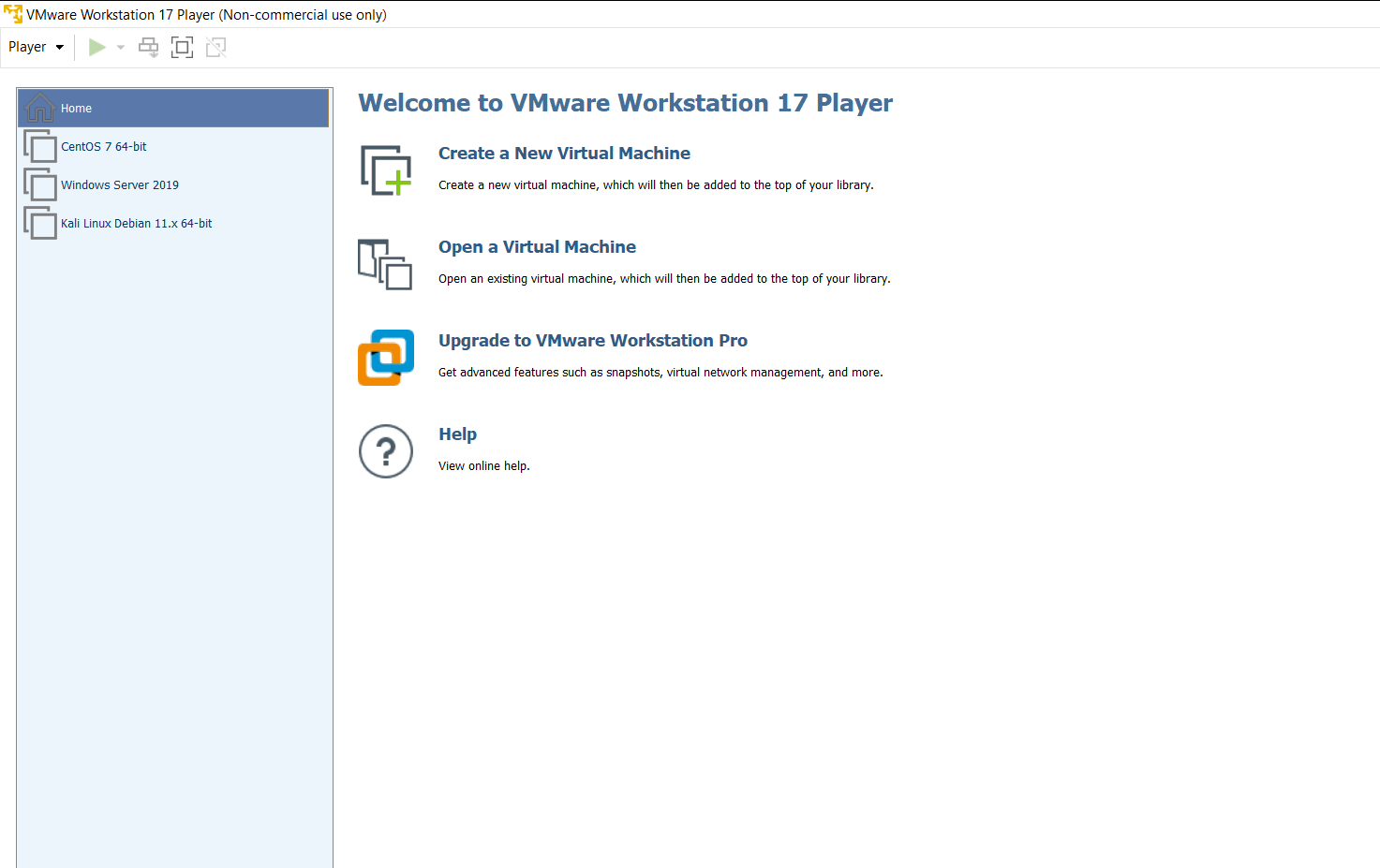
**Introduction to Cybersecurity**

**Capstone Project: Performing Reconnaissance Using Kali Linux VM and Windows Server VM**

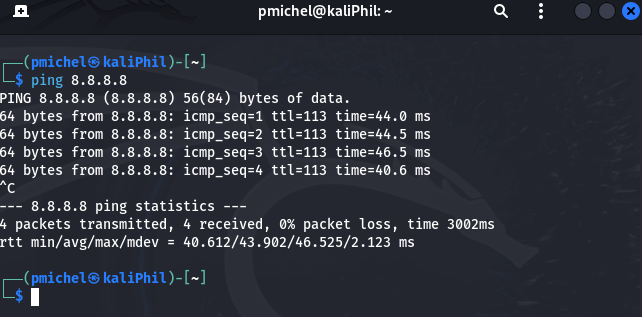
**There are three Virtual Machines (VMs) installed on VMware Workstation 17 Player on my laptop: Centos7 64-bit, Windows Server 2019 and Kali Linux 64-bit. However the two VMs that will be used for this Capstone Project are Windows Server 2019 and Kali Linux.**

****

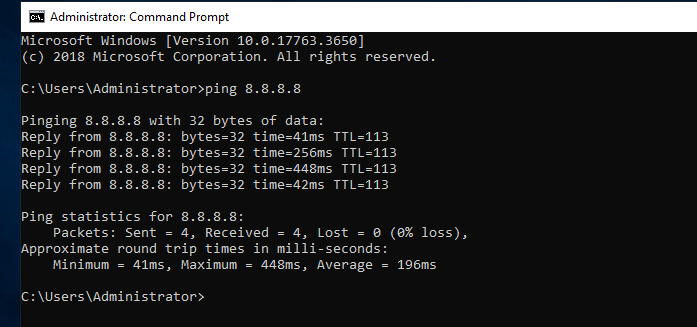
1. **Ensure VMs are Active and Have Network Connectivity.**

Both VMs Windows Server and Kali Linux are active and have network connectivity. Both are configured with network bridge adapters set to the same virtual network.

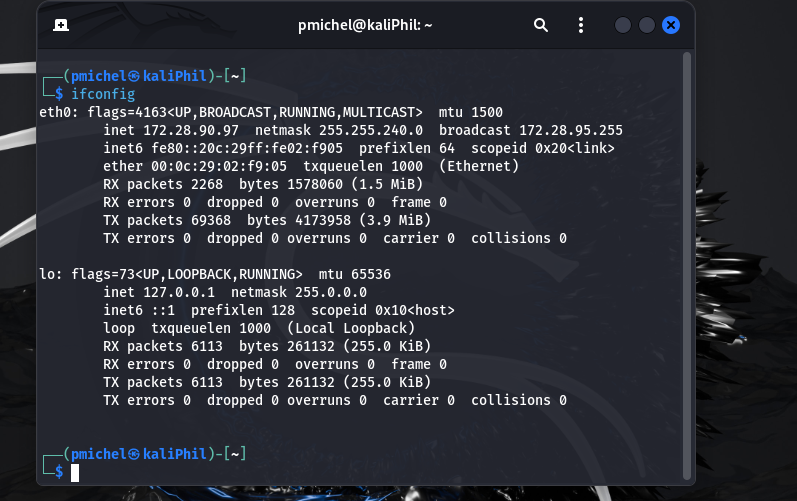
Kali Linux pinging 8.8.8.8



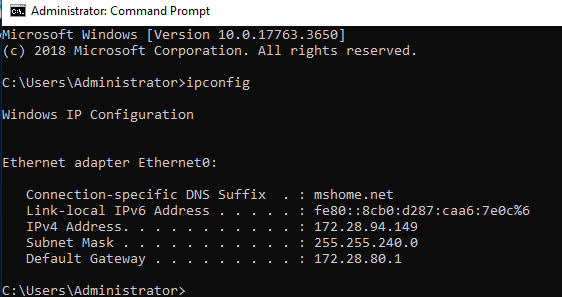
Windows Server pinging 8.8.8.8



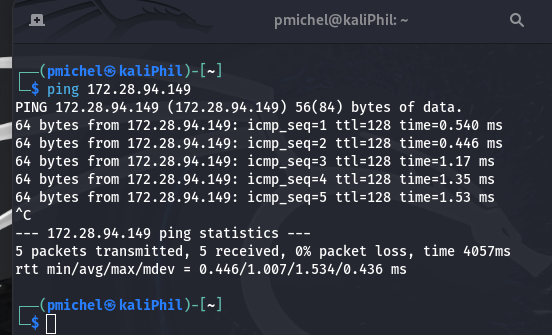
1. **Run ifconfig on Kali Linux VM, ipconfig on Windows Server VM and** **Verify Connectivity and IP addresses**
2. Kali Linux VM from ifconfig command: 172.28.90.97



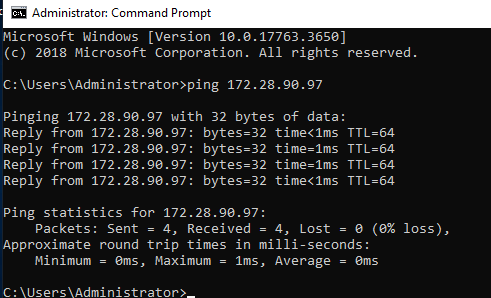
1. Windows Server VM from ipconfig command: 172.28.94.149



Kali Linux VM pinging Windows Server VM’s IP address 172.28.94.149

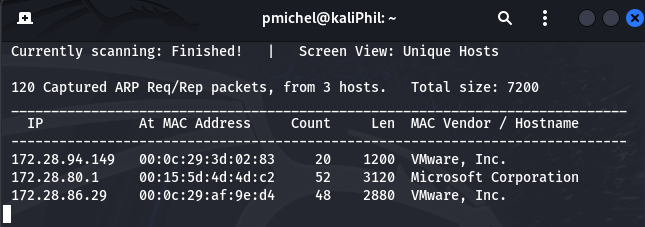


Windows Server VM pinging Kali Linux VM’s IP address 172.28.90.97



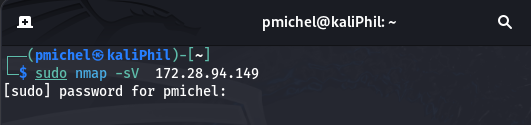
1. **Use the ‘netdiscover’ command on the Kali Linux VM to perform a network discovery scan.**

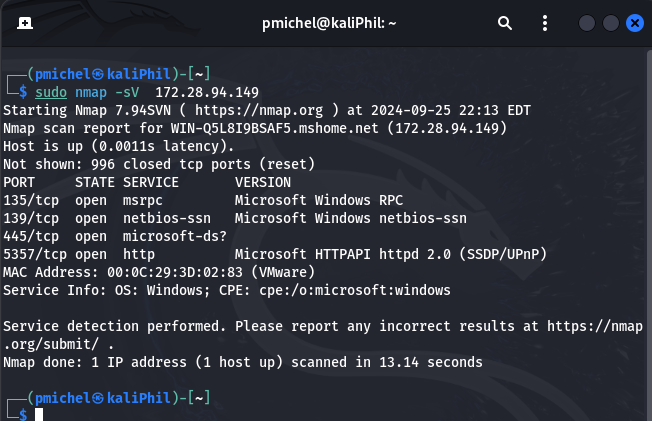
****

****

The command was performed and the results scanned a range of three live hosts with their respective IP addresses currently running in 172.28.0.0/16 network.

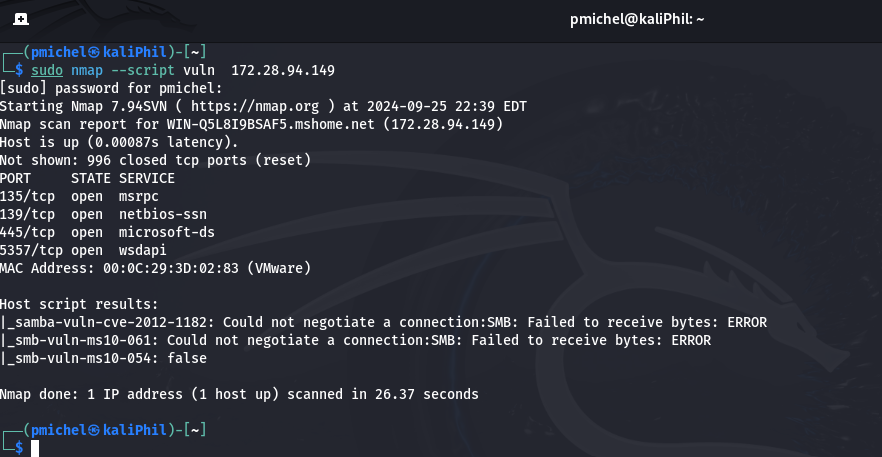
1. **Perform NMAP Scan to identify Running Services:**





The results for port scan show a list of four open tcp ports but 996 tcp ports are closed.

1. **Perform NMAP Vulnerability Scan**



The Nmap vuln script command scanned for common vulnerabilities. The results show that the Windows Server VM is not vulnerable for these vulnerabilities.