Wireshark

Display Filters

Network

`ip.src == #ip`	
`ip.dst == #ip`	
`ip.addr`	src or dst (careful with negation!)
`tcp.srcport == #port`	
`tcp.dstport == #port`	

`eth.addr[0:3]==00:06:5B`	Filter for manufacturer (example: Dell)

DNS

dns.qry.name == “”

Content

frame contains “” frame.length > 1500 fame.time >= “” ssl.handshake.extensions_server_name == “”

Protocols

`tcp`
`udp`
`icmp`
`http`
`tls`
`dns`
`arp`
`ftp`
`smtp`

TCP

`tcp.flags.syn == 1 && tcp.flags.ack == 0`	Syn scan
`tcp.flags.reset == 1`	Reset
`tcp.flags.fin == 1`	Fin
`tcp.flags.urg == 1`	Urgent
`tcp.analysis.retransmission`	

tcp.analysis.flags	
tcp.len > 1000	Large packets
tcp.window_size == 0 && tcp.flags.reset != 1	TCP Buffer full

http

http.request.method == “GET”	http get
http.host = “”	
http.request.uri matches “last$”	

Windows

smb || nbns || dcerpc || nbss || dns	Client/AD traffic

Capture Filters

Network

Command	Alternative	Description
host #ip		
net #ip/net	net #ip #netmask	
src net #ip/net		
dst net #ip/net		
post #port	tcp.port < #high	
ip	only IP traffic	
not broadcast and not multicast		
vlan		

http

port 80 and tcp[((tcp[12:1] & 0xf0) » 2):4] = 0x47455420	http get

Ipv6

dst host ff02::1	“All nodes” traffic

Bin

```
tcp portrange #low-#high''|''(tcp[0:2] > #low and tcp[0:2] < #high) or
(tcp[2:2] > #low and tcp[2:2] < #high)
```

Template