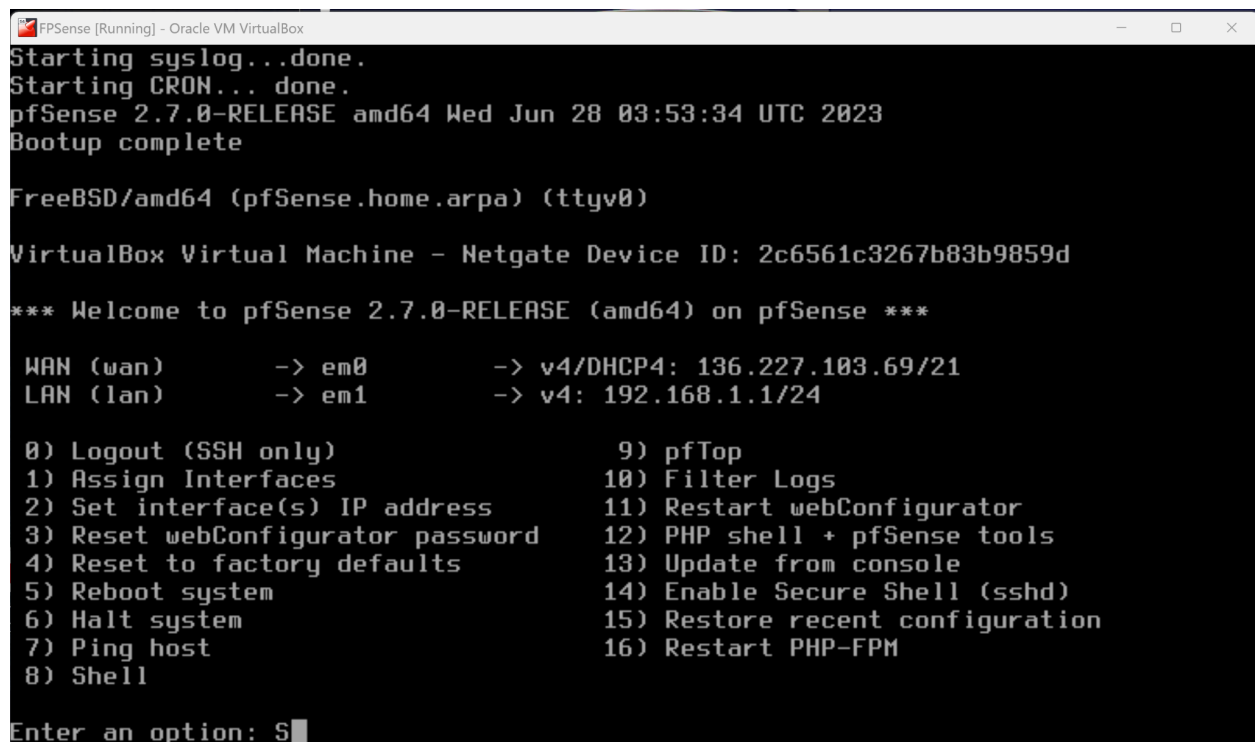


Project 0. Setting Up Virtual Machines

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:



```
PFsense [Running] - Oracle VM VirtualBox
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

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

VirtualBox Virtual Machine - Netgate Device ID: 2c6561c3267b83b9859d

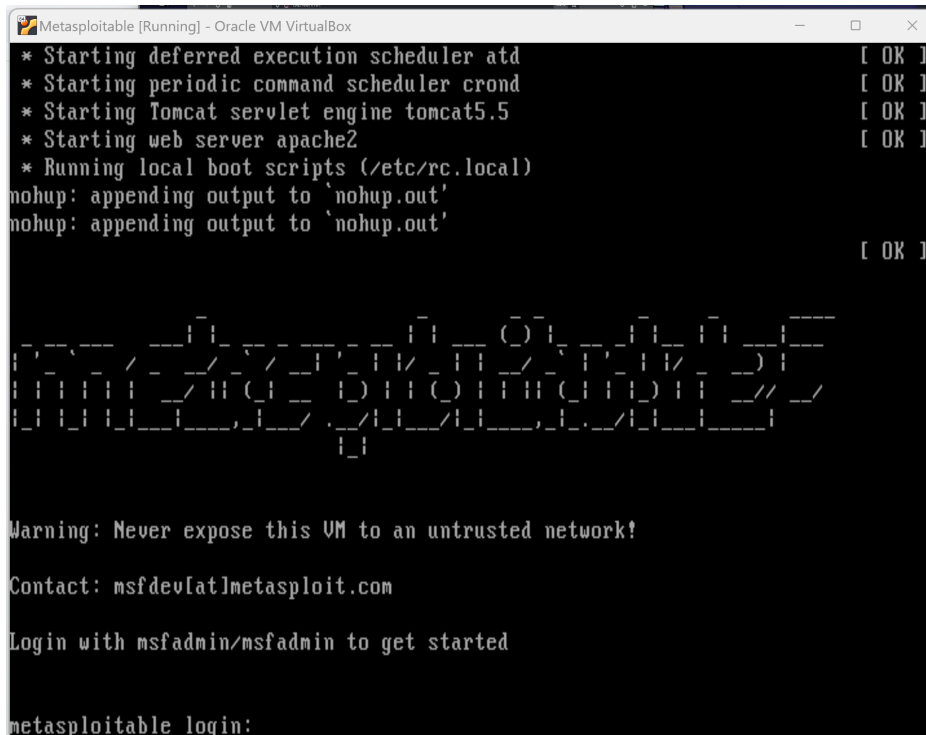
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

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

0) 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: S
```

Metasploitable Set Up:



The screenshot shows the startup sequence of the Metasploitable virtual machine. It lists the starting of several services: atd, cron, tomcat5.5, and apache2, all of which start successfully. It also shows the execution of local boot scripts and the appending of output to 'nohup.out'. A large ASCII art logo for Metasploit is displayed. Below the logo, a warning message states: 'Warning: Never expose this VM to an untrusted network!'. It also provides contact information 'msfdev[at]metasploit.com' and login instructions 'Login with msfadmin/msfadmin to get started'. The prompt 'metasploitable login:' is visible at the bottom.

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler cron [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

Warning: Never expose this VM to an untrusted network!

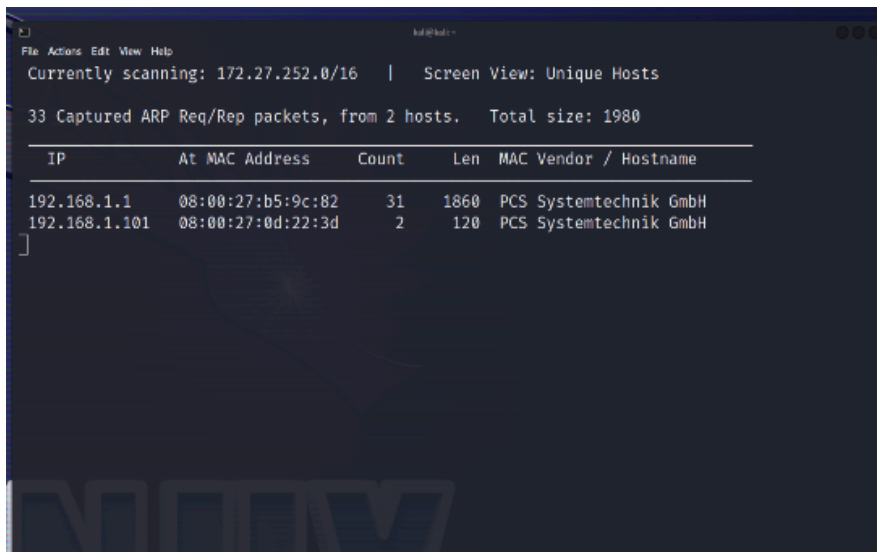
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:
```

Kali Linux Set Up & Connected to Metasploitable through pfSense:

Step 1: Run the netdiscover command.



The screenshot shows the output of the netdiscover command in a Kali Linux terminal. It indicates that 33 ARP request/reply packets were captured from 2 hosts, with a total size of 1980 bytes. A table lists the discovered hosts with their IP addresses, MAC addresses, counts, lengths, and vendor/hostnames.

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	08:00:27:b5:9c:82	31	1860	PCS Systemtechnik GmbH
192.168.1.101	08:00:27:0d:22:3d	2	120	PCS Systemtechnik GmbH

The screenshot displays a Kali Linux desktop environment. The background is the Kali Linux logo with the text "come, the more you are able to hear".

In the foreground, there are two windows:

- Terminal Window (Left):** Displays a network diagram showing a central host connected to several other hosts. Below the diagram, it says:


```
Warning: Never expose this VM to an untrusted network!
Contact: info[at]metasploit.com
Login with metasploit/metasploit to get started
```

 A list of links is provided:
 - [Tools](#)
 - [p0wn3dAdmin](#)
 - [Metasploit](#)
 - [DVWA](#)
 - [P0wn3dX](#)
- Wireshark Window (Right):** Shows a packet capture of ARP requests. The top status bar indicates:
 - File: /home/.local/share/wireshark/packets/172.17.252.0/16
 - Currently scanning: 172.17.252.0/16
 - Screen View: Unique Hosts
 The main display shows 33 captured ARP Req/Rep packets from 2 hosts, with a total size of 1500 bytes. A table lists the captured packets:

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	08:00:27:1b519c182	31	1860	PCS Systemtechnik GmbH
192.168.1.101	08:00:27:8d:22:13d	2	120	PCS Systemtechnik GmbH

The taskbar at the bottom shows various application icons, including the Windows logo, file explorer, and several web browsers.

The image shows a Kali Linux virtual machine environment. The desktop has a blue and black abstract background. Several terminal windows are open, displaying network-related commands and results. The top-left terminal shows a netcat listener on 192.168.1.101 port 6200, which has received a connection from 192.168.1.101. The bottom-left terminal shows a directory listing of the root filesystem. The bottom-right terminal shows a netcat listener on 192.168.1.101 port 6200, which has received a connection from 192.168.1.101. The top-right terminal shows a Wireshark capture of the netcat traffic, displaying a SYN packet from 192.168.1.101 to 192.168.1.101 on port 6200.