holmesglen

Assessment Task 2: Case Study

Student Version

Section A – Program/Course details			
Qualification code:	22334VIC	**Qualification title:**	Certificate IV in Cyber Security
Unit code:	VU21988	**Unit title:**	Utilise basic network concepts and protocols required in cyber security
Department name:	BDIT, Computer and Information Technology	**CRN number:**	Enter CRN number

Section B – Assessment task details			
Assessment number:	2 of 2	**Semester/Year:**	1/2021
Due date:	Session 16	**Duration of assessment:**	15 weeks
Assessment method	Portfolio	**Assessment task results**	☒Ungraded result ☐Other: Click here to enter text.

Section C – Instructions to students

Task instructions:

Student will have to answer all the questions to be deemed competent.
This is an individual task and answers must be in your own words, do not copy and paste from internet.
Case study is given on page no. 5, there are five parts of the given case study is described on page 5. These are
part A – you have to write a report and provide background information
part B - in addition to background information, you have are required to provide additional information described in part B.
part C - In part C, you continued your report and add additional information in which you should provide difference between Network Security and Cyber Security and relate the key difference to the case study.
Part D - Additionally you have to provide security policy document in relation to your case study.
Part E - The network scenario is given in part E, you have to use Hypervisor software VMware Workstation or Fusion or Oracle Virtual Box to install windows and Linux virtual machine to test the configuration of the given scenario.

You are required to complete all parts of the Assessment Task.

Section D – Conditions for assessment

Conditions:

Student to complete and attach Assessment Submission Cover Sheet to the completed Assessment Task.

- Assessment to be completed individually.
- Discuss with your assessor if you feel you require special consideration or adjustment for this task.
- Students must meet all criteria listed in the marking guide to be satisfactory in this task.
- Students may resubmit this task if not successful within the enrolment period as per Holmesglen conducting assessment procedure.
- This is an open book assessment.
- The learner may use the internet for research
- This Assessment task must be uploaded to Brightspace along with a complete and signed coversheet.
- It is expected all documents will be completed and submitted electronically but if this is not possible, make alternative arrangements for submitting the documents with your assessor.
- You will have the opportunity to resubmit if any part of the assessment is deemed unsatisfactory (one resubmit allowed per task).

Assessment Task 2: Case Study

- You can appeal an assessment decision according to the Holmesglen Assessment Complaints and Appeals Procedure.
- If you feel you require special allowance or adjustment to this task, please decide with your assessor within one week of commencing this assessment.
- The learner may use the internet research answers for this assessment

Equipment/resources students must supply:	**Equipment/resources to be provided by the RTO:**
N/A	N/A

holmesglen

Assessment Task 2: Case Study

Section E – Marking Sheet - Student Answer Sheet			
Student ID:		**Student name:**	
Unit code:	VU21988	**Unit title:**	Utilise basic network concepts and protocols required in cyber security
Date:			

Criteria for assessment		Satisfactory		Comment
		Yes	No	
The following has been submitted for assessment:				
Part A - Background		☐	☐	
Part B - Ransomware and DDoS		☐	☐	
Part C - Network Security vs. Cyber Security		☐	☐	
Part D - Security Policy		☐	☐	
Part E – Test Configuration		☐	☐	
Part A - Background **Marking criteria for each product document/s supplied:**				
1.	Prepare a Physical AND Logical topology diagram	☐	☐	
2.	Implement IPv4/IPv6 address scheme.	☐	☐	
3.	List of security equipment, both hardware & software.	☐	☐	
4.	Recommendations of software that increase the security of the business from cyber security attacks.	☐	☐	
5.	List all external resources used in response to the case study	☐	☐	
Part B - Ransomware and DDoS **Marking criteria for each product document/s supplied:**				
1	Research and current example of DDoS Attack	☐	☐	
2	Research and current example of Ransomware Attack	☐	☐	
Part C - Network Security vs. Cyber Security **Marking criteria for each product document/s supplied:**				
1	Network Security definitions with appropriate examples given	☐	☐	
2	Cyber Security definitions with appropriate examples	☐	☐	
3	Differences between the two concepts explained.	☐	☐	

holmesglen

Assessment Task 2: Case Study

Part D - Security Policy **Marking criteria for each product document/s supplied:**				
1	Draft Security Policy covering three (3) elements.	☐	☐	
Part E – Test Configuration **Marking criteria for each product document/s supplied:**				
1	Create x2 Virtual machines and configure both machines with IPv4 addresses.	☐	☐	
2	Test connectivity of the virtual machines using CMD commands (Netstat/Ping)	☐	☐	
3	Testing your machines for external connectivity by pinging a public IP Server. (8.8.8.8).	☐	☐	
4	Identify and test the tools for network/Cyber security testing - Nmap commands	☐	☐	
5	Advise of any connectivity issues that you may have from an unsuccessful ping attempt.	☐	☐	
6	Basic Configuration of a Router or Switch using Packet Tracer & script.	☐	☐	
7	Connect the cables to network – Console & Straight Through cabling	☐	☐	

Section F – Feedback to Student				
Has the student successfully completed this assessment task?			**Yes**	**No**
			☐	☐
Additional Assessor comments (as appropriate):				
Resubmission allowed:	**Yes** ☐	**No** ☐	**Resubmission due date:**	
Assessor name:				
Assessor signature:				
Student signature:				
Date assessed:				

Assessment Task 2: Case Study

Supporting document

Assessment Task 2: Case Study

Unit code:	VU21988	**Unit title:**	Utilise basic network concepts and protocols required in cyber security
Student ID:		**Student name:**	
Date of submission:		**Student signature**:	

Part A: Background

You are a consultant for a small IT Consulting firm and have been approached by Metasploitable Pty Ltd to put forward a recommendation/solution to enhance their security stance.

The firm currently has 20 desktops, 15 laptop computers and a few iPad and mobile phones connected to local internet. The CEO of Metasploitable uses their own suite of end devices which consists of x1 Desktop; x1 Laptop, x1 iPad, and x1 iPhone. The remaining end devices are shared amongst the employees. Metasploitable is considering BYOD policy.

The business is housed in a small premise with a reception area, staff lounge, common are housing 10 workstations and 3 office spaces.

There is 1 reception desktop, each staff member has their own desktop. The Firm uses local email and file servers. There are 5 trainees that will be joining the firm next month. The CEO is concerned about internal security of files/data in general and does not want all staff members to have access to all areas of the network server, this includes trainees.

Staff have reported increased abnormal amount of suspected phishing emails and complaints regarding unusual/slow performance of computer networks have increased. Although Metasploitable Pty Ltd have no plausible reason for the increased receipt of threats/suspect emails, the CEO is wanting to implement a suitable data backup system which backs up daily to the cloud and an in-house physical device. This would also cover password complexity and periodic changing of passwords.

Further requirements for consideration are that the CEO requires a solid end-point solution which will check all endpoints on the current network for unusual behaviour.

To ensure you meet the client's requirements, **your report** should include the following areas

1. A logical and physical topology.
2. An IP design (IPv4 only) that meets the needs of their new office and business.
3. A list of any network and (if necessary) security equipment required to run the office, you must include a switch, router, wireless access point and firewall (hardware or software)
4. Recommendations for securing their business at a software level and how it protects from cyber-attacks (give 2 examples)

Assessment Task 2: Case Study

Your client has also expressed concern regarding the firm's vulnerability to cybersecurity attacks. You are required to provide the following additional reports to the client:

Part B - Ransomware and DDoS

Research one (1) **current** DDoS & Ransomware Attack with focus on the following criteria.

- How was each attack conducted/started?
- How did the attack spread?
- List any specific targets, if none, who were the targets
- What were the effects/consequences of your chosen attack?
- Who was held responsible for the attacks – individual or group
- Were there any business consequences?

Part C - Network Security vs. Cyber Security

Your client has significant confusion regarding the differences between 'Network & Cyber' Security. Conduct some research regarding the key differences between both and document your research accordingly. Consider reviewing the following resources as a start of your own research.

- www.nist.gov
- www.cisco.com
- www.acsc.gov.au
- www.sans.org

Part D - Security Policy

All organizations, particularly corporate organizations are required to have a policy document called a 'Security Policy' this policy document is generally a smaller section of a larger document called an Information Technology Policy.
Based on the Case Study Scenario, you are required to conduct research into a security policy, create your own 'draft' SecPol. Your draft SecPol should cover three (3) of the following areas:

- Acceptable Use Policy
- Confidential data Policy
- Password Policy
- Email Policy
- Physical Security Policy
- BYOD Policy

Part E – Test Configuration

You are now required to 'test' a segment of your network solution as a demonstration to your client.

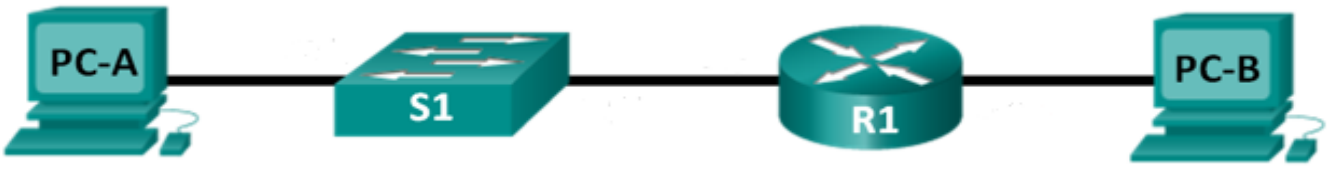
a) **Create two (2) virtual machines using VMware Workstation or Oracle VirtualBox. Create a Windows Operating System & a Linux OS.**
b) **Assign both machines a host IPv4 address using a network address of your choice.**

Assessment Task 2: Case Study

c) **Test connectivity of each machine to each other by using different CMD commands**
d) **Using one (1) machine, verify connectivity to a public server address.**
e) **Using Packet Tracer, build the PC – Switch – Router - PC topology. Cable the topology using the appropriate cables and demonstrating a console cabling for both PCs. You must identify the types of cabling you have used.**

f) **Use the following script to configure some basic settings. You are then required to finalise all other basic configurations.**

conf t
hostname TRS-80CoCo
enable secret class
no ip domain-lookup
banner motd $NO UNAUTHORISED ACCESS ALLOWED$
exit



holmesglen

Assessment Task 2: Case Study

Assessment Submission Cover Sheet (VET)

Student to complete relevant sections and attach this cover sheet to each assessment task for submission.

Student information			*To be completed by Student*
Student name:		**Student ID:**	

Program/Course details			
Qualification code:	22334VIC	**Qualification title:**	Certificate IV in Cyber Security
Unit code:	VU21988	**Unit title:**	Utilise basic network concepts and protocols required in cyber security
Department name:	BDIT, Computer and Information Technology	**CRN number:**	Enter CRN number

Assessment information					*To be completed by Student*
Teacher name:					
Due date:	Session 16	**Date submitted:**		**Re-submission:**	☐

Student declaration
By submitting this assessment task and signing the below, I acknowledge and agree that: This completed assessment task is my own work. I understand the serious nature of plagiarism and I am aware of the penalties that exist for breaching this. I have kept a copy of this assessment task. The assessor may provide a copy of this assessment task to another member of the Institute for validation and/or benchmarking purposes.

Student signature For electronic submissions: By typing your name in the student signature field, you are accepting the above declaration.	

Note:

Assessor to attach a photocopy of the completed Marking Guide (Section E) from the Student version of the Assessment Task.

Final result of the subject/unit will be entered on Banner by the teacher/assessor once all assessment tasks have been assessed.