Suricata IDS Workshop

IDS vs IPS

IDP Conceptualmente

“Analizar la información de sistemas informáticos para identificar y potencialmente bloquear los intentos de intrusión”.

IDP Fuentes de Información

- Información almacenada en los sistemas
- Eventos ocurridos
- Tráfico de red

IDP según su ubicación

Al igual que los FW, los IDPs puede ubicarse en:

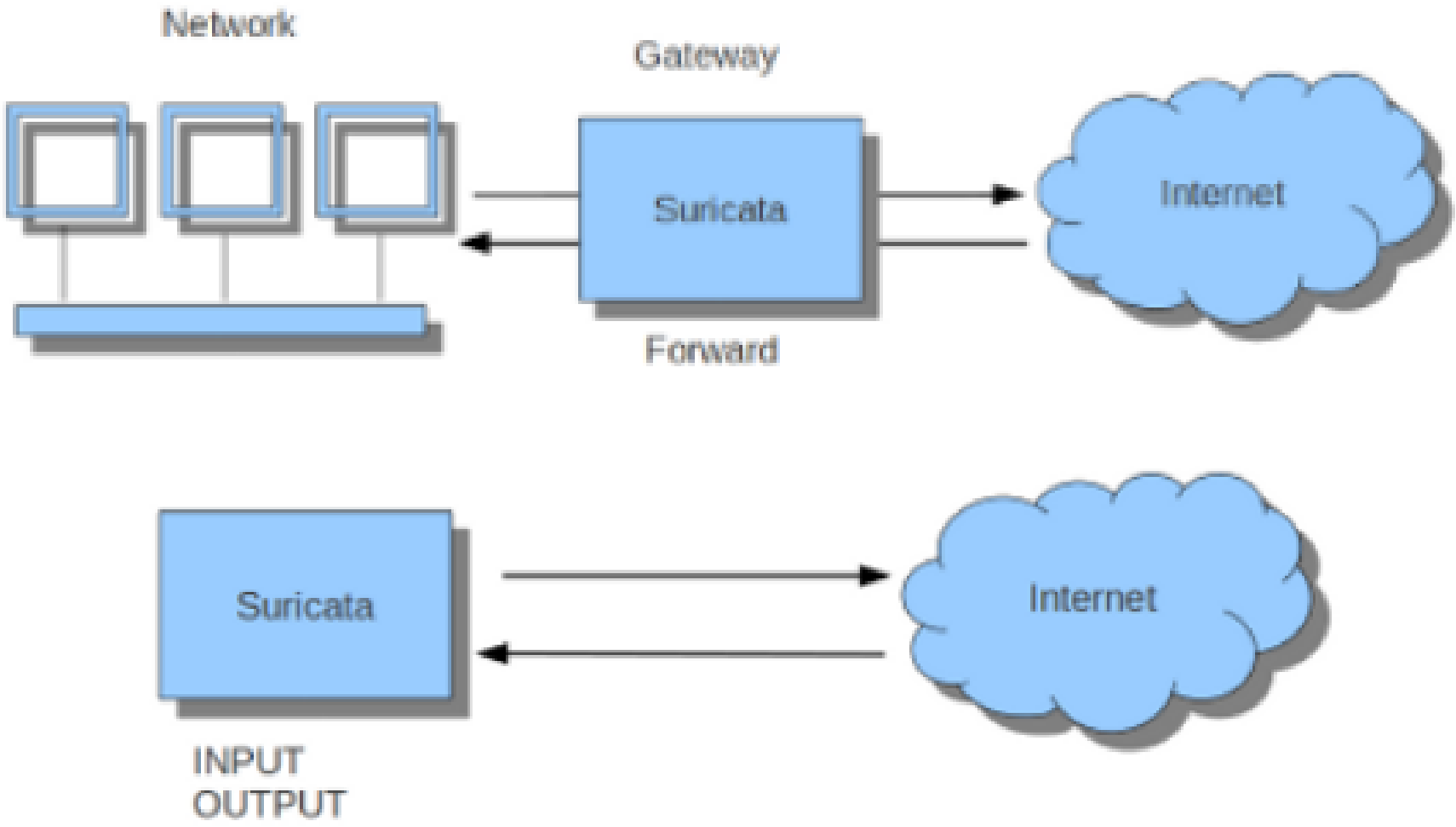
- Network: NIDS / NIPS
- Host: HIDS / HIPS

IDP Soluciones Open Source

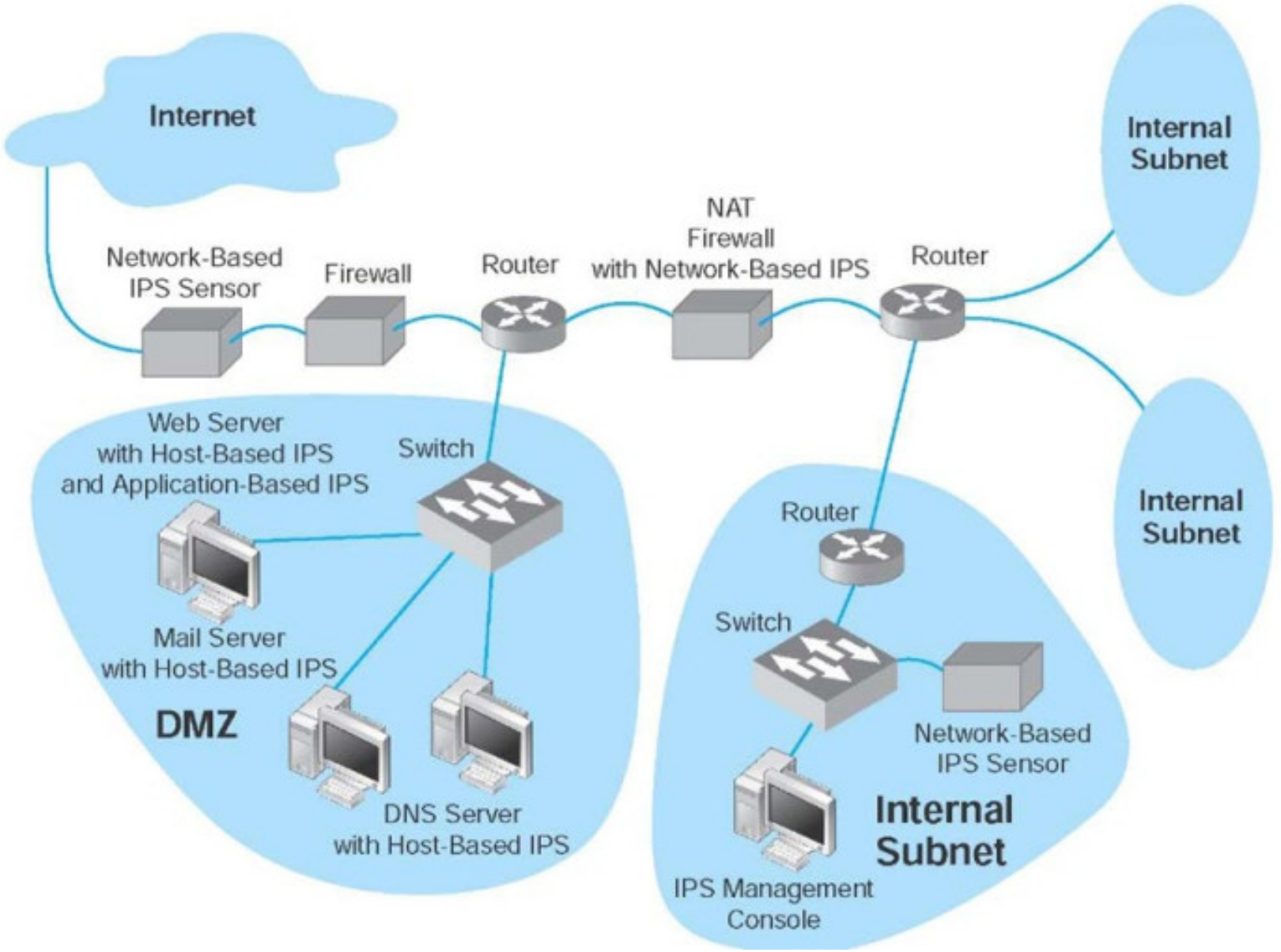
Suricata

- Open Source Next Generation Intrusion Detection and Prevention Engine
- Multi-threading
- La librería HTP es un normalizador y analizador de HTTP escrito por Ivan Ristic
- Funciona tanto como IDS e IPS
- Reglas compatibles con Snort

Suricata - Ubicaciones



Suricata - Sensores



Securetia

Sistemas Operativos Soportados

- Linux
- FreeBSD
- OpenBSD
- Mac OS X
- Windows

¿Detección Basada en Qué?

- Reglas
- Anomalías

Instalación

git clone https://github.com/securetia/suricata-workshop

apt-get install --no-install-recommends suricata

cd suricata-workshop

cp suricata.yaml /etc/suricata/

cp securetia.rules /etc/suricata/rules/

Ejecución y Archivos Importantes

suricata -i eth0

suricata -i eth0 -c /etc/suricata/suricata.yaml

tail -f /var/log/suricata/fast.log

Reglas

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Action

Header

Rule options

Reglas - Acción

pass | drop | reject | alert

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Reglas - Protocolo

tcp | udp | ip | http | ftp | ...

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Reglas - Origen

ip | variable

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Reglas - Destino

ip | variable

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Reglas - Puertos

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Reglas - Dirección

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Reglas - Meta Información

msg | sid | rev | classtype | reference | priority

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Reglas - Meta Información

msg | sid | rev | classtype | reference | priority

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Reglas - Meta Información

msg | sid | rev | classtype | reference | priority

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Reglas - Meta Información

msg | sid | rev | classtype | reference | priority

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Reglas - Meta Información

msg | sid | rev | classtype | reference | priority

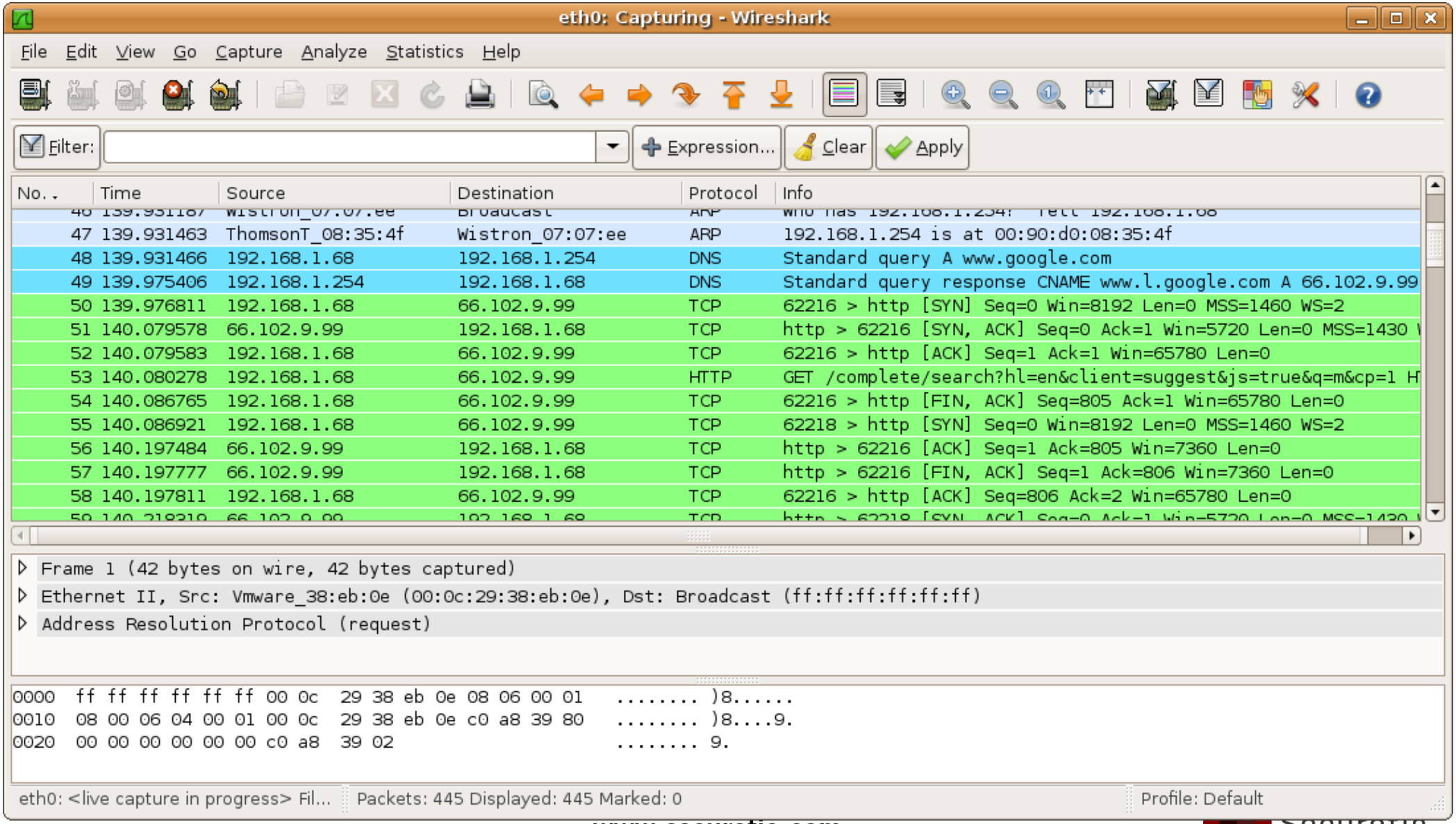
```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Reglas - Meta Información

msg | sid | rev | classtype | reference | priority

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Wireshark


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
47 139.931463 ThomsonT_08:35:4f Wistron_07:07:ee ARP 192.168.1.254 is at 00:90:d0:08:35:4f
48 139.931466 192.168.1.68 192.168.1.254 DNS Standard query A www.google.com
49 139.975406 192.168.1.254 192.168.1.68 DNS Standard query response CNAME www.l.google.com A 66.102.9.99
50 139.976811 192.168.1.68 66.102.9.99 TCP 62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51 140.079578 66.102.9.99 192.168.1.68 TCP http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52 140.079583 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53 140.080278 192.168.1.68 66.102.9.99 HTTP GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54 140.086765 192.168.1.68 66.102.9.99 TCP 62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55 140.086921 192.168.1.68 66.102.9.99 TCP 62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56 140.197484 66.102.9.99 192.168.1.68 TCP http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57 140.197777 66.102.9.99 192.168.1.68 TCP http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58 140.197811 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01 ....)8......
0010 08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 80 ....)8....9.
0020 00 00 00 00 00 00 c0 a8 39 02 .... 9.
eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

Conexiones FTP

alert tcp any any -> any 21 (msg:”FTP”; sid:10; rev:1;)

Conexiones FTP

alert tcp any any -> $FTP_SERVERS 21 (msg:”FTP”; sid:10; rev:1;)

Detección de Protocolo FTP

alert ftp any any -> any 21 (msg:"FTP"; sid:11; rev:2;)

FTP Anónimo

```
alert tcp any any -> any 21 (msg:"FTP Anonimo";
content:"anonymous"; sid:12; rev:1;)
```

FTP Anónimo (depth)

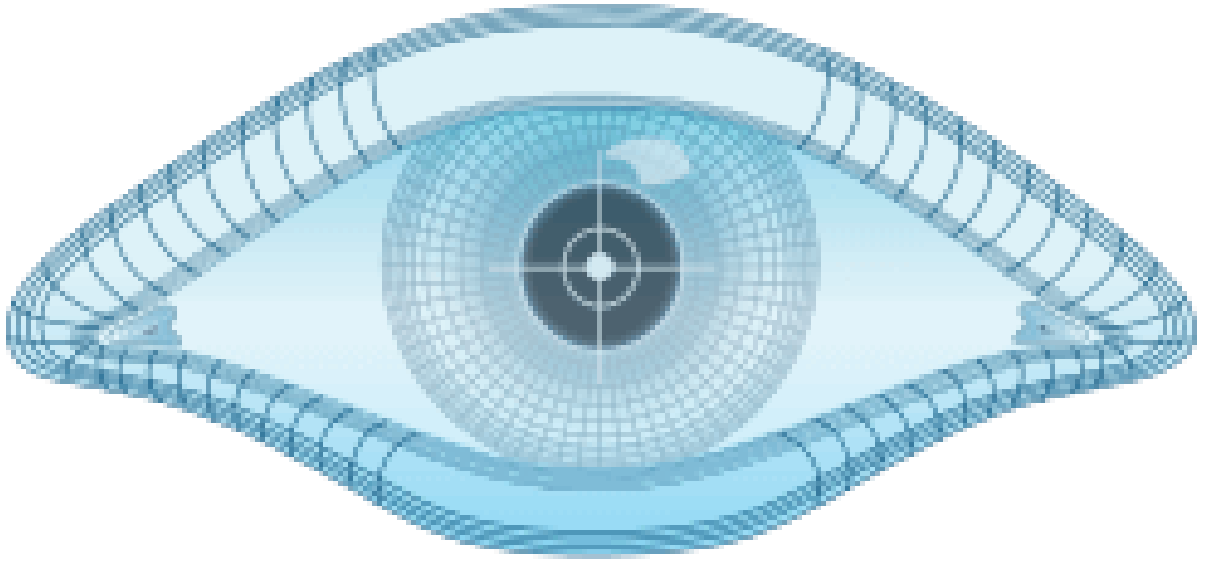
```
alert tcp any any -> any 21 (msg:"FTP Anonimo";
content:"anonymous"; depth:32; sid:13; rev:1;)
```

FTP Anónimo (nocase)

```
alert tcp any any -> any 21 (msg:"FTP Anonimo";
content:"anonymous"; nocase; depth:32; sid:14; rev:2;)
```

FTP Anónimo (user anonymous)

```
alert tcp any any -> $FTP_SERVERS 21 (msg:"FTP Anonimo";
content:"user anonymous"; nocase; depth:32; sid:15; rev:3;)
```



NMAP

Nmap -sT en Wireshark

Suricata flags

F - FIN (LSB in TCP Flags byte)
S - SYN
R - RST
P - PSH
A - ACK
U - URG
2 - Reserved bit 2
1 - Reserved bit 1 (MSB in TCP Flags byte)

There are also logical operators that can be used to specify matching criteria for the indicated flags:

+ - ALL flag, match on all specified flags plus any others
* - ANY flag, match on any of the specified flags
! - NOT flag, match if the specified flags aren't set in the packet

Regla Nmap -sT

```
alert tcp any any -> any any (msg:"Port Scan"; flags:S; threshold: type both, track by_src, count 20, seconds 3; sid:3; rev:1;)
```

Suricata thresholds

threshold:
    type <threshold|limit|both>, track <by_src|by_dst>, count <N>, seconds <T>

Nmap -sS en Wireshark

Regla Nmap -sS

alert tcp any any -> any any (msg:"Nmap -sS"; flags:S; COMPLETAR; sid:4; rev:1;)

Nmap -sA en Wireshark

Regla Nmap -sA

alert tcp any any -> any any (msg:"Port Scan"; flags:A; threshold: type both, track by_src, count 20, seconds 3; sid:5; rev:1;)

Nmap -sF en Wireshark

Regla Nmap -sF

alert tcp any any -> any any (msg:"Port Scan"; flags:F; threshold: type both, track by_src, count 20, seconds 3; sid:6; rev:1;)

onesixtyone en Wireshark

onesixtyone -c /usr/share/doc/onesixtyone/dict.txt 127.0.0.1

Regla onesixtyone

```
alert udp any any -> any 161 (msg:"onesixtyone"; threshold: type
both, track by_src, count 5, seconds 10; flow:to_server; sid:7; rev:1;)
```

Regla onesixtyone

```
alert udp any any -> any any (msg:"onesixtyone"; content:"|02 01 00
02 01 00 30 0E 30 0C 06 08 2B 06 01 02 01 01 01 00 05 00|";
threshold: type both, track by_src, count 5, seconds 10; sid:7; rev:2;)
```

Reglas complejas y probadas

https://rules.emergingthreats.net/

Preguntas