Module 1.2: Terminal commands, network scanning

9.1.26: terminal commands

Reference:

Download Take Control of the Mac Command Line with Terminal (3.4).pdf (application/pdf, 2.2 MB)

We will be using macbook air computers, with OS version 12.7.6 on the elab network wifi. IPNM was version 2.7.3 or 2.8c1

terms and commands to know:

- whoami
- last
- history
- ping
- traceroute
- ssh
- say (mac only)
- shutdown -r now
- sudo
- IPnet monitor
- TCPdump
- DOS and ddos
- flags
- ctrl-c and ctrl-z
- wifi pulldown on mac to determine network info and signal strength

- whoami: who are you logged in as. first step in detecting hacking incidents on your computer, the command who does the same thing
- last: the last users logged in
- history: the last commands that were issued on your computer, good for tracking invasion, but also for recording notes on your work
- ping: just like it sounds, sends a small packet (ICMP, more on this later) and records the time in milliseconds to return to you. useful for seeing if a machine at an IP address is active, hidden or far away
- traceroute: traces the path to the website or computer. boring if you are all in the same room, but exciting if you want to know why COD is so slow where you are. it records each step of the path in milliseconds
- ssh: secure shell, how you get access to the terminal on another machine. in our lab, we all know the login for others' computers, so we can login and look around. this can be used multiple steps, e.g. you can login to John's computer then ssh over to Mary's computer, and Mary will think John is attacking her.
- say: loads of fun, makes the remote computer say what you type. use the -v flag (more on flags next) to change voices
- shutdown: tells the computer to shutdown. useful in the format shutdown -r now, meaning shut the computer down, restart, and do it now. one can also add time like shutdown -r +600 which is ten hours from now, to cover your tracks
- sudo: treat me as "root" or god on the computer for this command. used to do commands that are blocked. really not a good idea to login as root on any computer unless you know what you are doing. it is possible with root access to erase your entire computer, or to create hidden files, cover your tracks, install malware and so on. rootkits are software packages to gain root access on a remote computer, doing these things
- IPnetmonitor: an excellent GUI (graphical user interface) for many of these commands
- TCPdump: a "dump" of all traffic on the network, useful for diagnosing issues, or to see invasions
- DOS: denial of service, sending many pings at once, called a "ping flood attack" overwhelming the remote computer. a dDOS is a distributed attack using many computers at once
- flags: after a command, there is a space, then a hyphen (dash) where one can add a letter to make the command to special things, for example ping -f means run ping and "flood" the victims computer. shutdown -r means reboot after shutting down.
- ctrl-c (stop) and ctrl-z (halt): control-c is a common stop command, or cancel, to halt (less gentle) use ctrl-z
- wifi pulldown menu: shows connection strength (RSSI) and connection speed (RX and TX). useful for diagnosing wireless issues and network status (router, IP address, subnet mask)

Next:
netstat
nmap
lsof
port mapping

network scanning
protocols (ICMP, TCP and IP)
rootkits
file structure (ls, cd, pwd)
brew
wild cards
man pages
top
ls -la
hidden files
cd .., mkdir
chmod
finding files
networks
html
open and closed web pages ssl
ifconfig
routers and gateways
wifi sniffing
wired sniffing
MiM attacks
nslookup and dns
pi setup attack-defend
Kali linux
pentesting
wireshark

Network scanning: nmap arp-scan and IPNM (GUI)
May need to install homebrew to run some of these

/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
nmap -v -sn 10.14.253.0/24
arp-scan 10.14.253.0/24 (use sudo)

Advanced tools:
netstat, tcpdump, iftop, netcat, dig, nslookup, hping3, lsof, wireshark (GUI)

Fun challenges:
1. scan our local network, find one of our laptops, remote login
2. make the laptop say something
3. show that you are logged into the computer from their terminal
4. remotely reboot their computer (with permission)

8.19.25:

- resources, icloud, apps

- nmap and arp-scan from terminal (using brew)
- wireshark demo
- FTP password demo using tcpdump -i en0 port 21 (setup server on victim machine)
- wireshark demo using web traffic
- nslookup demo
- subnets and IP addresses
- 10.14.253.0/24 network
- NAT for internal servers (e.g. home)
- DNS and dig

8.21.25:
port scan
service ports:
21 FTP (file transfer protocol)
22 ssh (secure shell)
80 http (web)
138 smb (windows file sharing)
443 https (secure web)
82 (web alternate)
8080 (web proxy)

ARIN.net and nslookup
stealth mode on macs
ping proof
email headers-find sender
browser tracking-disable

8.26.25
pwd: where am I?
ls: list the files where I am
cd: change my directory

IP Net monitor:
address scan: 10.14.253.0/24 in the elab
bonjour scan: printers
connections: watch what your computer is connecting to
DHCP lease: when you got an address, when it expires
DHCP test: test the local server for speed, and if there is a rogue server present (2 will show up)
DNS lookup: names to numbers, you can specify which server is answering, internal or external
Interface info: useful for detecting errors or collisions
Link rate: test link speed to a server
Ping: like it sounds, link to a device
Port scan: scanning for ports or "doors" on a host
Subnet calc: really useful in setting up addresses on a network
TCPdump: dumps entire conversation into your computer
TCP info: useful for setting up your web servers
Traceroute: traces the path to a server

cb52f155-5158-5158-1f64-f762f81e63a3

Migrated from Apple Server Wiki. Original page ID: v94988R

Revision #3
Created 2026-09-29 15:59:53 UTC by Admin
Updated 2026-09-29 16:49:14 UTC by Admin