

HND CYBER SECURITY & NETWORKING

PROGRAMME	COMPUTING PORTFOLIO
MODULE	L4 - NETWORK AND CYBERSECURITY ESSENTIALS
ASSIGNMENT TITLE	ANALYSE THE NETWORKS & DISCUSS ITS SECURITY POSTURES
MODULE CODE	ACCA4024
LECTURER	MUNYARADZI N MURIRA
STUDENT	ORIN MCGINN
STUDENT NUMBER	2304621
DATE DUE	03/05/2024



TABLE OF CONTENTS

INTRODUCTION.....	3
PART 1 (A) - NIST CYBER SECURITY FRAMEWORK	4
PART 1 (B) - NMAP & WIRESHARK	6
PART 1 (C) - CYBER-ATTACKS AND MITIGATIONS STRATEGIES	7
PART 2 (A) - NETWORK TOPOLOGY – SECURE NETWORK	10
PART 2 (B) – HARDWARE AND SOFTWARE TOPOLOGIES	11
REFERENCE LIST	14



INTRODUCTION

In this cybersecurity report, I will talk about different types of malwares and what you should look out for and be careful of. I will also look at different phishing attacks and the NIST framework including what measures you can take to protect yourself online.

PART 1 (A) - NIST CYBER SECURITY FRAMEWORK

In today's digital landscape, cybersecurity has become a concern for individuals, businesses, and governments. With threats like data breaches, ransomware attacks, and identity theft, safeguarding digital assets and personal data has become critical. In this context, the National Institute of Standards and Technology (NIST) Cybersecurity Framework emerges as a crucial tool in achieving this dominant objective.

The NIST Cybersecurity Framework provides a comprehensive, risk-based approach to managing cybersecurity risks. It offers a flexible framework that can be adapted to various organisations regardless of size, sector, or cybersecurity maturity level. The framework is designed to help organisations effectively identify, protect, detect, respond to, and recover from cyber threats and incidents.

One of the primary ways the NIST Cybersecurity Framework contributes to safeguarding digital assets and personal data is by promoting a proactive approach to cybersecurity. Rather than merely reacting to cyber threats as they arise, the framework encourages organisations to take a systematic and risk-based approach to cybersecurity management. By conducting risk assessments and identifying potential vulnerabilities, organisations can implement appropriate controls and safeguards to mitigate risks before they materialise into security incidents.

Furthermore, it emphasises the importance of collaboration and information sharing within and across organisations. In today's interconnected ecosystem, no single entity can address cybersecurity challenges in isolation. The framework encourages organisations to collaborate with stakeholders, including government agencies, industry partners, and cybersecurity experts, to exchange threat intelligence, best practices, and lessons learned. By leveraging collective knowledge and resources, organisations can enhance their cybersecurity posture and better protect digital assets and personal data against evolving threats.

Another critical aspect of the Framework is its focus on continuous improvement. Cyber threats constantly evolve, and organisations must adapt their cybersecurity measures accordingly. The framework advocates for a cyclical process of assessing, planning, implementing, and monitoring cybersecurity controls, with a continuous feedback loop for refinement and optimisation. By continuously evaluating and updating their cybersecurity practices, organisations can stay ahead of emerging threats and better safeguard their digital assets and personal data over time.

Moreover, the NIST Cybersecurity Framework aligns with various regulatory requirements and industry standards, making it a valuable tool for compliance. Many regulatory frameworks, such as the General Data Protection Regulation and the Health Insurance Portability and Accountability Act, require organisations to implement robust cybersecurity measures to protect sensitive data. By adopting the NIST Cybersecurity Framework, organisations can demonstrate their commitment to cybersecurity best practices and ensure compliance with relevant regulations.



In conclusion, the NIST Cybersecurity Framework plays a vital role in achieving the dominant objective of safeguarding digital assets and personal data in today's society.

By providing a flexible, risk-based approach to cybersecurity management, promoting collaboration and information sharing, emphasising continuous improvement, and facilitating compliance with regulatory requirements, the framework equips organisations with the tools and strategies to mitigate cyber risks effectively. As cyber threats evolve, the NIST Cybersecurity Framework will remain essential for enhancing cybersecurity resilience and protecting critical assets in the digital age.

PART 1 (B) - NMAP & WIRESHARK

WIRESHARK

Wireshark is a network protocol analyser that captures and displays packets transmitted over a network. It allows for in-depth analysis of network traffic, which can be crucial during reconnaissance.

Packet Capture: Wireshark can capture packets flowing through a network interface, allowing an attacker to analyse the traffic to understand the network topology and communication patterns.

Protocol Analysis: Wireshark can dissect and analyse various network protocols, including HTTP, FTP, and SMTP. This can help attackers identify vulnerabilities or misconfigurations in-network services.

Traffic Filtering: Wireshark allows for the filtering of captured packets based on various criteria such as source/destination IP address, port numbers, protocol, etc., allowing attackers to focus on specific traffic of interest.

Malware Analysis: Wireshark can analyse network traffic for signs of malicious activity, such as command and control communications or data exfiltration.

NMAP

Nmap (Network Mapper) is a free open-source network discovery and security auditing tool. It's primarily used for scanning networks and identifying hosts, services, and open ports on a network.

Host Discovery: Nmap can identify live hosts on a network. It sends ICMP echo requests (ping) or TCP/UDP packets to discover active hosts.

Port Scanning: Nmap can perform various port scans to identify open ports on target systems. This information can help attackers identify potential entry points into the network.

Service Version Detection: Nmap can identify the version of services running on open ports, which can provide valuable information about potential vulnerabilities.

Operating System Detection: Nmap can attempt to identify the operating systems of target hosts based on subtle differences in how they respond to network probes.

PART 1 (C) - CYBER-ATTACKS AND MITIGATIONS STRATEGIES

EXPLAIN HOW MALWARE (WANNACRY & TELERAT) OPERATE

WannaCry, AKA EternalBlue, is a notorious ransomware that popped up around May 2017. Nobody overthought of it at first until it started to spread across the networks at a rapid pace. It was used to exploit a vulnerability within an unpatched version of the Windows XP OS, encrypting files and holding them for ransom payment only in Bitcoin. This ransomware would be more directed at Organisations because their computers ran older and outdated window XP systems. The patch that Windows came out with was updating all Windows systems and ensuring all computers were updated regularly. It also added a patch to stop WannaCry altogether. As of 7th of February 2023, windows has stopped supporting Windows XP altogether.

Mitigation Strategies for WannaCry.

Patch Management: Ensure all systems are regularly updated with the latest security patches the operating system vendor provides.

Network Segmentation: Segmenting networks can limit the spread of malware like WannaCry.

Security Awareness Training: Educate users about the dangers of phishing emails and suspicious attachments.

Backup and Recovery: Regularly back up important data and verify the integrity of those backups.

TeleRAT is a remote access trojan or RAT. That was known to target androids. Its attackers could remotely control the infected devices without the user's knowledge, stealing information, recording audio, taking photos, stealing data, sending premium-rate SMS messages and selling all this information on the black market.

The Mitigation Strategies for TeleRAT.

Download Apps from Trusted Sources: Only download apps from official app stores like Google Play Store, as they have security measures to detect and remove malicious apps.

Keep Software Updated: Regularly update your device's operating system and apps to patch known vulnerabilities.

Be Cautious of Links and Attachments: Avoid clicking on suspicious links or downloading attachments from unknown or untrusted sources.

Use Mobile Security Solutions: Install reputable mobile security apps that detect and remove malware from your device.



DESCRIBE IMPLEMENTATION OF PHISHING ATTACKS (WHALING & PHARMING)

Whaling is not typically a type of malware. Still, it is a specific form of phishing attack that targets high-profile individuals. "whaling" is derived from "phishing" for big fish, meaning targeting the most critical individuals. Whaling attacks are highly sophisticated and often involve extensive research on the targeted individual to craft convincing and personalised messages.

Mitigation Strategies for Whaling

Employee Training: Educate employees, especially high-profile individuals, about the risks of whaling attacks, and how to recognise suspicious emails. Provide training on best practices for email security, including verifying the sender identities and avoiding clicking on links or downloading attachments from unknown sources.

Multi-Factor

Authentication (MFA): Enable MFA for sensitive.

Accounts and systems to add an extra layer of security beyond passwords. Even if attackers obtain login credentials through phishing, MFA can help prevent unauthorised access.

Email Filtering: Use email filtering and spam detection solutions to automatically identify and block phishing emails before they reach users' inboxes. These solutions can analyse email content, attachments, and sender reputation to flag suspicious messages.

Incident Response Plan: Develop and regularly test an incident response plan for handling whaling attacks. Please ensure employees know how to report suspicious emails and respond appropriately if they have been targeted.

Pharming is a cyber-attack that redirects website traffic from legitimate websites to fraudulent ones. This can occur at the DNS (Domain Name System) level or by manipulating the host's file on a victim's device.

Mitigation Strategies for Pharming

Secure DNS Configuration: Ensure that DNS servers are correctly configured and regularly monitored for signs of tampering or unauthorised access.

Hosts File Protection: Protect the host's file on user devices to prevent unauthorised modification. Restrict access to the host's file to privileged users only and monitor for suspicious changes.



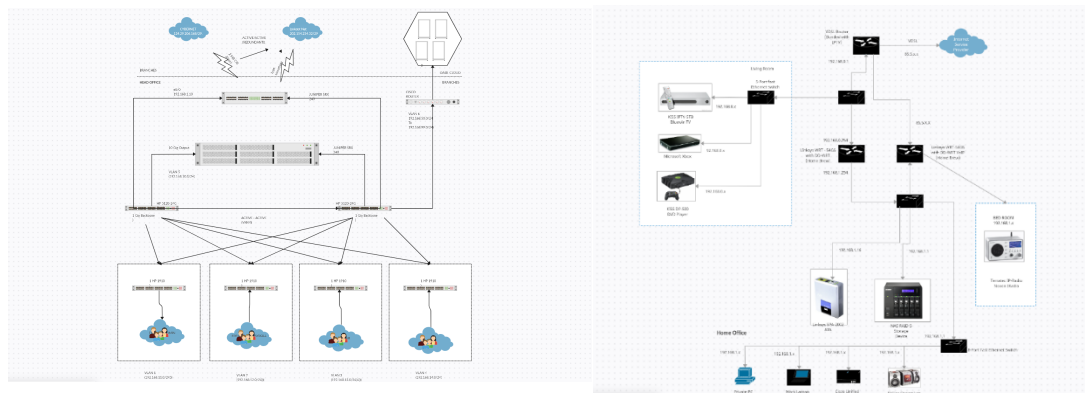
Use HTTPS: Encourage using HTTPS (Hypertext Transfer Protocol Secure) for website communication, which provides encryption and helps prevent man-in-the-middle attacks that could be used in phishing.

Network Monitoring: Implement network monitoring solutions to detect and block suspicious DNS requests or traffic patterns indicative of phishing attacks. Monitor for unauthorised changes to DNS settings or unusual network activity that may indicate a compromise.

Education and Awareness: Educate users about the risks of phishing attacks and how to recognise suspicious website behaviour. Encourage users to check for HTTPS encryption and verify website addresses before entering sensitive information.



PART 2 (A) - NETWORK TOPOLOGY – SECURE NETWORK



In this network topology designed for high availability, redundancy is implemented at critical layers to ensure continuous operation. Two Layer 3 switches are configured with Virtual Router Redundancy Protocol at the core layer to provide gateway redundancy. If one core switch fails, the other takes over seamlessly, minimising downtime.

In the distribution layer, redundant Layer 2/3 switches are connected to the core layer using EtherChannel for link aggregation and load balancing. This setup enhances network resilience and ensures traffic can be rerouted in case of a link failure.

Multiple Layer 2 switches connect end devices at the access layer, and EtherChannel is configured here for link redundancy and load distribution. The network topology optimises uptime and fault tolerance by implementing these redundancies and protocols, which are crucial for critical applications and business continuity. Testing and simulating failures validate the effectiveness of the design in providing high availability.

PART 2 (B) – HARDWARE AND SOFTWARE TOPOLOGIES

Enhancing network security during its operation requires a combination of software and hardware technologies to protect against various threats effectively. Here are some technologies, along with detailed explanations of their functionality:

Firewalls:

Hardware Firewalls: These are physical devices placed at the perimeter of a network, acting as gatekeepers between internal and external networks. They inspect incoming and outgoing traffic based on predetermined security rules. Hardware firewalls offer high performance and are particularly effective for protecting entire networks.

Software Firewalls: These are installed on individual devices, such as computers or servers, to control incoming and outgoing network traffic. Software firewalls provide granular control over specific applications and processes running on the device.

Cloud firewall: Cloud firewalls are deployed within the cloud infrastructure, protecting virtual machines, containers, and other cloud-based resources. They secure traffic between these resources, the internet and traffic between different components within the cloud environment.

Virtual Private Networks (VPNs):

Hardware VPNs: These are implemented using dedicated hardware appliances to encrypt and secure communication between remote users or branch offices and the leading corporate network. They ensure confidentiality and integrity of data transmitted over public networks.

Software VPNs: are software applications that create encrypted tunnels over the internet, allowing remote users to access the corporate network from anywhere securely. They provide flexibility and scalability compared to hardware VPNs.

Key Generation and Management: built-in key generation and management capabilities allow organisations to generate vital cryptographic keys and securely distribute them across the network. Key management features may include key rotation, key backup, key escrow, and key lifecycle management, ensuring that cryptographic keys are correctly managed throughout their lifecycle and reducing the risk of key compromise.



INTRODUCTION TO PACKET TRACER



Cisco Networking Academy

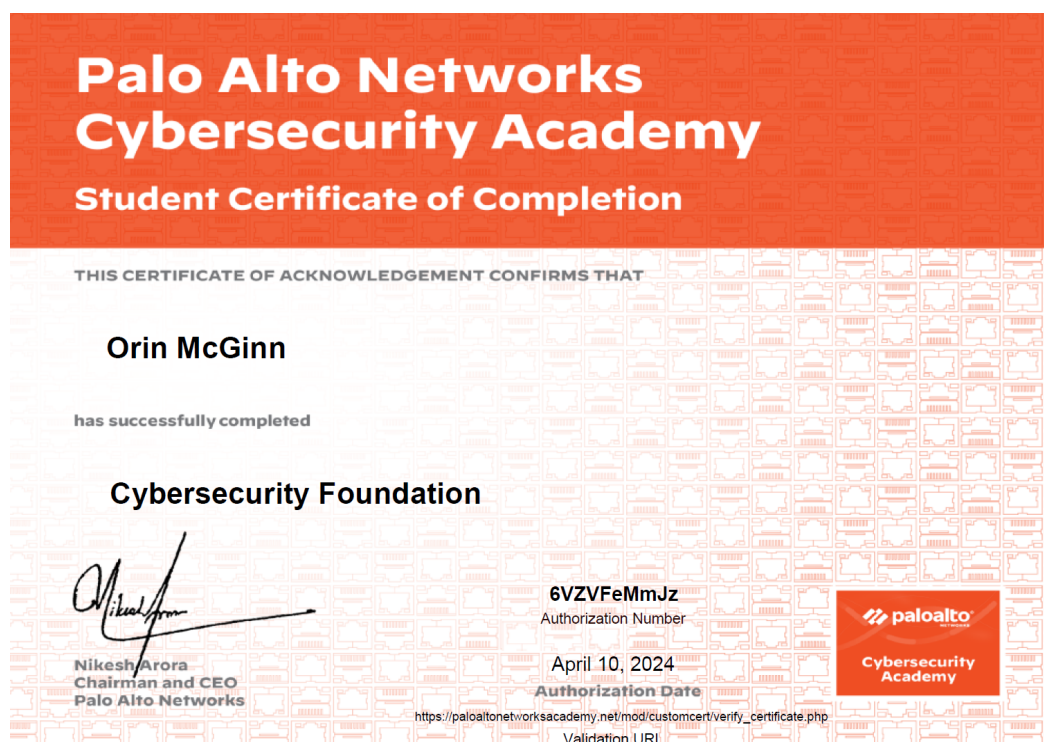
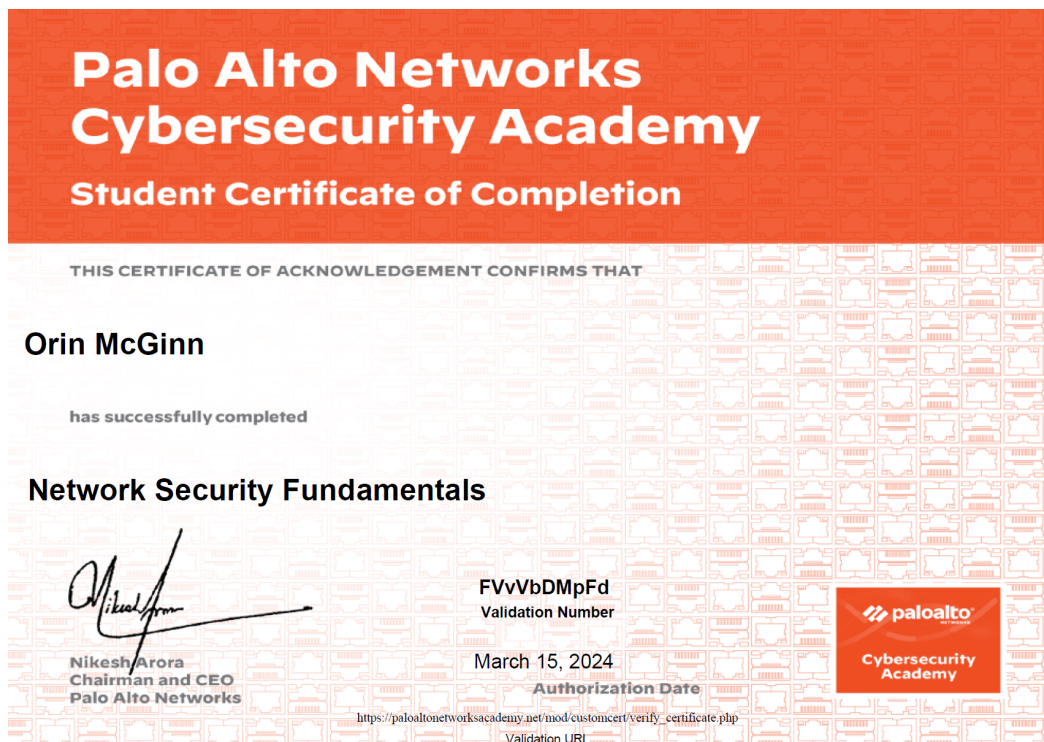
Introduction to Packet Tracer

For completing the Cisco Networking Academy® Introduction to Packet Tracer course.

Orin McGinn	
Student	
University of Wales Trinity Saint David	
Academy Name	
United Kingdom	6 Feb 2024
Location	Date
Munyaradzi Murira	
Instructor	Instructor Signature



PALO ALTO NETWORK SECURITY FUNDAMENTALS AND CYBER SECURITY FOUNDATION



REFERENCE LIST

I have consulted numerous online websites to conduct my research, these include

- YouTube
- Wikipedia
- Ted Talks
- Cisco
- Microsoft
- Palo Alto Networks
- Ubiquiti