Capturing the Data

Example Filters

Exclusive filter examples

1. `not tcp port 3389 and not tcp port 22`
2. `not arp`
3. `not broadcast and not multicast`
4. `not net 192.168.10.0/24`
5. `not tcp portrange 1-1023`

Exclusive filters explanations

1. Do not capture management traffic: remote desktop and ssh
2. Do not capture ARP traffic
3. Do not capture broadcast or multicast traffic
4. Do not capture any traffic to/from 192.168.10.0/24
5. Do not capture any traffic to/from TCP ports 1 - 1023 inclusive

Inclusive filter examples

1. `host 10.10.10.10 and (tcp port 80 or tcp port 443)`
2. `icmp or host 104.73.56.234`
3. `udp port 53`
4. `tcp[tcpflags]&2 != 0`
5. `ip[8] < 5`

Inclusive filter explanations

1. `Capture traffic to/from host 10.10.10.10 on tcp port 80 or 443`
2. `Capture ICMP or traffic to/from host 104.73.56.234 (testing MTU)`
3. `Capture DNS traffic`
4. `Capture SYN and SYN/ACK packets`
5. `Capture packets with a TTL less than 5`

Filter Notes

- It is better to not use any capture filters and filter later when doing analysis
- If a filter must be used, an exclusive filter is preferred
- When using inclusive filters take into account associated protocols like ARP, DNS, ICMP, GRE, and NAT behavior
- Be careful using `src` or `dst` in filters as you may only capture unidirectional traffic
- Before running a capture to a file, do a sanity check on your filter by running it live with output to the screen to make sure you're seeing the traffic you expect

Advanced Filtering

- http://www.wains.be/pub/networking/tcpdump_advanced_filters.txt
- https://danielmiessler.com/study/tcpdump/