação nos órgãos e entidades da administração pública federal.

- Determinou objetivos para a política de segurança da informação.
- Atribuiu as diretrizes da política ao Conselho de Defesa Nacional, assessorado pelo Comitê Gestor da Segurança da Informação.
- Incluiu a participação da Agência Brasileira de Inteligência (ABIN) no processo de condução da política.
- Criou o Comitê Gestor da Segurança da Informação.

Consulte o Decreto no 3.505, de 13 de junho de 2000 em https://www.planalto.gov.br.

DSIC

Departamento de Segurança da Informação e Comunicações (DSIC):

- Ligado ao Gabinete de Segurança Institucional (GSI).
- Responsável pelo planejamento e coordenação de segurança da informação na Administração Pública Federal.

O DSIC coloca à disposição uma vasta documentação sobre segurança da informação e comunicações. Pode ser acessado em http://dsic.planalto.gov.br/.

Princípios básicos de segurança

Nada e nenhum tipo de informação é mais importante que a vida humana.

Menor privilégio (least privilege):

- Princípio fundamental. Define que cada objeto (usuário, administrador, programa etc.) deve possuir apenas o mínimo de privilégio.

Defesa em profundidade (defense in depth):

- Não se deve confiar em um único mecanismo de segurança; deve-se sempre utilizar defesas redundantes.

Gargalo (choke point):

- Obriga intrusos a usar um canal estreito que pode ser monitorado e controlado.

- **Menor privilégio**: por exemplo, ao criar um usuário de correio eletrônico em um sistema operacional, o administrador deve fazê-lo com os menores privilégios possíveis, não lhe permitindo, por exemplo, acesso via shell para o servidor.
- **Defesa em profundidade**: ao se conectar a rede de uma instituição à internet, por exemplo, deve-se obrigatoriamente usar um firewall institucional. Ao mesmo tempo, deve-se ativar o firewall em cada estação de cliente da rede interna.
- **Gargalo**: ao se conectar a rede de uma instituição à internet, deve-se obrigatoriamente usar um *firewall*, o único canal de conexão, sempre monitorado e controlado.
- **Ponto mais fraco**: o ponto mais fraco de uma rede é sempre o ser humano. Cuidado com ataques de engenharia social.

Exercício de fixação 2
Princípios básicos de segurança

Explique o que é “menos privilégio” e cite um exemplo.

Explique o que é “defesa em profundidade” e cite um exemplo.

Princípios básicos de segurança



Falha Segura (fail-secure):

- Quando o sistema de segurança falha, deve falhar de tal forma que bloqueie só acessos.

Falha Protegida (fail-safe):

- Quando o sistema de segurança falha, deve falhar de tal forma que libere os acessos.

Participação universal (universal participation):

- O sistema de segurança deve envolver todos os objetos (pessoas).

Diversidade de defesa (diversity of defense):

- Não é um princípio geral. Afirma que o uso de sistemas diferentes torna o sistema (como um todo) mais seguro.
- **Falha Segura**: por exemplo, em uma configuração de Falha Segura, caso ocorra uma falha elétrica, as portas ficarão bloqueadas por padrão.
- **Falha Protegida**: em uma configuração de Falha Protegida, por exemplo, caso ocorra uma falha elétrica, as portas ficarão abertas por padrão.



Para pensar

A maioria dos termos que utilizamos em segurança da informação foi herdada da língua inglesa. Assim, algumas traduções não ficam muito claras na língua portuguesa. É o exemplo das palavras “safe” e “secure”. Em uma tradução livre, poderíamos dizer que as duas palavras significam segurança. Porém, “safe” está relacionada à segurança no intuito de proteção de pessoas. E “security” refere-se a medidas contra coisas inesperadas ou perigosas.

- **Participação universal**: por exemplo, dentro de uma instituição, quais funcionários estão submetidos à política de segurança? Todos, pois a participação na política é universal.
- **Diversidade de defesa**: esse princípio é polêmico. Exemplo: para vários servidores poderíamos usar vários sistemas operacionais, o que aumentaria enormemente o custo administrativo. Mas, para os mesmos servidores, é importante que todos tenham diferentes senhas de *root*. Outro exemplo seria ter um servidor de antivírus institucional diferente do programa de antivírus nas estações dos clientes da rede.
- **Simplicidade**: a segurança habita em meio à simplicidade. As coisas simples são fáceis de entender. O entendimento é fundamental para conhecer o nível de segurança. Exemplo: o programa servidor de correio sendmail é complexo; isso talvez seja a principal razão de ele ter se tornado tão inseguro. Outros programas fáceis de usar e programar, como o servidor de correio postfix, são considerados muito mais seguros (vale notar que existem diversos outros motivos para um programa/software/sistema ser considerado inseguro.)

Roteiro de Atividades 1

Atividade 1.1 – Listas e informações complementares de segurança

1. Visite e assine listas nos sites do CAIS, da Módulo e da Microsoft no Brasil:

- http://www.rnp.br/cais/listas.php
- http://www.modulo.com.br/comunidade/newsletter
- http://www.microsoft.com/brasil/security/alertas.mspx

2. Visite e assine as listas de algumas das instituições mais respeitadas sobre segurança no mundo:

- http://www.securityfocus.com/archive/
- http://www.sans.org/newsletters/

Você é capaz de dizer em poucas palavras a diferença entre as listas assinadas, principalmente no foco de abordagem?

3. O Cert.br disponibiliza uma cartilha com informações sobre segurança na internet através do link cartilha.cert.br. Acesse o fascículo "Segurança na internet". Você consegue listar quais são os riscos a que estamos expostos com o uso da internet, e como podemos nos prevenir?

4. Veja os vídeos educativos sobre segurança do NIC.BR em http://antispam.br/videos/, pesquise na internet e indique um exemplo relevante de cada categoria:

- Vírus;
- Worms;
- Cavalos de troia (trojan horses);
- Spyware;
- Bot;
- Engenharia social;
- Phishing.

5. O site Antispam.br apresenta um conjunto de políticas e padrões chamados de "Gerência de Porta 25", que podem ser utilizados em redes de usuários finais ou de caráter residencial para:

- Mitigar o abuso de proxies abertos e máquinas infectadas para o envio de spam;
- Aumentar a rastreabilidade de fraudadores e spammers.

Saiba mais

Acesse a "Recomendação para a adoção de gerência de porta 25" em http://www.antispam.br/ e conheça as ações que os órgãos de segurança da informação no Brasil estão tomando para diminuir a quantidade de spams que trafegam diariamente na internet.

2

Conceitos de segurança física e segurança lógica

objetivos

Apresentar os conceitos básicos de segurança física, segurança lógica e suas diferenças; as principais tecnologias disponíveis, sua aplicação, e os níveis de segurança física, de acordo com a norma NBR ISO/IEC 27001:2005.

conceitos

Segurança física, soluções open source e níveis de segurança.

Introdução

A área de segurança de redes é parte de uma área maior chamada de segurança da informação. Para proteger a informação, nossa preocupação deve começar no próprio ambiente físico que compõe a instalação onde a informação se localiza. Depois, partiremos para o ambiente computacional, onde a proteção se dará logicamente por meio de programas (*softwares*) e protocolos. Neste capítulo, trataremos especificamente de segurança em sistemas computacionais.

Exercício de nivelamento 1
Conceitos de segurança física e segurança lógica

O que é segurança física? Cite um exemplo.

Segurança física

- Segurança externa e de entrada.
- Segurança da sala de equipamentos.
- Segurança dos equipamentos.
- Redundância.
- Segurança no fornecimento de energia.
- Salvaguarda (*backup*).
- Descarte da informação.

A segurança física abrange todo o ambiente onde os sistemas de informação estão instalados, incluindo o prédio, portas de acesso, trancas, pisos, salas e os próprios computadores. Incorpora as áreas da engenharia civil e elétrica.

A norma NBR ISO/IEC 17799:2001 divide a área da segurança física da seguinte forma:

Áreas de segurança

1. Perímetro da segurança física.
2. Controles de entrada física.
3. Segurança em escritórios, salas e instalações de processamento.
4. Trabalho em áreas de segurança.
5. Isolamento das áreas de expedição e carga.

Segurança dos equipamentos

1. Instalação e proteção de equipamentos.
2. Fornecimento de energia.
3. Segurança do cabeamento.
4. Manutenção de equipamentos.
5. Segurança de equipamentos fora das instalações.
6. Reutilização e alienação segura de equipamentos.

Controles gerais

1. Política de mesa limpa e tela limpa.
2. Remoção de propriedade.

Segurança externa e de entrada



Consiste na proteção da instalação onde os equipamentos estão localizados contra a entrada de pessoas não autorizadas.

Atua também na prevenção de catástrofes como:

- Enchentes.
- Raios.
- Incêndios etc.

Mecanismos de controle de acesso físico nas entradas e saídas como:

- Travas.
- Alarmes.
- Grades.
- Sistemas de vigilância etc.

A localização do prédio é importante quando se trata de enchentes ou raios. Em locais sujeitos a enchentes, a sala de computadores deve ficar nos andares superiores. Em áreas abertas ou sujeitas a queda de raios, é recomendada a utilização de um para-raios.
É recomendável utilizar, sempre que possível, barreiras físicas, como muros externos.

O controle de acesso pode ser realizado por um vigilante humano ou por um sistema de vigilância, ou até pelos dois simultaneamente. A permissão de acesso de todos os visitantes deve ser verificada e os horários de entrada e saída devem ser registrados para auditoria.

O controle de acesso deve restringir os setores aos quais o funcionário ou visitante deve ter acesso. Essa restrição deve, se possível, ser reforçada por meio de portas com senha, crachá ou cartão de acesso.



Controle de acesso: gerencia e documenta todos os acessos em ambientes, salas, andares e áreas específicas.

Pode ser interligado a vários outros sistemas, como:

- Sistema de alarme.
- Circuito Fechado de Televisão (CFTV).
- Cartão de identificação (ID cards).
- Sistemas biométricos de identificação através do reconhecimento de mão, impressão digital, face ou íris.

Equipamentos como câmeras de vídeo podem proporcionar proteção adicional para controlar a entrada e a saída de pessoas. Nesses casos, as mídias utilizadas devem ser armazenadas de forma segura, de modo a permitir auditoria posterior. Graças a *softwares* com tecnologia de ponta, os cartões de identificação com o tamanho de cartões de crédito – com ou sem foto – podem ser produzidos de maneira rápida e fácil, usando um simples PC.

CFTV
Sistema de televisão que distribui sinais provenientes de câmeras localizadas em locais específicos, para um ou mais pontos de visualização.

Os modernos circuitos de **CFTV** destacam-se em conjunto com os sistemas de alarme, além da possibilidade de fornecimento de informações valiosas para intervenção em casos de emergência.

Segurança da sala de equipamentos



Sala de equipamentos:

- Local físico onde os servidores e equipamentos de rede estão localizados.
- Acesso com controle físico específico e somente por pessoal autorizado.
- Todo acesso deve ser registrado através de algum mecanismo de entrada.
- O conteúdo da sala não deve ser visível externamente.

Essa sala deve ser protegida contra:

- Vandalismo;
- Fogo;
- Interferências eletromagnéticas;
- Fumaça;
- Gases corrosivos;
- Poeira etc.

Supressão de incêndio



Dependendo do tipo de instalação, diferentes métodos de supressão de incêndio podem e devem ser adotados. Cada opção tem seus prós e contras. Entre as opções temos:

- Extintores de incêndio tradicionais: para cada tipo de fogo, existe um tipo de extintor adequado a ser utilizado.

- Sprinklers:
  - Canos com água no teto, ativados por temperatura.
- Gases:
  - Produtos que interferem quimicamente no processo de combustão.
  - Exemplo: FM-200, NAF-S-III, CEA-410 etc.

Alguns fabricantes fornecem soluções de sala-cofre, como mostra a Figura 2.1. Essas salas, em geral, possuem revestimentos especiais e controle de acesso para proteção contra os problemas listados anteriormente.



Figura 2.1
Exemplo de sala-cofre (Fonte: Aceco TI: http://www.aceco.com.br).

Algumas recomendações básicas para tornar o ambiente da sala de equipamentos mais seguro, com pouco investimento:

- A sala deve preferencialmente ficar nos andares mais altos;
- Deve-se evitar que a sala esteja no caminho das pessoas; escolher preferencialmente uma sala de canto;
- Ter preferencialmente paredes de concreto;
- Ter preferencialmente portas de madeira de lei ou de ferro;
- Ter a porta fechada permanentemente, com tranca ou com chave;
- Ter extintor contra incêndio;
- Ter ar-condicionado que controle umidade e temperatura;
- Ter proteção contra raios solares nas janelas;
- Ter as janelas e as portas bem protegidas contra arrombamentos;
- Ter carpete ou piso elevado à prova de fogo e antiestático;
- Não ter material combustível como madeira (mesas, cadeiras e armários) e papel (livros, arquivo morto etc.);
- A sala não deve ser usada para o trabalho de qualquer funcionário. O funcionário só deve estar na sala quando houver necessidade de intervenção.
- É proibido entrar com qualquer material líquido (água ou café) ou com comida dentro da sala;
- Incentivar o uso de acesso remoto para os servidores na sala (sempre que possível com protocolos seguros, como o SSH);
- Verificar a possibilidade de uso de cabeamento aéreo;
- No nível físico: formação de perímetros e aplicação de três princípios básicos de segurança: defesa em profundidade, gargalo e diversidade de defesa.



Figura 2.2
Perímetros de segurança.

Gargalos (choke point):

- Guarita;
- Catraca;
- Porta de vidro;
- Porta de aço;
- Porta do *rack*;
- Porta da sala-cofre.

Exercício de fixação 1
Segurança em perímetro

Como é feita a segurança em perímetro na sua organização?

Segurança dos equipamentos

- Os equipamentos de rede e servidores devem estar em uma sala segura.
- Os equipamentos devem ser protegidos contra acessos indevidos no seu console, através de periféricos como teclado, *mouse* e monitor.
- Travas para disquetes ou CDs são recomendadas.
- Os equipamentos devem ser protegidos contra acessos indevidos ao interior da máquina.



Figura 2.3
Tranca para gabinete de computador.



Figura 2.4
Gabinete de computador com porta e chave.

Boas dicas que aumentam a segurança:

- Colocar senha na BIOS para impedir que terceiros tenham acesso e mudem a configuração de inicialização;
- Configuração de inicialização apenas pelo disco rígido, para impedir acessos por disquetes ou CD-ROMs;
- Proteger o console com senha;
- Não dar acesso de superusuário (root ou administrador) via console;
- Usar trava na traseira do gabinete: cadeado, etiqueta de papel e trava plástica.

Redundância

- O problema mais comum de segurança é a falha de hardware.
- O mecanismo mais importante para tolerar falhas é a redundância.
- A redundância cria alta disponibilidade, mantendo o funcionamento em caso de falhas de componentes ou sobrecargas:
  - Redundância de interface de rede.
  - Redundância de CPUs.
  - Redundância de discos (Raid).
  - Redundância de fontes de alimentação interna.
  - Redundância de servidores etc.

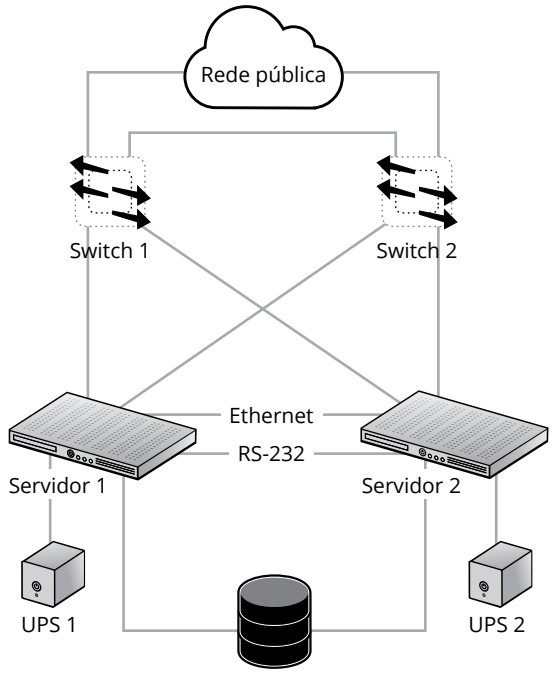


Figura 2.5
Redundância: importante contra falhas.

Foram desenvolvidas métricas para entender e antecipar as falhas:

- Mean Time Between Failures (MTBF);
- Mean Time To Repair (MTTR).

Tempo médio entre falhas (MTBF) e tempo médio de reparo (MTTR) são métricas que devem ser usadas principalmente no período de aquisição dos equipamentos. Devem ser escolhidos periféricos que tenham o maior MTBF. Atualmente discos rígidos SATA possuem 1,2 milhão de horas de MTBF (137 anos).

Devem ser escolhidas as empresas fornecedoras que tenham o menor MTTR. Um valor típico de MTTR é de 4 horas *on-site* (garantia de atendimento).

- Raid é a sigla de Redundant Array of Inexpensive (Independent) Disks, conjunto redundante de discos independentes ou de baixo custo.
- Implementado por:
  - Controladora física (hardware).
  - Através do Sistema Operacional (software).
- **Redundant**: dados redundantes em múltiplos discos fornecem tolerância a falhas.
- **Array**: conjunto de múltiplos discos acessados em paralelo dão vazão maior (gravação e leitura de dados).

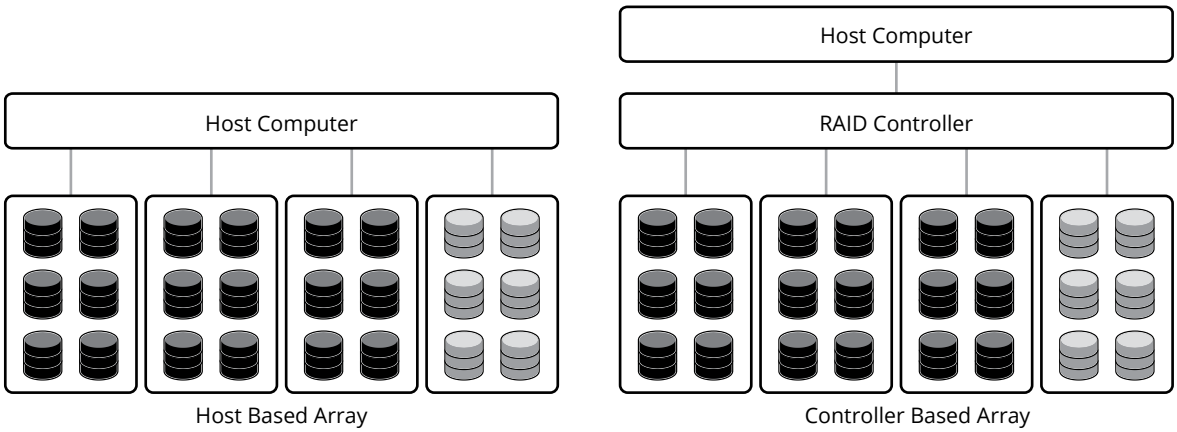


Figura 2.6
Reduntant Array of Independente Disks (Raid).

Raid é uma sigla que significa Redundant Array of Independent Disks, ou seja, conjunto redundante de discos independentes. A ideia por trás do Raid é fornecer um recurso barato de disponibilidade em discos rígidos. Os discos rígidos, por terem componentes mecânicos, são altamente sujeitos a falha; além disso, uma falha fatalmente causa perda de dados. O Raid hoje se tornou um padrão quando se fala de redundância de discos.

O Raid pode ser implementado através de uma controladora física (hardware) ou através do Sistema Operacional (software). A figura anterior mostra a diferença básica entre as duas implementações. No caso do hardware, o Sistema Operacional desconhece a existência de uma implementação Raid da controladora e visualiza o disco como se fosse um disco comum. Apesar de mais caro, o Raid via hardware tem maior desempenho, uma vez que usa um processador separado para fazer a redundância.

Toda a tecnologia Raid baseia-se em uma publicação de 1988 da Universidade de Berkeley, intitulada *A Case for Redundant Arrays of Inexpensive Disks.*

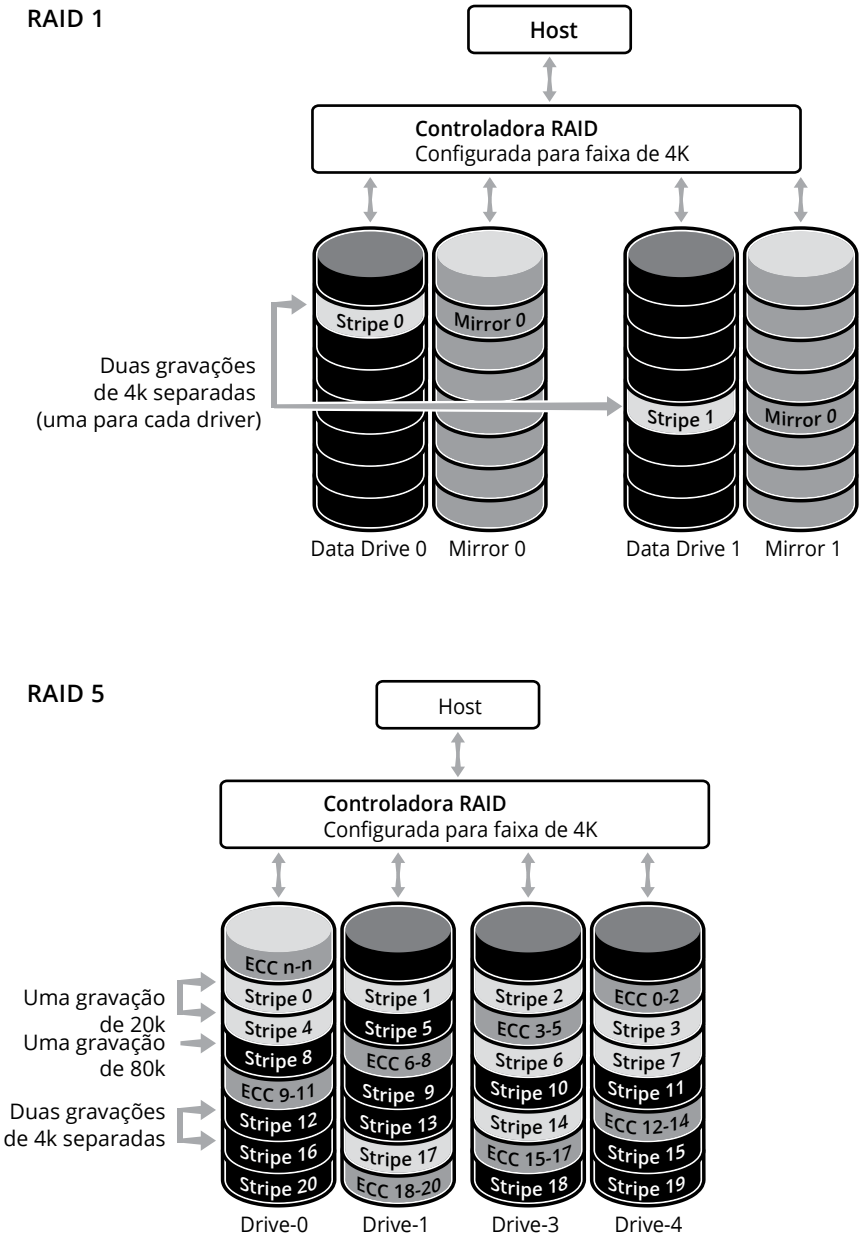


Figura 2.7
O Raid em detalhes.

Raid 0

Os dados são distribuídos através dos discos, método conhecido como data striping, sem gerar paridade ou redundância. A gravação e a leitura dos dados é feita paralelamente, uma vez que cada disco possui a sua controladora. Com isso, há grande ganho de performance; porém, por não haver redundância alguma, se um dos discos falhar, os dados são perdidos. Raid 0 é utilizado quando uma máxima performance é mais importante do que possíveis perdas de dados.

Raid 1

Os discos da matriz são divididos em dois grupos. Na escrita, os dados são gravados igualmente nos dois grupos. Na leitura, os dados podem ser lidos de qualquer um dos grupos. Normalmente, ela é feita alternando-se os discos, processo conhecido por “round robin”, mas pode haver um disco preferencial para leitura, no caso de haver um disco mais rápido que outro. Não há geração de paridade, mas sim uma redundância completa dos dados.

Esse método tem se tornado popular pela sua simplicidade e praticidade em caso de falha de um dos discos. Porém, possui as desvantagens de utilizar apenas metade da capacidade total de discos, além de não trazer nenhum aumento de performance.

Raid 5

Esse nível de Raid também utiliza o conceito de "*data striping*", mas acrescenta uma forma de obter redundância dos dados através do gerador de paridade. Para cada escrita, é gerada uma paridade calculada pela operação dos *bits* gravados. A paridade fica espalhada pelos três discos, ou seja, a cada gravação ela é gravada em um disco diferente. São necessários, no mínimo, três discos para sua implementação, sendo o espaço "desperdiçado" do conjunto devido ao armazenamento da paridade, equivalente ao espaço de um disco. É possível, com esse esquema, reconstituir os dados de um disco perdido a partir dos outros e da paridade. Caso mais de um disco falhe ao mesmo tempo, os dados não poderão ser recuperados. É um método muito empregado nos *storages* atuais, porque alia o aumento de performance à segurança oferecida pela redundância, com ótimo aproveitamento de recursos.

Existem outros tipos de Raid com combinações mais arrojadas:

Raid 6

Por ser ainda um padrão relativamente novo, não é suportado por todos os modelos controladores. Necessita de no mínimo quatro HDs e é parecido com o Raid 5, com a diferença de usar o dobro de bits de paridade, garantindo a integridade dos dados até no caso dos 2 HDs falharem ao mesmo tempo. Usando 10 HDs de 500 GB cada um em Raid 6: um total de 5 Tera no volume, com parte útil de 4 Tera de dados e 1 Tera dedicados à paridade.

Raid 0 (zero) + 1

É uma combinação dos níveis 0 (*Striping*) e 1 (*Mirroring*), onde os dados são divididos entre os discos para melhorar o rendimento, utilizando outros discos para duplicar as informações. Assim, é possível utilizar o bom rendimento do nível 0 com a redundância do nível 1. No entanto, é necessário o mínimo de 4 discos para montar um Raid desse tipo. Tais características fazem do Raid 0 + 1 o mais rápido e seguro, porém o mais caro de ser implantado.



Se um dos discos falhar, o sistema vira um Raid 0.

Raid 1+0 (ou 10)

Exige o mínimo de quatro discos rígidos. Cada par será espelhado, garantindo redundância, e os pares serão distribuídos, melhorando o desempenho. Até metade dos discos pode falhar simultaneamente, sem colocar o conjunto a perder, desde que não falhem os dois discos de um espelho qualquer — razão pela qual são usados discos de lotes diferentes de cada "lado" do espelho. É o nível recomendado para bases de dados, por ser o mais seguro e dos mais velozes, assim como qualquer outro uso onde a necessidade de economia não se sobreponha à segurança e desempenho.

Raid 50

É um arranjo híbrido que usa as técnicas de Raid com paridade em conjunção com a segmentação de dados. Um arranjo Raid 50 tem as informações segmentadas através de dois ou mais arranjos; em outras palavras, podemos compor um Raid 50 colocando dois ou mais volumes Raid 5 em Striping (Raid 0).

Tipo	Quantidade mínima de discos	Volume de dados (úteis)	Tolerância à falha
Raid 0	2	(Discos x Tamanho)	0 (nenhuma)
Raid 1	2	(1 x Tamanho)	n-1 discos
Raid 5	3	(Discos x Tamanho) – (1 x Tamanho)	1 disco
Raid 6	4	(Discos x Tamanho) – (2 x Tamanho)	2 discos

Tabela 2.1
Comparativo dos Raids 0, 1, 5 e 6.

Veja o tutorial sobre o Raid: http://www.acnc.com/04_01_00.html.

Note que, sempre que pensamos em Raid, estamos pensando em disponibilidade das informações e não no custo direto dos discos.

Exercício de fixação 2
Redundância

Explique o que é redundância.

O que é Raid 5?

Segurança no fornecimento de energia

A disponibilidade da informação armazenada depende da operação contínua dos equipamentos. Para garantir o suprimento de energia elétrica é necessário:

- Eliminar a variação da voltagem (estabilização).
- Proporcionar ausência de interrupção da energia elétrica (*nobreak*).
- Proporcionar aterramento elétrico perfeito.



Figura 2.8
Nobreak de grande porte.



Figura 2.9
Estabilizadores de voltagem domésticos e institucionais.

Os computadores são sensíveis às variações da voltagem da energia elétrica e, por isso, é recomendado o uso de um estabilizador.

O nobreak ou Uninterruptible Power Supply (UPS) garante o fornecimento de energia elétrica, mesmo em caso de falta, porque possui um banco de baterias. Ele estabiliza a energia elétrica e possui tempo máximo de fornecimento de energia, de minutos a horas.

O bom nobreak deve ter três características:

- On-line (quando a energia elétrica cai, a carga não percebe nenhuma variação);
- Senoidal (a carga recebe uma senoide pura de 60 hertz, sem ruídos);
- Capacidade de desligar as máquinas ligadas ao nobreak.

O banco de baterias do nobreak exala gases tóxicos e, por isso, não deve estar na mesma sala dos computadores onde os funcionários trabalham.

- O gerador usa fonte de energia alternativa, como óleo diesel ou gasolina.
- O gerador é usado em conjunto com o nobreak para garantir o fornecimento ininterrupto de energia elétrica por horas ou por dias.



Figura 2.10
Gerador.

No gerador, a energia da combustão é transformada em energia mecânica; o alternador transforma energia mecânica em energia elétrica.

O gerador é muito barulhento. Por isso, costuma ser colocado longe da sala de computadores e, às vezes, fora do prédio.

Salvaguarda (backup)

- É o último recurso no caso de perda de informação.
- O Plano de Continuidade de Negócios (PCN) prevê o uso de mídias de backup para a recuperação de desastres.
- Observar uso de compressão e criptografia no programa.
- Item importante do PCN: backup off-site.
- Mídias mais usadas: fitas, HD, CD e DVD.



Figura 2.11
Cofre para armazenamento de mídias.

- **Fitas**: possuem baixo custo e alta capacidade de armazenamento, chegando atualmente até a 600 GBytes em uma única fita;
- **Mídias**: devem ser guardadas em cofre e protegidas contra calor, umidade, roubo, enchentes etc;
- **Backup off-site**: consiste em guardar as mídias de backup fora do local onde ficam os dados.

Descarte da informação

- Documentos com informações confidenciais requerem descarte seguro, impossibilitando qualquer recuperação das informações.
- Principais mídias de descarte: papel, fitas e discos rígidos.
- A instituição deve ter uma política de descarte de papel, de fitas e de discos rígidos.
- Documentos em papel devem ser fragmentados no mínimo por uma fragmentadora de corte transverso.
- As mídias magnéticas devem ser destruídas.



Figura 2.12
Fragmentador de papel e mídias.

Documentos que requerem descarte seguro: documentos em papel, fotocópias, impressões ou qualquer documento que contenha informação classificada como "confidencial", como cheques, microfilmes, gravações de voz e imagem, papel-carbono, relatórios, fitas de impressão descartáveis, fitas magnéticas, disquetes, HDs, CD-ROMS, listagem de programas, memórias não voláteis (pen drives, memory sticks, memory keys, smart cards etc.), dados de testes e documentação de sistemas.

O padrão internacional DIN 32757 determina o tamanho máximo das tiras ou partículas e os classifica em cinco níveis:

- **1**: largura máxima de tiras de 12 mm.
- **2**: largura máxima de tiras de 6 mm.
- **3**: largura máxima de tiras de 2 mm ou fragmento máximo de 4 mm x 80 mm.
- **4**: fragmento máximo de 2 mm x 15 mm = 30 mm2.
- **5**: fragmento máximo de 4 mm x 80 mm = 10,4 mm2.

Alguns procedimentos devem ser seguidos a fim de garantir a confidencialidade das informações: guardar documentos em armários ou gavetas com chave, trancar gavetas e armários, ativar proteção de tela com bloqueio de senha, apagar quadros e remover folhas, anotações e rascunhos da sala, retirar cópias da impressora, imprimir documentos com a opção de impressão segura, utilizar cabo de segurança para notebooks e estar atento a qualquer situação que possa ocasionar o extravio de informações sigilosas.

Segurança lógica



Firewall.

- Packet filtering.
- Stateful packet filter.
- Application proxy.
- Deep packet inspection.

Detector de intruso.

- IDS Snort.
- IDS Tripwire.

Rede virtual privada.

Autenticação, autorização e auditoria.

A segurança lógica compreende os mecanismos de proteção baseados em *software*. Existe uma infinidade de mecanismos de segurança lógica, como senhas, controle de acesso, criptografia, firewalls, sistemas de detecção de intrusão, redes virtuais privadas e muitos outros. Neste Capítulo, será dada uma introdução a alguns desses mecanismos.

Firewall



- "Parede corta-fogo", que protege a rede interna contra os perigos da internet.
- Exemplo do princípio do *choke-point* (gargalo).

Serve a propósitos específicos:

- Restringe a entrada a um único ponto controlado.
- Previne que invasores cheguem perto de suas defesas mais internas.
- Restringe a saída a um único ponto controlado.

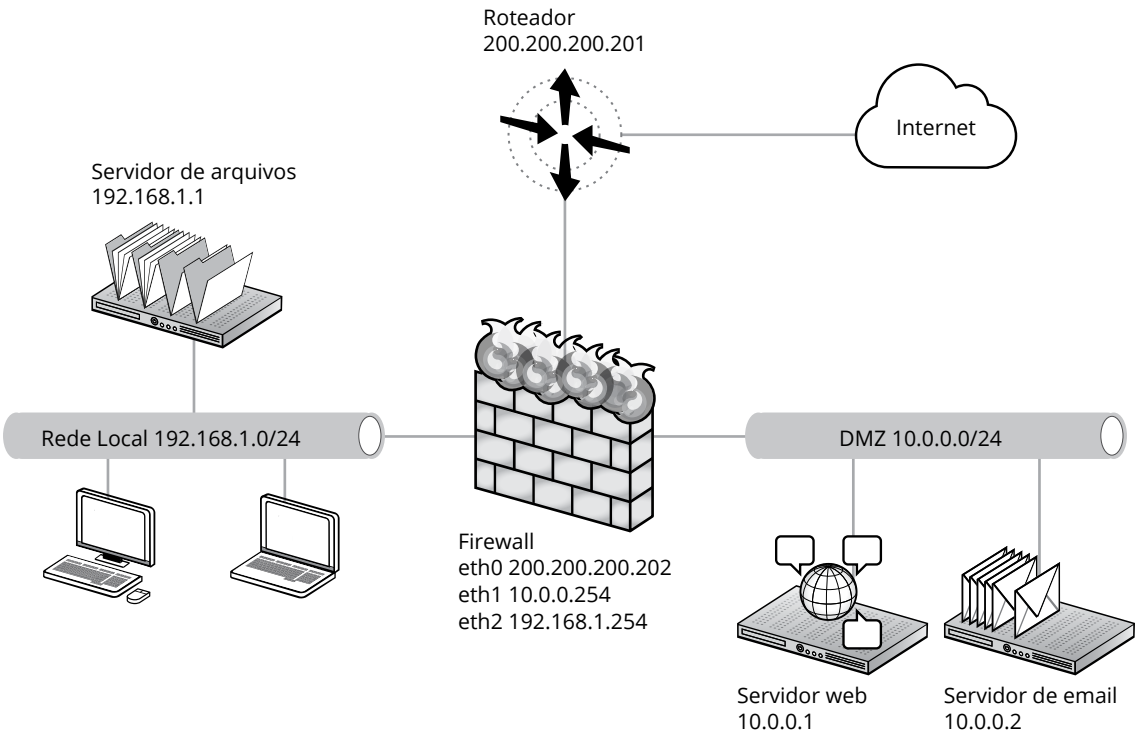


Figura 2.13 Como funciona o firewall.

Regra de ouro da segurança: a instituição só deve ter uma porta de entrada ou de saída para a internet, e essa porta deve estar diretamente conectada ao firewall, que é uma solução de segurança. Os componentes do firewall são:

- Filtros de pacotes;
- Proxies;
- NAT;
- Redirecionamento de portas.

O firewall popular do Linux é o netfilter, sendo conhecido pelo nome de sua interface, o Iptables.

Necessidades em um firewall

Capacidade para lidar com os desafios de gerência e controle de tráfego de rede, como:

- Tratamento de TCP – RFC 793.
- Construindo regras "Stateful".
- Tratando pacotes UDP – RFC 768.
- Tratamento de ICMP – RFC 792.
- Ataques DOS de "*flood*" de pacotes.
- Aplicações P2P.
- Jogos na rede.
- Nat 1:1.
- Nat N:1.
- Nat N:N.

Packet filtering (filtro de pacotes)



Filtro de pacotes estático:

- Tecnologia mais simples, que analisa individualmente pacotes que chegam e passam do nível de enlace para o nível de rede.
- Evita ataques mais sofisticados, como IP Spoofing, pacotes truncados ou *flooding* de pacotes.
- Regras de filtragem mais difíceis de configurar.
- Limitado, não filtra adequadamente protocolos que abrem portas dinamicamente.
- Permite ataque às vulnerabilidades de protocolos e serviços no nível de aplicação.

Exemplo: Iptables liberando acesso a um servidor web interno:

```
-A FORWARD -p tcp -m tcp -d 200.200.200.200 -i ppp0 --dport 80 -j ACCEPT

-A FORWARD -p tcp -m tcp -s 200.200.200.200 -o ppp0 --sport 80 -j ACCEPT
```

Stateless



Filtro arrojado de pacotes:

- Tecnologia mais simples, que analisa individualmente pacotes que chegam e passam do nível de enlace para o nível de rede, mas também verifica algum detalhe, como a interpretação do "flag SYN" de início de conexão.
- Possui todas as capacidades de um filtro de pacotes.
- Foi uma tecnologia de transição entre o conceito de Packet Filter e a tecnologia Stateful.
- No Linux, teve sua época de utilização através do Ipchains.

Stateful packet filter



- O filtro de pacotes com estado usa conjunto de regras de filtragem e informações de estado das conexões.
- A primeira filtragem ocorre com o primeiro pacote (SYN), depois o SPF cria uma entrada para essa conexão (sessão) na tabela de estados.
- Fornece maior desempenho.
- Configuração mais simples.
- Guardam na memória o estado de uma conexão.

Atua como um porteiro: as pessoas que saem são identificadas e somente elas podem voltar. Essa mesma ideia é aplicada aos pacotes. Exemplo: Iptables liberando acesso a um servidor web interno:

- -A FORWARD -p tcp -m tcp -m state -d 200.200.200.200 -i ppp0 --dport 80 --state NEW -j ACCEPT
- -A FORWARD -p tcp -m tcp -m state -s 200.200.200.200 -o ppp0 --sport 80 --state ESTABLISHED, RELATED -j ACCEPT

Application proxy



- O proxy de aplicação permite análise e filtragem até a camada de aplicação.
- Controla toda a comunicação de um serviço entre as máquinas internas e externas.

- Necessita de duas conexões: cliente proxy, proxy servidor remoto.
- Extranet: cliente externo proxy interno, proxy interno servidor interno.
- Não há comunicação entre as máquinas internas e os servidores remotos.
- Pode agregar outros serviços.

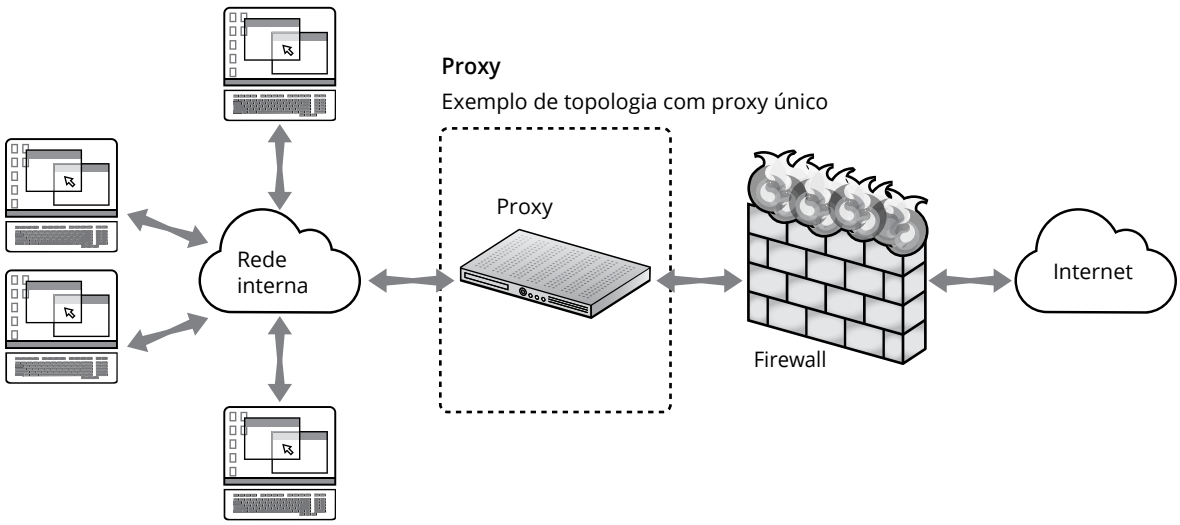


Figura 2.14
Proxy de aplicação.

Permite controle total da comunicação, impedindo os ataques que tentam explorar, por exemplo, vulnerabilidades nas aplicações dentro dos servidores. Como exemplo, um packet filtering firewall permitiria a passagem de pacotes na porta 80 (geralmente protocolo HTTP), mesmo que ninguém os tivesse requisitado; um stateful inspection firewall permitiria a passagem do protocolo HTTP para o servidor web da empresa, porque está de acordo com as regras definidas; somente o application proxy firewall bloquearia uma sequência especial de caracteres misturada nas informações HTTP que fazem travar a aplicação dentro do servidor.

Squid é o proxy popular Linux de navegação na internet, que agrega serviço de cache e de autenticação. O serviço de cache estatisticamente fornece economia de 30% de uso da banda do link de internet. O Squid pode ser usado em conjunto com o dansguardian e o serviço de **blacklist**, fornecendo administração robusta de bloqueio de páginas.

Blacklist
Lista de e-mails, domínios ou endereços IP reconhecidos como fontes de spam.

Deep packet inspection

- No conceito de inspeção profunda, toda a informação é verificada e não somente os cabeçalhos.
- Verifica se o protocolo correto está passando pela porta correta.
- Examina cada *bit* e *byte* que cruza o *firewall*, filtrando mais de 95% dos ataques.
- Integra várias tecnologias:
  - Gateway antivírus.
  - Gateway antispyware.
  - Gateway antispam.
  - Gateway antiphishing.
  - Serviço de prevenção de intrusos (IPS).
  - Serviço de detecção de intrusos (IDS).
  - Serviços IPsec VPN.

Alguns fabricantes:

- SonicWall;
- Cisco;
- Juniper.

Exercício de fixação 3
Firewall

Justifique a necessidade de um firewall para a sua organização.

O que é um proxy de aplicação?

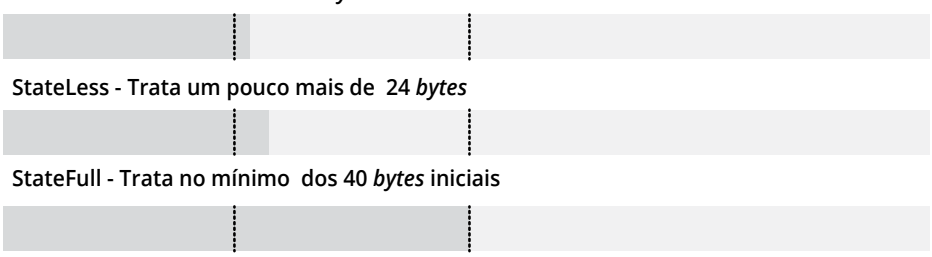
Uma visão a partir do datagrama

Endereçamento IP	Transporte TCP/UDO/ICMP*	Área de Dados (MSS)
20 bytes	20 bytes	1460 bytes

Packet Filter - Trata de 20 a 24 *bytes*

StateLess - Trata um pouco mais de 24 *bytes*

StateFull - Trata no mínimo dos 40 *bytes* iniciais



Valor máximo do Datagrama (MTU): 1500 *bytes*

*O protocolo de transporte, porter o cabeçalho de até 20 *bytes*

Figura 2.15
Datagrama, onde o firewall atua.

- **Packet Filter**: trata de 20 a 24 bytes, ou seja, de todo o cabeçalho IP (primeiros 20 bytes), e de parte do cabeçalho de transporte no que diz respeito à porta de origem e destino, lembrando que esse campo tem 4 bytes (16 bits: 2^16 = total de 65536 portas).
- **StateLess**: trata um pouco mais de 24 bytes, variando de acordo com a forma com que a ferramenta foi implementada. Em alguns casos analisa o flag de início de conexão TCP, mas não é capaz de tratar o conceito de estado de conexão.
- **StateFul**: trata no mínimo dos 40 bytes iniciais, ou seja, todo o cabeçalho IP; seja qual for o protocolo de transporte (UDP, TCP), sabe tratar do estado de conexão.

O fato de um firewall ter a capacidade de atuar nos 40 bytes iniciais do datagrama não quer dizer que não permita realizar tratamento no estilo Packet Filter ou mesmo Stateless.

Exemplos de firewalls

Linux Kernel 2.0.x:

- IPF: Packet FilterB.
- IPFWADM: Packet Filter.

Linux Kernel 2.2.x:

- IPchains: StateLess.
- Sinus: Packet Filter.

Linux Kernel 2.4.x / 2.6.x:

- Netfilter (Iptables): StatefulPacket.

Outras soluções OpenSource:

- IPFW (FreeBSD).
- PF (OpenBSD e FreeBSD 5.x).
- IPFilter (Solaris 10).

Acesse o site do Firewall Builder e conheça em detalhes o projeto: http://www.fwbuilder.org/

Visando facilitar a criação e gerenciamento de regras, existe um projeto chamado Firewall Builder. Através de uma plataforma gráfica, o administrador pode criar sua rede e depois gerar as regras de firewall. O diferencial é poder escolher para qual plataforma deseja gerar as regras.

Detectores de intrusos

IDS é a sigla de Intrusion Detection Systems (Sistemas de Detecção de Intrusão).

Analisa o comportamento da rede ou do sistema, em busca de tentativa de invasão.

- Baseado no sistema imunológico do corpo humano.
- Monitora um servidor específico ou host IDS (Hids).
- Monitora uma rede específica network IDS (Nids).
- Monitora chamadas de sistemas Kernel IDS (Kids).

Saiba mais sobre ferramentas de IDS: http://www.rnp.br/newsgen/9909/ids.html

Utiliza dois métodos distintos.

- Detecção por assinatura.
- Detecção por comportamento.
- Usa sensores espalhados pela rede ou pelo host.

Uma ferramenta de IDS deve possuir algumas características, entre elas:

- Rodar sem interação humana, de forma a permitir sua operação em *background*.
- Ser tolerante a falhas, de forma a não ser afetada por uma queda do sistema; sua base de conhecimento não deve ser perdida quando o sistema for reinicializado.
- Resistir a tentativas de mudança (subversão) de sua base; deve fazer automonitoramento.
- Ter o mínimo de impacto no funcionamento do sistema.
- Poder detectar mudanças no funcionamento normal.
- Cobrir as mudanças do sistema, como no caso de uma nova aplicação que comece a fazer parte do sistema.
- Nids Linux popular: Snort.
- Kids Linux popular: SELinux.

Busque mais ferramentas Free and Open Source Software (FOSS) nos sites http://www.freshmeat.net e http://www.sourceforge.net

IDS Snort

Ferramenta de detecção de invasão Nids open source (Linux); popular, rápida, confiável, exigindo poucos recursos do sistema:

- Flexível nas configurações de regras.
- Possui grande cadastro de assinaturas.
- Atualizada constantemente frente às novas ferramentas de invasão.
- Monitora tráfego de pacotes em redes IP, realizando análises em tempo real de diversos protocolos (nível de rede e aplicação) e sobre o conteúdo (hexa e ASCII).

Modos de operação:

- Sniffer;
- Packet Logger;
- Nids.

Leia mais sobre o Snort em http://www.snort.org/http://www.snort.org

Fluxo de funcionamento do Snort

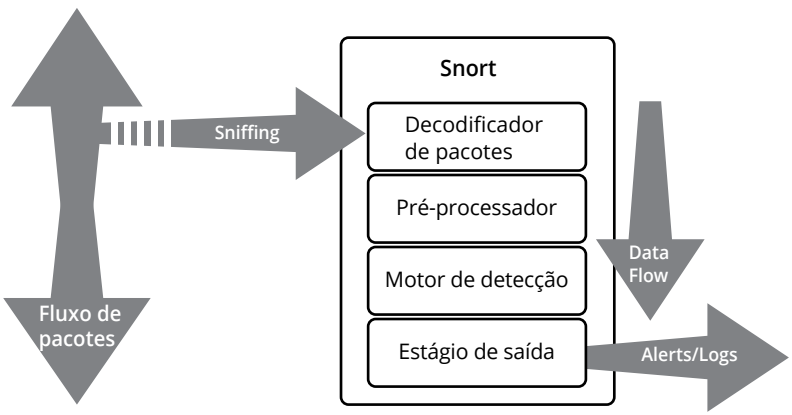


Figura 2.16 Fluxo de funcionamento do Snort.

Por ser muito popular, existem diversos projetos que trabalham junto ou complementam o Snort, entre eles o Acid (Figura 2.17) e o Base (Figura 2.18), ajudando a visualizar graficamente os alertas e suas estatísticas.

Mais detalhes podem ser encontrados em:

- Analysis Console for Intrusion Databases (Acid): http://acidlab.sourceforge.net/
- Basic Analysis and Security Engine (Base): http://base.secureideas.net/

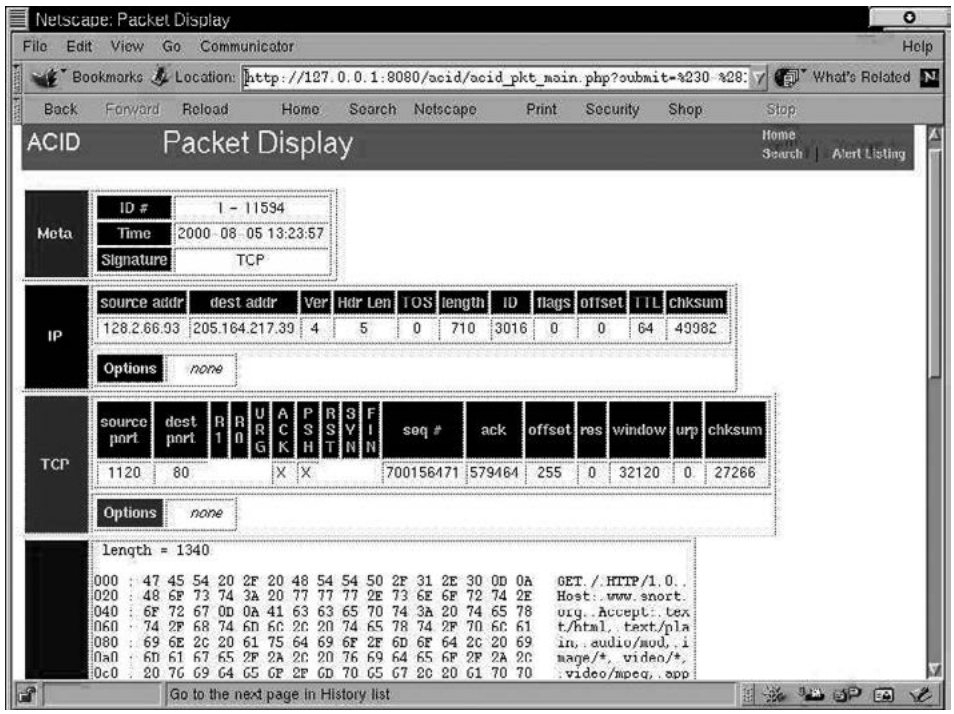


Figura 2.17
Acid.

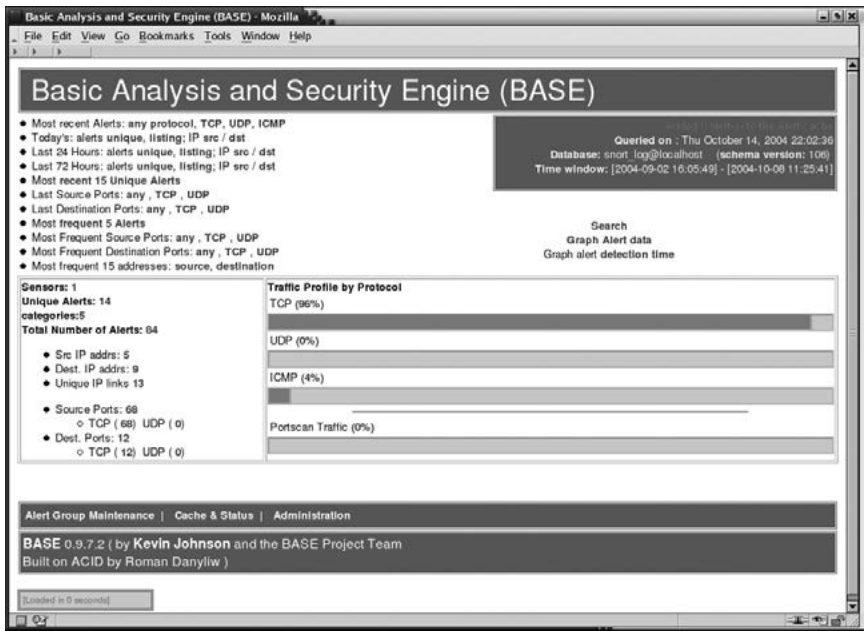


Figura 2.18
Base.

Hids

- Ferramenta desenvolvida para monitoramento das modificações ocorridas no sistema de arquivos.
- Verifica a integridade dos arquivos e comandos do Sistema Operacional, manualmente ou através de programação "via cron".
- São muitas e interessantes as soluções disponíveis, como Osiris, Ossec, Samhaim, Tripwire e Aide.
- Destaque para Osiris, que além de ter arquitetura cliente servidor, possui clientes para vários Sistemas Operacionais, possibilitando ter um servidor Osiris Linux monitorando servidores Windows e MacOS, por exemplo.

Os benefícios do Hids Ossec (http://www.ossec.net/), Hids Samhaim (http://la-samhna.de/samhain/), Hids Aide (http://aide.sourceforge.net/) e Hids Tripwire (http://www.tripwire.org) estão em seus sites.

Kids

- Ferramenta desenvolvida a partir das chamadas de sistemas e do controle das funcionalidades do kernel.
- Um conceito ainda recente de IDS, gradualmente adotado pelos Sistemas Operacionais.
- Exemplos clássicos: Lids, GRsecurity e SELinux.

IPS

- IPS é a sigla de Intrusion Prevention System (Sistema de Prevenção de Invasão).
- Podemos considerá-lo a evolução do IDP.
- Como o nome diz, o IDS Detecta, porém o IPS tem o "poder" de barrar o ataque, antes que atinja seu destino.
- Pode ser utilizado sozinho ou em conjunto com o IDS.
- Na maioria dos produtos, pode-se escolher trabalhar no modo de prevenção ou detecção.
- Como exemplo, podemos citar o Sourcefire (versão comercial do Snort).

Redes virtuais privadas

Virtual Private Network (VPN) interliga duas redes privadas usando a internet como meio de interligação.

Usa normalmente canal de criptografia:

- Rápida, para não comprometer o desempenho.
- Segura, para impedir ataques.
- Substitui linhas dedicadas a um custo reduzido.
- Sujeita a congestionamento e interrupções na internet.

Tipos:

- Entre redes.
- Discada.

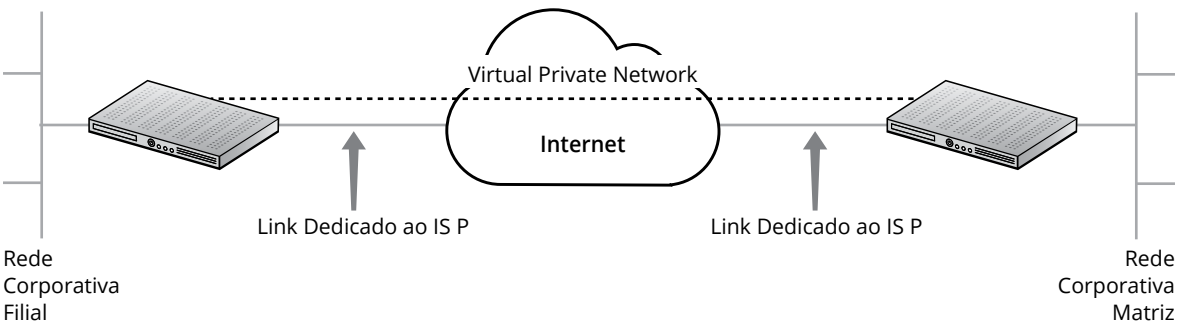


Figura 2.19
Rede virtual privada (VPN).

A segurança é uma importante função da VPN. Dados privados serão transmitidos pela internet, que é um meio de transmissão inseguro. Eles devem ser protegidos de forma a não permitir que sejam modificados ou interceptados.

O uso de VPN nos permite trabalhar remotamente (de casa, por exemplo), como se estivéssemos dentro da rede da empresa. Permite também interligar dois ou mais escritórios, como se todo mundo estivesse dentro do mesmo prédio, proporcionando inclusive acesso a recursos compartilhados, como impressoras e servidores de arquivos, que não estariam localmente disponíveis sem o uso dessa tecnologia.

Outro serviço oferecido pelas VPNs é a conexão entre corporações (extranets) através da internet.

Autenticação, autorização e auditoria

Autenticação: estabelece a identidade do indivíduo.

- Identificação:
  - Via login.
  - Via Personal Identification Number (PIN).
- Método de prova:
  - Via algo que você sabe.
    - Uma senha (menor nível de segurança).
  - Via algo que você tem:
    - Smartcard ou token.
  - Via algo que você é:
    - Impressão digital, leitura da íris, voz etc. (maior nível de segurança).



Figura 2.20
Token USB (Fonte: http://www.ealaddin.com).

Autenticação, autorização e auditoria

Autorização:

- A autorização traça o perfil de acesso do indivíduo e o que ele pode fazer.
- O perfil contém todas as permissões para cada recurso que o indivíduo acessa.

Auditoria:

- A auditoria implica em: quem fez o quê, quando, onde?
- Os registros de eventos (*logs*) são os primeiros objetos a serem consultados em uma auditoria.

É possível combinar métodos distintos de autenticação. Um usuário pode inserir um cartão magnético e digitar uma senha para obter acesso.

Quando utilizamos mais de um método para a autenticação, chamamos o processo de "autenticação forte".

Roteiro de Atividades 2

Atividade 2.1 – Segurança física e lógica

1. Como você planejaria a segurança da sua empresa seguindo os tópicos abaixo?

Contenção de catástrofes:

Proteção das informações (backup):

Controle de acesso:

Garantia de fornecimento de energia:

Redundância:

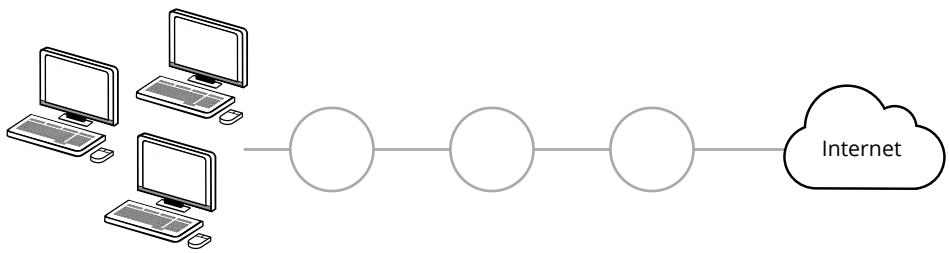
2. Quantos níveis de segurança possui a rede da sua instituição? Quais são? Faça um desenho da topologia da solução.

3. Cite 5 controles que podemos utilizar para aumentar a segurança física de um ambiente.

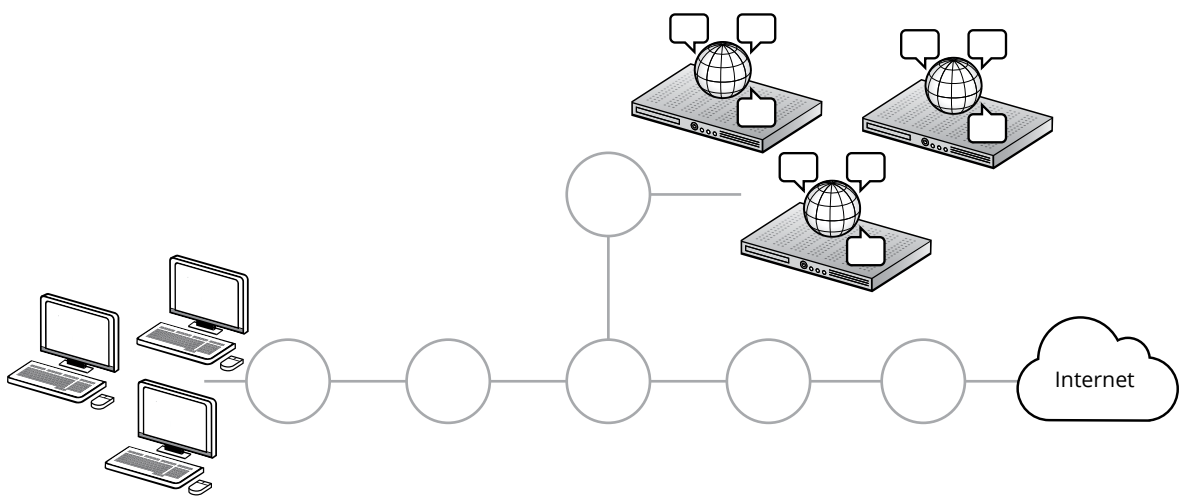
4. Cite 5 controles que podemos utilizar para aumentar a segurança lógica de um ambiente.

5. Informe em cada círculo dos diagramas seguintes o equipamento correto para a rede, que proporcione um nível de segurança satisfatório. Justifique suas respostas.

Número	Equipamento
1	IDS
2	Modem
3	Firewall
4	Proxy
5	Switch
6	Roteador







3

Panorama atual da área de segurança

objetivos

Apresentar informações sobre ameaças na rede e estatísticas recentes sobre ataques e suas fontes; indicar o perfil das pessoas que invadem sistemas.

conceitos

Controles de informática e ameaças digitais.

Introdução

Atualmente a segurança tornou-se um item obrigatório. Usar a internet sem um antivírus ou um firewall pessoal é quase um pedido para ser infectado ou invadido. Instalar um Sistema Operacional em uma máquina conectada diretamente à internet pode levar a um comprometimento em poucos minutos. Esse é o panorama atual da rede: um lugar público onde, junto com aquela informação valiosa de que tanto precisamos, existe um mundo de hackers, crackers, vírus, worms e outras ameaças.

A rede ainda pode ser usada de forma segura, desde que cuidados básicos sejam tomados. Neste Capítulo, veremos quais são as ameaças do dia a dia, como elas funcionam e as formas de se proteger contra elas. Além disso, veremos as estatísticas dos incidentes de segurança, diversas fontes de informação diária sobre segurança e o perfil das pessoas que ameaçam a segurança da rede.

Panorama atual da internet



Conexões mais rápidas (banda larga).

- Estações se tornam “atraentes” para invasores.
  - Fazer uso da banda larga.
  - Fazer uso dos recursos computacionais.
  - Roubo de identidade.

Internet pública: mais ameaças

- Hackers.
- Crackers.
- Vírus.
- Worms.

Exercício de nivelamento 1
Panorama atual da área de segurança

Como é o acesso a internet da sua organização?

Acesso em banda larga modem bridge

Banda larga modem bridge ADSL.

- Modo padrão de configuração da operadora.

Vantagens:

- Computador pode disponibilizar serviços.
- IP fixo pode usar DNS.

Desvantagens:

- IP dinâmico usando DDNS.
- Exige segurança reforçada.
- Computador pode ser acessado diretamente da internet.

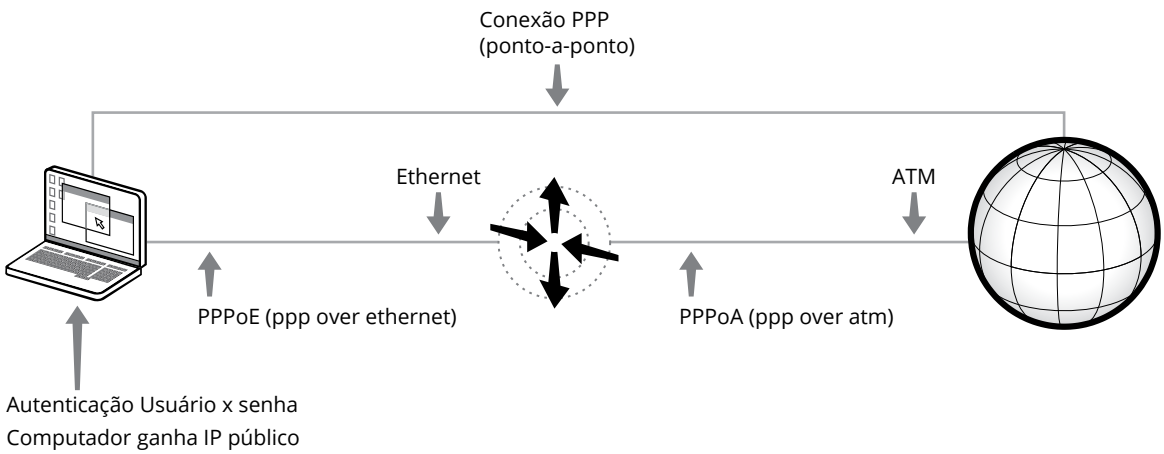


Figura 3.1
Banda larga modem bridge ADSL.

Acesso banda larga modem router

Banda larga modem router ADSL.

Vantagens:

- Modo de operação mais seguro.
- Computador não é acessado diretamente a partir da internet.
- Proporciona acesso a uma rede interna (intranet).
- IP fixo pode usar DNS.

Desvantagens:

- Router deve usar firewall.
- Computador deve usar NAT para disponibilizar serviços.
- IP dinâmico usando DDNS.

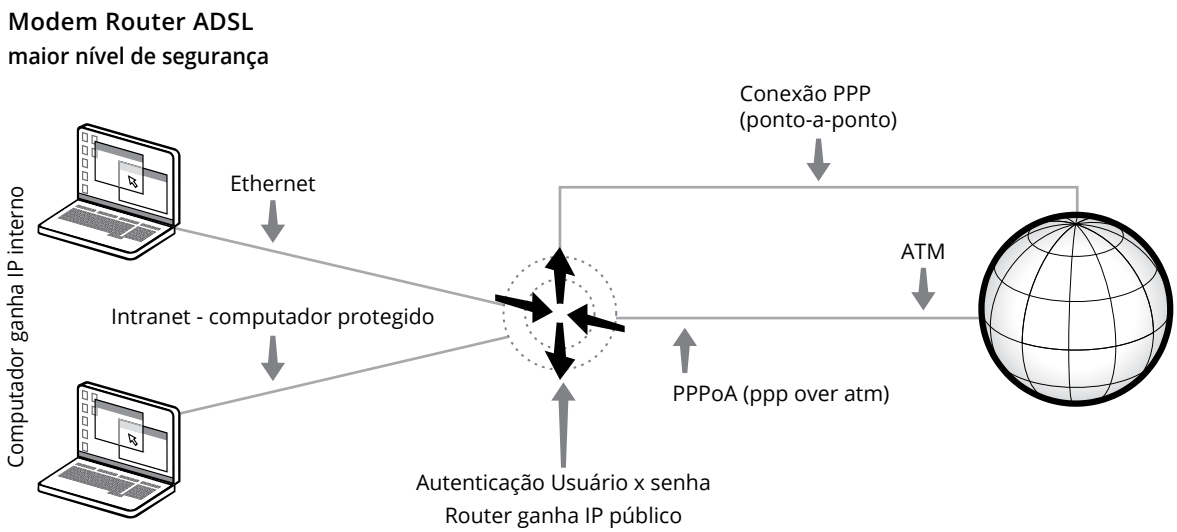


Figura 3.2
Banda larga modem router ADSL.

Principais erros

- Mesmo erros conhecidos são recorrentes, tanto de projeto como de administração de sistemas.
- Os erros facilitam a atividade dos invasores; todavia, mesmo sem cometer erros a possibilidade de ameaça continuará existindo.
- Conectar sistemas na internet sem testá-los.
- Conectar com contas e senhas padrão.
- Não atualizar erros de segurança, quando estes são encontrados e divulgados.
- Deixar que pessoas sem o devido treinamento cuidem de segurança.
- Deixar serviços desnecessários nos computadores:
  - Ftpd, telnetd, finger, RPC, mail e RServices.
- Manter no servidor ligado à internet a base de arquivos da empresa, não diferenciando serviços de LAN e WAN.
- Conhecer a segurança física, mas desconhecer segurança de informação.
- Falta de ambiente de laboratório, de teste.
- Manter somente um firewall protegendo a rede, acreditando que é suficiente.
- Permitir o uso indiscriminado de protocolos específicos, como o ICMP.
- Implementar firewalls com políticas genéricas.
- Usar protocolos não seguros para administrar sistemas remotos, firewalls etc.
- Não idealizar perímetros para melhorar a segurança da rede.
- Não ter servidores com horário sincronizado.
- Não ter concentradores de logs e analisadores dos registros de logs.
- Possuir um concentrador e logs, mas com os horários dos servidores não sincronizados.
- Achar que, se esquecendo dos problemas, eles somem rapidamente.
- Falhar na implementação de antivírus ou listas de vírus.
- Falhar na capacitação e conscientização dos usuários.

Ameaças frequentes



- Vírus.
- Worms.
- Trojans.
- Spywares.
- Hackers, crackers e outros.

Vírus



- Microprograma alojado em arquivo hospedeiro, precisa da intervenção humana para se propagar.
- Autoexecutável, duplica a si próprio.
- A principal forma de contágio é via correio eletrônico com arquivo anexo infectado.
- Principais extensões de arquivos perigosos no Windows:
  - A interrogação indica a presença de qualquer caractere.
  - Exemplo: PP? indica tanto PPT quanto PPA:
    - 386, ACM, ACV, BAT, BTM, CDR, CHM, CLA, COM, CPL, CSC, DLL, DOC, DOT, DRV, DVB, EML, EXE, FON, GMS, HLP, HT?, HTA, INF, INI, MDB, MPP, MPT, MSG, MSO, OBD, OBJ, OBT, OBZ, OCX, OFT, OV?, PIF, POT, PP?, PWZ, RTF, SCR, SHS, SMM, SYS, TDO, TLB, TSK, TSP, VBS, VBX, VXD, WBK, WBT, WK?, WPD, XL? e XML.

Extensão	Comentário
.com	Executável DOS/Windows.
.exe	Executável DOS/Windows.
.pif	Descrição de ambiente de execução DOS.
.vbs	Scripts em Visual Basic .
.htr	Scripts em servidores web Microsoft.
.cpl	Extensões do painel de controle.
.hta	Scripts em servidores web Microsoft.
.scr	Screens savers do Windows.
.bat	Arquivos de lotes do DOS/Windows.
.doc	Arquivos do Microsoft Word.
.ppt	Arquivos do Microsoft PowerPoint.
.xls	Arquivos do Microsoft Excel.
.js	Scripts em Javascript.

Tabela 3.1
Tipos de arquivos mais comuns.

Apesar de existirem vírus para outros Sistemas Operacionais (Linux, MacOS e PalmOS), essa quantidade é infinitamente menor, quando comparamos com a quantidade de vírus do sistema Windows.

Um antivírus detecta os vírus em arquivos através de assinaturas de vírus, que são conjuntos de informação que identificam unicamente um determinado vírus. Essas assinaturas devem ser frequentemente atualizadas, de modo que o antivírus seja capaz de detectar os vírus mais recentes.

Diversos fabricantes de produtos de segurança disponibilizam programas chamados antivírus. Um antivírus é um programa capaz de detectar e remover os vírus de uma estação. Muitos deles possuem recursos avançados, como verificação de vírus em correio eletrônico e a verificação em tempo real dos arquivos que estão sendo executados pelo Sistema Operacional.

Alguns desses fabricantes e seus sites:

- Symantec: http://www.symantec.com/avcenter/
- McAfee: http://home.mcafee.com/VirusInfo/
- Trend Micro: http://www.trendmicro.com/vinfo/virusencyclo/
- F-Secure: http://www.f-secure.com/v-descs/

Tipos de vírus



- Vírus de boot:
  - Fixa-se num setor onde está localizado o código de boot do micro (inicialização).
- Vírus de arquivo:
  - Fixa-se em arquivo de programa executável.
- Vírus de macro:
  - Vincula macros a modelos de documento (templates) e outros arquivos.
- Vírus parceiro (companion virus):
  - Junta-se ao Sistema Operacional (programa ".com" roda primeiro que ".exe").
- Vírus multipartido:
  - Combinação do vírus de boot e do vírus de arquivo.
  - Infecta tanto arquivo quanto área de boot.

Um vírus pode provocar:

- Perda de desempenho do micro; exclusão de arquivos e alteração de dados.
- Acesso a informações confidenciais por pessoas não autorizadas.
- Perda de desempenho da rede (intranet e internet).
- Desconfiguração do Sistema Operacional; acionamento e desligamento de periféricos da máquina.



Prevenção:

- Implantar política de uso de antivírus nas estações de trabalho.
- Manter antivírus sempre atualizado via internet.
- Varrer os discos rígidos com o antivírus no mínimo uma vez por semana.
- O antivírus deve checar os e-mails on-line que chegam e saem.
- Não abrir arquivo anexado em e-mail com extensão perigosa.
- Habilitar técnica de antispam no antivírus.

O CAIS indica dois bons antivírus gratuitos:

- Kaspersky: http://www.kaspersky.com
- Avira AntiVir: http://www.free-av.com

Antivírus on-line:

- Kaspersky: http://www.kaspersky.com/virusscanner
- Trendmicro: http://housecall.trendmicro.com
- F-Secure: http://support.f-secure.com/enu/home/ols.shtml
- Bit Defender: http://www.bitdefender.com/br/scanner/online/free.html

Worms



- O worm (verme) infecta uma estação em vez de infectar arquivos.
- Programa que não precisa da intervenção humana para se propagar.
- Difere do vírus porque não precisa se fixar em arquivo ou setor.
- Rasteja pela rede tentando infectar outras estações, podendo utilizar múltiplas formas de replicação, tornando-se muito eficiente.

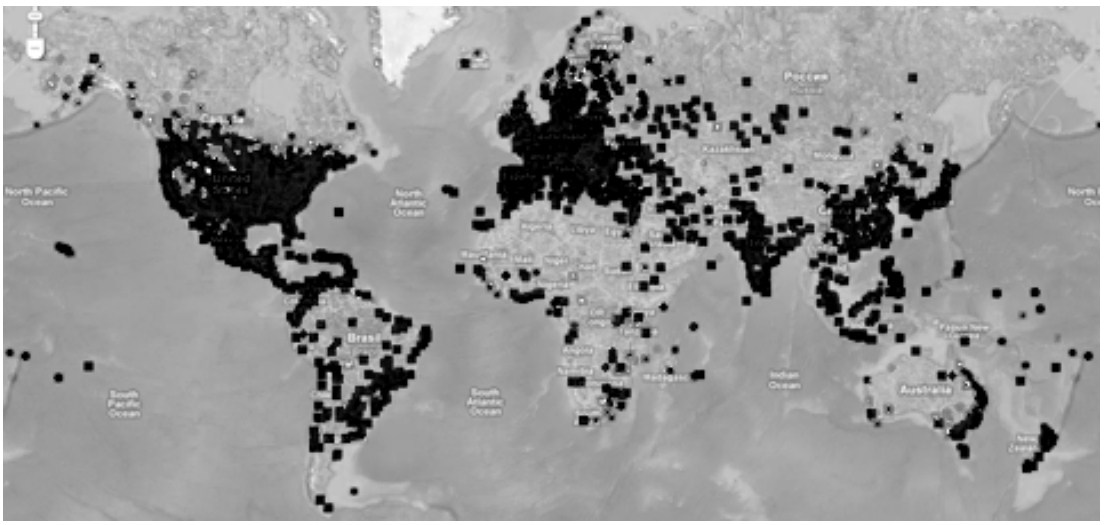


Figura 3.3
Propagação do worm Sapphire (Fonte: Caida).

A contenção da propagação dos worms depende muito das atualizações feitas no Sistema Operacional. Como essas atualizações não são realizadas pelos administradores e usuários na maioria dos casos, contaminações são frequentes sempre que um novo worm é lançado na internet. Entretanto, na grande maioria dos casos, o worm explora vulnerabilidades já conhecidas pelos fabricantes, que disponibilizam em seus sites as atualizações que as eliminam.

- O worm Code Red infectou em 19 de julho de 2001 mais de 359 mil computadores em menos de 14 horas.
- O worm SQL Slammer infectou 75 mil computadores em 10 minutos em 2003.
- O worm Confiker infectou mais de 10 milhões de máquinas em janeiro de 2009.
- A prevenção contra os worms é feita da mesma forma que a do antivírus.

Cavalo de troia



- Cavalo de troia (trojan horse) é um programa que promete uma ação ou funcionalidade, executando outra totalmente diferente.
- Pode parecer ou simular programas legítimos.
- Tem o objetivo de enganar as pessoas, permitindo acesso e roubo de informações em seus computadores.

- Incluído em software disponível para transferência gratuita.
- Diferentemente de vírus e worms, não cria réplicas de si.
- Famoso por facilidade de uso, é considerado “ferramenta de script kid”.

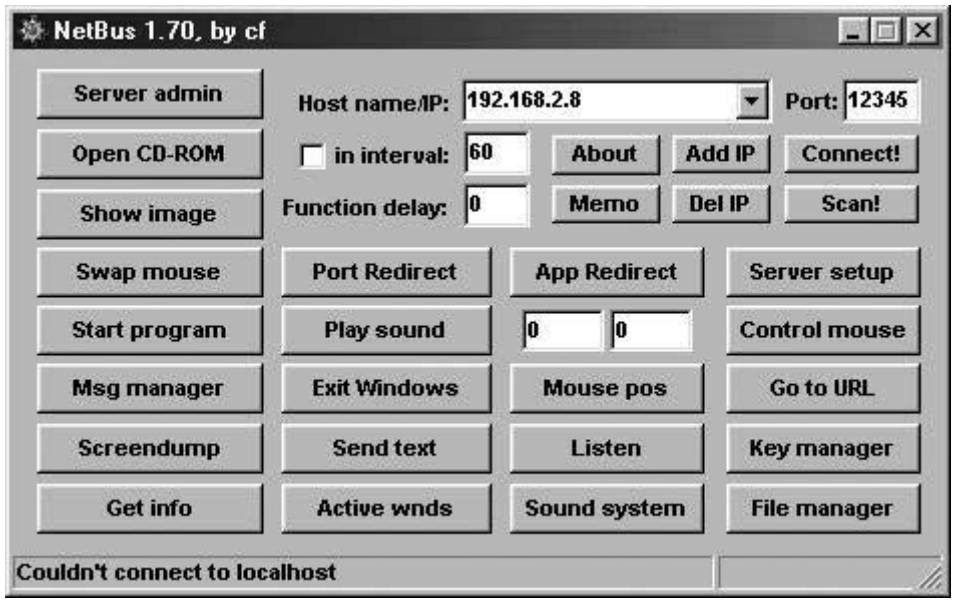


Figura 3.4
Cliente do trojan NetBus.

Alguns cavalos de troia são divididos em duas partes: servidor e cliente.

- A vítima executa arquivo hospedeiro; o servidor é instalado e ocultado no computador;
- O cliente acessa o servidor e executa operações no computador da vítima;
- É aberta uma porta de comunicação não monitorada (backdoor).

O que um trojan pode fazer?

- Expor usuário a esquemas fraudulentos via página de site.
- Encontrar arquivos: vê-los, copiá-los, alterá-los ou apagá-los.
- Registrar o que se escreve e enviar essa informação para outro computador.
- Capturar vídeo e áudio de dispositivos ligados ao computador.
- Executar ou encerrar um programa, processo ou conexão no computador.
- Criar janelas pop-up para aborrecer ou conduzir a websites maliciosos.
- Atacar outros computadores.

Trojans mais famosos:

- Back Orifice;
- NetBus;
- WinCrash.

Prevenção:

- Não revelar seu endereço de correio eletrônico a desconhecidos.
- Evitar incluir seu endereço de correio eletrônico em listas extensas de endereços.
- Usar software fidedigno de empresas conceituadas.

- Manter o computador atualizado:
  - Windows update on-line.
  - Linux update on-line.



Para prevenir-se é preciso usar software de segurança recente e mantê-lo instalado e atualizado.

- Antivírus;
- Firewall;
- Antispyware.

Ao instalar programas no micro, escolha um diretório diferente do padrão; por exemplo, ao instalar Windows, escolha diretório diferente de "C:\windows\".

- Trocar senhas assim que for invadido ou suspeitar de uma invasão;
- Não usar ou desabilitar a opção "salvar senha" onde for possível.

Para verificar as portas que estão abertas na máquina:

- Execute: C:\netstat –ab (Windows);
- Execute: # netstat –atunp (Linux).

Spyware



- Programa que se instala de maneira furtiva, trazido por outro programa.
- Difere do trojan, pois não tem objetivo de deixar que o sistema do usuário seja dominado externamente por um cracker.
- Monitora o usuário, capturando informações confidenciais, hábitos de consumo, senhas bancárias, informações de cartões de crédito etc.
- Meios de infecção:
  - Download não intencional em programas shareware e freeware.
  - Através de infecção de vírus e worms.
  - Instalações automáticas de alguns programas.

Os spywares (programas espiões) são associados a adwares. Os adwares são conhecidos por trazerem para a tela algum tipo de propaganda. Inicialmente os adwares procuravam exibir propagandas em janelas, chamadas de banners. Passaram a monitorar a atividade do usuário na internet, podendo mostrar propagandas personalizadas, enviar dados sobre hábitos do usuário a certos sites, tendo então funções de spyware e adware, de forma simultânea.

Certos adwares passaram a exibir janelas do tipo pop-up. Passaram a se instalar no navegador do usuário, acrescentando certas funcionalidades duvidosas, principalmente no Internet Explorer. Sofisticaram-se, incluindo propagandas persistentes, com inúmeras variantes. Sua desinstalação passou a ser uma tarefa bastante penosa ou mesmo impossível, sem ajuda externa. Isso levou os usuários a classificá-los como pragas ou spywares, e não mais como simples adwares.

Prevenção:

- Usar programas antispyware em conjunto com antivírus;
- Verificar configurações de segurança do navegador;
- Ler cuidadosamente anúncios em janelas pop-ups;
- Não instalar programas antes de conhecer as credenciais de quem o forneceu.

Assista ao vídeo "Proteja seu computador contra Spyware": http://www.microsoft.com/brasil/athome/security/videos/spyware_hi/Spyware6--hi.html

- Spywares podem vir acompanhados de hijackers.
- Exemplos de spyware: GAIN, Aurora;

Assista aos vídeos e saiba como se proteger:
http://antispam.br/videos/

Malware

- Junção de duas palavras: **"**malicious**"** e "software".
- Utilizado para designar qualquer tipo de software que atue contra o usuário.
- Podem ser vírus, spywares, trojans ou worms de todos os tipos e categorias.

Existem malwares para todos os tipos de computadores existentes hoje, não importando marcas e modelos. Já existem provas de conceito sobre malwares em consoles de vídeo games inclusive.

Para pensar

Mesmo existindo diversas categorias de softwares maliciosos, como demonstrado anteriormente, o termo malware começou a ser vastamente utilizado de forma incorreta. A frase "fui vítima de um malware" indica que uma pessoa foi vítima de um programa malicioso, não importando se é um vírus, worm ou trojan. Deixemos as definições corretas para os especialistas.

Prevenção:

- Tenha sempre um software do tipo antivírus instalado;
- Evite softwares piratas e/ou de procedência desconhecida;
- Mantenha o sistema operacional atualizado.

Mobile Malware

- Também conhecido "genericamente" como vírus para celular.
- Utilizando as técnicas de um cavalo de troia, incentivam o usuário a instalar o programa malicioso.
- Podem fazer tecnicamente qualquer coisa com o aparelho da vítima.

Com as mudanças da tecnologia e de hábitos, aparelhos portáteis como celulares estão ficando cada vez mais populares e potentes, além de estarem sempre conectados à internet. Após a pessoa fazer o download e instalação do aplicativo malicioso, o aparelho já está comprometido. Saber quais as reais intenções ou ações desses programas é bem difícil. O atacante pode ter controle total do aparelho celular da vítima. Assim pode efetuar ligações, ver, apagar e remover contatos, mensagens e fotos.

Na Europa existem muitas fraudes associadas a serviços do tipo "premium rate phone", conhecidos no Brasil como 0900 (serviços telefônicos de valor adicionado). Após invadido, o telefone da vítima passa a ligar para esses números. No final do mês, alguém terá de pagar

a conta. O golpe tem maior sucesso quando a vítima possui um aparelho de celular pago pela empresa, e nem a vítima nem a empresa controlam essa conta.

Prevenção:

- Escolha fontes de distribuição de softwares confiáveis;
- Utilize um software antivírus;
- Desconfie de ações ou atividades suspeitas em seu aparelho;
- A economia é sempre inimiga da segurança.

Exercício de fixação 1
Malwares

O que são malwares?

_____

_____

_____

Prevenção



Dicas de comportamento como as dicas de comportamento humano nem sempre são fáceis de atender (sempre há um risco).

Por mais que tomemos cuidado sempre existe risco. O que fazemos em nosso dia a dia é minimizar esse risco. Independente da plataforma ou Sistema Operacional, a situação fica difícil quando necessitamos utilizar um software (qualquer). Não temos como saber se existem componentes maliciosos no software ou se ele irá fazer alguma ação inesperada. É difícil até de saber onde, durante a instalação desse software, foram colocados seus arquivos, se desejarmos removê-lo futuramente.

Já existiram casos de softwares que saíram das empresas desenvolvedoras infectados, assim como pendrives que saíram da fábrica com malwares. Nenhum desses fatos foi intencional. Isso demonstra que existem situações que não podemos evitar, porém, quanto maior o cuidado que tenhamos, menores serão as chances de termos dores de cabeça.

Vulnerabilidades



São falhas presentes em um programa, protocolo ou Sistema Operacional.

Decorrem de erros de especificação ou de programação.

Prevenção para erros de programação:

- Aplicar patches ou hotfix.
- Aplicar service pack ou maintenance level.

Muitas listas de discussão fornecem informações sobre vulnerabilidades, além de sites de fabricantes. Alguns desses sites:

- http://www.microsoft.com/security/default.aspx
- http://www.debian.org/security/
- http://www.cert.org/advisories/
- http://www.rnp.br/cais/alertas/

Existem pessoas e grupos na internet que buscam e divulgam a existência de vulnerabilidades. Normalmente, elas são divulgadas em listas de discussão como a Bugtraq: http://www.securityfocus.com/archive/1

Uma prevenção para erros de especificação é fazer a revisão da especificação do protocolo ou do produto, se possível.

Vulnerabilidades do protocolo TCP/IP sem solução perfeita:

SYN flood

- Atacante envia grandes quantidades de solicitações ao servidor.
- Servidor fica à espera da conclusão da negociação para início da comunicação (que nunca ocorre).
- Quando a solicitação inicial finaliza por time-out, outras solicitações estão chegando e o clico continua.
- Esse processo impede que solicitações lícitas sejam atendidas.

Ataques Smurf

- Atacante A envia um pacote para a rede B, solicitando resposta de toda a rede.
- Porém, o pacote de origem foi modificado indicando que a origem veio de C.
- Rede B responde para a origem C.
- Máquina C recebe em pouco tempo muitos pacotes de resposta da rede B sem saber o motivo e, dependendo da quantidade de pacotes, para de funcionar ou de atender novas solicitações lícitas.

Os dois exemplos anteriores não demonstram os detalhes técnicos dos problemas, mas como os problemas funcionam.

Não podemos esquecer que o protocolo TCP/IP foi criado por volta de 1970 e suas características principais foram mantidas até hoje. Assim, muitas das vulnerabilidades existentes no protocolo não foram previstas durante o desenvolvimento.

Exploit é um programa que explora uma vulnerabilidade. Nasce como a prova de conceito de que uma vulnerabilidade existe, podendo evoluir para ações maliciosas.

Estatísticas

Entidades como Cert/CC e CAIS/RNP mantêm número de vulnerabilidades e de incidentes reportados anualmente.

- Cert/CC: http://www.cert.org/stats/cert_stats.html
- CAIS/RNP: http://www.rnp.br/cais/estatisticas/index.php

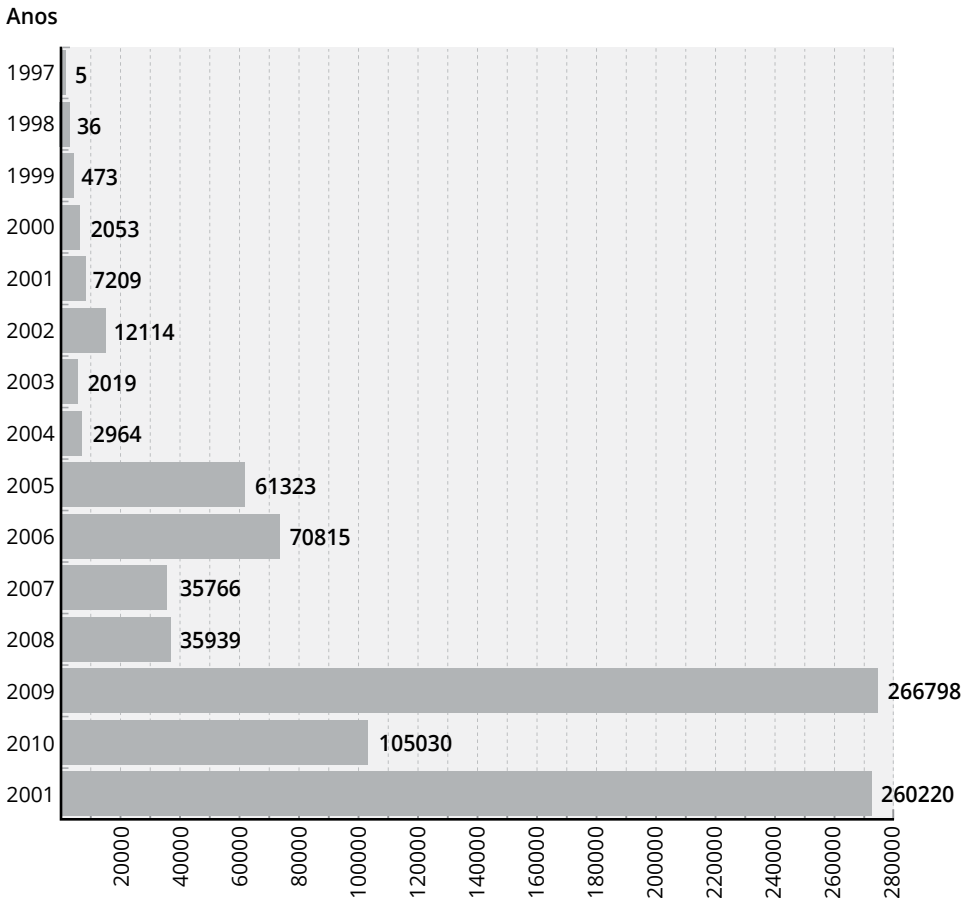


Figura 3.5
Estatísticas de incidentes por ano reportados ao CAIS.

O CERT/CC oferece estatísticas sobre incidentes, vulnerabilidades, alertas e notas de segurança publicadas, mensagens de correio eletrônico atendidas e chamadas telefônicas recebidas.

O CAIS é o órgão responsável pela segurança da RNP. As estatísticas do Cais referem-se a incidentes reportados mensal e anualmente.

Hacker, cracker e outros personagens

Vírus, worms, vulnerabilidades, exploits e ataques:

- Quem são as pessoas que os produzem?
- O que elas pensam?
- Quais são suas motivações?
- Por que fazem esse tipo de ação?

Hacker:

- Especialista em informática, “problem solver”, descobre falhas e cria exploits; possui “ética hacker”.

Cracker:

- Especialista em informática, “problem creator”, hacker malicioso, criminoso.

Para pensar

Hoje fala-se muito da "ética hacker", que trata da questão do software livre, entre outras coisas. Os hackers procuram se diferenciar dos crackers, que tentam efetivamente invadir sistemas e causar danos.

O livro *A Ética dos Hackers e o Espírito da Era da Informação: a Diferença Entre o Bom e o Mau Hacker*, editado no Brasil pela editora Campus, mostra um pouco do que essas pessoas pensam:

- Hacker: o termo hacker foi, por muitos anos, associado a pessoas mal-intencionadas.

Um hacker é apenas uma pessoa que detém muitos conhecimentos sobre a área de computação. Em geral, são pessoas interessadas em Sistemas Operacionais, softwares, segurança, internet e programação. Um hacker tem interesse em descobrir coisas novas (inclusive vulnerabilidades em programas), mas não possui nenhuma motivação destrutiva.

É possível usar a rede de forma segura? Qual o nível de perigo na internet neste momento? Veja em: https://webapp.iss.net/gtoc/index.html

- Cracker: um cracker é um hacker com propósitos maldosos de invadir e violar a integridade de sistemas.

Script kiddies normalmente não estão interessados em algo específico, mas simplesmente em invadir um site qualquer. São responsáveis por boa parte dos ataques na internet e provavelmente serão os responsáveis caso o seu site seja atacado. No site do projeto Honeynet (http://project.honeynet.org/papers/) podem ser encontradas diversas informações sobre script kiddies e o seu modo de ação.

Script kiddies:

- Com pouco conhecimento de informática, usam exploits criados pelo hacker e executam ataques na internet.
- Possuem muito tempo ocioso.

Lammer:

- Considerado o nível mais baixo, ou seja, aquele indivíduo que não conhece o poder do computador e se autodenomina hacker ou pensa ser um cracker e sai invadindo o host pela internet, sem ao menos saber o que está fazendo.
- Conhecimento ainda menor do que o de um script kiddie.

Newbie:

- Aprendiz de hacker; pergunta muito, é ignorado e ridicularizado.
- Possui personalidade fraca.

Wannabe:

- Indivíduo que já consegue assimilar a metodologia hacker, começando a ter afinidade com a tecnologia "underground".
- Não é necessariamente um script kiddie, mas alguém iniciado no uso de ferramentas mais básicas.
- Terminologia pouco utilizada.

Larva:

- Indivíduo capaz de executar invasões a partir de "receitas de bolo" e exploits encontrados na internet, mas diferente dos script kiddies, já que são capazes de compreender o que estão fazendo e até de melhorar técnicas e ferramentas.
- Estão mais próximos do nível de conhecimento de um cracker.

Virus Maker (virii):

- Crackers que se dedicam a programar vírus.

Carding:

- Criminosos digitais que se especializam na manipulação de clonagem de cartões magnéticos de bancos.
- No cenário brasileiro, tem sido registrado o aumento das atividades de Carding.

Phreakers:

- Crackers com profundos conhecimentos de telecomunicações, além dos conhecimentos em computação.

Motivação

O que leva uma pessoa a invadir um sistema?

- Impunidade.
- Delinquência
- Tentativa de chamar a atenção.
- Notoriedade.
- Vingança.
- Compensação financeira.
- Espionagem.
- Entrar para o grupo.

"Ninguém se torna um hacker, hackers nascem assim. Está certo! Muitos deles nunca terão acesso a um computador, logo nunca serão hackers de fato, mas o espírito hacker está presente naquela pessoa e vai acompanhá-la pelo resto da vida. Respondendo a essa pergunta, me sinto um pouco como The Mentor no manifesto hacker, quando ele pergunta 'But did you (...) ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?' (Mas você já olhou por trás dos olhos de um hacker? Você já imaginou o que faz pulsar, que forças deram-lhe forma, o que pode tê-lo moldado?). A resposta de hoje é a mesma que a de 1986, quando o manifesto foi escrito: hackers são pessoas inquietas, que não são facilmente convencidas por argumentos de autoridade sem valor técnico. São céticos sempre prontos a duvidar de qualquer coisa. A simples menção de que algo é impossível para um hacker é um poderoso convite para que ele tente fazê-lo. Eles querem saber mais sobre tudo (mais ainda sobre informática), simplesmente pelo fato de saber, para obter iluminação pessoal."

Roteiro de Atividades 3

Atividade 3.1 – Controles de informática

1. Sua instituição possui segurança e controle sobre a informática? Faça o teste em: http://securityassessment.trendmicro.com/Default.aspx?lang=pt-BR
2. Quais portas e serviços estão acessíveis na sua máquina? Faça a auditoria em: https://www.grc.com/x/ne.dll?bh0bkyd2
3. Use todas as portas de serviço e descreva as que estão abertas em seu computador, assim como seus serviços.

4. Teste os servidores de DNS e de correio eletrônico de sua instituição, fazendo a auditoria nos seguintes sites:

http://www.ipok.com.br/

http://www.dnsstuff.com

Você encontrou alguma vulnerabilidade conhecida?

Atividade 3.2 – Serviços e ameaças

1. Verifique as seguintes listas de portas:

- Ataque: http://www.portalchapeco.com.br/~jackson/portas.htm
- Aplicações especiais: http://www.practicallynetworked.com/sharing/app_port_list.htm
- Usadas por trojans: http://www.pypbr.com/infovir/port_alf_trojan.asp
- Usadas por serviços: http://www.pypbr.com/infovir/port_usad_a.asp
- No Windows: c:\windows\system32\drivers\etc\services
- No Linux: /etc/services

2. De posse dessas informações, você consegue informar as portas mais vulneráveis? Explique.

3. Baixe o programa spybot no link http://www.safer-networking.org/spybot2-own-mirror-1/.
4. Instale-o em seu computador e verifique se você foi vítima de algum tipo de malware.

5. O hijackthis é um programa que auxilia o usuário a eliminar uma grande quantidade de malwares conhecidos. Apesar de ser uma ferramenta poderosa, não tem a automatização de ferramentas como o spybot, e exige conhecimento mais avançado por parte do usuário.
6. Baixe o programa no link http://sourceforge.net/projects/hjt/ e faça a instalação do programa no computador.

Instalação

1. Crie uma pasta chamada C:\HijackThis\;
2. Copie o instalador para a pasta criada;
3. Rode o instalador.

Criação de log

Um log do HijackThis pode conter várias informações sobre malwares infectados no computador. Você pode gerar um log através da opção "Do a system scan and save a logfile".

Corrigindo entradas

1. Clique em "Do a system scan only".
2. Marque as entradas necessárias com atenção, pois uma entrada errada pode causar instabilidade no sistema.
3. Clique em "Fix Checked".
4. Você constatou algum tipo de arquivo malicioso encontrado pela ferramenta?

4

Arquitetura TCP/IP – conceitos básicos

objetivos

Apresentar o funcionamento da família de protocolos TCP/IP, desde o nível físico até o nível de aplicação em questões de segurança; diferenciar as camadas da família TCP/IP e identificar seus principais protocolos; mostrar o funcionamento de aplicações básicas, como serviço de nomes, transferência de arquivos, correio eletrônico e páginas www; ensinar a captura de tráfego real em uma rede e identificar o que foi capturado.

conceitos

Projetos de rede, sniffers, família de protocolos TCP/IP, camadas física, de rede, de transporte e de aplicação.

Exercício de nivelamento 1
Arquitetura TCP/IP

O que são protocolos?

Introdução

Características da arquitetura TCP/IP:

- Baseado na arquitetura cliente/servidor.
- O IP usa esquema de endereçamento universal.
- Trabalha com:
  - Dados, voz e vídeo.
  - Velocidades: de 9.600 bps a Gbps.
  - Redes: LAN, MAN, WAN e WLAN.
  - Máquinas: servidores, computador pessoal, mainframe, laptop e celular.
  - Plataformas: Mac, Intel, PowerPC, Sun, AMD etc.
  - Sistemas Operacionais: Windows, Linux, MacOS, FreeBSD, Solaris etc.

O TCP/IP foi criado por volta de 1974, a partir de um artigo escrito por VintCerf. Nos anos 80, ele foi se popularizando e se tornando o protocolo padrão de comunicação na internet. Atualmente, o TCP/IP é considerado um "padrão de fato" e é o protocolo mais usado para interconexão de sistemas heterogêneos. Neste Capítulo, veremos o funcionamento básico do protocolo TCP/IP, além de algumas considerações sobre segurança.

Família de protocolos TCP/IP

- Formada por vários protocolos; TCP e IP são os dois mais importantes:
  - Transmission Control Protocol (TCP): protocolo da camada de transporte.
  - Internet Protocol (IP): protocolo da camada de rede.
- Dividida em camadas com funções bem definidas.
- Cada camada presta serviço para a camada superior.
- Funcionalidades das camadas de sessão, apresentação e aplicação do modelo OSI são fornecidas por uma única camada de aplicação no TCP/IP.

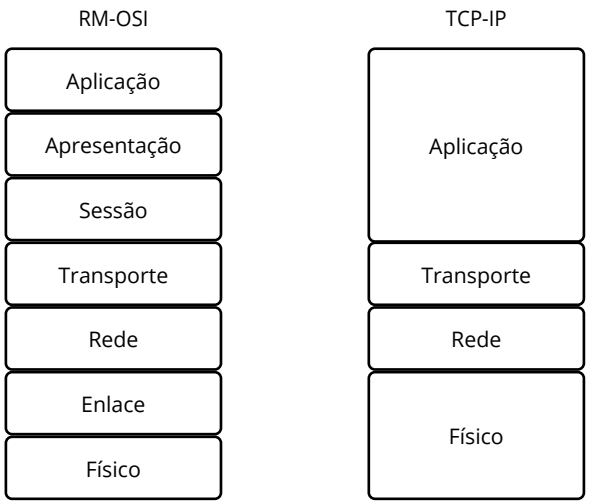


Figura 4.1
Comparação entre os modelos RM-OSI e TCP/IP.

Camada física

Equipamentos de interconexão física.

- Hub.
- Bridge.
- Switch.

Endereçamento físico.

A camada física não é padronizada no TCP/IP. Ela varia de acordo com a tecnologia de acesso físico utilizada (exemplo: Ethernet, ATM e PPP). Compreende tanto a camada física quanto a camada de enlace do modelo RM-OSI.

Do ponto de vista de segurança, é importante conhecer os principais tipos de dispositivos de interconexão física utilizados e as implicações de segurança de cada um desses dispositivos.

Hub (Ethernet)

- Forma mais simples de interconexão em LANs.
- Não possui inteligência (processador).
- Atua somente na camada física OSI.
- Possui n portas.
- Problemas:
  - Propaga ruído elétrico para todas as portas.
  - Faz broadcast do pacote a nível físico.
  - Segurança facilita escuta na rede (sniffing).
  - Interface de rede em modo promíscuo (sniffer).
  - Cria domínio de colisão.
  - Permite apenas uma comunicação simultânea.
- Uso de HUB está diminuindo gradativamente.



Figura 4.2
Modelo de hub.

Bridge (Ethernet)

- É um equipamento que conecta dois segmentos LAN.
- Possui inteligência (processador).
- Atua na camada de enlace OSI.
- Possui duas portas.
- Soluções:
  - Imune a ruído elétrico.
  - Não faz broadcast dos pacotes a nível físico.
  - Segurança evita sniffing entre suas portas.
  - Retransmissão seletiva: tabela porta x MAC (Ethernet).
  - Gera confinamento de tráfego entre suas portas.
  - Divide domínio de colisão.



Figura 4.3
Transceivers e bridges Ethernet.

Problemas:

- Permite apenas uma comunicação simultânea entre suas portas.
- Cria domínio de broadcast nível de enlace.

Switch (Ethernet)

É uma bridge inteligente de *n* portas.

Soluções:

- Permite várias conexões simultâneas entre suas portas.
- Densidade maior de portas para conexão.
- Dificulta "escuta" na rede.
- Recursos avançados (autenticação, filtragem etc.).

Problemas:

- Custo mais elevado.
- Crescimento da rede (escalabilidade).
- Broadcast nível de enlace.



Figura 4.4
Switch de pequeno porte.

Em termos de segurança, um switch é sempre preferível para interconexão em rede local a um hub, porém o custo de um switch é muito maior. Nesse caso, a relação entre custo e segurança deve ser posta na balança. No caso do hub, os problemas de segurança podem ser amenizados de outras formas, como o uso de criptografia.

Prevenção:

- Topologia hierárquica.
  - Nível 1: switch de núcleo (core) chassi.
    - Uma unidade, muitos recursos, alta performance, custo elevado.
  - Nível 2: switch de distribuição.
    - Algumas unidades.
  - Nível 3: switch de acesso.
    - Muitas unidades, menos recursos, menor performance, custo baixo.
- Redes Microsoft Windows: uso de servidor Wins.
  - Diminui drasticamente o broadcast.
    - Uso de router para dividir domínios de broadcast.



Figura 4.5
Família de switches de grande porte (chassi).

Um switch pode suportar diversas tecnologias de acesso físico (ATM, Ethernet e Gigabit Ethernet) e diversos tipos de cabos e conectores (par trançado e fibra ótica).

Endereçamento físico

Camada de enlace OSI: protocolo Ethernet.

- Usa endereço universal Media Access Control (MAC).
- Hexadecimal: 6 conjuntos de 8 bits – exemplo: 00:00:0c:40:df:51.
  - Três primeiros conjuntos identificam o fabricante.
- Endereços reservados.
  - FF:FF:FF:FF:FF:FF (broadcast).
  - 01:00:5E:xx:xx:xx (multicast).

Padrões:

- Ethernet: 10 Mbps half duplex.
- Fast Ethernet: 100 Mbps full duplex.
- Gigabit Ethernet: 1 Gbps full duplex.

Para encontrar uma tabela com os fabricantes associados aos três primeiros conjuntos de 8 bits, acesse: http://standards.ieee.org/regauth/oui/oui.txt

O protocolo Ethernet foi criado a partir do protocolo Aloha, criado na Universidade do Havaí, nos anos 70. Posteriormente, foi aprimorado pela Xerox, que criou o padrão Ethernet de 10 Mbps de transmissão. Hoje temos, ainda, o Fast Ethernet a 100 Mbps e o Gigabit Ethernet a 1 Gbps. O protocolo Ethernet opera com diversos tipos de cabeamento, como fibra ótica, par trançado (UTP) e coaxial.

Camada de rede

- Protocolo IP.
- Endereçamento IP
- Subnetting.
- Protocolos auxiliares.
- Endereçamento dinâmico.
- Roteamento.

A camada de rede é responsável por interligar as diferentes redes presentes na internet. É composta, principalmente, pelo protocolo IP (Internet Protocol). A camada de rede tem por objetivo prover uma forma de transportar informação entre uma origem e um destino, independentemente de essas máquinas estarem na mesma rede.

Protocolo IP (Internet Protocol)

- Entrega o pacote e escolhe a rota entre os pontos local e remoto.
- Na camada de rede, a informação é representada por datagramas IP.
- Datagrama IP: cabeçalho (64 bytes no máximo) + área de dados.

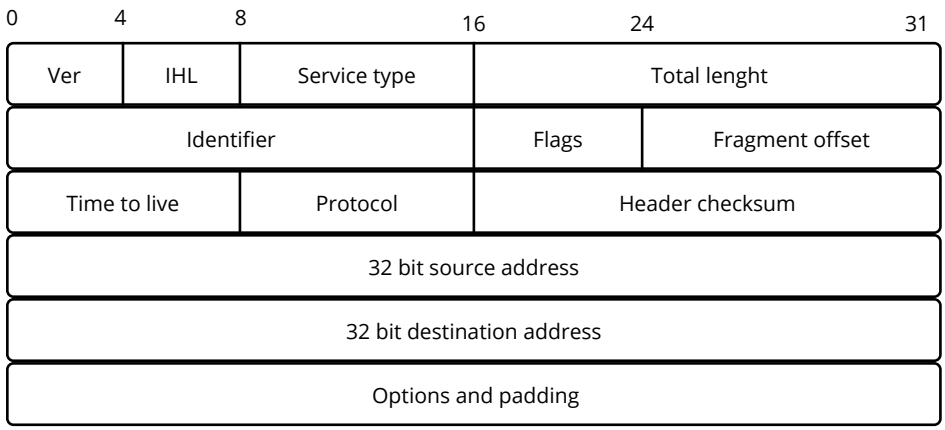


Figura 4.6
Cabeçalho IP.

Campos do cabeçalho :

- **Ver**: define a versão do protocolo. Atualmente, versão 4 (IPv4) e versão 6 (IPv6).
- **IHL**: define o tamanho do cabeçalho, uma vez que ele não é fixo.
- **Service Type ou Type of Service (TOS)**: representa uma classe de serviço que pode ser usada para priorizar certos tráfegos, como voz e vídeo.
- **Total Length**: define o tamanho total do datagrama IP. Tamanho máximo: 65535 bytes.
- **Identifier**: identifica um fragmento no caso de o datagrama ter sido quebrado em pedaços menores (fragmentos).
- **Flagse Fragment offset**: campos auxiliares para ajudar a recompor fragmentos.
- **Time To Live (TTL)**: determina o tempo de vida do datagrama.
- **Protocol**: define protocolo da camada de transporte; as opções são o TCP e o UDP.
- **Header checksum**: verifica se as informações do cabeçalho foram transmitidas sem erros; o IP não garante a transmissão dos dados, apenas a do cabeçalho.
- **Source address**: endereço IP de origem.
- **Destination address**: endereço IP de destino.
- **Options**: opções extras do IP.

O protocolo IP não é um serviço confiável:

- Entrega com menor esforço.
- Recuperação do pacote na camada superior.

O protocolo IP não é um serviço orientado à conexão:

- Pacotes são roteados independentemente.
- Pacotes são entregues fora de ordem; reordenamento na camada superior.

Endereçamento IP

Endereço universal de 32 bits escrito com quatro números decimais que identifica unicamente uma interface de rede. Exemplo: 200.221.2.45.

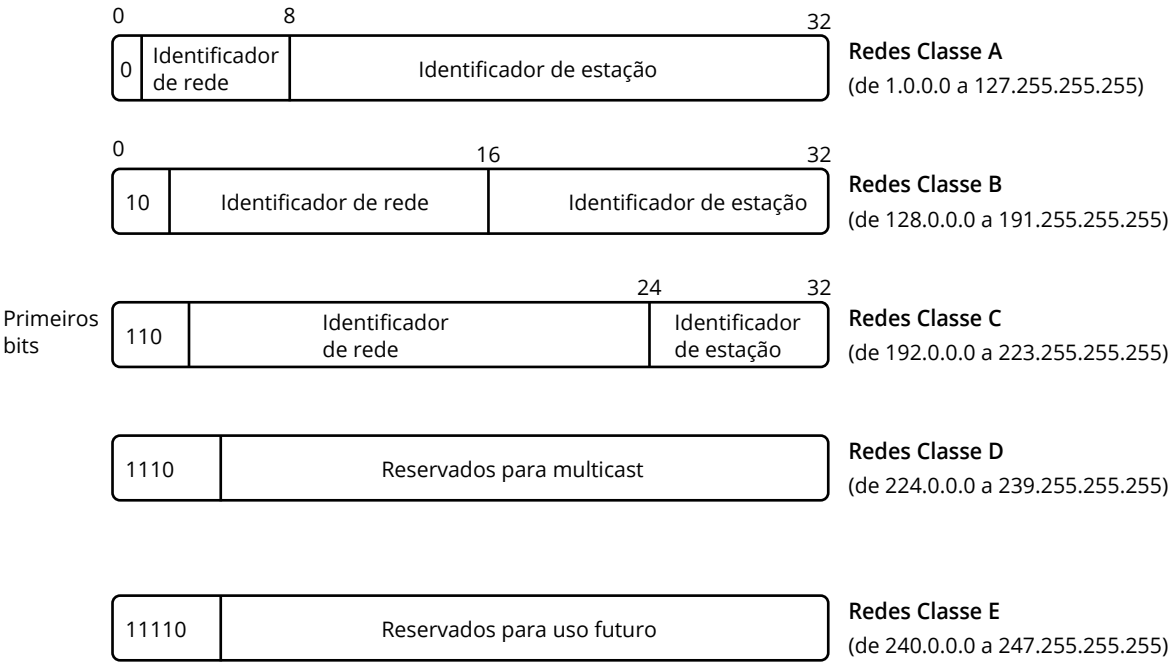


Figura 4.7 Classes de endereçamento IP.

- Estrutura hierárquica, com divisão em duas partes: rede e estação.
- Divisão feita de duas formas: classe ou máscara.
- Endereçamento por classe (classful).

Endereços para propósitos específicos:

- 0.0.0.0 – Máquina em processo de inicialização.
- 127.xx.yy.zz – Loopback (127.0.0.1 auto-teste da pilha TCP/IP).
- Primeiro IP da rede, por exemplo: 200.200.200.0 (endereço da rede 200.200.200.0/24).
- Último IP da rede, por exemplo: 200.200.200.255 (endereço de broadcast).

Tabela 4.1 Faixa de endereços privados.

Nome	Faixa de endereços IP privados	Números de IPs	Classful Descrição	Maior bloco CIDR	Referência
8-bit block	10.0.0.0 – 10.255.255.255	16,777,216	Uma classe A	10.0.0.0/8	RFC 1597 RFC 1918
12-bit block	172.16.0.0 – 172.31.255.255	1,048,576	16 classes A	172.16.0.0/12	
16-bit block	192.168.0.0 – 192.168.255.255	65,536	256 classes C	192.168.0.0/16	
16-bit block	169.254.0.0 – 169.254.255.255	65,536	Uma classe B	169.254.0.0/16	RFC 3330 RFC 3927

Endereços reservados (intranet):

- Não é necessário que todas as máquinas internas possuam IP público.
- Os roteadores da internet descartam qualquer tráfego que use IP privado.
- Proíbe que uma máquina interna abra conexão direta com servidor na internet e vice-versa.
- Existem outras classes de IP e IPs especiais definidos na RFC 5735.

Subnetting (endereçamento por sub-rede)

Subnetting é a divisão de uma classe em redes menores.

- Classes A, B e C alocam muitos endereços para uma rede.
- As faixas disponíveis para endereços IP regulares estão terminando.
- Intranet e servidores proxy permitem "economia" com endereços IP públicos.

Parte do endereço reservado para estações é usada para endereçar sub-redes.

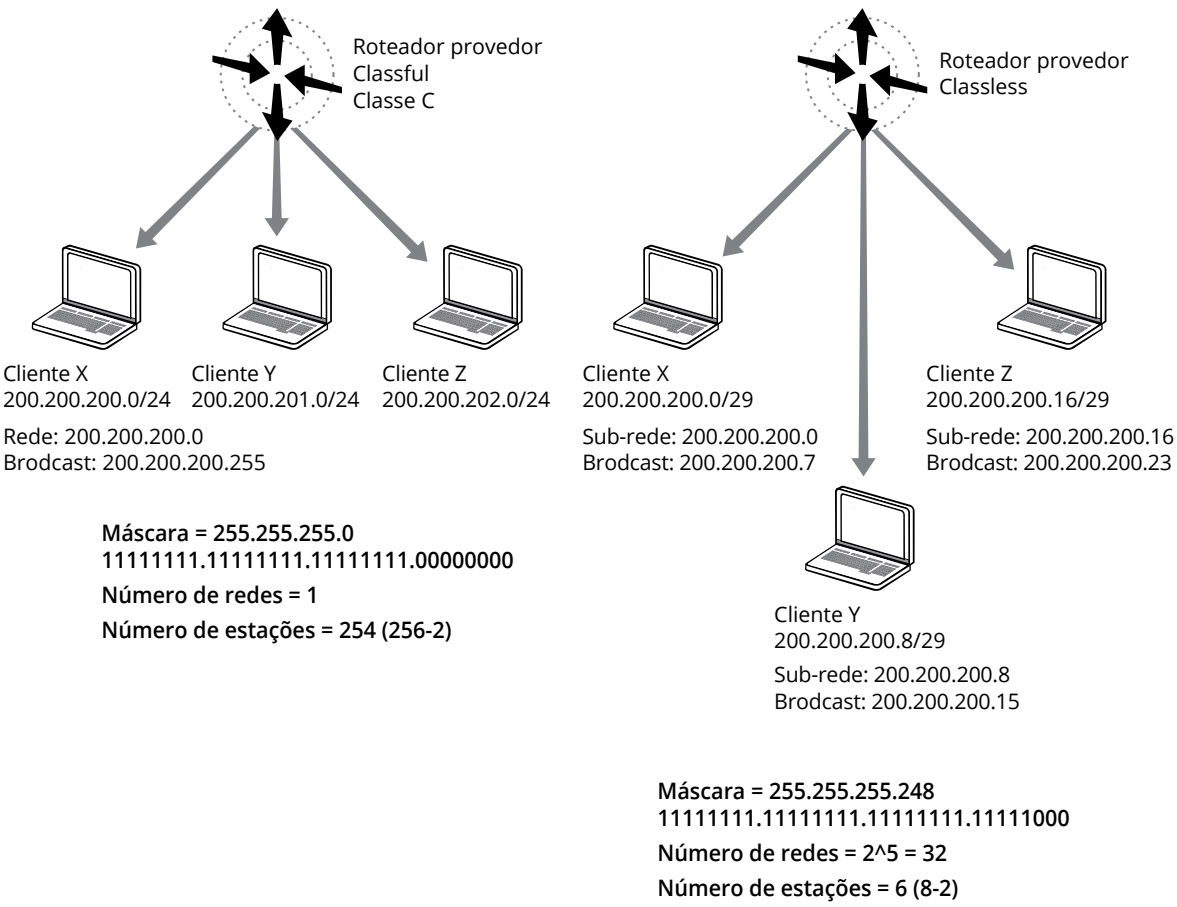


Figura 4.8
Endereçamento por sub-rede.

Protocolos auxiliares (ARP, RARP e ICMP)

- Na LAN Ethernet, o tráfego segue endereçamento MAC e não endereçamento IP.
- Como descobrir o MAC de um IP qualquer de uma estação na LAN?
  - Address Resolution Protocol **(ARP)**: mapeia endereço IP em endereço MAC.
- Como descobrir o IP de um MAC qualquer de uma estação na LAN?
  - Reverse Address Resolution Protocol **(RARP)**: mapeia endereço MAC em endereço IP.

- Cache ARP: mantido em cada estação com os últimos mapeamentos.

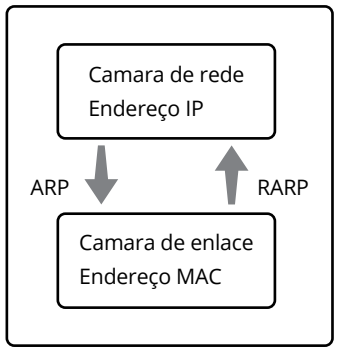


Figura 4.9
ARP e RARP.

O ARP é um protocolo fundamental para permitir que o IP trabalhe em cima de diferentes tecnologias físicas. Em uma rede local, a máquina de IP A quer falar com a máquina de IP B. A máquina de IP A envia uma pergunta (ARP Broadcast) para toda a rede, querendo saber qual máquina possui o IP B. Se a máquina de IP B estiver ativa na rede, então responde para a máquina A, se identificando.

A máquina com IP A mantém durante algum tempo uma tabela chamada "tabela ARP", onde fica mapeado o endereço (físico) ARP e o endereço IP. Existem variações do ARP para outras tecnologias, como o Atmarp, por exemplo, para redes **ATM**.

ATM
Asynchronous Transfer Mode (Modo de Transferência Assíncrono) é uma tecnologia de rede que permite transferir simultaneamente numa mesma linha dados e voz.

No Sistema Operacional Windows, execute:

```
C:\ arp -a
```

ICMP

Internet Control Messages Protocol (ICMP):

- Protocolo utilizado para a troca de mensagens de erro e controle entre estações e outros equipamentos de rede.
- Ping: pacote ICMP dos tipos echo request e echo reply.

Principais tipos de ICMP:

- **Tipo 0 (echo-reply)**: a resposta de um ping.
- **Tipo 3 (destination unreachable)**: destino inalcançável, usado para avisar ao host solicitante sobre uma possível falha de alcance a um host de destino.
- **Tipo 4 (sourcequench)**: avisa ao host solicitante para diminuir a intensidade da comunicação: "fale mais devagar".
- **Tipo 5 (redirect)**: redirecionamento é um host informando ao solicitante para alterar uma rota.
- **Tipo 8 (echo-request)**: é a solicitação do ping.
- **Tipo 9 (router advertisement)**: anúncio de roteador, usado para descobrir um roteador na rede.
- **Tipo 10 (router solicitation)**: seleção de roteador, usado para descoberta de um roteador.
- **Tipo 11 (Time to Live exceeded)**: timeout de TTL (tempo de vida); um pacote pode estar em loop, ou a rede congestionada.
- **Tipo 12 (IP header bad)**: cabeçalho do pacote IP com problemas.

Endereçamento dinâmico

- Como configurar pilha TCP/IP de centenas ou milhares de estações da rede?
- DHCP faz a atribuição automática do endereçamento IP para as estações:
  - Configura automaticamente as estações da rede quando conectadas.
  - Atribui endereço IP, máscara, default gateway e servidores de DNS.
  - Protocolo mais usado, sucessor do BOOTP, descrito na RFC 1541.
  - Atribui endereço com prazo definido.

A vulnerabilidade do DHCP é permitir ao usuário malicioso ocultar sua identidade. Como identificar uma estação através de seu endereço IP dinâmico? Como filtrar o acesso de uma máquina estranha à rede?

Prevenção:

- Filtrar MAC das estações;
- Fixar IP a um MAC;
- Tratar logs dos pedidos ao servidor DHCP.

Exercício de fixação 1
Endereçamento dinâmico

O que é DHCP?

Roteamento

Roteador:

- Estação que pode traspassar pacotes entre suas interfaces de rede.
- Hardware específico ou PC com Sistema Operacional e suporte ao roteamento TCP/IP.

Roteamento:

- Processo inteligente que define a interface para qual o pacote será enviado, valendo-se de uma tabela de rotas.
- Roteamento estático ou manual.
- Roteamento dinâmico: protocolos RIP, OPSF, BGP etc.



Figura 4.10
Modelo de roteador.

Tabela de rotas:

- Conjunto de regras que define a interface ou roteador que receberá o pacote de acordo com o endereço IP de destino.
- A rota se baseia no endereço de destino.
- Comunicação entre cliente A e servidor B.
- Vulnerabilidade: não há verificação do endereço de origem ao longo do caminho.

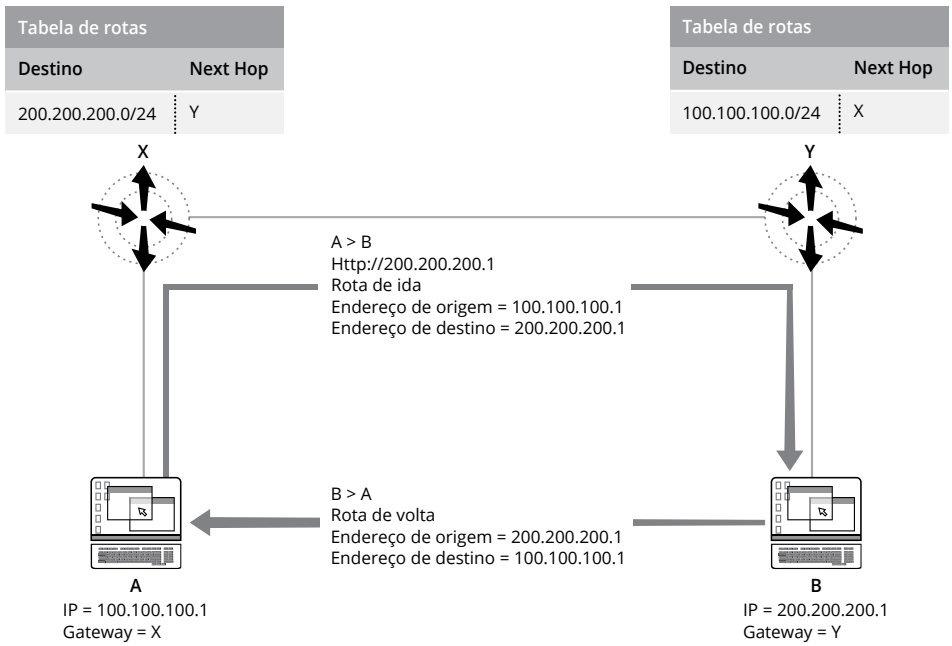


Figura 4.11
Tabela de rotas.

Exercício de fixação 2
Roteamento

O que é roteamento?

O que são tabelas de rotas?

Camada de transporte

A camada de transporte do TCP/IP possui dois protocolos:

- TCP.
- UDP.

A camada de transporte é responsável por criar um canal de comunicação entre duas aplicações. Esse canal pode ser confiável ou não, dependendo do protocolo usado. A aplicação utiliza diretamente os serviços da camada de transporte, sendo essa camada a responsável por toda a transmissão entre a aplicação de origem e a de destino. A camada de transporte do TCP/IP possui dois protocolos: TCP e UDP. No momento da programação da aplicação, deve ser informado o protocolo a ser usado de acordo com a necessidade.

TCP

- Orientado para conexão, provê canal confiável fim a fim em rede não confiável, criando socket no emissor e no receptor.
- **Confiabilidade**: o dado chegou ao destino? Retransmite.
- **Integridade**: os dados chegaram em ordem correta? Reordena.

- **Socket**: canal por onde fluem os dados; elo bidirecional de comunicação entre dois programas
  - IP (ID rede + ID estação) + TCP-UDP (ID porta) + ID processo (servidor/cliente).



Figura 4.12
TCP: orientado para conexão.

- **TCP**: foi definido na RFC 793 e corrigido na RFC 1122, com extensões definidas na RFC 1323.
- **Porta TCP**: número inteiro entre 0 e 65535 (16 bits) que, junto com os endereços IP associados, identificam uma conexão no nível de transporte do TCP/IP. Um processo servidor necessita "escutar" uma porta para oferecer um serviço, e um processo cliente necessita alocar uma porta dinâmica (maior que 1024) para utilizar o serviço oferecido pelo servidor.

As portas TCP podem ser divididas em ranges, como demonstrado na tabela a seguir.

Início	Fim	Nome
0	1023	Portas conhecidas
1024	49151	Portas registradas
49152	65535	Portas particulares

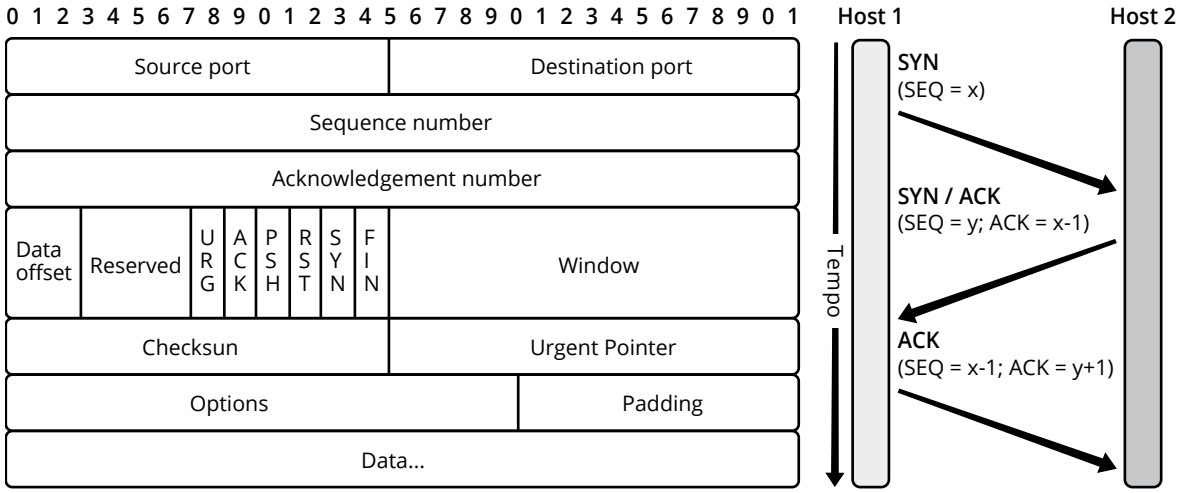
Tabela 4.2
Tabela das portas TCP.

Cabeçalho TCP

Estabelecimento de conexão TCP:

- Host1 envia sinal SYN para host2.
- Host2 responde enviando sinal SYN combinado com sinal ACK.
- Host1 responde com outro sinal ACK.
- Conexão feita em três transmissões.
- Three-way handshake (triplo aperto de mãos).

Mais informações podem ser obtidas em http://www.iana.org/assignments/port-numbers



Cabeçalho TCP

Figura 4.13 Cabeçalho TCP e o triplo aperto de mãos.

Os campos do cabeçalho são:

- **Source port**: porta de origem. Dinamicamente, primeira porta livre maior que 1024.
- **Destination port**: porta de destino. Deve ser conhecida.
- **Sequence number**: número de sequência.
- **Acknowledgement number**: informa o próximo byte esperado pelo receptor.
- **TCP header length**: informa o tamanho do cabeçalho TCP.
- **Reserved**: seis bits reservados para uso futuro.
- **Flags**: campos de 1bit que podem estar ligados (1) ou desligados (0).
- **URG (Urgent pointer)**: informa que existe informação urgente no pacote.
- **ACK (Acknowledge)**: indica a presença do campo Acknowledgement number.
- **PSH**: indica que os dados devem ser imediatamente entregues para a aplicação.
- **RST**: usado para reinicializar uma conexão com problemas.
- **SYN**: usado para estabelecer conexões.
- **FIN**: usado para finalizar conexões.
- **Window size**: indica quantos bytes podem ser enviados de uma vez; controle de fluxo.
- **Checksum**: verifica erros no cabeçalho e nos dados. Torna o TCP confiável.
- **Urgent pointer**: indica onde estão os dados urgentes (flag URG).
- **Options**: opções extras do cabeçalho TCP.

UDP

Protocolo não orientado para conexão, é uma versão simplificada do TCP.

- Não garante entrega.
- Não garante ordenamento.
- Não garante ausência de erros.

Proporciona velocidade.

- Usado para streaming de vídeo.
- Sinal de voz (VoIP).
- Montagem de rede NFS.

Aplicações de requisições e respostas simples.

- Requisições de DNS.

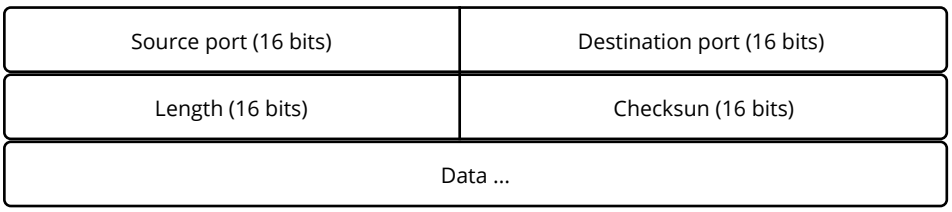


Figura 4.14
Cabeçalho UDP.

Os dois primeiros campos têm o mesmo propósito que o TCP, o de identificar as aplicações de origem e de destino. O campo length define o tamanho do pacote UDP (inclusive os dados) e o checksum apenas verifica erros no cabeçalho. O UDP, por ser mais simples, é muito usado em serviços em que a velocidade de transmissão é mais importante que a ausência de erros, como a transmissão de voz e vídeo.

Camada de aplicação

Há muitas aplicações na internet. A lista seguinte mostra algumas delas e suas portas padrão.

Aplicação	Portas	Descrição
Gmail	TCP 465 TCP 995	Correio eletrônico SMTP com segurança (SSL). Correio eletrônico POP3 com segurança (SSL).
Skype	TCP 80 TCP 1024-65535 UDP 1024-65535	Telefonia VoIP via internet. Tráfego de voz.
eMule	TCP 4662 UDP 4672	P2P popular.
www	TCP 80	World wide web, serviços de páginas com hipertexto.

Tabela 4.3
Portas UDP.

Tipos de firewalls versus modelo OSI

- O modelo OSI é um modelo de referência para que possamos compreender melhor a organização hierárquica de serviços e dispositivos de rede.
- Podemos compreender melhor os tipos de firewalls a partir do ponto de vista do modelo OSI, tanto quanto a atuação, quanto em relação à categoria, que pode ser Ativo ou Bridge.

Camada OSI

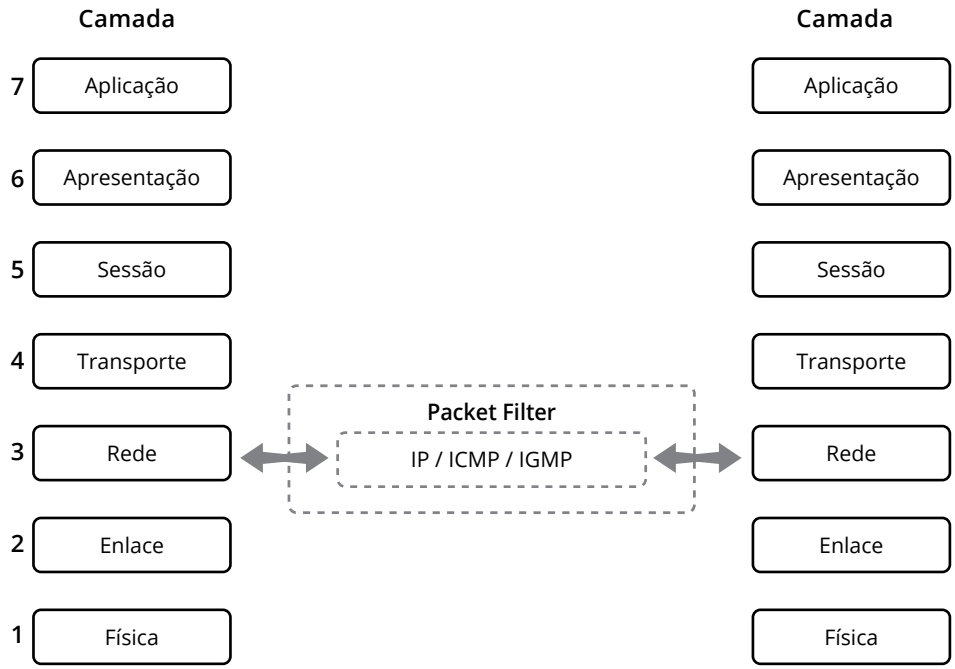


Figura 4.15
Packet Filter – Camada OSI.

Packet Filter (filtro de pacotes)

Controle seletivo do fluxo de dados de uma rede, possibilitando o bloqueio ou não de pacotes, através de regras normalmente baseadas em:

- Endereços IP;
- Protocolos (portas).

Possibilidade de tratar o início da conexão (TCP SYN). Nesse caso, deixando de ser um mero Packet Filter para ser um StateLess.

Embora um Packet Filter seja um firewall de camada 3, é importante lembrar que informações de número de porta vêm do cabeçalho UDP ou TCP, mas mesmo assim definimos que um Packet Filter é de camada 3. Todavia, devemos considerar porta de origem e porta de destino, embora endereçamento ainda seja um tratamento simples para uma comunicação de dados.

Stateful (Filtragem com Estado de Conexão)

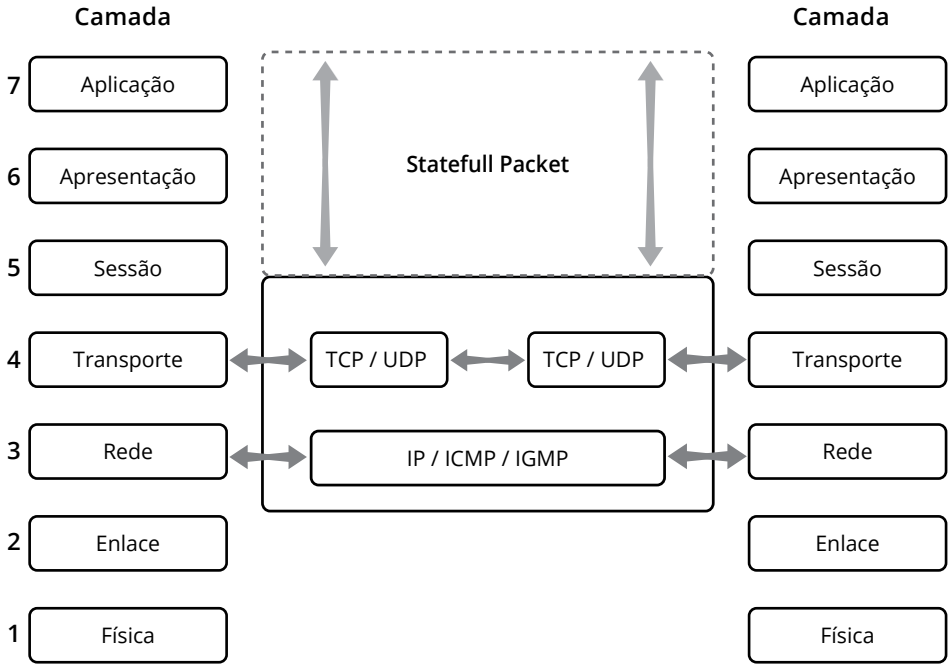


Figura 4.16
Stateful – Camada OSI.

Além de ter a mesma capacidade de tratamento de pacotes que um firewall Packet Filter, esse tipo de tecnologia também pode manter o estado das conexões por meio de máquinas de estado. Alguns firewalls ainda são capazes de atuarem como proxy de conexões de serviços específicos ou simplesmente analisarem o conteúdo de um pacote buscando perfis de ataques, embora muitos administradores optem por ter essa análise de ataques em sistemas de detecção de intrusos (IDS). Dessa forma, os firewalls que se enquadram nessa tecnologia possibilitam:

- Detecção e bloqueio de stealth scans;
- Realização do controle seletivo do fluxo de dados e tratamento do cabeçalho TCP;
- Ser capaz de lidar com protocolos mais específicos, como FTP (ativo e passivo);
- Manter informações de estado de conexão;
- Manipulação de campos de um datagrama.
- Capacidade de manipular o payload do pacote, inclusive tendo a possibilidade de atuar procurando strings de ataque.

Bridge Statefull

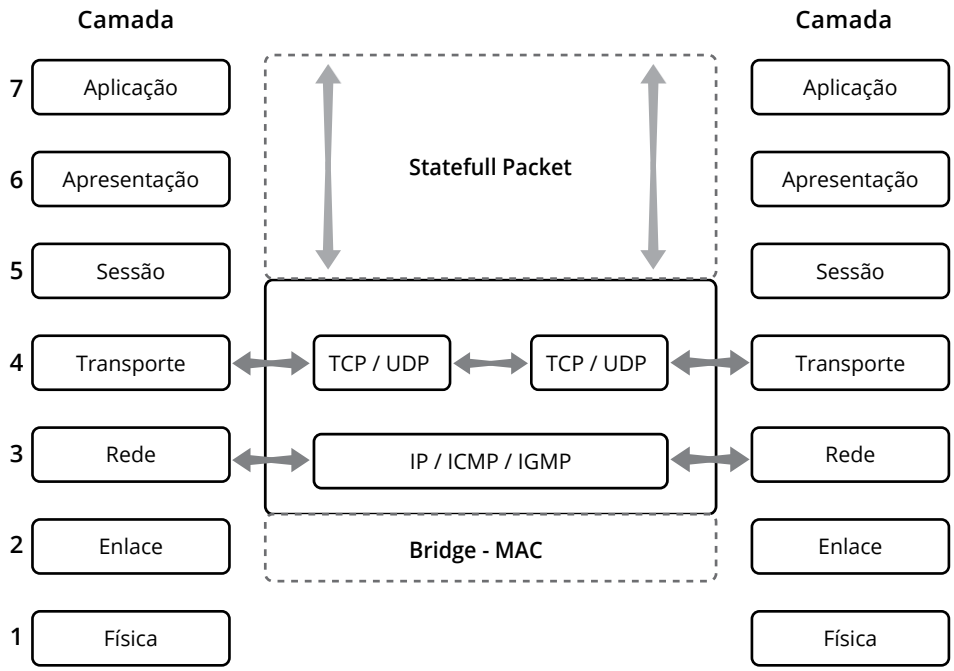


Figura 4.17
Bridge Statefull – Camada OSI.

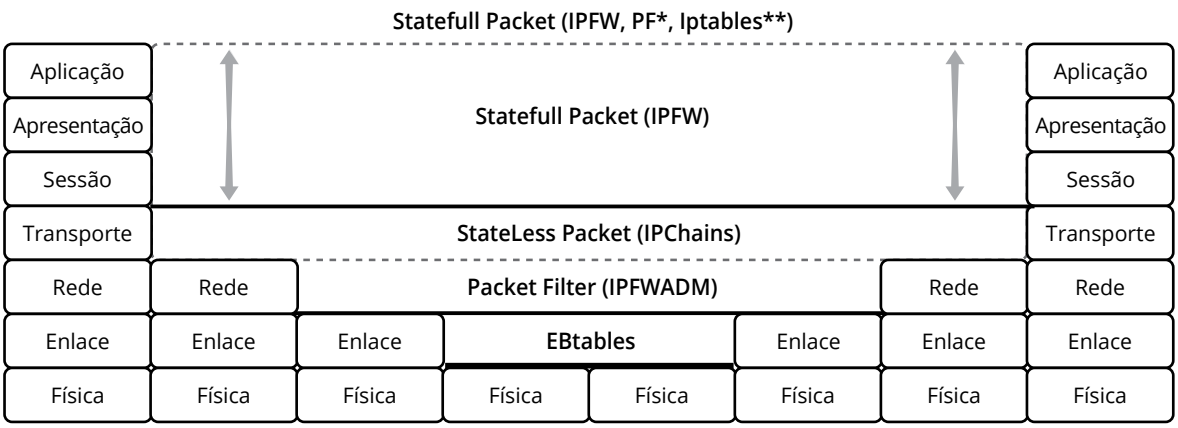
Tipos de firewall

Ativos que podem ser implantados tanto em fronteira de redes com gateway, como também em ambiente departamental são identificáveis com host, pois possuirão um IP e serão acessíveis através dele. Todavia, um firewall que atua com um proxy ARP (bridge como uma ponte na camada de enlace) na fronteira da rede é extremamente estratégico, pois não tem IP, isto é, só é acessível localmente ou por outra máquina que tenha uma comunicação serial com o firewall.

Soluções de firewall

- **PF***: original do OpenBSD, disponível na série 5 do FreeBSD.
- **Iptables (netfilter)****: solução Stateful nativa do Linux.
- **Ebtables**: solução de Firewall Bridge para Linux.

Figura 4.18
Soluções de firewall – Camada OSI.



Kernel 2.0.x

- **IPF**: PacketFilter.
- **IPFWADM**: PacketFilter.

Kernel 2.2.x

- **IPChains**: PacketFilter.
- **Sinus**: PacketFilter.

Kernel 2.4.x / 2.6.x

- **Iptables (Netfilter)**: Stateful Packet.

Soluções "Open Source Stateful"

- **IPFW2**: disponível em sistemas FreeBSD.
- **IPFW2 e PF**: disponível em sistemas FreeBSD e OpenBSD.
- **IPF**: Solaris 10.

No Linux, o nome do firewall presente no Kernel é o Netfilter, sendo o Iptables a interface para acessá-lo.

Sniffers



- Sniffer (farejador).
- Equipamento ou software para "escutar" ou "farejar" o que passa pela rede.
- Geralmente associado a um analisador de protocolos.

Normalmente uma placa de rede somente "escuta" o que foi direcionado para ela (seu equipamento) ou pacotes que são enviados para a rede toda (broadcast). Um sniffer coloca a placa de rede em um modo chamado de "promíscuo", onde a placa passa a "escutar" tudo o que está passando pela rede. Dependendo do tipo de equipamento de interconexão, hub ou switch, é possível "escutar" os pacotes passando pela rede com maior facilidade.

Mesmo não sendo impossível, o uso de switches dificulta o "sniffing", pois os pacotes direcionados a uma máquina são enviados diretamente para aquela máquina, diferente do hub, que replica todos os pacotes por todas as portas.

Em conjunto com um analisador de protocolos, podemos ver o que está acontecendo em nossa rede. As ferramentas mais conhecidas são as do TcpDump, atuando em linha de comando, e o Wireshark, em ambiente gráfico. Ambas as ferramentas são abertas e estão disponíveis para um grande número de sistemas operacionais e distribuições diferentes.

Roteiro de Atividades 4

Atividade 4.1 – Sniffers para captura de dados

1. Abra o Wireshark:

- Ative a captura de pacotes da placa de rede ethernet;
- No campo “Filtro”, digite FTP e clique em “Apply”.
- Acesse o site ftp.unicamp.br;
- Digite *aluno* como usuário e como senha digite 123456;
- Pare a captura de pacotes e verifique se você consegue visualizar o usuário e a senha informados.

Atividade 4.2 – Estados de firewall

O Netfilter é um framework dentro do kernel do Linux, onde os módulos do Iptables se conectam para realizar a filtragem de pacotes.

Tabelas

- Filter – filtragem de pacotes;
- NAT – tradução de endereços;
- Mangle – marcação de pacotes, QoS.

Políticas

Começar em DROP ou ACCEPT.

Chains

- INPUT – entrada no firewall;
- OUTPUT – saída do firewall;
- FORWARD – passagem pelo firewall.

Criação de regras

- -A – adiciona a regra ao final da chain;
- -I – insere a regra no começo da chain;
- -D – apaga a regra.

Padrões de casamento

- -s – casa com origem do pacote;
- -d – casa com destino do pacote;
- -i – interface de entrada;
- -o – interface de saída;
- -p – protocolo, que pode ser dos tipos TCP, UDP e ICMP.

1. Filtragem simples (Stateless)

- Logue no shell como root e mude a política padrão da chain OUTPUT para DROP:

```
# iptables -P OUTPUT DROP
```

- Tente estabelecer uma conexão http;
- Crie uma regra na chain OUTPUT para permitir que sua máquina estabeleça uma conexão http:

```
# iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
```



Não se esqueça de criar uma regra para conexões DNS do tipo UDP porta 53.

- Mude a política padrão da chain INPUT também para DROP. Ainda é possível estabelecer conexões http?

- Crie uma regra na chain INPUT para permitir que sua máquina estabeleça uma conexão http.

2. Filtragem com Estado (Stateful)

- Remova as regras da chain INPUT;
- Crie uma regra genérica para permitir conexões estabelecidas:

```
# iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
```

- Tente novamente estabelecer uma conexão http;
- Você é capaz de descrever a diferença entre filtros Stateless e Statefull?

5

Arquitetura TCP/IP e segurança

objetivos

Mostrar os problemas inerentes à família TCP/IP (exploits e vulnerabilidades) e informar as soluções disponíveis; apresentar os problemas específicos em implementações da família de protocolos; indicar mecanismos de defesa contra vulnerabilidades de protocolo.

conceitos

Varreduras, DOS básico e conceitos relacionados à segurança em rede TCP/IP.

Exercício de nivelamento 1
Arquitetura TCP/IP e segurança

O que é TCP/IP?

Introdução

Tipos de ataques inerentes ao protocolo:

- Sniffers.
- Sourcerouting.
- DoS.
- Spoofing.
- SYN flood.
- Smurf.
- Portscan.
- DDoS.

Vulnerabilidade em implementações específicas:

- Ping da morte.
- Teardrop.
- Land.

A família de protocolos TCP/IP, apesar de largamente utilizada, não é perfeita. Existem falhas conhecidas no projeto do protocolo e também na implementação em alguns sistemas específicos. Essas falhas são frequentemente exploradas por usuários maliciosos, especialmente as falhas de projeto, uma vez que não são facilmente resolvidas.

Muitas das falhas não têm solução total em muitos casos, sendo possível apenas diminuir seu efeito.

No capítulo anterior, vimos o funcionamento da família TCP/IP com padrão para acesso à internet. Neste capítulo, faremos algumas considerações sobre a família de protocolos e veremos alguns ataques conhecidos referentes ao protocolo TCP/IP. Alguns desses ataques são inerentes ao projeto do protocolo, enquanto outros são problemas de uma implementação específica.

Sniffers (farejadores)



Programa que "escuta" a rede em busca de informações importantes.

- **Uso benigno**: análise de tráfego, diagnóstico de problemas e base para IDS.
- **Uso maligno**: quebra de confidencialidade e captura de senhas.
- **Detecção**: uso da placa Ethernet em modo promíscuo.
- **Hub**: alvo fácil de um sniffer.

```
No. Time      Source          Destination      Protocol  Info
7   0.296046  192.188.11.45   200.144.121.118  IMAP      Response: *ok [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPAC
8   0.297487  192.188.11.45   200.144.121.118  IMAP      Response: *ok [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPAC
9   0.301595  200.144.121.118 192.188.11.45    IMAP      Request: xqbn CAPABILITY
10  0.305416  200.144.121.118 192.188.11.45    IMAP      Request: z1s1 CAPABILITY
11  0.449008  192.188.11.45   200.144.121.118  IMAP      Response: * CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPAC TH
12  0.449010  200.144.121.118 192.188.11.45    IMAP      Request: 8011 LOGIN "1vocarv" [redacted]
13  0.619910  192.188.11.45   200.144.121.118  IMAP      Response: 80j1 OK LOGIN OK
14  0.622805  200.144.121.118 192.188.11.45    IMAP      Request: 8udg IDLE
15  0.770388  192.188.11.45   200.144.121.118  IMAP      Response: + entering idle mode
16  0.771295  200.144.121.118 192.188.11.45    IMAP      Request: DONE
17  0.918462  192.188.11.45   200.144.121.118  IMAP      Response: 8udg OK IDLE completed
18  0.919316  200.144.121.118 192.188.11.45    IMAP      Request: fylu STATUS "INBOX" (MESSAGES UNSEEN)
19  1.085944  192.188.11.45   200.144.121.118  IMAP      Response: * STATUS "INBOX" (MESSAGES 567 UNSEEN 0)
20  1.087351  200.144.121.118 192.188.11.45    IMAP      Request: nki2 IDLE
21  1.220460  192.188.11.45   200.144.121.118  IMAP      Response: + entering idle mode
22  1.221308  200.144.121.118 192.188.11.45    IMAP      Request: DONE
23  1.368564  192.188.11.45   200.144.121.118  IMAP      Response: nki2 OK IDLE completed
24  1.369383  200.144.121.118 192.188.11.45    IMAP      Request: 55I1 STATUS "INBOX.drafts" (MESSAGES UNSEEN)

▪ Frame 12 (90 bytes on wire , 90 bytes captured)
▪ Ethernet II, src: 00:02:55:5d:0a:a0, Dst: 00:04:ac:66:21:a6
▪ Internet Protocol, Src Addr: 200.144.121.118.(200.144.121.118), Dst Addr: 192.188.11.45 (192.188.11.45)
▪ Transmission Control Protocol, Src Port: 2725 (2725), Dst Port: imap (143), seq:18, Ack: 404, Len:36
▪ Internet Message Access Protocol

0010 00 4c 39 13 40 00 80 06 b3 a8 c8 90 79 76 c0 bc    .L9.@... ....yv..
0030 fe 6c 6a 79 00 00 38 30 6a 31 20 4c 4f 47 49 4e    .ljy..80 j1 LOGIN
0040 20 22 69 76 6f 63 61 72 76 22 20 22 66 69 73 68     "ivocar v" "[redacted]
0050 40 72 6e 70 34 35 21 22 0d 0a                      [redacted]  ..
```

Figura 5.1
Ferramenta sniffer capturando uma sessão IMAP.

Podemos comparar um sniffer a um grampo telefônico; a diferença é que, no caso do sniffer, existe a possibilidade de "escutar" diversas conversas ao mesmo tempo. É claro que as informações capturadas podem ser usadas para o "bem" ou não. Utilizando placas de rede Ethernet em modo promíscuo, é possível capturar tráfego com destino a outras máquinas da rede.

Switch: impede a escuta da rede:

- Sofre ataque CAM table flooding (MAC spoofing).
- Envio de requisições ARP falsas com endereços MACs randômicos.
- Estouro da tabela de MACs.

Prevenção:

- Configurar manualmente uma tabela CAM.
- Filtrar MAC na porta.
- Usar criptografia.

Detectar um sniffer em uma rede é tarefa árdua e trabalhosa. Um sniffer não necessita ser um equipamento (ou máquina) independente: pode ser um microcomputador (servidor, desktop ou notebook), configurado para esse fim. Em sistemas baseados em Unix, somente o administrador (root) consegue colocar a placa de rede em "modo-promíscuo". Colocar uma placa de rede em modo-promíscuo altera seu funcionamento, fazendo com que a placa de rede tenha acesso a todo o tráfego de rede que está passando pelo segmento, e não somente ao tráfego direcionado a esse equipamento.

Em equipamentos do tipo Linux, o comando ifconfig pode auxiliar na detecção de placas de rede em modo-promíscuo.

```
root@laptop:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:f1:5d:77
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef1:5d77/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:434 errors:0 dropped:0 overruns:0 frame:0
          TX packets:454 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:252773 (252.7 KB)  TX bytes:36161 (36.1 KB)
          Interrupt:10 Base address:0xd020
```

No exemplo anterior, podemos ver a mensagem "PROMISC", indicando que a placa de rede está em modo-promíscuo. O uso de switches em redes não resolve 100% o problema, pois existem varias técnicas que se empregadas e/ou combinadas podem fazer com o que o tráfego seja direcionado para outros equipamentos e capturado.

Source routing (roteando pela fonte)

- Opção especial do pacote IP, facilita o spoofing.
- O invasor faz o datagrama passar por uma rota específica.



- Prevenção:
  - Desabilitar o roteamento de pacotes source-routed.
  - No roteador Cisco, executar o comando:

```
no ip source-route
```

  - No roteador Linux:

```
/etc/sysctl.conf→ysctl.conffLinux: executar o ce_route=0
```

Hoje, no ambiente da internet, não existem motivos legítimos que provocariam a necessidade de ditar o caminho que o pacote deverá percorrer até chegar ao seu destino.

Desde que o roteamento seja feito apenas de ou para uma respectiva rede privada, deve-se atentar para o cuidado de não aceitar pacotes no roteador de borda que instruam esse roteador a encaminhar pacotes para outra rede.

Mais informações sobre source routing podem ser obtidas na RFC 791.

DoS (Denial of Service)



Denial of Service (DoS – negação de serviço) é uma tentativa explícita de impedir o uso de serviço por usuário legítimo.

Exemplos:

- Inundação da rede, impedindo seu tráfego legítimo.
- Quebra de conexão entre duas máquinas, impedindo acesso ao serviço.
- Indisponibilidade de serviço para uma rede ou usuário.

Tipos de ataque:

- Consumo de recursos escassos, não renováveis.
  - Banda, CPU, memória, espaço em disco: SYNflood, smurf, e-mail, bombing e spamming.
- Destruição ou alteração de configuração.
  - Alteração de configuração em Sistemas Operacionais e roteadores.
- Destruição ou alteração física de componentes de redes.
  - Acesso não autorizado à sala dos servidores e destruição intencional de máquina.

De acordo com a definição do Computer Emergency Response Team (CERT), os ataques DoS, também denominados Ataques de Negação de Serviço, consistem em tentativas de impedir usuários legítimos de utilizarem um determinado serviço de um computador. Para isso, são usadas técnicas que podem:

1. Sobrecarregar uma rede a tal ponto que os seus verdadeiros usuários não consigam usá-la.
2. Derrubar uma conexão entre dois ou mais computadores.
3. Fazer tantas requisições a um site até que ele não consiga mais ser acessado.
4. Negar acesso a um sistema ou a determinados usuários.



Prevenção:

- Implementar filtros em roteadores e firewalls.
- Implementar proteção contra SYNflood.
- Habilitar “quota” para as contas.

- Monitorar: espaço em disco, consumo de CPU, memória e tráfego de rede.
- Examinar periodicamente itens de segurança física com respeito às necessidades atuais.
- Usar IDS (tripwire) para checar alterações em arquivos de configuração.
- Manter máquinas “hot spare”.
- Manter configurações de rede redundantes e tolerantes a falhas.
- Manter agendamento de backup regularmente.
- Manter política rígida de senhas.
- Desabilitar qualquer serviço de rede desnecessário ou que não seja usado.
- Servidor Linux: # netstat –atunp (quais serviços estão ativos e por quê?).

É difícil falar em prevenção desse tipo de ataque, pois a maioria das ocorrências vistas atualmente exploram o consumo de recursos, como link de internet ou CPU do servidor.

Exercício de fixação 1
Negação de serviço

O que é Denial of Service (DoS) e como pode se prevenido?

Spoofing

- E-mail spoofing.
- IP spoofing:
  - Blind-spoofing.
  - Non-blindspoofing.
  - ARP spoofing.
  - DNS spoofing.
  - Roteamento.
- Spoofing significa “enganando”.
  - Ato de falsificar identidade na rede para enganar um usuário.
- Existem diversas formas de enganar:
  - IP: burlando mecanismos de autenticação
  - DNS: domínio apontando para endereço falso
  - Web: página falsa de serviços legítimos
  - E-mail: mensagem falsa
  - Roteamento etc.

É qualquer procedimento que envolva personificação de usuários ou máquinas, incluindo endereços IP e consultas em servidores de nomes. São usados para obter acesso não autorizado ou para esconder tentativas de ataque.

E-mail spoofing

- Invasor forja remetente da mensagem.
- Servidor SMTP envia mensagem, não verificando identidade do remetente.
- Spam: forma usual de "e-mail spoofing" usada por spammers.
- Exemplo de ataque de engenharia social:
  - Solicitação ao usuário legítimo de acesso a site suspeito.
  - Solicitação ao usuário legítimo de envio de senha para um endereço determinado.
- Prevenção:
  - Evitar servidor open relay.
  - Verificar MX do domínio do servidor do remetente.
  - Usar autenticação segura para SMTP e POP3.
  - Usar servidor antispam. Solução Linux popular: SpamAssassin.
  - Usar RealTime Blackhole List (RBL): cadastro de spammers.
  - Reforçar configuração do servidor de correio.
  - Conscientização dos usuários.

Spam

Nome originado de uma marca americana de presunto enlatado. Num filme da série Monty Phyton, um grupo de vikings repete esse nome diversas vezes em um bar. Consiste em correio eletrônico não solicitado, associado a correntes e malas diretas de propaganda. De acordo com estimativas atuais, mais de 50% do correio eletrônico que trafega no mundo é spam.

O CERT disponibiliza uma série de recomendações sobre e-mail spoofing no endereço http://www.cert.org/tech_tips/email_spoofing.html

IP spoofing

Falsificação do endereço de origem do pacote IP.

- Atacante na estação A envia para C um pacote com origem igual a B.
- Resposta de C irá para a estação B.

Técnicas associadas para ataque no protocolo TCP:

- Blind spoofing (ataque cego):
  - Conexão usa tree-way handshake e Initial Sequence Number (ISN) randômico.
  - Atacante tenta predizer número sequencial e executar código.
- Non-blind spoofing:
  - Atacante está no meio da conexão, capturando tráfego com sniffer.
  - Atacante conhece o número da sequência gerado.
  - Uso de DoS para sequestro de conexão: Man-in-the-middle.

O protocolo TCP possui alguns métodos de controle, tentando evitar que esse tipo de ataque aconteça. Alguns sites com informações sobre IP spoofing:

- http://www.symantec.com/connect/articles/ip-spoofing-introduction
- http://www.cert.org/advisories/CA-1996-21.html

- **ARP spoofing**: envenenamento da tabela ARP (ARP poisoning).
- **DNS spoofing**: "servidor" falso responde a consultas redirecionando o acesso.

Saiba Mais

Leia o artigo "Compreendendo Ataques Denial of Services", de Leandro Márcio Bertholdo, Andrey Vedana Andreoli e Liane Tarouco. http://www.cert-rs.tche.br/docs_html/ddos--errc-2003.pdf

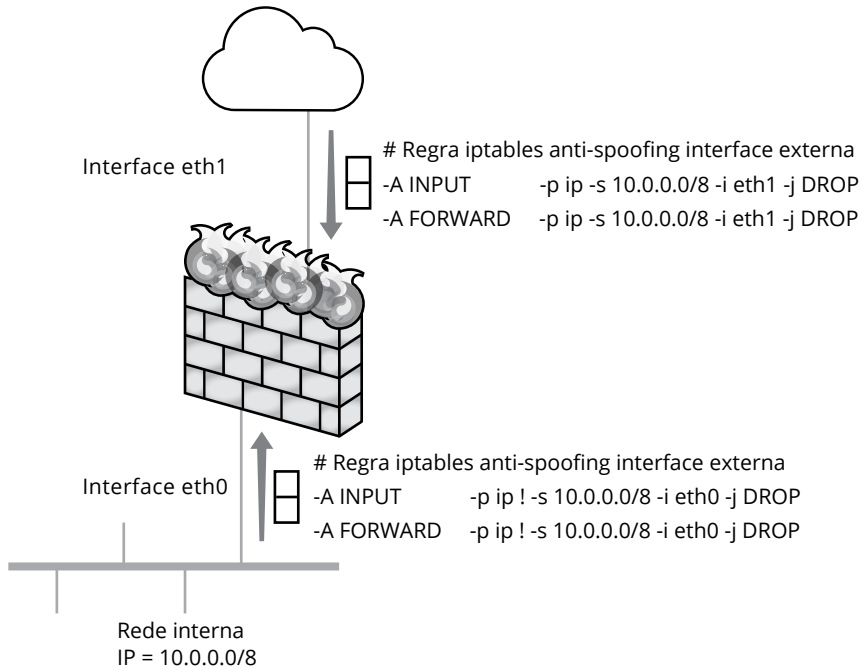


Figura 5.2 Regras antispoofings.

Medidas tomadas pelos administradores:

- **Usar filtros ingress e egress**: nenhum pacote deve sair da sua rede com um endereço IP de origem que não pertença a essa rede; tampouco devem entrar pacotes com endereços de origem de dentro da sua rede. Esse tipo de filtragem é comum, e muitas ferramentas de firewall já a implementam automaticamente.
- **Números de sequência randômicos**: se a regra de formação dos números de sequência for suficientemente randômica, o atacante não conseguirá sequestrar ou falsificar uma conexão.
- **Criptografia e autenticação**: confiar somente no endereço IP é uma política que favorece o spoofing. Sistemas seguros devem criptografar a informação sensível e exigir meios de obter uma autenticação forte entre as partes.

Prevenção

- Portsecurity: especificações de segurança de switch Ethernet.
- ARP watch: monitora mudanças na tabela ARP.
- ISN "mais" randômico (kernel).
- Criptografia e autenticação forte.
- Filtros ingress-egress no firewall.
- Kernel Linux:

```
for f in /proc/sys/net/ipv4/conf/*/rp_filter; do echo 1 > $f done
```

Roteamento:

- Ataque combinando IP spoofing e roteamento dirigido.
- Redireciona a resposta para a máquina do atacante.

Protocolo de roteamento dinâmico.

- Ausência de mecanismos de autenticação.
- Proporciona anúncio indevido de rota falsa.
- Exemplo: RIP.

Prevenção.

- Uso de roteamento estático ou manual.
- Uso de protocolos mais modernos com autenticação: RIPv2 e OSPF.

SYN flood

Ataques de Flood ou Flooding consistem em "inundar" um sistema ou canal de comunicação, numa tentativa de utilizar ao máximo os recursos e causar um DoS.

Popular ataque de negação de serviço (DoS), afeta critério de disponibilidade.

Entendendo o ataque:

- Envio de pacotes SYN com endereços de origem randômicos (IP spoofing).
- Excesso de conexões no servidor sem confirmação.
- Estouro de buffer: novas conexões não são aceitas até o esvaziamento do buffer (DoS); ataque contínuo.

Prevenção.

- Não existe solução 100% segura.
- Configurações específicas para cada Sistema Operacional.

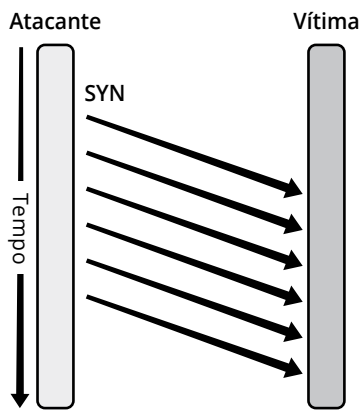


Figura 5.3
Ataque SYN flood.

Algumas sugestões de configuração visando mitigar esse tipo de ataque em sistemas Linux.

```
/etc/sysctl.conf → net.ipv4.tcp_syncookies=1

Firewall iptables:

# chama chain flood

$iptables -A INPUT -p tcp -syn -j flood

# cria chain flood

$iptables -n flood

$iptables -A flood -m limit -limit 12/second --limit-burst 24 -j return

$iptables -A flood -j log_flood
```

Mais informações sobre SYN flood podem ser encontradas em: http://www.cert.org/advisories/CA-1996-21.html e http://cr.yp.to/syncookies.html

Apesar de muitos fabricantes terem tomado medidas para diminuir os efeitos desse ataque, ainda não existe uma forma 100% eficiente para impedi-lo.

Smurf

Ataque do tipo DoS, que usa o recurso directed broadcast da pilha TCP/IP.
Entendendo o ataque:

- Atacante descobre uma lista de endereços que podem ser utilizadas como redes amplificadoras.
- Atacante "pinga" broadcast das redes (echo request) com IP da vítima (IP spoofing).
- Redes respondem com echo reply, inundando a vítima com pacotes ICMP.

Prevenção:

- Filtrar broadcast.
- Roteador Cisco: no IP "directed-broadcast".
  - Kernel Linux: "/etc/sysctl.conf → net.ipv4.icmp_echo_ignore_broadcasts=1"

Mais informações podem ser obtidas no endereço: http://www.cert.org/advisories/CA-1998-01.html

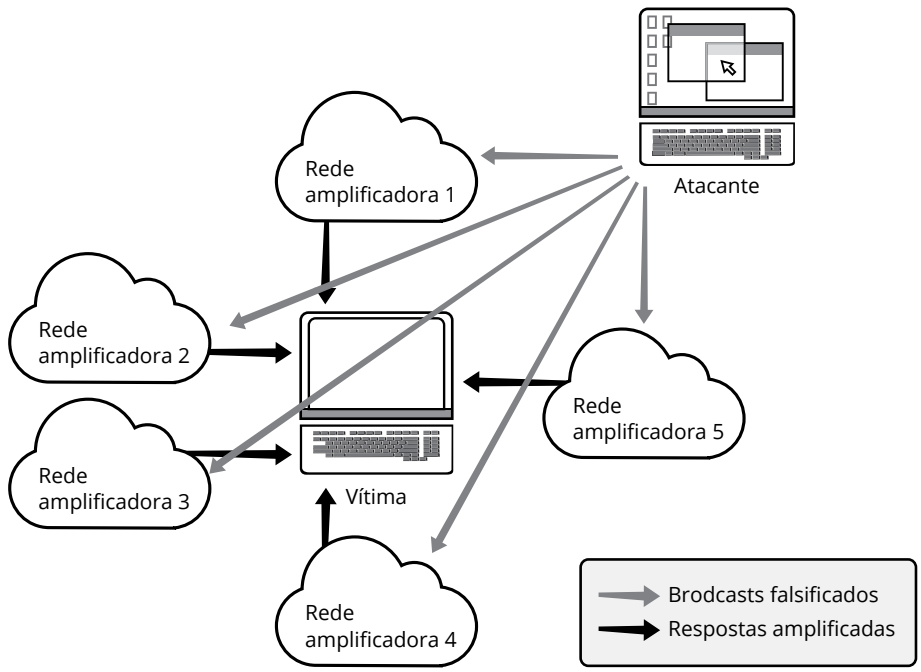


Figura 5.4
Ataque smurf.

Infelizmente, não existe forma eficiente de a vítima se proteger, mas as redes amplificadoras podem bloquear pacotes directed broadcast. Toda difusão externa à rede deve ser bloqueada no primeiro roteador disponível.

Modelo de ataque fraggle

Todas as máquinas que receberam o datagrama UDP com IP de origem forjado respondem para a máquina vítima com ICMP Type3.

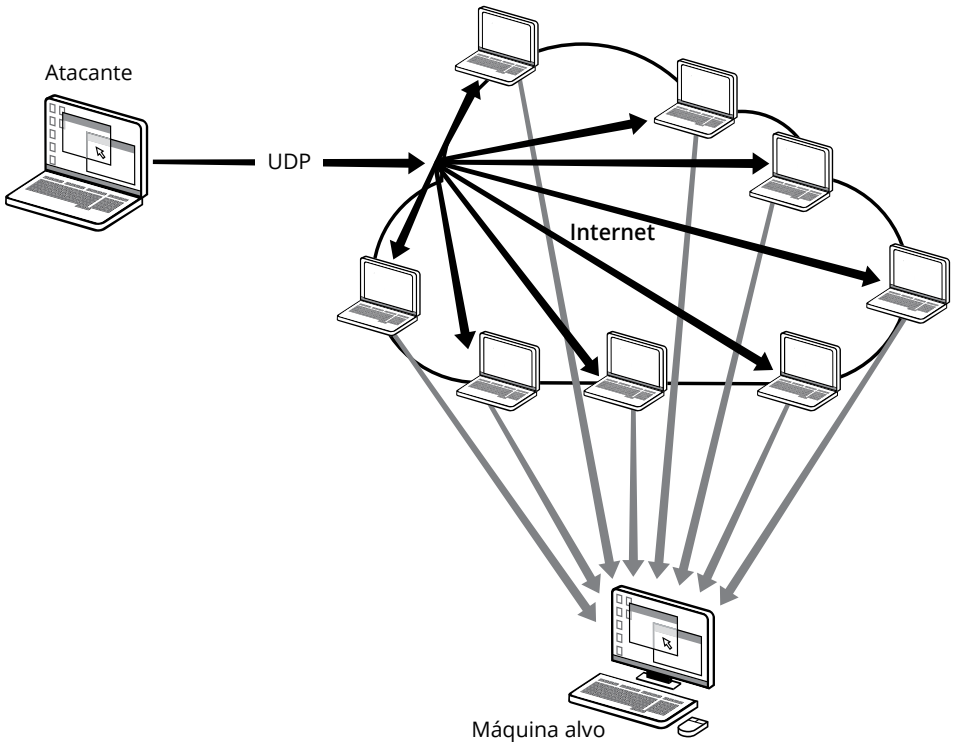


Figura 5.5
Modelo de ataque fraggle.

Ataques com fraggle e smurf são mais difíceis de ocorrer, devido ao fato de muitas redes terem métodos para não permitir tráfego muito alto desses tipos de pacote.

Modelo de ataque DRDOS

Todas as máquinas que receberam o TCP/SYN com o IP de origem forjado respondem para a máquina vítima com TCP/SYN-ACK e, por sua vez, a máquina vítima responde a todos os pacotes com TCP/RST.

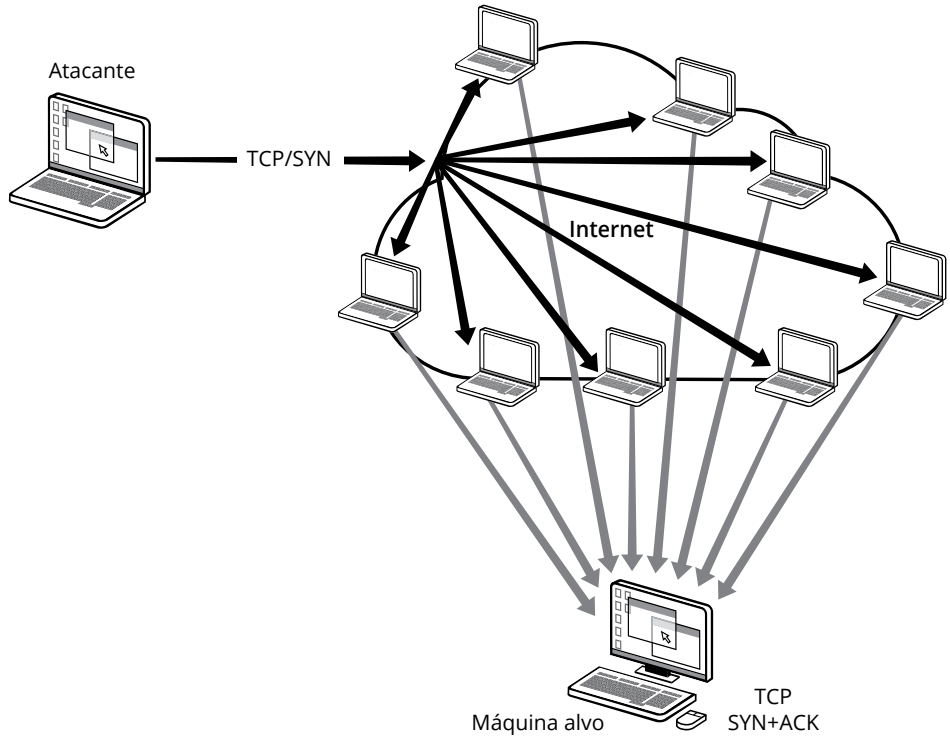


Figura 5.6
Modelo de ataque DRDOS.

Portscan (varredura de portas)

Atividade maliciosa de reconhecimento que descobre serviços ativos na máquina.

- Primeira medida para descobrir vulnerabilidades em serviços.
- Passo inicial de muitos ataques.
- Verificação das respostas com endereço de retorno necessário permitindo rastrear origem.
- Detectável via logs: servidor, firewall e IDS.

Prevenção.

- Realizá-lo periodicamente na sua rede.
- Analisar periodicamente os logs e reportar portscan.
- Teste sua rede: http://www.pcflank.com/scanner1.htm

Em máquinas com o protocolo TCP/IP instalado, serviços estão associados a portas, que variam de 0 a 65535. Cada serviço tem ou pode ter uma porta associada. Assim um servidor Web funciona na porta 80 e um servidor Web seguro (HTTPS) funciona na porta 443.

O Portscan é o processo de verificação da existência de algum serviço em uma porta. Para fazer isso, o atacante tenta basicamente se conectar (efetuar um "three-way-handshake" do protocolo TCP/IP) em cada porta. Dependendo do tipo de resposta, sabemos se a porta está aberta (funcionando e atendendo a requisições) ou não.

Entre as muitas ferramentas existentes para esse fim, o Nmap (http://nmap.org) é uma das mais completas ferramentas, funcionando em diversos Sistemas Operacionais diferentes. O Nmap possui funções permitindo a identificação do Sistema Operacional alvo, assim como modelo e versão dos serviços testados. Conta com diversas técnicas, explorando ao máximo os protocolos vinculados ao IP. Atualmente possui inclusive a capacidade de scripts, podendo efetuar tarefas automatizadas. Mesmo existindo uma interface gráfica chamada ZenMap, o Nmap utilizado em linha de comando continua sendo o mais utilizado.

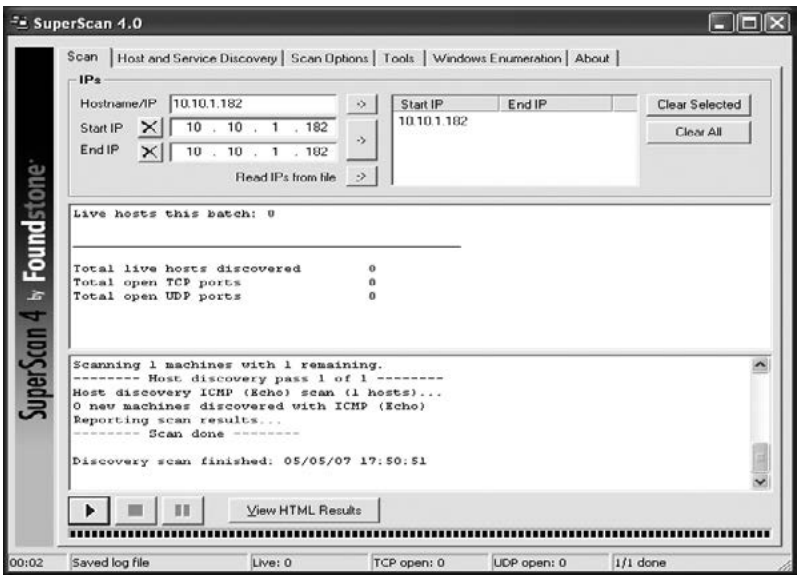


Figura 5.7
Programa de portscan.

Distributed Denial of Service (DDoS)

- O mal possui poder de organização – ataque distribuído de negação de serviço.
- Ataque coordenado com múltiplas origens atacando, difícil de executar.
- Características:
  - IP spoofing, difícil de rastrear.
  - Largura de banda intensiva.
  - Combina: SYN flood, UDP flood, ICMP flood, smurf e fraggle.
  - Ferramentas: Trin00, TFN e TFN2k.

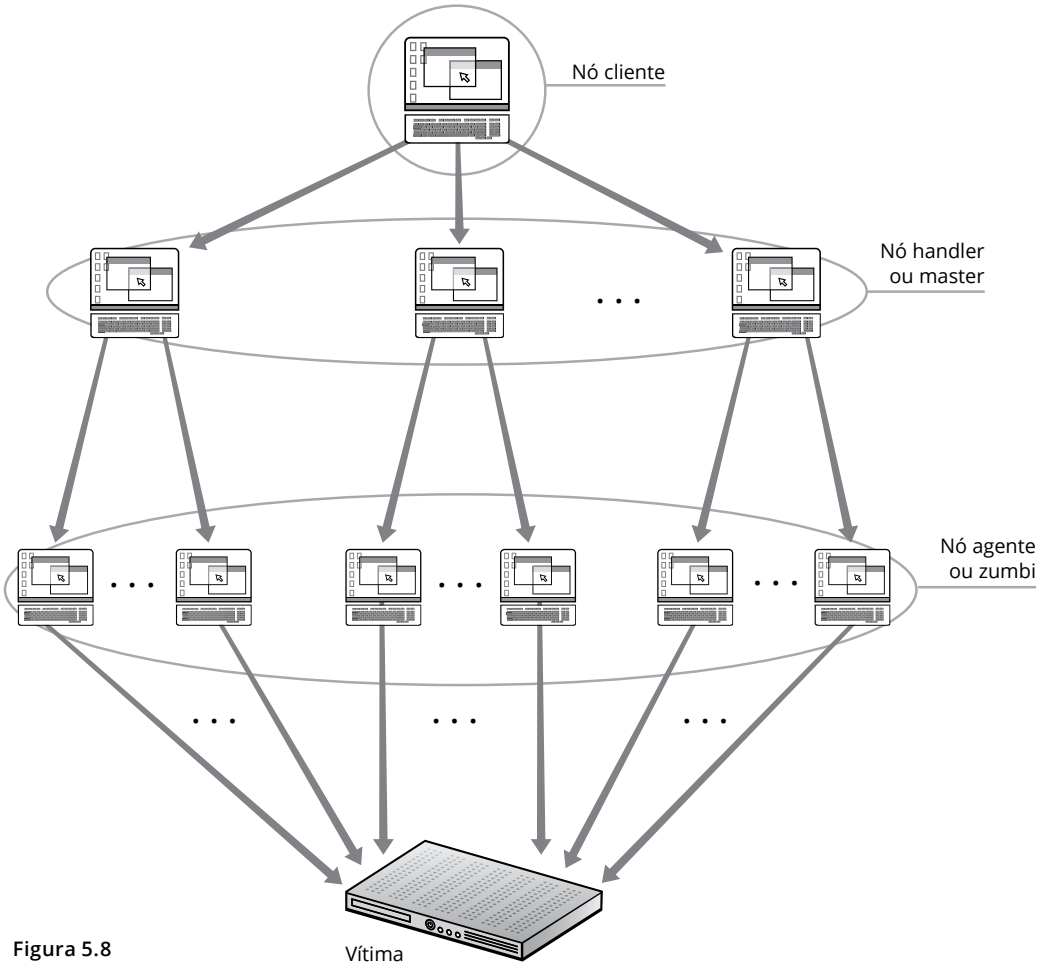


Figura 5.8
Ataque DDoS.

Entendendo o ataque:

- Atacante invade máquinas explorando vulnerabilidades, vírus e worms.
- Programa DDoS é instalado nas máquinas (escravas ou zumbis).
- Controle central direciona todos os "escravos" para ataque DoS concentrado.

Sites famosos, como Yahoo! e eBay, já sofreram ataques desse tipo. Mais informações sobre DDoS podem ser encontradas em:

- http://www.sans.org/dosstep/roadmap.php
- http://www.cert.org/incident_notes/IN-2000-01.html

Recentemente, tem crescido uma atividade relacionada ao DDoS: as "botnets". São redes de máquinas infectadas com algum programa malicioso que faz com que um atacante remoto seja capaz de ter controle total sobre essas máquinas. Elas se conectam automaticamente a uma rede de "Redes de conversação on-line" (Internet Relay Chat – IRC) por um servidor IRC comprometido. Esse servidor normalmente é chamado de Command and Control Server (C&C). Conectando-se nesse servidor, o atacante pode enviar um comando para todas as máquinas que estão naquele canal do servidor, comandando um ataque DDoS contra uma vítima.

Mais informações sobre botnets e IRC: http://www.irc.org/ e http://www.securityfocus.com/news/9543

DDoS (DoS distribuído)

Prevenção:

- Link de internet com adicional de largura de banda, disponibilizado ou em modo hot standby, para operação normal, ou a pedido para o provedor.
- Tráfego separado: um provedor para acesso da internet aos servidores públicos e outro provedor para acesso da rede interna à internet.
- Conversar com o seu provedor sobre:
  - Defesas DoS implementadas e disponíveis.
  - Informações sobre contatos de emergência (qual é o CSIRT do provedor?).
  - Qual é o backbone (provedor) do seu provedor?

Prevenção:

- Implementar filtros de tráfegos maliciosos.
- Implementar endereços privados para entrada e saída no firewall (interface externa).
  - Tráfego com endereço de origem ou de destino, como broadcast, provavelmente é malicioso (quarto octeto igual a 0 ou 255).
- Endereços de loopback não podem trafegar na rede.
- Filtrar tráfego utilizando regras antispoofing.
- Implementar política rigorosa de antimalware.

Exercício de fixação 2
DDoS

O que é DDoS (DoS distribuído) e como pode ser prevenido?

Modelo de ataque DDoS em duas camadas

Exemplo simples, onde o cracker ativa todos os zumbis diretamente; esse primeiro modelo foi implementado na ferramenta TFN.

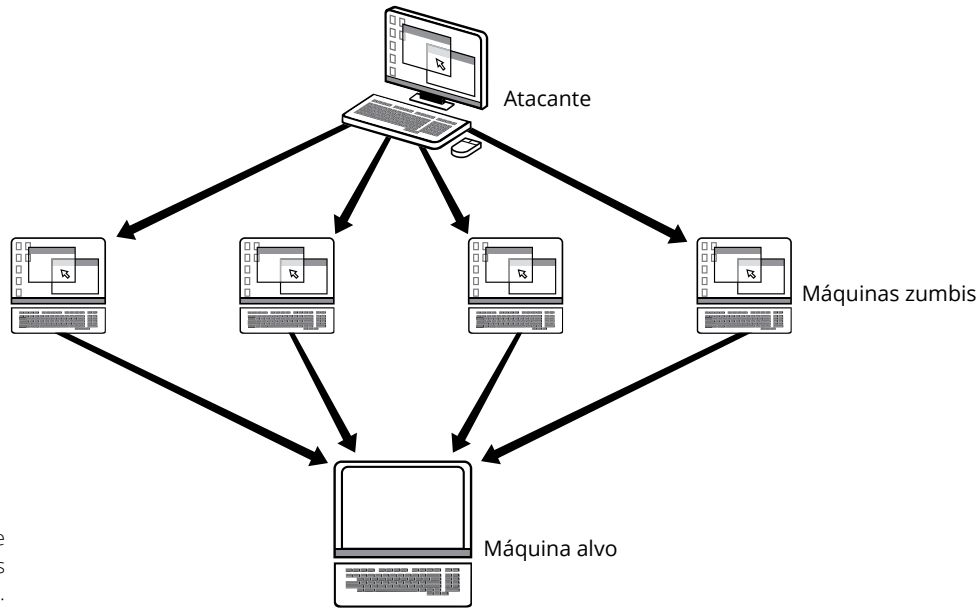


Figura 5.9
Modelo de ataque DDoS em duas camadas.

Modelo de ataque DDoS em três camadas

- Exemplo mais arrojado, onde o cracker ativa todos os zumbis através de uma ou mais máquinas de controle denominadas Master.
- Esse modelo foi implementado na ferramenta TFN2K.

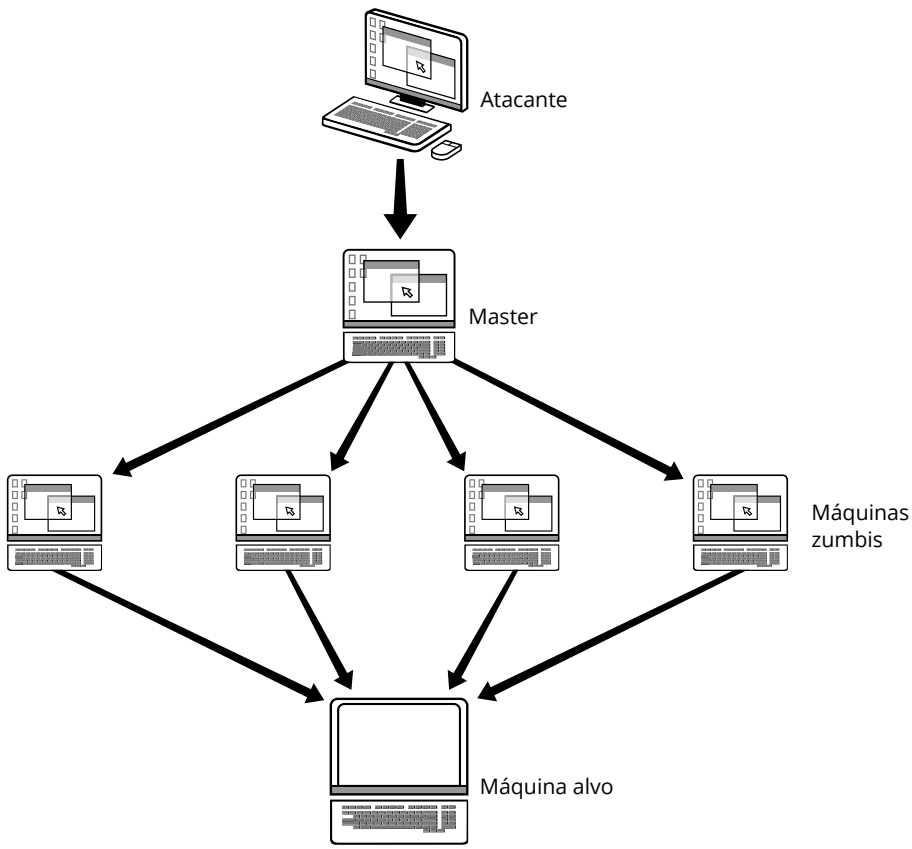
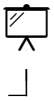


Figura 5.10
Modelo de ataque DDoS em três camadas.

Modelo de ataque DDoS/Worm



A evolução de DDoS é como o worm Mydoom; o conceito de verme agregado ao DDoS mostra seu poder.

Observamos que uma ação comum nos desenvolvedores de worm é usá-los para criar possibilidades de ataques DDoS, tornando os computadores infectados zumbis; outra possibilidade é tornar os computadores infectados parte de uma grande botnet.

Vulnerabilidades em implementações específicas



- Ping of death (ping da morte).
- Teardrop.
- Land.

Ping da morte



- Tipo de ataque DoS.
- Consiste no envio de ICMP ping com pacote de dados maior que 64 Kbytes, causando travamento ou reinicialização da máquina Microsoft Windows atacada.
- Vulnerabilidade muito antiga.
- Prevenção:
  - Upgrade das versões dos Sistemas Operacionais.
  - Firewall iptables Linux:

```
$iptables -A FORWARD -p icmp --icmp-type echo-request -m limit
   --limit 1/s -j ACCEPT
```

Teardrop



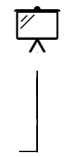
- Ataque do tipo DoS.
- Campo “fragmentation offset” do TCP com valores nulos ou negativos.
- Afeta Microsoft Windows 3.1, Windows 95, Windows NT, versões do kernel Linux até 2.0.32 e 2.1.63.
- Causa travamento da máquina atacada.
- Prevenção:
  - Upgrade das versões dos sistemas operacionais.
  - Firewall iptables Linux:
  - $iptables -A INPUT -f -j DROP
  - $iptables -A FORWARD -f -j DROP

Land



- Ataque do tipo DoS.
- Envio de pacotes SYN com IP e porta de origem iguais ao IP e porta de destino.
- Usa técnica de “IP spoofing”.
- Afeta vários sistemas operacionais.

- Causa travamento da máquina atacada.
- Prevenção:
  - Fazer upgrade das versões dos sistemas operacionais.



Roteiro de Atividades 5

Atividade 5.1 – Conceito de varreduras

Primeiros passos para um ataque e para uma auditoria:

1. Acesse http://www.whatsmyip.org/port-scanner/server/
2. Faça um scan de portas na sua máquina. Quais portas estão no ar?

Utilizando Nmap

Nmap é um programa de análise de recursos de rede e auditoria de segurança capaz de realizar varreduras em redes de computadores a procura de recursos disponíveis.

- Acesse a máquina virtual;
- Instale o programa Nmap através do comando *apt-get install nmap*;
- Escaneie a sua máquina com Nmap:

```
# nmap <ip>
```

- Agora faça um scan das máquinas do laboratório:

```
# nmap <rede>
```

- Verifique vários níveis de scan e extraia o maior número possível de informações: http://insecure.org/nmap/man/pt-br/

Atividade 5.2 – Simulando ataques com Hping

Antes de iniciar os ataques é importante conhecer a ferramenta Hping, um programa em linha de comando de construção e análise de pacotes com orientação para TCP/IP. Suporta TCP, UDP, ICMP e RAW-IP. Com ele podemos construir pacotes específicos para envio por uma rede.

Principais opções:

-V	Modo Verbose
-c	Contador de pacotes
-d	Tamanho do dado
-p	Porta de destino
-s	Porta de origem
--rand-source	Randomização da origem
--fast	10 pacotes por segundo
--faster	100 pacotes por segundo
--flood	Máximo de pacotes possíveis por segundo

Atividade 5.3 – Simulando um ataque DoS Land

Essa atividade deve ser feita em dupla:

- Ataque do tipo Land é um tipo de DoS que envia uma inundação de pacotes com a flag SYN ativada com IP e porta de origem iguais ao IP e porta de destino
- Na máquina alvo, instale o serviço http apache

```
# apt-get install apache2
```

- Abra o Wireshark e tente "Sniffar" as conexões no segmento do servidor;
- Na máquina atacante, Instale o pacote "hping3", iniciando ataque ao servidor "http" Linux Apache na porta 80; com o comando

```
# hping3 -V -c 1000000 -S -w 64 -p 80 -s 80 --flood --rand-source
<ip_servidor>
```

- Verifique o comportamento dos pacotes com o Wireshark.

Principais modos Hping:

Modo	Descrição
Nenhum	Modo default TCP
-0	Modo RAW-IP
-1	Modo ICMP
-2	Modo UDP
-8	Modo Scan

Simulando um ataque SMURF

Um ataque SMURF é um tipo de DoS que usa Direct Broadcast.

- Na máquina alvo, abra o Wireshark e escute a conexão no segmento do servidor;
- Na máquina atacante, digite o comando seguinte e verifique o comportamento dos pacotes no Wireshark:

```
# hping3 -1 --flood -a <ip_broadcast>
```

6

Criptografia I – Fundamentos

objetivos

Apresentar os fundamentos básicos de criptografia e seus princípios básicos, como funções hash; diferenciar a criptografia simétrica e assimétrica, e as aplicações de cada uma, e mostrar os principais algoritmos de criptografia.

conceitos

Uso de criptografia em e-mails e arquivos, tipos de criptografia, certificação digital e Public Key Infrastructure (PKI).

Introdução



- *kriptós* = oculto; *grápho* = grafia; *análysis* = decomposição; *logo* = estudo.
- Criptografia: ciência de escrever mensagens cifradas, ocultamente.
- Criptoanálise: ciência de quebrar códigos e decifrar mensagens; ataque é uma tentativa de criptoanálise.
- Criptologia: ciência que reúne criptografia e criptoanálise.

Criptografia é a base para muitas aplicações de segurança:

- Autenticação segura, comunicação segura.
- Dinheiro eletrônico, certificados digitais.
- Identidade digital, assinatura digital.

A criptografia garante três propriedades de segurança:

- Confidencialidade.
- Integridade.
- Autenticidade.

Primórdios: Criptografia de César – método simples usado no Império Romano:

- Troca cada letra do alfabeto por três letras depois.
- Fácil de ser quebrado.

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Cifrado	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
Normal	E	S	C	O	L	A		S	U	P	E	R	I	O	R		D	E		R	E	D	E	S				
Cifrado	H	V	F	R	O	D		V	X	S	H	U	L	R	U		G	H		U	H	G	H	V				

Figura 6.1
Criptografia de César.

Durante a Segunda Guerra Mundial, outros avanços foram feitos na área da criptografia, a partir da necessidade que os alemães tinham de enviar mensagens. Na época, os aliados desenvolveram máquinas para "quebrar" a criptografia dos alemães. Posteriormente, foi formalizada a criptoanálise, ciência de quebrar códigos e decifrar informação sem conhecer a chave.

Hoje, a criptografia é uma ciência bastante estudada, e seus métodos vão sendo melhorados à medida que a computação avança e processadores mais rápidos são criados.

Exercício de nivelamento 1
Fundamentos de criptografia

Como a sua organização utiliza criptografia?

Criptografia – algoritmos e chaves

Elementos básicos.

- Algoritmo: função matemática para cifrar e decifrar.
- Um bom algoritmo é conhecido publicamente, com segurança testada.
- Chave: valor secreto usado para realizar as operações.
- Possui tamanho em bits; quanto maior, mais segura (exemplo: chave de 128 bits).
- Ataque por força bruta: testa todas as combinações possíveis para a chave.
- Quanto maior a chave, mais dificuldade para um ataque por força bruta.

Tabela 6.1
Custo de plataforma x tempo médio estimados.

1995 – Custo Hardware	Comprimento útil da chave secreta					
	40 bits	**56 bits**	**64 bits**	**80 bits**	**112 bits**	**128 bits**
US$ 100 mil	2 seg	35 h	1 ano	$7x10^{14}$ anos	10^{14} anos	10^{19} anos
US$ 1 milhão	0.2 seg	3,5 h	37 dias	$7x10^{13}$ anos	10^{13} anos	10^{18} anos
US$ 10 milhões	0.02 seg	21 m	4 dias	700 anos	10^{12} anos	10^{17} anos
US$ 100 milhões	2mseg	2 min	9hs	70 anos	10^{11} anos	10^{16} anos
US$ 1 bilhão	0.2 mseg	13 seg	1 hs	7 anos	10^{10} anos	10^{15} anos
US$ 10 bilhões	0.02 mseg	1 seg	5.4 seg	245 dias	10^{9} anos	10^{14} anos
US$ 100 bilhões	2 m seg	0.1 seg	32 seg	24 dias	10^{8} anos	10^{13} anos
US$ 1 trilhão	0.2 m seg	0.01 seg	3 seg	2.4 dias	10^{7} anos	10^{12} anos
US$ 10 trilhões	0.02 m seg	1mseg	0.3 seg	6 hs	10^{6} anos	10^{11} anos

Robusto
Significa que não é conhecido nenhum método de ataque sobre criptograma.

Quebra por força bruta de chaves de algoritmos simétricos **robustos** (106 cifragens/seg por CPU)

Descobrindo senhas

Alguns algoritmos criptográficos são unidirecionais, significando que após cifrado o texto ou a mensagem, é impossível revertê-los ao estado original. Por exemplo: o texto "123456", passado pelo algoritmo MD5, retorna o texto "e10adc3949ba59abbe-56e057f20f883e". Mesmo tendo acesso ao texto cifrado e conhecendo o algoritmo, não conseguimos, a partir do texto "e10adc3949ba59abbe56e057f20f883e", chegar novamente ao texto original ("123456").

Como descobrir o texto original? Como conhecemos o algoritmo utilizado (MD5), podemos testar várias possibilidades de texto até encontrar alguma que seja igual ao texto cifrado.

Original	MD5	Valor procurado	Igual ?
123450	149787a6b7986f31b3dcc0e4e857cd2a	e10adc3949ba59abbe56e057f20f883e	Não
123451	078563f337ec6d6fedf131ddc857db19	e10adc3949ba59abbe56e057f20f883e	Não
123452	7692dcdc19e41e66c6ae2de54a696b25	e10adc3949ba59abbe56e057f20f883e	Não
123453	0f3e84acb19dff22f695f31dbe3e972a	e10adc3949ba59abbe56e057f20f883e	Não
123454	268e27056a3e52cf3755d193cbeb0594	e10adc3949ba59abbe56e057f20f883e	Não
123455	00c66aaf5f2c3f49946f15c1ad2ea0d3	e10adc3949ba59abbe56e057f20f883e	Não
123456	**e10adc3949ba59abbe56e057f20f883e**	**e10adc3949ba59abbe56e057f20f883e**	SIM

Tabela 6.2
Ataque de força bruta.

A técnica apresentada é conhecida como ataque de força bruta, onde todas as possibilidades de um conjunto (letras ou números ou combinados) são testadas e comparadas a um valor já conhecido.

Dificuldades para quebra de chave por força bruta

Para descobrir senhas por força bruta é necessário um número $n!n^1!n^2!...nx!$ de tentativas para esgotar as possibilidades, sendo n o número de caracteres e n1, n2...nx a quantidade de caracteres possíveis para a chave. Podemos afirmar também que quanto menos complexa a senha, mais rápido a força bruta irá alcançá-la. Outro fato é que em média (algumas vezes acima, outras vezes abaixo, mas na média) a força bruta alcança seu objetivo em 50% das iterações necessárias para esgotar o todo.

Sabendo que o tamanho da chave é medido pela quantidade de bits e que quanto mais bits, mais complexa é a senha, e que quanto mais rápido os computadores ficam, mais iterações são feitas por segundo para algoritmo de força bruta, qual é o tamanho perfeito de chave de criptografia?

Uma chave de 56 bits atinge 50% na força bruta em uma média de 1 minuto. Uma chave de 128 bits atinge 1% na força bruta em 146 milhões de anos, e 50% em 8 trilhões de anos.

Se cada átomo do universo (2 x 10E300) fosse um computador, e se cada um deles pudesse verificar 2 x 10E300 chaves por segundo, levaria cerca de 2 x 10E162 milênios para se chegar a 1% de uma chave de 512 bits (64 bytes). De acordo com a teoria do Big Bang, o tempo da criação do universo até hoje não passa de 2 x 10E24 milênios, ou seja, uma chave dessas não pode ser quebrada tão facilmente. É claro que pode ser vendida, roubada, extorquida...

Observação: os cálculos foram retirados do livro *Criptografia e Segurança – O Guia Oficial da RSA,* de Steve Burnett e Stephen Paine.

- A criptografia transforma premissas de confiança em mecanismos de proteção.
  - Controle de acesso.
    - Transforma premissa de posse de segredo em identificação do agente em processo digital.
  - Cifragem.
    - Transfere sigilo de uma chave para sigilo da informação em mensagem por ela cifrada.
  - Integridade.
    - Transforma premissa de sigilo em verificação de integridade de origem ou conteúdo.
  - Certificação.
    - Transforma premissas de sigilo e integridade em autenticação recursiva com verificação aberta.
- Divisão dos algoritmos de criptografia:
  - Algoritmos simétricos.
  - Algoritmos assimétricos.
  - Funções hash one-way.
- O que a criptografia não protege:
  - Criptografia não impede um atacante de apagar todos os seus dados.
  - Um atacante pode comprometer seu programa de criptografia, modificando o programa para usar uma chave diferente da que você gerou, ou talvez gravar todas as chaves de cifragem em um arquivo para análise posterior.
  - Um atacante pode encontrar uma forma fácil de decifrar as mensagens conforme o algoritmo que você esteja usando.
  - Um atacante pode acessar seus arquivos antes de você cifrá-lo ou após a decifrá-lo.
- Por tudo isso, a criptografia deve fazer parte da sua estratégia de segurança, mas não deve ser a substituta de outras técnicas de segurança.

Tipos de criptografia

- Criptografia simétrica:
  - Cifragem por blocos:
    - ECB
    - CBC
    - CFB
    - OFB
  - Principais algoritmos de cifragem por blocos:
    - DES
    - 3DES
    - RC-4
    - IDEA
    - AES

- Algoritmo para troca de chaves: Diffie-Hellman.
- Criptografia assimétrica:
  - Funções de hash.
  - Assinatura digital.

Criptografia é a ciência de ler e escrever mensagens cifradas. Muitas aplicações de segurança usam a criptografia como base. Para existir criptografia é necessário que exista um algoritmo, uma ou mais chaves e a informação a ser cifrada ou decifrada.

Existem, atualmente, dois tipos de criptografia:

- Criptografia assimétrica.
  - Duas chaves distintas.
    - Uma para cifrar.
    - Uma para decifrar.
- Criptografia simétrica.
  - Mesma chave é usada para cifrar e decifrar.

Muitas aplicações podem ser viabilizadas através de criptografia, como autenticação, assinaturas digitais, dinheiro digital etc.

Criptografia simétrica

- Usa mesma chave e algoritmo para cifrar e decifrar.
- A chave precisa ser pré-combinada entre os participantes.
- Out ofband: chave enviada por fora da rede, via disquete ou CD-ROM.

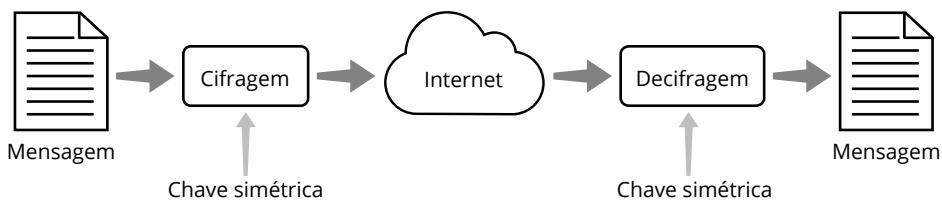


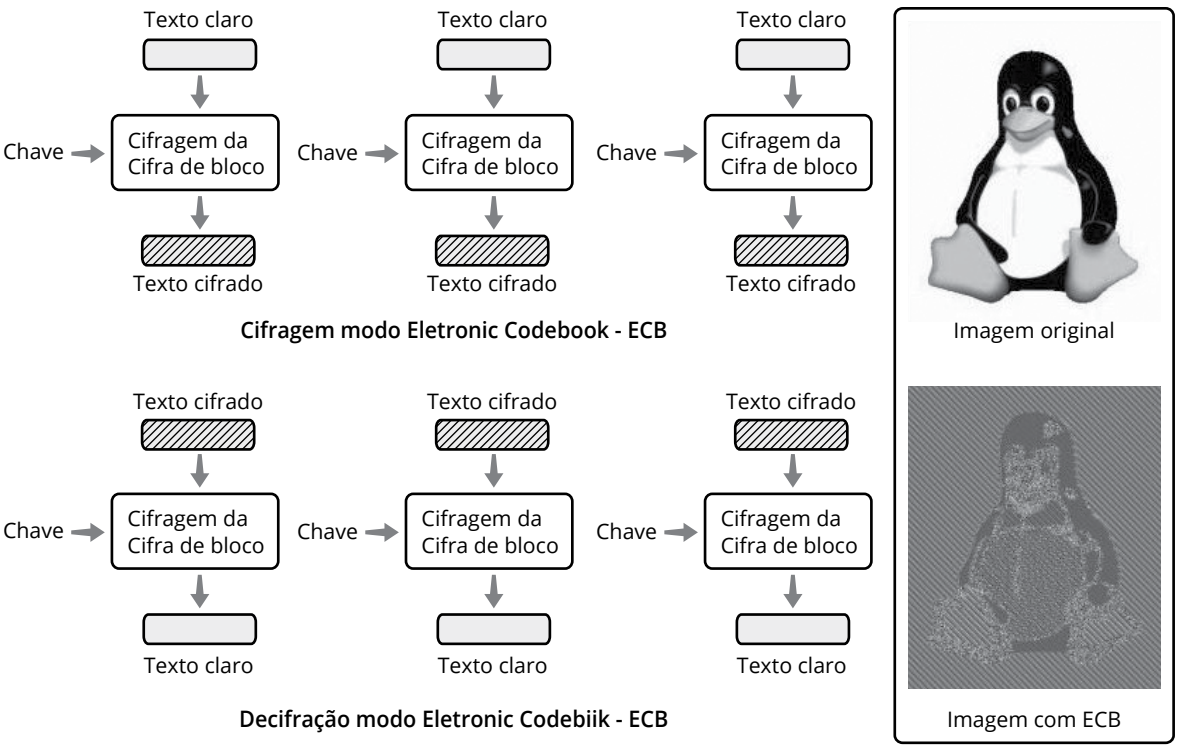
Figura 6.2 Criptografia simétrica.

- Transmissão de chave via rede:
  - Algoritmo Diffie-Hellman para troca de chaves.
  - Utilização de criptografia assimétrica.
- Vantagens:
  - Velocidade e algoritmos rápidos.
  - Facilidade de implementação em hardware.
  - Chaves pequenas e simples geram cifradores robustos.
- Desvantagens:
  - Distribuição das chaves dificulta gerenciamento.
  - Não permite autenticação e não repúdio do remetente.
- Métodos de crifragem:
  - Cifragem por fluxo (streamcipher).
  - Cifragem em blocos (block cipher), mais utilizada.

- Cifragem por blocos, modos de operação:
  - Eletronic Code Book (ECB).
  - Cipher Block Chaining (CBC).
  - Cipher Feed Back (CFB).
  - Output Feed Back (OFB).
- Principais algoritmos de cifragem por blocos:
  - DES (inseguro), 3DES, RC-4, IDEA e AES.

Eletronic Code Book

- Método mais simples, cifra bloco de modo independente usando a mesma chave.
- Não randômico; mensagem cifrada é obtida por concatenação dos blocos cifrados.



O Electronic Code Book (ECB) cifra cada bloco de 64 bits de forma independente, usando a mesma chave. O mecanismo ECB não é considerado muito seguro, pois um intruso pode perceber quando uma mensagem muda pela mudança no bloco. No ECB, uma mesma mensagem cifrada várias vezes vai gerar sempre o mesmo bloco.

Figura 6.3
Eletronic Code Book – ECB (Livro de Código Eletrônico).

Desvantagens:

- Blocos iguais de textos claros produzem blocos cifrados iguais;
- Não esconde padrão de dados;
- Nada acrescenta à confidencialidade proporcionada pela cifra.

Cipher Block Chaining

Cipher Block Chaining – CBC (Corrente de Blocos):

- Modo de operação mais usado.
- Operação XOR entre novo bloco de texto claro com bloco cifrado obtido na etapa anterior.
- Bloco cifrado depende de todos os blocos anteriores de texto claro (feedback).

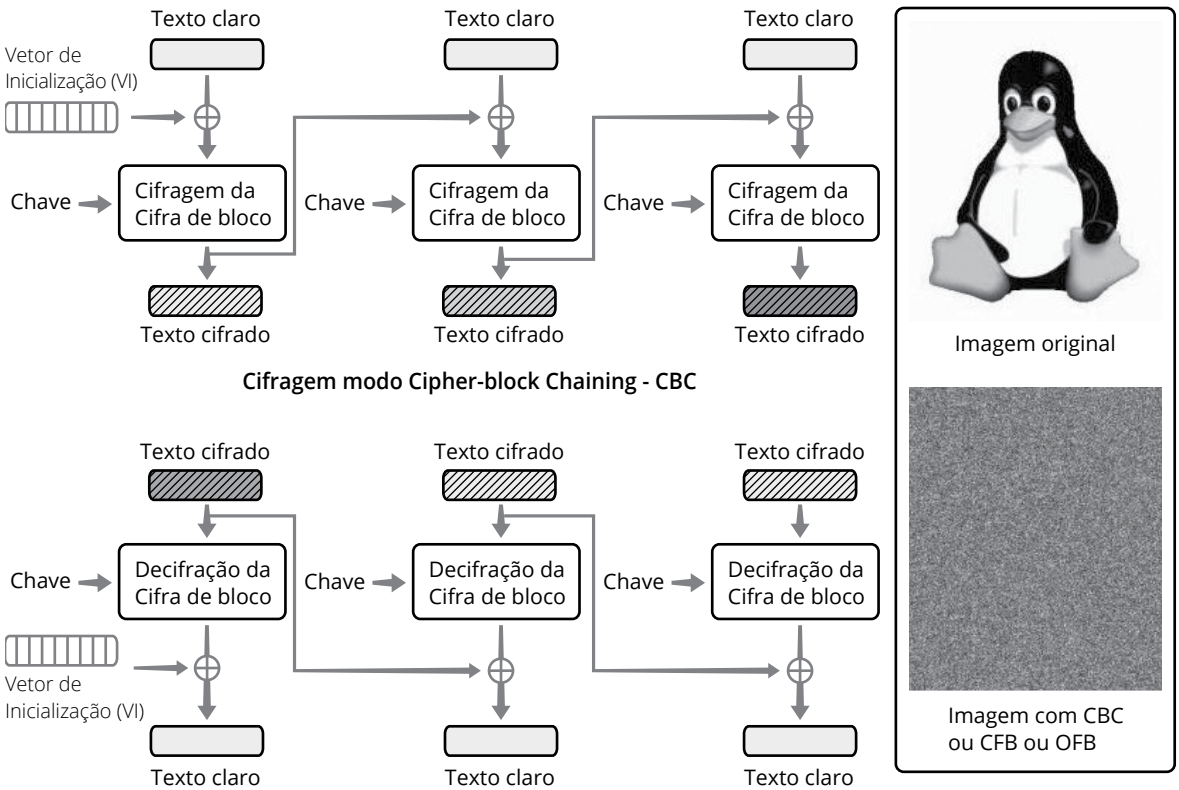


Figura 6.4 Cipher Block Chaining – CBC (Corrente de blocos).

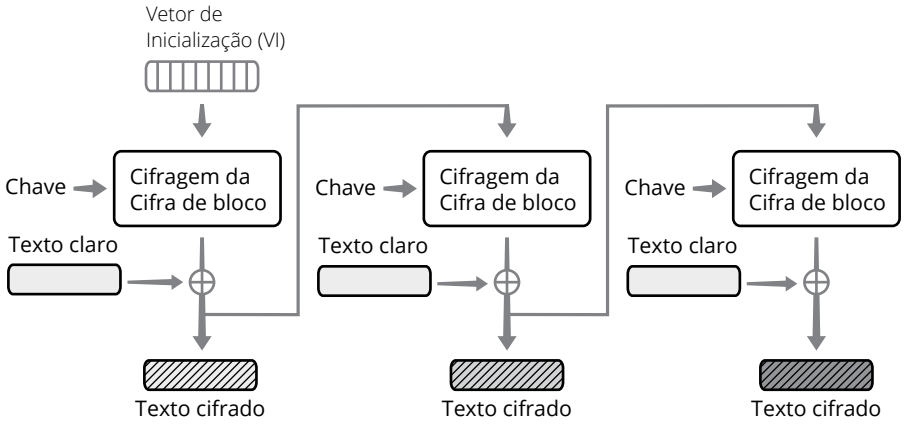
Nesse modo, cada bloco depende do resultado do bloco anterior. Através de um método chamado feedback, o bloco anterior é utilizado no processo de cifragem do bloco seguinte. Um sistema que usa CBC deve garantir que todos os blocos cheguem corretamente, pois um erro em um bloco se propagará para todos os outros.

Sua desvantagem é ser sequencial, que não pode ser usado em paralelo e tem maior tempo de processamento.

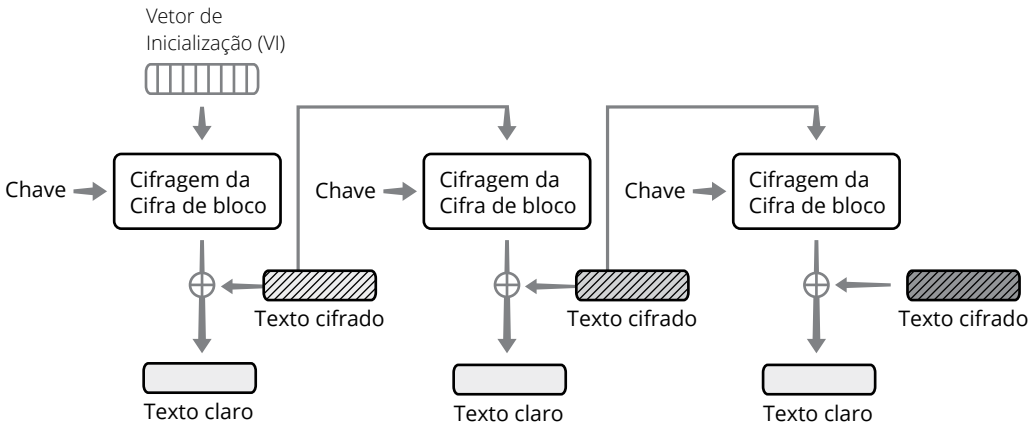
Cipher Feed Back

Cipher Feed Back – CFB (Cifra Realimentada):

- Cifra dados de qualquer tamanho, independentemente do bloco.
- Útil para cifrar informações que devem ser imediatamente transmitidas.
- Difere do OFB porque o texto cifrado realimenta o método em vez da saída da cifra de bloco.



Cifragem modo Cipher Feedback - CFB



Decifração modo Cipher Feedback - CFB

O CFB é capaz de cifrar dados de qualquer tamanho, independentemente do bloco. É útil para cifrar pequenas quantidades de informação ou informações que devem ser imediatamente transmitidas, independentemente de completar um bloco ou não.

Figura 6.5
Cipher Feed Back (CFB) – Cifra Realimentada.

Output Feedback



Output Feedback – OFB (Saída Realimentada):

- Transforma cifra de blocos em gerador de números pseudoaleatórios.
- Gera bloco de fluxo de chave cifrando bloco de fluxo de chave anterior.

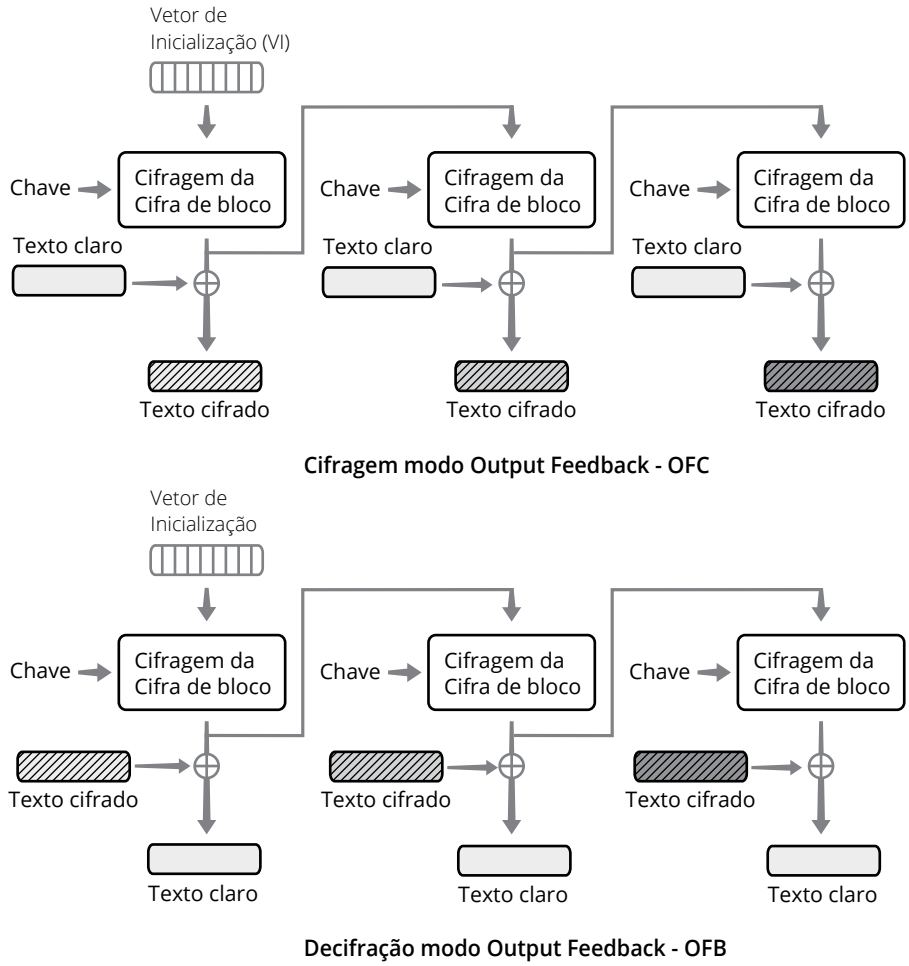


Figura 6.6
Output Feedback (OFB) – Saída Realimentada.

Parecido com o CBC, porém não existe dependência entre os blocos. Múltiplas cifragens da mesma mensagem produzem mensagens diferentes, ainda que utilizando a mesma chave.

Data Encryption Standard (DES)

- Durante muitos anos foi o algoritmo padrão usado para criptografia simétrica.
- Criado pela IBM em 1977 com tamanho de chave pequeno (56 bits randômicos e 8 bits de paridade).
- Quebrado por força bruta em desafio lançado pelo National Institute of Standards and Technology (NIST), em 1997.

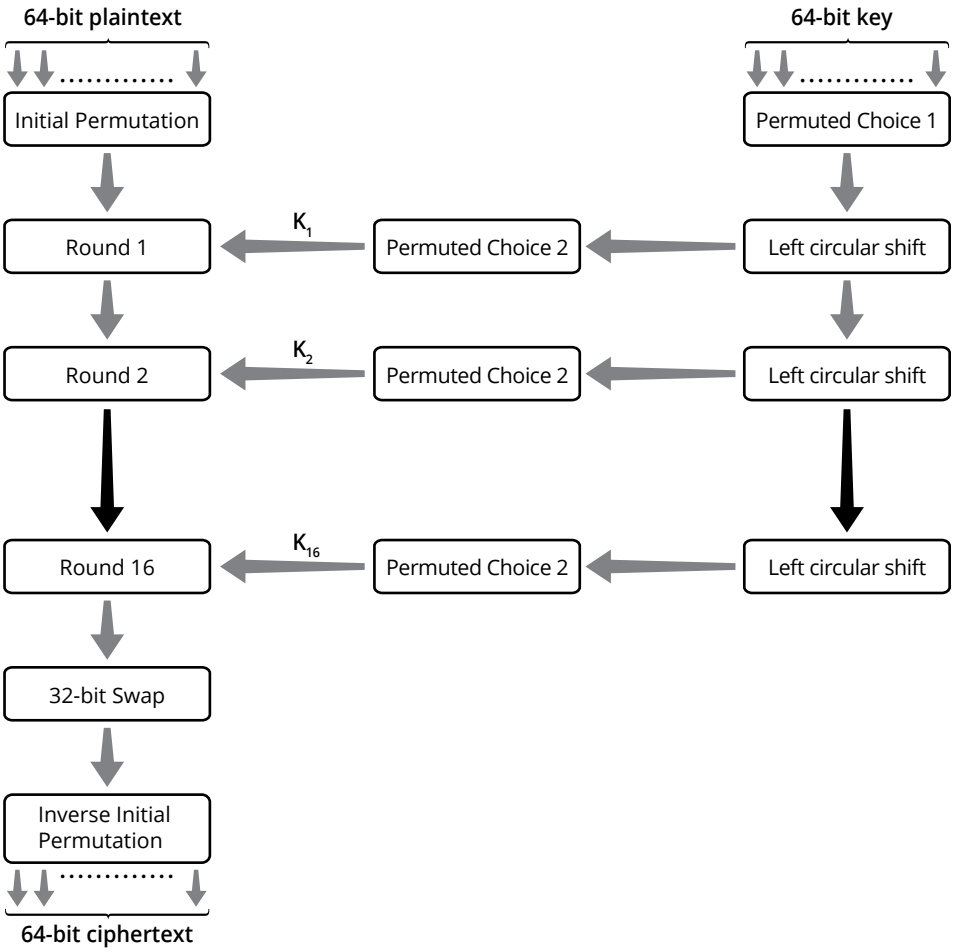


Figura 6.7
Data Encryption Standard (DES).

Opera em blocos de 64 bits. Em sua forma padrão, usa uma chave de 64 bits, na qual 56 bits são randômicos e os oito bits restantes são informações de paridade, usadas para verificar a integridade da chave. O DES pode ser usado em qualquer um dos quatro modos descritos anteriormente (ECB, CBC, CFB e OFB).

Existe uma variação do DES chamada de 40-bit DES. Essa variação foi criada pelo governo americano para permitir o uso do algoritmo fora dos Estados Unidos. Na época, eles não permitiam a exportação de qualquer sistema de criptografia com mais de 40 bits de chave. Ele era o próprio DES, sendo que 24 bits da chave eram fixos (40 + 24 = 64 bits).

A especificação do DES pode ser encontrada em: http://www.itl.nist.gov/fipspubs/fip46-2.htm

Algoritmo usado:

- Mensagem de 64 bits é dividida em duas partes de 32 bits.
- Chave de 56 bits é usada para gerar 16 chaves de 18 bits.
- O algoritmo é aplicado sucessivamente 16 vezes através das chaves geradas.

3DES, RC-4, IDEA e AES

3DES (Triple DES).

- DES aplicado em três ciframentos sucessivos, usa versão com duas ou três chaves diferentes. Seguro, porém lento.

RC-4 (RivestCipher4).

- Criado por Ron Rivest (do MIT), propriedade da RSA Data Security, usa chave de 128 bits, funciona em fluxo contínuo. Quatro vezes mais rápido que o DES.

International Data Encryption Algorithm (IDEA).

- Algoritmo patenteado, usa chave de 128 bits; mais rápido que o DES, é usado no mercado financeiro e no PGP.

Advanced Encryption Standard (AES)

Assista a um vídeo sobre o Rijndael: http://www.conxx.net/rijndael_anim_conxx.html

- Aprovado pelo Federal Information Processing Standards (FIPS) para ser adotado pelo NIST; algoritmo usado: Rijndael.
- Substituto do DES, livre de royalties, tamanho de bloco e de chave variável; fácil implementação.

O AES foi o resultado de uma seleção de diversos algoritmos, candidatos a se tornarem um padrão para criptografia em entidades governamentais nos Estados Unidos. Foi aprovado em novembro de 2001. O algoritmo AES é capaz de utilizar chaves criptográficas de 128, 192 e 256 bits para cifrar e decifrar blocos de 128 bits. Junto com o AES, foram criados dois novos modos de cifragem: o CCM e o CTR.

Informações sobre o AES e os novos modos de cifragem podem ser encontradas em:

- http://csrc.nist.gov/CryptoToolkit
- http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf
- http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

Algoritmo Diffie-Hellman

- Primeiro uso do conceito de chave pública/chave privada proposto por Diffie e Hellman em 1976.
- Serve para a troca de chaves simétricas em meio inseguro sem conhecimento prévio de segredo.
- Usado para distribuição de chaves, mas não para cifrar ou decifrar mensagens.



Figura 6.8
Whitfield Diffie e Martin Hellman, criadores do algoritmo. Fonte: http://commons.wikimedia.org

O algoritmo foi criado em 1976, em um artigo chamado *New Directions in Cryptography*.

Leia mais sobre o algoritmo em http://www.rsa.com/rsalabs/node.asp?id=2248

Seu nome faz referência aos autores do algoritmo. Atualmente, existem ataques contra o Algoritmo Diffie-Hellman. Existem propostas de versões que usam certificados digitais para reduzir a possibilidade de ataques, mas o algoritmo ainda é muito usado para troca de chaves simétricas.

Criptografia assimétrica

Também chamada de criptografia de chave pública e chave privada.

Usa par de chaves:

- Chave pública: distribuída livremente.
- Chave privada: guardada pelo usuário.

Propriedades importantes:

- Mensagem cifrada com chave pública só é decifrada com chave privada do par.
- Mensagem cifrada com chave privada só é decifrada com chave pública do par.
- Derivar chave privada a partir da chave pública é computacionalmente inviável.

O algoritmo mais conhecido de chave pública é o algoritmo RSA, que se tornou público em 6 de setembro de 2000. Foi criado por Ron Rivest, Adi Shamir e Leonard Adelman (a sigla RSA foi formada a partir da letra inicial do sobrenome de seus criadores).

Mais informações sobre o RSA podem ser obtidas no padrão Public Key Cryptography Standard#1 (PKCS #1), encontrado em: http://www.rsa.com/rsalabs/node.asp?id=2125

No RSA, a segurança do sistema baseia-se na dificuldade da fatoração de números grandes.

No El Gamal, a segurança do sistema baseia-se na dificuldade do cálculo de logaritmos discretos em um corpo finito.

O Digital Signature Algorithm (DSA), unicamente destinado a assinaturas digitais, foi proposto pelo NIST em agosto de 1991, para utilização no seu padrão.

O Digital Signature Standard (DSS) foi adotado como padrão no final de dezembro de 1994. Trata-se de uma variação dos algoritmos de assinatura El Gamal e Schnorr. Foi inventado pela NSA e patenteado pelo governo americano. O DSS é mais rápido na geração de chaves, comparado ao RSA; o RSA, porém, é mais rápido na verificação de assinaturas.

Algoritmos mais usados:

- RSA;
- DSA;
- El Gamal;
- DSS.

- Alice e Bob criam par de chaves individuais.
- Alice e Bob trocam chaves públicas.
- Alice escreve mensagem.
- Alice usa chave pública de Bob para cifrar.
- Alice envia resultado para Bob.
- Bob usa sua chave privada para decifrar.
- Bob escreve resposta, cifra com chave pública de Alice e envia para Alice.
- Alice usa sua chave privada para decifrar a resposta.

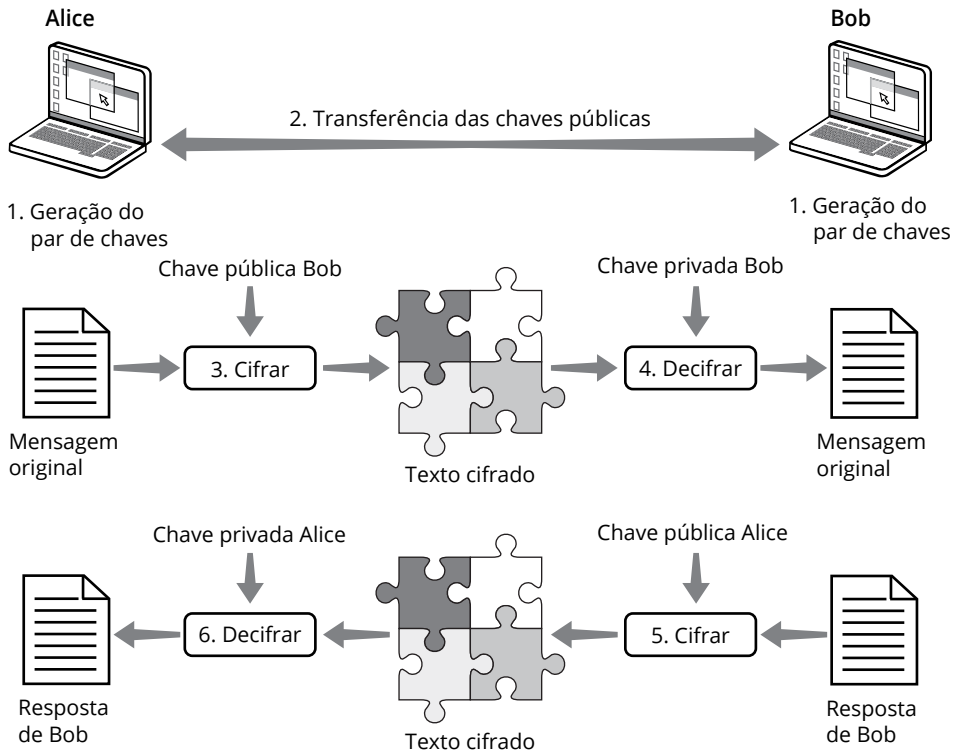


Figura 6.9
Transferência de chaves.

Para pensar

Esse tipo de comunicação levanta uma questão básica: como garantir que a chave pública de Alice realmente pertence à Alice, e não a uma pessoa se fazendo passar por Alice? Pelo esquema anterior, qualquer pessoa poderia gerar um par de chaves como se fosse Alice e distribuir uma chave pública falsa. Nesse caso, precisamos de um mecanismo que nos permita atestar a autenticidade de uma chave pública. Esse mecanismo chama-se certificação digital e será examinado mais adiante.

Funções de hash

- A partir de entrada de tamanho variável, produz saída de tamanho fixo.
- A saída é chamada de hash (digest), impressão digital da mensagem.
- Propriedades de um algoritmo de hash:
  - **Consistência:** mesma entrada produz sempre a mesma saída.
  - **Randômico:** a saída não permite descobrir informações sobre a mensagem original.
  - **Único:** quase impossível duas mensagens produzirem hashes iguais.
  - ***One-way* (mão única):** a partir do hash é impossível descobrir a mensagem original.

O Message Digest 4 (MD4) e o MD5 foram criados por Ron Rivest, no MIT. O Secure Hash Algorithm (SHA) foi desenvolvido pelo NIST. O MD5 processa a entrada em blocos de 512 e produz uma saída de 128 bits. O SHA processa a entrada em blocos de 512 e produz uma saída de 160 bits. O SHA necessita de um processamento mais intensivo e pode rodar um pouco mais lentamente que o MD5. Em 1995, o SHA original foi atualizado, por problemas de segurança, e foi proposto o SHA-1 (o anterior costuma ser chamado de SHA-0 para

evitar confusão). Posteriormente, foram criadas mais quatro variações: SHA-224, SHA-256, SHA-384 e SHA-512. Essas últimas variações são eventualmente chamadas de SHA-2.

Pesquisadores chineses anunciaram a descoberta de uma série de colisões (mensagens diferentes produzindo o mesmo hash) nos algoritmos MD4 e MD5.

Essas descobertas foram anunciadas em uma conferência sobre criptografia no ano de 2004 e causaram grande impacto, uma vez que boa parte dos sistemas em produção utilizam esses algoritmos. Mais informações sobre as colisões podem ser encontradas nos seguintes artigos:

- http://eprint.iacr.org/2004/199.pdf
- http://eprint.iacr.org/2004/146.ps

Algoritmos:

- Message Digest-4 (MD4): saída de 128 bits.
- Message Digest-5 (MD5): saída de 128 bits.
- SecureHashAlgoritm (SHA): saída de 160 bits (um pouco mais lento).

Calcule seu hash:

- http://www.yellowpipe.com/yis/tools/encrypter/index.php



Usado para garantir integridade da mensagem transferida.

- Alice escreve uma mensagem.
- O hash é calculado para representar a mensagem.
- A mensagem original é enviada para Bob junto com o hash.
- Bob separa a mensagem original e calcula o hash localmente.
- Bob compara os hashes.
- Caso os hashes sejam iguais, a mensagem não foi alterada.

Exercício de fixação 1
Criptografia assimétrica

Quais as principais vantagens da criptografia assimétrica sobre a simétrica?

Assinatura digital



Hash da mensagem cifrado com chave privada: garante a identidade do remetente e a integridade da mensagem ou do documento.

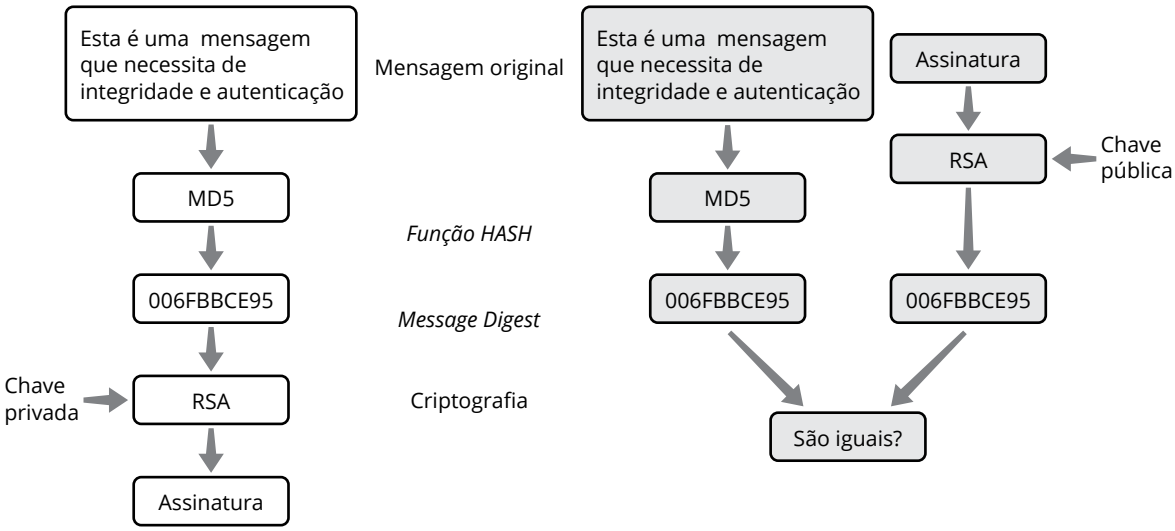


Figura 6.10
Assinatura digital.

As assinaturas digitais não garantem confidencialidade e sofrem o mesmo problema de autenticidade das chaves públicas, como foi visto na criptografia assimétrica. Para resolver esse problema, é necessário o uso de certificados digitais.

- Bob: escreve mensagem, calcula hash da mensagem, cifra hash com sua chave privada (assinatura digital), envia assinatura e mensagem para Alice.
- Alice: separa assinatura da mensagem original, utiliza chave pública de Bob para decifrar assinatura, calcula hash local da mensagem original, utilizando a mesma função usada por Bob. Caso os dois hashes sejam iguais, a mensagem foi enviada por alguma pessoa utilizando chave privada de Bob, e não foi modificada na transmissão.

Certificação digital

Como confiar em uma chave pública? A chave pública de Alice é realmente de Alice?

Carteira de identidade (Secretaria de Segurança Pública) assinada por delegado de polícia, tem "fé pública".

- Indivíduo → chave pública.
- Carteira de identidade → certificado digital.
- Secretaria de Segurança → autoridade certificadora ou Certification Authoritie (CA).

Um certificado, para ser considerado válido, deve ser assinado por uma Certification Authoritie (CA). CAs são entidades confiáveis que emitem e atestam certificados, análogas aos cartórios, que verificam assinaturas normais. Um ponto chave da certificação digital é o fato de a chave pública da CA ser amplamente distribuída (necessária para verificação da assinatura) por meios que impeçam fraudes. Um exemplo prático de distribuição de chaves públicas de CAs é o webbrowser, que já vem com as chaves pré-instaladas no próprio programa. Uma entidade certificadora é responsável por criar, distribuir e invalidar certificados. A invalidação de certificados é feita através de listas especiais chamadas de Certificate Revogation Lists (CRLs). Apesar de todo certificado ter uma validade, em certos casos é necessário expirar um certificado antes do tempo. Essa expiração é feita através das CRLs.

Certificado digital

- Contém chave pública do usuário e dados informando a sua identidade;
- É uma mensagem emitida e assinada pela CA, que valida a chave pública do usuário;

- A chave pública da CA é amplamente distribuída.

O certificado segue o padrão X.509 do ITU-T, contendo:

- Versão do X.509 e número serial do certificado;
- Informação do algoritmo gerador do certificado;
- Identificação do gerador do certificado;
- Datas de validade;
- Informações sobre o algoritmo assimétrico da chave pública do usuário;
- Assinatura digital da CA.

Public Key Infrastructure (PKI)

O certificado digital deve ser solicitado a uma AC ou a uma AR.

- AC: Autoridade Certificadora.
- AR: Autoridade de Registro, solicita certificado a uma AC.

PKI = ICP (Infraestrutura de Chaves Públicas).

- Hierarquia: AC raiz autoriza operações de outras ACs.

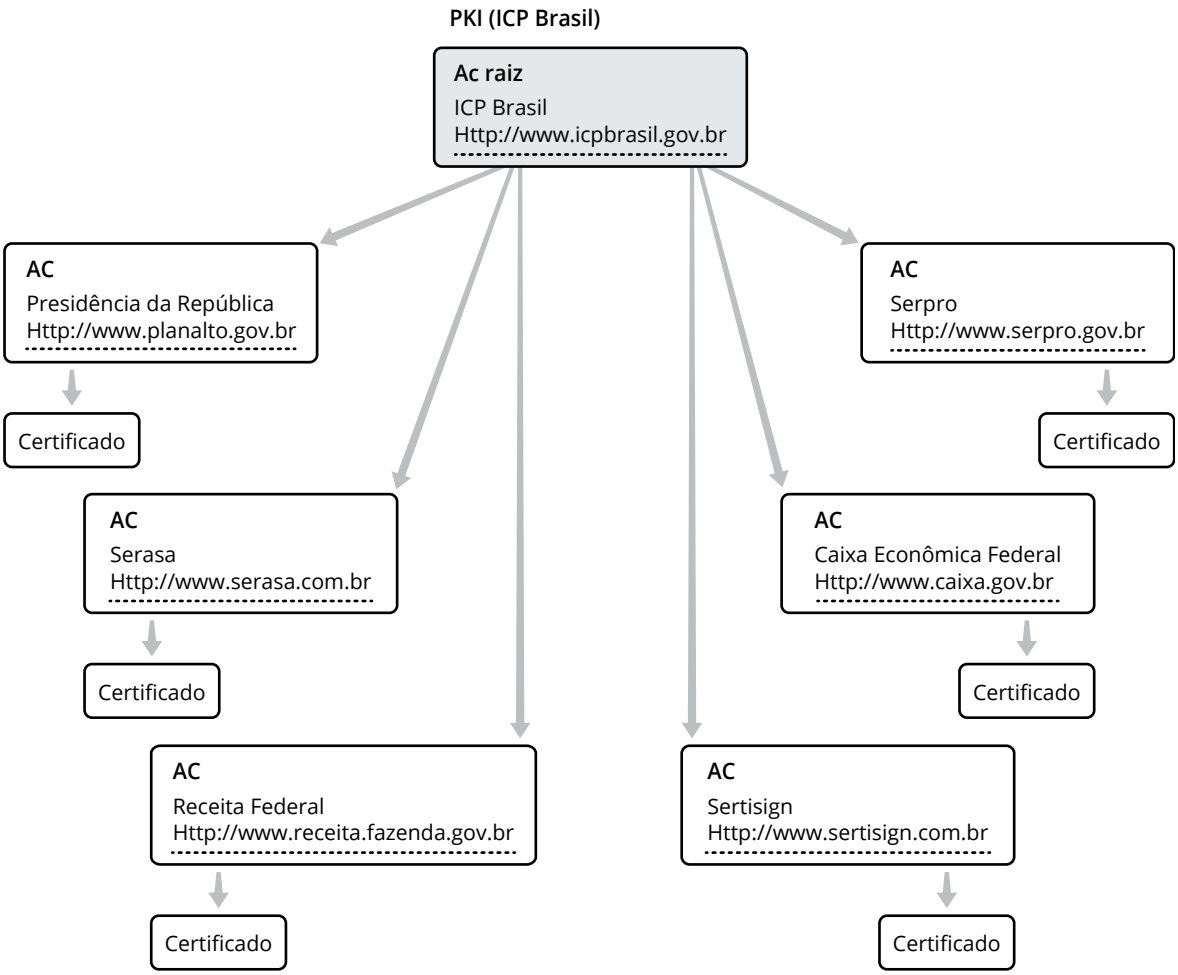


Figura 6.11
Public Key Infrastructure (PKI).

O conjunto de hardware e software pessoal, políticas e procedimentos necessários para criar uma infraestrutura de certificação digital chama-se Public Key Infrastructure (PKI) ou Infraestrutura de Chaves Públicas (ICP).

No Brasil, a ICP Brasil controla seis ACs: Presidência da República, Receita Federal, Serpro, Caixa Econômica Federal, Serasa e Certisign. Para que tenha valor legal diante do governo brasileiro, uma dessas instituições deve prover o certificado. Para que isso seja feito, cada instituição pode ter requisitos e custos diferentes para a emissão, uma vez que cada entidade pode emitir certificados para finalidades distintas.

Atualmente, o Governo Federal possui uma infraestrutura nacional de chaves públicas chamada de ICP Brasil, que pode ser lida no site: http://www.iti.gov.br/icp-brasil/estrutura

Qualquer instituição pode criar uma ICP, independente de seu porte. Se uma empresa criou uma política de uso de certificados digitais para a troca de informações entre a matriz e suas filiais, não vai ser necessário pedir tais certificados a uma AC controlada pela ICP Brasil. A própria empresa pode criar sua ICP e fazer com que um departamento das filiais atue como AC ou AR, solicitando ou emitindo certificados para seus funcionários.

Exemplo completo

- Como garantir confidencialidade, integridade e autenticidade (não repúdio)?
- Combinando tecnologias: criptografia simétrica, assimétrica, hash e certificado digital.

1. Alice e Bob geram seus respectivos pares de chaves.
2. Alice e Bob obtêm seus certificados digitais em uma CA.
3. Alice e Bob trocam certificados.
4. Alice:
   - Prepara chave simétrica randômica e calcula hash.
   - Cifra hash com chave privada (assina).
   - Cifra chave simétrica e assinatura com chave pública de Bob e transmite.
5. Bob:
   - Decifra o conjunto recebido, extrai chave simétrica e assinatura.
   - Decifra a assinatura de Alice, extrai hash transmitido por Alice.
   - Calcula o hash local da chave simétrica.
   - Hashes são iguais? Caso sejam, a chave simétrica foi enviada por Alice e não foi alterada.
6. Alice e Bob:
   - Realizam conversa cifrada utilizando chave simétrica.
   - Para garantir integridade, cada mensagem é cifrada junto com hash.

Roteiro de Atividades 6

Atividade 6.1 – Conhecendo mais sobre certificação digital

1. Assista o vídeo do Instituto Nacional de Tecnologia da Informação (ITI) em http://www.youtube.com/watch?v=YEy2uKG2nB8 e conheça mais sobre a certificação digital e sobre a ICP-Brasil.

Descreva em poucas palavras o que você entende por certificação digital.

Atividade 6.2 – Uso de criptografia em e-mails

1. Tenha certeza de ter instalado os pacotes Firefox e Thunderbird.
2. Instale o pacote GnuPG, programa gratuito de criptografia:
   - http://www.gnupg.org/download/
   - Hash do pacote: b806e8789c93dc6d08b129170d6beb9e1a5ae68f
3. Certifique-se de que o pacote está íntegro.
4. Instale o plugin "enigmail" no Thunderbird: http://www.enigmail.net/download/index.php
5. Gere seu par de chaves e compartilhe com seus colegas.

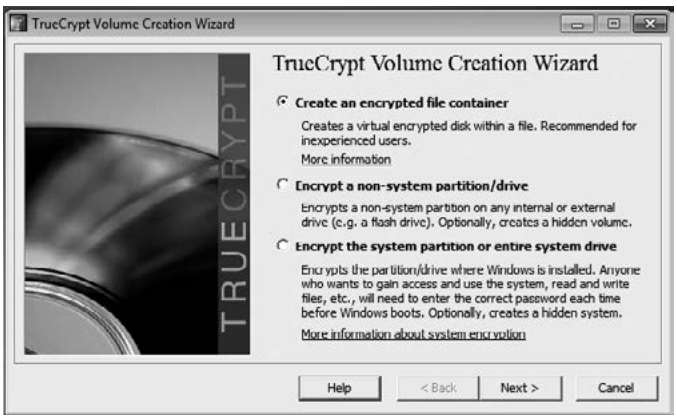
Atividade 6.3 – Uso de criptografia em arquivos

1. Cifre um arquivo usando sua chave pública.
2. Peça ao seu colega para tentar decifrá-lo.
3. Decifre o arquivo com sua chave privada.
4. Cifre um arquivo usando criptografia simétrica.
5. Envie a chave privada utilizada para seu colega e peça para ele decifrar o arquivo.

Atividade 6.4 – Criando um contêiner seguro

1. Baixe o programa truecrypt em http://www.truecrypt.org/downloads

2. Rode o instalador.



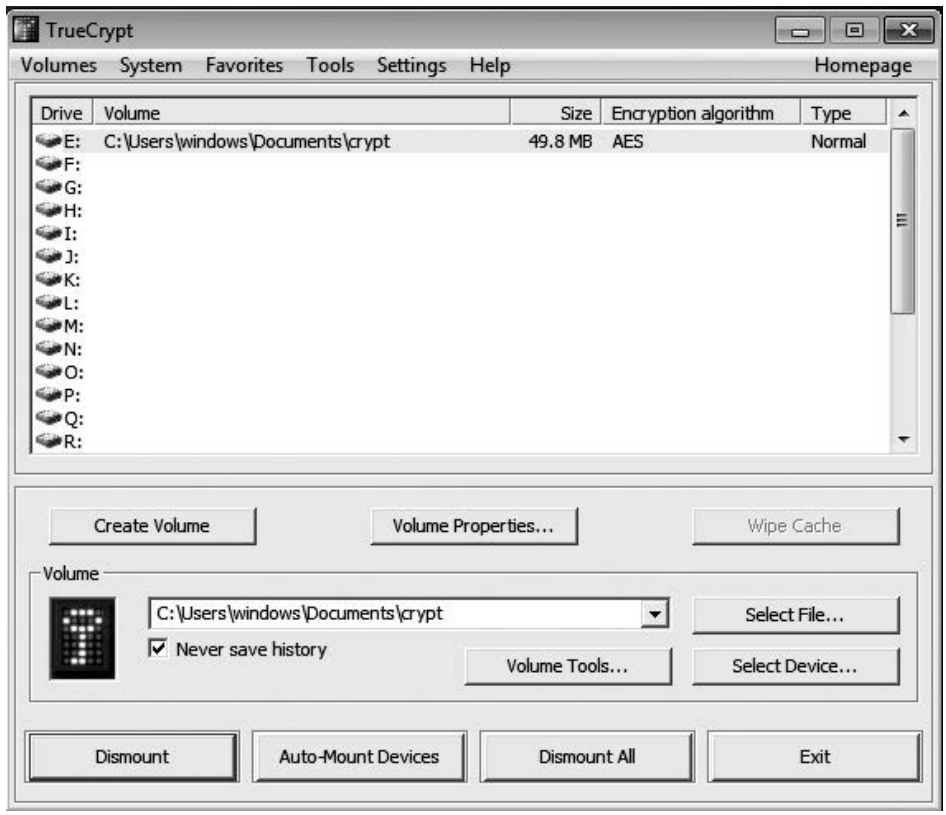
3. O truecrypt pode criptografar uma unidade inteira ou apenas criar um contêiner seguro. Com isso podemos salvar arquivos em um espaço de disco criptografado e transportá-lo para outro computador com bastante conveniência.

Vamos usar a segunda opção: clique em “Create volume”:



4. Selecione um local e um nome para o contêiner.

5. Selecione o tipo de criptografia. Para esse exemplo selecione AES e clique em “Next”. Na próxima tela, informe 50MB para o tamanho do volume, e na tela seguinte informe uma senha para o arquivo. Na tela seguinte, escolha o formato da partição (nesse exemplo foi utilizado FAT). Observe que o programa pede para o usuário mover o cursor do mouse para gerar uma chave com um nível de criptografia maior para as chaves geradas.



6. Pronto. Para usar o contêiner, clique em uma letra de unidade e selecione o arquivo criado.



7

Criptografia II – Aplicações

objetivos

Apresentar aplicações práticas de criptografia; contextualizar os conceitos básicos de criptografia com as aplicações; mostrar como navegar de forma segura; explicar o funcionamento de assinaturas digitais, criptografia de servidor www (SSL/TLS) e VPNs criptografadas; indicar programas para melhorar a segurança de um computador pessoal.

conceitos

SSH, transferência de arquivos e gerenciamento de senhas.

Introdução



A criptografia é a base para várias aplicações:

- Autenticação e autorização.
- Transferência de informação confidencial.
- Assinatura digital.
- Votação eletrônica.
- Dinheiro eletrônico.
- Privacidade e autenticação no acesso a servidores (SSL/TLS).
- Acesso remoto criptografado e autenticado (VPN).

A criptografia permite a existência de uma série de aplicações, como autenticação, assinaturas digitais, transferência de informação confidencial, dinheiro eletrônico, acesso remoto criptografado (**VPN**) e privacidade de dados em servidores (SSL). Uma assinatura digital atesta que um documento eletrônico não foi alterado e garante a autenticidade do indivíduo que assinou o documento. O SSL permite o acesso a servidores www com segurança e garantia de que os dados não foram alterados nem vistos no caminho. As redes virtuais privadas (VPNs) criam um canal seguro para acesso a redes privadas de empresas, usando a internet como meio de transmissão. As VPNs reduzem custos em relação a linhas discadas e linhas dedicadas.

VPN
Rede Privada Virtual, é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a internet). O tráfego de dados é levado pela rede pública utilizando protocolos padrão.

Exercício de nivelamento 1
Criptografia

Quais as vantagens da sua organização utilizar a criptografia?

Assinatura digital



Uso básico da criptografia para:

- Atestar identidade do assinante do documento (autenticação).
- Garantir que o documento não foi alterado (integridade).

A robustez depende de duas propriedades básicas:

- Função hash randômica o suficiente para não provocar colisão.
- Certificação digital para garantir autenticidade da chave pública.

Algoritmos mais usados:

- RSA e DSS.

Blind signature (assinatura cega)



Assinatura digital onde o assinante não conhece o conteúdo da mensagem assinada.
Usada em:

- Voto eletrônico.
- Dinheiro digital.

Entendendo o processo:

- Alice multiplica mensagem por fator randômico (blinding factor), tornando a mensagem ilegível.
- Alice envia mensagem resultante para Bob.
- Bob assina digitalmente a mensagem e retorna para Alice.
- Alice divide a mensagem pelo fator randômico, retornando a mensagem original, agora assinada por Bob.

Podemos imaginar o processo de assinatura cega da seguinte forma: colocamos a mensagem em um envelope, envolta em uma folha de papel carbono. Ninguém pode ler a mensagem através do envelope. A assinatura, então, é feita na parte externa do envelope e transmitida para a mensagem através do papel carbono. Quando a mensagem é retirada do envelope, ela está assinada e o assinante não sabe o que foi assinado.

A função de assinatura e o fator randômico devem ser comutativos.

Propriedades:

- A assinatura, depois de dividida pelo fator randômico, é a mensagem assinada normalmente;
- Não se pode provar o uso de protocolo de assinatura cega em uma mensagem assinada digitalmente.

Votação eletrônica

O protocolo ideal para uma eleição segura tem seis requisitos:

- Somente eleitor autorizado pode votar.
- Nenhum eleitor pode votar mais de uma vez.
- Ninguém pode determinar o voto de ninguém.
- Ninguém pode duplicar voto.
- Ninguém pode alterar o voto de alguém sem ser descoberto.
- Todo eleitor tem de ter certeza de que seu voto entrou na contagem final.



Figura 7.1
Urna eletrônica.

O sistema de eleição se baseia em três características fundamentais:

- Votação, através da qual os membros da população reconhecidos como eleitores podem expressar, anonimamente, sua vontade;
- Apuração, que permite a contabilização dos votos emitidos por esses eleitores;
- Fiscalização, que visa garantir a idoneidade do processo, de modo a assegurar que o resultado da apuração dos votos seja realmente a expressão da vontade dos eleitores.

Um sistema eletrônico de eleição deveria ser tal que assegurasse essas três características fundamentais, de preferência melhorando cada um de seus aspectos, jamais sendo menos seguro e confiável do que um sistema não eletrônico.

Entendendo o processo com assinatura cega:

Eleitor:

- Gera n mensagens; cada mensagem contém voto válido para cada resultado possível e número serial de identificação randômico.
- "Cega" as mensagens, enviando-as para a Central de Votação (CV) junto com fator de cegueira.

Central de Votação (CV):

- Abre "n – 1" mensagens, checa mensagens e eleitor, grava eleitor.
- Assina todas as mensagens e envia-as de volta para eleitor.

Eleitor:

- Retira fator de cegueira; cada voto está assinado, mas não cifrado.
- Escolhe seu voto, cifra-o com chave pública da CV e envia voto para a CV.

Central de votação:

- Decifra, checa, grava número serial e computa o voto.
- Anuncia resultado da eleição com voto associado ao número serial.

Dinheiro eletrônico

O dinheiro tem algumas características básicas:

- Aceitação universal: forma mais universalmente aceita.
- Pagamento garantido: recebimento já garante pagamento efetuado.
- Sem custo de transação: não há custo para pagamentos em espécie.
- Anonimidade: não guarda informação em si sobre quem usou-o para pagamento.

Substituto para o dinheiro tradicional (papel). Qual o problema com o pagamento de cartão de crédito digital ou cheque? Mantém rastro para auditoria, e não permite ocultar o destinatário do dinheiro. O dinheiro eletrônico pode ser considerado como uma moeda estrangeira, uma vez que para utilizá-lo é preciso antes convertê-lo de dinheiro real (moeda corrente) para dinheiro digital.

Bitcoin

O bitcoin é uma moeda virtual criada por Satoshi Nakamoto. Funciona com um programa em código aberto projetado por ele mesmo que se liga em uma rede peer-to-peer. Permite a propriedade e a transferência anônima de valores, que são armazenados em uma carteira virtual. Como não existe nenhuma entidade por trás da administração da moeda, sua manipulação indiscriminada é inviabilizada por governos ou empresas, como por exemplo em sua supervalorização, o que poderia gerar inflação ou mesmo a impressão de mais moeda. Em outubro de 2009, 1 dólar americano comprava o equivalente a 1309 bitcoins. Em fevereiro de 2011, o bitcoin alcançou a equivalência com o dólar. De lá para cá, a coisa explodiu. No início de 2012, 1 bitcoin estava valendo cerca de 13 dólares, um salto significativo desde o início das operações, mas nada perto do que viria a acontecer nos meses seguintes. No dia 10 de abril, chegou a ser negociado a 266 dólares, o que indica uma valorização de 1900% (Fonte: mtgox.com).

Saiba mais sobre bitcoin acessando "What is bitcoin?" no Youtube.

Amazon Webpay

O serviço de pagamento da Amazon permite aos usuários cadastrados transferir dinheiro entre si via e-mail. Para isso, é necessário apenas ter uma conta na Amazon.com. A qualquer hora e de qualquer lugar, você recebe ou envia dinheiro para amigos e familiares, bastando estar on-line.

Google Wallet

O Google Wallet é um sistema de pagamento desenvolvido pelo Google que permite o armazenamento de cartões de crédito e transações financeiras. Através do Google Wallet, um usuário pode fazer pagamentos virtuais em sites de e-commerce ou físicos, através de estabelecimentos credenciados com a tecnologia Near Field Communication (NFC). O Google Wallet permite também que qualquer usuário possa enviar valores por e-mail (valor mínimo de U$ 0,30) para outro usuário (o valor vai "anexado" na mensagem).

Entendendo o processo com dinheiro digital anônimo:

- Alice:
  - Prepara 100 ordens de pagamento anônimo de R$ 1.000 cada.
  - Envelopa todas as ordens (cega-as) e envia-as para o banco.

- Banco:
  - Abre 99 envelopes, confirma que cada envelope é um pedido de R$ 1.000.
  - Assina o único envelope que não foi aberto.
  - Envia envelope assinado de volta para Alice, deduz R$ 1.000 de sua conta.
- Alice: abre o envelope e gasta ordem de pagamento com lojista.
- Lojista: verifica assinatura do certificado com o banco e saca ordem de pagamento.
- Banco: verifica sua própria assinatura e credita R$ 1.000 na conta do lojista.

PayPal

- Localizada em San Jose, na Califórnia (EUA).
- Criado por Peter Thiel e Max Levchin, em 1998, para pagamentos via PDAs.
- Adquirido pelo eBay em outubro de 2002.
- Disponível em 190 países (incluindo Brasil) e em 24 moedas correntes.

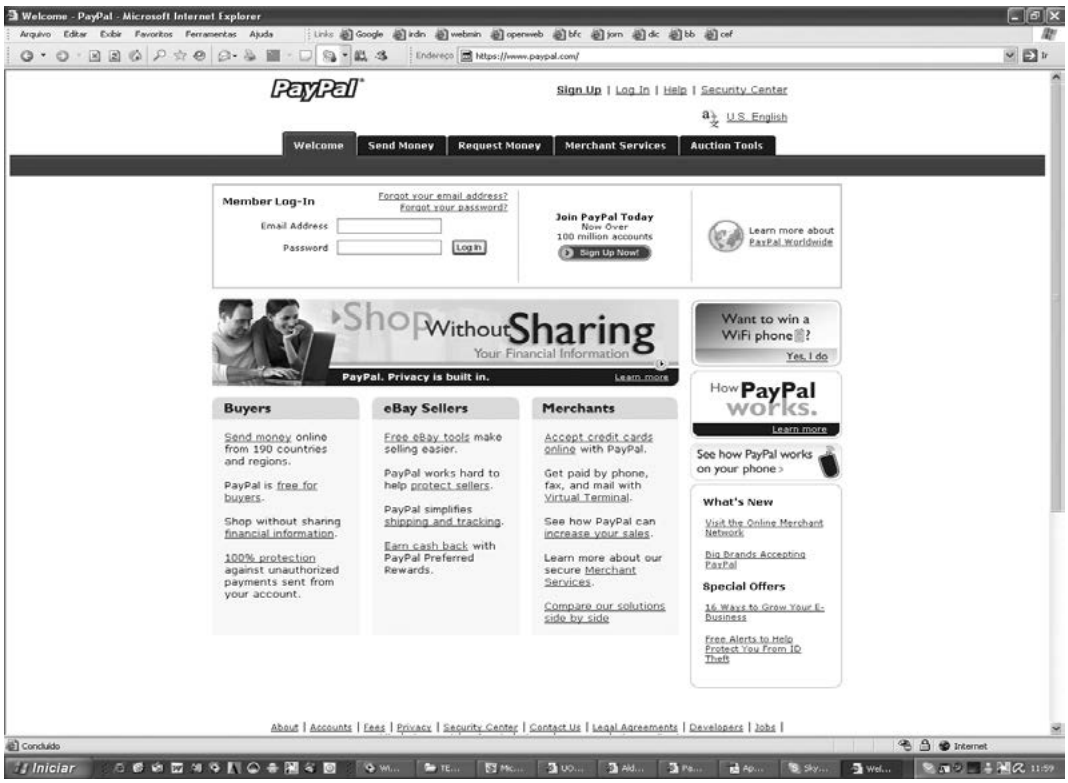


Figura 7.2
Site do PayPal.

O PayPal é um sistema on-line de envio e recebimento de dinheiro. Possibilita realizar pagamentos de leilões e compras de inúmeros itens em vários sites na internet, saque de fundos por transferência em conta corrente ou via recebimento de cheque pelo correio, tudo em dólares ou em euros. É um sistema seguro que protege vendedores e compradores; é a moeda preferida pelo eBay e conta com mais de 150 milhões de usuários.

Qualquer pessoa pode se cadastrar no PayPal e abrir uma conta pessoal ou empresarial, bastando apenas ter um endereço de correio eletrônico válido e um cartão de crédito internacional.

É necessário ter:

- Endereço de correio eletrônico;
- Cartão de crédito internacional;
- Conta de acesso ao PayPal.

Usado para pagamentos de:

- Registros de domínios;
- Comércio eletrônico;
- Serviços de hospedagem de sites.

Mais informações: http://www.paypal.com

Criptografia de servidor (SSL/TLS)



Uso comum de criptografia em comunicação segura com servidor internet.

- Padrão internet: Tecnologia Secure Sockets Layer (SSL), da Netscape.
- SSL: túnel em nível de aplicação. TLS: túnel em nível de transporte.
- Transport Layer Security (TLS): RFC 2246 baseado na versão 3.0 do SSL, provê infraestrutura de criptografia, autenticação e integridade na camada de transporte TCP.

Segurança Camadas		Criptografia	Níveis	
	Compatível com cliente.	Baixo RC4 de 56 bits.	Alto RC4 de 128 bits.	Compatível com FIPS.
Negociar	Válido. A camada de segurança Máxima e o nível de criptografia para os quais o cliente oferece suporte são usados.	Válido	Válido	Válido
SSL (TSL 1.0)	Válido. O TLS é necessário para autenticação do servidor. O nível Alto ou Compatível com FIPS é usado. Se não houver suporte para o TLS, as conexões falharão.	Inválido. É usado o padrão do nível de criptografia em vez de Compatível com o Cliente. O nível Alto ou Compatível com FIPS é usado se o cliente oferecer suporte.	Válido	Válido
RDP	Válido. Entretanto, o TLS não pode ser usado para autenticação de servidor. A criptografia RDP e o nível de criptografia máximo para os quais o cliente oferece suporte são usados.	Válido	Válido	Válido

Tabela 7.1
Configurações de autenticação e criptografia – SSL/TLS no Windows Server 2003.

O TLS foi baseado no SSL versão 3.0. Apesar das diferenças serem pequenas, são suficientes para que os protocolos não sejam compatíveis. É muito comum encontrar clientes que suportam as duas tecnologias. Para efeitos didáticos, trataremos apenas do TLS, que é uma proposta mais recente que o SSL.

Mais informações em "The Transport Layer Security (TLS) Protocol Version 1.1" em http://www.ietf.org/rfc/rfc4346.txt

Lista de servidores:

- HTTP: HTPPS;
- FTP: SFTP via SSH ou FTP via TLS;
- SMTP: SMTPS;
- POP3: POP3s;
- IMAP: IMAPS;
- Telnet: SSH.

Regra de ouro de segurança: nenhuma senha trafega na rede em modo legível.

Criptografia de servidor

TLS é formado por dois protocolos básicos:

- TLS Hand Shake:
  - Autentica par cliente/servidor usando criptografia assimétrica.
  - Escolhe algoritmos de criptografia e chaves.
  - Negociação confiável da chave simétrica feita de forma segura.
- TLS Record:
  - Codifica e encapsula os dados e cria o túnel.
  - Conexão privada usando criptografia simétrica: algoritmos DES ou RC4.
  - Chaves privadas de sessão geradas dinamicamente.

Entendendo o processo:

Cliente

Envia lista de algoritmos e número randômico usado para geração de chaves.

Servidor

Escolhe algoritmo da lista, gera número randômico e envia-o junto com seu certificado assinado por entidade certificadora (X.509).

Cliente

- Verifica certificado do servidor e obtém chave pública do servidor;
- Gera chave secreta, criptografa-a com chave pública do servidor e envia para o servidor;
- Servidor e cliente trocam informações usando chave simétrica;
- Informação trocada tem digest para verificação de integridade;
- Opcionalmente o cliente pode se identificar usando seu certificado digital.

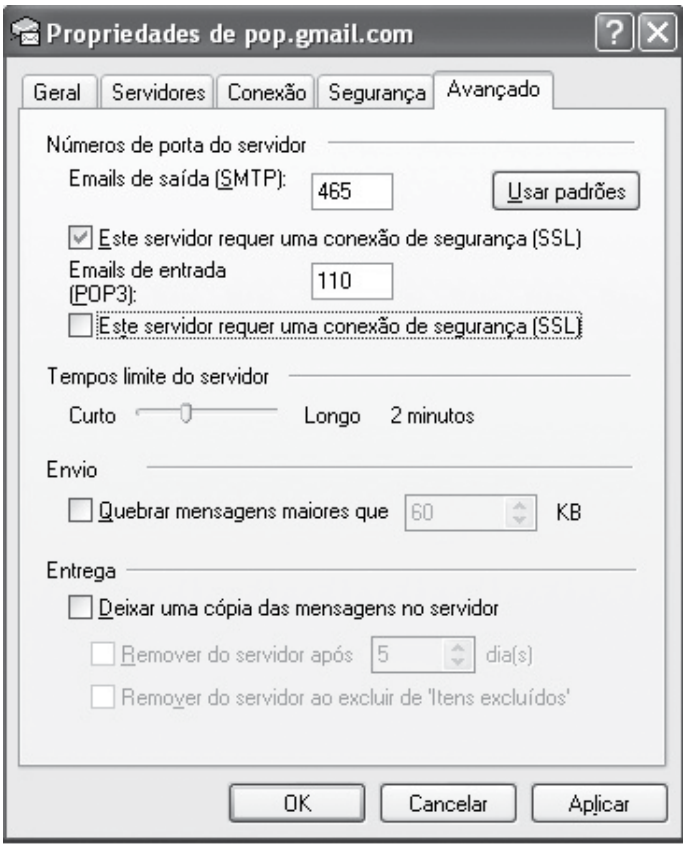


Figura 7.3
Gmail usando POP3 e SMTP, autenticado como POP.

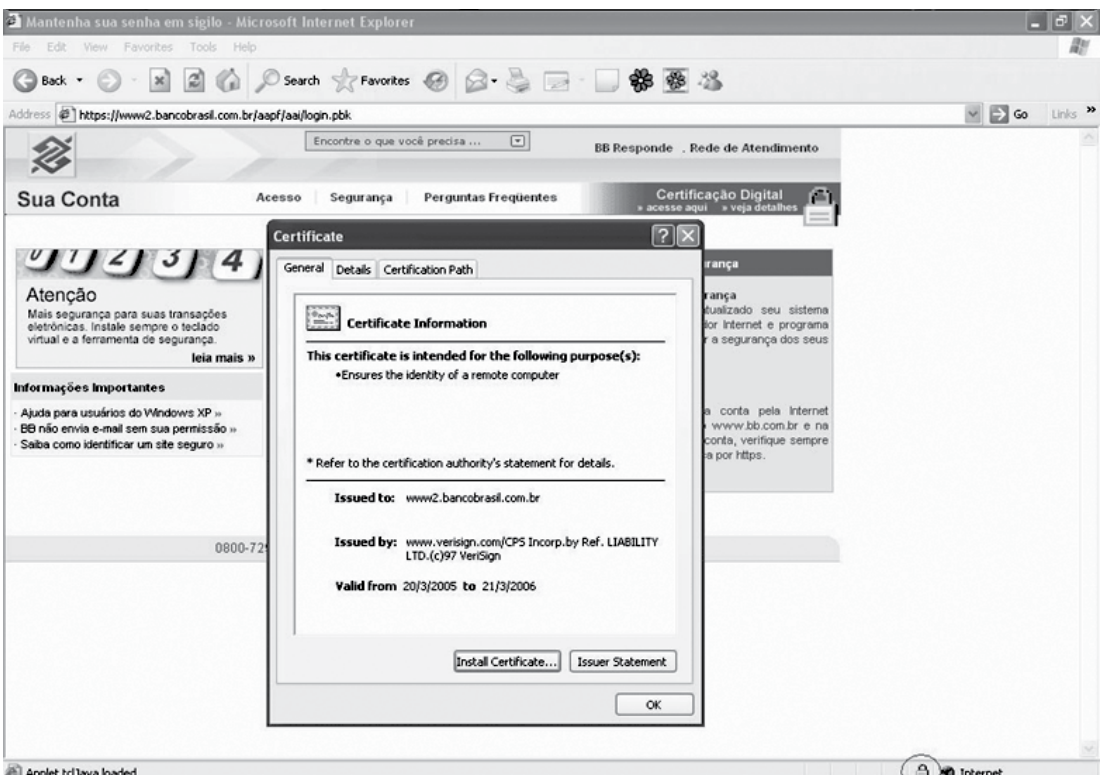


Figura 7.4
Internet Explorer acessando página segura.

Redes virtuais privadas (VPN)

- VPN é uma conexão segura através de uma rede pública ou outro tipo de ambiente inseguro.
- Rede montada virtualmente em cima de outra rede; se pública, a internet.
- Cria túneis com protocolo de criptografia, fornecendo:
  - Confidencialidade.
  - Autenticação.
  - Integridade.
  - Garantia de privacidade na comunicação.

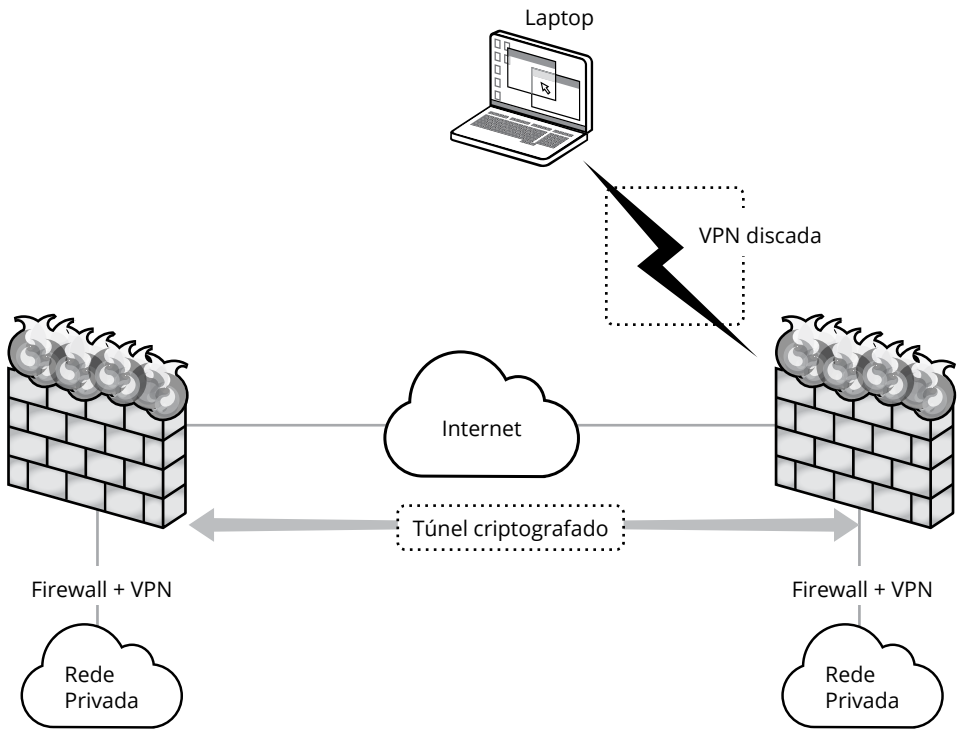


Figura 7.5 Redes virtuais privadas (VPN).

- Por que virtual? Porque não é física, não tem cabos, switches nem roteadores.
- Por que privada? Porque conecta redes e equipamentos para acesso privado e protegido.

Quando adequadamente implementados, os protocolos criptográficos podem assegurar comunicação segura através de redes inseguras.

Hoje, diversas empresas interligam suas bases operacionais através de uma VPN na internet.

Um sistema de comunicação por VPN tem custo de implementação e manutenção insignificante, se comparado aos antigos sistemas de comunicação física, como por exemplo Frame Relay e ATM, que têm alto custo. Por esse motivo, muitos sistemas de comunicação estão sendo substituídos por VPNs que, além do baixo custo, oferecem também uma alta confiabilidade, integridade e disponibilidade dos dados trafegados. Sistemas de comunicação por VPN estão sendo amplamente utilizados em diversos setores, até mesmo em setores governamentais no mundo inteiro.

IPSEC

- Padrão para criptografia de pacotes IP no nível de rede;
- Protocolo padrão para VPN;
- RFCs: 2401, 2402, 2406 e 2408.

Há dois tipos de VPN:

- "Host to network" (estação para rede), conhecida como VPN discada;
- "Network to network" (rede para rede), conecta duas redes privadas.

Redes virtuais privadas



Necessidades:

- Endereçamento IP e máscara das duas redes privadas.
- Endereço público de cada dispositivo responsável por fazer a VPN.
- Algoritmos e chaves de criptografia.

Vantagens:

- Reduz custos.
- Provê acesso entre redes privadas de forma segura através de rede pública.
- Provê acesso remoto à rede privada de forma segura através de rede pública.

Desvantagens:

- Dados trafegando em rede pública: contexto facilitador de ataques de criptoanálise.
- Internet sem garantia de qualidade: gera atraso, indisponibilidade e dificuldade para suporte.
- Degradação de desempenho:
  - Criptografia consome muito processamento;
  - Mais perceptível com maiores velocidades de conexão.

Exercício de fixação 1

Redes Virtuais Privadas (VPNs)

O que é uma VPN e quais as suas vantagens?

Segurança na www



- Seleção de um navegador.
- Recursos de um navegador.
- Cookies.
- Segurança no navegador.
- Pagamentos na internet.

Acessar a internet, nos dias de hoje, pode ser um sério problema, se levarmos em conta a quantidade de ameaças existentes. É importante que o usuário conheça as formas de se prevenir e use programas específicos de proteção. Os recursos do browser, programas anti-vírus, programas de detecção e remoção de spyware e certificados digitais são algumas das formas de proteção contra ameaças na internet.

Seleção de um navegador

Selecione um navegador seguro:

Browser	Plataformas suportadas	URL
Internet Explorer	Família Windows	http://www.microsoft.com/ie
Firefox	Windows, MacOS X e Linux	http://www.mozilla.org/products/
Opera	Windows, MacOS X, Linux, FreeBSD, Solaris, OS/2 e QNX	http://www.opera.com/download/
Safari	MacOS X	http://www.apple.com/safari/
Chrome	Windows, MacOS X e Linux	http://www.google.com/chrome/

Tabela 7.2
Opções de browser.

A internet está cada vez mais presente nas nossas vidas. Transações bancárias, compras em lojas virtuais, busca de informações em mecanismos de busca, telefonia e conversas através de mensagens instantâneas são apenas alguns exemplos de utilização da rede. As formas de acesso também evoluíram. Hoje, é comum o acesso doméstico a pelo menos 1 megabit por segundo, velocidade que há alguns anos era exclusividade de provedores de acesso. Com toda essa evolução, os perigos também aumentaram.

O usuário necessita tomar alguns cuidados ao acessar a internet. Problemas como fraudes, páginas falsas, vírus, worms, spam e "escutas" clandestinas estão presentes a todo momento. O ISC do Sans afirma que são necessários menos de 10 minutos para que uma máquina desprotegida na internet sofra algum problema de segurança (fonte: http://isc.sans.org/survivaltime.html).

Qual navegador é mais seguro?

O resultado dos testes pode ser verificado em "Is Your Browser Putting You At Risk? Part 1 - General Malware Blocking" e em NSS Labs Research Library.

Em maio de 2013, a empresa NSS Labs (http://nsslabs.com/) efetuou teste nos cinco navegadores mais utilizados e mais conhecidos do mercado.

Vale ressaltar que existem diversos tipos de golpes e ações maliciosas que independem do navegador utilizado. Sendo assim, as melhores dicas são: 1) manter softwares (incluindo sistema operacional) sempre atualizados; 2) prestar atenção nas ações tomadas durante a navegação.

Recursos de um navegador

- Uso preferencial de criptografia (SSL/TLS), site iniciando com https://...
- Verificação do cadeado fechado indica acesso a endereço seguro.
- Clicando no cadeado, veremos a robustez da criptografia usada.



Figura 7.6
Acesso seguro https, cadeado fechado.

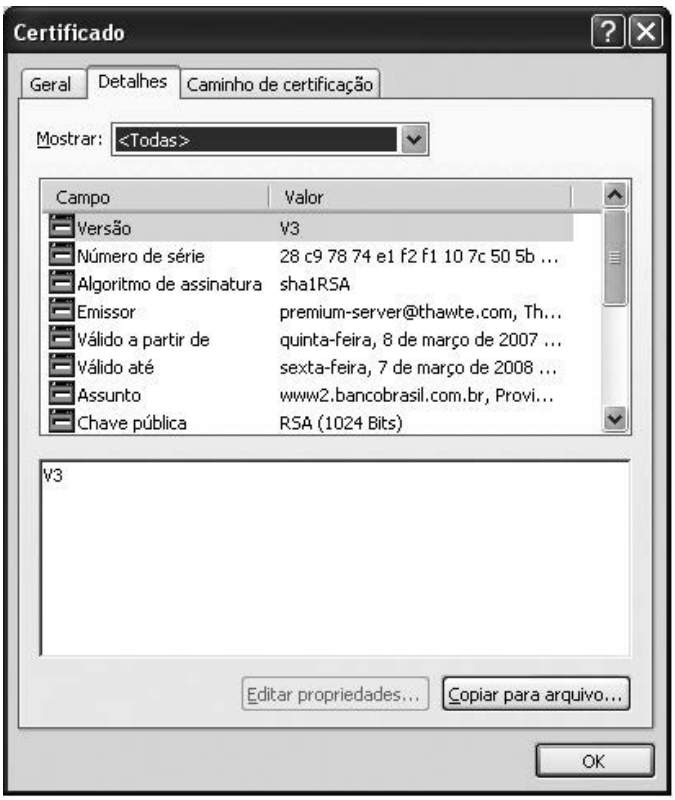


Figura 7.7
Clicando no cadeado: certificado digital do servidor.

Os navegadores mais novos fazem uma verificação de segurança ao acessar um site. Se por exemplo o site estiver com um certificado inválido, desatualizado ou mesmo autoassinado, o navegador exibe uma mensagem de alerta para o usuário informando o problema.

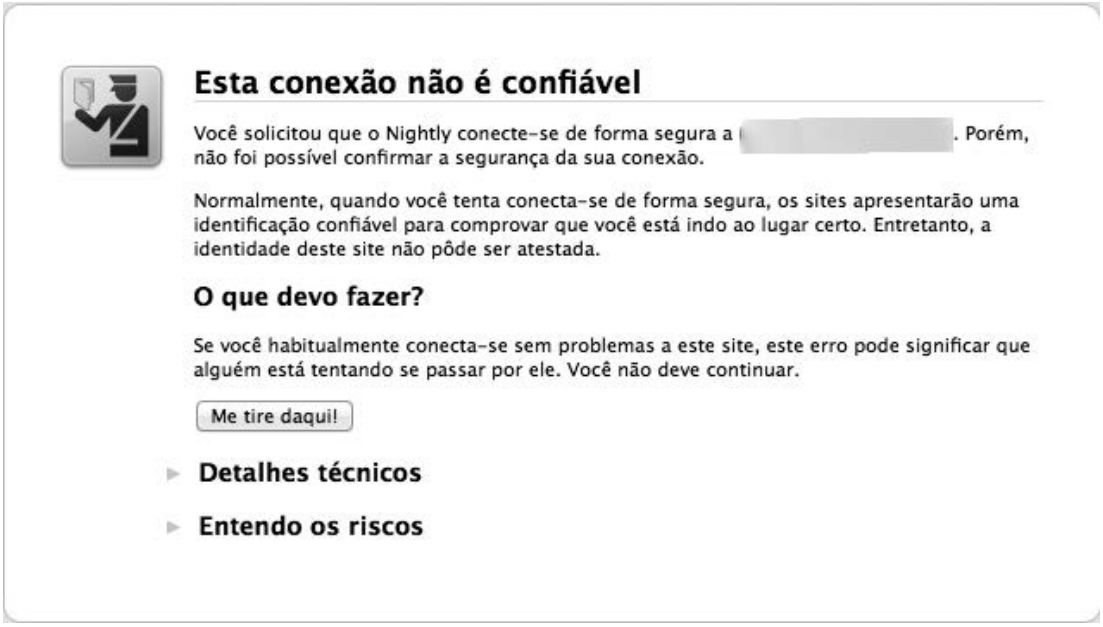


Figura 7.8 Mensagem de alerta para o usuário.

Tipos de certificados

Na ICP-Brasil estão previstos 8 tipos de certificados, divididos em duas séries:

- **Série A (A1, A2, A3 e A4)**: reúne certificados de assinatura digital, utilizados para confirmação de identidades na internet, principalmente em documentos eletrônicos com verificação de integridade de suas informações.
- **Série S (S1, S2, S3 e S4)**: reúne os certificados para sigilo, utilizados na codificação de documentos de bases de dados, de mensagens e de outras informações eletrônicas sigilosas. Os tipos são diferenciados pelo uso, nível de segurança e pela validade.

Teste seu certificado em: http://www.certisign.com.br

Nos certificados do tipo A1 e S1, as chaves privadas ficam armazenadas no próprio computador do usuário. Nos outros tipos, as chaves privadas e as informações referentes ao seu certificado ficam armazenadas em um hardware criptográfico, que pode ser um cartão inteligente (smart card) ou cartão de memória (token USB ou pen drive). Para acessar essas informações, o usuário necessita de uma senha pessoal determinada no momento da compra.

Tabela 7.3 Tipos de certificados (Fonte: ICP-Brasil).

Tipo	Tamanho (Bits)	Meio	Mídia de Armazenamento	Validade Máxima
A1 e S1	1024	Software	Arquivo	1
A2 e S2	1024	Software	Smart card ou token, sem capacidade de geração de chave	2
A3 e S3	1024	Hardware	Smart card ou token, sem capacidade de geração de chave	3
A4 e S4	2048	Hardware	Smart card ou token, sem capacidade de geração de chave	3

Cookies

- Que CD você comprou? Qual é seu tipo musical preferido?
- Pequenas quantidades de informações armazenadas pelo browser; último acesso a um site, dados do usuário etc.

- Servidor grava suas preferências no disco local em arquivo texto “cookie file”.
- Um ano de cookies pode revelar algo sobre sua personalidade?
- Servidor A pode livremente acessar cookie gravado pelo servidor B.
- Pode causar vazamento de informações.
- Conteúdo de um cookie:

```
cVisita
ataVisita=1%2F12%2F2004
www.centraldocarnaval.com.br/
1536
2938927104
29777976
2791820000
29677500
*
```

- Prevenção: política de segurança deve incluir limpeza periódica de cookies.

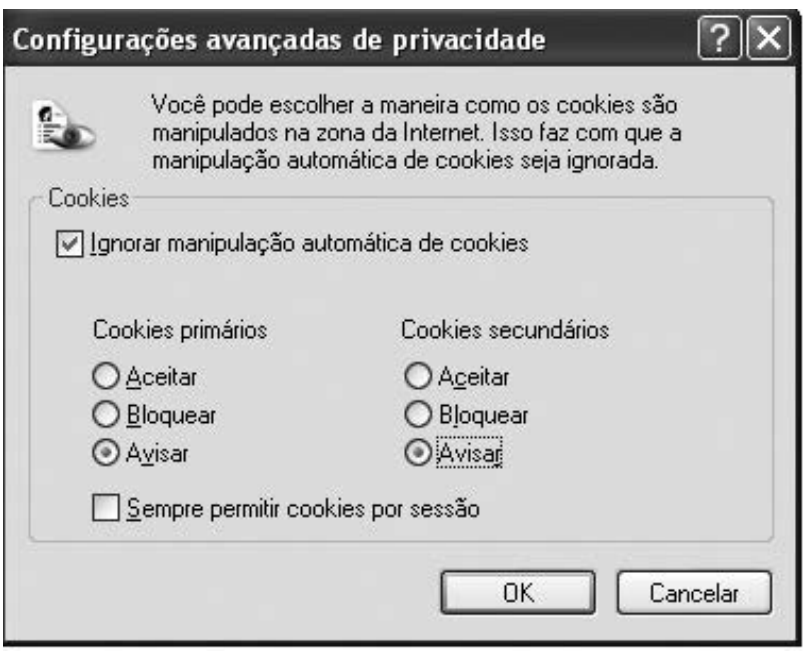


Figura 7.9
Configurando cookie.

Exercício de fixação 2
Cookies

Por que os cookies devem ser controlados?

Para mais informações sobre cookies: http://www.cookiecentral.com/faq/

Segurança no navegador

Aumente a segurança do navegador:

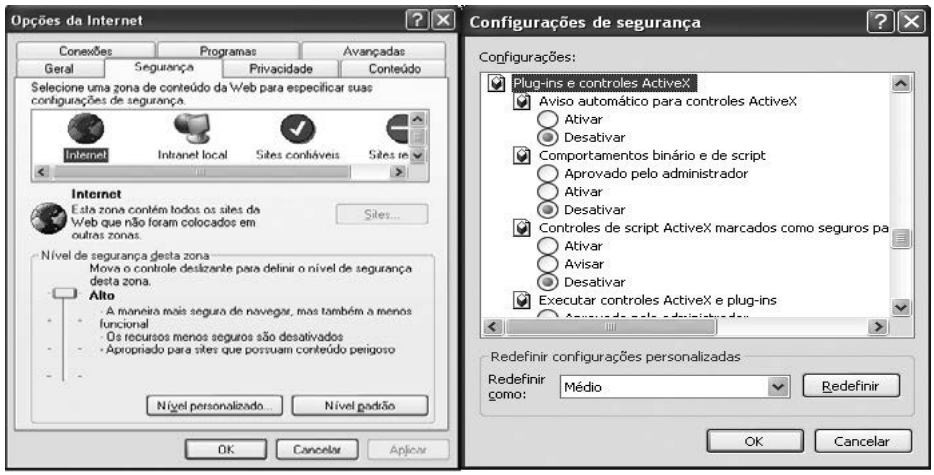


Figura 7.10
Aumentando a segurança no navegador.

A política de segurança deve incluir:

- Prevenção contra vazamento de informações, através de limpeza periódica do cache do browser (Windows guarda mais de 1Gbyte) e do histórico de navegação.
- Aumento do nível de segurança da zona internet para “alto”.
- Desativação dos controles e plugins Active-X.

Pagamentos na internet

É preciso ter maior receio em usar comércio eletrônico.

- Risco de fornecer número de cartão de crédito para o site.

Dicas para comprar na internet de forma segura:

- Evite comprar em loja desconhecida; escolha loja conhecida.
- Ao digitar o cartão, observe se o cadeado está fechado.
- Na dúvida, peça à loja para pagar através de boleto bancário.
- Verifique sua fatura de cartão de crédito para identificar possíveis compras estranhas.
- Verifique se a loja possui a opção de não manter número de cartão de crédito armazenado.
- Jamais autorize a loja a guardar o número de seu cartão.

Roteiro de Atividades 7

Atividade 7.1 – Recurso do SSH

1. Instale o pacote PuTTY em “PuTTY Download Page”.
2. Ative um sniffer na sua máquina com Wireshark;
3. Acesse sua conta shell no servidor SSH usando autenticação com senha.
   O sniffer capturou sua senha?

---

4. Crie seu par de chaves;
5. Use sua chave privada para se autenticar no servidor via SSH;
6. Abra uma sessão no servidor Linux via SSH, e torne-se super usuário (usuário root) sem digitar senha (use “ssh-copy-id”);
7. Crie um túnel utilizando SSH.

Atividade 7.2 – Uso de criptografia em arquivos

1. Instale o pacote cliente FileZilla: http://filezilla.sourceforge.net/;

- Ative um sniffer;
- Abra uma sessão de FTP com um cliente FileZilla (FTP via TLS).

Você conseguiu capturar a senha de autenticação?

---

2. Instale o pacote KeePass: http://portableapps.com/apps/utilities/keepass_portable

- Crie suas senhas e manipule-as.

Atividade 7.3 – Criptografando arquivos no Linux

1. Instale o programa ccrypt:

```
# apt-get install ccrypt
```

2. Crie um arquivo e insira alguns dados nele:

```
# nano teste.txt
```

3. Criptografando o arquivo:

```
# ccrypt teste.txt
```

Enter encryption key:

Enter encryption key: (repeat)

4. Tente listar o arquivo com o comando:

```
# cat teste.txt
```

5. Decriptando o arquivo:

```
ccrypt -d teste.txt
```

8

Política de segurança da informação

objetivos

Apresentar fundamentos, utilidade, importância e tópicos principais para a construção de uma política de segurança, e também metodologias para uma análise de risco.

conceitos

Política de segurança, auditoria em Microsoft Windows, cálculo de mau uso da web e políticas de uso aceitável (AUP).

Introdução

Definição de política de segurança segundo o RFC 2196 (The Site Security Handbook):

- Conjunto formal de regras às quais pessoas que obtêm acesso à tecnologia e aos ativos de informação devem estar sujeitas.

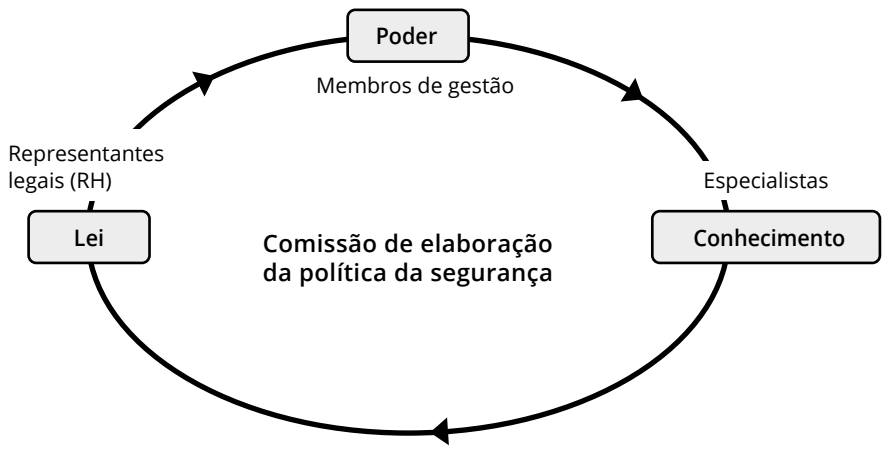


Figura 8.1 Comissão de elaboração da política de segurança.

Política de segurança é o elemento mais importante no projeto de segurança institucional de uma organização. Através dela são definidos os papéis de cada membro da organização no que tange à informação, além da listagem de direitos, deveres e punições aplicadas ao não cumprimento da política. Antes de definir uma política, é importante realizar uma análise de risco, que consiste em classificar os ativos de informação de acordo com sua importância. Construir uma política de segurança é uma atividade que envolve experiência; porém, esse processo pode ser visto em linhas gerais através de exemplos e recomendações.

Infelizmente, não existe uma regra geral para a criação de uma política de segurança. Cada organização tem particularidades que devem ser levadas em consideração. Este capítulo tem por objetivo fornecer conhecimento básico para a elaboração de uma política de segurança, além de alguns direcionamentos sobre os itens que merecem receber maior atenção. A elaboração de políticas de segurança é um processo que engloba a experiência dos profissionais envolvidos e o nível de comprometimento da organização na elaboração de uma política desse tipo.

Quais são as dificuldades de se implantar uma política de segurança? Quem deve participar da elaboração da política de segurança?

Exercício de nivelamento 1
Políticas de segurança da informação

A sua organização possui políticas de segurança da informação? Quais?

Análise de risco



Risco:

- Perigo ou possibilidade de perigo. Situação de probabilidade previsível de perda ou ganho; por exemplo, um jogo de azar ou uma decisão de investimento.
- Nem sempre associado à perda.

Segurança implica na probabilidade de risco tendendo a zero. Necessário administrar situações de risco.

A segurança da informação adota controles físicos, tecnológicos e humanos personalizados, viabilizando redução e administração dos riscos.

É o primeiro passo para a criação de uma política de segurança. Inclui as seguintes medidas:

- Definir escopo de abrangência da política;
- Identificar e classificar todos os ativos de informação importantes;
- Definir valores de importância para cada ativo;
- Determinar probabilidades de ocorrência de vulnerabilidades;
- Calcular impacto potencial dessas vulnerabilidades.

Identificação, classificação, valoração e criticidade

Identificação de todos os ativos de informação importantes:

Ativo	Descrição
Hardware	Estações, computadores pessoais, impressoras, roteadores, switches, modems, servidores de terminal e firewalls.
Software	Código-fonte, programas executáveis, utilitários, programas de diagnóstico, Sistemas Operacionais e programas de comunicação.

Ativo	Descrição
Dados	Dados armazenados online e dados arquivados, backups, logs de auditoria, bancos de dados e dados em trânsito em meios de comunicação.
Pessoas	Usuários, administradores e operadores.
Documentação	Manuais de programas, hardware interno, sistemas e procedimentos locais de administração.

Tabela 8.1 Identificação dos ativos.

Os dados de uma organização podem assumir diversas formas, dependendo da experiência de cada um na determinação da classificação daquela informação. Para uma universidade, por exemplo, talvez dados de pesquisa não sejam altamente confidenciais, mas para uma instituição que esteja prestes a lançar um produto revolucionário essa informação pode ser essencial para a sobrevivência do negócio. Além da criticidade, outros tipos de classificação podem ser atribuídos aos dados da organização.

Classificações

- Dados administrativos;
- Dados financeiros;
- Dados de clientes;
- Dados de pesquisa;
- Dados proprietários.

Valoração para cada ativo

- Alguns ativos possuem valores subjetivos;
- Alguns ativos não têm valor mensurável em termos monetários;
- O uso de uma escala simples facilita a valoração:
  - Valor alto.
  - Valor moderado.
  - Valor baixo.

Nível de criticidade:

- Nível de importância dentro da instituição.
- Alta.
- Média.
- Baixa.

Tabela 8.2 Exemplo de valoração e criticidade de um ativo.

Ativo	Classificação	Valoração	Criticidade
Correio eletrônico interno	Administrativo	Moderado	Média
Salário de empregados	Financeiro	Alto	Média
Tendências de mercado	Pesquisa	Baixo	Baixa
Patentes pendentes	Proprietário	Alto	Alta
Balanço anual	Financeiro	Moderado	Alta

Vulnerabilidades e ameaças

Vulnerabilidade:

- Evidência ou fragilidade que eleva o grau de exposição do ativo, aumentando a probabilidade de sucesso da investida de uma ameaça.
- É preciso conhecer as vulnerabilidades de cada ativo.

Vulnerabilidades		
Físicas	**Tecnológicas**	**Humanas**
Cabeamento de baixa qualidade.	Defeito de software.	Falta de conscientização dos usuários.
Ausência de fragmentadora de papel.	Sistema Operacional desatualizado.	Ausência de rotinas de backup.
Instalação elétrica mal dimensionada.	Senha fraca.	Descuido e despreparo.

Tabela 8.3
Exemplo de vulnerabilidades.

Ameaça:

- Atitude ou dispositivo com potencial para explorar uma vulnerabilidade e causar danos à segurança da informação, atingindo ao menos um de seus atributos: confidencialidade, integridade ou disponibilidade.
- É preciso conhecer a probabilidade de uma ameaça de explorar uma vulnerabilidade e causar alguma falha.

Ameaças		
Físicas	**Tecnológicas**	**Humanas**
Curto-circuito	Spam	Erro humano
Raio	Phishing	Engenharia social
Inundação	DDoS	Curiosidade

Tabela 8.4
Exemplo de ameaças.

Risco

- Para todas as ameaças possíveis, devemos fazer uma avaliação de risco.
- Há muitas formas de se medir o risco.
- Pessoas que tomam decisões de como se proteger contra riscos devem ter a noção exata da quantificação e da probabilidade de perda da informação.
- Há ferramentas automatizadas capazes de quantificar e representar de forma adequada os riscos e prejuízos.

De acordo com a norma NBR ISO/IEC 27001, a análise de risco é uma consideração sistemática:

- Do impacto nos negócios como resultado de uma falha de segurança, levando-se em conta as potenciais consequências da perda de confidencialidade, integridade ou disponibilidade da informação ou de outros ativos.
- Da probabilidade de tal falha realmente ocorrer à luz das ameaças e vulnerabilidades mais frequentes e nos controles atualmente implementados.

Forma genérica para avaliação de risco:

- **Risco** = valor x criticidade x vulnerabilidade x ameaça.
- **Valor**: qual o valor do ativo?
- **Criticidade**: o quão crítico é o ativo?
- **Vulnerabilidade**: o quão vulnerável se encontra o ativo?
- **Ameaça**: qual a probabilidade de uma ocorrência causar falha de segurança?

Impacto

- Um dos objetivos da análise de risco é o cálculo do impacto causado por determinada ameaça ou vulnerabilidade levantada previamente.
- Pode-se classificar o impacto em:
  - **Aceitável**: não será criado nenhum plano de contenção para diminuir a probabilidade de ocorrência do impacto, tampouco um plano de contingência.
  - **Aceitável com reação**: poderá ser criado apenas um plano de contingência caso ocorra o evento.
  - **Terceirizar**: transferir os riscos e suas consequências para terceiros.
    - Essa ação não visa diminuir ou eliminar a possibilidade de ocorrência do evento.
    - O terceiro deverá elaborar os planos de contenção e contingência para o evento.
  - **Mitigar**: reduzir a probabilidade de ocorrência e/ou impacto do risco através de medidas proativas como, por exemplo, a criação de um plano de contenção do risco em si, que se desdobrará em medidas de segurança antes que o evento ocorra.

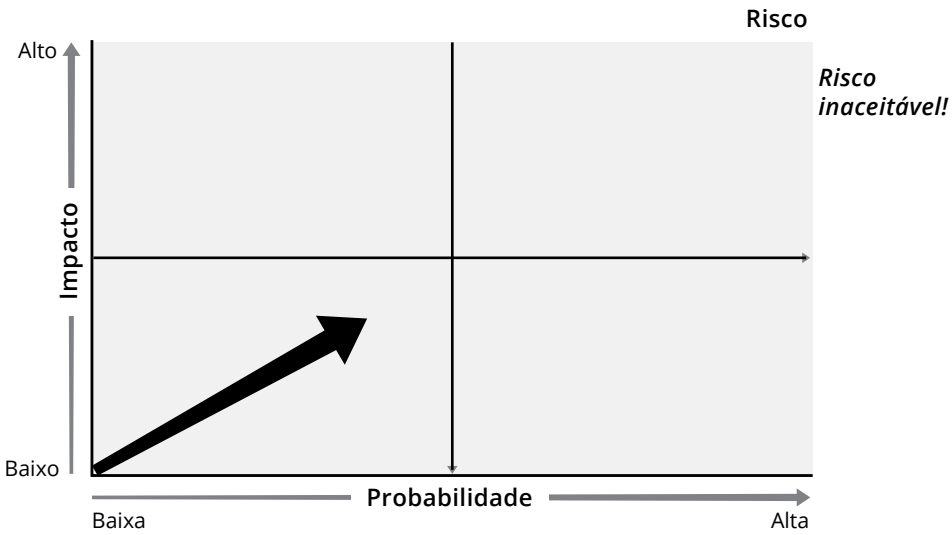


Figura 8.2
Impacto.

Exercício de fixação 1
Risco, ameaças e vulnerabilidades

O que são ameaças?

O que são vulnerabilidades?

O que é risco?

Saiba mais

A Escola Superior de Redes oferece o curso *Gestão de riscos de TI – NBR 27005*, que detalha o uso da norma: http://esr.rnp.br/gti9

Metodologias para análise de risco

Algumas das metodologias disponíveis atualmente:

- Cobra: http://www.riskworld.net
- Octave: http://www.cert.org/octave/omig.html
- Sprint: http://www.securityforum.org/

Apesar de o funcionamento geral e a importância de uma análise de risco serem de fácil entendimento, as informações obtidas não nos tornam capazes de fazer uma análise desse tipo de forma profissional e consistente. Sendo assim, foram criadas metodologias padronizadas e bem definidas para facilitar esse processo para os consultores de segurança.

Construindo uma política de segurança

- Quais os principais fatores para o sucesso de uma política de segurança?
- Fator mais importante para o sucesso da política.
  - Envolvimento de cada segmento da instituição na construção da política: pessoal técnico especializado, gerentes, diretores e usuários.
- Recomendações básicas para a política.
  - Deve ser integrada com outras políticas da empresa.
  - Deve ser validada pelo pessoal de suporte de redes e pessoas da gerência.
  - Dever ser reforçada por equipamentos, softwares e procedimentos de segurança.

Uma vez identificados os riscos para a instituição, o passo seguinte consiste em criar um documento que sirva de apoio e guia para a segurança da informação. Esse documento é chamado de política de segurança. Não existe uma regra geral para a criação de uma política de segurança. Ela depende da experiência e do conhecimento do pessoal envolvido na tarefa.

Há necessidade do uso de uma política de segurança?

Orientações da norma ISO 27001

Definição de segurança da informação.

- Resumo das metas e do escopo importância da segurança como um mecanismo que possibilita o compartilhamento da informação.

Declaração do comprometimento da alta direção, apoiando as metas e princípios da segurança da informação.

Breve explanação das políticas, princípios, padrões e requisitos de conformidade de importância específica para a instituição:

- Conformidade com a legislação e cláusulas contratuais;
- Requisitos na educação de segurança;
- Prevenção e detecção de vírus e softwares maliciosos;
- Gestão da continuidade do negócio;
- Consequências das violações na política de segurança da informação.



- Definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança.
- Referências à documentação que possa apoiar a política.
  - Políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos.
  - Regras de segurança que devem ser seguidas pelos usuários.

Norma ISO 27002



A Norma ISO 27002 (antiga NBR ISO/IEC 17799:2005).

- Considerada um código de boas práticas.
- Recomendações.
- Item 5 – Política de segurança da informação.
- Dicas e orientações sobre o que é, o que deve conter e diretivas para implementação.



Saiba mais

A Escola Superior de Redes oferece o curso *Gestão da Segurança da Informação – NBR 27001 e NBR 2700*, que detalha as normas ISO 27001 e 27002: http://esr.rnp.br/gti8

A ISO 27002, antiga ISO 17799, especifica em seus controles, mas especificamente no Capítulo 5, Políticas de Segurança da Informação.

Nesse documento podemos encontrar dicas e orientações sobre o que é, o que deve conter e diretivas para a implementação de uma política de segurança da informação.

Orientações do NBSO



O NIC BR Security Office (NBSO) lista alguns itens que devem ser cobertos pela política:

- Aspectos preliminares.
- Políticas de senhas.
- Direitos e responsabilidades dos usuários.
- Direitos e responsabilidades do provedor de recursos.
- Ações previstas em caso de violação da política.

Lista dos itens cobertos pela política (NBSO)

1. Aspectos preliminares:

- Abrangência e escopo de atuação da política;
- Definições fundamentais;
- Normas e regulamentos aos quais a política está subordinada;
- Pessoas autorizadas a sancionar, implementar e fiscalizar o cumprimento da política;
- Meios de distribuição da política;

- Modo e frequência de revisão da política.

2. Política de senhas:

- Requisitos para formação de senhas;
- Período de validade das senhas;
- Normas para proteção de senhas;
- Reutilização de senhas;
- Senhas padrão.

3. Direitos e responsabilidades dos usuários:

- Utilização de contas de acesso;
- Utilização de software e informações, incluindo questões de instalação, licenciamento e copyright;
- Proteção e uso de informações, como senhas, dados de configuração de sistemas e dados confidenciais;
- Uso aceitável de recursos como e-mail, news e páginas web;
- Direito à privacidade, e condições nas quais esse direito possa ser violado pelo provedor dos recursos;
- Uso de antivírus.

4. Direitos e responsabilidades do provedor dos recursos:

- Backup;
- Diretrizes para configuração e instalação de sistemas e equipamentos de rede;
- Autoridade para conceder e revogar autorizações de acesso, conectar e desconectar sistemas e equipamentos de rede, alocar e registrar endereços e nomes de sistemas e equipamentos;
- Monitoramento de sistemas e equipamentos de rede;
- Normas de segurança física.

5. Ações previstas em caso de violação da política:

- Diretrizes para tratamento e resposta a incidentes de segurança;
- Penalidades cabíveis.

Orientações do CERT.BR



O CERT.BR define ainda alguns fatores importantes para o sucesso de uma política:

- Apoio por parte da administração superior.
- A política deve ser ampla, cobrindo todos os aspectos que envolvem a segurança dos recursos computacionais e da informação sob responsabilidade da organização.
- A política deve ser periodicamente atualizada de forma a refletir as mudanças na organização.
- Deve haver um indivíduo ou grupo responsável por verificar se a política está sendo respeitada.

Todos os usuários da organização devem tomar conhecimento da política e manifestar a sua concordância em se submeter a ela antes de obterem acesso aos recursos computacionais.

A política deve estar disponível em um local de fácil acesso aos usuários, tal como a intranet da organização.

Acceptable Use Police (AUP)

- Política de Uso Aceitável (PUA): subconjunto da política de segurança.
  - Define como os recursos computacionais podem ser utilizados.
  - Define os direitos e responsabilidades dos usuários.
- Provedor de acesso deixa sua política de uso aceitável disponível em sua página.
- Instituição entrega AUP no momento da contratação do funcionário.
- AUPs mais comuns:
  - Acesso correto com segurança à internet.
  - Uso correto e seguro do serviço de correio eletrônico.
  - Uso correto e seguro do computador.

Exemplo de política de segurança

Exemplos de políticas de uso aceitável:

- http://www.allnet.com.br/aup/
- http://www.earthlink.net/about/policies/use.faces
- http://www.tutopia.com/access/brasil/pua.asp

Exemplo completo da política de segurança da ICP-Brasil, aprovada pela Resolução nº 2, de 25 de setembro de 2001, do Comitê Gestor da ICP-Brasil:

- http://siabi.trt4.jus.br/biblioteca/direito/legislacao/atos/federais/res_pres_cc_2001_2.pdf

Saiba mais

Exemplos de políticas de diversos tipos: http://www.sans.org/security-resources/policies/

Mensurando

- As métricas de controle de risco podem ser aplicadas não somente a situações de ameaça aos ativos da empresa, mas também ao mau uso desses ativos.
- Imagine um cenário onde 50 funcionários de uma empresa com total acesso à web perdem em média uma hora por dia com acesso de conteúdo não relacionado à sua atividade profissional e ao negócio da empresa.
- Como podemos justificar o valor da implementação de um controle de conteúdo web?

Existem algumas siglas e equações que nos ajudam e efetuar esses cálculos.

Exposure Factor (EF):

- Fator de exposição.
- Valor percentual de exposição frente a uma ameaça.

O fator de exposição representa a porcentagem de perda que uma ameaça pode causar a um ativo. Por exemplo:

Um acidente automobilístico pode ser somente um amassado na lataria, custando 5% do valor do automóvel para o conserto, ou 100% do valor nos casos de perda total.

O roubo do carro significa 100% de perda.

Single Loss Expectancy (SLE)



- Expectativa de Perda Pontual.
- SLE = valor do bem X Fator de Exposição (EF).

Expectativa de Perda Pontual (SLE) é o valor do bem multiplicado pelo fator de exposição (valendo para uma única ocorrência).

Annualized Rate of Ocurrance (ARO)



- Proporção Anual de Ocorrência.
- Valor percentual representado a frequência de uma ocorrência (anual).

Proporção Anual de Ocorrência (ARO) é o valor percentual representando a frequência de uma ocorrência, durante um ano. O valor pode variar de:

- 0.0: nunca;
- 1.0: pelo menos uma vez ao ano;
- Maior que 1.0: várias vezes ao ano.

Onde:

- 0.1: uma vez a cada 10 anos.
- 4.0: quatro vezes ao ano.

Annualized Loss Expectancy (ALE)



- Expectativa de Perda Anual.
- ALE = SLE X ARO.

Expectativa de Perda Anual (ALE) é a expectativa de perda pontual (SLE) multiplicada por quantas vezes isso pode ocorrer em um ano (ARO).

Calculando



- Um funcionário:
  - R$ 10,00 (custo/hora) x 8 (horas/dia) x 240 (dias/ano).
    - Funcionário custa por ano R$ 19.200,00.
  - Uma hora por dia corresponde a 12,5% em um período de 8 horas.
    - Isso corresponde a 12,5% de desperdício.
  - R$ 10,00 (custo/hora) x 1 (hora/dia) x 240 (dias/ano).
    - Valor do desperdício por ano: R$ 2.400,00.
- Expectativa de Perda Pontual (SLE):
  - SLE = Valor Anual do Funcionário X porcentagem de desperdício (exposição).
  - Valor Anual do Funcionário = R$ 19.200,00.
  - Fator de Exposição (EF) = 12,5%.
  - SLE = R$ 19.200,00 x 12,5 %.
  - SLE = R$ 2.400,00.

- Proporção Anual de Ocorrência (ARO):
  - Como sabemos que a situação realmente ocorre, temos um valor de ARO = 1.0
- Expectativa de Perda Anual (ALE):
  - ALE = SLE x ARO
  - ALE = R$ 2.400,00 X 1.0
  - ALE = R$ 2.400,00
- Temos, assim, R$ 2.400,00 de perda (prejuízo) anual por funcionário.

Ainda neste cenário, imagine essa empresa com 50 funcionários, onde 100% possuem acesso à web, totalizando em média 5 horas semanais de uso indevido não relacionado ao negócio. Com essas informações, conseguimos agora mostrar o valor do prejuízo acumulado durante um ano.



- 50 funcionários custando R$ 19.200,00 cada anualmente.
  - 50 (funcionários) x R$ 19.200,00 (valor anual/funcionário) = R$ 960.000,00.
- Expectativa de Perda Anual (ALE) por funcionário = R$ 2.400,00.
  - 50 (funcionários) x R$ 2.400,00 (valor prejuízo/funcionário) = R$ 120.000,00.

Valor final



- Custo Fixo Anual com 50 funcionários: R$ 960.000,00.
- Prejuízo Anual (desperdício de tempo/navegação indevida): R$ 120.000,00.
- Valor efetivo (útil): R$ 840.000,00.
- Mostrar o total em valores de horas perdidas. Prejuízo é um argumento bem convincente para demonstrar um risco e possivelmente conseguir investimentos na área (filtro de conteúdo, por exemplo).

Esse tipo de cálculo pode ser aplicado em várias situações como, por exemplo, para mensurar o valor vinculado à indisponibilidade de determinado serviço, o tempo perdido com spams e a indisponibilidade das estações de trabalho por falta de um sistema de antivírus eficiente.

Roteiro de Atividades 8

Atividade 8.1 – Elaboração de políticas

1. Esboce uma Política de Uso Aceitável (AUP) para os seguintes assuntos:
   - Uso correto com segurança da estação de trabalho;
   - Uso correto com segurança do serviço de correio eletrônico;
   - Uso correto com segurança do serviço de "www".
2. Que tipo de punição você acha que deve ser aplicada em casos de violação da política de segurança?

Veja algumas sanções passíveis a servidores públicos no "Quadro da Legislação relacionada à Segurança da Informação": http://www.presidencia.gov.br/gsi/cgsi/quadro_legislacao.htm

3. Discuta sua opinião com o instrutor e os colegas.

Atividade 8.2 – Auditoria em Microsoft Windows

1. Instale o pacote de auditoria da Microsoft MBSA:

   http://www.microsoft.com/technet/security/tools/mbsahome.mspx

   http://technet.microsoft.com/en-us/security/cc184923

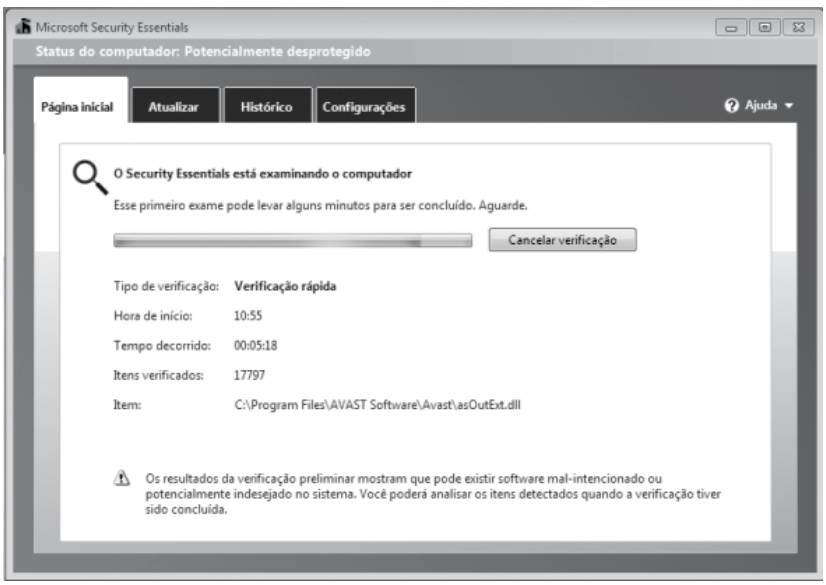
2. Execute-o na sua estação de trabalho e na sua rede local. Que benefícios este programa pode fornecer para a segurança da informação?

Atividade 8.3 – Aumentando a segurança da sua estação de trabalho

1. Instale o pacote Microsoft Security Essentials:
   http://windows.microsoft.com/pt-br/windows/security-essentials-download

2. Faça uma varredura na sua estação de trabalho.





- Você constatou algum problema de segurança? Qual?

Atividade 8.4 – Calculando o impacto do mau uso da web

1. Calcule o prejuízo de uma empresa decorrente do mau uso do acesso à web, considerando o cenário:

A empresa Gato Molhado tem 500 funcionários, onde 70 deles têm acesso indiscriminado à web. Esses usuários gastam em média 1 hora por dia, ao custo de R$ 20,00 a hora, com acesso a conteúdo não relacionado às suas atividades e ao negócio da empresa (utilize as métricas ALE e SLE).

9

Ameaças recentes

objetivos

Apresentar os mais recentes e perigosos mecanismos de fraudes on-line; explicar o uso seguro do correio eletrônico e de navegadores, e a importância da aplicação de uma política de segurança rigorosa para downloads; mostrar as vulnerabilidades exploradas pelos fraudadores em golpes virtuais; ensinar os cuidados para realizar uma operação financeira segura via internet e formas de se manter informado.

conceitos

Malware, Antirootkit, Phishing, Pharming, Bot, Rootkit.

Exercício de nivelamento 1
Ameaças recentes

Quais as maiores ameaças para a sua organização atualmente?

Introdução

Fraude on-line:

- Visa sequestro de dados bancários e informações úteis ao malfeitor.
- Aborda em larga escala usuários via e-mail.
- Usa assunto atrativo como disfarce.
- Induz a vítima a fornecer dados sigilosos.
- Instala programa que rouba informações no computador.

Entre as mensagens indesejadas e não solicitadas de correio eletrônico (spam) que circulam atualmente na internet, as fraudes on-line (scam) já chegaram a ultrapassar a ocorrência de anúncios, propagandas e pornografia, segundo dados da unidade de monitoramento Brightmail, da Symantec, empresa especializada em segurança digital.

Prevenir é muito mais simples e eficaz do que remediar. Informação é sempre um meio válido de combater este tipo de mal, para que cada vez menos pessoas sejam enganadas pelas fraudes.

Serão apresentados e explicados diversos exemplos de fraude, na forma de imagens reproduzindo a visualização de mensagens de fraude que circulam por correio eletrônico.

Scam (golpe virtual)

Ação eletrônica fraudulenta que tem como finalidade obter vantagem, geralmente financeira.

Fatores de ocorrência e proliferação:

- Facilidade do e-mail de ser forjado e fraudado;
- Proliferação de listas e programas para envio de spam em larga escala;
- Facilidade de publicar qualquer conteúdo e arquivo executável na web;
- Carência de legislação, meio de controle e segurança que permita rastrear, identificar, coibir e punir ação criminosa de forma rápida, eficaz e globalizada;
- Usuário com pouco conhecimento técnico, ingênuo e despreparado para desconfiar de perigo existente.

Phishing



- Link para programa malicioso.
- Página falsificada de comércio eletrônico ou internet banking.
- E-mail contendo formulário.
- Uso de computador alheio.

Cuidados ao usar comércio eletrônico ou internet banking.

Proteção antiphishing.

Phishingscam:

- Tipo de fraude eletrônica.
- Termo veio de fishing (pescaria), analogia criada onde "iscas" são usadas para "pescar".

Não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial. Os invasores têm concentrado seus esforços na exploração de fragilidades dos usuários para realizar fraudes comerciais e bancárias através da internet.

Para obter vantagens, os fraudadores têm utilizado amplamente e-mails com discursos que, na maioria dos casos, envolvem engenharia social e tentam persuadir o usuário a fornecer seus dados pessoais e financeiros. Em muitos casos, o usuário é induzido a instalar algum código malicioso ou acessar uma página fraudulenta, para que dados pessoais e sensíveis, como senhas bancárias e números de cartões de crédito possam ser furtados.



Dessa forma, é muito importante que usuários da internet tenham certos cuidados com os e-mails que recebem e ao utilizarem serviços de comércio eletrônico ou internet banking.

Como pegar (o que seria a isca)?

- Envio de mensagem eletrônica não solicitada, falsamente oriunda de instituição conhecida, como banco, empresa ou site popular.
- Procura induzir acesso a páginas fraudulentas (falsificadas), projetadas para furtar os usuários.

O que pegar (o que seria o peixe)?

- Senhas;
- Dados financeiros;

- Número de cartão de crédito;
- Dados de contas.
- Informações pessoais.

Formas atuais de phishing

Quatro situações de phishing usadas por fraudadores:

- Mensagem contendo link para programa malicioso.
- Página falsificada de comércio eletrônico ou internet banking.
- E-mail contendo formulário para fornecimento de informação sensível.
- Uso de computador alheio.


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Figura 9.1
Exemplo de phishing.

Existem variantes para as situações apresentadas. Novas formas de phishing podem surgir. É importante manter-se informado sobre os novos tipos de phishing que vêm sendo utilizados pelos fraudadores, através dos veículos de comunicação, como jornais, revistas e sites especializados. Também é importante que, ao identificar um caso de fraude via internet, notifiquemos a instituição envolvida, para que ela possa tomar as providências cabíveis.

Vários veículos utilizados:

- Mensagem instantânea.
- Mensagem de texto de celular (SMS).
- Sala de chat.
- Anúncio falso tipo banner.
- Site falso de procura e oferta de emprego.
- Barra de ferramentas de navegador falsa.
- Recado no Orkut (scrap).

Exercício de fixação 1
Phishing

Explique como o phishing funciona.

Programa malicioso

Também chamado de malware, é qualquer programa que atue contra o usuário:

- Vírus.
- Worm.
- Cavalo de troia.

Programa malicioso ou malware (malicious software) é qualquer tipo de programa que faz alguma coisa contra o usuário. Assim, em vez de tentar categorizar um tipo de arquivo malicioso como vírus, worm, cavalo de troia etc., chamamos eles simplesmente de malware.

Link para programa malicioso

Entenda o processo:

- Um programa malicioso é criado e colocado na web.
- Spam é enviado.
- Usuário clica no link para o programa, faz o download e executa-o.

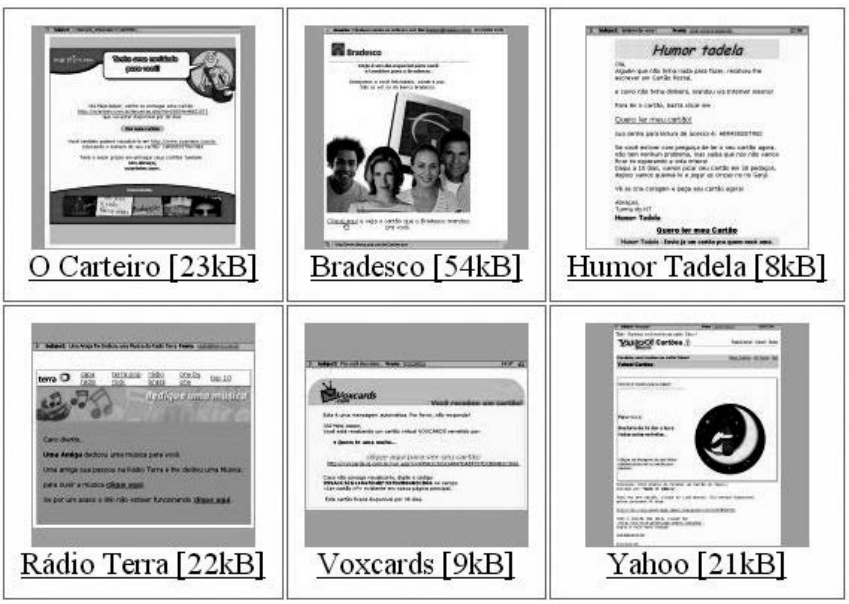


Figura 9.2
Mensagens com links maliciosos.

Malwares mais usados

- Spyware;
- Cavalo de troia.

Assuntos mais usados

- Cartões e mensagens;
- Notificações financeiras e cadastrais;
- Notícias bombásticas e apelos dramáticos;
- Download de programas;
- Prêmios, promoções e campanhas;
- Pornografia.

Como identificar uma mensagem maliciosa?



- Contém erros gramaticais e de ortografia.
- Compare link real na barra de status com link malicioso.
- Procure extensão de arquivo malicioso no link real:
  - Por exemplo: “.exe”, “.zip”, “.com”, “.dll”.
- Suspeite de mensagem que solicita instalação de arquivo ou programa.



Prevenção:

- Suspeite de mensagem que desperta curiosidade, ambição e impulso emocional.
- Não confie sempre no remetente da mensagem .
- Contate instituição para certificar-se sobre o assunto, antes de transmitir informação sensível.

Página falsificada de comércio eletrônico ou internet banking



Mensagem maliciosa:

- Solicita recadastramento ou confirmação dos dados do usuário.
- Solicita participação em nova promoção.
- Tenta persuadi-lo a clicar em link no texto, em imagem ou página de terceiro.

Página falsa solicita dados pessoais e financeiros:

- Número, data de expiração e código de segurança do seu cartão de crédito.
- Número da agência e conta bancária, senha do cartão e senha de acesso ao internet banking.
- Clicando no botão de confirmação, os dados são enviados para o fraudador.

Como identificar uma mensagem maliciosa?

- Site de comércio eletrônico/internet banking confiável sempre usa conexão segura.
- Se a página não usa conexão segura, desconfie imediatamente.
- Se a página falsificada usa conexão segura, abra e leia o certificado digital.
- Fraudador não consegue fraudar o certificado digital.

E-mail contendo formulário



Como identificar mensagem maliciosa?

- Nenhuma instituição bancária ou de comércio eletrônico usa mensagem eletrônica para solicitar informação sensível do cliente.



Figura 9.3
E-mail contendo formulário.

Abordagem mais direta:

- Tenta enganar usuário de modo a fazê-lo preencher um formulário com dados pessoais e bancários.
- Formulário é apresentado na própria mensagem de fraude ou a mensagem contém link que leva à página com o formulário.

Uso de computador alheio



- Uso de computador de outra pessoa para acessar site de comércio eletrônico ou internet banking.
  - Lan house.
  - Cybercafé.
  - Stand de evento.
- Risco:
  - Ação monitorada por programa instalado anteriormente.
- Prevenção:
  - Não usar computador alheio para operações que solicitem senha, dados pessoais ou financeiros.

Roubo de identidade



- Roubo de identidade (Identity Theft) é o ato pelo qual uma pessoa se passa por outra, atribuindo-se uma identidade falsa com o objetivo de obter vantagens indevidas.
- Quanto mais você disponibiliza informações pessoais na internet, mais fácil fica para um golpista furtar sua identidade, pois quanto mais dados ele possuir, mais convincente ele pode ser.
- Caso a sua identidade seja furtada, você poderá arcar com consequências como perdas financeiras, perda de reputação e falta de crédito.

Golpes em sites de comércio eletrônico e compras coletivas



- Sites de comercio eletrônico vêm sendo usados com bastante frequência em fraudes eletrônicas.
- Neste golpe, cria-se um site de e-commerce fraudulento com o objetivo de enganar potenciais clientes que, após efetuarem o pagamento, não recebem as mercadorias solicitadas.
- Esse golpe pode ser amplificado com a moda de sites de compras coletivas.

Cuidados ao usar comércio eletrônico e internet banking



- Realizar transações em sites de instituições confiáveis.
- Digitar no browser o endereço desejado.
- Não usar links em páginas de terceiros ou recebidos por e-mail.
- Antes de qualquer ação, ter certeza de que o endereço no navegador corresponde ao site desejado.
- Ter certeza de que o site usa conexão e tamanho de chave seguros.
- Ao aceitar o certificado digital, verificar dados e prazo de validade.
- Não acessar site de comércio eletrônico e/ou internet banking em computador alheio.
- Desligar webcam ao acessar site de comércio eletrônico e/ou internet banking.
- Manter browser sempre atualizado.
- Restringir execução de JavaScript, Java ou ActiveX.
- Bloquear pop-up Windows.
- Configurar leitor de e-mail para não abrir arquivo ou executar programa automaticamente.

Proteção antiphishing



- Navegadores adotam sistema antiphishing:
  - IE a partir da versão 7.0:
    - Analisa a página e gera alerta sobre site suspeito.
  - Firefox a partir da versão 2.0:
    - Bloqueia comparando com lista negra (blacklist).
  - Chrome:
    - Bloqueia comparando com lista negra (blacklist).
- Modo incorporado para denúncia de sites suspeitos:
  - Usuário envia informação para avaliação, que se confirmada é adicionada à lista negra.

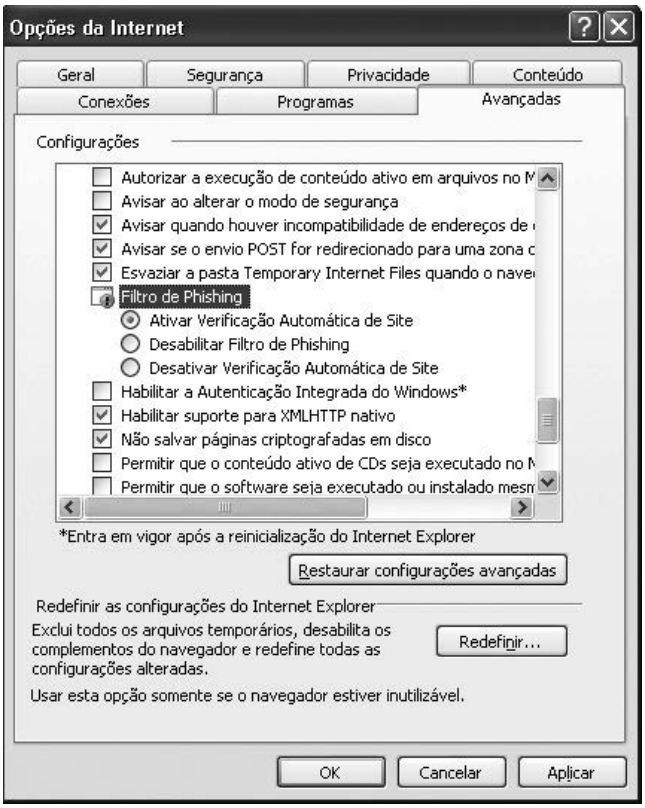


Figura 9.4
Sistema antiphishing no IE 7.

Pharming

- Subcultura de linguagem on-line em constante evolução.
- Variante de phishing, redireciona o browser para web site falso.
- Objetiva também roubar identidade digital e informação sensível.
- Mais traiçoeiro, funciona sem participação ou conhecimento do usuário.
- Modifica a relação entre o nome de um site e o endereço IP do servidor web.

Pharming usa as seguintes técnicas:

- **DNS poisoning**: envenenamento do cache de Domain Name System (DNS), ataque ao servidor de rede.
- **Hosts poisoning**: envenenamento do arquivo de hosts da pilha TCP/IP, ataque à estação de usuário.
- **Phone phreaking**: escuta ou uso incorreto na rede telefônica.
- **Phishing**: roubo de identidade na internet.
- **Pharming**: redirecionamento para web site falso.

Prevenção

- Habilitar no antivírus proteção contra ameaças desconhecidas, analisando comportamento de arquivo suspeito (análise heurística).

Novo ataque "Drive-By Pharming" (pharming casual).

- Permite que o invasor modifique a configuração do modem ADSL da vítima se uma página web maliciosa for aberta.

- Reconfigura servidores de DNS do modem ADSL.
- Usa técnica chamada de Cross Site Request Forgery (CSRF).
- Site malicioso instrui computador do usuário a acessar modem e modificar configuração.
- Nenhuma falha de segurança é explorada, apenas senha vulnerável.

- Prevenção: alterar senha padrão do modem ou roteador.
- Regra de ouro de segurança: altere o padrão, sempre que possível: **endereço IP**, porta, usuário, senha etc.

Endereço IP
Identificação de um dispositivo (computador, impressora etc) em uma rede local ou pública. Cada computador na internet possui um IP único, que é o meio que as máquinas usam para se comunicar na internet.

Exercício de fixação 2
Pharming

Quais as medidas preventivas devem ser adotadas contra ataques pharming?

Bot

Programa malicioso que se propaga automaticamente, explora vulnerabilidades e pode ser controlado remotamente.

Diminutivo de robot, utilitário concebido para simular ações humanas.

- Roda tarefa automatizada sobre a internet.
- Usa Mensageiro Instantâneo (MI) ou IRC para comunicação com master.
- Usado no ataque automatizado DDoS formando botnets.

- Anatomia de um bot: http://www.f-secure.com/v-descs/agobot_fo.shtml
- Botnet: rede de computadores (bots) usando software de computação distribuído; formada por milhões de bots.
- Symantec Internet Security Threat Report: nos primeiros seis meses de 2006, havia 4.696.903 computadores em botnets ativas.
- Symantec e Kasper Sky Labs Report (30/01/2007): classifica a botnet como o maior perigo da internet.

Rootkit

- Programa projetado para ocultar a si mesmo e outros programas, dados e atividades, incluindo vírus, backdoors, keylogger, spyware e bots.
- Coleção de ferramentas que habilita acesso ao nível de administrador (root).
- Roda de modo que processos do Sistema Operacional ou antivírus não podem detectá-lo.
- Realiza download de trojan, vírus; transmite informação confidencial, com os mesmos privilégios do Sistema Operacional hospedeiro.

O nome rootkit tem origem no mundo Unix PC/Linux, onde kit é uma coleção de ferramentas que fornece poderes de superusuário root ao invasor.

Tecnologia rootkit em DRM da Sony

Rootkit é instalado por CD da Sony BMG dificultando remoção do software DRM.

- Instalado como filtro de acesso ao CD-ROM.
- Esconde programa que proíbe "ripar" músicas do CD para o formato mp3.
- Removê-lo impede acesso ao drive de CD.

Digital Rights Management (DRM):

- Tecnologia que controla cópia de dados multimídia como músicas e vídeo.

Problemas de segurança:

- Programa é instalado sem conhecimento e autorização do usuário.
- Envia informações para a Sony sem conhecimento e autorização do usuário.
- Trojan Backdoor.IRC.Snyd.A usou rootkit da Sony.

Em 31/10/2005, Mark Russinovich anunciou a descoberta em seu blog. O clamor foi grande e a Sony suspendeu a proteção contra cópia ilegal. Leia o anúncio em: http://blogs.technet.com/markrussinovich/

Kernel malware

Kernel malware é outro nome para rootkit.

- Soluções atuais, incluindo antivírus e firewalls, não foram projetadas para proteção contra kernel malware.
- Está se popularizando e muitas ameaças têm alto interesse em rootkit.

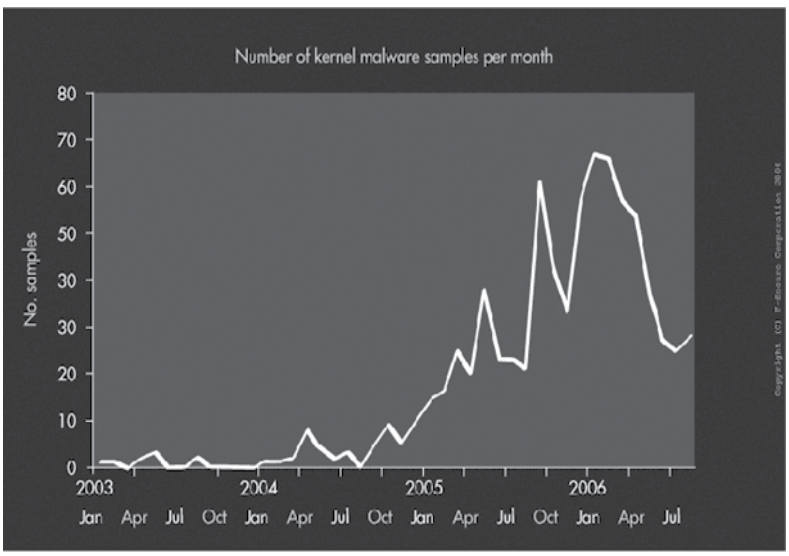


Figura 9.5
O crescimento do kernel malware
Fonte: http://www.f-secure.com/weblog/archives/00001118.html.

Prevenção

- Não usar servidor como estação de trabalho de usuário ou de administrador.
- Usar conta de "administrador" (root) apenas para instalação ou manutenção.
- Execute antirootkit periodicamente em todas as máquinas.

Mailbot aka Costrat

- É o mais poderoso e oculto rootkit produzido.
- Um único "driver kernel mode".
- Transporta DLL cifrada com payload, que é um spambot sofisticado com capacidade de backdoor.

Instruções para a remoção do Mailbot aka Costrat em "Removing Mailbot.AZ (aka Rustok.A) Rootkit" em: http://swatrant.blogspot.com/

- Detecção e remoção são desafios para detentores de rootkit e soluções de antivírus.

Remoção:

- AVG antirootkit.
- ADS Spy (ou HijackThis).

Spear phishing

- Ataques direcionados.
- Mensagem parece vir de alguém confiável.
  - Informações do remetente falsas.
  - Quando você clica no anexo, sua máquina é infectada.
    - Processo transparente.
    - Anexo pode conter informações aparentemente reais.
- Spear phishing é um tipo de ataque altamente direcionado;
- Pessoa mal-intencionada fica na internet procurando formas de iludir o usuário;
- Desde monitorar fóruns técnicos, para verificar suas necessidades de equipamentos, até o envio de currículos, se fazendo passar por um candidato;
- Pessoa abre o arquivo anexo, pois tem a necessidade real (não curiosidade) daquela informação;
- Após infectada, a máquina da pessoa abre conexões com as máquinas mal-intencionadas, deixando que o atacante tenha acesso total à máquina da vítima.

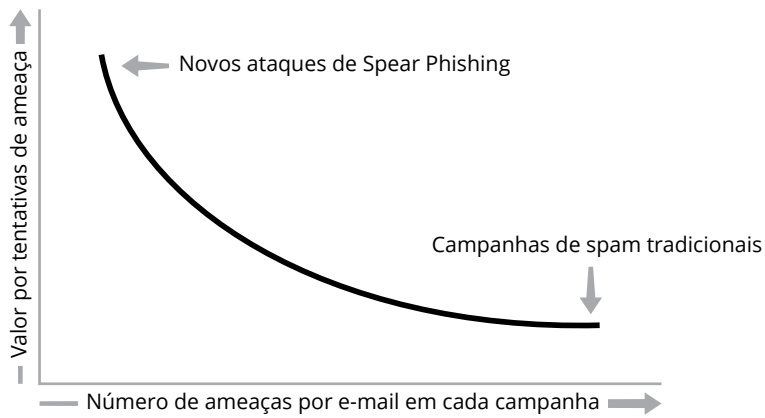


Figura 9.6
Retorno de ataques Spear phishing em relação aos ataques tradicionais.

Campanhas de Spear phishing são enviadas para poucos destinatários, mas oferecem maior retorno para os atacantes quando os destinatários respondem a eles.

Páginas contaminadas

Página legítima é atacada.

- Conteúdo visual não é alterado.
- Utiliza falhas de XSS (cross site scripting) e SQL Injection (SQLi).
- Scripts capazes de detectar tipo e versão do equipamento e do navegador utilizados.

Outra forma de ataque é a exploração de falhas de Cross Site Scripting e de SQL injection em páginas de grandes instituições (confiáveis), como provedores de acesso, comércio eletrônico, jornais ou revistas.

O atacante, em vez de alterar a página (ataque visualmente fácil de ser reconhecido), inclui scripts maliciosos na página. Os scripts serão entendidos e processados pelo seu navegador.



Possibilidades:

- Solicitação de "confirmação" de informações pessoais.
- Código oculto na página, redireciona a pessoa para a página.
- Possibilidade de download de plugin específico para ver a página.
  - Como você confia na página, você clica e instala o plugin malicioso (malware qualquer).

Entre as possibilidades desse ataque, tempos:

1. Inclusão de uma página solicitando a confirmação dos dados. Como a pessoa confia na página, ela coloca seus dados. Porém, ela está colocando seus dados em uma página falsa.
2. Código oculto, redireciona a pessoa para outra página, que pode conter somente propagandas ou outro tipo qualquer de software malicioso.
3. Página informa que a pessoa necessita atualizar algum plugin para visualizar algum tipo de conteúdo, geralmente um banner ou filme. A pessoa, confiando na página, faz o download desse plugin e o instala, porém o arquivo não lhe dará vantagem alguma.



Ataques exploram falhas em navegadores e plug-ins:

- Flash.
- Java.
- Adobe Reader.

Alguns desses tipos de ataques exploram falhas em outros softwares, como o Flash, Java ou Adobe Reader.

Redes sociais



Redes sociais utilizadas para campanhas fraudulentas:

- E-mail falso com convite para adicionar alguém (conhecido ou não como amigo).
- Ao clicar no convite, a pessoa é redirecionado para uma página solicitando seu usuário e senha.
- Tudo parece normal, porém a página é falsa e está roubando os dados para futuro uso, incluindo roubo de identidade.

Exploração de fragilidades nas páginas das redes sociais.

- Execução de scripts.
- Pessoa pode ser "infectada" somente ao visitar uma página.
- Redes sociais também são utilizadas atualmente para fraudes;
- Campanhas fraudulentas de todos os tipos são montadas, com foco em comunidades ou grupos de amigos;
- Nesse tipo de golpe, a pessoa pode receber um e-mail, do tipo convite para adicionar um novo amigo à sua rede de relacionamento;

- O e-mail deve ser um desconhecido ou parecer vir de um amigo;
- Ao clicar no convite, a pessoa é redirecionada para uma página solicitando usuário e senha;
- Tudo normal até então, a não ser um detalhe: a página em questão é falsa;
- Após colocar seus dados, a página apresenta um erro e a pessoa é redirecionada finalmente para a página real;
- Porém, o atacante já possui os dados e pode efetuar alguns golpes, incluindo roubo de identidade.
- Outra possibilidade com redes sociais é a exploração de vulnerabilidades nas próprias páginas das redes sociais (páginas confiáveis).
- Mais uma vez um script mal-intencionado é incluído, e somente visitando a página infectada o navegador pode efetuar ações como entrar em outros sites, clicar outros links ou até mesmo infectar outras páginas e tudo isso completamente invisível para o usuário.

Como se proteger



Spear Phishing, páginas contaminadas ou redes sociais:

- Mantenha os softwares de sua máquina atualizados.
- Verificar sempre situações ou e-mails estranhos ou duvidosos.
- Manter o software de antivírus sempre atualizado.
- Comunicar qualquer situação estranha, anormal ou inesperada ao administrador da rede ou ao responsável pela segurança da informação.

Exercício de fixação 3 
Redes sociais

Que proteções devem ser adotadas para evitar as fraudes em redes sociais?

SANS Top 20 Internet Security Attack Targets



- Lançado no ano 2000 pelo SANS e NIPC (FBI).
- Documento original:
  - As dez vulnerabilidades de segurança mais críticas da internet (Top 10).
- Lista confiável e expandida para Top 20.
- Indica as vulnerabilidades de segurança que devem ser priorizadas para tratamento.
- Vulnerabilidades exploradas por worms como Blaster, Slammer e CodeRed estiveram nas listas SANS.
- CAIS/RNP ampliou divulgação da SANS Top 20.
  - http://www.sans.org/top20/
  - Esse recurso está desatualizado, porém suas informações continuam válidas, visando entender o que aconteceu e qual a evolução das ameaças e das medidas de proteção.

Como se manter atualizado, quando o assunto é segurança?

Sendo a área de segurança bem abrangente, não existe uma resposta objetiva. Depende do que você está buscando, de seus interesses e ramo de atuação.



- Mailling Lists.
- Blogs.
- Twitter.

Durante muito tempo, listas de distribuição de e-mail, também conhecidas como mailling lists, foram a forma mais rápida e objetiva para trocar informações e manter-se informado. Com o crescente volume de mensagens ficava difícil filtrar e ler tudo sobre um determinado assunto (e continua assim). Mesmo ainda existindo e sendo bem valiosas em termos de informação, as listas de distribuição de e-mail servem mais para debates e troca de informações do que propriamente para manter as pessoas informadas. Para essa finalidade (manter as pessoas informadas) os blogs e microblogs têm ganho cada vez mais espaço.

O Twitter é atualmente a melhor alternativa para quem deseja manter-se atualizado. Através dele, há a opção de seguir tanto empresas como pessoas. Quanto mais gente, mais mensagens serão recebidas, porém tudo via web. A grande vantagem são os textos reduzidos. Quem posta alguma coisa no Twitter tem no máximo 140 caracteres para se expressar. A leitura por parte do usuário é rápida. Se o usuário achou o texto interessante, pode efetuar uma busca mais detalhada sobre o tema ou clicar e ler o texto completo (quando existe essa possibilidade).



Figura 9.7
Página de abertura do Twitter.

Existem clientes Twitter para a maioria das plataformas de celular, assim como alguns clientes para Windows, como o Tweetdeck (http://www.tweetdeck.com/).



Figura 9.8
Tela ilustrativa do TweetDeck.

Uma compilação com mais de 380 profissionais e 95 entidades/empresas da área de segurança da informação pode ser encontrada em http://tinyurl.com/TwitterSeg

Sugestões para começar:

- http://twitter.com/g1seguranca
- http://twitter.com/seginfo
- http://twitter.com/FSecure
- https://twitter.com/modulogrc

Na linha de blogs existe também muita coisa boa escrita em português. Uma compilação de mais de 100 blogs brasileiros pode ser encontrado em http://tinyurl.com/blogseg

Existem outros sites sobre segurança, alguns muito úteis, como:

- Site do Centro de Atendimento a Incidentes de Segurança da RNP, com alertas de segurança: http://www.rnp.br/cais/alertas/
- Site dedicado a ajudar usuários com problemas de segurança com matérias informativas: http://www.linhadefensiva.org/
- O site conhecido como Internet Storm Center (ISC) mantém atualizações diárias: http://isc.sans.org
- Site de um grupo especializado em segurança da informação com informações atualizadas: http://www.team-cymru.org/News/
- Inscreva-se na lista de e-mail desse site e receba as principais notícias por e-mail: https://lists.cymru.com/mailman/listinfo/ians_dragon_newsbytes

Vale sempre lembrar que a internet nasceu em território americano, assim, muito material ainda é escrito e divulgado em inglês, valendo a pena o estudo dessa língua, para os que desejam focar sua carreira na segurança da informação.

Manter-se atualizado pode ser uma tarefa difícil: às vezes, por causa da falta de informação sobre assuntos específicos; outras vezes por causa de excesso de informação, que acaba nos tomando um tempo muito grande. É preciso saber "filtrar" o que é realmente útil e interessante.

Roteiro de Atividades 9

Atividade 9.1 – Conceitos de malware

1. Teste seus conhecimentos sobre phishing:

- http://www.microsoft.com/canada/smallbiz/sgc/quiz.mspx
- http://www.mailfrontier.com/forms/msft_iq_test.html
- http://www.sonicwall.com/furl/phishing/

2. Entre no site da Web of Trust (http://www.mywot.com/):

- Teste a reputação de alguns sites conhecidos.
- Caso deseje, instale também esse add-on.

3. Instale o pacote antiscam do EarthLink.

- http://www.earthlink.net/software/domore.faces?tab=toolbar
- Navegue nos sites de sua preferência verificando o status do plug-in.

Atividade 9.2 – Antirootkit

1. Verifique as alternativas de anti-rootkits, nomes, plataformas e licenças de uso em: http://www.antirootkit.com/software/index.htm

   1.1. Escolha um pacote compatível com sua plataforma e instale.

   1.2. Examine o computador em busca de rootkits.

2. Instale o pacote chrootkit:

```
# apt-get install chrootkit
```

3. Para fazer uma varredura no computador execute:

```
#chrootkit
```

Quais problemas foram encontrados no seu computador?

10

Fundamentos de segurança da informação

objetivos

Apresentar os fundamentos de segurança da informação, as normas existentes sobre o assunto e a importância nas organizações; explicar a relação entre o Cobit e a segurança da informação.

conceitos

Segurança da informação, vulnerabilidades e descarte de informação.

Introdução



A segurança da informação transcende a informática.

- Não existe sistema 100% seguro.
- O elo mais fraco da corrente sempre será o ser humano.
- Os riscos e as vulnerabilidades transcendem o mundo tecnológico.
- Vulnerabilidades físicas, tecnológicas e humanas estarão sempre presentes.
- Necessidade de assumir, gerenciar e gerir riscos.

A informação é um dos bens mais preciosos que uma empresa pode ter. Planejamentos estratégicos, folhas de pagamento, projetos secretos e dados de clientes são apenas alguns exemplos de informações sensíveis que uma empresa pode ter. Com a chegada da tecnologia, vieram as facilidades da informática para guardar, gerenciar e apresentar a informação (é importante lembrar que o termo "informática" é derivado de "informação automática").

Hoje temos consciência de que o objetivo da informática é a manipulação da informação, o que deu origem ao termo Tecnologia da Informação (TI). Na área de segurança, surge o termo Segurança da Informação, para representar tudo que diz respeito à proteção da informação, eletrônica ou não.

O que é segurança da informação?

Área do conhecimento dedicada à proteção dos ativos da informação contra acessos não autorizados, alterações indevidas ou indisponibilidade.

Por que proteger as informações?

- Pelo seu valor direto;
- Pelo impacto de sua ausência;
- Pelo impacto resultante de seu uso por terceiros;
- Pela relação de dependência com a sua atividade.

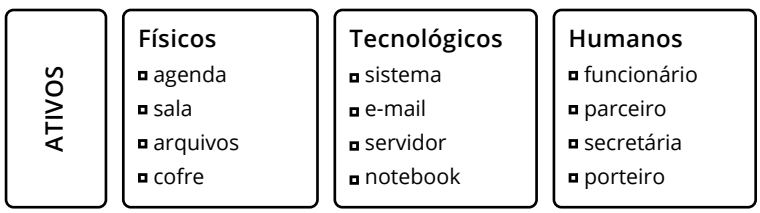
Fundamentos

Quando proteger as informações?

- Durante seu ciclo de vida.

Manuseio.

- Momento em que a informação é criada e utilizada, incluindo coleta.
- Armazenamento da informação.



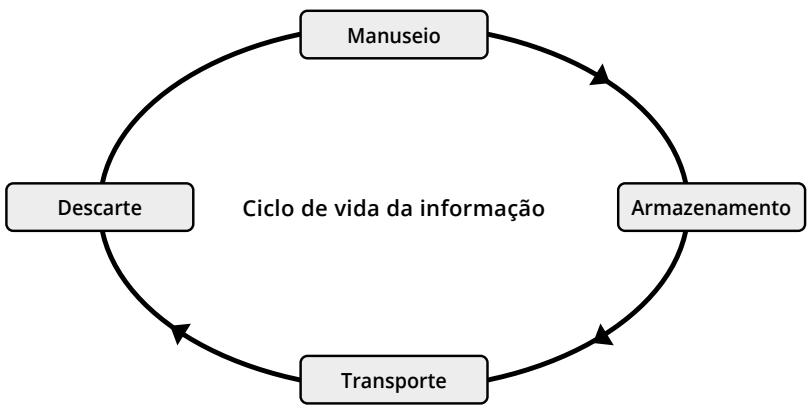


Figura 10.1
O Ciclo de Vida da Informação e alguns de seus ativos.

Transporte

- Importante etapa que inclui conectividade da rede (e-mail, fax, carta etc.);
- A divulgação faz parte dessa etapa, pois transporta a informação de um ponto a outro;
- Processamento é um misto entre transporte e manuseio.

Descarte

- Eliminação total e completa da informação;
- Onde proteger as informações? Nos ativos que as custodiam.

O que proteger nas informações?

Os atributos:

- Confidencialidade;
- Integridade;
- Disponibilidade.

Os aspectos:

- Autenticidade:
  - Autenticação;
  - Autorização;
  - Auditoria;
- Legalidade.



- Podem ser atingidos por exploração de falha ou vulnerabilidade presente em ativo.
- Do que proteger as informações?

Ameaças:

- Físicas:
  - Incêndio;
  - Inundação;
  - Curto circuito;
  - Apagão.
- Tecnológicas:
  - Vírus;
  - Bug software;
  - Defeito técnico;
  - Invasão web.
- Humanas:
  - Sabotagem;
  - Fraude;
  - Erro humano;
  - Descuido.

Conceitos básicos



- Confidencialidade:
  - Garante que a informação seja acessada somente por pessoas autorizadas.
- Integridade:
  - Salvaguarda da exatidão, completeza da informação e dos métodos de processamento.
- Disponibilidade:
  - Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.
- Informação:
  - São todos os dados de uma empresa, independentemente do formato em que se encontram. Está presente nos ativos, que são alvo da proteção da segurança da informação.
- Ativo:
  - Todo elemento que contém informação, inclusive a informação em si. Exemplos: servidores, discos, roteadores, arquivos, pastas, pessoas etc.

- Vulnerabilidade:
  - Falha presente no ativo e explorada por ameaça que causa quebra na segurança.
- Ameaça:
  - Explora vulnerabilidade presente no ativo, que custodia informação causando "impacto" (incidente ou falha de segurança) no negócio.
- Ameaças:
  - Naturais:
    - Provenientes da natureza, como enchentes, raios etc.
  - Involuntárias:
    - Causadas por acidentes ou erros provocados por usuários e administradores de sistema.
  - Voluntárias:
    - Causadas propositadamente por usuários maliciosos e invasores de sistemas.

Padrões existentes de segurança

- Norma.
  - Aponta o que fazer na administração da segurança da informação.
- Metodologia (em conformidade com a norma).
  - Aponta como fazer a administração da segurança da informação.
- Norma + metodologia = melhores práticas (best practice).

Documentos que tornam a segurança da informação previsível e tratável:

- RFC 2196: Site Security Handbook.
- ISO 27001.
- Control Objectives for Information and Related Technology (Cobit).

RFC 2196: Site Security Handbook

- Site oficial: http://www.ietf.org/rfc/rfc2196.txt
- Política traduzida: http://penta.ufrgs.br/gereseg/rfc2196/
- Propósito de fornecer um guia de implantação de políticas de segurança de computadores e procedimentos para sites que têm sistemas na internet.
- Público-alvo: administradores de sistemas e redes, tomadores de decisão, gerentes dos sites.

Esse manual é um guia para desenvolvimento de políticas de segurança de computador e procedimentos para sites que têm seus sistemas na internet. O propósito desse manual é proporcionar um guia prático aos administradores, tentando tornar segura uma grande variedade de informações e serviços. Os assuntos abordados incluem os conteúdos de política e formação, tópicos técnicos de segurança de redes e, também, reações a incidentes de segurança. O enfoque desse documento está nas políticas e procedimentos que precisam ser usados para viabilizar as características técnicas de segurança que um site deve implementar.

Guia básico em cinco passos:

- Identifique o que está tentando proteger;
- Determine do que está tentando se proteger;
- Determine a probabilidade das ameaças;
- Implemente medidas que protegerão recursos importantes de maneira efetiva;
- Revise o processo continuamente, fazendo melhorias cada vez que encontrar uma falha.

Lema

O custo da proteção contra uma ameaça deve ser menor que o custo da recuperação no caso de ser atingido pela ameaça (é melhor prevenir que remediar).



1. Introdução.
2. Políticas de segurança.
3. Arquitetura:
   - Parte 1 – Plano de segurança.
   - Parte 2 – Proteção de serviços.
4. Serviços de segurança e procedimentos:
   - 4.1. Serviços e procedimentos seguros.
   - 4.2. Autenticação.
   - 4.3. Confiança.
   - 4.4. Integridade.
   - 4.5. Autorização.
   - 4.6. Acesso.
   - 4.7. Auditoria.
   - 4.8. Proteção de backups.
5. Tratamento de incidentes de segurança.
6. Atividades em andamento.
7. Ferramentas e endereços.
8. Mailing list.

RFC 3227



O manual Site Guidelines for Evidence Collection and Archiving é um guia para o desenvolvimento de políticas para respostas a incidentes de segurança.

Site oficial: http://www.ietf.org/rfc/rfc3227.txt

Propósito:

- Guia de melhores práticas e procedimentos para respostas a incidentes de segurança em sistemas na internet.

Público-alvo:

- Administradores de sistemas e redes, tomadores de decisão e gerentes dos sites.

ISO 27001



Certificação NBR ISO / IEC 27001:2005.

- ISO 27000 (Segurança da Informação).

Evoluiu da norma britânica BS7799.

- BS7799-1:
  - Introdução, definição de extensão e condições principais de uso da norma.
  - Disponibiliza 148 controles divididos em dez partes distintas.
  - Referência para implementar "boas práticas" de segurança.
- BS7799-2:
  - Define requisitos para um Sistema de Gestão de Segurança da Informação.

A norma ISO 27001 define dez áreas de conformidade:

1. **Política de segurança**

Define orientações para a segurança da informação: como usar a informação, quem deve usá-la e as punições aplicadas aos que não agirem em conformidade com a política.

2. **Segurança organizacional**

Define a estrutura responsável pela gerência da segurança. Sugere a criação de área especializada em segurança da informação e contatos com especialistas externos.

3. **Classificação e controle dos ativos**

Define recomendações para a classificação dos ativos de informação. Deverá garantir que cada ativo receba nível de proteção adequado, seja inventariado e tenha um responsável.

4. **Segurança sobre pessoas**

Define recomendações para a atribuição de responsabilidades de segurança a pessoas da organização, visando reduzir problemas como erro humano, roubo, fraude etc.

5. **Segurança física e do ambiente**

Estabelece perímetro físico de segurança, para que as instalações estejam protegidas contra ameaças externas. Recomenda que recursos e instalações sejam mantidos em áreas com nível de segurança adequado e sejam empregados controles de acesso.

6. **Gerenciamento das operações e comunicações**

Define recomendações para garantir o funcionamento seguro e correto dos recursos computacionais e da comunicação entre eles. Inclui a segurança dos computadores individualmente e da rede.

7. **Controle de acesso**

Define formas e permissões de acesso à informação, ligadas aos conceitos de autenticação e autorização. O gerenciamento de senhas de usuários faz parte desse item.

8. **Desenvolvimento e manutenção de sistemas**

Recomendações para o desenvolvimento de sistemas, de modo a incluir controles de segurança. Inclui criptografia, validação de dados, autenticação e assinaturas digitais.

9. **Gestão da continuidade do negócio**

Regras para minimizar a interrupção das atividades, no caso de incidente de segurança. Define plano de continuidade de negócio (PCN), e é uma estratégia para garantir que a instituição continue funcionando na ocorrência de desastres e falhas.

10. **Conformidade**

Consiste em evitar conflito com outras leis vigentes. Inclui direitos autorais, propriedade de software, privacidade pessoal e uso indevido, entre outros.



- Implementa modelo de gestão de segurança da informação dentro de parâmetros internacionais para um bom ambiente de negócios.
- Garante segurança das práticas internas e informações para parceiros e clientes.
- Selo com mesmo reconhecimento de mercado alcançado pelas famílias:
  - ISO 9000 (qualidade).
  - ISO 14000 (práticas ambientais).
- Define dez áreas de conformidade:

1. Política de segurança.
2. Segurança organizacional.
3. Classificação e controle dos ativos.
4. Segurança de pessoas.
5. Segurança física e do ambiente.
6. Gerenciamento das operações e comunicações.
7. Controle de acesso.
8. Desenvolvimento e manutenção de sistemas.
9. Gestão da continuidade do negócio.
10. Conformidade.

Empresas brasileiras certificadas ISO/IEC 27001 (1º/2/2012):

Name of the Organization	Country	Certificate Number	Certification Body
Atos Origin Brasil Ltda.	Brazil	IS 98429	BSI
Axur Information Security	Brazil	IS 509742	BSI
BT	Brazil	LRQ 4003984	LRQA
BT Global Services São Paulo SOC/NOC	Brazil	4003984	LRQA
Cardif do Brasil Vida e Previdência S/A	Brazil	IS 521855	BSI
CIP Câmara Interbancária de Pagamentos	Brazil	IS 96934	BSI
Fucapi-Fundação	Brazil	IS 504391	BSI
IBM ITD Brazil	Brazil	62691	Bureau Veritas Certification – Brazil
Módulo Security Solutions S/A	Brazil	IS 510466	BSI

Name of the Organization	Country	Certificate Number	Certification Body
Poliedro - Informática, Consultoria e Serviços Ltda.	Brazil	44121081309	BSI
Prodesp	Brazil	IS 512881	BSI
Promon Engenharia Ltda.	Brazil	IS 500248	BSI
Promon Tecnologia Ltda.	Brazil	IS 500564	BSI
Samarco Mineração S/A	Brazil	IS 524157	BSI
SERASA S.A.	Brazil	262326 ISMS	DQS
Serviço Federal de Processamento de Dados – SERPRO	Brazil	IS 515421	BSI
Superior Tribunal de Justiça	Brazil	IS 538457	BSI
Telefonica Empresas S/A	Brazil	IS 501039	BSI
Tivit Tecnologia da Informação S.A.	Brazil	00017-2006-AIS-OSL--NA	DNV
TIVIT Terceirização de Tecnologia e Serviços S.A.	Brazil	16203-2007-AIS-BRA--NA	DNV
T-Systems Brazil	Brazil	336227 ISMS	DQS
T-Systems do Brasil Ltda.	Brazil	341898 ISMS	DQS
UNISYS Global Outsourcing	Brazil	IS 97102	BSI
Zamprogna S/A Importação	Brazil	IS 518855	BSI

Tabela 10.1
Empresas brasileiras certificadas com o ISO/IEC 27001.

A Módulo Security foi a primeira empresa do mundo a obter a certificação ISO 27001.

Software de verificação de conformidade com a norma:

- Callio Secura 17799 /27001: http://www.callio.com/
- The Security Risk Management Toolkit: http://www.risk.biz/iso27001.html

A norma estabelece um Sistema de Gestão de Segurança da Informação (SGSI) implementado em oito fases:

1. Inicialização do projeto.
2. Definição do SGSI.
3. Análise de riscos.
4. Tratamento de riscos.
5. Treinamento e conhecimento.
6. Preparação para auditoria.
7. Auditoria.
8. Controles e melhoramentos contínuos.





Mais informações sobre a ISO 27001: http://www.iso27001security.com/, http://www.callio.com/ e http://www.modulo.com.br

Cobit



Common Objectives for Information and related Technology (Cobit).

- Metodologia criada pela Information Systems Audit and Control Association (Isaca) – http://www.isaca.org/ –, através do IT Governance Institute (http://www.itgi.org/).
- É uma estrutura de relações e processos para dirigir e controlar o ambiente de TI, orientada às metas da organização e à gestão de TI.
- O Cobit não é uma metodologia específica para segurança da informação, mas sim uma metodologia para gestão de TI que contém alguns aspectos de segurança da informação.

Common Objectives for Information and Related Technology (Cobit) é uma metodologia criada pela Isaca através do IT Governance Institute. Longe de ser uma metodologia específica para segurança da informação, o Cobit foi concebido para a gestão de TI e contém alguns aspectos relacionados à segurança da informação. Orientada a metas, possui uma estrutura de relação e processos para dirigir e controlar o ambiente de TI.

- IT Governance Institute's: http://www.itgovernance.org
- Information System Audit & Control Association: http://www.isaca.org/cobit.htm



O Cobit está dividido em quatro domínios:

- Planejamento e organização.
- Aquisição e implementação.
- Entrega e suporte.
- Monitoração.

Abaixo as subdivisões do Cobit em seus domínios com seus detalhes.

- Processos de Planejamento e Organização;
- Define plano estratégico de TI;
- Define arquitetura da informação;
- Determina direção tecnológica;
- Define organização de TI e relacionamentos;
- Gerencia investimento de TI;
- Gerencia comunicação das direções de TI;
- Gerencia recursos humanos;
- Assegura alinhamento de TI com requerimentos externos;
- Avalia os riscos;
- Gerencia os projetos;
- Gerencia a qualidade.

Processos de Aquisição e Implementação

- Desenvolve e mantém os procedimentos;
- Instala e certifica softwares;
- Gerencia as mudanças;
- Identifica as soluções de automação;

- Adquire e mantém os softwares;
- Adquire e mantém a infraestrutura tecnológica.

Processos de Entrega e Suporte

- Define e mantém os acordos de níveis de serviços (SLA);
- Gerencia os serviços de terceiros;
- Gerencia performance e capacidade do ambiente;
- Assegura a continuidade dos serviços;
- Assegura a segurança dos serviços;
- Identifica e aloca custos;
- Treina os usuários;
- Assiste e aconselha os usuários;
- Gerencia a configuração;
- Gerencia os problemas e incidentes;
- Gerencia os dados;
- Gerencia a infraestrutura;
- Gerencia as operações.

Processos de Monitoração

- Monitora os processos;
- Analisa a adequação dos controles internos;
- Provê auditorias independentes;
- Provê segurança independente.



A ABNT possui uma série de documentos chamada de família 27000. Esses documentos podem ser utilizados como base para quem deseja começar a implementação de procedimentos de segurança em suas empresas. Os documentos possuem códigos de prática e diretrizes para a implementação de segurança da informação, incluindo documentos sobre gestão de risco.

Outras normas, padrões e leis

Existem várias outras normas, padrões, leis e documentos sobre segurança da informação. Alguns desses documentos são genéricos, outros específicos para diferentes ramos de atividade. Existem, por exemplo, documentos e especificações diferentes para empresas do ramo financeiro e para empresas do ramo médico.

Família 27000



- ABNT NBR ISO/IEC 27001:2006.
  - Sistemas de gestão de segurança da informação – requisitos.
- ABNT NBR ISO/IEC 27002:2005.
  - Código de prática para a gestão da segurança da informação.
- ABNT NBR ISO/IEC 27003:2011.
  - Diretrizes para implantação de um sistema de gestão da segurança da informação.
- ABNT NBR ISO/IEC 27004:2010.
  - Gestão da segurança da informação – medição.
- ISO/IEC 27005:2011.
  - Gestão de Riscos de Segurança da Informação.

- ISO/IEC 27006:2011.
  - Especifica requisitos e fornece orientações para os organismos que prestem serviços de auditoria e certificação de um sistema de gestão da segurança da informação.



Sarbanes Oxley (SOX)



- Criada depois de diversos escândalos financeiros ocorridos em grandes companhias nos Estados Unidos.
- Composta por 11 títulos.
- Diz respeito à responsabilidade corporativa pela veracidade de conteúdo dos relatórios financeiros produzidos e pelo gerenciamento e avaliação dos controles internos.
- Voltada principalmente para companhias de capital aberto com ações nas bolsas de valores ou com negociação na Nasdaq (bolsa de valores das empresas de tecnologia).
- Aperfeiçoa os procedimentos de demonstração e de governança corporativa.
- Definem as responsabilidades de gerenciamento nos relatórios anuais e semestrais.

A lei Sarbanes Oxley visa garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas, de modo a mitigar riscos aos negócios e evitar a ocorrência de fraudes ou assegurar que haja meios de identificá-las quando ocorrem, garantindo a transparência na gestão das empresas. Atualmente grandes empresas com operações financeiras no exterior seguem essa lei.

PCI-DSS



- Padrão de segurança de dados desenvolvido pela indústria de pagamentos de cartões.
- Deve ser utilizado como guia para ajudar as organizações a prevenir fraudes de cartão de crédito, pirataria e outras questões de segurança.
- https://pt.pcisecuritystandards.org/

Visando proteger a privacidade dos consumidores portadores de cartão de crédito, algumas bandeiras de cartão de crédito criaram um conselho com a finalidade de criar e recomendar as melhores práticas de segurança de dados, para que sejam seguidas pelos estabelecimentos comerciais que aceitam cartões de crédito como forma de pagamento.

O PCI-DSS se aplica a toda e qualquer empresa que coleta, processa, armazena ou transmite informação de cartão de crédito, estando, portanto, obrigada a se adaptar ao padrão.

O PCI-DSS contempla 12 requerimentos básicos que têm por objetivo:

- Manter a rede de dados segura;
- Proteger as informações de portadores de cartão de crédito;
- Manter um programa de gerenciamento de vulnerabilidades;
- Implementar forte controle de acessos;
- Manter política de segurança de informações.

Documentação GSI/DSIC



- Norma Complementar 01:
  - Estabelecer critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta
- Norma Complementar 02:
  - Metodologia de Gestão de Segurança da Informação e Comunicações.
- Norma Complementar 03:
  - Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública.
- Norma Complementar 04:
  - Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal.
- Norma Complementar 05:
  - Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.

O Departamento de Segurança da Informação e Comunicações (DSIC) é o braço normativo do Gabinete Institucional de Segurança (GSI). Dentre seus objetivos destacam-se a produção de documentação referente à segurança cibernética na Administração Pública Federal.

Além das Normas Complementares mencionadas acima, podemos encontrar uma vasta documentação sobre segurança da informação e comunicações em http://dsic.planalto.gov.br.

Roteiro de Atividades 10

Atividade 10.1 – Segurança da informação

1. A segurança da informação consiste de três pilares básicos: confidencialidade, integridade e disponibilidade. Classifique os problemas de segurança abaixo de acordo com um (ou mais) destes pilares. Todos os problemas de segurança podem ser mapeados em uma destas características?

- Uso incorreto de criptografia;
- Acesso aos documentos sigilosos da organização por pessoas não autorizadas;
- Servidores da organização sem plano de contingência ou backup;
- Site de comércio eletrônico sem proteção para transações eletrônicas;
- Modificação de notas escolares por um aluno através do sistema da escola.

Atividade 10.2 – Vulnerabilidades

1. Quais as vulnerabilidades de sua estação de trabalho? Veja em: http://secunia.com/software_inspector

Atividade 10.3 – Descartes

1. A etapa do descarte é importante, visto que a informação, em muitos casos, possui prazo de validade. Algumas empresas estabelecem procedimentos de descarte até para informações pessoais, como correio eletrônico e papéis, de forma a prevenir que caiam em mãos erradas. Aparelhos como picotadoras são utilizados para o descarte seguro de informações, no caso de informação em papel. Determine o tempo que você levaria para armazenar cada uma das seguintes informações, caso fosse o responsável por elas:

- Logs de sistema;
- Arquivos de correio eletrônico;
- Notas fiscais;
- Fitas de backup.

2. Nos dias atuais, devemos sempre nos preocupar com o descarte de informações. Existem no mercado diversas soluções para recuperação de dados apagados, mesmo que o usuário formate o disco rígido. Baixe e instale o programa Eraser em http://eraser.heidi.ie/download.php e utilize-o para apagar arquivos em seu computador de maneira segura.

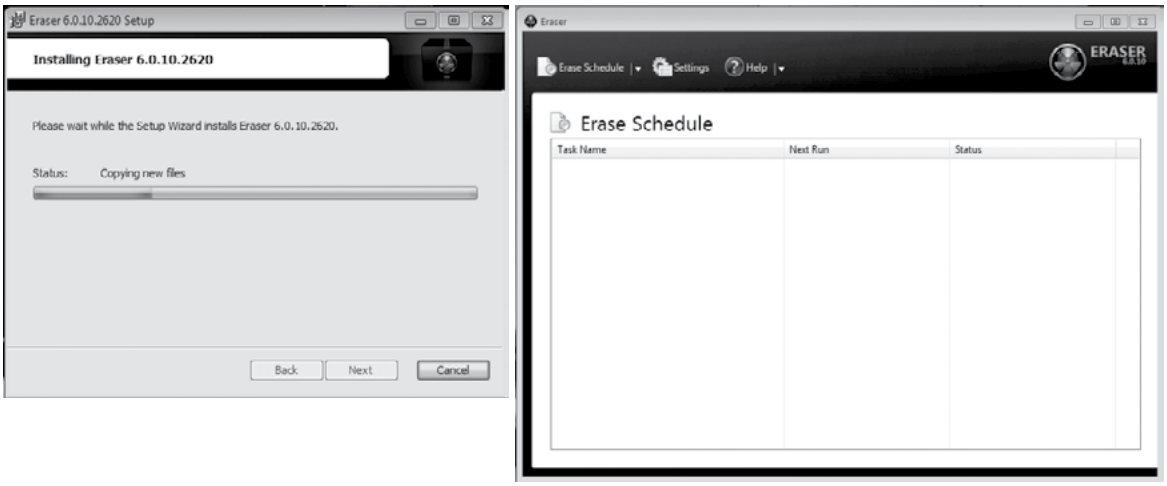


Figura 10.2
Eraser.

Bibliografia

- Administração e segurança da informação: http://www.informabr.com.br/nbr.htm#3
- APWG Committed to wiping out internet scams and fraud: http://www.antiphishing.org/
- Ataques DoS: http://www.cert.org/tech_tips/denial_of_service.html
- BEAL, Adriana. *Segurança da Informação – Princípios e melhores práticas para a proteção dos ativos de informação nas organizações*. Editora Atlas.
- Cartilha de segurança: http://cartilha.cert.br/
- Comércio eletrônico e segurança na internet: http://www.serpro.gov.br/publicacao/tematec/1997/ttec35
- Como funciona o dinheiro? http://dinheiro.hsw.com.br/dinheiro6.htm
- Como funciona o phishing: http://informatica.hsw.com.br/phishing.htm
- Comunicação cliente/servidor com sockets: http://www.imasters.com.br/artigo/2414/dotnet/usando_a_comunicacao_cliente_-_servidor_com_sockets/
- Criptografia Numaboa: http://www.numaboa.com/content/section/11/57/
- CSIRT Unicamp: http://www.security.unicamp.br/links.html
- Defesa de perímetros: http://www.magicweb.com.br/afreire/defesaperimetros_vi.htm
- DIERKS, T.; ALLEN, C. *The TLS Protocol, Version 1.0. Network Working Group, Request for Comments: 2246, Category: Standards Track*. 1999.
- Especialista em segurança da informação: http://www.semola.com.br
- FRASER, B. RFC 2196 – Site Security Handbook. Editor SEI/CMU, 1997. http://www.faqs.org/rfcs/rfc2196.html
- FREIER, Alan O. *et alli*. The SSL Protocol, Version 3.0. Transport Layer Security Working Group. Internet draft: http://wp.netscape.com/eng/ssl3/draft302.txt
- Informações sobre spyware: http://www.microsoft.com/protect/computer/spyware/default.mspx
- Informações sobre vírus: http://br.mcafee.com/virusInfo/default.asp
- Introdução ao DHCP: http://www.rnp.br/newsgen/9911/dhcp.html

- IP Spoof: http://www.hackemate.com.ar/ezines/the_virii_hacking_guide/vhg01/ip_spoof.html
- KAEO, Merike. *Designing Network Security*. Cisco Press, 1999.
- KASSLIN, Kimmo et al. Kernel Malware: The attack from within: http://www.f-secure.com/weblog/archives/kasslin_AVAR2006_Kernel-Malware_paper.pdf
- Manual de criptografia GnuPG: http://docs.indymedia.org/view/Sysadmin/GnuPGpt
- NBSO. Cartilha de segurança para internet. Versão 2.0. Março de 2003. Copyright© NBSO. http://www.nbso.nic.br/docs/cartilha/
- NIC BR Security Office – Brazilian Computer Emergency Response Team. Práticas de segurança para administradores de redes internet. Versão 1.2, 2003. http://www.nbso.nic.br/docs/seg-adm-redes/
- Norma NBR ISO/IEC 17799 – Tecnologia da informação – Código de prática para a gestão da segurança da informação.
- O que são vírus, worms e cavalos de troia? http://www.microsoft.com/brasil/athome/security/viruses/virus101.mspx
- O'MAHONY, D.; PEIRCE, M.; TEWARI, H. *Electronic Payment Systems*. Artech House, 1997. ftp://ftp.isi.edu/in-notes/rfc2246.txt
- Pequeno histórico sobre o surgimento de normas de segurança: http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos?id=69
- Portas TCP e UDP: http://www.infowester.com/portastcpudp.php
- Proteção contra rede banda larga: http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20070216_01
- Proteja-se contra fraudes on-line: http://www.microsoft.com/brasil/athome/security/online/phishing_filter.mspx
- Rede privada virtual: http://www.rnp.br/newsgen/9811/vpn.html
- Revista de segurança: http://www.linuxsecurity.com.br/revista/LinuxSecurityMagazine-Outubro02.pdf
- SANS: http://www.sans.org/rr
- SCHNEIER, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley. 1995.
- Segurança em roteador: http://www.rnp.br/newsgen/9903/seg-router.html
- SÊMOLA, Marcos. *Gestão da segurança da informação – uma visão executiva*. Ed. Campus, 2002.
- SOARES, L. F. Gomes et alli. *Das LAN's, MAN's, WAN's às redes ATM*. Ed. Campus, 1995.
- TANEMBAUM, Andrew. *Computer Networks*. Prentice Hall PTR, 2002.

- Táticas de defesa DDoS: http://www.iwar.org.uk/comsec/resources/dos/ddos-defense.pdf
- TCP/IP: http://www.pop-rs.rnp.br/ovni/tcpip/
- Túneis seguros de VPNs: http://br.attachmate.com/pt-BR/TechTalks/Secure+Tunnels.htm
- WOOD, Charles C. *Information Security Policies Made Easy*. Baseline Software, 2001.



Ivo de Carvalho Peixinho é Bacharel em Ciência da Computação pela UFBA e Especialista em Gestão de Segurança da Informação pela UnB. Possui mais de 15 anos de experiência na área de Segurança da Informação. Foi Diretor Técnico na XSite Consultoria e Tecnologia e Analista de Suporte na Universidade Federal da Bahia. Em 2004 atuou como Analista de Segurança Sênior no CAIS/RNP por dois anos, e atualmente é Perito Criminal Federal do Departamento de Polícia Federal desde 2007, lotado no Serviço de Repressão a Crimes Cibernéticos - SRCC/CGPFAZ/DICOR/DPF. É professor de pós-graduação nas disciplinas de Análise Forense em Sistemas Unix e Análise de Malware, e é palestrante em diversos eventos nacionais e internacionais como GTS, Seginfo, CNASI, ICCyber e FIRST.

esr.rnp.br

LIVRO DE APOIO AO CURSO

O livro de apoio ao curso Introdução à Segurança de Redes fornece conhecimentos introdutórios da área de segurança, através da apresentação dos conceitos básicos sobre segurança de redes, com apoio de atividades práticas em laboratório. Aborda a história da segurança física e lógica, apresenta um panorama atual da área (vulnerabilidades, tipos de ataques mais comuns, estatísticas), arquitetura TCP/IP (endereçamento, serviços, protocolos, DNS, roteamento), criptografia, políticas, padrões e normas de segurança da informação.

Este livro inclui os roteiros das atividades práticas e o conteúdo dos slides apresentados em sala de aula, apoiando profissionais na disseminação deste conhecimento em suas organizações ou localidades de origem.

ISBN 978-85-63630-23-0
9 788563 630230