|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Student Name |  | Student Number | |  |
| Unit Code/s & Name/s | VU23213 Utilise basic network concepts and protocols required in cyber security | | | |
| Cluster Name  *If applicable* | N/A | | | |
| Assessment Name | Network Security Protocols Portfolio | Assessment Task No. | | 2 of 2 |
| Assessment Due Date | Week 8 | Date submitted | | / / |
| Assessor Name | Tony Wilson | | | |
| **Student Declaration:** I declare that this assessment is my own work. Any ideas and comments made by other people have been acknowledged as references. I understand that if this statement is found to be false, it will be regarded as misconduct and will be subject to disciplinary action as outlined in the TAFE Queensland Student Rules. I understand that by emailing or submitting this assessment electronically, I agree to this Declaration in lieu of a written signature. | | | | |
| Student Signature |  | | Date | / / |
| **PRIVACY STATEMENT:** TAFE Queensland is collecting your personal information on this form for the purpose of assessment. In accordance with the Information Privacy Act 2009 (Qld), your personal information will only be accessed by staff employed by TAFE Queensland for the purposes of conducting assessment. Your information will not be provided to any other person or agency unless you have provided TAFE Queensland with permission, if authorised under our Privacy Policy (available at <https://tafeqld.edu.au/global/privacy-policy.html>) or disclosure is otherwise permitted or required by law. Your information will be stored securely. If you wish to access or correct any of your information, discuss how it has been managed or have a concern or complaint about the way the information has been collected, used, stored, or disclosed, please contact the TAFE Queensland Privacy Officer at [privacy@tafeqld.edu.au](mailto:privacy@tafeqld.edu.au) | | | | |

|  |  |
| --- | --- |
| **Instructions to Student** | **General Instructions:**  You are employed by MidTown IT as a network security specialist. Your job is to utilise and test network concepts and protocols required in cyber security.  Your teacher/assessor will take on the role of the Project Manager assigned to this project by MidTown IT.  For the practical LABS, read the documentation presented and familiarise yourself with the Project Scenario(s) or Case Study before proceeding with portfolio tasks. Confirm anything you are not sure about the project with your manager (teacher/assessor).  This assessment instrument requires the student to complete a project portfolio that is divided into four (4) parts:   * PART 1 – Network communication, security and security policies   + Task 1 Network communication models and network security concepts   + Task 2 Security Policy review   + Task 3 Transmission Control Protocol/Internet (TCP/IP) suite of protocols, IP addressing and binary and hexadecimal conversions * PART 2 – Security services, standards and protocols * PART 3 – Networking devices, components and security testing environment   + Task 1 Network devices and testing tools   + Task 2 Investigation and presentation of current cyber network attacks   + Task 3 Contingency task * PART 4 – LAB Security testing environment   + LAB 1 – New building network solution   + LAB 2 – File sharing testing   **Storage Devices:**   * Students are required to provide their own storage device.   **Materials Required:**   * Access to PCs and peripherals * Access to the Internet * Access to Connect (LMS) * Access to computer network system and devices * Access to a network security laboratory and testing environment * Access to organisation security documentation * Access to Word processing software, such as Microsoft Word * Access to special purpose tools, equipment and materials to complete the assessment.   **Online Delivery:**   * Students to supply their own PC or laptop and peripherals and internet access * Students will require permission to install the required software * Students will require access to Microsoft Office or similar application   **Documentation:**   * MidTown IT Scenario or Case Study * MidTown IT Security Policy * MidTown IT Network Security Protocols Portfolio Template   **Assessment Criteria:**  To achieve a satisfactory result, your assessor will be looking for your ability to demonstrate the following key skills/tasks/knowledge to an acceptable industry standard. Demonstrated ability to:   * Understand network security concepts and terminology * Identify threats, risks and vulnerabilities * Identify and manage cyber security breaches * Understand the OSI model and its layers’ functionality and protocols * Understand the TCP/IP model, its standards and protocols * Work with organisational security policies * Convert between decimal, binary and hexadecimal notation * Work with Server Message Block (SMB) * Use QUIC UDP to secure network traffic * Investigate NB-Io and IoT and LoRa-IoT standards for IoT * Demonstrate functionality of key network devices * Implement security of network components in a LAB practical * Investigate and present current cyber security attacks   Refer to the marking criteria for specific details:  VU23213\_AT2\_MC\_TQM\_V1  **Details of location:**  TAFE will provide a simulated work environment in the classroom. Research activities may be conducted in the classroom or at home.  If you are unable to attend a scheduled assessment activity, you must notify your teacher before the assessment is due and supply a doctor's certificate and approval from the team manager for an extension.  **Time restrictions:**  This assignment is designed to take place over 8 weeks or approximately 32 hours. The student is expected to attend classes as per timetable details and should be able to commit up to 3 hours per week of their own time to study or study related activities.  **Interactions:**  Teamwork skills are essential in the IT industry therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  **Level of assistance permitted:**  Staff cannot directly show students answers or solutions but support and guide them to complete tasks individually. Teachers and tutors should be available in class, and accessible by email for students working from home.  **Reasonable Adjustments:**  Reasonable adjustments are available to students for a variety of reasons, including: disability, language, literacy and numeracy (LLN) problems or extenuating circumstances. Talk to your teacher, counsellor or disability officer if you require extra support or an extension based on the conditions identified.  **Number of Attempts:**  You will receive up to two (2) attempts at this assessment task. Should your 1st attempt be unsatisfactory (U), your teacher will provide feedback and discuss the relevant sections / questions with you and will arrange a due date for the submission of your 2nd attempt. If your 2nd submission is unsatisfactory (U), or you fail to submit a 2nd attempt, you will receive an overall unsatisfactory result for this assessment task. Only one re-assessment attempt may be granted for each assessment task.  ***For more information, refer to the Student Rules.***  **Work, Health and Safety:**  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT related hazards such as tripping hazards, electromagnetic radiation, ergonomics, and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| **Submission details** | **Evidence Required to be Submitted:**  Insert your details on the cover page and sign the Student Declaration. Include this template with your submission.  **Submission via Connect:**  Upload a single file into Assessment 2 (AT2) Assignment Folder in Connect.  Multiple files can be compressed into a single file.  Name the file:  VU23213\_AT2\_Surname\_Student Number  TAFE Queensland Learning Management System (Connect)  **Accessing Connect:**  Connect URL: https://connect.tafeqld.edu.au/d2l/login  Username: 9 digit student number  Password: <your password>  For password reset go to: <https://passwordreset.tafeqld.edu.au/default.aspx> |
| **Instructions to Assessor** | **Specifications of assessment:**  To be judged competent in this assessment item the student is required to demonstrate competence in all indicators shown in the marking guide.  Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the cyber security field of work and include access to:   * project requirements   Ensure that students read and familiarise themselves with the Project Scenario provided and relevant files and/or resources before attempting the assessment.  **Storage Devices:**   * Students are required to provide their own storage device.   **Materials Required:**   * Access to PCs and peripherals * Access to the Internet * Access to Connect (LMS) * Access to computer network system and devices * Access to a network security laboratory and testing environment * Access to organisation security documentation * Access to Word processing software, such as Microsoft Word * Access to special purpose tools, equipment and materials to complete the assessment.   **Online Delivery:**   * Student to supply their own PC or laptop and peripherals and internet access * Students will require permission to install the required software * Students will require access to Microsoft Office or similar application   **Documentation:**   * MidTown IT Scenario or Case Study * MidTown IT Security Policy * MidTown IT Network Security Protocols Portfolio Template   **Level of Assistance Permitted:**  Teachers and tutors should be available in class, and accessible by email for students working from home. Staff cannot directly show students answers but support and guide them to complete tasks individually. Students with disability will receive reasonable adjustments.  **Interactions:**  Teamwork skills are essential in the IT industry therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  **Contingencies:**  Reasonable adjustment is available to students for a variety of reasons, including: disability, language, literacy and numeracy (LLN) problems or extenuating circumstances.  **Work, Health and Safety:**  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT related hazards such as tripping hazards, electromagnetic radiation, ergonomics, and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| **Note to Student** | An overview of all Assessment Tasks relevant to this unit is located in the Unit Study Guide.  If you have any question or need help regarding this assessment item please contact your teacher/tutor through email or during face-to-face sessions. |

# Project Scenario for PRACTICAL LABS

LAB 1 - SCENARIO

You have been put in charge of testing a new network solution for MidTown IT. The organisation is expanding to a second building. The requirements of the new network include the following:

* Routers (1 Router per building)
* Switches (2 Switches per building)
* Wireless Access Points (1 per building)
* 40 End devices (20 end devices per building // 15 Wired & 5 Wireless)

**IP Address to be subnetted 172.16.0.0/16:**

* + This should be subnetted to the closest useable addresses ensuring 20% free for future growth within each subnet.
  + Statically assigned

**Router Requirements:**

* Naming convention used (Device Type\_Building(Letter,Number,GeoLocation)\_Floor\_Room Number\_Router Number within specific location example (R\_G\_2\_9\_1 or R\_Bris\_2\_9\_1)
* Authentication configured to access the device
  + Password: Testing123
* SSH configured
  + Domain: testing123.com
  + Version: 2
  + Modulus: 1024
  + Username: Admin
  + Password: Testing123
* OSPF routing protocol used
* All device passwords encrypted at the highest level available

**Switch Requirements:**

* Naming convention used (Device Type\_BuildinPC0(4)PC.B1.103.1g(Letter,Number,GeoLocation)\_Floor\_Room Number\_Switch Number within specific location example (S\_G\_2\_9\_1 or S\_Bris\_2\_9\_1)
* Authentication configured to access the device
* Password: Testing123
* SSH configured
  + Domain: testing123.com
  + Version: 2
  + Modulus: 1024
  + Username: Admin
  + Password: Testing123
* Management IP address configured
* Default Gateway configured
* All device passwords encrypted at highest level available

**Wireless Access Point Requirements:**

* Building 1
  + SSID: Testing123\_B1
  + WPA2-PSK Security protocol
  + AES Encryption
  + Password: Testing123\_B1
* Building 2
  + SSID: Testing123\_B2
  + WPA2-PSK Security protocol
  + AES Encryption
  + Password: Testing123\_B2

LAB 2 – SCENARIO

The organisation has asked you to demonstrate to the other members of your team, how file sharing over the network can work within the new building. As this is just a demonstration within a testing environment, the use of virtual machines will be required.

**Instructions:**

Use the template provided to complete the tasks of this portfolio.

**Template:** MidTownIT\_Network\_Security\_Protocols\_Portfolio\_Template

**PART 1 – Network communication, security and security policies**

**Task 1 Network communication models and network security concepts**

This section of the portfolio requires you to demonstrate a working understanding of key network security concepts.

* 1. Identify and define three (3) cyber security vulnerabilities of a data network. Provide examples to illustrate your answer.
  2. Explain at least two (2) differences between network security and cyber security.
  3. Identify and briefly describe three (3) business implications of cyber security breaches. Provide examples to illustrate your answer.
  4. OSI Data communication model

1. Define the OSI data communication model
2. Identify and describe the overall purpose of the OSI model, the functionality of each layer and the protocols associated with each layer. Use the table below to provide your answer.

|  |  |  |
| --- | --- | --- |
| **Open Systems Interconnection (OSI) Model** | | |
| **OSI model definition:** | | |
| **LAYER NAME** | **FUNCTIONALITY** | **PROTOCOLS** |
| 7. |  |  |
| 6. |  |  |
| 5. |  |  |
| 4. |  |  |
| 3. |  |  |
| 2. |  |  |
| 1. |  |  |

**Task 2 Security Policy review**

1.5 Access and review the MidTown IT Security Policy provided and write detailed explanations to the following questions:

1. Identify if the policy includes provisions for visitors’ access and external technical personnel access. Do you consider this access information needed in the policy? Why?
2. Review the current policy stand on social media usage. How could this section be improved?
3. Identify and briefly describe the people in the organisation with access to official-sensitive data and the process to access that data. Do you consider current measures secure? Outline potential improvements.
4. Review the *Privacy Impact Statement* section. How could this section be improved?
5. Review the *Bring your Own Device* section. Consider the potential risks of using external devices and evaluate the consequences. Would you change this section? Why?

**Task 3 Transmission Control Protocol/Internet** **(TCP/IP) suite of protocols, IP addressing and binary and hexadecimal conversions**

* 1. Define the TCP/IP communication model and its layers.

|  |  |  |
| --- | --- | --- |
| **Transmission Control Protocol/Internet (TCP/IP)** | | |
| **TCP/IP Suite definition:** | | |
| **LAYER NAME** | **Description** | **PROTOCOLS** |
| 4. Application |  |  |
| 3. Transport |  |  |
| 2. Internet |  |  |
| 1. Network access |  |  |

* 1. Explain how the TLS and the HTTPS protocols contribute to providing security for network communications.
  2. Identify and describe two (2) differences and two (2) commonalities between the OSI and the TCP/IP models.

1.9 Explain the addressing schemes of IPv4 and IPv6. Provide one (1) example of each protocol version to illustrate your answer.

1.10 Explain the binary and hexadecimal number systems.

1.11 **Binary conversion** – Convert the following decimal numbers into 8-bit binary representations:

1. 129
2. 78
3. 54

1.12 **Hexadecimal conversion** - Convert the following decimal numbers into hexadecimal notation:

1. 8193
2. 3512
3. 61697

**PART 2 – Security services, standards and protocols**

2.1 Define the purpose of a Server message Block (SMB) in a local area network. Provide examples to demonstrate its functionality.

2.2 **QUIC User Datagram Protocol (UDP)**

a) Investigate and define QUIC User Datagram Protocol (UDP)

b) Explain how QUIC UDP can be used to increase the security of HTTP traffic on the network. Provide at least two (2) examples to illustrate your answer.

2.3 **Narrowband Internet of Things (NB-IoT)**

a) Investigate and describe the purpose of NB-IoT standards

b) Identify the type of communication and devices NB-IoT standards are suited for. Provide examples to illustrate your answer.

2.4 **Long Range IoT (LoRa-IoT)**

a) Investigate and describe the purpose of LoRa-IoT standards

b) Identify the type of communication and devices LoRa-IoT standards are suited for. Provide examples to illustrate your answer.

**PART 3 – Networking devices and components and cyber network attacks**

**Task 1 Network devices and testing tools**

3.1 Describe in detail the functions and operations of the following network devices:

a) Switches

b) Routers

c) Wireless access point (WAP)

d) Wireless enabled end point

3.2 Describe the functions and operation of a firewall in a network.

3.3 Identify and describe three (3) tools that can be used in a networking testing environment.

3.4 Explain how virtualisation tools can be used in a network testing environment.

3.5 Describe how virtualisation tools can be interconnected in a network testing environment.

**Task 2 Investigation and presentation of current cyber network attacks**

3.6 This section requires you to investigate and present to an audience current cyber network attacks of the types described below.

For each attack, explain in detail the attack mechanism.

a) Distributed Denial of Service (DDoS) attack

b) Ransomware breach attack

c) LAN Address Resolution Poisoning (ARP) attack

3.7 Investigate and identify three (3) resources that could be used to increase industry cyber security awareness.

**Task 3 Contingency task**

3.8 Assume that a recent network check report has identified a significant increase in the number of ARP attacks detected. Although the current detection tool works, you are concerned that the current security system may not be sufficient in the long term.

List and describe at least two (2) reasons you can use to justify and convince management about the need to update the current security systems and tools.

**PART 4 – LAB Security testing environment**

4.1 **LAB 1 – New building network solution**

Read the scenario for LAB 1 and test the proposed network solution for the network expansion into a second building. The new network requirements include:

* Routers (1 Router per building)
* Switches (2 Switches per building)
* Wireless Access Points (1 per building)
* 40 End devices (20 end devices per building // 15 Wired & 5 Wireless)

To complete the task you need to provide:

1. Logical network diagram
2. Physical network diagram including rack diagram
3. Screenshots of router and switch configurations
4. Screenshots of wireless access point configurations
5. Screenshots of wireless device Wi-Fi configuration
6. Screenshots of testing and troubleshooting end-to-end connectivity of the below devices:

* Any wired end device in Building 1 to any wireless end device in Building 1
* Any wired end device in Building 1 to S\_1\_1\_1\_1
* Any wired end device in Building 1 to R\_1\_1\_1\_1
* Any wired end device in Building 1 to R\_2\_1\_1\_1
* Any wired end device in Building 1 to S\_2\_1\_1\_1
* Any wired end device in Building 1 to any wired end device in Building 2
* Any wired end device in Building 1 to any wireless end device in Building 2
* SSH from Wireless Device in Building 2 to S\_2\_1\_1\_1
* SSH from Wireless Device in Building 2 to R\_2\_1\_1\_1
* SSH from Wireless Device in Building 2 to R\_1\_1\_1\_1
* SSH from Wireless Device in Building 2 to S\_1\_1\_1\_1

4.2 **LAB 2 – File sharing testing**

Read the scenario for LAB 2 and using virtual machines, demonstrate and test how file sharing over the network can work within the new building.

You need to provide screenshots of the following settings and processes:

1. Virtual Machine Network Settings
2. Testing connectivity between virtual machines
3. Ensuring SMBv2/3 is Enabled via PowerShell command. If not enabled, enable it using PowerShell command
4. Create a shared folder to be accessed over the network
   * FolderName: Share
5. Configure share permission so everyone has read/write access to the folder
6. Create a text file within the shared folder
   * FileName: testing
7. Test to ensure your other virtual test machine can access the shared folder and copy the test file to its local desktop

**End of Assessment**