**Finding Malware**

**WireShark**

Select interface and capture

Top panel is thehigh level view

Shows frame number, time, source ip and dst, protocol and commands

The detailed view

Shows details of a selected packet

Frame – layer 2, data link layer

Data units are known as frames

* Ethernet frames, atm, wifi, arp, macsec

Eth2

* MAC source and dst as part of layer 2

IP (internet protocol)

* Layer 3, network layer
* Data units are called packets
* IPSec, ICMP, IGMP, NAT, DHCP, NAT

TCP (Transmission control)

* Layer 4, transport
* Source and dst
* data units are TCP segments and UDP datagrams
* TCP, UDP, SSL, TLS, SSH2
* Port info, source, dst

Application protocol (HTTP, SNMP, Telnet, FTP)

* Unencrypted sent by HTTP, can see conversation

Command for external connections

* Host 192.168.1.device and not src net 192.168.1.0/24

Capture filter

* Filters everything that you want to capture

Looking for suspicious traffic

* Start removing traffic that you know is valid
* Cmd = not(tcp.port==80) and not(tcp.port==443) and not(udp.port=53)
* Removes HTTP, all web traffic (SSL) and DNS
* Can right click on VPN server and apply a filter to it – ‘and not selected’ so that it filters out any traffic heading to the VPN server destination
* ‘&& not arp’
* If its just on a protocol level, this syntax can be used
  + Not dns ││ http ││ ssl
  + Not smb ││nbns ││ dcerpc ││ nbss (windows noisy protocols)
* Tcp.srcport==80 (to analyse network traffic through port 80)
* Src == 192.168.1.0/24 and ip.dst 192.168.1.0/24
  + Will look at traffic sourced from local and dst to local
  + Will look at local traffic only
  + To look at Intercommunication locally
* Ip.dst == 192.168.1.device and !ip.src == 192.168.1.0/24
  + Looking at a device that you are concerned about and finding connections from a src that isn’t internal
  + ! = not
  + External connections to the device e.g., reverse connections

Httprecipes.com/1/2/cookies-set.php

* Cookie generator

Httprecipes.com/1/2/forms.php

* Allows a login with a username and password

Will send browser a cookie which you can name specifically for testing

* Will be sent over without https so wireshark will be able to capture usernames, passwords and cookies

Start capture

* http filter 🡪 apply
* should show the cookie value in ‘Set-Cookie’ under the http section/layer
* http.cookie 🡪 apply
  + will show just the traffic with cookies in
  + will also show uid and pwd
* http.request.method==POST
  + will also show where data has been submitted to servers such as uid and pwds
  + although if sent over https then the data would be encrypted and unreadable
* follow TCP stream
  + follows stream and puts together the conversation
  + will show if you’re sending anything in the clear that you shouldn’t be
* IPv6 for leakage from a VPN
* IPv4 shows your ip traffic from source to destination
  + Determine if traffic is legitimate
  + Apply filter on any potentially illegitimate traffic to analyse in more depth later
* Name resolution allows you to change ips into domain names
* Can select specific src and dst as filters
* Statistics 🡪 show address resolution – will show domains that have been resolved, shows all domains communicated with
* Statistics 🡪 end points – see end points of traffic (dst)

**Wireshark cheat sheet**

WinPcap install

* Windows 🡪 point wireshark at it, remote traffic analysis
* Similar to SSH however that was on mac, linux and routers

Network Security Toolkit (NST)

* Live CD
* Comes with network tools for some more conmclusive analysis

Network Miner

* Protocol analyser
* Better for forensics like malware on your network
* Linux and Mac
* NetWorx for windows