tcpdump

Resources

- tcpdump filters
- tcpdump Cheat Sheet by comparitech
- A tcpdump Tutorial with Examples — 50 Ways to Isolate Traffic

Purpose

Capture, display, and filter network traffic

Useful Commands

Read Traffic Capture

- tcpdump -r pathtofile -n
- tcpdump -r pathtofile -n -A

-r - reads from local file

-n - doesn't resolve hosts/ports

-A - prints to ASCII

Traffic Capture

- tcpdump -i interface
- tcpdump -i interface -w file

-i - choose interface, i.e., any, eth0, etc. -D or --list-interfaces will print a list of available options

-w - write the raw packets to file rather than parsing and printing them out, ex: tcpdumpoutput.pcap

Filtering

Examples

- tcpdump -r pathtofile host MAINFILESERVER — Print all packets arriving at or departing from host MAINFILESERVER
- tcpdump -r pathtofile host MAINFILESERVER and \(MAINDC or MAINAVSERVER \) — Print traffic between MAINFILESERVER and either MAINDC or MAINAVSERVER
- tcpdump -r pathtofile ip host MAINFILESERVER and not MAINDC — Print all IP packets between MAINFILESERVER and any host except MAINDC

Berkley Packet Filters (BPF)

Qualifiers

tcpdump -r pathtofile host 10.10.1.13
tcpdump -r pathtofile host MAINFILESERVER
tcpdump -r pathtofile net 10.10.1.0/16
tcpdump -r pathtofile port 80
tcpdump -r pathtofile portrange 12-52

- Type: host, net, port, portrange
- Direction: src, dst
  - tcpdump -r pathtofile src 10.10.1.13
  - tcpdump -r pathtofile dst 10.10.1.13
- Protocol: icmp, ip, tcp, udp, ether, fddi, ip6, ppp, radio, rarp, slip, wlan
  - Most common: icmp, ip, tcp, udp
  - tcpdump -r pathtofile -i protocol
  - tcpdump -r pathtofile -i any

Subtopic 2

These can be combined, as needed

- tcpdump -r pathtofile -n src 10.10.1.13 and dst port 80 — AND: and, &&
- tcpdump -r pathtofile dst 10.10.1.13 or src host MAINFILESERVER — OR: or, ||
- tcpdump -r pathtofile dst 10.10.1.13 and not udp — EXCEPT: not, !
- tcpdump -r pathtofile <50 — LESS: <
- tcpdump -r pathtofile >=50 — GREATER: >

Logical Operators (with tcpdump syntax)

Mahyar TajDini

- Mahyar@TajDini.net
- Github.com/mahyarx
- Linkedin.com/in/mahyartajdini
- TajDini.net