



---

# ASSIGNMENT 1

---

7809ICT – Offensive Cyber Security



MUHAMMAD HAMZA ASLAM  
SAMUEL ZAVUGA  
SHEHRYAR MALLICK  
MONA YADI

S5348038  
S5307726  
S5328488  
S5273500

## Contents

1. Executive Summary: .....	2
2. Statement Of Individual Contribution: .....	3
2.1. Muhammad Hamza Aslam - S5348038 – 192.168.34.161 .....	3
2.2. Samuel Zavuga – S5307726 – 192.168.34.251 .....	3
2.3. Shehryar Mallick – S5328488 – 192.168.34.241.....	3
2.4. Mona Yadi – S5273500 – 192.168.34.52.....	4
3. Comprehensive Analysis: Open Ports, Services, and Operating Systems for Each Host: .....	5
4. Network Map Of The Network: .....	6
5. Flags Description: .....	6
6. Analysis And Recommendations On Network Protection: .....	9
6.1. Host: 192.168.24.52: .....	9
6.1.A. Analysis: .....	9
6.1.B. Recommendation: .....	9
6.2. Host: 192.168.24.161: .....	9
6.2.A. Analysis: .....	9
6.2.B. Recommendation: .....	9
6.3. Host: 192.168.24.251: .....	10
6.3.A. Analysis: .....	10
6.3.B. Recommendation: .....	10
6.4. Host: 192.168.24.241: .....	10
6.4.A. Analysis: .....	10
6.4.B. Recommendation: .....	10
7. References: .....	12

# **1. Executive Summary:**

This report provides a detailed analysis of the network security penetration testing conducted to evaluate the security status of the specified network infrastructure. The primary goal of this report is to identify vulnerabilities within the network, exploit them, and offer recommendations to improve overall security. Additionally, it includes an analysis of open ports.

The penetration testing followed a systematic and controlled methodology carried out by the team, encompassing the following steps:

- **Reconnaissance:** The team gathered information about the target network, including IP addresses of the target machines, network topology, and running services.
- **Scanning and Enumeration:** The team extensively used Nmap to scan the machines for open ports, services, and potential vulnerabilities.
- **Vulnerability Assessment:** A comprehensive assessment was conducted to uncover security weaknesses and misconfigurations within the network.
- **Exploitation:** Known vulnerabilities, such as the MS17-010 vulnerability, Drupal vulnerability, and local privilege escalation exploits, were leveraged to gain unauthorised access to the target machines.
- **Post-Exploitation:** After gaining access, the team searched for flags related to cryptography, brute-force attacks, and network packets (pcap).
- **Reporting:** The findings were collaboratively documented, and recommendations were developed to mitigate the identified risks.

The objective of this assignment was to conduct penetration testing to gain access to a remote machine by breaching the security of various applications and services, bypassing firewall protections, and overriding administrative privileges. The goal was to locate flags on the hosts based on the theme "Ballad of Songbirds and Snakes" on the "192.168.34.0/24" gateway.

Penetration testing, or pen testing, involves evaluating the security of a computer system or network by simulating an attack from a potentially malicious entity. This proactive approach is crucial for identifying and rectifying security weaknesses before they are exploited. Furthermore, it assists organisations in adhering to industry regulations and ensures the effectiveness of their security measures (Ghanem & Chen, 2019).

In conclusion, the network penetration testing revealed significant vulnerabilities in the local environment. The report includes recommendations to address these issues, enhance privilege management, strengthen the security posture, reduce the risk of unauthorised access and data breaches, and effectively protect sensitive information.

## **2. Statement Of Individual Contribution:**

### **2.1. Muhammad Hamza Aslam - S5348038 – 192.168.34.161**

My role in the project was pivotal as I focused on vulnerability assessment and scanning. Using tools such as Nmap, Nessus, and Nikto, I performed comprehensive scans to identify vulnerabilities and misconfigurations. One of my key tasks involved working on the host 192.168.34.161, where I conducted a DNS zone transfer to reveal additional hosts. During this process, I discovered a new host, 172.18.55.69, which contained valuable information and two flags. From the identified vulnerabilities, I conducted targeted exploitations using Metasploit and reverse shell scripts to gain access to the hosts. Documented steps for testing and exploitation activities, ensuring our findings were well-organized and accessible for review, analysis, and reporting. This documentation facilitated knowledge sharing among team members. I actively participated in team discussions, sharing insights and brainstorming strategies, which shaped our collective approach. Attending weekly team meetings, I monitored task progress and collaborated closely with my teammates to ensure our penetration testing efforts were thorough and effective.

### **2.2. Samuel Zavuga – S5307726 – 192.168.34.251**

In our 4-man team tasked with scanning and exploiting network hosts, I was assigned the host with IP address 192.168.34.251.

I Conducted a detailed Nmap scan on 192.168.34.251 to confirm the open ports and gather additional information I identified that port 22 was running an SSH service and port 80 was hosting a web server. I attempted common username and password combinations to check for weak credentials, Checked for known vulnerabilities in the SSH version to determine if there were any potential exploits. I Performed a directory brute force attack to find hidden directories and files using Dirbuster, Conducted a web vulnerability scan using tools like Nikto to identify common web application vulnerabilities such as SQL injection, XSS, and directory traversal.

My efforts yielded results because I was able to find a file upload point on the host that was not adequately secured, I uploaded a reverse shell and got access to the host and was able to find 3 flags. I documented all findings, including the identified services, potential vulnerabilities, and exploitation attempts. Provided detailed reports and screenshots to the team, highlighting successful exploitation steps and any sensitive information retrieved. Collaborated with the team to cross-verify results and integrate my findings into the overall assessment. Through these efforts, I contributed significantly to our team's objective, providing valuable insights and actionable intelligence on the target host 192.168.34.251 I was assigned.

### **2.3. Shehryar Mallick – S5328488 – 192.168.34.241**

During the project, I performed various activities such as contributing significantly to our penetration testing and security assessment efforts. Maintaining documentation of all the penetration testing and exploitation activities. This meticulous record-keeping ensured our findings were organized and accessible for review, analysis, and reporting, facilitating knowledge sharing among team members. I performed extensive penetration testing to identify vulnerabilities within our target systems. Using tools like Nmap for network scanning, Nikto for web server vulnerabilities, and Metasploit for exploiting weaknesses, I conducted thorough assessments. I also performed DNS zone transfers for domain intelligence and used Meterpreter for advanced exploitation techniques. Additionally, I executed the Google Squid Proxy exploit by setting the proxy on 192.168.34.241, uploading the reverse shell script to wolfcms, accessing the bash, and acquiring the hidden flag in the lucy directory. Beyond technical tasks, I actively participated in

team discussions and collaborated closely with my teammates, sharing insights and brainstorming strategies. This collaboration helped shape our collective approach and ensured our penetration testing efforts were thorough and effective. Attending weekly team meetings was another vital aspect of my contribution.

#### **2.4. Mona Yadi – S5273500 – 192.168.34.52**

My role in the project was central, focusing on vulnerability assessment and scanning. I utilised tools like Nmap, Nessus, and Nikto to perform detailed scans to uncover vulnerabilities and misconfigurations. My primary task involved working on the Windows host 192.168.34.52, where I exploited the EternalBlue vulnerability to gain access. During this process, I discovered a new host containing crucial information and flags. Leveraging the identified vulnerabilities, I performed targeted exploitations using Metasploit and reverse shell scripts to gain access to the hosts. I meticulously documented each step of the testing and exploitation activities, ensuring our findings were well-organized and accessible for review, analysis, and reporting. This documentation was vital for knowledge sharing among team members. I actively engaged in team discussions, offering insights and brainstorming strategies that shaped our collective approach. Regularly attending weekly team meetings allowed me to monitor task progress and collaborate closely with my teammates, ensuring our penetration testing efforts were comprehensive and effective.

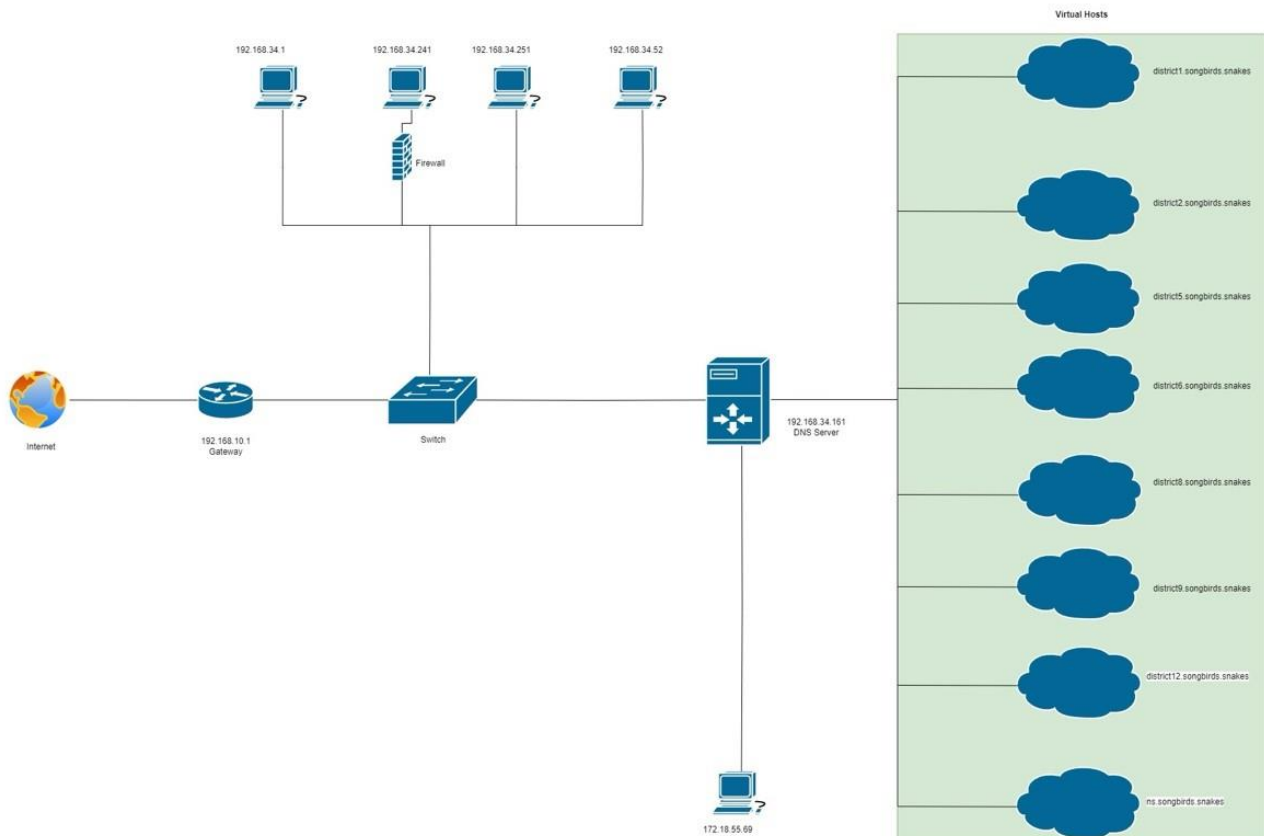
### 3. Comprehensive Analysis: Open Ports, Services, and Operating Systems for Each Host:

By the “ip a” command, we could access the network address through eth1, which is “192.168.34.0/24” for this assignment. Then, by the “sudo nmap -sV -O 192.168.34.0/24” command, we can find the hosts that are up with the open ports and running services (by the -sV flag) and operating systems (by the -O flag) that can help us to find potential vulnerabilities by knowing this information. So that 4 up hosts are identified, the information can be found in Table 1:

IP Address	Hostname	Open Ports (Associated Services)	Operating System	OS Detail
192.168.34.52	thecapital.songbirds.snakes	135/tcp (open msrpc) 139/tcp (open netbios-ssn) 445/tcp (open microsoft-ds) 554/tcp (open rtsp?) 2869/tcp (open http) 5357/tcp (open http) 10243/tcp (open http) 49152/tcp (open msrpc) 49153/tcp (open msrpc) 49154/tcp (open msrpc) 49155/tcp (open msrpc) 49156/tcp (open msrpc) 49157/tcp (open msrpc)	Microsoft Windows 7 2008 8.1	Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
192.168.34.161	district1.songbirds.snakes	21/tcp (open ftp) 22/tcp (open ssh) 53/tcp (open domain) 80/tcp (open http) 443/tcp (open ssl/http)	Linux 4.X 5.X	Linux 4.15 - 5.8
192.168.34.241	thearena.songbirds.snakes	22/tcp (open ssh) 3128/tcp (open http-proxy) 8080/tcp (closed http-proxy)	Linux 3.2 - 4.9	Linux 3.2 - 4.9
192.168.34.251	thehangingtree.songbirds.snakes	22/tcp (open ssh) 80/tcp (open http)	Linux 4.X 5.X	Linux 4.15 - 5.8
172.18.55.69	Apache server	22/tcp (open ssh) 80/tcp (open http) 111/tcp (open rpcbind) 139/tcp (open netbios-ssn) 443/tcp (open https)		

Table 1. nmap scan report

## 4. Network Map Of The Network:


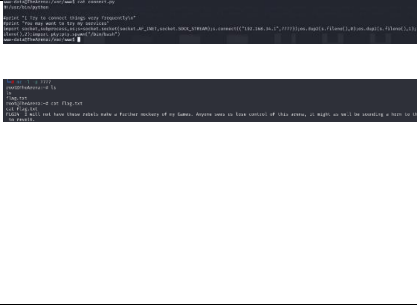
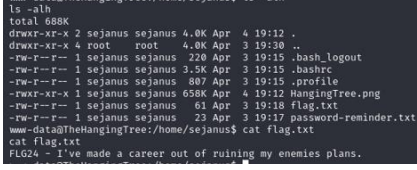
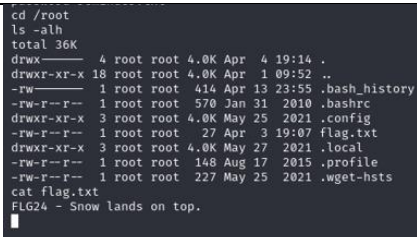


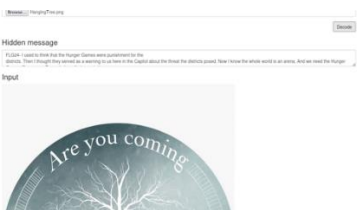
## 5. Flags Description:

Flag No	Flag Name (IP Location)	Screenshot	Exploitation Technique
1	Wallpaper.png (192.168.24.52)		Using Metasploit MS17-010, we exploited the EternalBlue vulnerability: Launched Metasploit (mfconsole), searched for EternalBlue (search ms17-010), used the "auxiliary/scanner/smb/smb_ms17_010" module (use 3), set RHOSTS and LHOST (set RHOSTS 192.168.34.52, set LHOST 192.168.10.1), and ran the exploit (run) to gain shell access. Inside the system, we found the flag in "C:\Users\Coriolanus\Pictures\Wallpaper.png"
2	Flag REG_SZ (192.168.24.52)		It was found in one of the registry files HKLM by the "reg query HKLM\SOFTWARE\Microsoft /s   findstr "FLG" command in shell (C:\Users\Coriolanus\Documents directory)

3	decode.me (192.168.24.52)		we found the third flag in a file named “decode.me” located in the “\Users\Coriolanus\Documents” directory. The file contained cipher-text encoded with Base58. We decrypted it using an online tool - CyberChef.
4	District9.songbirds.snakes (192.168.34.161)		We used a DNS zone transfer for the host with the dig axfr songbirds.snakes @192.168.34.161 command. Navigated to the “/etc” directory and used nano hosts to add entries associating hostnames with their IP addresses. Accessed each district via HTTP in a browser (e.g., http://district9.songbirds.snakes). Found a photo with a QR code, which, when scanned, revealed the flag.
5	district5.songbirds.snakes (192.168.34.161)		Due to a vulnerability in opendocman v1.2.7 an open-source document manager running on <a href="http://district5.songbirds.snakes">http://district5.songbirds.snakes</a> , we were able to perform SQL injection that gave us administrative access to the MySQL server running on the host. We then brute forced our way into the databases using sqlmap and found a flag in the password_vault db/credentials table.
6	district12.songbirds.snakes Flag.txt (192.168.34.161)		Through the access got from the previous flag, we were able to get the wordpress credentials (Username:admin, Password: hungergames) from the <b>wordpressdb</b> database, <b>wp_users</b> table. We logged into the dashboard and used the <b>404.php</b> to upload a reverse shell and gain access to the webserver. The flag was in the <b>/home/drgaul</b> directory.
7	Flag.txt (192.168.34.241)		For this host, we had to first set a proxy to be able to reach it. We then checked the robots.txt and found <b>wolfcms</b> running. Then by going to <a href="http://192.168.34.241/wolfcms/?/admin/login">http://192.168.34.241/wolfcms/?/admin/login</a> we logged into wolfcms by trying the default username/password: admin/admin which worked. The version of wolf cms is 0.8.2 which has



			<p>“Arbitrary PHP File Upload” vulnerability. We uploaded a reverse shell script and got access to the server. The flag was in the home directory of a user called <b>lucy</b>.</p>
8	<p>hello_world</p> <p>(192.168.34.241)</p>		<p>After gaining access to the host, we found a file “hello_world” in the same directory, we copy the whole content of “hello_world” and create a new file in our local kali host and paste the data into “hello_world” file. After running command strings “hello_world”   grep FLG24, we got the flag from it. Or another way you can do it by running the following command: strings hello_world   grep -i “FLG” in the lucy directory we can get the flag.</p>
9	<p>Flag.txt</p> <p>(192.168.34.241)</p>		<p>The last flag was got by modifying the contents of the "<b>connect.py</b>" file with a script that opened a new shell but as the root user. We then read the contents of flag.txt to find the flag. We used the dirty cow as an unprivileged user to gain write access potentially allowing us to gain root access on the system that was originally read-only mapping .</p>
10	<p>Flag.txt</p> <p>(192.168.34.251)</p>		<p>We use gobuster to do directory enumeration using the command <b>gobuster dir -u http://192.168.34.251 -w -x .php,.bak,.txt,.html,.php.bak</b>. From the files enumerated, the /dashboard.html provides us with a file upload capability to try to upload a reverse shell file. However, only .txt files were allowed to be uploaded so we had to find a way of uploading a <b>.php</b> file. To do that, we open the <b>ajax.php.bak</b> where we find a hint about using a cookie to help in uploading the shell. We use burpsuite proxy to intercept traffic, perform a payload to find the last letter of the cookie and subsequently upload the shell. With a successful shell, we now have access to the server and find the flag by navigating to the home directory of user “<b>sejanus</b>”</p>
11	<p>Flag.txt</p> <p>(192.168.34.251)</p>		<p>Using the same access as above, we navigate to the root user directory where we find another flag.</p>

12	Hanging Tree.png (192.168.34.251)	<pre> root@TheHangingTree:/# ls bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 libx32 root@TheHangingTree:/# cd home/ root@TheHangingTree:/home# ls HangingTree.png kali sejanus team-tasks root@TheHangingTree:/home# cd sejanus/ root@TheHangingTree:/home/sejanus# ls files.txt flag.txt HangingTree.png log.txt password-reminder.txt root@TheHangingTree:/home/sejanus# </pre> 	<p>Using the same access as above, in the sejanus home directory we found the image “HangingTree.png”. We download this image by using this command on new terminal “scp sejanus@TheHangingTree:~/HangingTree.png /home/kali”</p> <p>After downloading the file, we use online decryption tool steganography to decode the image to find the hidden flag.</p>
----	--------------------------------------	--	---

## 6. Analysis And Recommendations On Network Protection:

### 6.1. Host: 192.168.24.52:

#### 6.1.A. Analysis:

by the “sudo nmap --script vuln 192.168.34.52”, we can find that this port is highly vulnerable to smb-vuln-ms17-010. A critical remote code execution vulnerability exists in Microsoft SMBv1. Port 445 in this host is open. This port is used by the Server Message Block (SMB) protocol already implemented on Windows OS to allow file and printer sharing across a Local Area Network (LAN). It is sometimes very vulnerable (ManageEngine, 2023). The operating system, Microsoft Windows 7|2008|8.1, is also vulnerable since support for Windows 8.1 ended on January 10, 2023.

#### 6.1.B. Recommendation:

To secure host 192.168.34.52, update the operating system and software regularly. Upgrade to Windows 10 or 11, as support for Windows 8.1 has ended. Disable unnecessary services, particularly SMBv1, and use SMBv2 or SMBv3 instead. Configure firewall rules to restrict access to essential ports and IP addresses. Implement strong password policies and data encryption using HTTPS instead of HTTP. Deploy intrusion detection systems (IDS) and conduct regular vulnerability assessments. Educate users on security best practices and consult a cybersecurity expert for additional support.

### 6.2. Host: 192.168.24.161:

#### 6.2.A. Analysis:

This host has an open DNS service on port 53, running ISC BIND 9.16.27 (Debian Linux). It is vulnerable to “SSL POODLE information leak” and “Diffie-Hellman Key Exchange Insufficient Group Strength”. This allows for a DNS zone transfer, a method to replicate DNS data across DNS servers but can be exploited to gather critical DNS information about the network if not properly secured.

#### 6.2.B. Recommendation:

First, mitigate the SSL POODLE vulnerability by disabling SSL 3.0 on your web server and configuring it to use more secure protocols like TLS 1.2 or 1.3. Additionally, resolve the Diffie-Hellman Key Exchange vulnerability by configuring your web server to use a stronger DH group (at least 2048-bit). Disable the HTTP TRACE method to prevent potential Cross-Site Tracing

(XST) attacks. Regularly update all software and operating systems to the latest versions to ensure all known vulnerabilities are patched. Use strong, unique passwords for all services and implement multi-factor authentication (MFA) for SSH access. Configure a robust firewall to restrict access to necessary services only and employ intrusion detection systems (IDS) to monitor and alert on suspicious activity. Lastly, ensure that all sensitive data is encrypted in transit using secure protocols and educate users on security best practices to reduce the risk of social engineering attacks.

### **6.3. Host: 192.168.24.251:**

#### **6.3.A. Analysis:**

The host is running the Linux operating system. Preliminary scans with Nmap show that the host has two open ports, port 22 running OpenSSH 7.9p1 Debian and port 80 running apache httpd 2.4.38 for web services. A vulnerability scan using nmap --script vuln 192.168.34.251 -v didn't reveal any XSS or CSRF vulnerabilities that could be exploited. A directory enumeration resulted in finding <http://192.168.34.251/dashboard.html> and <http://192.168.34.251/owls> for uploading text files and displaying the uploaded files respectively. It was through <http://192.168.34.251/dashboard.html> that we were able to intercept the traffic, manipulated it and uploaded a reverse shell using **BurpSuite** proxy to gain access to the host.

#### **6.3.B. Recommendation:**

Deploy a Robust Firewall, most reverse shell incidents use outgoing traffic to compromise devices—therefore, it is necessary to take extra precautions with the firewall to make attacks less likely. A robust firewall system can block incoming IP addresses that aren't on the allowed list, prevent outgoing connections to websites unless they're on the allowed list and monitor network traffic so unauthorized users trying to access the system can be easily detected.

The use of SSL to encrypt traffic is strongly advised for this host to avoid eavesdropping and intercepting traffic that is in plain text.

### **6.4. Host: 192.168.24.241:**

#### **6.4.A. Analysis:**

According to Table 1, and investigation on those open ports, we can find vulnerability in the 3128 ports. After configuring the proxy setting, according to (medium, 2023), we check robots.txt and find wolfcms running. Then by going to "http://192.168.34.241/wolfcms/?/admin/login" address, we can access the login page by trying the default username and password (admin, admin) and logging in the wolf cms, we can see that the version of wolf cms is 0.8.2 which has "Arbitrary PHP File Upload" vulnerability.

#### **6.4.B. Recommendation:**

One of the most common ways that the attacker exploit vulnerabilities are by identifying the open ports within the network and what are the associated attacks to those ports during the reconnaissance and enumeration stage. One of the things that could be done is closing the unused ports. The vulnerability on port 3128 should be addressed by closing any unused ports or restricting access to trusted IP addresses only. Another thing that could be done to prevent the reverse shell scripting is updating WolfCMS to the latest version to patch known vulnerabilities, including the "Arbitrary PHP File Upload" vulnerability in version 0.8.2. also, other things that can be done to prevent the reverse shell script attack include security training and awareness, endpoint protection, and SIEM for early detection, respond and then remediation (Daniel, 2022). One more interesting thing was the admin dashboard did not have a secure password. A strong password should have these

three important factors composition, blocklist and minimum strength, min of eight characters, has a combination of letters and numbers for the composition factor, make sure that the password is not in the wordlist as per blocklist factor requirement, and can withstand guessing attack as per minimum strength requirement (Tan et al., 2020). Finally implement a WAF to monitor and filter malicious traffic to the web application, providing an additional layer of security against exploitation.

## **7. References:**

Ghanem, M. C., & Chen, T. M. (2019). Reinforcement Learning for Efficient Network Penetration Testing. Information, 11(1), 6. <https://doi.org/10.3390/info11010006>

Tan, J., Bauer, L., Christin, N., & Cranor, L. F. (2020, October). Practical recommendations for stronger, more usable passwords combining minimum-strength, minimum-length, and blocklist requirements. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (pp. 1407-1426).

(2022, February 10). How to detect and prevent a TCP 445 exploit and attack using firewall log analysis? ManageEngine EventLog Analyzer.

<https://www.manageengine.com/products/eventlog/logging-guide/firewall/how-to-detect-and-prevent-tcp-445-exploit-and-attack.html#:~:text=Port%20445%20is%20a%20Microsoft,be%20opened%20for%20external%20network>

P. (2023, May 27). Sick0s1.1 Walkthrough (VulnHub). Medium.

<https://medium.com/@pawelverma1/sick0s1-1-walkthrough-vulnhub-1900c1fdd1e>

D. (2022, July 12). DNS Zone Transfer Tutorial (Subdomain Discovery). Medium.

<https://medium.com/@dw3113r/dns-zone-transfer-tutorial-subdomain-discovery-ba4eba534bff>

[Junhua Wong]. (2024, May 23). Cyber Security | Ethical Hacking | Pentesting Lab | Vulnhub | Walkthrough | Napping 1.0.1 [Video]. YouTube.

<https://www.youtube.com/watch?v=AwBHJ7UUYdE>

Daniel, T. (2022, May 23). Defending against persistent reverse shell attack on end-user devices.

[https://medium.com/@daniel\\_toh/defending-against-persistent-reverse-shell-attack-on-end-user-devices-71b6b2a24d9a](https://medium.com/@daniel_toh/defending-against-persistent-reverse-shell-attack-on-end-user-devices-71b6b2a24d9a)