Enumerating Hosts Using Wireshark, Windows, and Linux Commands

ETHICAL HACKING & Lab # 2

Student Info
Name: SRIJA PABBA
Student ID: 00866719
Email:
spabb6@unh.newhaven.edu

Table of Contents

I. **Executive Summary** 2

Highlights

Objectives

II. **Lab Description Details** 2

Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives

III. **Supporting Evidence** 12

IV. **Conclusion & Wrap-Up** 14

Summary with observations, Success & Failures, Challenges

Executive Summary

Highlights

In this lab, I explored system enumeration using various tools, including command line utilities like db_nmap, net, nbtstat, and ifconfig, as well as GUI tools like Wireshark and Armitage. I learned about active scanning techniques that are detectable on the network, alongside passive scanning methods that allow for stealthy data collection. This hands-on experience enhanced my skills in identifying network services and vulnerabilities, providing me with a comprehensive understanding of effective network analysis and security assessment

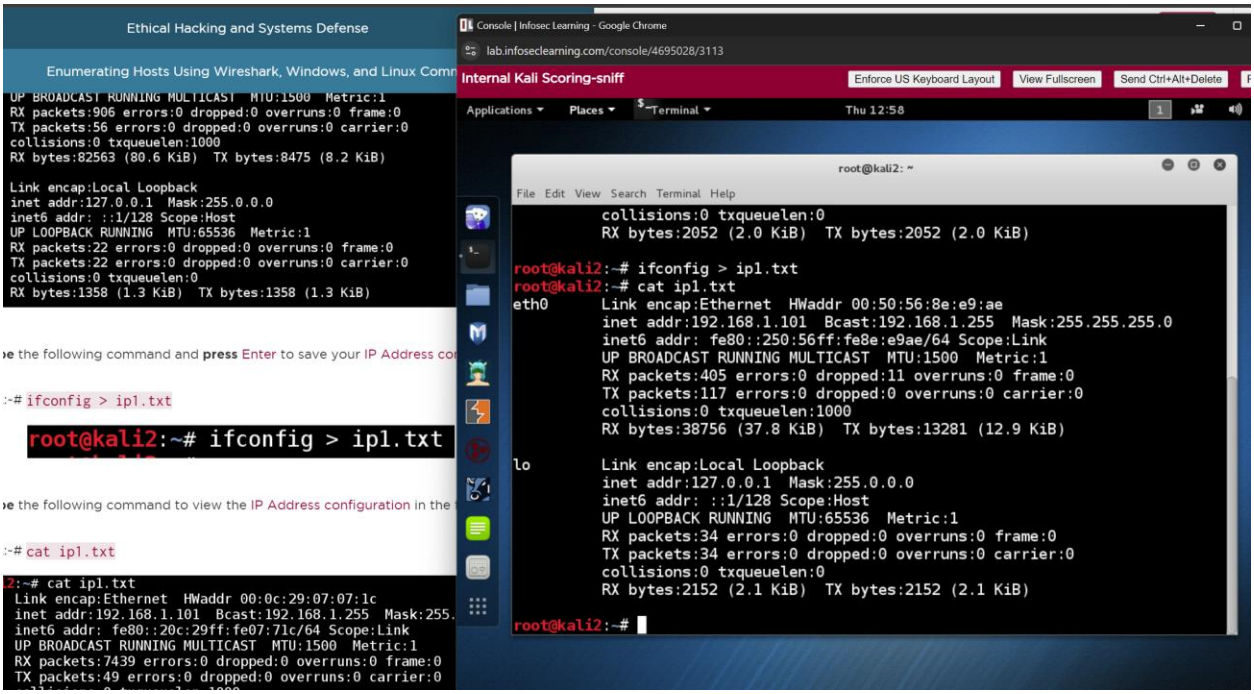
Objectives

The objective of this lab is to explore system enumeration techniques using command line and GUI tools on Linux and Windows. I aim to identify network services and vulnerabilities through tools like db_nmap, net, nbtstat, ifconfig, Wireshark, and Armitage. Additionally, I will differentiate between active scanning, which is detectable, and passive scanning, which allows for stealthy data collection, to enhance my understanding of network analysis and security.

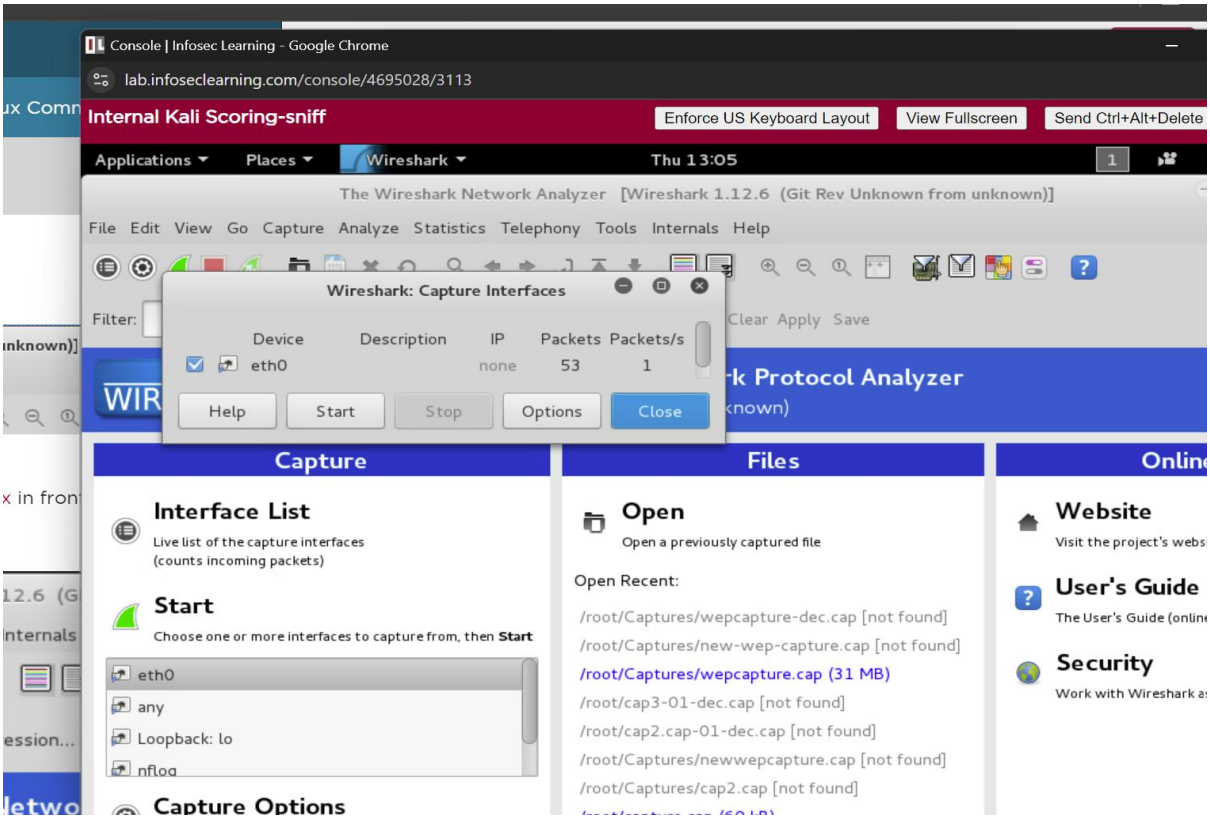
Lab Description Details

Ifconfig

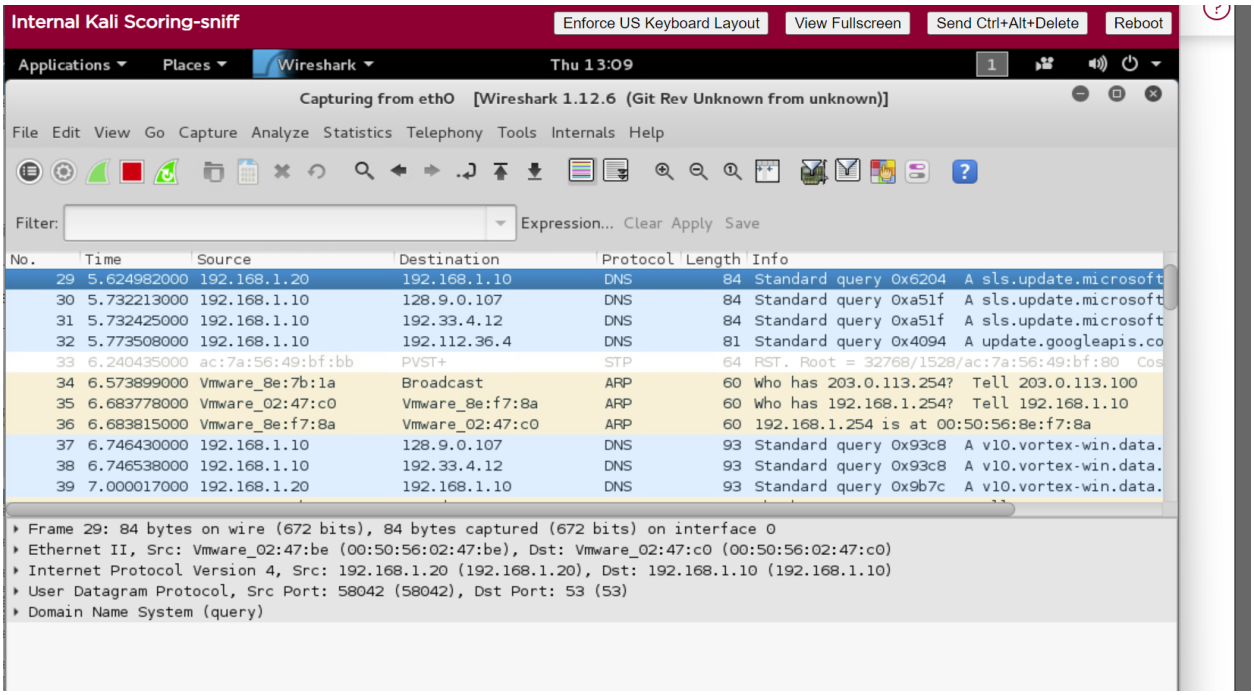
Ifconfig > ip1.txt



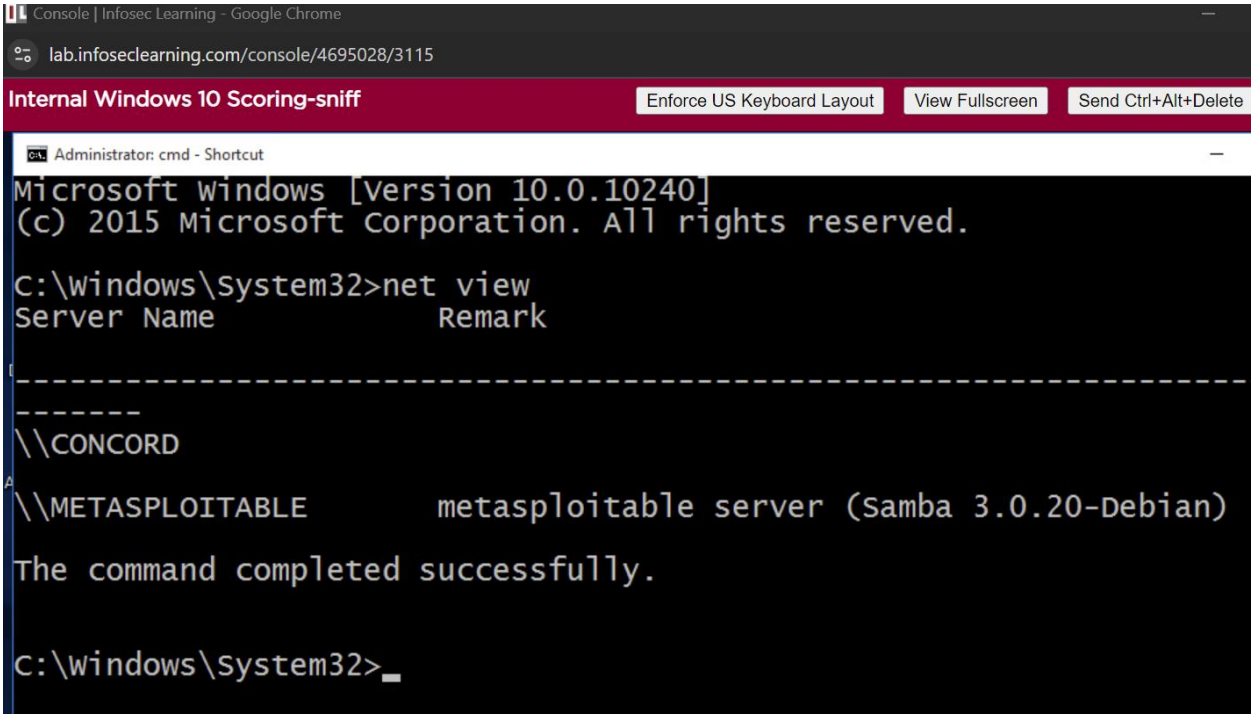
Interface window in Wireshark



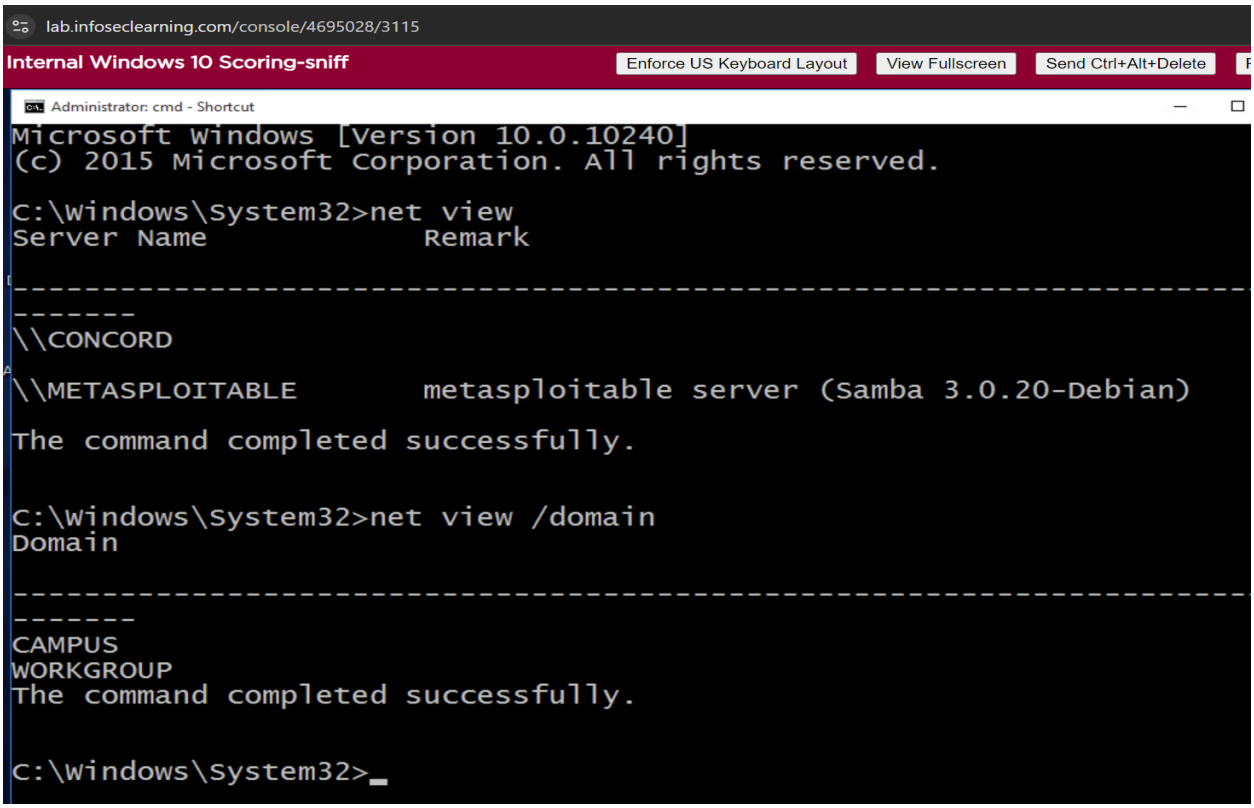
Packets appearing list



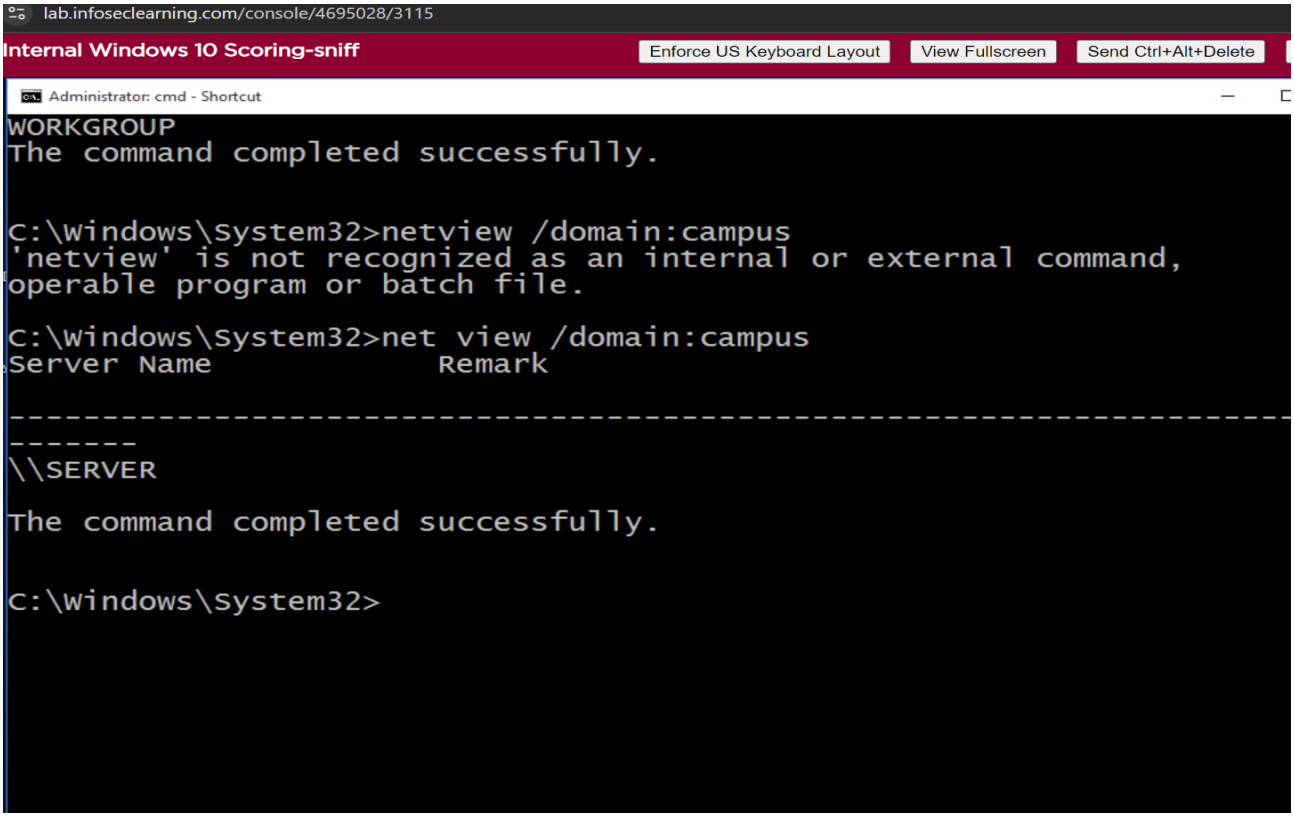
net view



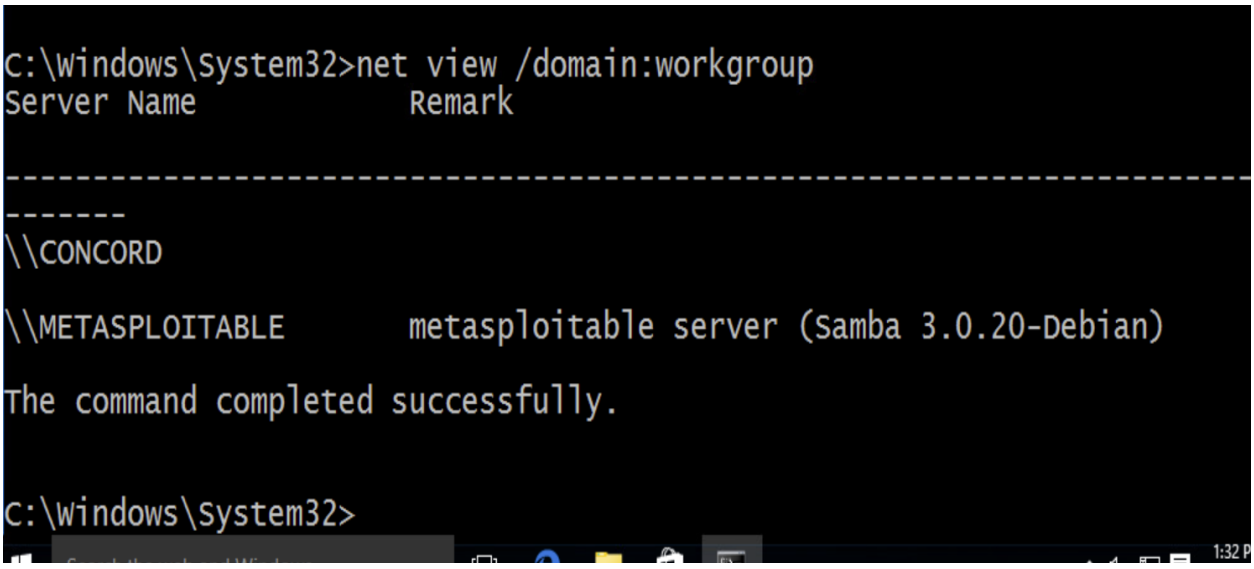
Net view /domain



Net view /domain:campus



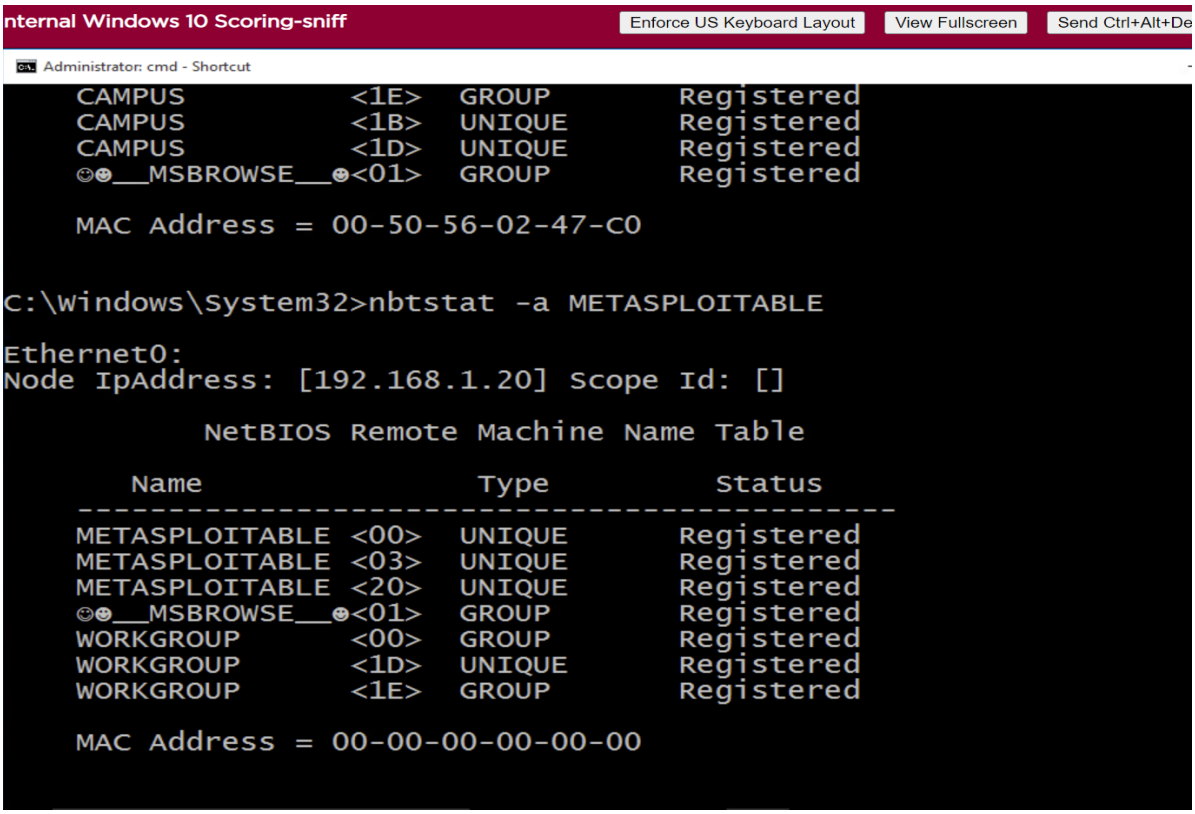
Net view /domain:workgroup



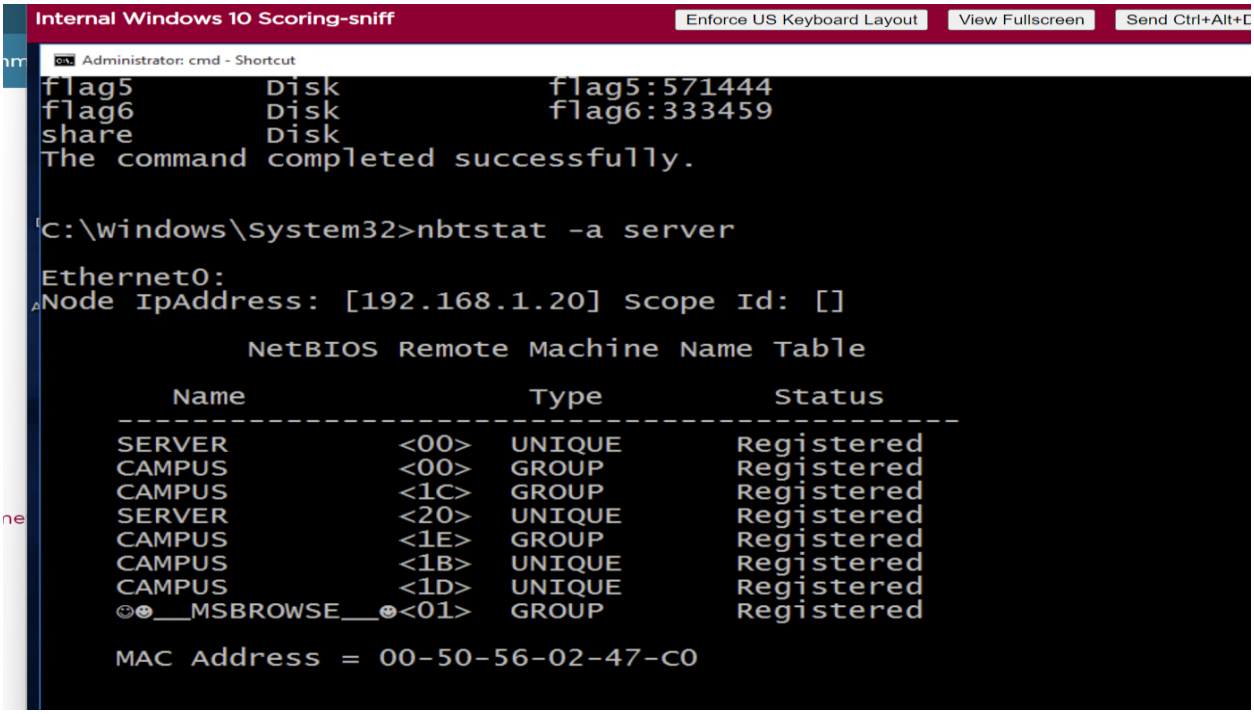
Net view \\server

```
C:\Windows\System32>net view \\server
Shared resources at \\server


Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
NETLOGON    Disk           Logon server share
share       Disk
SYSVOL      Disk           Logon server share
The command completed successfully.
```

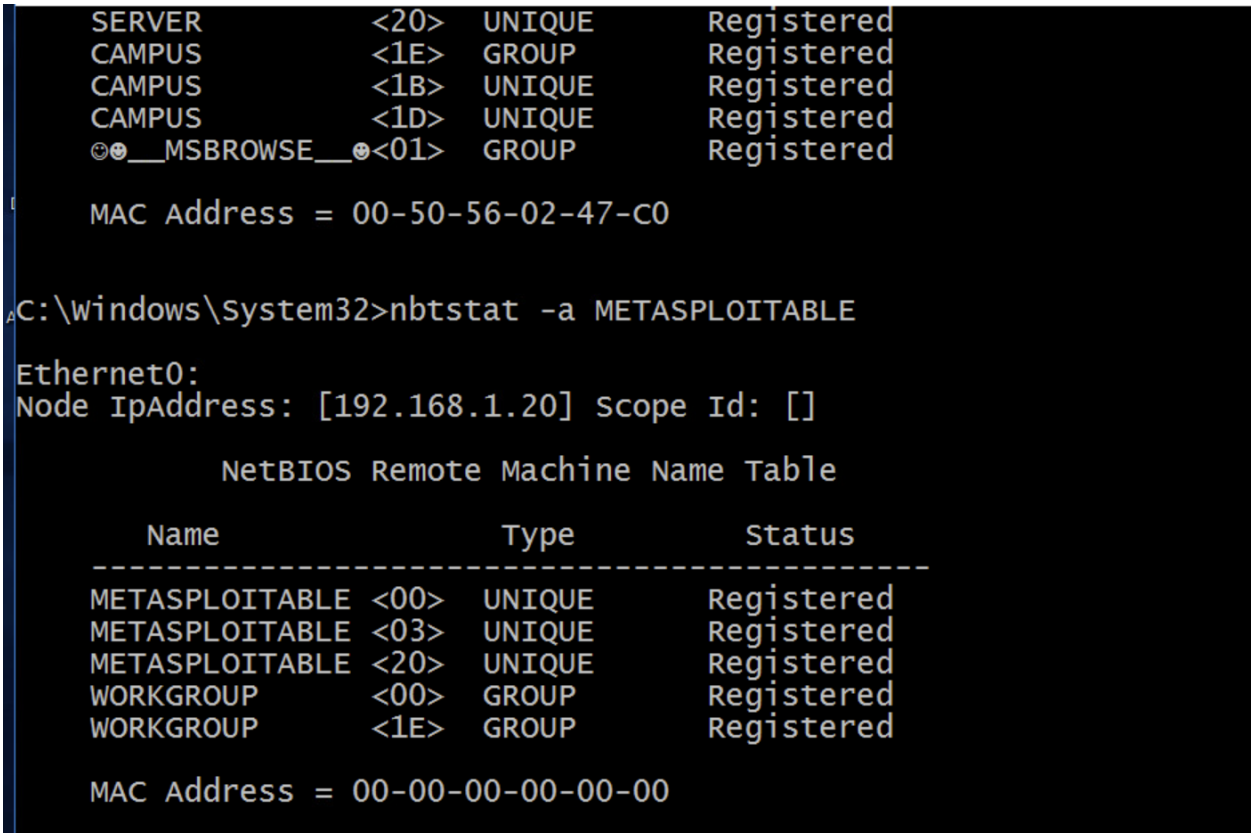
Net view \\metasploitable



nbstat -a server

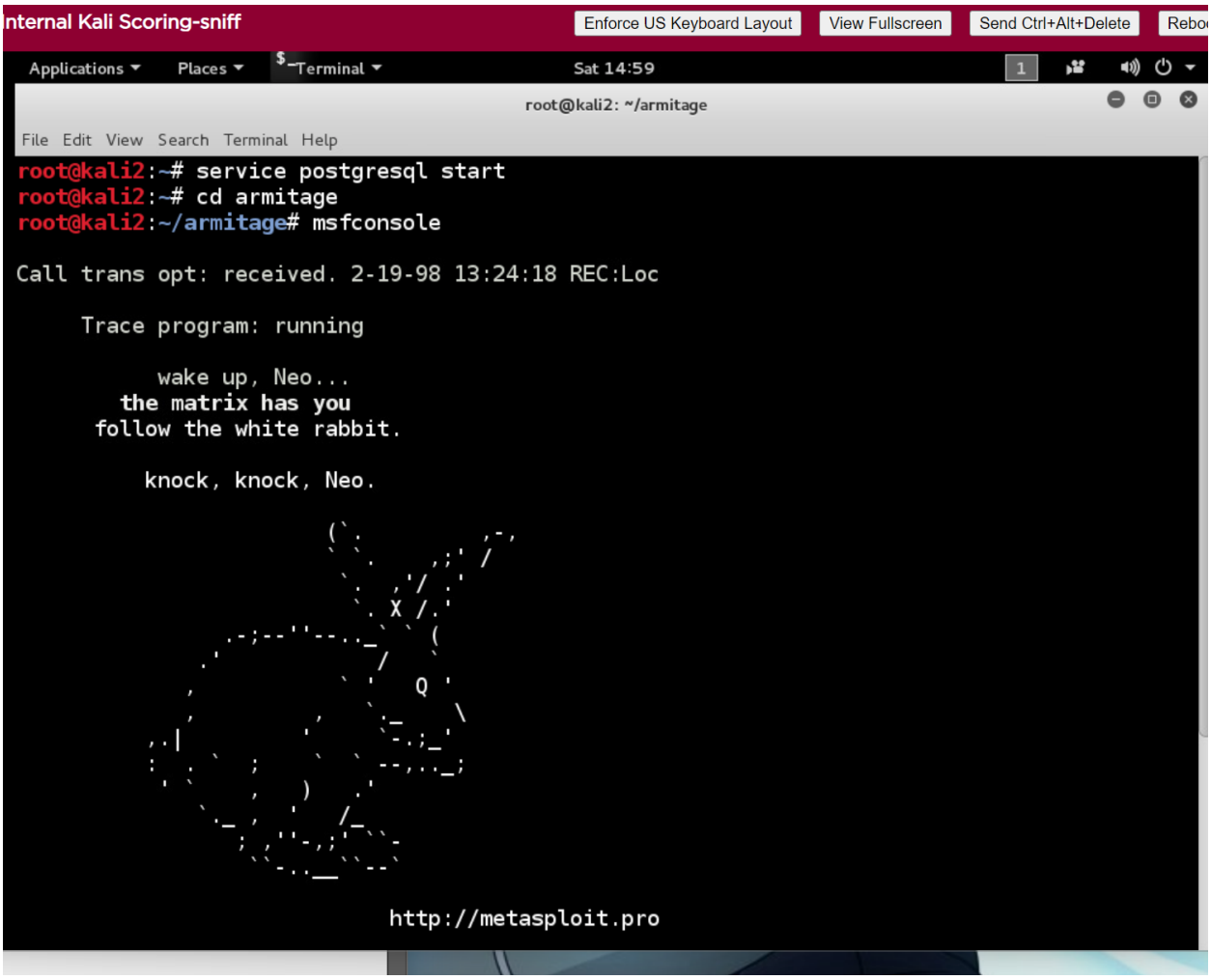


Nbstat -a METASPLOITABLE

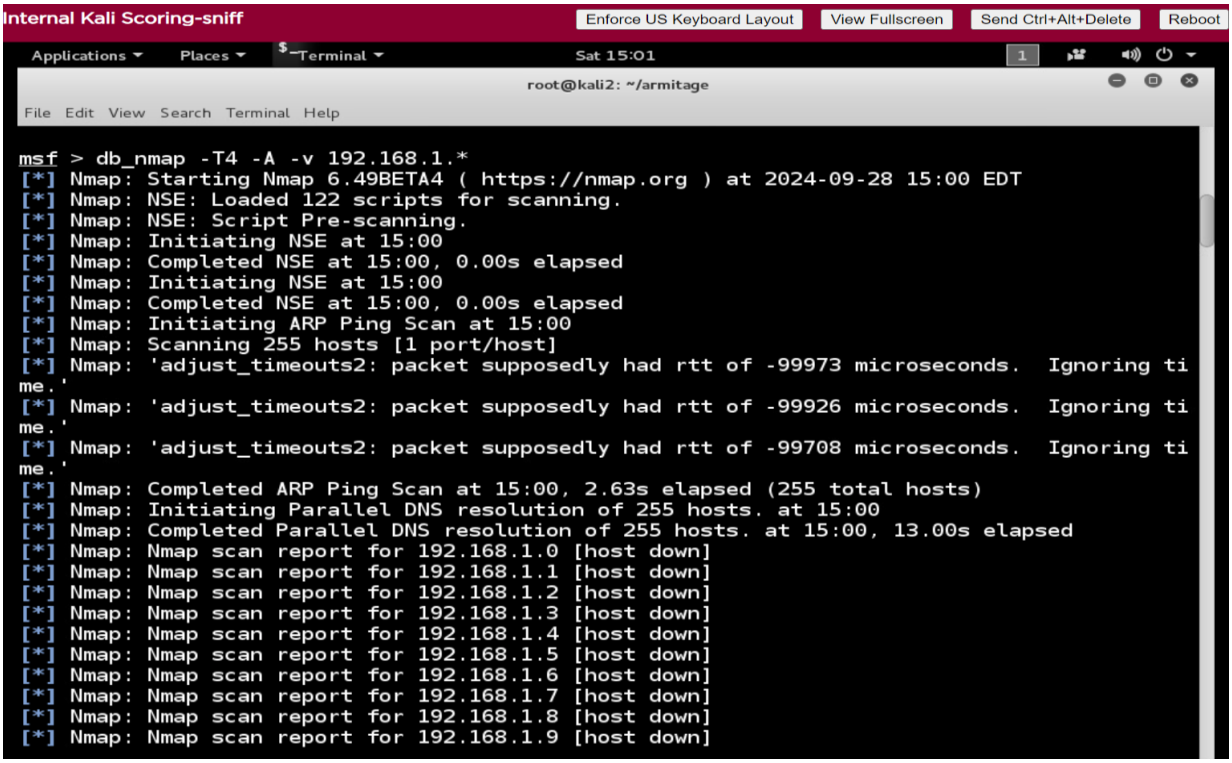


Service postgresql start

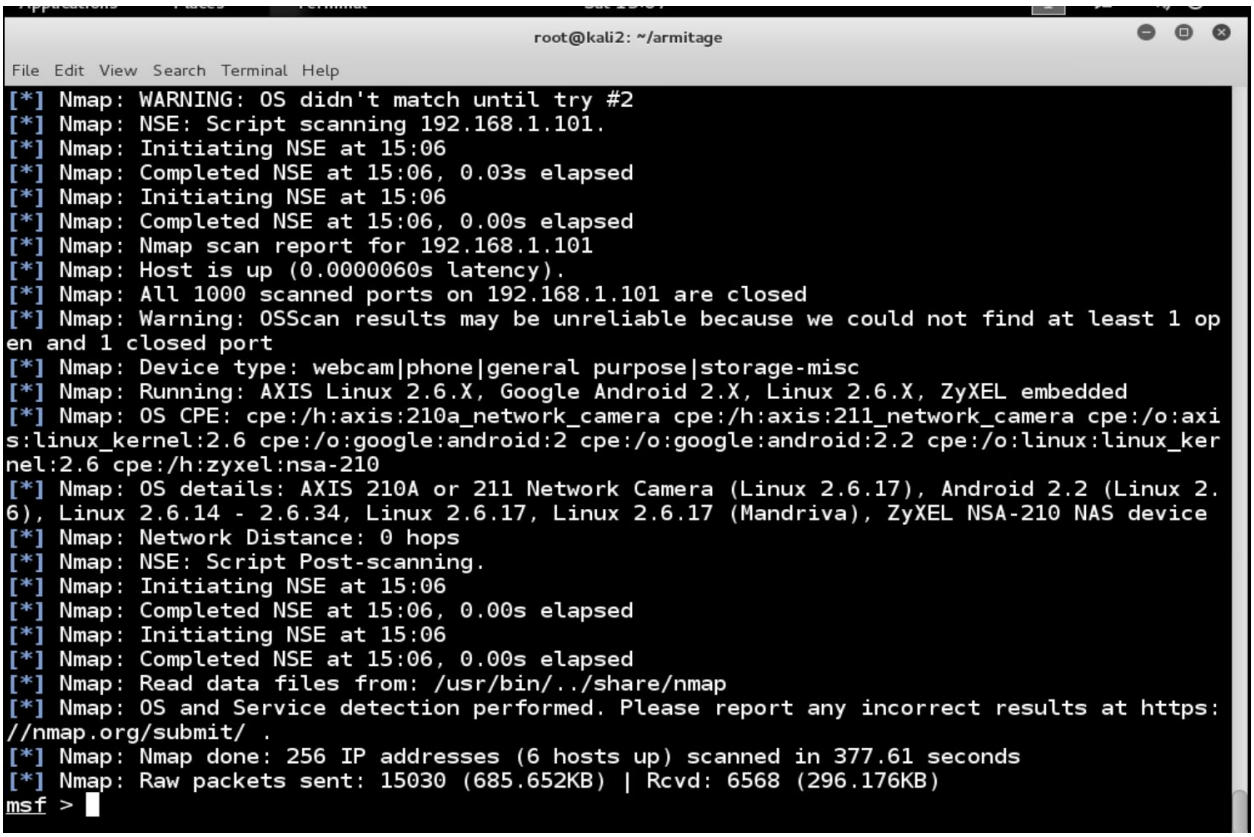
msfconsole



Db_nmap -T4 -A -v 192.168.1.*



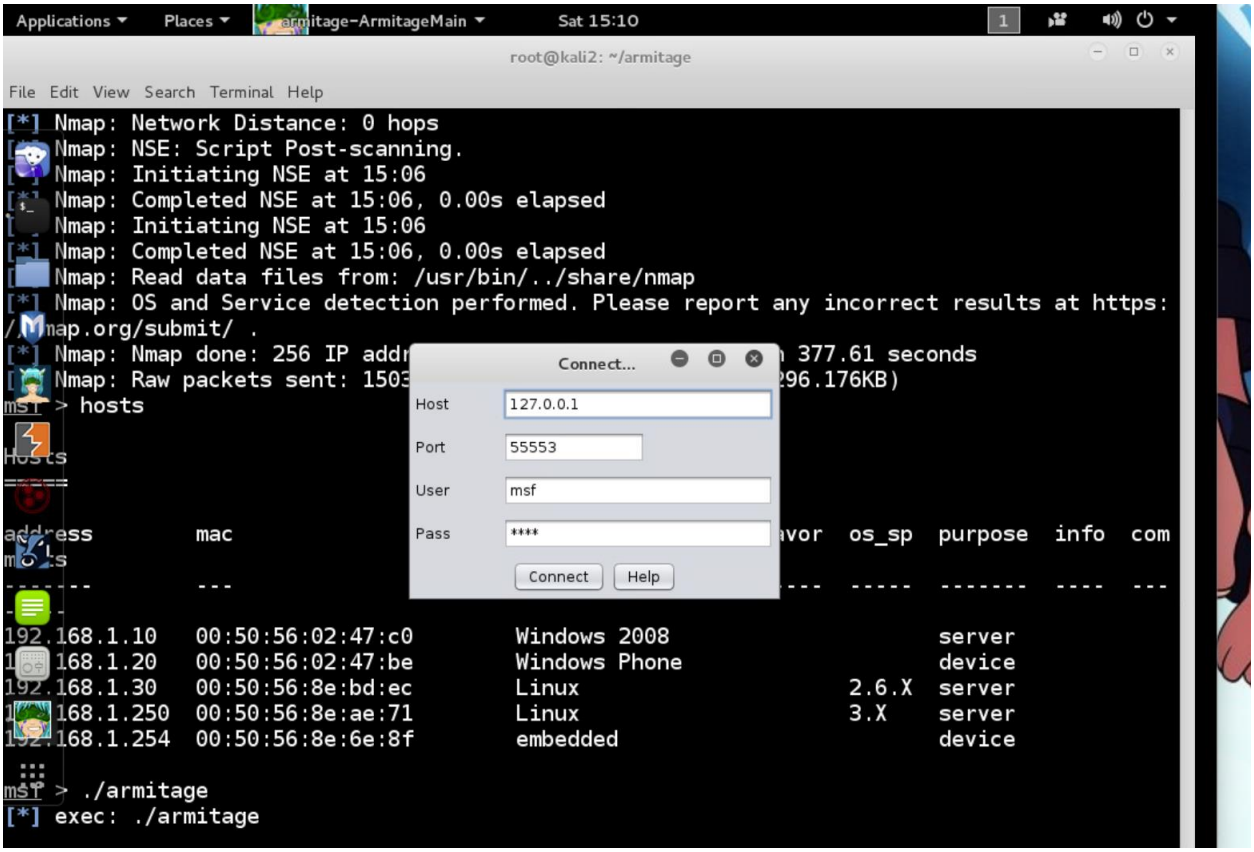
The time of Scan and no .of hosts up are displayed



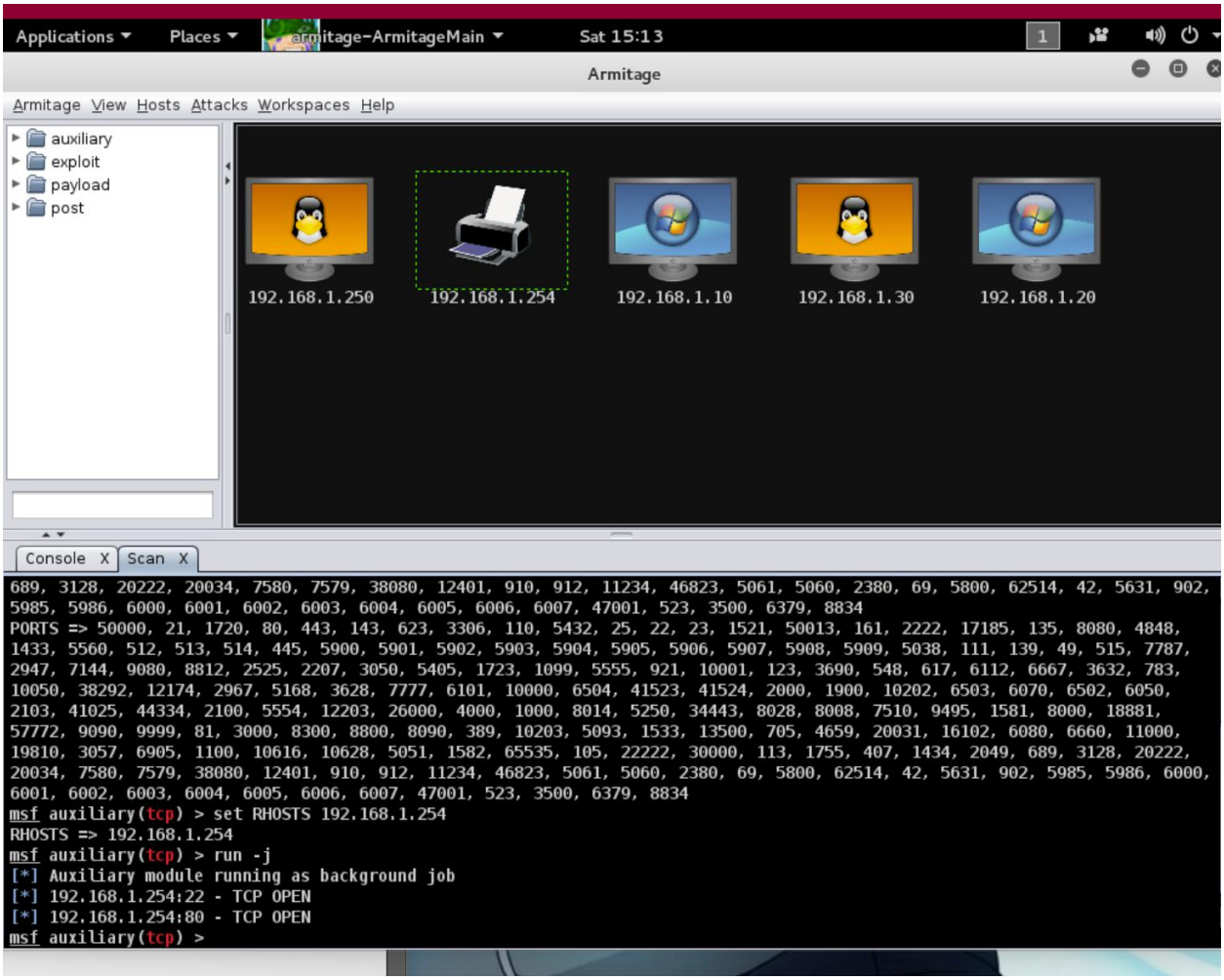
msf > hosts

```
[*] Nmap: Raw packets sent: 15030 (685.652KB) | Rcvd: 6568 (296.176KB)
msf > hosts

Hosts
=====

address        mac                name  os_name        os_flavor  os_sp  purpose  info  com
ments
-------        ---                ----  -------        ---------  -----  -------  ----  ---
-----
192.168.1.10   00:50:56:02:47:c0        Windows 2008                     server
192.168.1.20   00:50:56:02:47:be        Windows Phone                    device
192.168.1.30   00:50:56:8e:bd:ec        Linux                  2.6.X     server
192.168.1.250  00:50:56:8e:ae:71        Linux                  3.X       server
192.168.1.254  00:50:56:8e:6e:8f        embedded                         device

msf >
```

To start Armitage and clecked connect button to start Metasploit

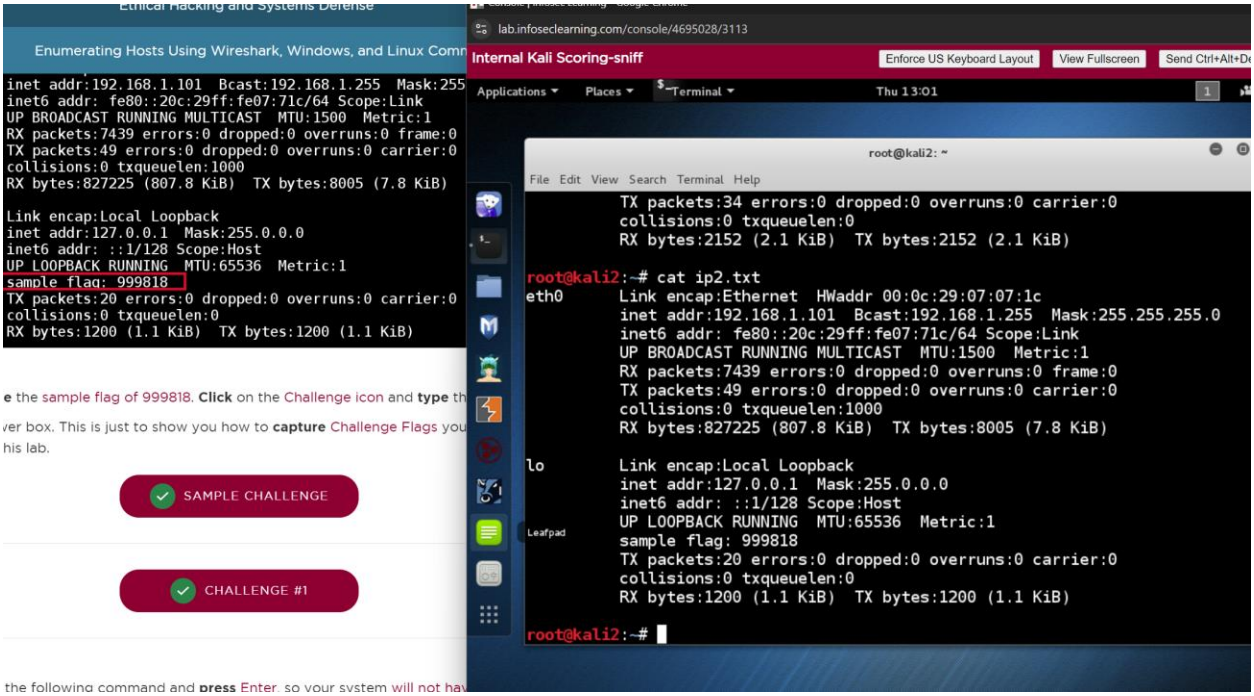


Scanning the hosts

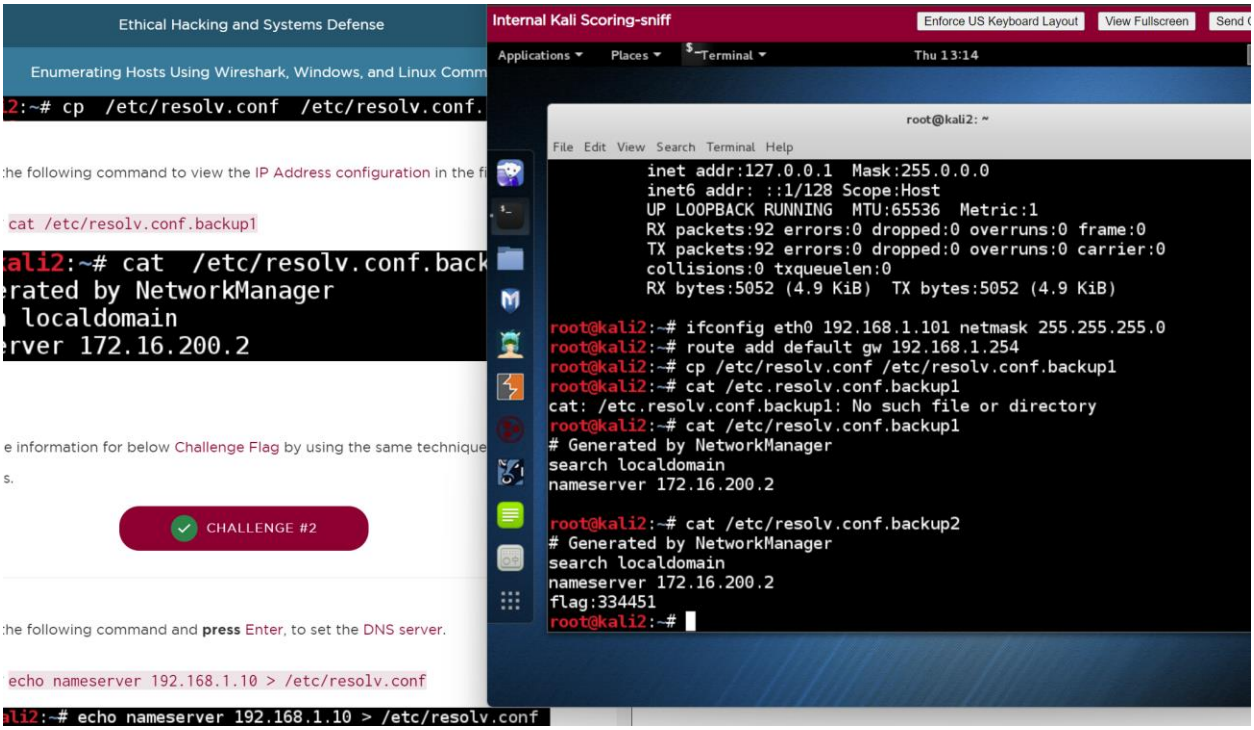


Supporting Evidence

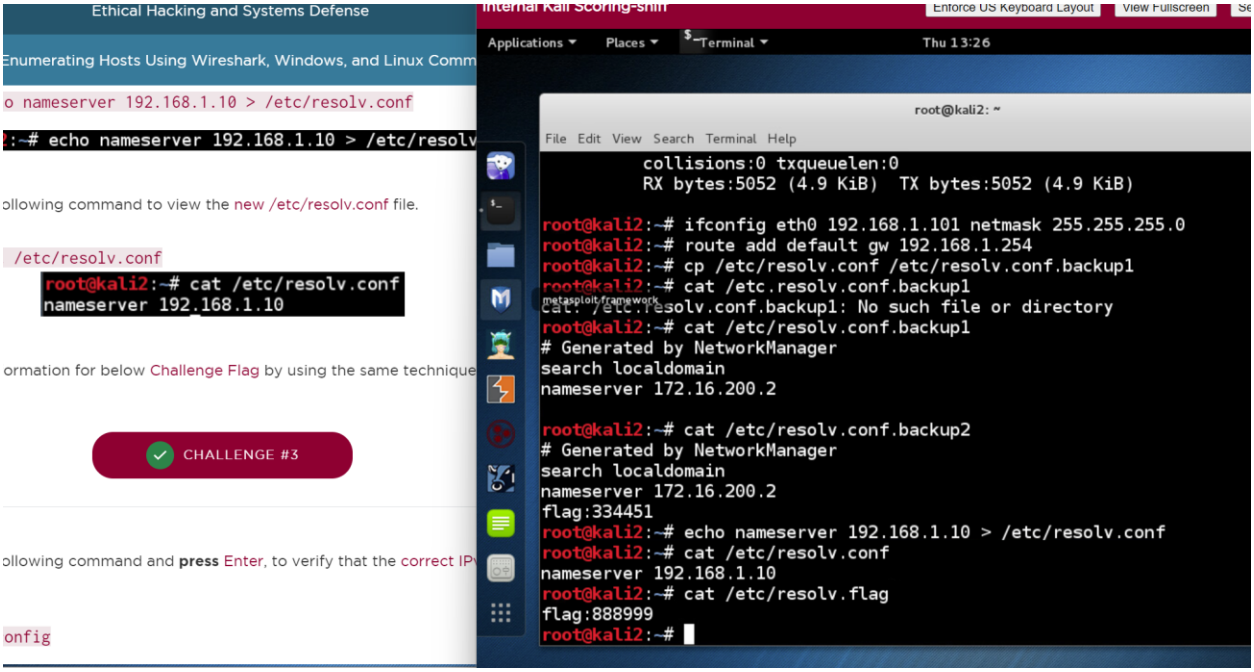
Capturing the Challenge Flag and cat ip2.txt



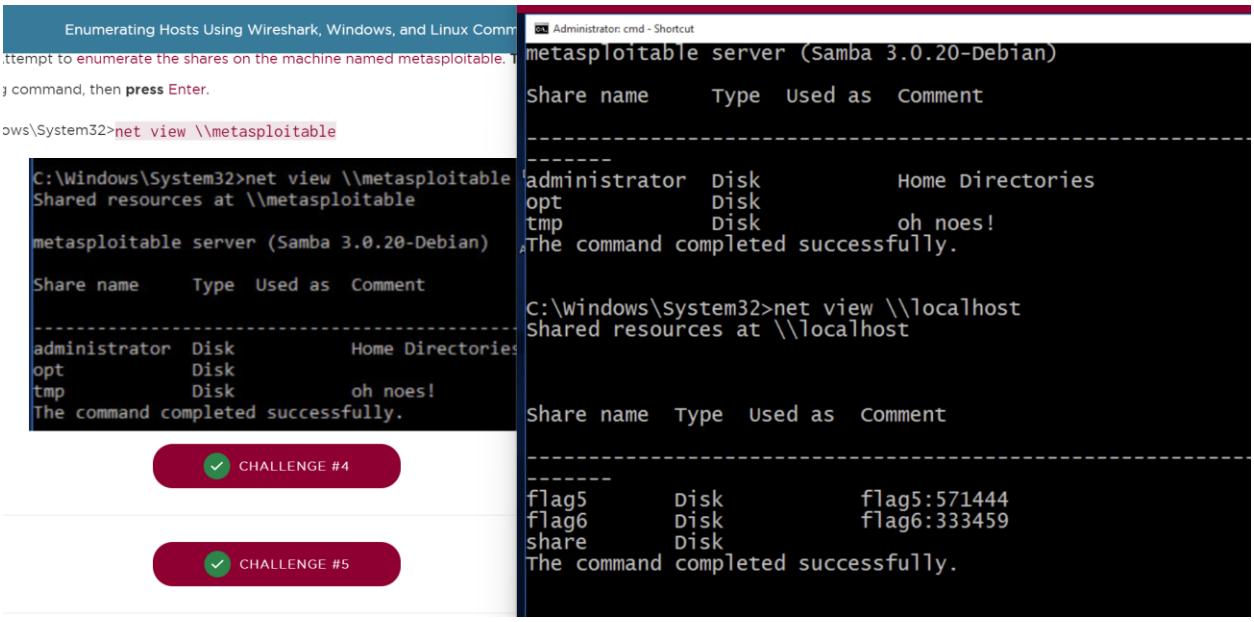
cat /etc/resolv.conf.backup2



cat /etc/resolv.flag



Captured the Flag 5 and 6 from the net view \\localhost



Conclusion & Wrap-Up

Summary with:

Observations

In this lab, I explored system enumeration using various command line and GUI tools, including db_nmap, net, nbtstat, ifconfig, Wireshark, and Armitage. I noted that active scanning techniques revealed significant information about network services and devices, but they also increased the risk of detection. In contrast, passive scanning provided insights without alerting network defenses, demonstrating its value for stealthy assessments.

Identified risks

The main risk was how easily the Postgres service could be exploited, giving unauthorized access. Once inside, the ability to escalate privileges meant full control of the system was possible. Also, using scanning tools like Nmap could alert the target, increasing the chance of being detected.

Suggested recommendations

To avoid this type of attack, it's important to keep services like Postgres updated and secured with strong passwords and configurations. Firewalls and access controls should be in place. Regular vulnerability scans can help detect and fix these issues before attackers find them.

Your successes & failures

I successfully exploited the Postgres service and gained higher privileges, showing how a simple vulnerability can lead to complete system takeover. However, I struggled with setting up openVAS at first, which slowed down the scanning process.

Challenges

I faced challenges in analyzing large volumes of data from Wireshark, requiring more time and focus for effective interpretation. Variations in network configurations complicated the enumeration process, making it difficult to draw clear conclusions. Additionally, generating Nmap scans for hosts took a long time, and balancing thorough scanning with stealth remained a constant challenge, especially with active techniques.