Networking Tools with KaliLinux

Objective:

Expose students to different networking tools available through the Kali distribution of Linux. Give them the resources to further develop these skills on their own.

Full Walkthrough:

https://infosecwriteups.com/kioptrix-level-1-vulnhub-walkthrough-49bcc7306e72

Tools:

- Nmap
- Arp-Scan
- Netdiscover
- Dirbuster
- Nikto
- SMBClient
- Metasploit
- Git
- VulnHub
- SSH Connections
- Unshadow

Links to Resources:

- https://www.vulnhub.com/
- Specific Kioptrix Box OVA File: https://www.dropbox.com/s/1k9vkhgc1gci4vn/Kioptrix%20Level%201.ovf?dl=0
- https://github.com/Dewalt-arch/pimpmykali
- https://www.virtualbox.org/
- https://www.kali.org/

Links to Further Information:

- https://www.techtarget.com/searchsecurity/definition/Secure-Shell
-

Chapter 1: Setting Up Network of VM's

Install both the Kali VM and the Kioptrix Box OVA files. Import them into VirtualBox.
In VirtualBox, go to Tools > Preferences > Network > Create a new Network.
On each box, go to Settings > Network > Attached to NAT Network. Select your network you just made. Then, open both VM's.

For Kali Box, login is kali : kali.
For Kioptrix, login is john : TwoCows2

Test a network connection by pinging 8.8.8.8 with both machines.

Test with 127.0.0.1 loopback address.
Identify your IP address from the Kioptrix box based on what is sending the packets out.

Chapter 2: Prepping the Kali Box

Pimp My Kali is a program written by user Dewalt that contains lots of patches and fixes for Kali to make it an overall better system for penetration testing. It also boosts performance.

On the Kali Box, enter the command:

```
 $ git clone https://github.com/Dewalt-arch/pimpmykali
```

CD into pimpmykali and then enter the command:

```
 $ ./pimpmykali
```

Open up CherryTree and create a node titled Assessment 1: Kipto. Then create several sub-nodes: Enumeration, Evaluation, and Exploitation. These will be for note-taking throughout this process.

Chapter 3: Discovering Devices in the Network

Using Nmap, Arp-Scan, and NetDiscover, we can discover different devices on out network. To start, begin by using *ifconfig* to figure out your own IP address and then Nmap to find out the IP addresses of our other devices.

```
 $ ifconfig
```

```
$ nmap -T4 -A [ip]/24
```

Copy IP addresses of machines into Enumeration notes.

T = How many threads / speed. More isn’t always better.
A = Specifies the type of information you want to learn. Gives services and OS’s.

Copy Nmap output into a new subnode under enumeration titled NMap.

Next, use the commands: to do the same.

```
$ arp-scan -l
$ netdiscover -r [ip]/24
```

Chapter 4: Scanning for Vulnerabilities on the VulnBox.
First, try out HTTP server via Firefox.
Report under FINDING for Evaluation

Two primary tools for scanning for vulnerabilities: Nikto and DirBuster.
Nikto = Rocket Launcher version of NMap
DirBuster = Brute force testing for hidden directories in a site

```
$ nikto -h http://TARGET_IP
```

Paste information into subnode on Enumeration for Nikto

```
$ dirbuster
```

Add the wordlist.txt from usrs/share/wordlists/23 medium
Add html

From there, go to usage statistics page. Report that in Evaluation.

Use SMB Client to access information about Samba

```
$ smbclient -L \\\\TARGET_IP\\
```

Paste Information about smbclient in Enumeration

Chapter 5: Exploiting Vulnerabilities
Metasploit Exploitation Framework - Series of tools you can use to exploit vulnerabilities. It's built-in to Kali.

```
$ msfconsole
```

```
$ search smb
```

We're looking for information, so we want to look at the *auxiliary* labeled tags.

Search `smb_version`

```
0
Options
set RHOSTS TARGET_IP
```

=======================================

Reverse Shell

- Listening for inbound connection
- Target is connecting to MY machine
- I'm listening / setting trap for them

Bind Shell

- I am connecting to target
- I open a window on their end and climb through

=======================================

Payload → What comes through
Staged = Sends payload in stages. Less stable.
Non-Staged = Sends exploit shell all at once. Larger in size. Won't always work.

=======================================

Research:

Samba 2.2.1a exploits
Trans2open

Search trans2open with metasploit
Show payloads
Set payload to shell_reverse_tcp

33

Whoami
hostname

Chapter 6: Manual Exploitation
Manual exploitation is using tools from online rather than the built-in metasploit exploitations that are available through KaliLinux.

Search Mod_ssl 2.2.84

OpenFuck
Mkdir kioptrix
Install
Find version in nmap apache version w/ redhatlinux 0x6b 443

Cat /etc/passwd → Users
Cat /etc/shadow → Password Hashes

Unshadow passwd.txt shadow.txt