Week 6 - Supplementary Materials

Markdown | PDF | MS Word DOCX | Libre ODT | HTML

Intermediate Networking Commands

This week we continue discussing networking concepts, focusing on techniques for finding and exploiting weaknesses in a remote machine, and the associated commands in the CLI.

NOTE: You will need to use Kali Linux for these and future practical exercises. If you have not set it up yet, please see our instructions in the class README.

`nmap`

Servers running Unix-like operating systems such as GNU/Linux have many services running to handle external requests and maintain the system. For security hardening, these services should be disabled or removed to reduce the attack surface of the machine.

`nmap` has been used in the Matrix Reloaded and some other films.

The default `nmap` scan shows the ports, their state of being open or closed, and the associated protocols. To check which hosts on your network are up, you need to check the IP range you are currently on. In home networks, this often starts with an IP range of 192.168.x.x and therefore would be:

```
nmap -sn 192.168.0.0/24
```

Use the -O flag to identify which operating system a host is running.

```
nmap 10.0.0.50 -O
```

`netstat`

The `netstat` command outputs network statistics. It gives an overview of network activity and displays which ports are open or might have established connections. List all TCP ports by running:

```
netstat -at
```

List all UDP ports by running:

```
netstat -au
```

List the process ID or program name for a specific connection by adding the `-p` option:

```
netstat -pntul
```

`ping`

Use `ping` to see if a host is available on the network. `ping` sends an `ICMP ECHO_REQUEST` packet to the target host and waits to see if it replies. Notably, some hosts block ICMP echo requests using other software controls such as a firewall.

By default, `ping` runs in an infinite loop. To send a defined number of packets, use the `-c` option.

```
ping -c 3 lawfareblog.com
```

Using the `-o` option tries to send one packet.

```
ping -o lawfareblog.com
```

`traceroute`

This command shows you the actual path through the network that packets take to their destination.

```
traceroute lawfareblog.com
```

This will show you a sequence of intermediaries as well as the destination. To trace the path through a specific intermediary, add it to the command. For example:

```
traceroute -g 192.168.1.123 google.com
```

`tcpdump`

`tcpdump` is a "packet sniffing" tool.

To check which network interfaces are available to capture, use the `-D` option:

```
tcpdump -D
```

To capture only TCP packets:

```
tcpdump --interface any -c 5 tcp
```

You can use the `-A` and `-x` options to analyze the content of the network packet. The `-A` option stands for ASCII format:

```
tcpdump --interface any -c 1 -A
```

The `-x` option will use hexadecimal format:

```
tcpdump --interface any -c 1 -x
```