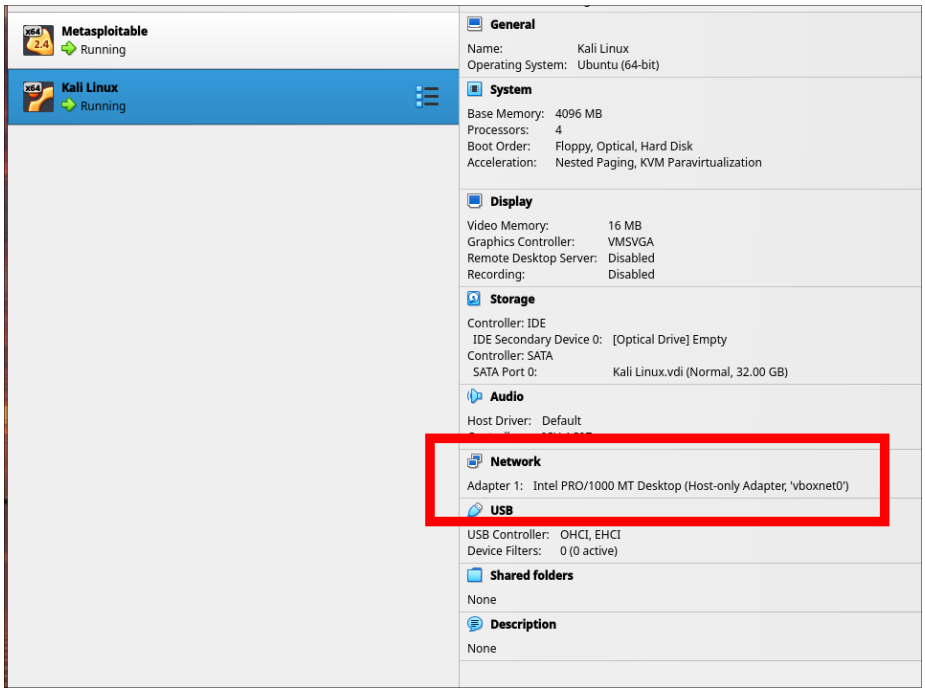
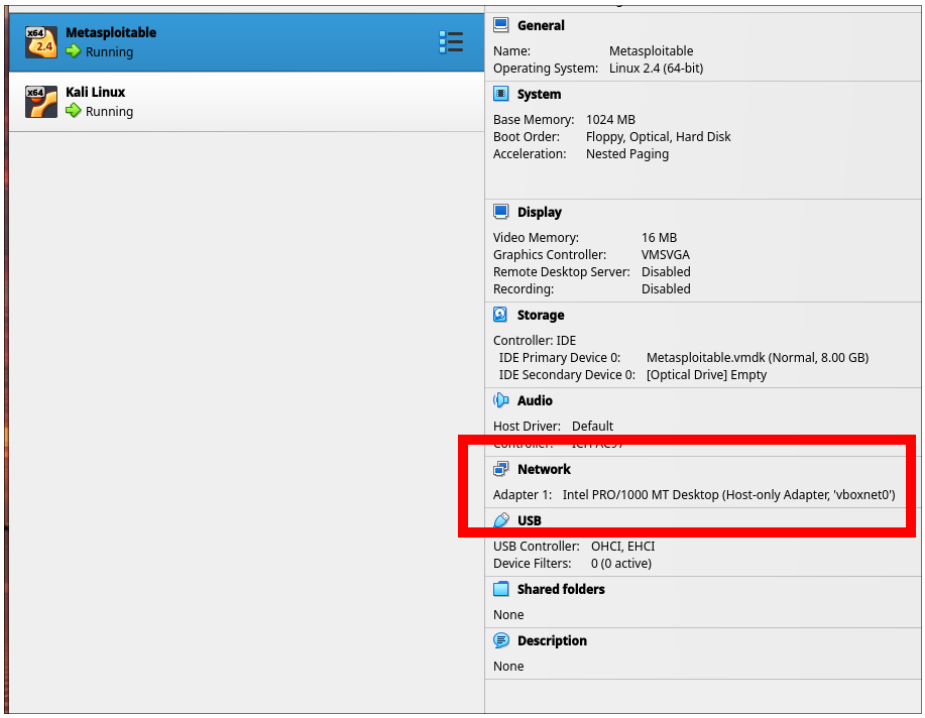
Ethical Hacking Assignment 3 - Aidan Sharpe

Task 1 - Network Configuration Between Kali and Metasploitable

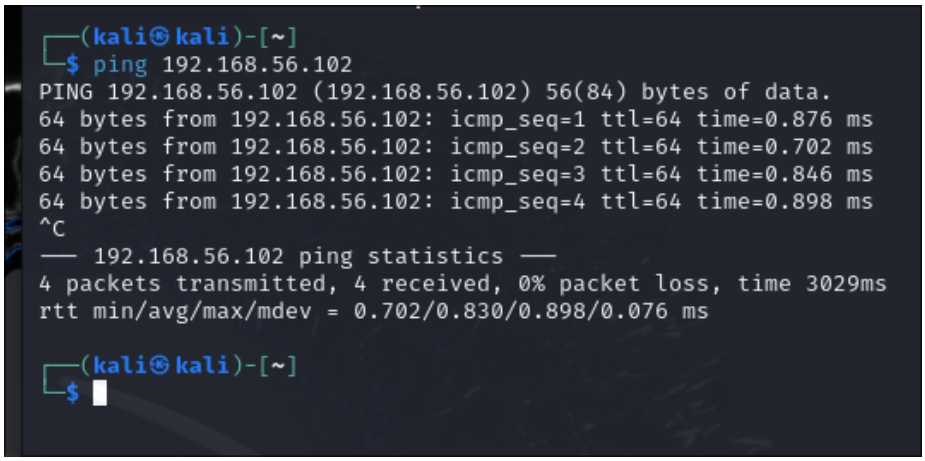
Ensure proper network connectivity between the attacker (Kali Linux) and victim (Metasploitable) virtual machines.

1. Configure both Kali Linux and Metasploitable VMs to use host-only adapters



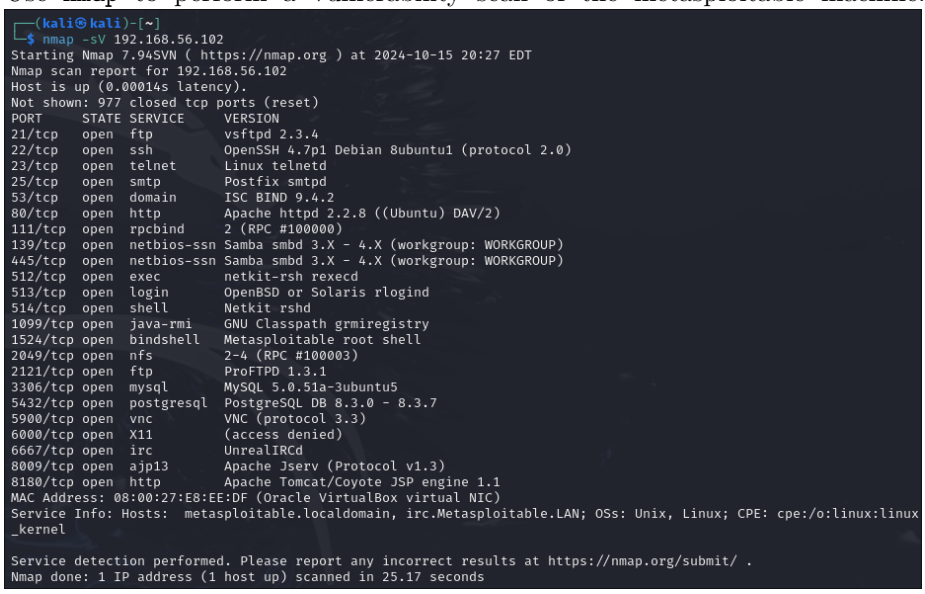


2. Verify the network connectivity by pinging Metasploitable from Kali Linux



Task 2 - Nmap Scan for Open Ports and Vulnerabilities

Use `nmap` to perform a vulnerability scan of the metasploitable machine.

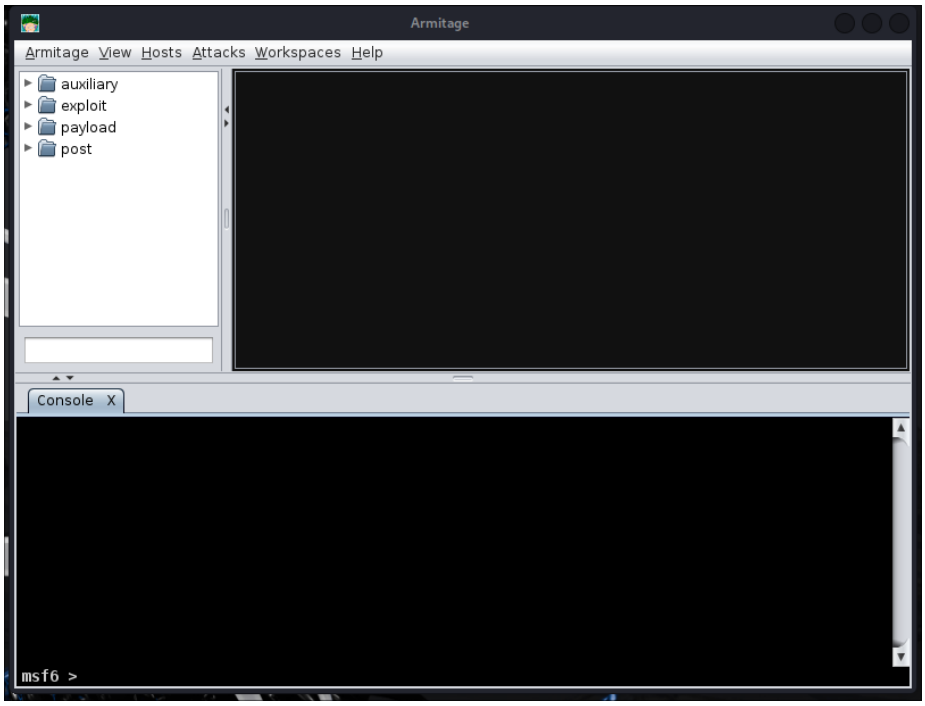


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 20:27 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:E8:EE:DF (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.17 seconds
```

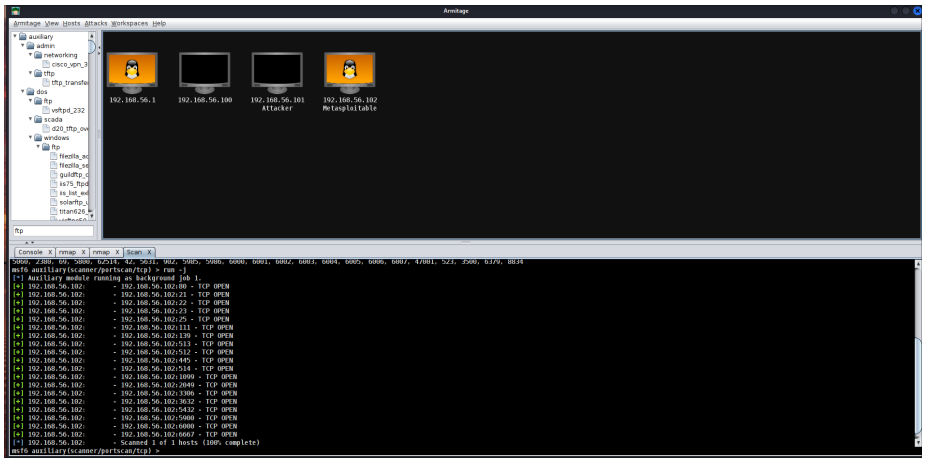
Task 3 - Installing and Launching Armitage

Install Armitage and set it up to connect with the Metasploit framework.



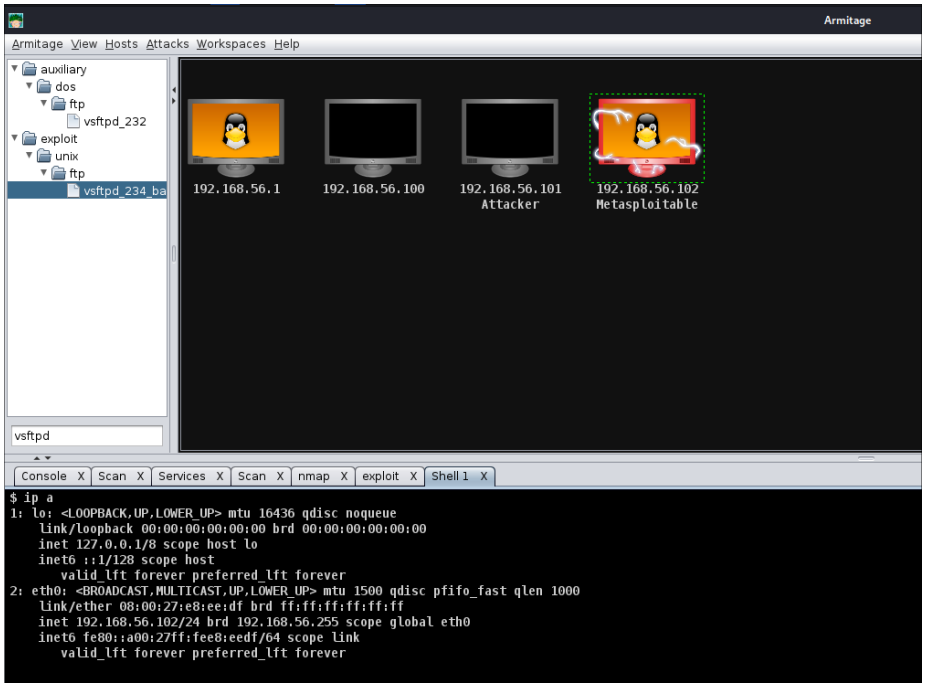
Task 4 - Perform a Vulnerability Scan with Armitage

Use Armitage to scan the Metasploitable machine and identify potential vulnerabilities.



Task 5 - Exploiting a Vulnerability Using Armitage

Use Armitage to exploit a vulnerability on the Metasploitable machine and gain access.



Reflection

The `nmap` tool is suprisingly easy, yet very powerful. After using it on this assignment, I used it to learn about vulnerabilities on my home server. I found that I had ports 80, 443, and 22 open. I did not realize that I had left it open, and I couldn't remembery why I had it open in the first place. I then used a remote network configuration tool to close port 80. After running `nmap` again, I saw that I had successfully closed the port.

I really enjoyed using Armitage as an easy introduction to the Metasploit Framework. At this point, I really only plan to use it as a learning tool to get used to deploying attacks and scanning networks. Today, for example, I learned about scanning IP ranges. My next step is to switch to the metasploit CLI.