**Network Security Protocols Portfolio**

**Template**

Created by

Dylan Wondal

**UPTOWN IT**

**PROJECT REFERENCE:**

**DATE:**

Contents

[1 Network security and communication models 2](#_Toc118100748)

[OSI Data communication model 2](#_Toc118100749)

[2 Security policy review 2](#_Toc118100750)

[3 TCP/IP, IP addressing and binary and hexadecimal conversions 3](#_Toc118100751)

[Binary and hexadecimal notation 3](#_Toc118100752)

[4 Security services, standards and protocols 4](#_Toc118100753)

[5 Network devices, components and cyber network attacks 4](#_Toc118100754)

[Network devices and components 4](#_Toc118100755)

[Investigation on current cyber network attacks 5](#_Toc118100756)

[Contingency task 5](#_Toc118100757)

[6 LAB: Security testing environment 5](#_Toc118100758)

[LAB 1 - SCENARIO 5](#_Toc118100759)

[LAB 2 – SCENARIO 7](#_Toc118100760)

[Appendix 8](#_Toc118100761)

Remove all blue text once your document is completed. The blue text is intended at giving you some pointers for the document content.

# 1 Network security and communication models

1.1 Identify and define three (3) cyber security vulnerabilities of a data network. Provide examples to illustrate your answer.

1. **The first cyber security vulnerability to a network is the use of weak passwords. By using weak passwords an attacker can easily guess the passwords and gain unauthorised access to the network.**
2. **Another vulnerability is outdated software. With new vulnerabilities being found every day, a system with outdated software will most likely have a vulnerabilities in it so an attacker can exploit that and gain access.**
3. **The last type is social engineering where an attacker can trick a user into giving passwords and physical access to the network. e.g. attacker could tell receptionist they are a technician and need to see the server room and from there take over the network.**

1.2 Explain at least two (2) differences between network security and cyber security.

**The first difference is that network security focuses mainly on the protection of a network whereas cyber security is a more broad term which involves anything cyber related. The second difference is that network security has more of a focus on the infrastructure of the network. This differs from cyber security as cyber security also focuses on the human behaviour and element which will include policies and restrictions. Network will have a focus on encryption and firewalls.**

1.3 Identify and briefly describe three (3) business implications of cyber security breaches. Provide examples to illustrate your answer.

**1. Financial loss: A breach to a company could lead to financial losses. This could be due to system outages which leads to a loss in business and a loss in profit. For instance, the 2017 Equifax breach exposed sensitive information of over 143 million individuals, leading to the company paying over $1 billion in settlements.**

**2. Cybersecurity breaches can severely damage a business's reputation, leading to loss of customer trust and loyalty. In the age of social media and instant communication, news of a breach can spread quickly, leading to negative publicity and media attention. For instance, in 2018, Facebook was hit with a data breach that affected over 50 million user accounts, leading to a significant loss of trust and credibility for the social media giant.**

**3. Businesses are increasingly subject to data privacy and cybersecurity regulations. A cybersecurity breach can lead to significant regulatory consequences, including fines, legal action, and mandatory remediation efforts. For example, in 2019, the UK's Information Commissioner's Office fined British Airways £183 million following a data breach that affected over 500,000 customers. The company also faced a class-action lawsuit and had to invest in significant cybersecurity measures to prevent future breaches.**

## 1.4 OSI Data communication model

|  |  |  |
| --- | --- | --- |
| Open Systems Interconnection (OSI) Model | | |
| OSI model definition**: The OSI model is a framework that explains how a network communicates with other networks and is broken into 7 layers. Each layer has its own purpose and communicates with the layer above and below it.** | | |
| LAYER NAME | FUNCTIONALITY | PROTOCOLS |
| 7. **Application** | **Allows user to connect and interact with systems.** | **HTTP, HTTPS, SSH** |
| 6. P**resenation** | **Converts data so other systems can use as well as decryption and decompression.** | **TLS, SSL** |
| 5. **Session** | **Estabalish and maintain sessiosn between different networks** | **NETBIOS, RPC, SMB** |
| 4. T**ransport** | **Ensures reliable data delivery and segmentation of data.** | **UDP, TCP** |
| 3. N**etwork** | **Provides the routing and connection establishment of connections** | **ARP, OSPF, RIP** |
| 2. **Data link** | **Provides MAC addresses and allows the data to be sent to other devices** | **Ethernet, Wifi** |
| 1. **Physical** | **Transport the raw bits using electrical signals or other means of physical transportation.** | **RJ-45, USB** |

# 2 Security policy review

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

* 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?

**The policy has not stated whether visitors or external technicians have access to any of the data and how they should access it. This information should be included in the document to make in clear what data visitors/techinicians have access to and how they need to access it.**

* Review the current policy stand on social media usage. How could this section be improved?

**It could be improved by explicity defining what *professional and responsible manner* is as well as what *limited and occasional* is. The policy should also specify the consequences for the violation of the social media police.**

* 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.

**According to the policy, only authorized employees have access to Official-Sensitive data and the folders that contain this data. The policy does not provide specific details on how employees are authorized. It is recommended that the organization clarify the process and define strict access controls. Access should be granted based on a need-to-know basis, and employees should be required to undergo regular security awareness training to ensure they understand the importance of safeguarding sensitive data.vThe policy also recommends using full disk encryption, hash functions, and encryption for removable devices that hold Official or Official-Sensitive data. However, there is no mention of two-factor authentication or other measures that can provide an additional layer of security to sensitive data. One potential improvement could be to implement a role-based access control system, where employees are granted access based on their job responsibilities and job roles. This can limit access to sensitive data only to those employees who require it, and reduce the risk of unauthorized access.**

* Review the Privacy Impact Statement section. How could this section be improved?

**To improve this section, the policy could provide more guidance on what information should be included in the Privacy Impact Statement. This could include a checklist of items to consider, such as the types of data being collected, how it is used, who has access to it, and how it is protected. The policy could also provide guidance on who should be involved in conducting the Privacy Impact Statement, such as privacy officers or data protection officers.**

* 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?

# 3 TCP/IP, IP addressing and binary and hexadecimal conversions

* Define the TCP/IP communication model and its layers

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

* Explain how the TLS and the HTTPS protocols contribute to providing security for network communications.
* Identify and describe two (2) differences and two (2) commonalities between the OSI and the TCP/IP models.
* Explain the addressing schemes of IPv4 and IPv6. Provide one (1) example of each protocol version to illustrate your answer.

## Binary and hexadecimal notation

* Explain the binary and hexadecimal number systems.
* **Binary conversion** – Convert the following decimal numbers into 8-bit binary representations:

1. 129
2. 78
3. 54

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

1. 8193
2. 3512
3. 61697

# 4 Security services, standards and protocols

Write an introductory paragraph for the section.

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

Quick (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.

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.

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.

# 5 Network devices, components and cyber network attacks

Write an introductory paragraph for the section.

## Network devices and components

* 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

* Describe the functions and operation of a firewall in a network.
* Identify and describe three (3) tools that can be used in a networking testing environment.
* Explain how virtualisation tools can be used in a network testing environment.
* Describe how virtualisation tools can be interconnected in a network testing environment.

## Investigation on current cyber network attacks

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

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

If applicable, include the presentation files, for example, PowerPoint. These files can be also included in an appendix.

## Contingency task

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.

# 6 LAB: Security testing environment

## 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\_Building(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

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

## 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.

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

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

# Appendix

Add any additional relevant documentation, for example:

* Presentation files
* Lab documentation (screenshots, etc)