Name : Amit S Terdal
CSU ID: 2887869

2. Exercise 2 - Complete **Lab_Port Scanning** in the Ohio Cyber Range Infrastructure accessed using -

Module Activity Description: Part One: Exploring Kali Linux

Look through the applications installed on your Kali Linux System.

1. List and identify any tools that you recognize.

- Inform gathering: nmap
- Password attacks: Wordlists, pyrit
- Exploitation tools: Soial-Engineering Toolkit
- Sniffing and Spoofing: Wireshark
- Post exploitations: Backdoor factory, Power Sploit
- Data Assessment: jSQL injections

Open the terminal application, type "nmap" and look at the man page for nmap. Read through this page and answer the following questions:

2. According to the description, what tasks do system and network administrators use nmap for?

Description: Nmap is not only used for security audits but also for routine administrative tasks such as:

- Network inventory: Keeping track of devices and services on the network.
- Managing service upgrade schedules: Planning updates based on the versions of services running.
- Monitoring host or service uptime: Ensuring hosts and services are operational.

Insight from man nmap: "While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime."

3. What option would you use to treat all hosts as online (skip host discovery)?

Description: The -Pn option skips the host discovery phase and assumes all hosts are online. This is useful when scanning targets that block ping requests or when you want to scan without checking if the host is alive.

Insight from man nmap: "-Pn: Treat all hosts as online -- skip host discovery."

4. What option would you use to specify specific ports to scan?

Description: The -p option allows you to specify specific ports or port ranges to scan. For example, -p 22,80,443 scans ports 22, 80, and 443.

Insight from man nmap: "-p <port ranges>: Only scan specified ports. Example: -p22, -p1-65535, -p U:53,111,137,T:21-25,80,139,8080."

5. What option would you use to determine service and version info on open ports?

Description: The -sV option enables version detection, which probes open ports to determine the service and its version running on them.

Insight from man nmap: "-sV: Version detection to determine service and version info on open ports."

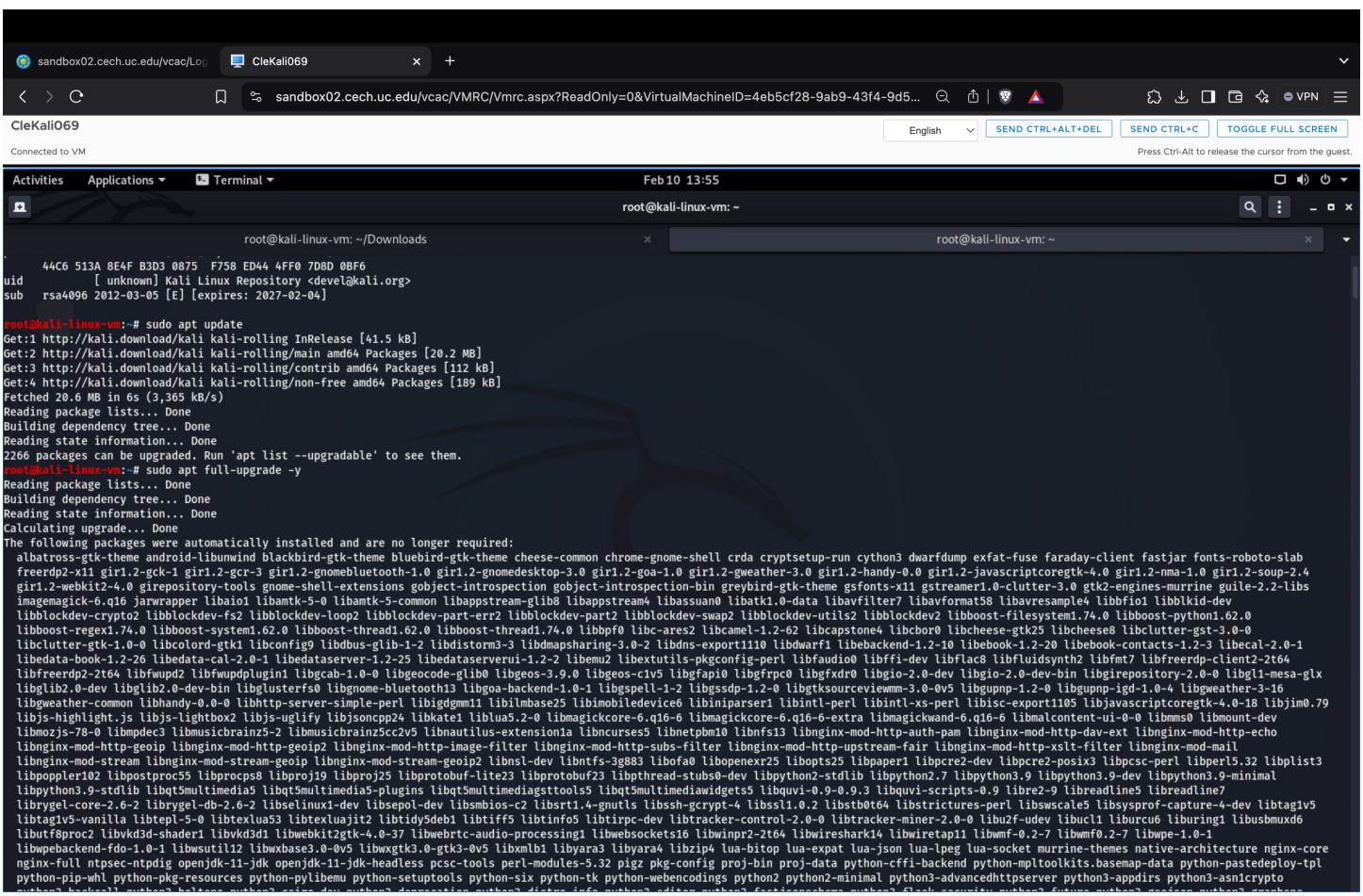
6. What option would you use to enable OS detection?

Description: OS detection in Nmap is -O. This option allows Nmap to attempt to determine the operating system of the target host(s) based on characteristics of the network stack and responses to probes.

Insight from man nmap: "-O: Enable OS detection. Attempts to determine the operating system of the target host(s) based on subtle differences in how they respond to network probes."

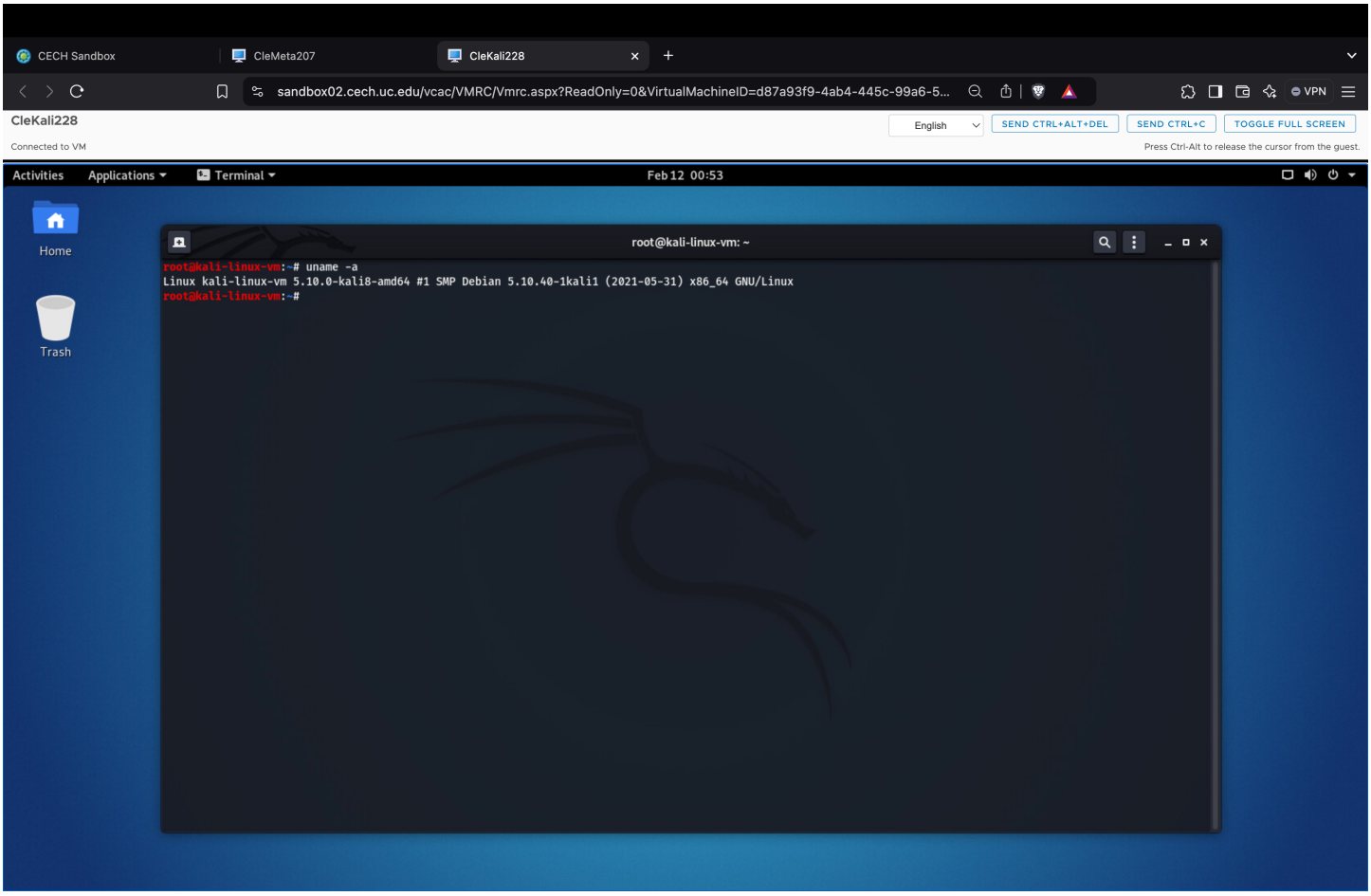
Check to see if you Kali system is up to date. If not, install all updates.

7. Paste a screen shot after updates are installed (or confirmed system is up to date.)



8. What distribution of Linux is Kali based on? (Hint: use the uname command)

Kali Linux is based on Debian.



Part Two: Starting Metasploit Framework

Use the Metasploit Unleashed site for help completing this portion of the lab.

9. In your own words, explain what the Meatasploit Framework is.

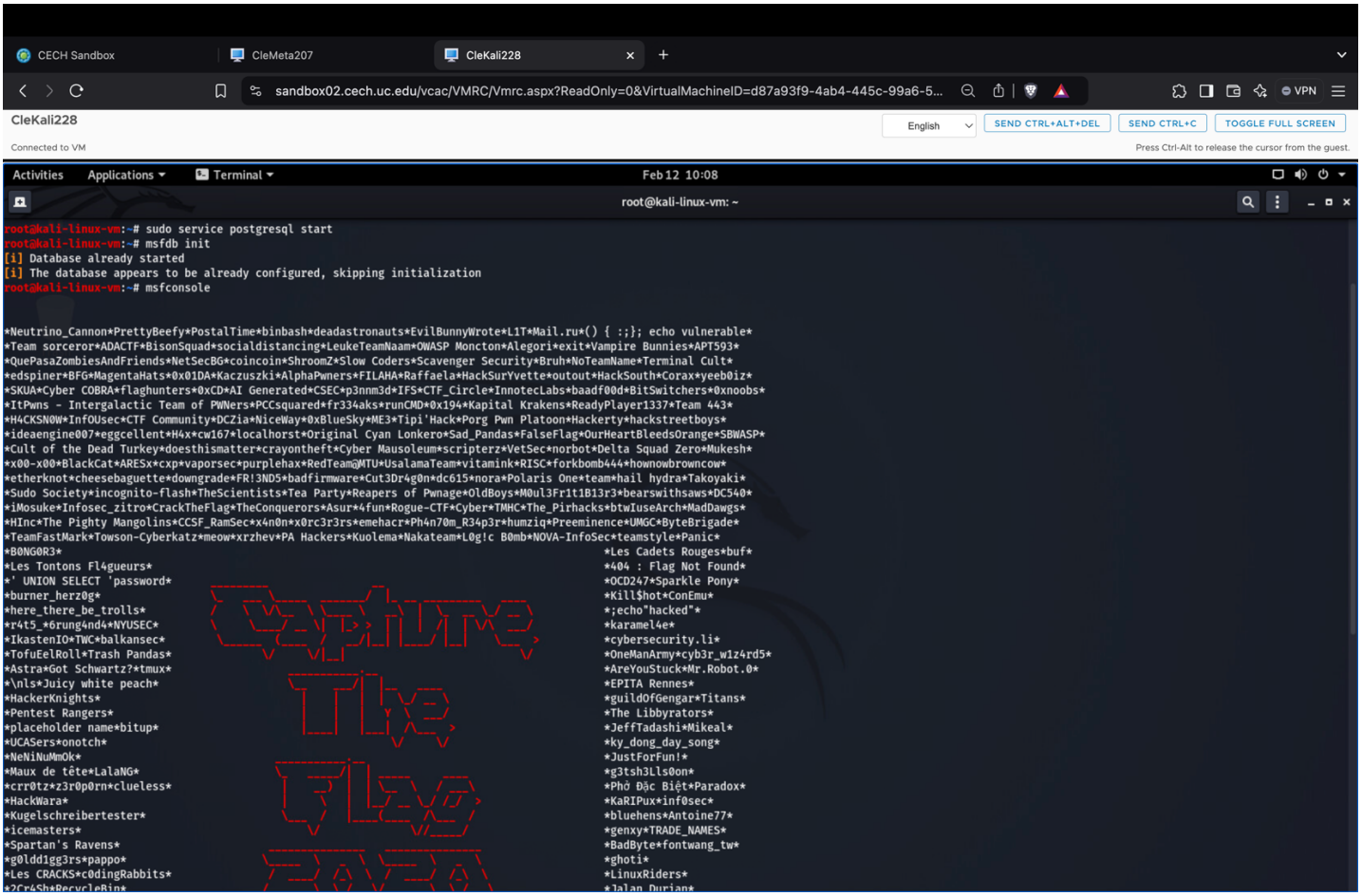
The Metasploit Framework is an open-source penetration testing platform that provides tools for developing, testing, and executing exploit code against remote targets. It is widely used by security professionals and ethical hackers to:

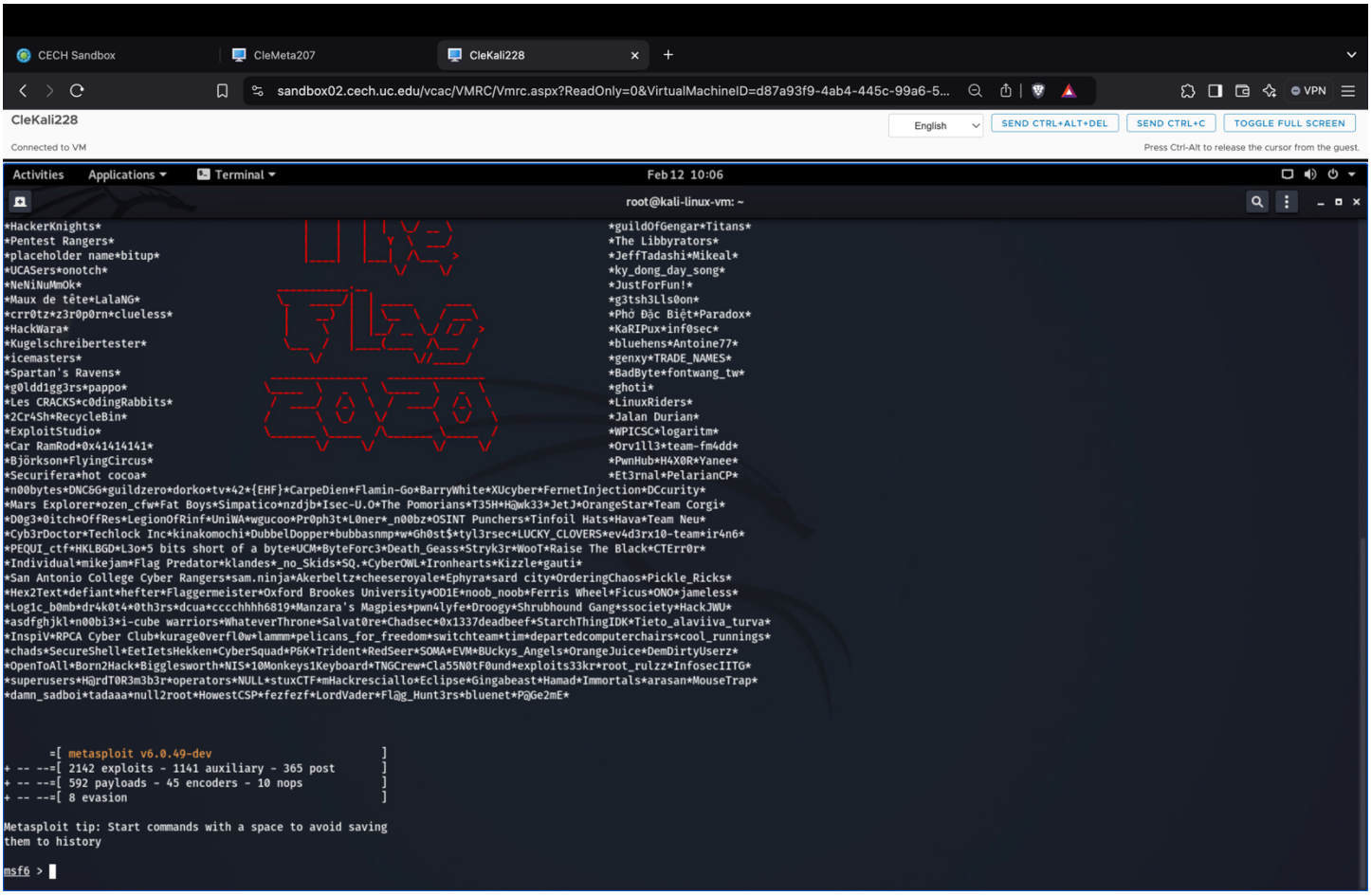
- Identify vulnerabilities in systems.
- Exploit vulnerabilities to gain access.
- Test the effectiveness of security defenses.
- Automate and streamline penetration testing tasks.

Metasploit includes a vast collection of exploits, payloads, auxiliary modules, and post-exploitation tools, making it a powerful framework for both offensive and defensive security operations.

Start the postgresql, make sure the 'msfdb' is initialized, and open the msfconsole.
In Terminal type: services postgresql start
In Terminal type: Msfdb init
In Terminal type: msfconsole

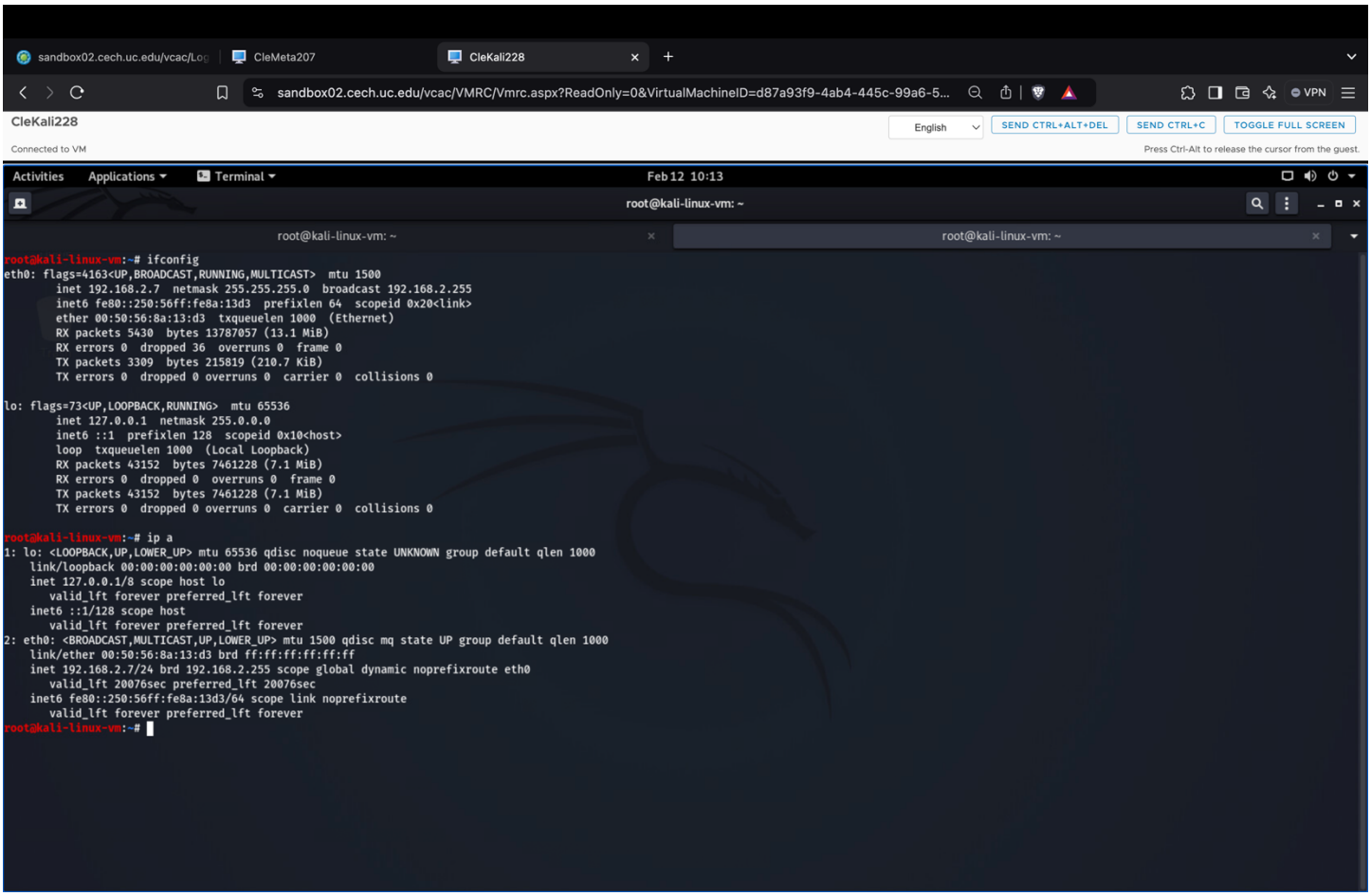
10. Paste as screen show of each of the commands used to complete these steps





Complete the rest of this section in the msfconsole. Hint: regular Linux commands will work here, and you can type help to find msf commands

11. What is the IP and subnet mask of your Kali Linux System?



IP Address: 192.168.2.7
Subnet Mask: 255.255.255.0 (or /24 in CIDR notation)

The inet field in the ip a output shows the IP address and subnet mask in CIDR notation (192.168.2.7/24).

The /24 indicates that the first 24 bits of the IP address are used for the network portion, leaving the remaining 8 bits for host addresses. This translates to a subnet mask of 255.255.255.0.

12. What is the Network Address of your network?

The network address is the base address of subnet. It is calculated by performing a bitwise AND operation between the IP address and the subnet mask.

<u>Calculation:</u>
Convert the IP address and subnet mask to binary:
IP Address: 192.168.2.7 → 11000000.10101000.00000010.00000111
Subnet Mask: 255.255.255.0 → 11111111.11111111.11111111.00000000
Performing a bitwise AND operation:

11000000.10101000.00000010.00000111 (IP Address)
AND
11111111.11111111.11111111.00000000 (Subnet Mask)

Which equals to: 11000000.10101000.00000010.00000000

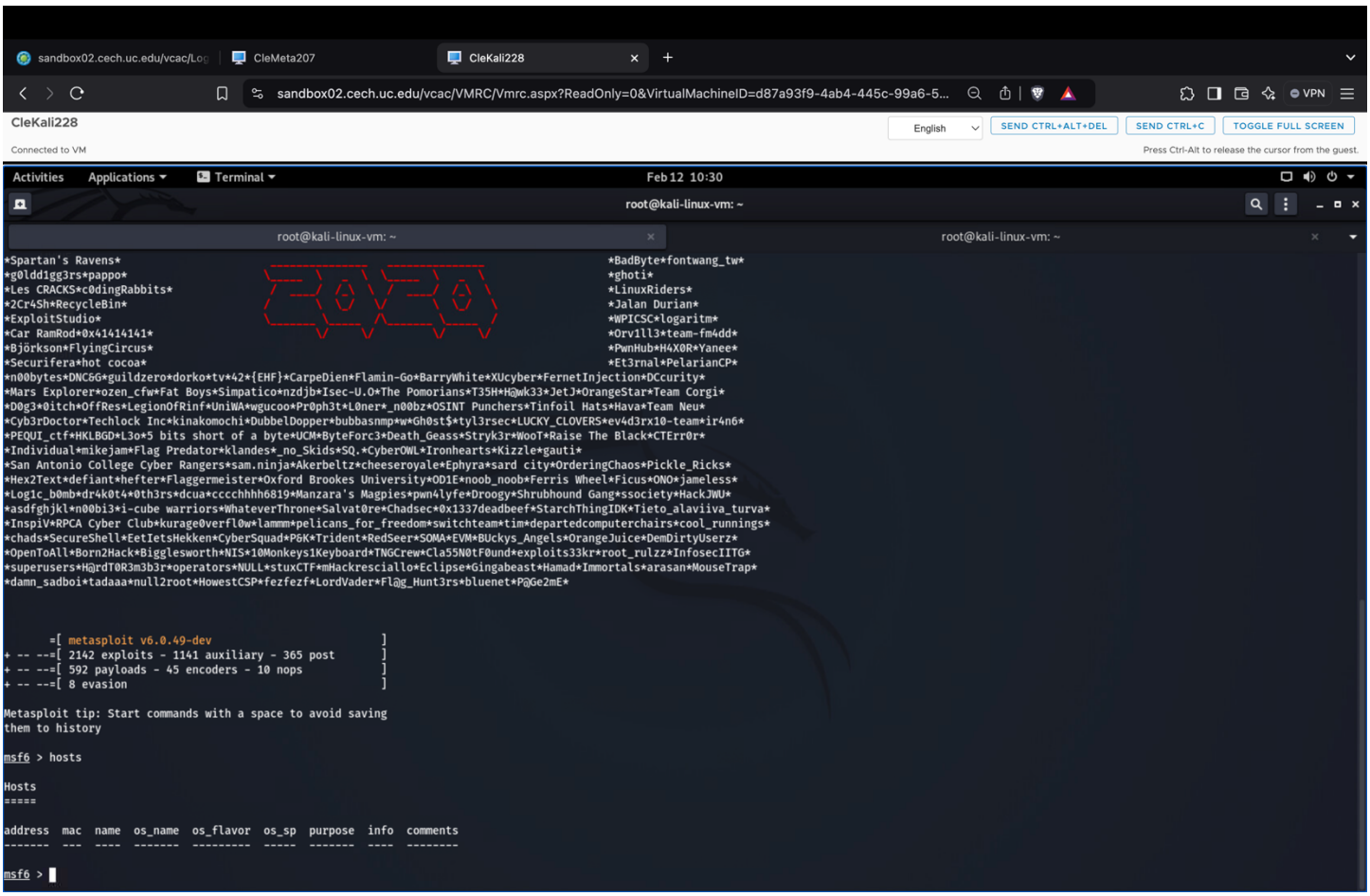
Converting the result back to decimal: 11000000.10101000.00000010.00000000 → 192.168.2.0

Network Address:
The network address for my subnet is: 192.168.2.0

- The network address is the first address in the subnet and is used to identify the network itself.
- In a /24 subnet, the first three octets (192.168.2) represent the network portion, and the last octet (0) represents the network address.

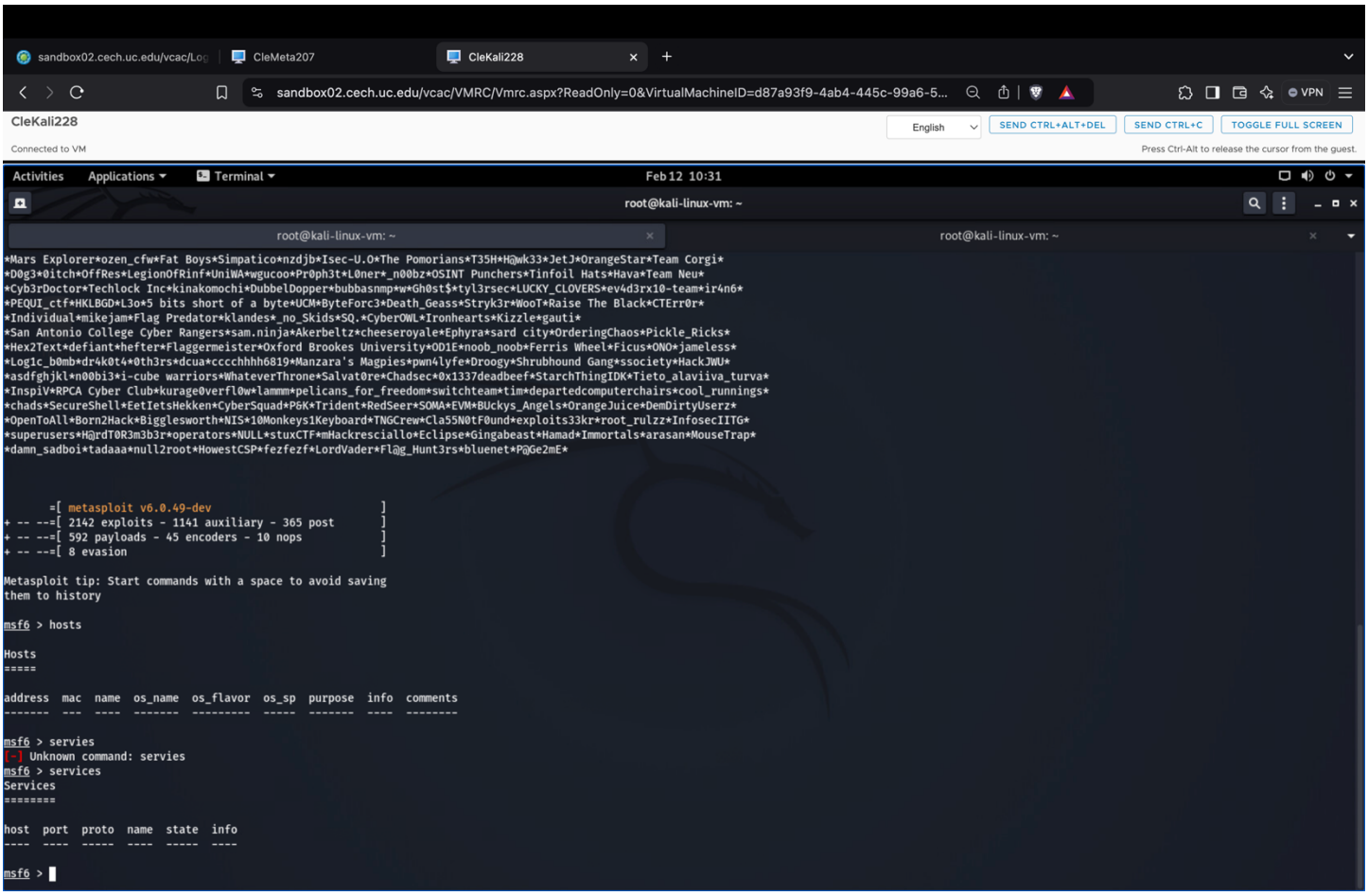
13. What hosts are listed in your database now? (Show a screen shot)

There aren't any host listed on my database now



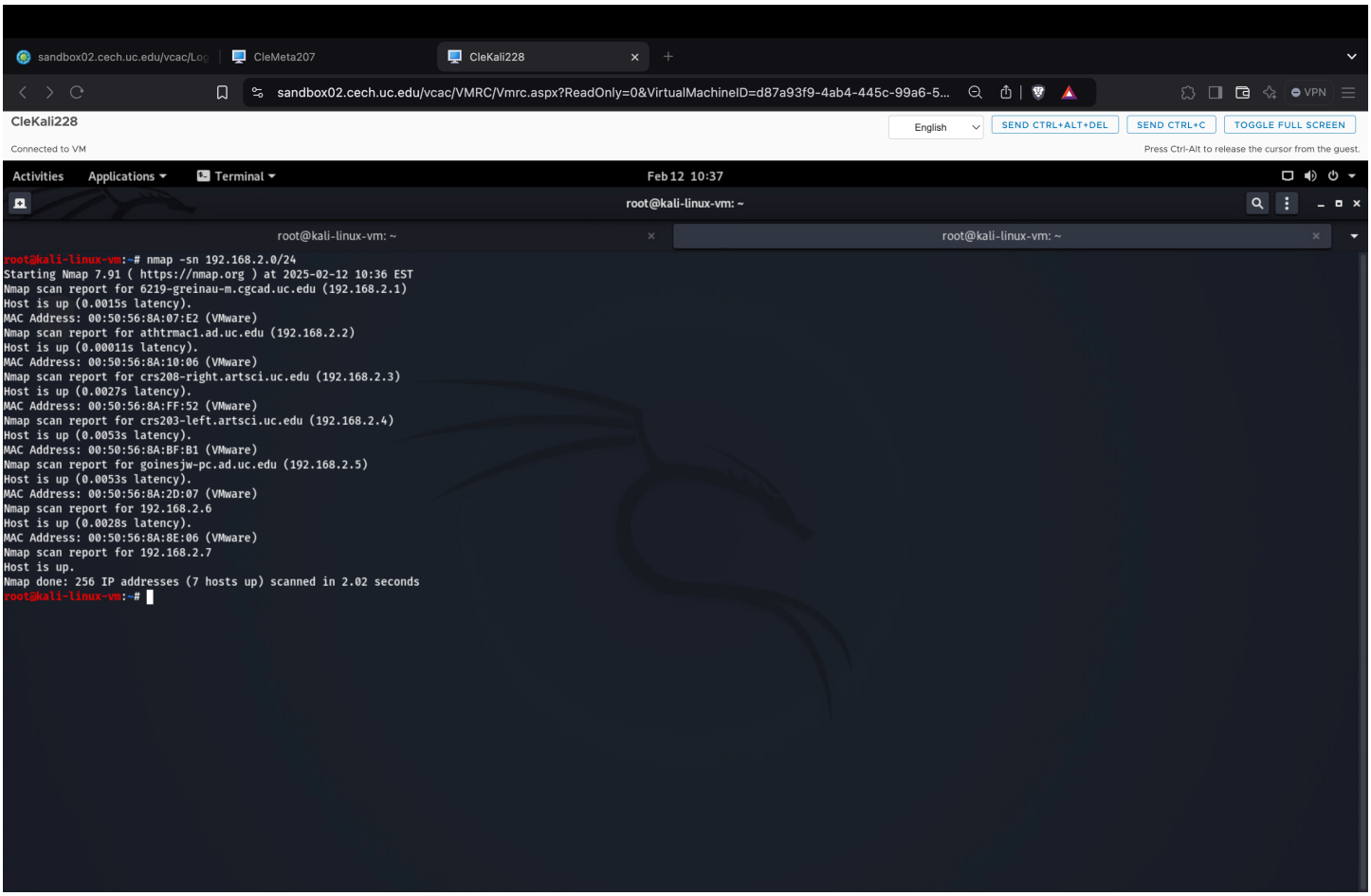
14. What services are listed in your database now? (Show a screen shot)

There aren't any Services listed on my database now



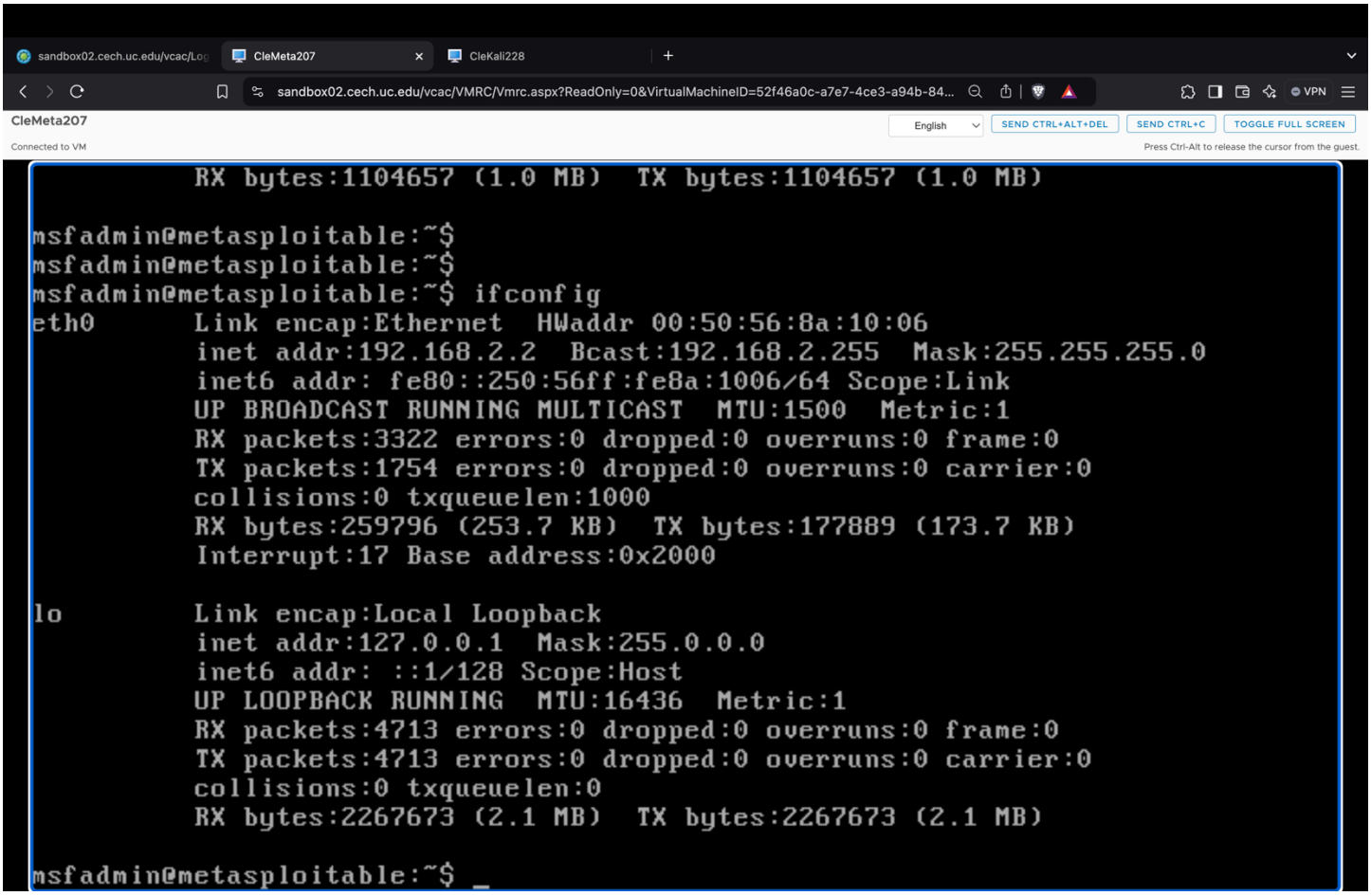
Run an nmap ping sweep in your network. (nmap -sn 192.168.2.0/24)

15. Paste a screen show of the command and results.



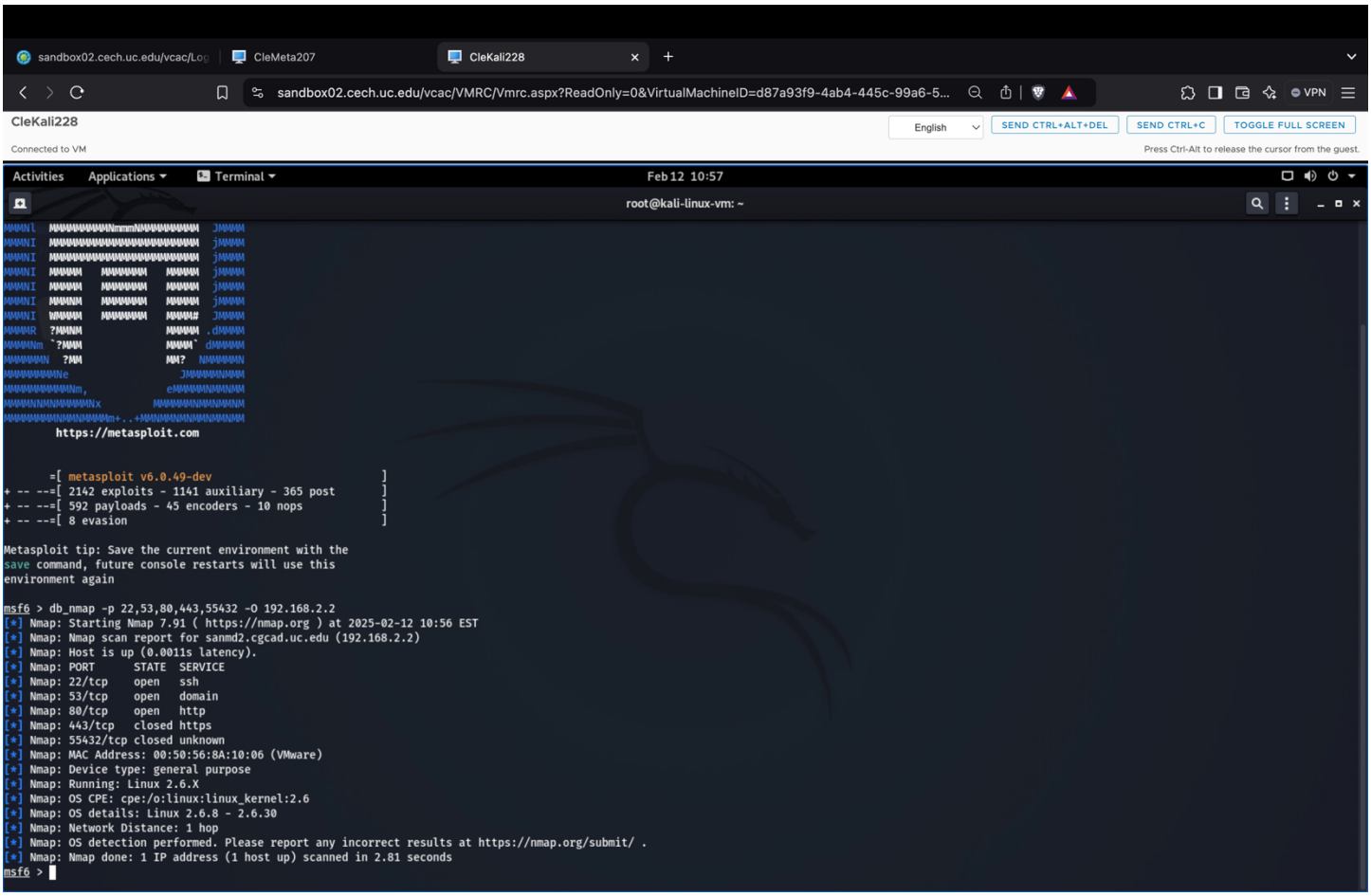
16. What is the IP address of you metasploit2 target? (Take note of this for future assignments)

The IP address of my Metasploit2 target is 192.168.2.2
The ifconfig command shows the network configuration of the metasploitable system.
The inet addr field under the eth0 interface displays the IP address of the system, which is 192.168.2.2.

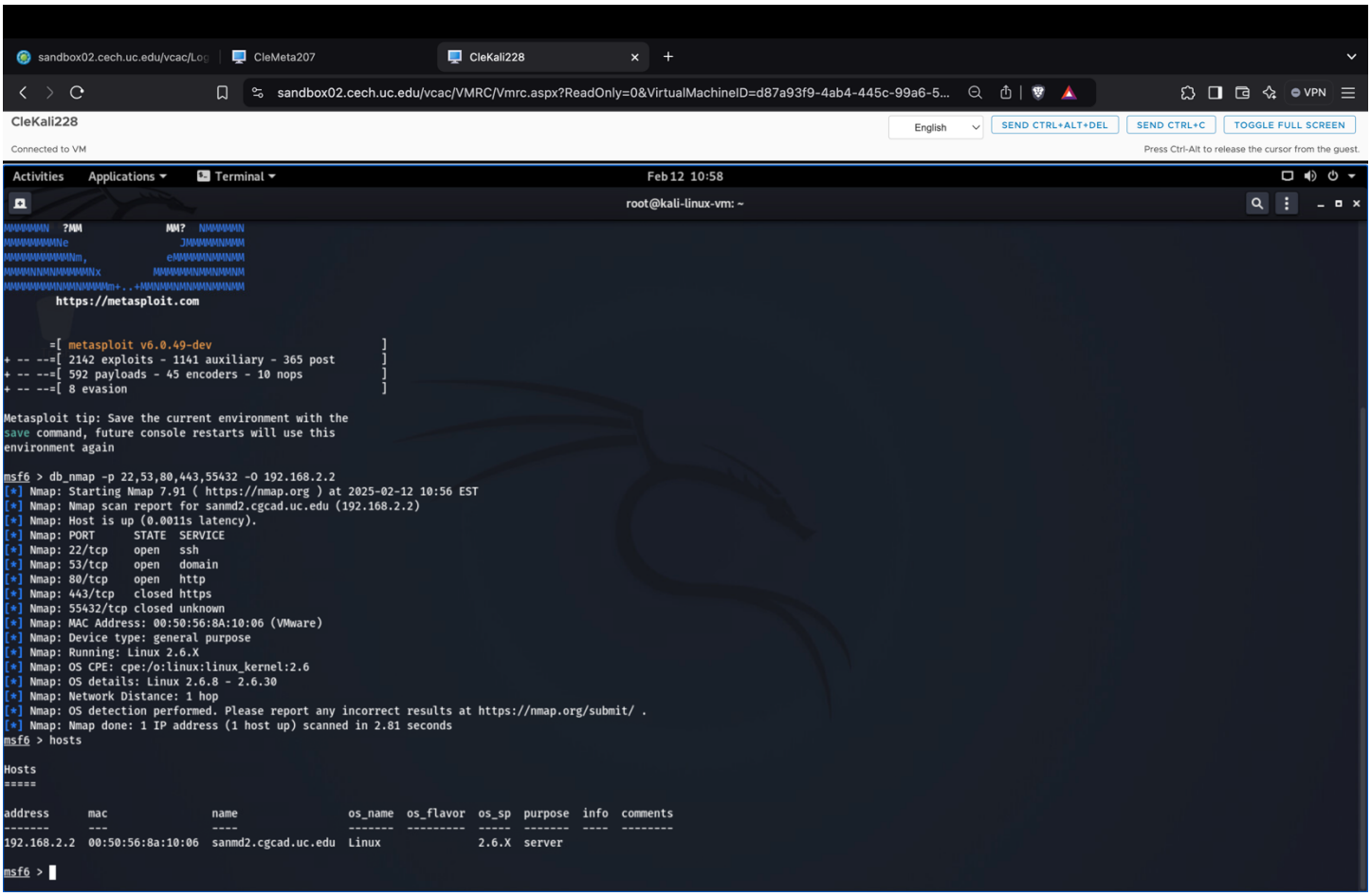


Run a nmap scan against your target. This time use db_nmap to store the results in your database. Specify options to meet the following criteria:
• Scan ports 22,53,80,443 and 55432
• Run OS detection

17. Show a screen show if the command and the results.



18. What services are now listed in your database? (Show a screen shot) (Type: hosts)



sandbox02.cech.uc.edu/vcac/Log | CleMeta207 | CleKali228

sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=d87a93f9-4ab4-445c-99a6-5...

CleKali228

Connected to VM

English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

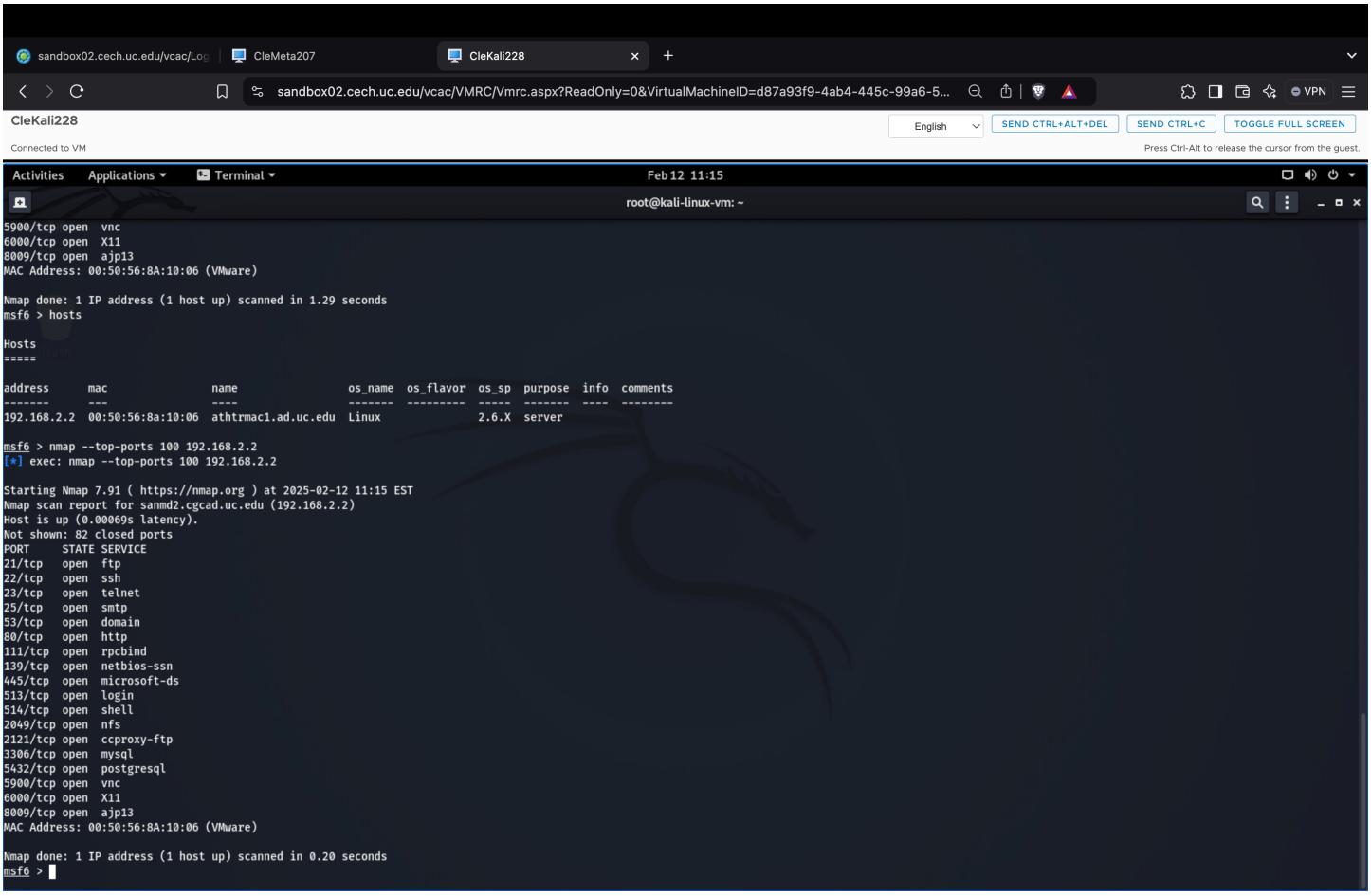
Press Ctrl-Alt to release the cursor from the guest.

Activities | Applications | Terminal | Feb 12 10:58

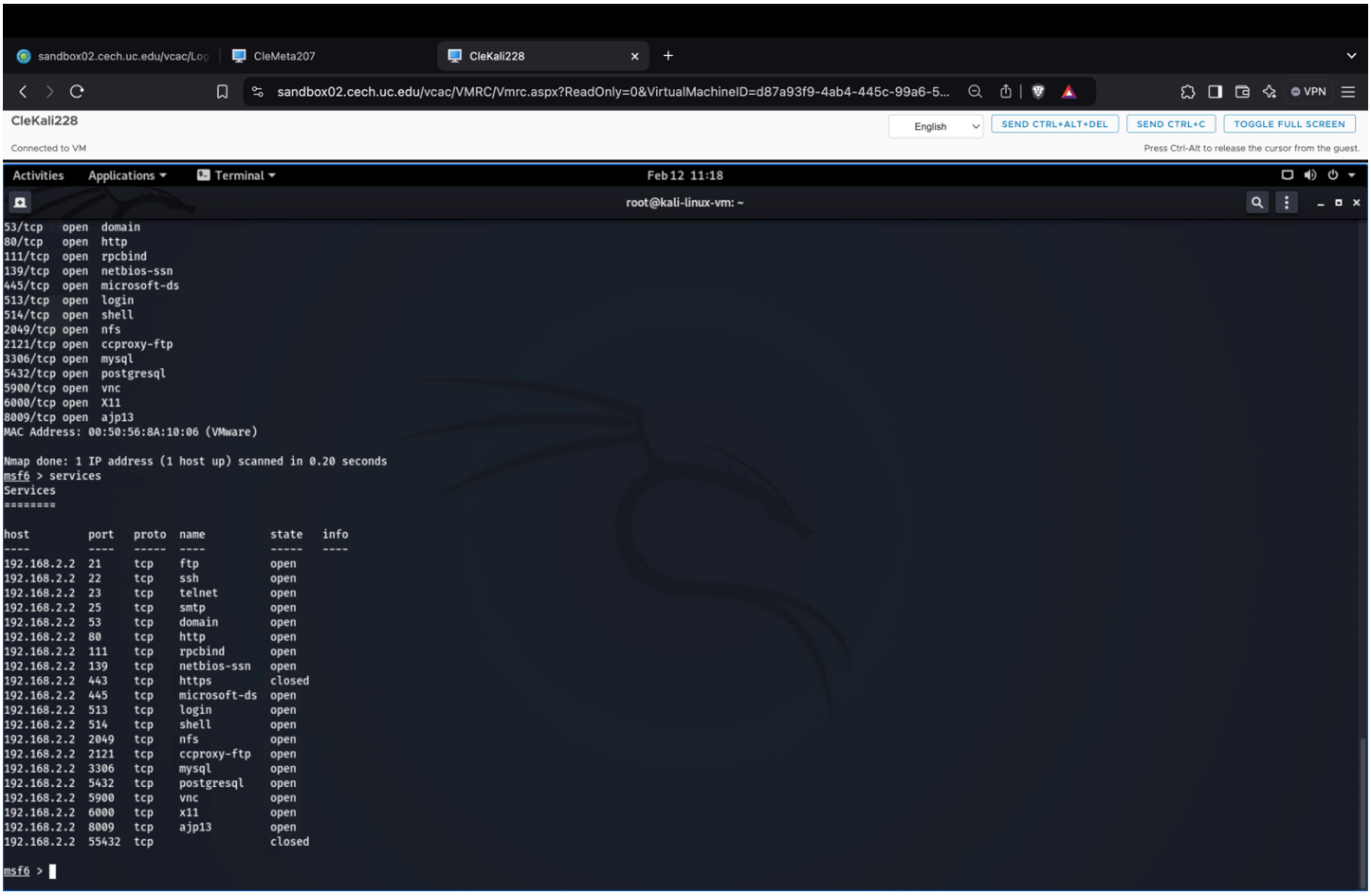
root@kali-linux-vm: ~

```
Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

msf6 > db_nmap -p 22,53,80,443,55432 -O 192.168.2.2
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-12 10:56 EST
[*] Nmap: Nmap scan report for sanmd2.cgcad.uc.edu (192.168.2.2)
[*] Nmap: Host is up (0.0011s latency).
[*] Nmap: PORT      STATE  SERVICE
[*] Nmap: 22/tcp    open   ssh
[*] Nmap: 53/tcp    open   domain
[*] Nmap: 80/tcp    open   http
[*] Nmap: 443/tcp   closed https
[*] Nmap: 55432/tcp closed unknown
[*] Nmap: MAC Address: 00:50:56:8A:10:06 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.8 - 2.6.30
[*] Nmap: Network Distance: 1 hop
[*] Nmap: OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds
msf6 > hosts

Hosts
=====

address      mac               name                os_name  os_flavor  os_sp  purpose  info  comments
-------      ---               ----                -------  ---------  -----  -------  ----  --------
192.168.2.2  00:50:56:8a:10:06  sanmd2.cgcad.uc.edu  Linux               2.6.X  server

msf6 > services
Services
========

host         port   proto  name    state   info
----         ----   -----  ----    -----   ----
192.168.2.2  22     tcp    ssh     open
192.168.2.2  53     tcp    domain  open
192.168.2.2  80     tcp    http    open
192.168.2.2  443    tcp    https   closed
192.168.2.2  55432  tcp            closed

msf6 >
```

19. Run another nmap scan against your target, this time choose the top 100 ports. (Show a screen shot)



20. What services are running on your target? (Show a screen shot)

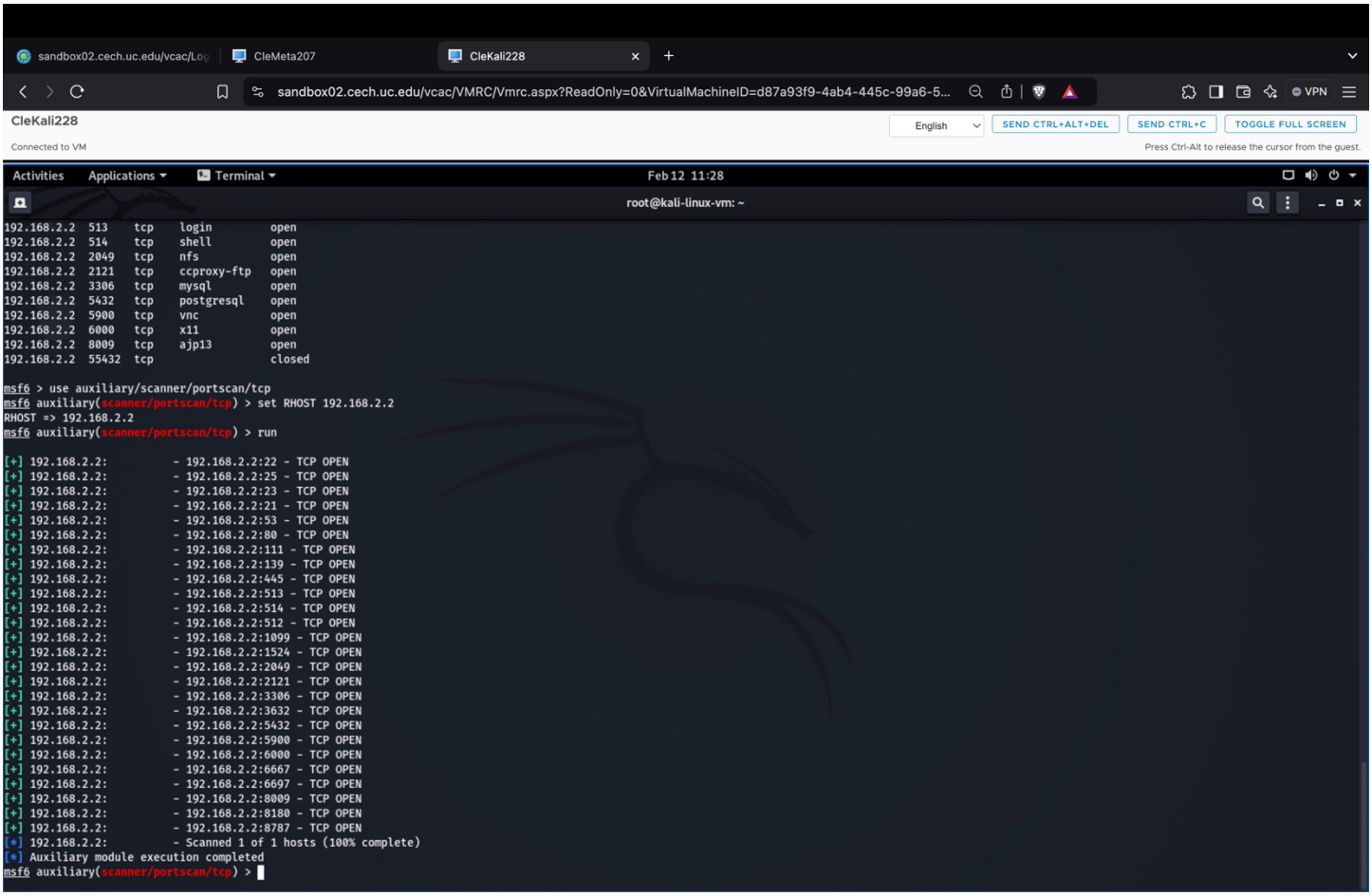


Run a scan with one of Metasploits built in port scanning tools against your target. You choose the tool and the options.

21. Paste a screen shot of the options you choose and the results of running the scanner

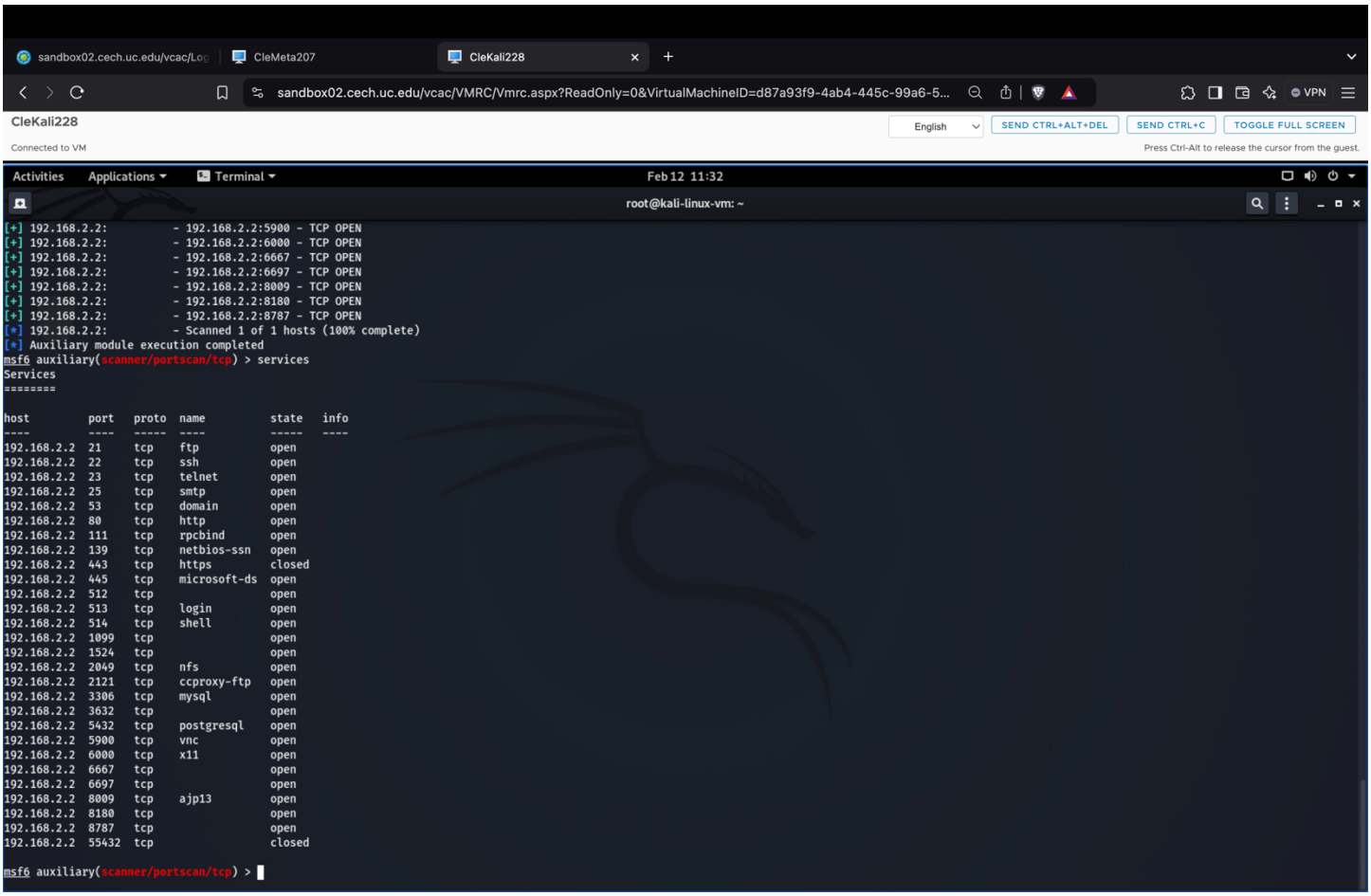
I Used a Metasploit auxiliary module to post scan my target.

use auxiliary/scanner/portscan/tcp
set RHOSTS 192.168.2.2
run



22. Did you find any additional services that are running? List the service and ports below.

Yes, I did find some new ports
During my second scan I revealed the following new open ports that were not present in the first scan:
512/tcp, 1099/tcp, 1524/tcp, 3632/tcp, 6667/tcp, 6697/tcp, 8180/tcp, 8787/tcp,



Exit the msfconsole.

Part Three: Bonus

Choose one of the other port scanning tools discussed in the course materials (p0f, Xprobe2, Masscan, Netcat). Run any kind of scan against your target system that you like. Then record a short video (under 3 minutes) and explain what options you choose and describe the results.

I have done short a video please do click below:

Click Here