

Assignment - Networks and Cyber Security Essentials

Ben Roberts (2205382)

Network and Cybersecurity Essentials (ACCA4024)

University of Wales Trinity Saint David – School of Applied Computing

Table of Contents

Abstract.....	4
Introduction.....	5
Part 1.....	6
Task A.....	6
Task B.....	7
Task C.....	8
Subtask 1.....	8
Subtask 2.....	8
Part 2.....	10
Task A.....	10
Task B.....	11
Subtask A.....	11
Subtask B.....	12
Conclusion.....	13
References.....	14

Table of Figures

Figure 1: Diagram showing the NIST Cybersecurity Framework [1].....6

Figure 2: Example high availability network layout produced in Packet Tracer.....10

Abstract

This document covers a variety of security practices and technologies, including but not limited to the NIST Cybersecurity Framework, the Cyber Kill Chain, mitigation strategies against particular kinds of phishing attacks, high availability network design and specific hardware and software technologies that can be used to secure a network.

Introduction

This report explores the importance of safeguarding digital assets and personal data against potential cyber attacks.

Part 1 covers optimal practices and mitigation strategies against certain attacks, while Part 2 includes an example of a network focused on high availability as well as discussion on certain kinds of cybersecurity technologies.

Part 1

Task A

The NIST Cybersecurity Framework (CSF) is a series of official guidelines published by the US National Institute of Standards and Technology (NIST) which, as stated by the official document published by NIST “provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks” and is designed to be used by all kinds organisations in every sector regardless of size [1]. While following it is optional, the purpose of the NIST Cybersecurity Framework is to assist businesses with reducing the risk of cyber attacks as well as improving their general cybersecurity infrastructure [2].

The NIST Cybersecurity Framework is made up of six core functions – Govern (establishing risk management strategies and protocols for cybersecurity), Identify (understanding an organisation’s cybersecurity risks), Protect (implementing safeguards to minimise any cybersecurity risks), Detect (analysis of potential threats and compromises), Respond (necessary actions to undertake in the event of an attack) and Recover (the process of restoring operations and assets which are affected). [1]

For example, in the Identify stage an organisation could collect information about all computing devices in its inventory and establish what their purposes are, then in the Protect stage the organisation could require the encryption of every file on their computers and have all data be backed up onto a magnetic tape cartridge at the end of the week to provide a safeguard against potential system corruption and ransomware attacks. In the Detect stage, an organisation could require that network-wide scanning be undertaken to locate intrusion, then in the Respond stage the organisation could require that an organisation-wide password change in the event of an intrusion. Finally, the organisation could require that after an attack any affected data must be restored from a tape backup.



Figure 1: Diagram showing the NIST Cybersecurity Framework [1]

Because every organisation has different requirements, there is no single implementation of the NIST Cybersecurity Framework. Instead, each organisation that follows the NIST

Cybersecurity Framework tailors a CSF profile specifically to their organisation. As per the documentation, using an organisational profile is composed of 5 steps:

1. Establish the scope of the organisation-specific profile
2. Gather any information that is required for assembling the organisation-specific profile
3. Create the initial draft of the organisational profile
4. Analyse any gaps within the profile and create a plan of action
5. Implement the plan of action and update the organisational profile based on the previous analysis

To further assist organisations with improving their security infrastructure, a variety of “CSF community profiles” are available to provide organisations with a template that can be used as a basis for forming their own profiles [3].

Task B

The Cyber Kill Chain is a model of the process used by cyber criminals during the process of system intrusion. It is used to “develop threat intelligence about attackers’ Tactics, Techniques and Procedures [4]”. The cyber kill chain is made up of seven stages: Reconnaissance (collecting information about the target), Weaponisation (configuring the attack vector for the purposes of intrusion), Delivery (sending the attack vector), Exploitation (exploiting the attack vector to infiltrate the system), Installation (installing any necessary payloads to hack the target’s system), Command and Control (gaining control over the system via the aforementioned payloads) and Actions on Objectives (performing any actions necessary after gaining control) [4]

As the reconnaissance stage of the cyber kill chain involves the attacker looking into their target to find any potential security issues which could be used to infiltrate the target’s systems, hackers will utilise a variety of software tools in order to locate any potential entry points. One of these tools which can be utilised by attackers to locate potential endpoints on a network is Nmap, which is a program which returns information about devices connected to a network [5]. Attackers will use Nmap to search a network for unsecured devices such as smart appliances which can serve as entry points into the network.

Another tool utilised by attackers to search for potential exploits is Wireshark, which is a network protocol analyser that scans and decrypts data packets which have been sent across a network [6]. An attacker may potentially utilise Wireshark or a similar utility in order to collect information such as login credentials that can be used to compromise a potentially insecure device.

Task C

Subtask 1

WannaCry was a computer worm and ransomware program that was used in a series of attacks in 2017, most notably against the NHS [4]. It utilised a security exploit in the Microsoft Windows operating system called EternalBlue that was leaked from the NSA [7]. EternalBlue utilises a vulnerability in the Server Message Block version 1.0 filesharing protocol to deliver a backdoor program called DoublePulsar [8] which then enables the installation of a computer worm that infects the victim's computer with a ransomware program [9]. The worm then spreads to and infects other computers connected to the same network [8]. Upon infecting a computer, WannaCry encrypts the target's files and demands a ransom in Bitcoin worth \$300 USD, with the victim being promised a decryption key if they pay within 7 days. The program also claims that if the victim does not pay within the allotted time then the decryption key will be destroyed [7].

TeleRAT is a trojan horse program that affects Android devices by utilising a security issue with the popular Telegram instant messaging client which was first discovered in 2017 [10]. TeleRAT works by exploiting a vulnerability in Telegram's bot account API [11]. Once it has infected a device, the remote access trojan collects a variety of information about the victim (such as SMS history and contact information), which it then sends back to a remote server.

The primary difference between WannaCry and TeleRAT is that WannaCry targets personal computers running Microsoft Windows, while TeleRAT targets mobile phones that run the Android operating system. What WannaCry and TeleRAT had in common however was that they were both frequently delivered using phishing scams.

Therefore, both kinds of malware can potentially be mitigated by implementing protections against phishing. Methods can include implementing an anti-phishing system such as a program that filters suspicious messages and/or URLs, using a model and/or framework of previous phishing attacks to train a phishing detection algorithm and training individuals to recognise and avoid phishing scams [12]. Additionally, the use of malware-detection software can help to reduce the risk of malware attacks [13]. Finally, making sure that all systems are fully up to date can ensure that the latest security patches have been installed [14].

Subtask 2

Phishing is a cyber attack that utilises social engineering to trick a victim into accessing the attack vector, usually with the intention of harvesting personal information [15]. Whaling and Pharming are both variations of the standard phishing attack.

Pharming attacks work by subverting the domain name system (DNS) and relocating the direction of a domain name to a different server. This means that the victim will be under the assumption that they have accessed a legitimate website that they are familiar with. Ways of redirecting the web addresses include DNS spoofing (which involves corrupting a

DNS database to redirect a mapped IP address [16]) and installing malware that silently redirects the user's traffic to a fraudulent website, where the user is then tricked into entering sensitive data. Pharming attacks can be mitigated by properly securing the DNS connection in a way that can be harder to manipulate. For example, changing the login credentials for a wireless access point from the default to something else will mean that an attacker will not be able to immediately break into the access point to corrupt the DNS system. Additionally, making sure that the computer is connected to a legitimate DNS service can ensure that the connection is not redirected to an unsafe site. Finally, using anti-malware software can detect any malware that is redirecting web connections, thus alerting the user to any potential risks.

Whaling is yet another kind of phishing attack that specifically targets high-level individuals within an organisation such as finance, human resources and chief executive officers. Unlike standard phishing attacks and pharming, which tend to be more general, whaling attacks are often personalised to the target and are usually designed to acquire large amounts of money and/or very specific information such as employee data and trade secrets. As whaling attacks target a very specific individual, the attacker must research their target to properly pull off the attack. This also means that the attempts to impersonate a legitimate source will often be far more sophisticated than a standard phishing attack. For example, a whaling attack may appear as a request from a business partner or an individual even higher up within the organisation than the target and will be worded specifically to appear benign to the target. One method of mitigating a whaling attack would be to confirm with whoever is being impersonated whether or not the request is legitimate. [17]

Part 2

Task A

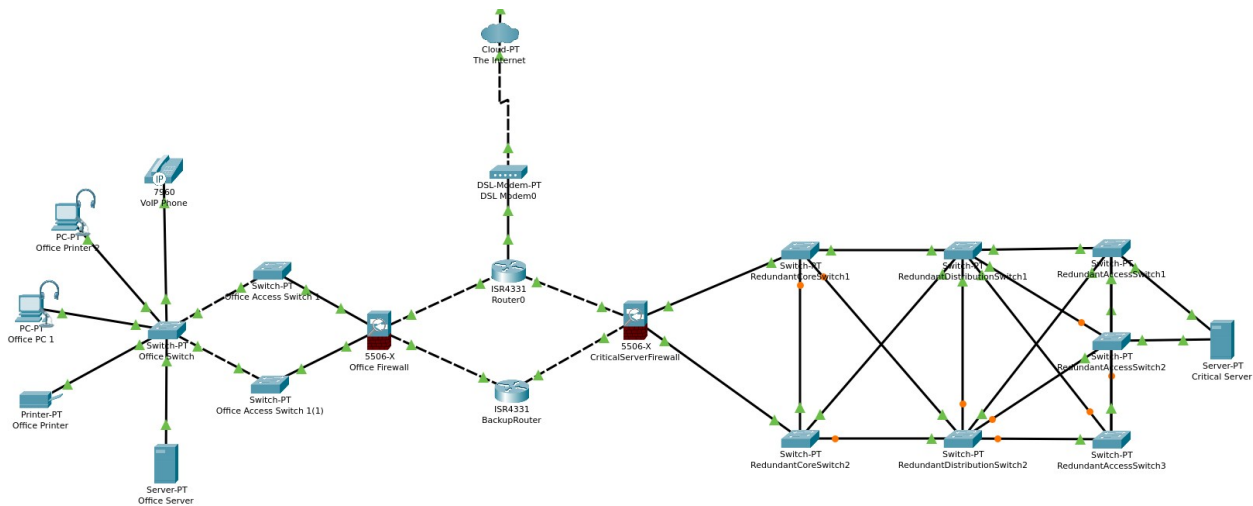


Figure 2: Example high availability network layout produced in Packet Tracer

High availability networking is a method of constructing a network to account for the lowest possible downtime. These networks are commonly achieved by using redundant equipment which is intelligently rerouted if a connection fails [18].

The pictured network is split into two LANs, each with separate firewalls. One LAN is to connect an office, while the other is used to route a critical server. This server utilises multiple network cards and has a variety of switches that it automatically routes through to ensure maximum availability. There are also two routers which connect both networks together.

However, as the modem only has one Ethernet connector, the backup router will not be able to access the internet. It does however still provide access to the mission critical server for debugging purposes and the modem can be manually reconnected to the backup router if necessary.

Task B

There are a variety of hardware and software technologies which can be implemented to secure a network. One of those technologies is a firewall, which is available in both hardware and software forms. The purpose of a firewall is to enforce a network's security policy by monitoring incoming and outgoing packets and filter out any malicious and/or unauthorised packets [19]. Firewalls can be configured to permit or deny certain packets based on specific requirements. For this reason, a firewall is best placed at the point at which the network intersects with the internet.

Another method of including security would be to use a data loss prevention system, such as automated backup servers. Data loss preventions systems can help with regulatory compliance and reporting breaches [20]. Because data loss can harm an organisation's reputation and may result in potential lawsuits, an organisation must use the method that is most suitable for it [21]. One method of preventing data loss is to configure all computers on the network to automatically copy all relevant data onto another server (possibly using lossless compression). It is also possible to copy compressed data onto another backup solution, such as optical discs or magnetic tape, for the purposes of long term storage. Since a physical backup solution may not be online, it is also harder for the data to be accessed without authorisation or physical access.

Subtask A

Introduction to Packet Tracer

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

Ben Roberts

Student

University of Wales Trinity Saint David

Academy Name

United Kingdom

Location

22 Feb 2024

Date

Munyaradzi Murira

Instructor

Instructor Signature

Subtask B

Palo Alto Networks Cybersecurity Academy

Student Certificate of Completion

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

Ben Roberts

has successfully completed

Network Security Fundamentals



Nikesh Arora
Chairman and CEO
Palo Alto Networks

ZeTBvU1wXE
Validation Number

December 13, 2022

Authorization Date

https://paloaltonetworksacademy.net/mod/customcert/verify_certificate.php

Validation URL



Conclusion

In conclusion, this document discussed a variety of techniques for improving the security and reliability of networks, including the NIST Cybersecurity Framework, the Cyber Kill Chain, malware mitigation strategies, mitigation strategies for a variety of phishing attacks and high availability networking. All of this can be used to ensure a fully secured network.

Despite these improvements security, it is vital that organisations and individuals stay up to date with security practices and technologies to protect against new threats.

References

- [1] G. M. Nist, ‘The NIST Cybersecurity Framework 2.0’, National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, 2023. doi: 10.6028/NIST.CSWP.29.
- [2] ‘Understanding the NIST cybersecurity framework’, Federal Trade Commission. Accessed: Jun. 18, 2024. [Online]. Available: <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework>
- [3] C. Pascoe, J. Nethery Snyder, and K. Scarfone, ‘A Guide to Creating CSF 2.0 Community Profiles’, National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 32 ipd, Feb. 2024. doi: 10.6028/NIST.CSWP.32.ipd.
- [4] T. Dargahi, A. Dehghantanha, P. N. Bahrami, M. Conti, G. Bianchi, and L. Benedetto, ‘A Cyber-Kill-Chain based taxonomy of crypto-ransomware features’, *J. Comput. Virol. Hacking Tech.*, vol. 15, no. 4, pp. 277–305, Dec. 2019, doi: 10.1007/s11416-019-00338-7.
- [5] ‘Chapter 15. Nmap Reference Guide | Nmap Network Scanning’. Accessed: Jun. 17, 2024. [Online]. Available: <https://nmap.org/book/man.html>
- [6] ‘Wireshark · About’, Wireshark. Accessed: Jun. 18, 2024. [Online]. Available: <http://localhost:3000/about.html>
- [7] ‘The WannaCry ransomware attack’, *Strateg. Comments*, vol. 23, no. 4, pp. vii–ix, 2017, doi: 10.1080/13567888.2017.1335101.
- [8] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, ‘Ransomware detection and mitigation using software-defined networking: The case of WannaCry’, *Comput. Electr. Eng.*, vol. 76, pp. 111–121, Jun. 2019, doi: 10.1016/j.compeleceng.2019.03.012.
- [9] Z. Liu, ‘Working mechanism of Eternalblue and its application in ransomworm’, *arXiv.org*, Dec. 2021, Accessed: Jun. 19, 2024. [Online]. Available: <https://www.proquest.com/docview/2616149293/abstract/7DC185E6BC434A30PQ/1?sourcetype=Working%20Papers>
- [10] V. Valeros and S. Garcia, ‘Growth and Commoditization of Remote Access Trojans’, in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Sep. 2020, pp. 454–462. doi: 10.1109/EuroSPW51379.2020.00067.
- [11] R. N. Wilhoit Kyle, ‘TeleRAT: Another Android Trojan Leveraging Telegram’s Bot API to Target Iranian Users’, Unit 42. Accessed: Jun. 19, 2024. [Online]. Available: <https://unit42.paloaltonetworks.com/unit42-telerat-another-android-trojan-leveraging-telegrams-bot-api-to-target-iranian-users/>
- [12] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, ‘Mitigation strategies against the phishing attacks: A systematic literature review’, *Comput. Secur.*, vol. 132, pp. 103387–, 2023, doi: 10.1016/j.cose.2023.103387.
- [13] Z. Zhao, J. Wang, and J. Bai, ‘Malware detection method based on the control-flow construct feature of software’, *IET Inf. Secur.*, vol. 8, no. 1, pp. 18–24, Jan. 2014.
- [14] ‘Mitigating malware and ransomware attacks’. Accessed: Jun. 22, 2023. [Online]. Available: <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>
- [15] C. Karlof, U. Shankar, J. D. Tygar, and D. Wagner, ‘Dynamic pharming attacks and locked same-origin policies for web browsers’, in *Proceedings of the 14th ACM conference on Computer and communications security*, Alexandria Virginia USA: ACM, Oct. 2007, pp. 58–71. doi: 10.1145/1315245.1315254.
- [16] S. A. Samarakoon, ‘Bypassing Content-based internet packages with an SSL/TLS Tunnel, SNI Spoofing, and DNS spoofing’, *arXiv.org*, Dec. 2022, Accessed: Jun. 24, 2024. [Online]. Available: <https://www.proquest.com/docview/2753896832?parentSessionId=1LAGqTr2kHh1ghyN%2FiIzRyHNTlvaDo51YF0VhkNNbyA%3D&pq-origsite=primo&sourcetype=Working%20Papers>

- [17] D. Pienta, J. B. Thatcher, and A. Johnston, ‘Protecting a whale in a sea of phish’, *J. Inf. Technol.*, vol. 35, no. 3, pp. 214–231, 2020, doi: 10.1177/0268396220918594.
- [18] K. Jørgen Hole, *Anti-fragile ICT Systems*. Springer Nature, 2016. doi: 10.1007/978-3-319-30070-2.
- [19] Kinsey Denise and Stewart James Michael, *Network security, firewalls, and VPNs.*, Third edition. Burlington, Massachusetts: Jones & Bartlett Learning, 2021.
- [20] L. Arbel, ‘Data loss prevention: the business case’, *Comput. Fraud Secur.*, vol. 2015, no. 5, pp. 13–16, 2015, doi: 10.1016/S1361-3723(15)30037-3.
- [21] S. Liu and R. Kuhn, ‘Data Loss Prevention’, *IT Prof.*, vol. 12, no. 2, pp. 10–13, Mar. 2010, doi: 10.1109/MITP.2010.52.