Tcpdump

Installation Commands

- $ sudo yum install tcpdump — CENT OS and REDHAT
- $ dnf install tcpdump — Fedora
- #apt-get install tcpdump — Ubuntu, Debian and Linux Mint

Packet Capturing Options

- Capture from all interfaces — tcpdump -i any — -i any
- Capture from specific interface (Ex Eth0) — tcpdump -i eth0 — -i eth0
- Capture first 10 packets and exit — tcpdump -i eth0 -c 10 — -c
- Show available interfaces — tcpdump -D — -D
- Print in ASCII — tcpdump -i eth0 -A — -A
- To save capture to a file — tcpdump -i eth0 -w tcpdump.txt — -w
- Read and analyze saved capture file — tcpdump -r tcpdump.txt — -r
- Do not resolve host names — tcpdump -n -I eth0 — -n
- Stop Domain name translation and lookups (Host names or port names) — tcpdump -n -i eth0 — -nn
- Capture TCP packets only — tcpdump -i eth0 -c 10 -w tcpdump.pcap tcp — tcp
- Capture traffic from a defined port only — tcpdump -i eth0 port 80 — port
- Capture packets from specific host — cpdump host 192.168.1.100 — host
- Capture files from network subnet — tcpdump net 10.1.1.0/16 — net
- Capture from a specific source address — tcpdump src 10.1.1.100 — src
- Capture from a specific destination address — tcpdump dst 10.1.1.100 — dst
- Filter traffic based on a port number for a service — tcpdump http
- Filter traffic based on a service — tcpdump port 80
- Filter based on port range — tcpdump portrange 21-125 — portrange
- http Display entire packet — tcpdump -S — -S
- Show only IPV6 packets — tcpdunp -IPV6 — ipv6
- display human readable form in standard output — tcpdump -d tcpdump.pcap — -d
- Use the given file as input for filter — tcpdump -F tcpdump.pcap — -F
- set interface as monitor mode — tcpdump -I eth0 — -I
- Display data link types for the interface — tcpdump -L — -L
- tcpdump.pcap not printing domian names — tcpdump -N — -N
- Do not verify checksum — tcpdump -K tcpdump.pcap — -K
- Not capturing in promiscuous mode — tcpdump -p -i eth0 — -p

Command Line Options

Display / Output Options

- Quite and less verbose mode display less details — -q
- Do not print time stamp details in dump — -t
- Little verbose output — -v
- More verbose output — -vv
- Most verbose output — -vvv
- Print data and headers in HEX format — -x
- Print data with link headers in HEX format — -xx
- Print output in HEX and ASCII format excluding link headers — -X
- Print output in HEX and ASCII format including link headers — -XX
- Print Link (Ethernet) headers — -e
- Print sequence numbers in exact format — -S

Main Topic

TCP Flags

- tcp-urg
- tcp-rst
- tcp-ack
- tcp-syn
- tcp-psh
- tcp-fin

ICMP Types

- icmp-echoreply
- icmp-routeradvert
- icmp-tstampreply
- icmp-unreach
- icmp-routersolicit
- icmp-ireq
- icmp-sourcequench
- icmp-timxceed
- icmp-ireqreply
- icmp-redirect
- icmp-paramprob
- icmp-maskreq
- icmp-echo
- icmp-tstamp
- icmp-maskreply

Capture Filter Primitives

- [src|dst] host <host> — Matches a host as the IP source, destination, or either
- ether [src|dst] host <ehost> — Matches a host as the Ethernet source, destination, or either
- gateway host <host> — Matches packets which used host as a gateway
- [src|dst] net <network>/<len> — Matches packets to or from an endpoint residing in network
- [tcp|udp] [src|dst] port <port> — Matches TCP or UDP packets sent to/from port
- [tcp|udp] [src|dst] portrange <p1>-<p2> — Matches TCP or UDP packets to/from a port in the given range
- (ether | ip | ip6) proto <protocol> — Matches an Ethernet, IPv4, or IPv6 protocol
- (ether | ip) — broadcast Matches Ethernet or IPv4 broadcasts
- (ether|ip|ip6) — multicast Matches Ethernet, IPv4, or IPv6 multicasts
- type (mgt|ctl|data) [subtype <subtype>] — Matches 802.11 frames based on type and optional subtype
- vlan [<vlan>] — Matches 802.1Q frames, optionally with a VLAN ID of vlan
- mpls [<label>] — Matches MPLS packets, optionally with a label of label
- Matches packets by an arbitrary expression

Protocols

- Ether
- fddi
- icmp
- ip
- ip6
- ppp
- radio
- rarp
- slip
- tcp
- udp
- wlan

Logical Operators

- Combine filtering options — tcpdump -n src 192.168.1.1 and dst port 21 — AND and, &&
- Either of the condition can match — tcpdump dst 10.1.1.1 && !icmp — OR or, ||
- Negation of the condition — tcpdump dst 10.1.1.1 and not icmp — EXCEPT not, !
- Shows packets size less than 32 — tcpdump <32 — LESS <
- Shows packets size greater than 32 — tcpdump >32 — GREATER >

@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles