Packets and Tools

Overview

- When a packet travels through the network, it has also a port associated with it.
- A port is a number that indentifies the process the packet is associated with.
- The port number is an identifier for which port the packet is using.
- Port numbers can be used for any process. but only one process can on a given port at a time.
- Common services/processes have common ports:
- HTTP (websites): 80 or 8080
- HTTPS (secure websites): 443
- SMTP (email): 25
- POP3: 110
- SQL (database): 156
- IMAP: 220
- LDAP: 389
- SSH: 22
- There are lots of tools for network enumeration and monitoring.
- Network enumeration and monitoring is the process of determining what devices are on a network (enumeration) and what the devices are doing (monitoring).
- nmap (network map): nmap is an enumeration tool that scans single or multiple ip addresses to see what ports are being used.
- Usage (Basic)
  - nmap ip address(es)
  - nmap ip address(es)> -p port(s)
- .nc/ncat/netcat: Versatile tool that can be used as a port scanner, port listener and more.
- Possible uses
  - nc -l -p port
- netstat/ss Short for network statistics. Can show tcp/ip processes running on a computer (what is YOUR device doing)

- Usage
  - netstat -a
  - ss -a
- After you've enumerated devices, how can you see the actual packets?
- You can dumb the traffic with tcpdumb, but this can be tedious.
- Wireshark: A packet capture & analysis program with GUI.
- You can save packet captures (pcap files) and analyze them later.
- You can also filter lots of things (IP, PORT, protocol, etc)