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:

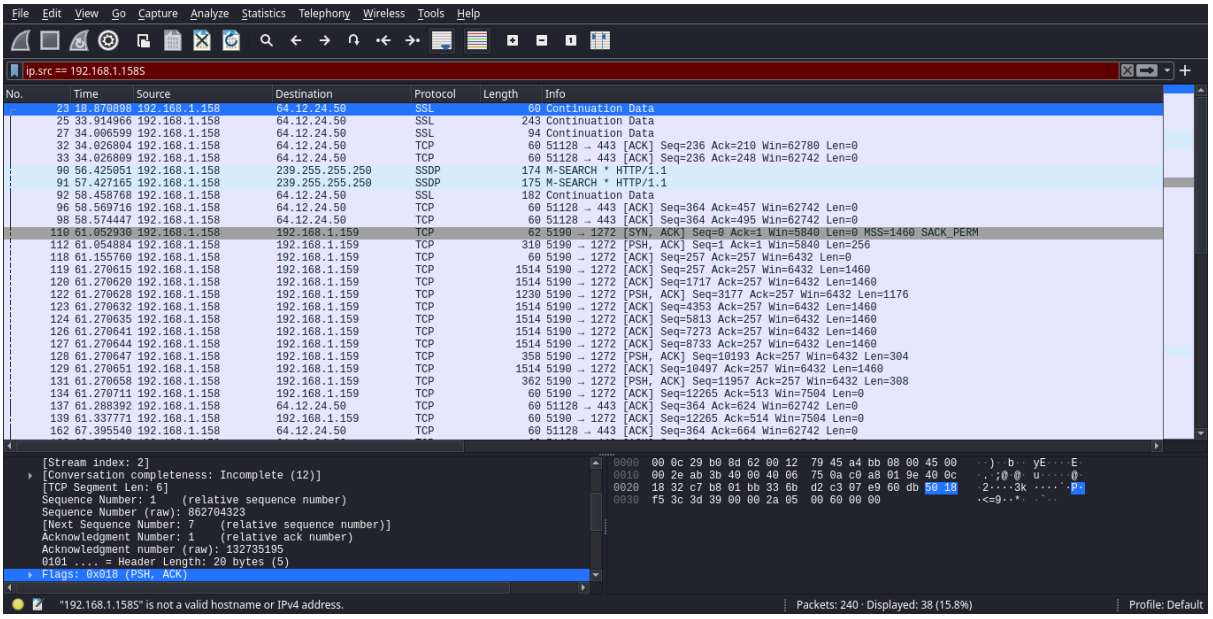
4 cups sugar

2 cups water

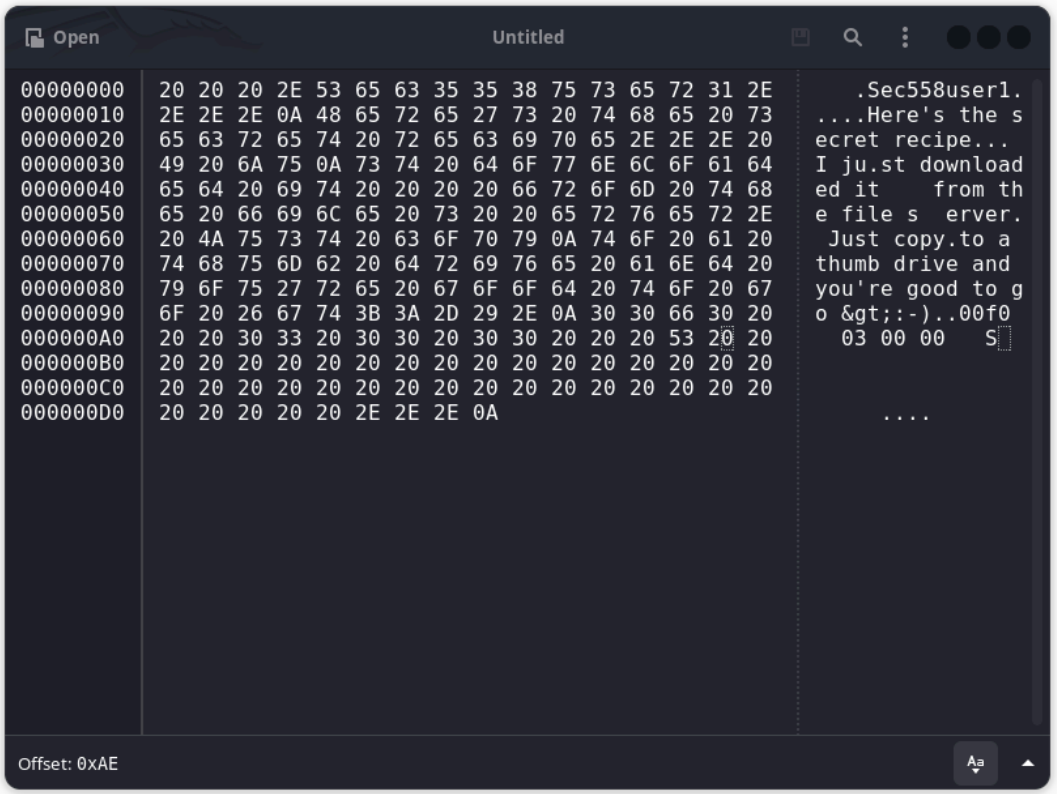
In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

Procedimiento

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



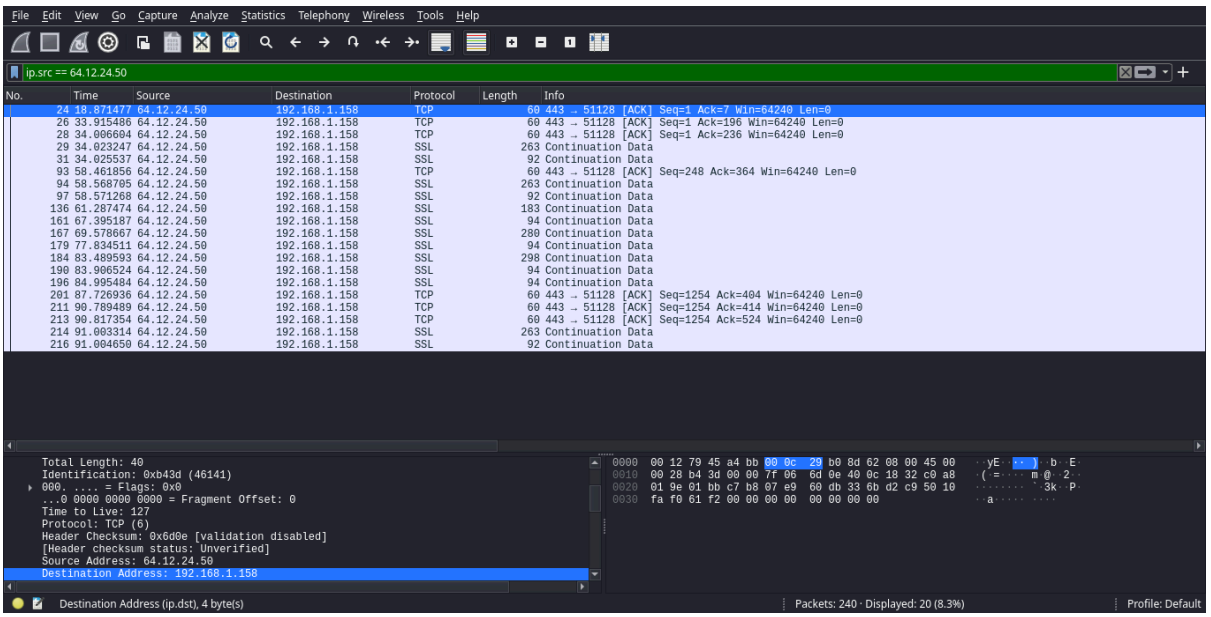
Después en la captura número 25 encontramos lo siguiente después de limpiar el hexadecimal:

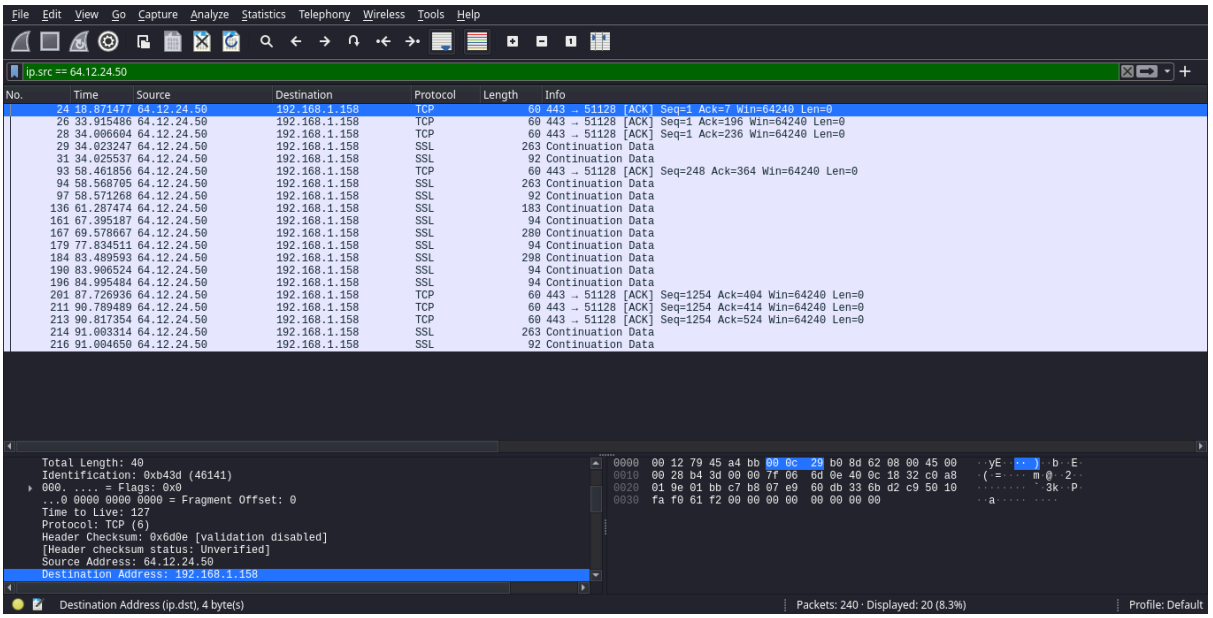


Una vez reconocido lo anterior procedemos a rastrear a quien se le envio el mensaje

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

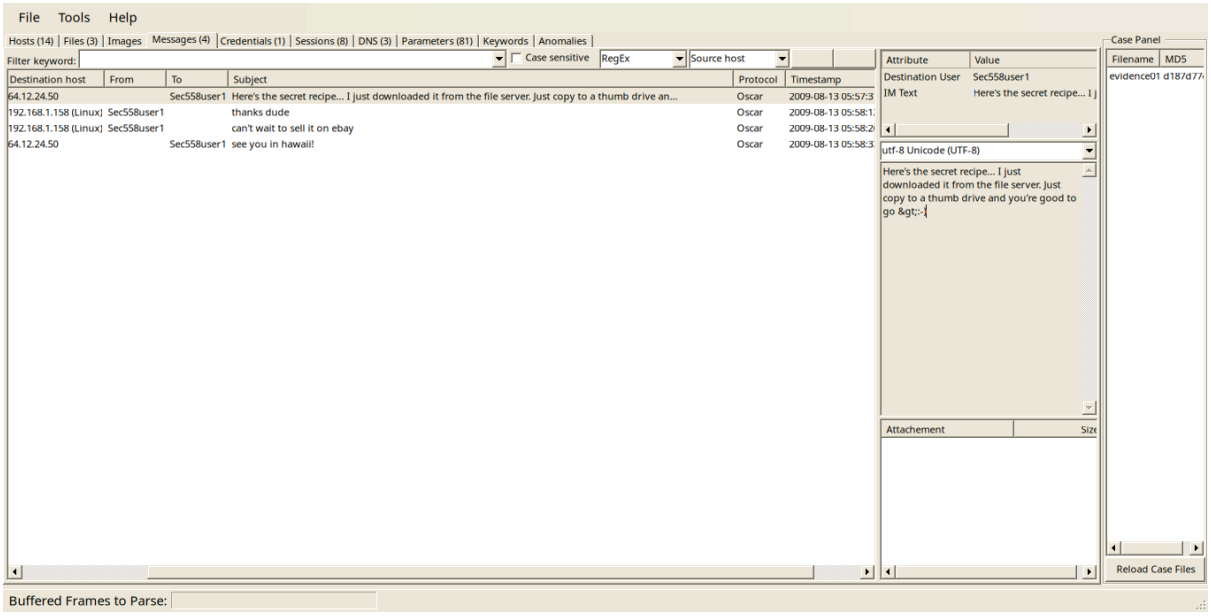
Al checar la entra y salida de la ip destino podemos ver que solo tuvo comunicación con la ip de Ana

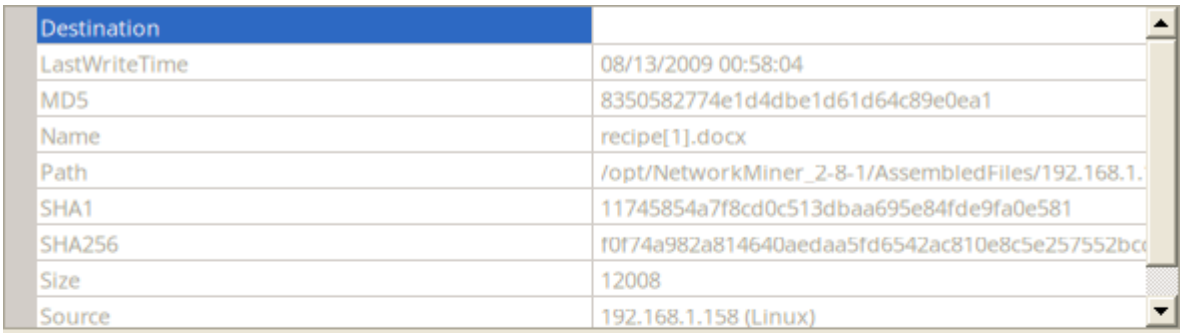


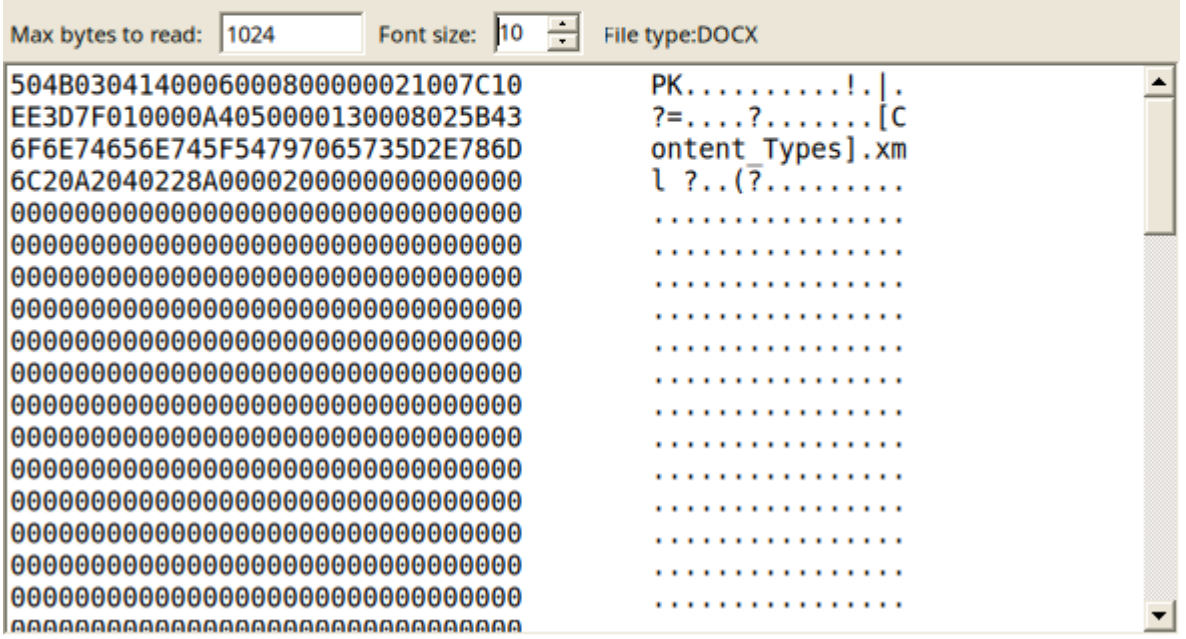


Una vez realizado lo anterior procedimos a manipular la información adquirida con un editor hexadecimal para adquirir las respuestas solicitadas.

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


File Tools Help
Hosts (14) Files (3) Images Messages (4) Credentials (1) Sessions (8) DNS (3) Parameters (81) Keywords Anomalies
Filter keyword:
Case sensitive
RegEx
Source host
Destination host From To Subject Protocol Timestamp
64.12.24.50 Sec558user1 Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive an... Oscar 2009-08-13 05:57:3
192.168.1.158 (Linux) Sec558user1 thanks dude Oscar 2009-08-13 05:58:1
192.168.1.158 (Linux) Sec558user1 can't wait to sell it on ebay Oscar 2009-08-13 05:58:2
64.12.24.50 Sec558user1 see you in hawaii! Oscar 2009-08-13 05:58:3
Attribute Value
Destination User Sec558user1
IM Text Here's the secret recipe... I j
utf-8 Unicode (UTF-8)
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 >:-]
Attachement
Case Panel
Filename MD5
evidence01 d187d77
Reload Case Files
Buffered Frames to Parse:


Destination
LastWriteTime 08/13/2009 00:58:04
MD5 8350582774e1d4dbe1d61d64c89e0ea1
Name recipe[1].docx
Path /opt/NetworkMiner_2-8-1/AssembledFiles/192.168.1.
SHA1 11745854a7f8cd0c513dbaa695e84fde9fa0e581
SHA256 f0f74a982a814640aedaa5fd6542ac810e8c5e257552bc
Size 12008
Source 192.168.1.158 (Linux)


Max bytes to read: 1024
Font size: 10
File type:DOCX
504B0304140006000800000021007C10 PK.....!.|.
EE3D7F010000A4050000130008025B43 ?=....?.....[C
6F6E74656E745F54797065735D2E786D ontent_Types].xm
6C20A2040228A0000200000000000000 l ?..(?.....