Wireshark

Display Filters

Network

ip.src == #ip
ip.dst == #ip
tcp.srcport == #port
tcp.dstport == #port
"| | | || | | || | | |"

DNS

dns.qry.name == “”

Content

frame contains “” frame.length > 1500 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
""	

http

<table>
<tr><td><code>http.request.method == “GET”</code></td><td></td><td>http get</td></tr>
<tr><td><code>"| | | || | | |"</code></td><td></td><td></td></tr>
</table>

Capture Filters

Network

<table>
<tr><th>Command</th><th>Alternative</th><th>Description</th></tr>
<tr><td><code>host #ip</code></td><td></td><td></td></tr>
<tr><td><code>net #ip/net</code></td><td><code>net #ip #netmask</code></td><td></td></tr>
<tr><td><code>src net #ip/net</code></td><td></td><td></td></tr>
<tr><td><code>dst net #ip/net</code></td><td></td><td></td></tr>
<tr><td><code>post #port</code></td><td><code>tcp.port < #high</code></td><td></td></tr>
<tr><td><code>ip</code></td><td>only IP traffic</td><td></td></tr>
<tr><td><code>not broadcast and not multicast</code></td><td></td><td></td></tr>
<tr><td><code>"| | | || | | |"</code></td><td></td><td></td></tr>
</table>

http

<table>
<tr><td><code>port 80 and tcp[((tcp[12:1] & 0xf0) » 2):4] = 0x47455420</code></td><td></td><td>http get</td></tr>
<tr><td><code>"| | | || | | || | | || | | |"</code></td><td></td><td></td></tr>
</table>

Ipv6

<table>
<tr><td><code>dst host ff02::1</code></td><td></td><td>“All nodes” traffic</td></tr>
<tr><td><code>"| | | || | | || | | || | | |"</code></td><td></td><td></td></tr>
</table>

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

<table>
<tr><td><code>"| | | || | | || | | || | | || | | || | | || | | || | | || | | || | | || | | |"</code></td><td></td><td></td></tr>
</table>