**Network Monitoring**

**WireShark**

Gold standard, free, cross-platform GUI protocol analyser for network traffic

**Tshark** Cmd line version

**TCP dump**

* Cmd line analyser available natively on MacOS and Kali
* WinDump is the windows version

Can be run on devices, on the router/firewall

Running them on devices will show limited traffic if using a switch

* Isolated collision domains will limit traffic you can see
* If malware is on the device, then it is not recommended to run the analyser on the same machine because the malware could provide false information about what is travelling on the network

**Best to run on router and/or firewall** (hub of the network)

* Any malware or rootkit on a device that’s hiding it from the device, will not be able to hide it from the router

Custom router firmware like DD-WRT or PFsense can usually have network traffic monitoring capabilities itself so an analyser may not be necessary

If it is, **an SSH directly into the router using TCP dump can be used**

* TCP dump cheat sheet necessary

What interface do we want to monitor?

* Ppp0 (modem interface)
* Eth0
* Vlan1
* Eth1
* Vlan2
* Eth2
* Lo
* Br0

Tcpdump -i eth0

* Returns a capture of the traffic on eth0

Tcpdump -I any

* Monitors whole network

Tcpdump **-n** -i any

* Shows IP addresses and ports

Tcpdump -i any dst port 80

* Dst = destination
* Shows traffic on port 80 (HTTP traffic)

Tcpdump -i any port 53 (DNS queries)

* Will show where your queries are being sent
* Confirms usage of VPN server
* Good for monitoring DNS leaks
* Monitor that DNS queries are actually being sent to where you want them to be

Tcpdump -i ppp0 -vv ip6

* Output to verbose
* Look at IPv6 traffic which can sometimes be leaked when using a VPN

Tcpdump -i any port 53 or port 80 or port 443

* All web traffic on network

Tcpdump -i any host 192.168.1.81 and not src net 192.168.1.0/24

* Looking at a specific device (1.81)
* Doesn’t show traffic coming from the internal network 1.0/24
* So will show if anything is connecting from external to the internal device or anything that is not part of the internal network
* Suspicious about having malware on a device

Tcpdump -i any dst net 192.168.1.0/24 and not src net 192.168.1.0/24

* Will show if there’s anything external connecting to the whole network

Tcpdump -i any -s 65535 -w capturefile.pcap

* Outputs into a file for later analysis in something like WireShark
* File can be big, so make sure router has enough storage to run this so that you don’t DOS your own router by running the command
* Again, if you have the storage capabilities
  + Can be stored remotely though
* -s will capture full size packets
* -w is to write to a file

**WireShark**

GUI that compiles info and has tools to analyse data

Wireshark.org

Apt-get install WireShark

Port mirroring of IP tables

Iptables -t mangle -A PREROUTING -d/s 192.168.ip.to.monitor -j TEE - -gateway 192.168.1.wireshark (router)

Best method is to SSH into router, capture traffic via TCPdump, save the output file and then analyse in WireShark

* Ssh root@198.168.1.1 - - tcpdump -w - -s 65535 ‘not port 22’ capture.pcap
* This will store the captures on the kali machine
* You can leave this for a few hours where you couldn’t do this on a router most likely because of storage
* -w = write
* -s full size packet capture
* Not port 22 because you don’t want to capture the traffic that is relaying back the tcp dump

Import the capture file into WireShark and perform analysis

Capturing traffic live via router/firewall in wireshark

Pipe tcpdump to wireshark over ssh

* Ssh root@192.168.1.1 tcpdump -U -s 65535 -w – ‘not port 22’ │ wireshark -k -i -
* -U = no buffering
* -s = full size packets
* -w = write to file
* -k -i = allows piping of tcpdump to wireshark