

Universidad Nacional Autónoma de México

Facultad de Estudios Superiores Aragón

Alumno: Bermeo Espino Juan Daniel

Reporte de practica: Ataque de fuerza bruta y diccionario

Temas especiales de seguridad informática

Grupo: 2060

Profesor: Jose Francisco Aguilar Hernandez

Semestre 2024-II

Su misión es descubrir con quién se está mensajeando Ana, que envió y recuperar evidencia de lo siguiente:

1. ¿Cuál es el nombre de IM del compañero de Ana?

Sec558u ser1

2 ¿Cuál fue el primer comentario de su conversación por IM?

Fue el siguiente:

Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go >:-)

3. ¿Cuál es el nombre del archivo que Ana transfirió?

recipe.docx

4. ¿Cuál es el número mágico del archivo (primeros cuatro bytes)?

504B

5. ¿Cuál es el MD5sum del archivo?

8350582774e1d4dbe1d61d64c89e0ea1

6. ¿Cuál es la receta secreta?

Recipe for Disaster:

1 serving

Ingredients:

4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

Procedimiento

Filtrar primero toda la actividad que viniera desde la ip de Ana

The image displays a Wireshark packet capture analysis of an IPsec tunnel. The top pane shows a list of 162 packets, with packet 110 selected. The middle pane shows the details of packet 110, which is an ESP packet (PUSH, ACK) with a sequence number of 132735195. The bottom pane shows the raw data of the packet in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
23	18.70809	192.168.1.158	64.12.24.50	SSL	60	Continuation Data
25	38.91496	192.168.1.158	64.12.24.50	SSL	243	Continuation Data
27	34.00659	192.168.1.158	64.12.24.50	SSL	94	Continuation Data
32	34.02680	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=210 Win=62780 Len=0
33	34.02689	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=248 Win=62742 Len=0
90	56.42591	192.168.1.158	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
91	57.42716	192.168.1.158	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
92	58.45876	192.168.1.158	64.12.24.50	SSL	182	Continuation Data
96	58.56971	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=364 Ack=457 Win=62742 Len=0
98	58.57447	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=364 Ack=495 Win=62742 Len=0
110	61.05239	192.168.1.158	192.168.1.158	TCP	62	5190 → 1272 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
112	61.05484	192.168.1.158	192.168.1.158	TCP	318	5190 → 1272 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=256
118	61.15576	192.168.1.158	192.168.1.158	TCP	60	5190 → 1272 [ACK] Seq=257 Ack=257 Win=6432 Len=0
119	61.270615	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=257 Ack=257 Win=6432 Len=1460
120	61.270620	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=1717 Ack=257 Win=6432 Len=1460
122	61.270628	192.168.1.158	192.168.1.158	TCP	1230	5190 → 1272 [PSH, ACK] Seq=3177 Ack=257 Win=6432 Len=1716
123	61.270632	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=4353 Ack=257 Win=6432 Len=1460
124	61.270635	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=5813 Ack=257 Win=6432 Len=1460
126	61.270641	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=7673 Ack=257 Win=6432 Len=1460
127	61.270644	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=8733 Ack=257 Win=6432 Len=1460
128	61.270647	192.168.1.158	192.168.1.158	TCP	358	5190 → 1272 [PSH, ACK] Seq=10193 Ack=257 Win=6432 Len=304
129	61.270651	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=16497 Ack=257 Win=6432 Len=1460
131	61.270658	192.168.1.158	192.168.1.158	TCP	382	5190 → 1272 [PSH, ACK] Seq=1957 Ack=257 Win=6432 Len=308
134	61.270711	192.168.1.158	192.168.1.158	TCP	60	5190 → 1272 [ACK] Seq=12265 Ack=513 Win=7504 Len=0
137	61.288392	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=364 Ack=624 Win=62742 Len=0
139	61.337771	192.168.1.158	192.168.1.158	TCP	60	5190 → 1272 [ACK] Seq=12265 Ack=514 Win=7504 Len=0
162	67.395540	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=364 Ack=664 Win=62742 Len=0

Packet 110 Details:

- [Stream index: 2]
- [Conversation completeness: Incomplete (12)]
- [TCP Segment Len: 6]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 862704323
- [Next Sequence Number: 7 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 132735195
- 0101... = Header Length: 20 bytes (5)
- Flags: 0x015 (PSH, ACK)

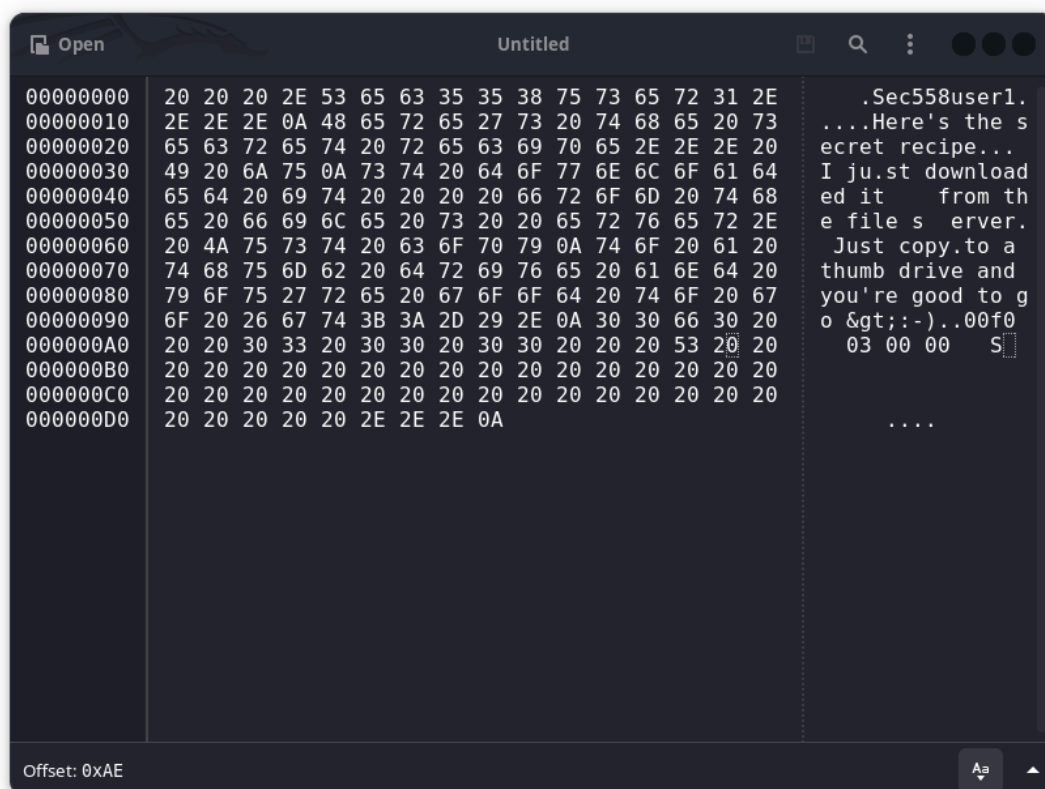
Raw Data:

```

0000  00 00 2c 00 2d 08 b2 60 02 12 79 45 a4 bb 08 00 45 00
0010  00 2e ab 3b 49 00 40 06 75 0a c0 a8 81 9e 40 0c
0020  18 32 c7 b8 81 bb 33 6b d2 c3 07 e9 60 db 50 18
0030  f5 3c 3d 39 00 2a 05 90 60 00 00
  
```

Summary: The capture shows a series of TCP connections and a specific IPsec tunnel session. Packet 110 is a SYN-ACK from the local host to itself, indicating a loopback or a specific test scenario. The raw data shows the packet structure and flags, including the PUSH and ACK flags.

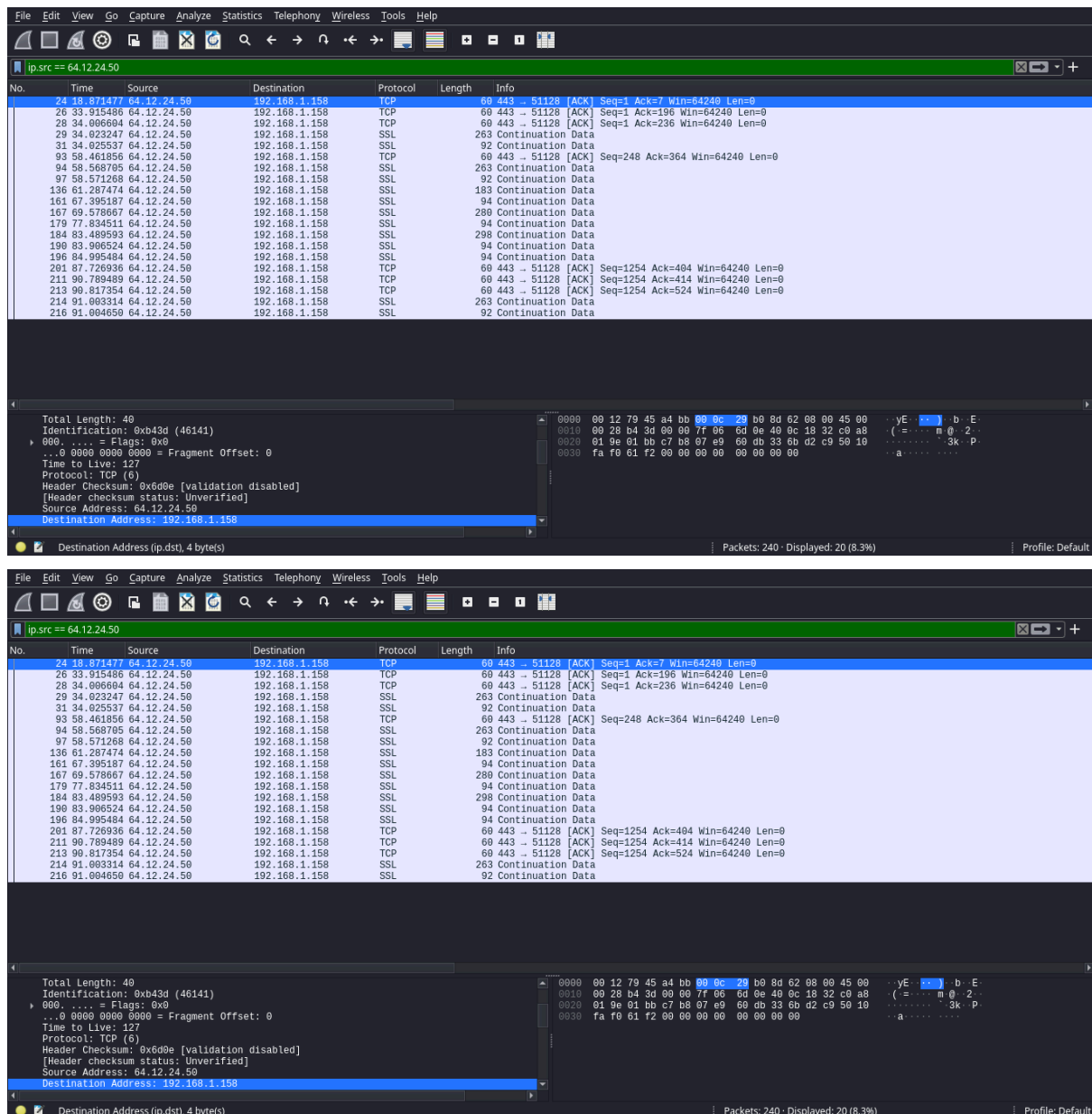
Después en la captura número 25 encontramos lo siguiente después de limpiar el hexadecimal:



Una vez reconocido lo anterior procedemos a rastrear a quien se le envio el mensaje

```
Source Address: 192.168.1.158
Destination Address: 64.12.24.50
```

Al checar la entra y salida de la ip destino podemos ver que solo tuvo comunicaci3n con la ip de Ana



Una vez realizado lo anterior procedimos a manipular la información adquirida con un editor hexadecimal para adquirir las respuestas solicitadas.

Para eficientizar la parte de la construcción del archivo se uso NetWork Miner que nos ayudo no solo a adquirir la información requerida del archivo, si no también a mejorar las respuestas antes adquiridas únicamente desde lo posible en nuestras capacidades con WireShark

