

Assessment

Zsolt Gyongyosi, 2227989

May 2024

Contents

1	Abstract	2
2	Introduction	2
3	Part 1a	3
4	Part 1b	4
5	Part 1c	4
6	Part 2 a	7
7	Part 2 b	7
8	Part 2 b i	8
9	Part 2 b ii	8
10	Future Work	11

1 Abstract

This coursework explores the field of cybersecurity, focusing on the difficulties presented by online threats like malware and phishing scams, as well as the tactical significance of strong network architecture to guarantee high availability. Understanding and countering threats like TeleRAT and the WannaCry ransomware, as well as advanced phishing tactics like Whaling and Pharming, are the main priorities. This assesment offers a thorough security plan that incorporates the use of cutting-edge hardware and software, including firewalls, intrusion detection systems, virtual private networks, and network access control systems, to counter these threats. Furthermore, a secure network architecture is described, with a focus on removing single points of failure and using trustworthy crossover methods. The proposals place a strong emphasis on the value of increased user education, frequent updates, and investments in cutting-edge security solutions. The conclusion emphasises the necessity of ongoing security practice improvement to stay up with changing cyberthreats and makes recommendations for future research areas in the application of cutting-edge cybersecurity technologies. This all-encompassing strategy improves network infrastructures' overall resilience against potential cyberattacks in addition to addressing present vulnerabilities.

2 Introduction

The security of information systems and networks is of utmost importance in the current digital age. The growing dependence on digital platforms in many industries has coincided with a rise in cyber threats that exploit weaknesses inside these systems. The dangers encompass a wide spectrum, including malware attacks like ransomware and Remote Access Trojans (RATs), as well as advanced phishing methods such as Whaling and Pharming. Each of these attacks carries substantial dangers, endangering not just the security of sensitive information but also the reliability and accessibility of vital infrastructure.

This coursework explores into the field of cybersecurity, with a specific focus on comprehending the operational mechanics of particular cyber threats and developing efficient tactics to counteract them. This assessment investigates the characteristics of prominent malware assaults, especially WannaCry and TeleRAT, and analyses the intricacies of sophisticated phishing attacks. The study highlights critical weaknesses targeted by hackers and presents a strategic framework for network architecture that emphasises strong defence measures and uninterrupted availability.

This assessment seeks to demonstrate the efficacy of comprehensive security frameworks and state-of-the-art technology in strengthening digital environments by combining theoretical knowledge with actual applications. Furthermore the assessment aims to provide practical insights and solutions that organisations can implement to improve their cybersecurity position in response to changing cyber threats.

3 Part 1a

The NIST Cybersecurity Framework (CSF) is an essential tool in the ever-changing domain of cybersecurity. Created by the National Institute of Standards and Technology, this resource provides organisations with optimal methods, recommendations, and criteria for efficiently controlling and reducing cybersecurity threats. The significance of the framework is emphasised by the changing difficulties and possibilities in cybersecurity, serving as a crucial factor in protecting digital resources and personal information. [1]

1. **Thorough Risk Management:** The CSF is structured based on five fundamental functions—Identify, Protect, Detect, Respond, and Recover. This framework facilitates organisations in effectively managing cyber threats by implementing proactive and reactive cybersecurity solutions. The Identify function is essential for detecting vulnerabilities that attackers exploit during the reconnaissance phase of the cyber death chain.
2. **Adaptable and Expandable:** The CSF’s versatility enables it to be adjusted to suit any organisation, irrespective of its size or intricacy. The capacity to adapt is crucial in a profession where threats are continually changing, allowing for customised security measures that are adapted to the organization’s requirements and the types of data being safeguarded.
3. **Strengthening Preemptive and Protective Abilities:** Cybercriminals exploit vulnerabilities utilising customised tools during the weaponization and delivery stages of an attack. The Protect and Detect capabilities of the CSF enable organisations to enhance their defences and proactively monitor for breaches. These features prioritise strong access control, data encryption, and ongoing monitoring to potentially prevent assaults before they result in substantial harm.
4. **Incident Response and Recovery:** Following a cyber assault, the functions of responding and recovering are of utmost importance. They offer a systematic method for handling the consequences of assaults, assisting organisations in containing incidents, and enabling quick and secure recovery. These functions also emphasise the significance of effective communication within the organisation and with external stakeholders, ensuring trust and openness.[2]
5. **Ongoing Enhancement:** The CSF facilitates an iterative approach, promoting frequent evaluations and revisions of cybersecurity protocols in order to address emerging threats. This is consistent with the ever-changing nature of cybersecurity, where the panorama of threats and technologies is constantly growing.

Ultimately, the NIST Cybersecurity Framework is essential for every organisation seeking to safeguard its digital resources and personal information. The broad and adaptive nature of this tool makes it an essential component in protecting against cyber threats and strengthening cybersecurity resilience in contemporary society.[3]

4 Part 1b

Nmap and Wireshark are robust tools extensively utilised in the field of cybersecurity, particularly in the initial phase of the cyber kill chain known as reconnaissance. This phase is crucial for attackers to collect knowledge on their targets, aiding in the identification of weaknesses and points of access.

Nmap, also known as Network Mapper, is a powerful network scanning application used to identify hosts and services within a computer network. Attackers can utilise this tool to determine the availability of hosts on the network, the specific services being offered by those hosts (including the application name and version), the operating systems and their respective versions, as well as the type of packet filters or firewalls being employed. For instance, a malicious individual may utilise Nmap to do a port scan on a specific network in order to ascertain the status of its ports, whether they are open, closed, or filtered. This information can identify potential weak spots where particular services are operating that can be manipulated.[4]

Wireshark is a network protocol analyzer that allows users to record and examine the traffic on a computer network in an interactive manner. The tool has the capability to break down the information from numerous protocols and is capable of analysing the data that flows through a network, encompassing activities such as internet usage, email, and chat messaging. Attackers employ Wireshark to intercept packets in real-time and subsequently scrutinise them to extract confidential data. For example, if the network uses unencrypted protocols, an assailant could employ Wireshark to intercept login credentials being communicated over the network, or to comprehend the network's configuration and traffic patterns, so facilitating the planning of further attacks.

Both tools, although commonly utilised by cybersecurity professionals for legal network administration and troubleshooting purposes, can also be exploited by hackers to acquire comprehensive information about a specific target. Cybercriminals might use the knowledge obtained by Nmap and Wireshark to better customise their future assaults, taking advantage of specific vulnerabilities they have discovered in the target's network configuration.[5]

5 Part 1c

- **Analysis and Countermeasures for WannaCry and TeleRAT**

WannaCry is a type of malicious software attack known as ransomware, which takes use of weaknesses in older versions of the Windows operating system. The malware employs encryption algorithms to secure files on the compromised machine and then extorts a payment in the form of Bitcoin in exchange for the decryption key. WannaCry propagates over networks by exploiting the EternalBlue vulnerability, specifically targeting the Windows Server Message Block (SMB) protocol.

Ways to Reduce the Impact of WannaCry:

- (a) **Patch Management:** Consistently update and apply patches to operating systems in order to address vulnerabilities that could be exploited by ransomware. To prevent the exploitation of the SMB protocol, it is necessary to install the MS17-010 patch provided by Microsoft.
- (b) **Data Backup:** Establish a routine for backing up data and be sure to keep it offline or on a separate network. Implementing this strategy can mitigate the consequences of data loss caused by ransomware.
- (c) **Security Awareness:** Educate personnel on identifying and avoiding dubious emails and URLs that may disseminate ransomware.

TeleRAT is a Remote Access Trojan (RAT) that commonly disguises itself as a genuine application and is mostly spread using social engineering methods. Attackers can utilise this to gain remote control over the compromised device, extract valuable data, and even exploit the device's camera and microphone.[6]

Mitigation Strategies for TeleRAT:

- **Endpoint Protection:** Employ resilient antivirus software and ensure its regular updates to identify and eliminate dangerous programmes.
- **Application Control:** Implement measures to prevent users from installing unauthorised applications, hence reducing the likelihood of unintentionally installing Trojans.
- **User Education:** Provide users with information regarding the potential hazards associated with downloading and installing software from unknown sources or clicking on links in unwanted emails.

● **Whaling and Pharming: Implementation and Mitigation Strategies**

Whaling attacks are focused on high level executives and employ sophisticated phishing techniques that try to obtain confidential information. These assaults frequently employ email or other electronic communication means, masquerading as a genuine source and soliciting confidential firm information.

Whaling Mitigation Strategies:

- **Email Verification Tools:** Integrate tools that can assist in authenticating the origin of emails, such as DMARC (Domain-based Message Authentication, Reporting and Conformance) and SPF (Sender Policy Framework).
- **2. Executive Training:** Deliver targeted training sessions to executives regarding the characteristics of these attacks and methods to identify them.
- **Verification Procedures:** Implement internal procedures to verify requests for sensitive information, particularly those received through email exchanges.

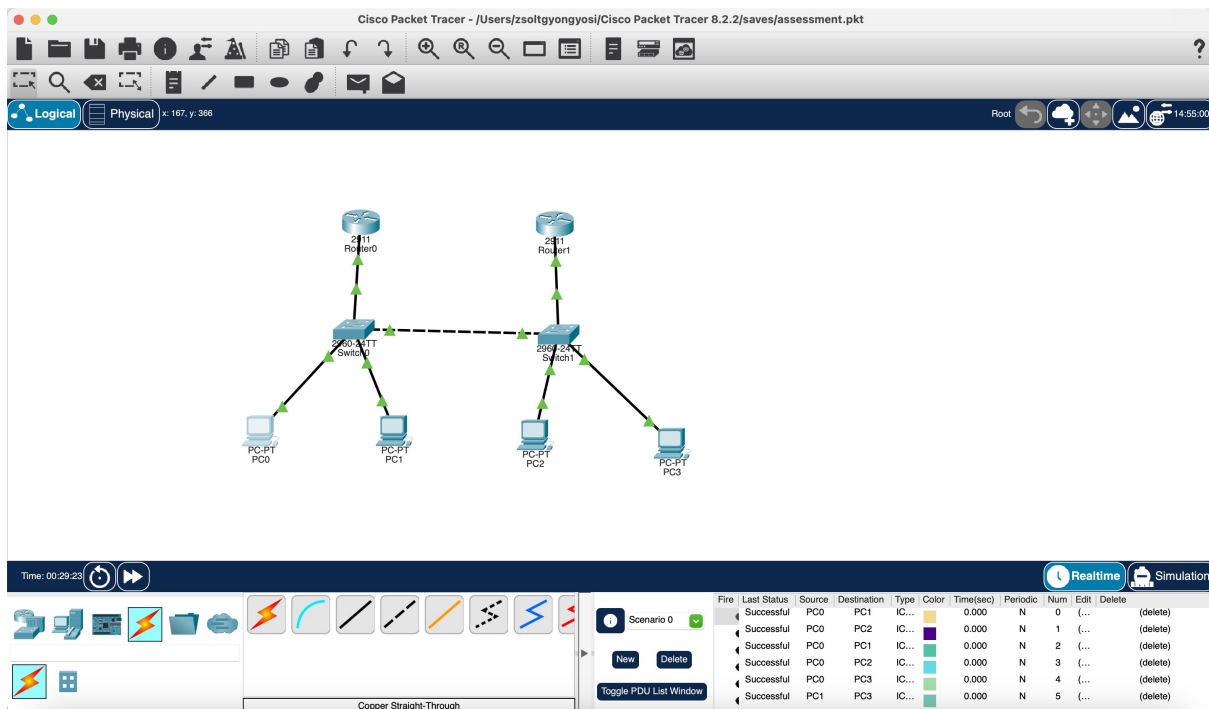
Pharming is a technique that involves redirecting people from genuine websites to deceptive ones in order to unlawfully obtain personal information such as usernames, passwords, and credit card numbers. This is commonly accomplished by taking advantage of weaknesses in DNS (Domain Name System) servers.

Mitigation Strategies for Pharming:

- (a) **Implementing Secure DNS Practices:** Employing DNS security extensions such as DNSSEC to safeguard DNS lookups against unauthorised alterations.
- (b) **Routine Audits:** Conduct periodic security audits on network and DNS setups to verify the absence of any vulnerabilities that could be potentially exploited.
- (c) **SSL Certificates:** Users should be encouraged to verify the presence of SSL certificates on websites (https) in order to confirm the site's validity.

To effectively mitigate the related risks of each cyber-attack, a strategic approach is necessary. This approach should involve a combination of technology solutions, process modifications, and user education.[7]

6 Part 2 a



The suggested network guarantees high availability through the implementation of redundancy across routers and switches. The Hot Standby Router Protocol (HSRP) is utilised to establish a configuration between two routers. In the event of a failure of the primary router, the secondary router seamlessly assumes control, ensuring continuous network connectivity. The purpose of enabling the Spanning Tree Protocol (STP) on switches is to prevent the occurrence of loops and to guarantee the presence of an alternative channel in case a link becomes unavailable. Cisco Packet Tracer allows for the configuration of routers using HSRP, while switches utilise default STP settings. This ensures uninterrupted communication between devices, even in the event of partial network failures. This configuration efficiently eliminates any individual components or systems that could cause the entire network to fail, and guarantees a dependable network connection between different networks.

7 Part 2 b

In order to improve network security when it is functioning, it is imperative to incorporate both hardware and software solutions. Here is a brief overview of fundamental technologies:

Firewalls, both in hardware and software, are used to regulate the flow of data between secure internal networks and potentially unsafe external networks by enforcing established security protocols. Hardware firewalls offer network-wide protection, whereas software firewalls offer customised security for specific devices. **Premise:** All network traffic is required to traverse firewalls in order to undergo comprehensive analysis in accordance with security regulations.[6]

Intrusion Detection and Prevention Systems (IDPS): IDPS oversee network

traffic to identify potentially harmful activity. Intrusion Detection Systems (IDS) identify and recognise threats by comparing them to established patterns, whereas Intrusion Prevention Systems (IPS) take proactive measures to obstruct possible threats. **Premise:** Ongoing updates to Intrusion Detection and Prevention System (IDPS) databases are necessary because of the ever-changing nature of network threats.

Virtual Private Network (VPN): VPNs employ encryption to safeguard the integrity of internet connections and preserve the anonymity of users. This is particularly important for distant access, where the security of the access sites may be compromised.

Network Access Control (NAC) is a security measure that implements policies based on user identification and device health. Its purpose is to allow only compliant devices to connect to the network. The underlying assumption is that devices may be hacked, which might potentially jeopardise the integrity of the network.[8]

These technologies collectively offer a strong framework for safeguarding networks from external threats and unauthorised access.

8 Part 2 b i

Introduction to Packet Tracer Certification digital key

 Corporate Social Responsibility Certificate of Course Completion		Cisco Networking Academy	
Introduction to Packet Tracer			
For completing the Cisco Networking Academy® Introduction to Packet Tracer course.			
Zsolt Gyongyosi			
Student			
University of Wales Trinity Saint David			
Academy Name			
United Kingdom		12 Feb 2024	
Location		Date	
Munyaradzi Murira			
Instructor		Instructor Signature	

9 Part 2 b ii

Palo Alto Network Security Fundamentals

Palo Alto Networks Cybersecurity Academy

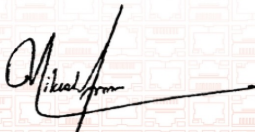
Student Certificate of Completion

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

Zsolt Gyongyosi

has successfully completed

Network Security Fundamentals



Nikesh Arora
Chairman and CEO
Palo Alto Networks

MjHZnIPiWf
Validation Number

March 13, 2024

Authorization Date

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

Validation URL



Palo Alto Networks Cybersecurity Academy

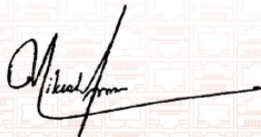
Student Certificate of Completion

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

Zsolt Gyongyosi

has successfully completed

Cybersecurity Foundation



Nikesh Arora
Chairman and CEO
Palo Alto Networks

SKOK34PBcV

Authorization Number

April 27, 2024

Authorization Date

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

Validation URL



10 Future Work

Future research should focus on:

Explore developing cybersecurity technologies, such as artificial intelligence and machine learning, to create security systems that are more flexible and responsive.

Analysis of Security Investments using quantitative methods: Perform research to measure the return on investment (ROI) of cybersecurity efforts, assisting organisations in making well-informed choices regarding their expenditure on security.

Conduct longitudinal studies to monitor the development of attack patterns and evaluate the efficacy of different cybersecurity measures over a period of time. This will facilitate comprehension of the enduring patterns and efficacy of various security solutions.

This paradigm not only assists in tackling present cybersecurity difficulties but also establishes the foundation for predicting future dangers and possibilities in the constantly changing field of cybersecurity.

References

- [1] G. F. Lyon, *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure, 2009.
- [2] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar, and T. Baker, “Security threats to critical infrastructure: the human factor,” *The Journal of Supercomputing*, vol. 74, pp. 4986–5002, 2018.
- [3] P. E. Williams-Banta, *Security technology and awareness training; do they affect behaviors and thus reduce breaches?* PhD thesis, Northcentral University, 2019.
- [4] C. Hadnagy and M. Fincher, *Phishing dark waters: The offensive and defensive sides of malicious Emails*. John Wiley & Sons, 2015.
- [5] M. Villareal, “Phishing: Improving organizational cybersecurity awareness,” 2020.
- [6] W. Stallings and L. Brown, *Computer security: principles and practice*. Pearson, 2015.
- [7] A. Greenberg, *Sandworm: A new era of cyberwar and the hunt for the Kremlin’s most dangerous hackers*. Anchor, 2019.
- [8] K. Scarfone, P. Mell, *et al.*, “Guide to intrusion detection and prevention systems (idps),” *NIST special publication*, vol. 800, no. 2007, p. 94, 2007.