Project 0. Setting Up Virtual Machines

Set up the following:

- VirtualBox: https://www.virtualbox.org//wiki/Downloads
- pfSense: https://www.pfsense.org/download/
- Metasploitable: https://sourceforge.net/projects/metasploitable/
- Kali Linux:

https://www.offensive-security.com/kali-linux-vmvmware-virtualbox-image-download

PFSense Set Up:

```
Starting syslog...done.
Starting SCON... done.
pfSense 2.7.8-RELEASE amd64 Hed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 2c6561c3267b83b9859d

*** Helcome to pfSense 2.7.8-RELEASE (amd64) on pfSense ***

HAN (wan) -> em0 -> v4/DHCP4: 136.227.103.69/21
LRN (lan) -> em1 -> v4: 192.168.1.1/24

8) Logout (SSH only) 9) pfTop
1) Assign Interfaces 10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system 14) Enable Secure Shell (sshd)
6) Halt system 15) Restore recent configuration
7) Ping host 16) Restart PHP-FPM
8) Shell

Enter an option: $
```

Metasploitabe Set Up:

```
* Starting deferred execution scheduler atd

* Starting periodic command scheduler crond

* Starting periodic command scheduler crond

* Starting Ioncat servlet engine tomcat5.5

* Starting web server apache2

* Running local boot scripts (/etc/rc.local)

nohup: appending output to `nohup.out'

nohup: appending output to `nohup.out'

[ OK ]

* OK ]

* Warning: Never expose this UM to an untrusted network!

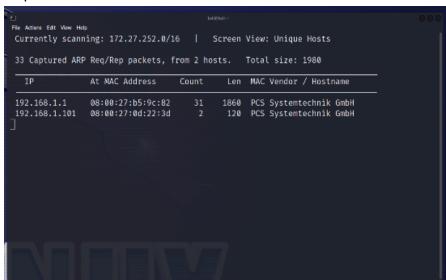
Contact: msfdev[atlmetasploit.com

Login with msfadmin/msfadmin to get started

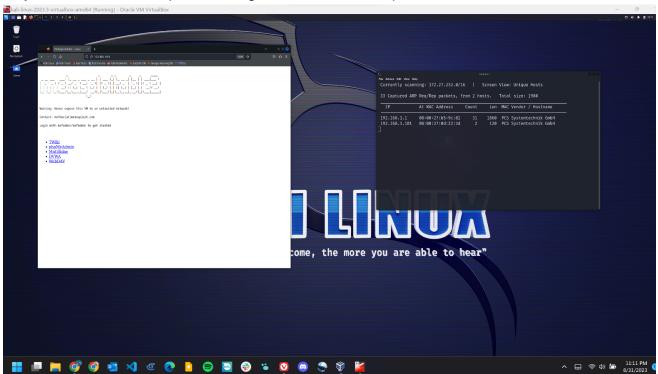
metasploitable login:
```

Kali Linux Set Up & Connected to Metasloitable through pfSense:

Step 1: Run the netdiscover command.



Step 2: Connect to Metaspoitabe using the known user and password hack.



Step 3: Communicate through FTP and run commands to confirm a connection.

