Introduction to Linux

Sudo Overview

root disabled for security reasons, use `sudo su`

Navigating the File System

use locate to find files, use `updatedb` to update the database if the file can't be found initially

Users and Privilege

Privileges

file type | owner permissions | group permissions | all other users

d|rw-|r--|r--

/tmp usually has full permissions for all users making it a good place for pentesters

chmod numbers

Number	Permissions	Totals
0	---	0+0+0
1	--x	0+0+1
2	-w-	0+2+0
3	-wx	0+2+1
4	r--	4+0+0
5	r-x	4+0+1
6	r-w	4+2+0
7	rwx	4+2+1

sudoers

/etc/sudoers for user privilege elevation

use `grep 'sudo' /etc/group` to see users in the sudoers group

Common Network Commands

Connections

`ip a` for wired and wireless, `ifconfig` for wired connections, `iwconfig` for wireless connections

ARP

`ip n` or `arp -a` for address resolution protocol information

Routing

`ip r` or `route` for routing table. Can add networks to the table allowing us to access them

`ping` for ICMP traffic to a given host, disabled in some machines

`netstat` to identify open ports and services

Starting and Stopping Services

Start and stop

```
sudo service <SERVICE-NAME> start
sudo service <SERVICE-NAME> stop
```

Start on boot

```
sudo systemctl enable <SERVICE-NAME>
```

Installing and Updating Tools

Before updating kali make a backup as it may break certain tools

Plmp my kali tool to fix issues

Scripting with Bash

Writing a network sweeper - ipsweeper.sh

```
#!/bin/bash

if [ "$1" == "" ]
```

```
then
echo "You forgot an IP!"
echo "./ipsweep.sh 192.168.1"

else
for ip in `seq 1 254`; do
ping $1.$ip -c 1 | grep "64 bytes" | cut -d " " -f 4 | tr -d ":" &
done
fi
```

Writing a oneliner

```
./ipsweeper 192.168.1 > ips.txt
for ip in $(cat ips.txt); do nmap $ip; done
```