Franklin Nuth

CSC432: Computer and Information Security

Lab #9: Vulnerability Assessment

29 March 2019

Abstract

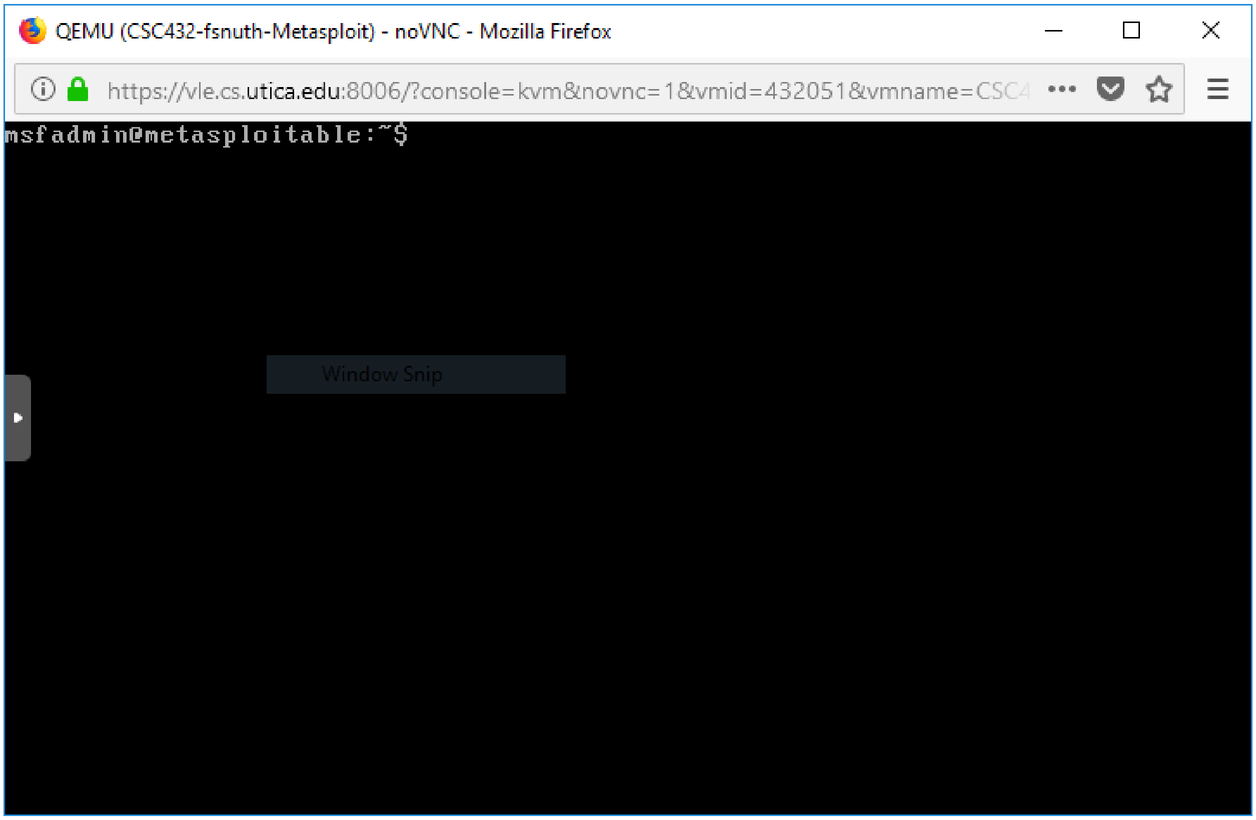
In Lab 9, I will be activating the Metasploit 2 machine on my network for testin vulnerability scanning. After configuring the Metasploit 2's interface, I will use NMAP on my Kali virtual machine to learn about looking for weaknesses in said machine. I will also attempt to install OpenVAS in my Kali Linux, an open-source software that scans for vulnerabilities on specific machines.

Introduction

Vulnerability assessment is a topic in Cybersecurity that security administrators of all levels can have a word in. One half argues that vulnerability assessment is a danger due to the fact that hackers can use it for reconnaissance. The other half argues that vulnerability assessment software can provide the information needed for admins to harden their networks. My job does not include getting involved in this debate, but learning to use the vulnerability assessment software for myself and see how much it can assist me in my administrator endeavors. I suspect that learning more about NMAP and OpenVAS will help me navigate networks with better efficiency.

Processes & Screenshots

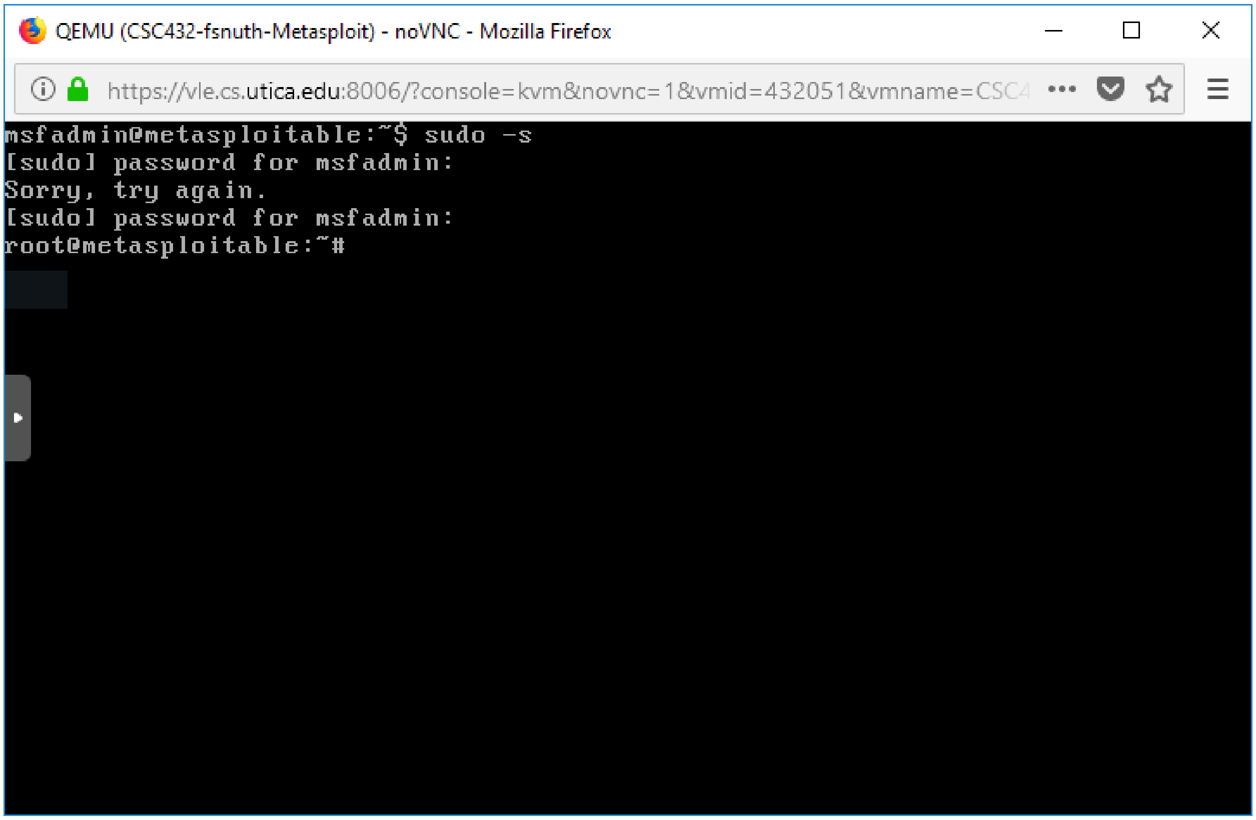
The first thing that I needed to do was start up the Metasploit 2 machine on my network. The purpose of the Metasploit 2 will be to act as a training dummy for my hacking or security shenanigans.


QEMU (CSC432-fsnuth-Metasploit) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432051&vmname=CSC4
Window Snip

```
msfadmin@metasploitable:~$
```

(Proof that I can log into my Metasploit 2 machine on my network. It is now ready for future labs and abuse.)

In order to the next couple of steps that involve configuring the network information of my Metasploit 2, I needed to elevate myself to become the root user.

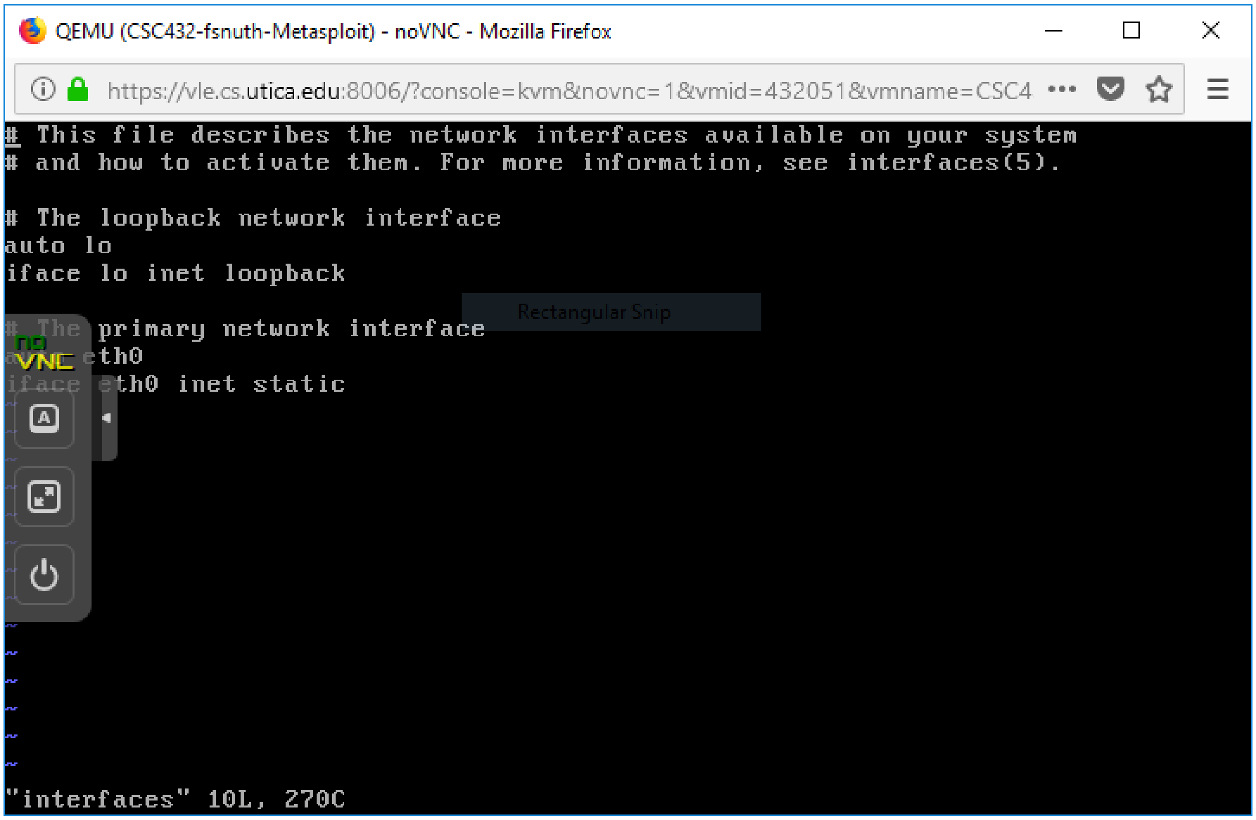


QEMU (CSC432-fsnuth-Metasploit) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432051&vmname=CSC4

```
msfadmin@metasploitable:~$ sudo -s
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
root@metasploitable:~#
```

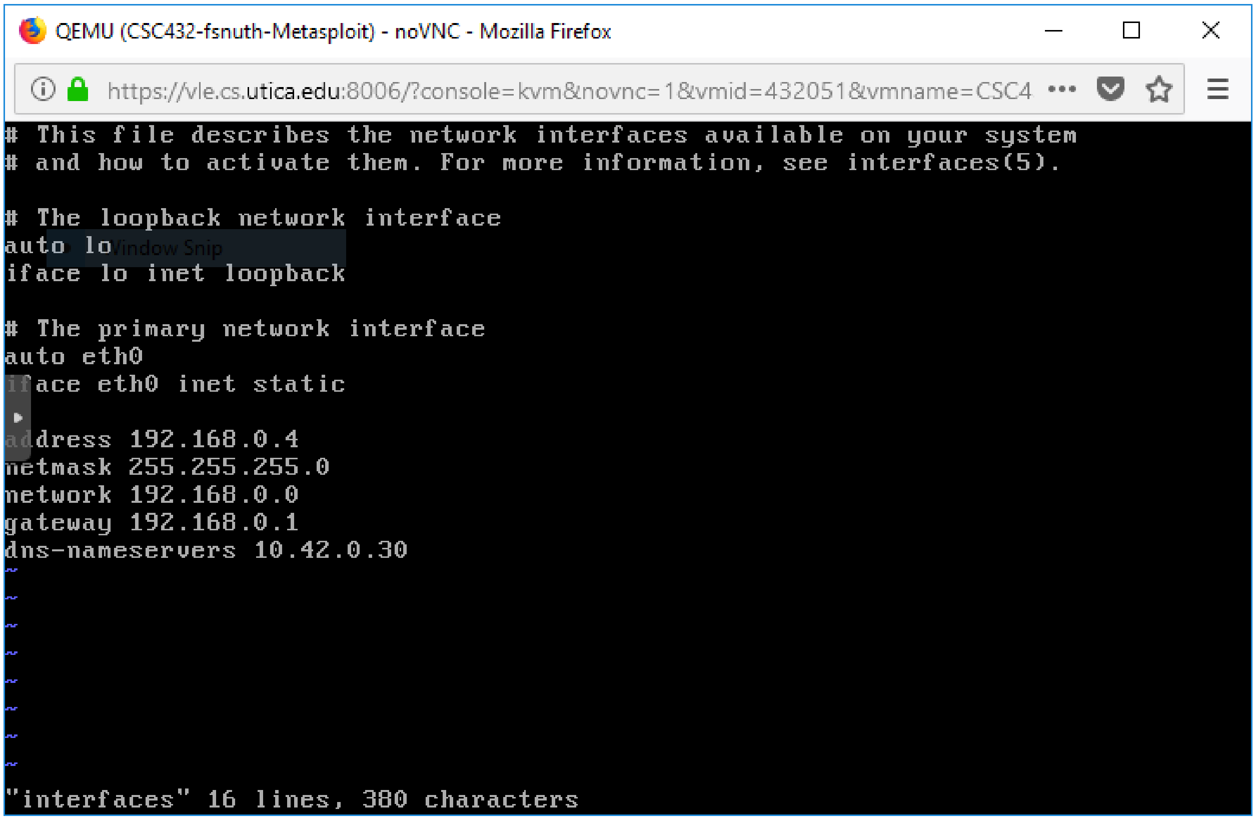
(Raising myself to become the root user. The Metasploit 2 now respects my authority.)

Now is the time to configure the network information of this machine. I typed "vi /etc/network/interfaces" to go to my interfaces file located in the network directory.


QEMU (CSC432-fsnuth-Metasploit) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432051&vmname=CSC4
Rectangular Snip
noVNC

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"interfaces" 10L, 270C
```

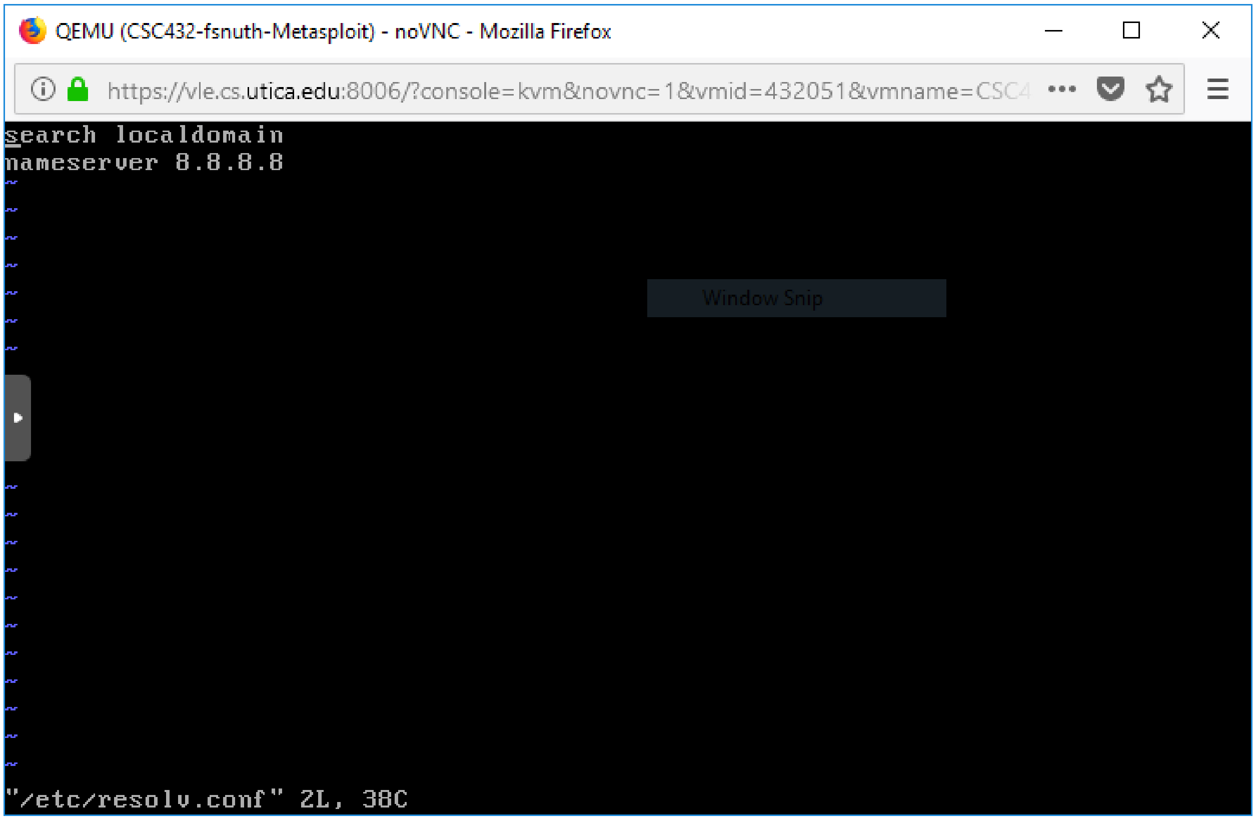
(Changing the line "iface eth0 inet dhcp" to "iface eth0 inet static". This change alone will allow me to set the network information that I want for this machine, rather than letting DHCP do the configuration for me.)


QEMU (CSC432-fsnuth-Metasploit) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432051&vmname=CSC4
Window Snip

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static

address 192.168.0.4
netmask 255.255.255.0
network 192.168.0.0
gateway 192.168.0.1
dns-nameservers 10.42.0.30
~
~
~
~
~
~
~
~
"interfaces" 16 lines, 380 characters
```

(Now that I can set up my own network information, I proceeded to do so. The address corresponds to the IP address for the Metasploit 2, the net mask is a class C, the network is the network ID for the WLAN, the gateway is the IP address of my router's external interface, and the dns-nameservers is the IP address of the Darknet server.)

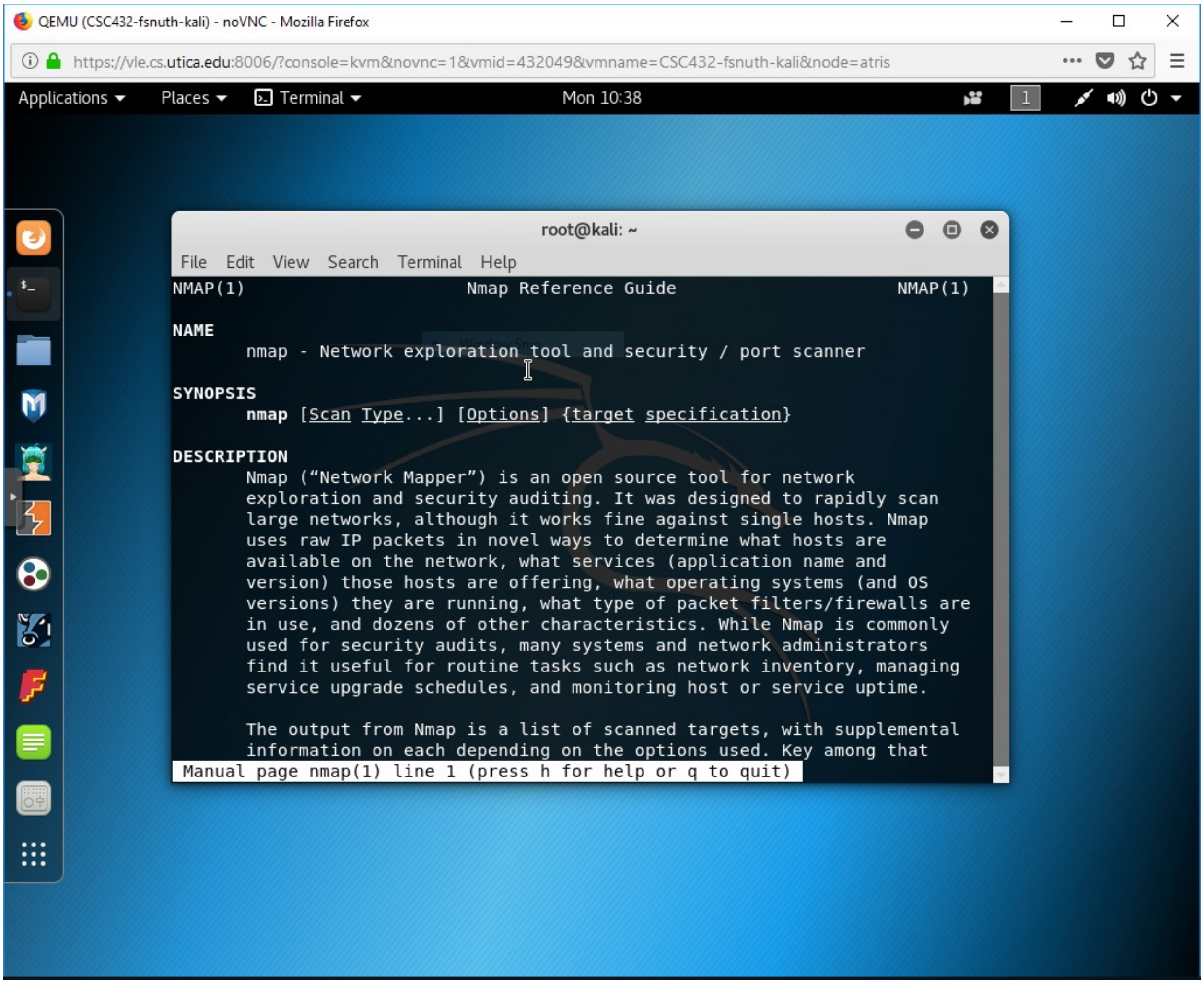
To further specify the DNS that I want to use, I typed "vi /etc/resolv.conf" so I can configure the resolv.conf file for my needs.


QEMU (CSC432-fsnuth-Metasploit) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432051&vmname=CSC4
Window Snip

```
search localdomain
nameserver 8.8.8.8
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/resolv.conf" 2L, 38C
```

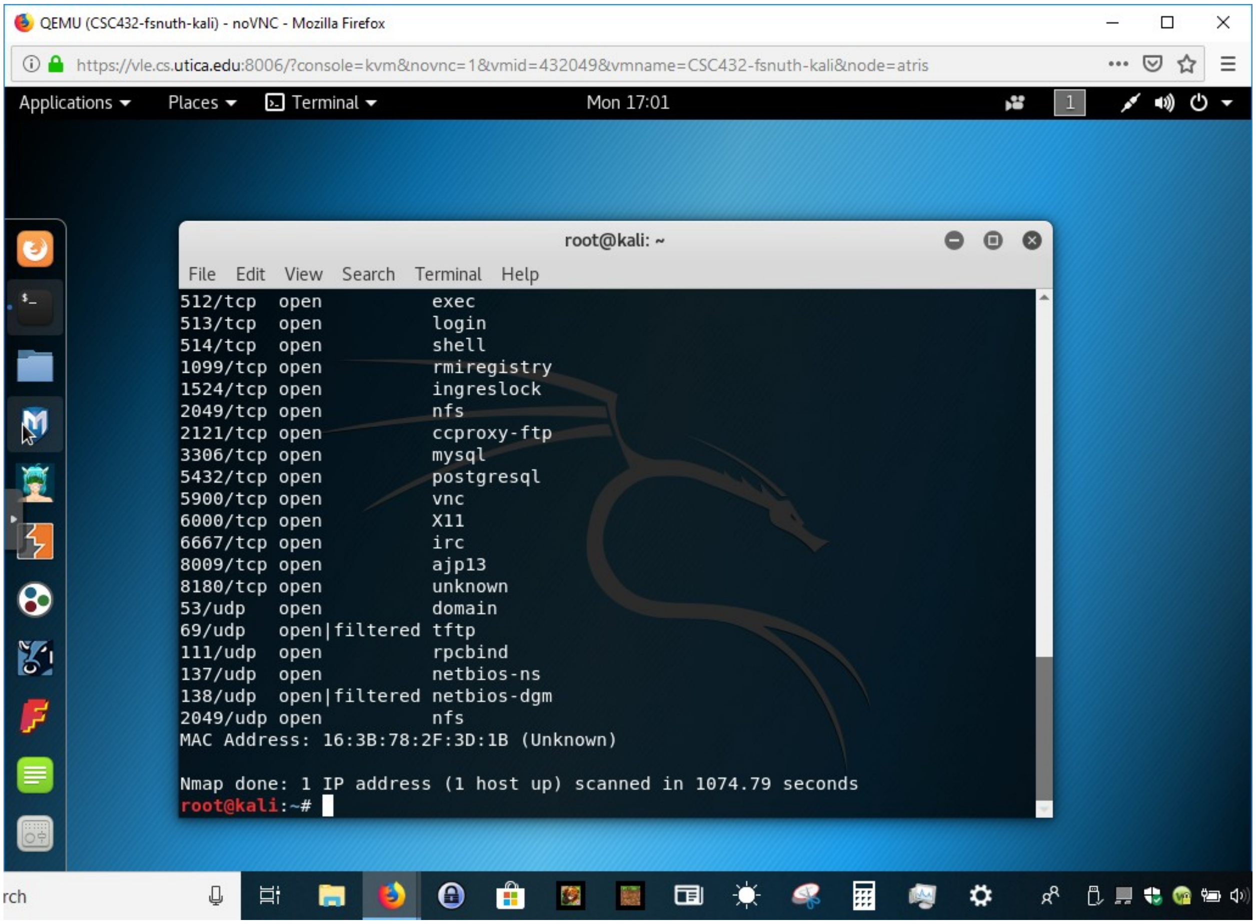
(Replacing the previous nameserver with the new information, 8.8.8.8)

After this, I typed "/etc/init.d/ networking restart", to restart the networking service so that the Metasploit 2 machine can put its new configuration into place. I confirmed that everything works by pinging the default gateway. For a finishing touch, I also pinged the Metasploit 2 machine from my Kali on the virtual network. NMAP, or Network Mapper, will profile whatever systems and devices that I point it to. I will be applying my knowledge with NMAP in four ways; I will check the manual that is implemented, check for all TCP and UDP services on my Metasploit 2, do it again except printing out the versions also, and looking up a service's vulnerability of my own choosing through the National Vulnerability Database's website.


QEMU (CSC432-fsnuth-kali) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432049&vmname=CSC432-fsnuth-kali&node=atris
Applications
Places
Terminal
Mon 10:38
1
root@kali: ~
File
Edit
View
Search
Terminal
Help

```
NMAP(1)                      Nmap Reference Guide                     NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
       Nmap (“Network Mapper”) is an open source tool for network
       exploration and security auditing. It was designed to rapidly scan
       large networks, although it works fine against single hosts. Nmap
       uses raw IP packets in novel ways to determine what hosts are
       available on the network, what services (application name and
       version) those hosts are offering, what operating systems (and OS
       versions) they are running, what type of packet filters/firewalls are
       in use, and dozens of other characteristics. 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.

       The output from Nmap is a list of scanned targets, with supplemental
       information on each depending on the options used. Key among that
 Manual page nmap(1) line 1 (press h for help or q to quit)
```

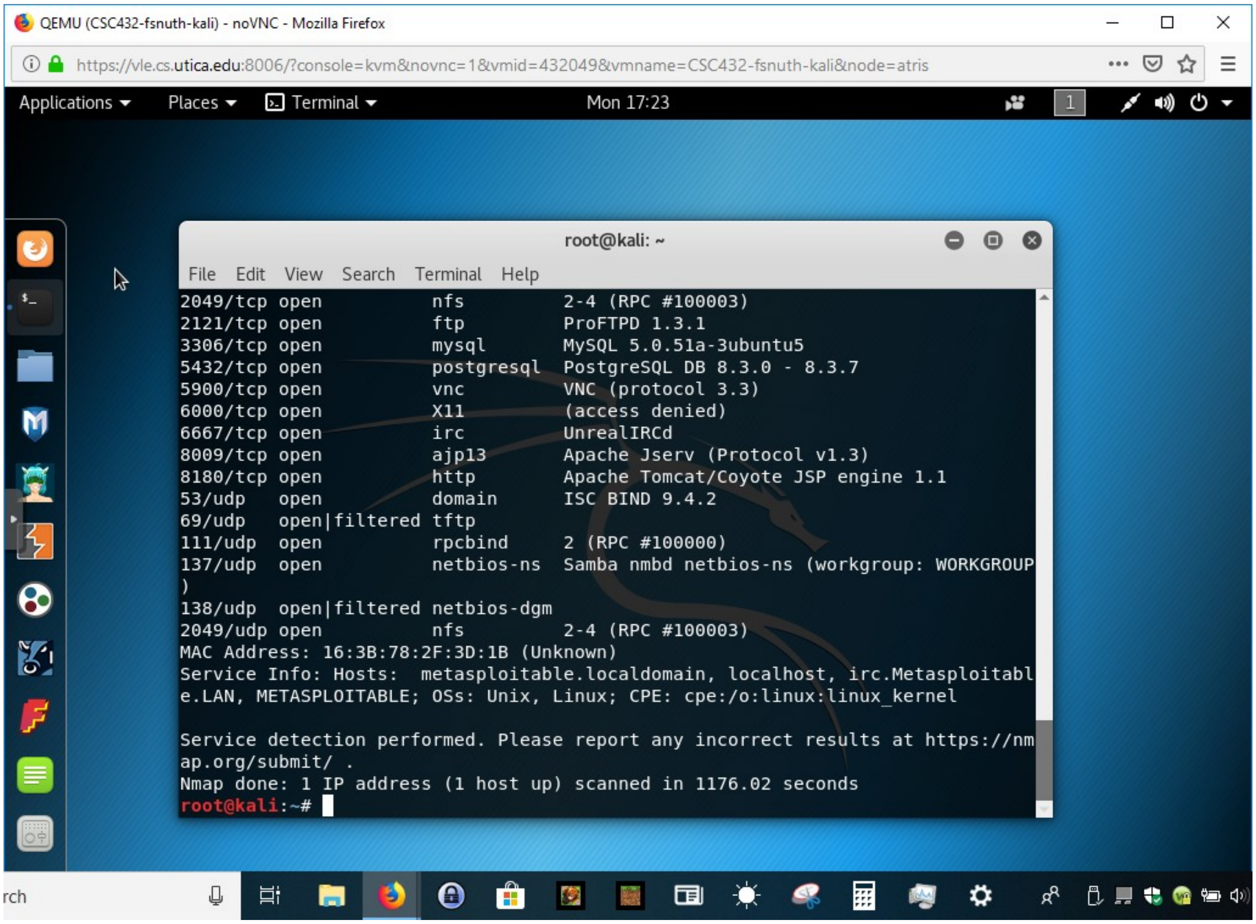
(The result of typing “man nmap” in the terminal. It shows everything I can do with nmap, if I were to scroll down.)



QEMU (CSC432-fsnuth-kali) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432049&vmname=CSC432-fsnuth-kali&node=atris
Applications
Places
Terminal
Mon 17:01
root@kali: ~
File Edit View Search Terminal Help

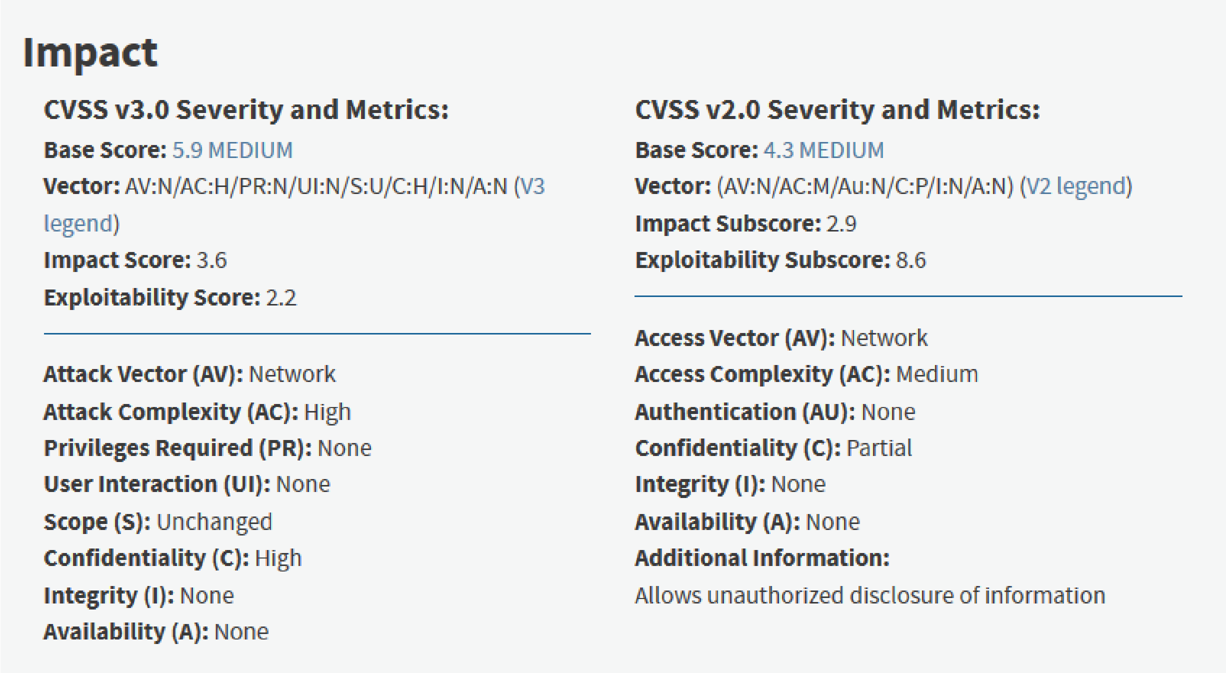
```
512/tcp  open          exec
513/tcp  open          login
514/tcp  open          shell
1099/tcp open          rmiregistry
1524/tcp open          ingreslock
2049/tcp open          nfs
2121/tcp open          ccproxy-ftp
3306/tcp open          mysql
5432/tcp open          postgresql
5900/tcp open          vnc
6000/tcp open          X11
6667/tcp open          irc
8009/tcp open          ajp13
8180/tcp open          unknown
53/udp   open          domain
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 16:3B:78:2F:3D:1B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1074.79 seconds
root@kali:~#
```

(Checking for all running TCP and UDP services on the Metasploit 2. This took about 20 minutes to scan.)


QEMU (CSC432-fsnuth-kali) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432049&vmname=CSC432-fsnuth-kali&node=atris
Applications
Places
Terminal
Mon 17:23
1
root@kali: ~
File Edit View Search Terminal Help
rch

```
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
53/udp   open          domain      ISC BIND 9.4.2
69/udp   open|filtered tftp
111/udp  open          rpcbind     2 (RPC #100000)
137/udp  open          netbios-ns  Samba nmbd netbios-ns (workgroup: WORKGROUP
)
138/udp  open|filtered netbios-dgm
2049/udp open          nfs         2-4 (RPC #100003)
MAC Address: 16:3B:78:2F:3D:1B (Unknown)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitabl
e.LAN, METASPLOITABLE; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1176.02 seconds
root@kali:~# 
```

(Using nmap to scan for TCP and UDP services, as well as their versions. This also took 20 minutes. That’s barely enough time to sit in the parking lot without looking suspicious.)



Impact

CVSS v3.0 Severity and Metrics:

Base Score: 5.9 MEDIUM
Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N (V3 legend)
Impact Score: 3.6
Exploitability Score: 2.2

Attack Vector (AV): Network
Attack Complexity (AC): High
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): None
Availability (A): None

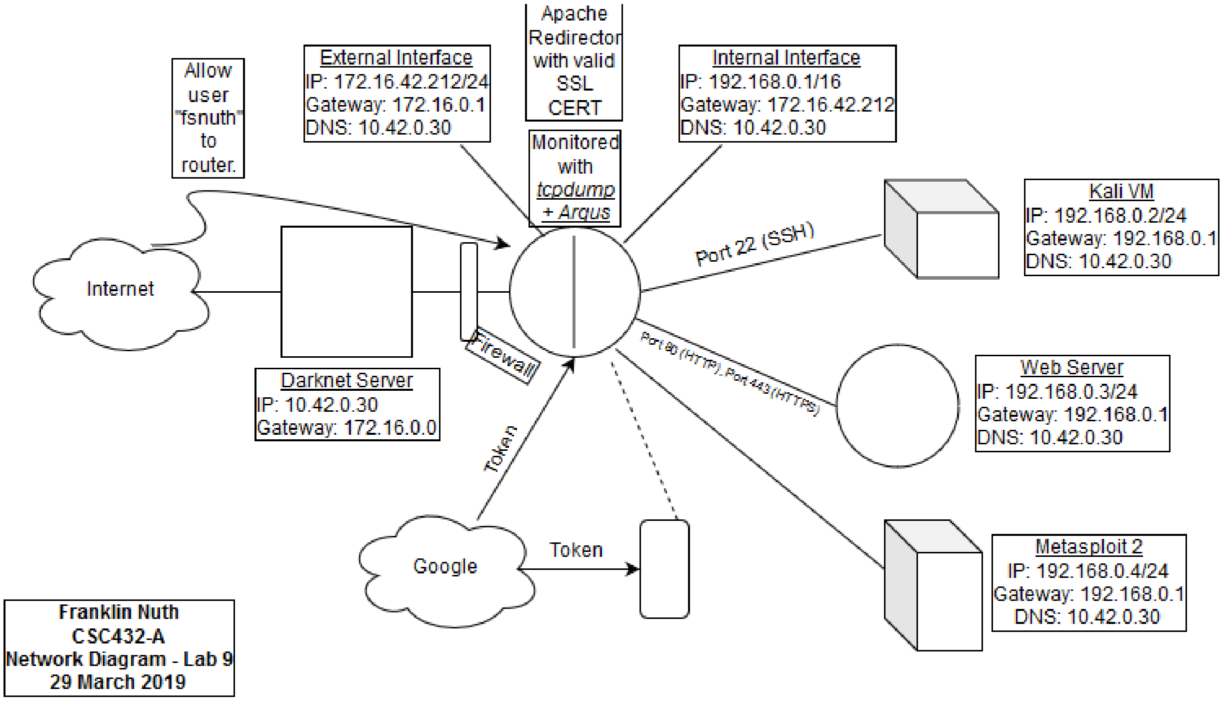
CVSS v2.0 Severity and Metrics:

Base Score: 4.3 MEDIUM
Vector: (AV:N/AC:M/Au:N/C:P/I:N/A:N) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 8.6

Access Vector (AV): Network
Access Complexity (AC): Medium
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): None
Availability (A): None
Additional Information:
Allows unauthorized disclosure of information

(One of the services that I decided to look up is called MySQL attack. This attack can be done when one has a rogue MySQL server, and the user has access to the web server. The hacker can then read any file with his permission.)

Now is the time for me to touch upon OpenVAS. OpenVAS is a vulnerability scanning software that is good at what it does, but its downside of consuming large amounts of memory kept it from becoming an excellent program in the eyes of both admins and hackers alike. Nevertheless, I will still use it to look for vulnerabilities on my Metasploit 2. I will do it when OpenVAS finish installing.



Issues & Resolutions

One of the issues I had in the lab was getting the packages for OpenVAS. Because the distribution used for my virtual Kali machine was of a newer version, it does not have the data needed to install and setup my OpenVAS software. Because of this, I spent at least two hours getting all the packages I need to install this. Although it took a long time, I have everything I need to start running OpenVAS and finish the lab.

Conclusion

This lab taught me that Metasploit 2 is a quality virtual machine to test out hacks and vulnerability scanning. I have learned that you can scan specific ports and IP addresses with NMAP. OpenVAS can be used for the same purposes. They are both great tools for vulnerability scanning, and I learned of the roles they can play in maximizing access control of my network. I now have ways of checking anything on my network for weaknesses. From now on, the only problem I should have with vulnerable devices is securing them properly.

References

National Vulnerability Database. 26 January 2019. *CVE-2019-6799 Detail.* Retrieved from: https://nvd.nist.gov/vuln/detail/CVE-2019-6799

Kali Docs Official Documentation. 2019. *Kali sources.list Repositories.* Retrieved from: https://docs.kali.org/general-use/kali-linux-sources-list-repositories