Universidad Francisco de Vitoria
UFV Madrid

Hacking Ético

Practica NetCat

Gonzalo Pascual Romero

Fecha: 12/11/2023

Índice

Alcance

1. Comprobar que en la máquina atacante y atacada está netcat instalado, si no, instalarlo

2. Ejecutar nc -h e instalar las posibilidades

3. Usar netcat a modo chat

    a. Lanzar nc en listening en la máquina atacada con parámetros “lvp” y en el puerto 4444
    b. Conectar la máquina atacante a esa máquina
    c. Lanzar chat
    d. Comprobar en la máquina atacante mediante wireshart el tráfico (filtrar por puerto)

4. Usar netcat para transferir archivos de la máquina atacante a la atacada
    a. Lanzar nc en listening en el puerto 4444 la máquina atacada
    b. Enviar un archivo(de texto para ser más visible en WS) desde el atacante al atacado
    c. Comprobar en la máquina atacante mediante wireshark el fichero enviado
    d. Comprobar en la máquina atacada que ha llegado el fichero

5. Bind Shell (escucha la máquina atacada)
    a. Levantar nc en modo listening en el puerto 4444 con la opción para ejecutar el comando bash
    b. Poner el atacante a la escucha del atacado
    c. Ejecutar varios comandos básicos y comprobar con WS

6. Reverse Shell
    a. La máquina atacante estará a la escucha y la máquina atacada será la que se conecte al atacante. Elegir la Shell que queremos que se ejecute en la máquina atacada
    b. Ejecutar varios comandos y comprobar con WS

Desarrollo del estudio

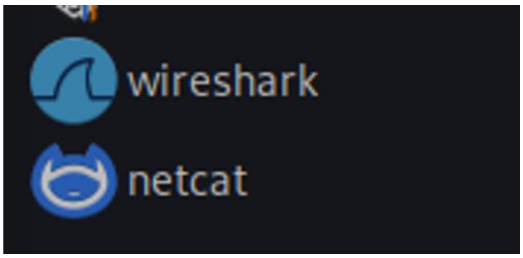
El estudio se ha realizado en dos máquinas virtuales Kali-Linux usando las siguientes aplicaciones:

NetCat: Es una herramienta de línea de comandos que permite la comunicación y transferencia de datos entre dos sistemas a través de una red usa los protocolos TCP/IP y UDP. Se utilizará para establecer conexiones entre una máquina "atacante" y una máquina "atacada" con el propósito de evaluar la seguridad y realizar pruebas de penetración.

WireShark: Wireshark es una herramienta de análisis de protocolos de red que permite la captura y el examen detallado del tráfico de red en tiempo real. Se utilizará para supervisar y analizar el tráfico de red entre una máquina "atacante" y una máquina "atacada." Esto facilita la identificación de posibles vulnerabilidades, problemas de seguridad y la evaluación de la comunicación en la red para fines de diagnóstico y seguridad.

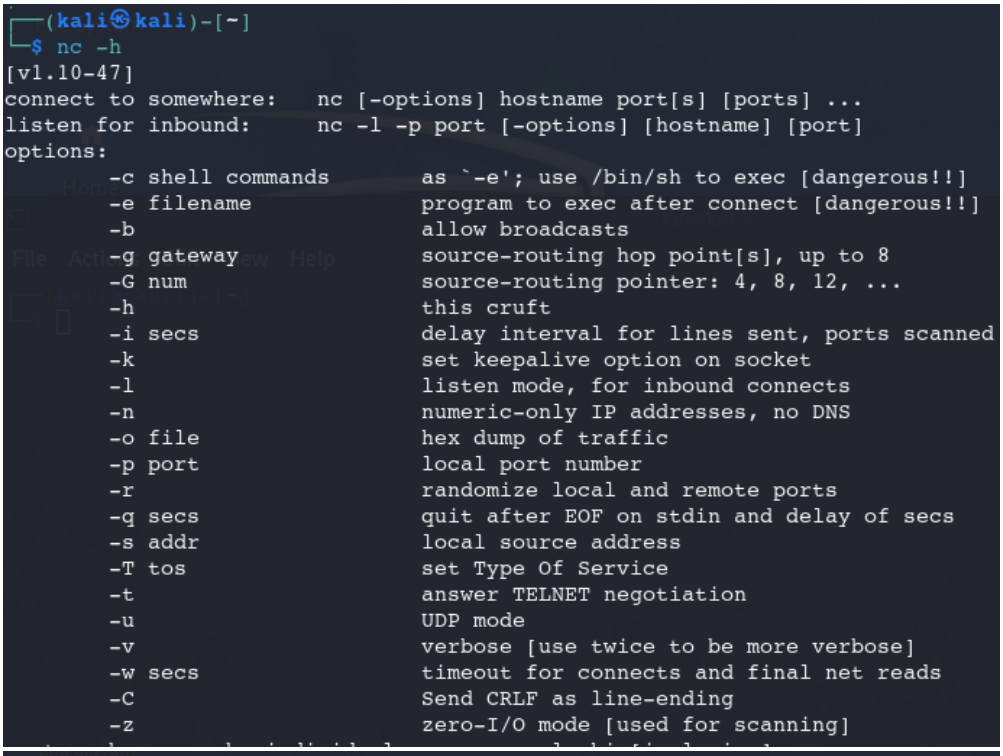
1.Comprobar que en la máquina atacante y atacada está netcat instalado, si no, instalarlo

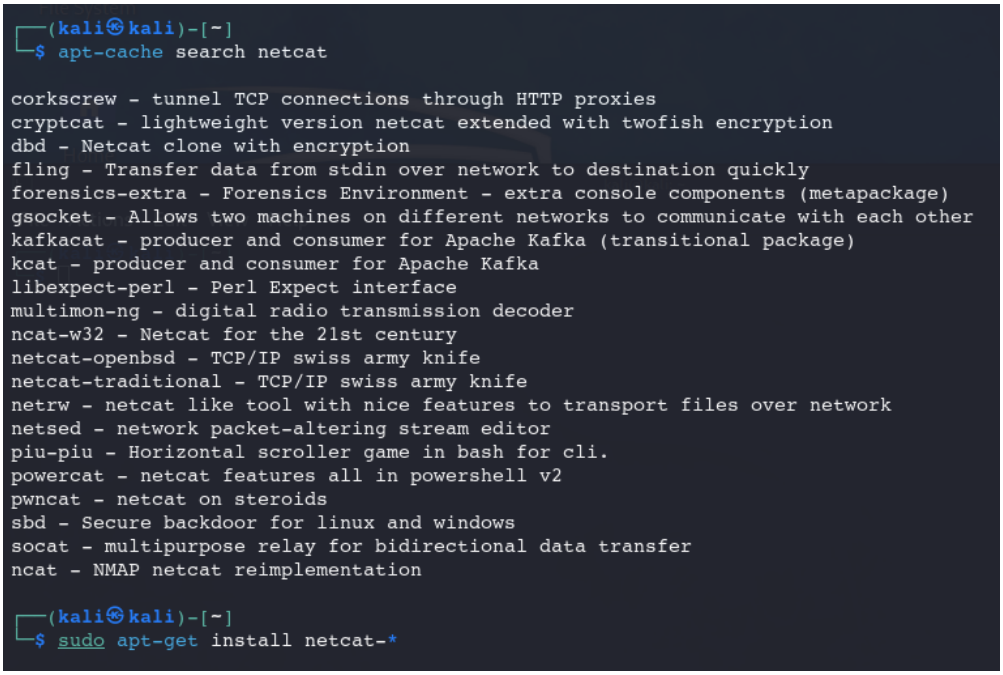
Al haber usado Kali-Linux no me ha hecho falta instalar nada ya vienen instaladas por defecto



2.Ejecutar nc -h e instalar las posibilidades

Ejecuté el comando nc -h para mostrar las opciones disponibles en NetCat. Para instalar opciones adicionales en Kali Linux, se pueden explorar los paquetes relacionados con NetCat utilizando “apt-cache search netcat” y luego instalar los paquetes deseados utilizando “apt-get install netcat-” seguido del nombre del paquete específico. Para este estudio en concreto no es necesario instalar nada más de lo que ya viene en NetCat





3. Usar NetCat a modo chat

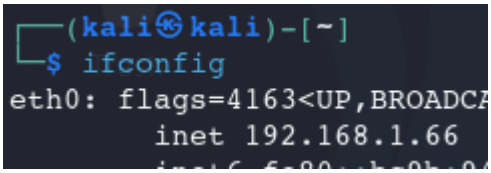
NetCat en modo chat significa comunicarse en tiempo real entre dos sistemas a través de la red utilizando NetCat. Uno actúa como servidor(atacada), el otro como cliente(atacante), y pueden intercambiar mensajes y datos en vivo.

Para ello usé dos máquinas virtuales de Kali como mencioné antes. La primera es la atacante y la segunda la atacada. Para iniciar el chat la atacada abrirá la comunicación del puerto y la atacante se conectará a ella.

Antes de iniciar la conexión hay que saber las IPs de las máquinas para poder conectarlas, por lo que hice un 'ifconfig' en ambas de tal forma que me la muestre

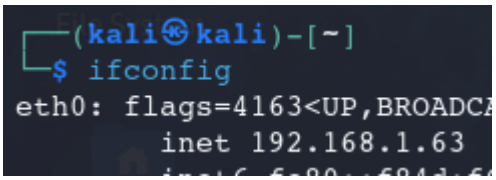
Máquina atacada:

192.168.1.66



Máquina atacante:

192.168.1.63



Máquina atacada:

Lo primero que hice fue abrir la comunicación de la máquina atacada a la que después la máquina atacante se conectara. Lo hice mediante el comando nc (inicia NetCat) con las opciones -l (escucha, de forma que espera una conexión entrante) -v (verbose o detallado, lo que significa que netcat mostrará más información adicional sobre las conexiones) y -p (Puerto, para especificar en que puerto se está escuchando) seguido del puerto 4444

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.1.63: inverse host lookup failed: Unknown host
connect to [192.168.1.66] from (UNKNOWN) [192.168.1.63] 51458
Hola
Todo bien?
Muy bien
```

Máquina atacante:

Como la máquina atacada abrí NetCat con el comando nc, seguí con la ip de la maquina atacada y terminé con el puerto al cual se va a conectar

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.66 4444
Hola
Todo bien?
Muy bien
```

Una vez enviado el comando, en la máquina atacada apareció que la máquina atacante se había conectado y a partir de ahí se pudo escribir mensajes desde ambas máquinas convirtiéndolo en un chat.

Comprobación WireShark:

WireShark lo inicié desde antes de establecer la conexión entre las máquinas para que se grabara todo el proceso, aunque buscaré y me centrare en buscar los mensajes que se han mandado entre ambas máquinas. Para ello en la máquina atacante abrí WireShark en la red a la que está conectada (eth0) y filtré por tcp.port==4444 || udp.port ==4444.

tcp.port == 4444 || udp.port == 4444

No.	Time	Source	Destination	Protocol	Length	In
616	85.356464391	192.168.1.63	192.168.1.66	TCP	74	6
619	85.357229131	192.168.1.66	192.168.1.63	TCP	74	4
620	85.357257688	192.168.1.63	192.168.1.66	TCP	66	6
684	98.449284201	192.168.1.63	192.168.1.66	TCP	71	6
685	98.449579925	192.168.1.66	192.168.1.63	TCP	66	4
758	114.781290904	192.168.1.63	192.168.1.66	TCP	77	6
759	114.781603182	192.168.1.66	192.168.1.63	TCP	66	4
805	125.501819639	192.168.1.66	192.168.1.63	TCP	75	4
806	125.501847605	192.168.1.63	192.168.1.66	TCP	66	6

Una vez terminado el chat comprobé en los paquetes los datos para buscar los mensajes que anteriormente mandé en el chat.

En uno de ellos en Data encontré un código hexadecimal que pasé a Ascii para ver el mensaje que había mandado de una máquina a otra.

```
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    TCP Option - No-Operation (NOP)
    TCP Option - No-Operation (NOP)
    TCP Option - Timestamps
  [Timestamps]
    [Time since first frame in this TCP stream: 29.424826513 seconds]
    [Time since previous frame in this TCP stream: 16.331710979 seconds]
  [SEQ/ACK analysis]
    [iRTT: 0.000793297 seconds]
    [Bytes in flight: 11]
    [Bytes sent since last PSH flag: 11]
  TCP payload (11 bytes)
Data (11 bytes)
  Data: 546f646f206269656e3f0a
  [Length: 11]
```

546f646f206269656e3f0a

22 1

Output

Todo bien?

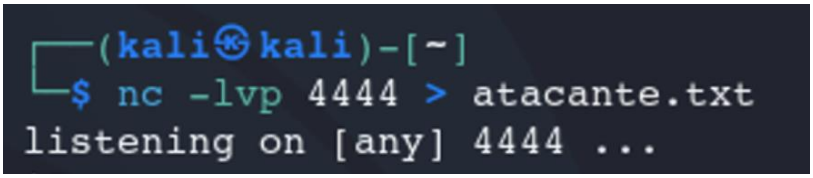
4. Usar NetCat para transferir archivos de la máquina atacante a la atacada

NetCat se puede usar para transferir archivos desde la máquina que envía (atacante) a la máquina receptora (atacada) a través de una conexión de red.

Para iniciar el chat la atacada abrirá la comunicación del puerto y la atacante se conectará a ella.

Máquina atacada:

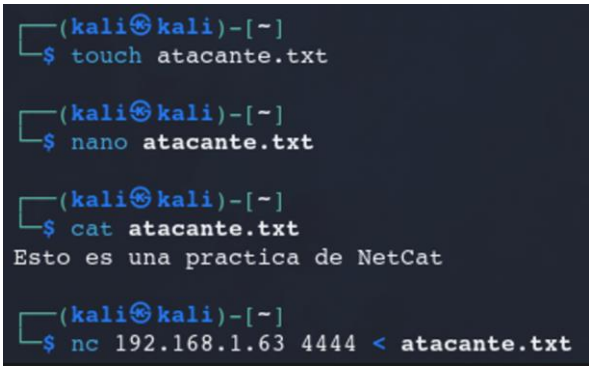
Como en la cuestión anterior la máquina atacada es la que abre la comunicación con para que la máquina atacante se conecte. Con nc se abre NetCat y se le dí las opciones -l (escucha) -v (detallado) y -p (puerto) seguido del puerto 4444 que será al que nos conectemos con la máquina atacante y '>' para indicar que recibe y "atacante.txt" para especificar que archivo de texto se va a enviar desde la máquina atacante.



Máquina atacante:

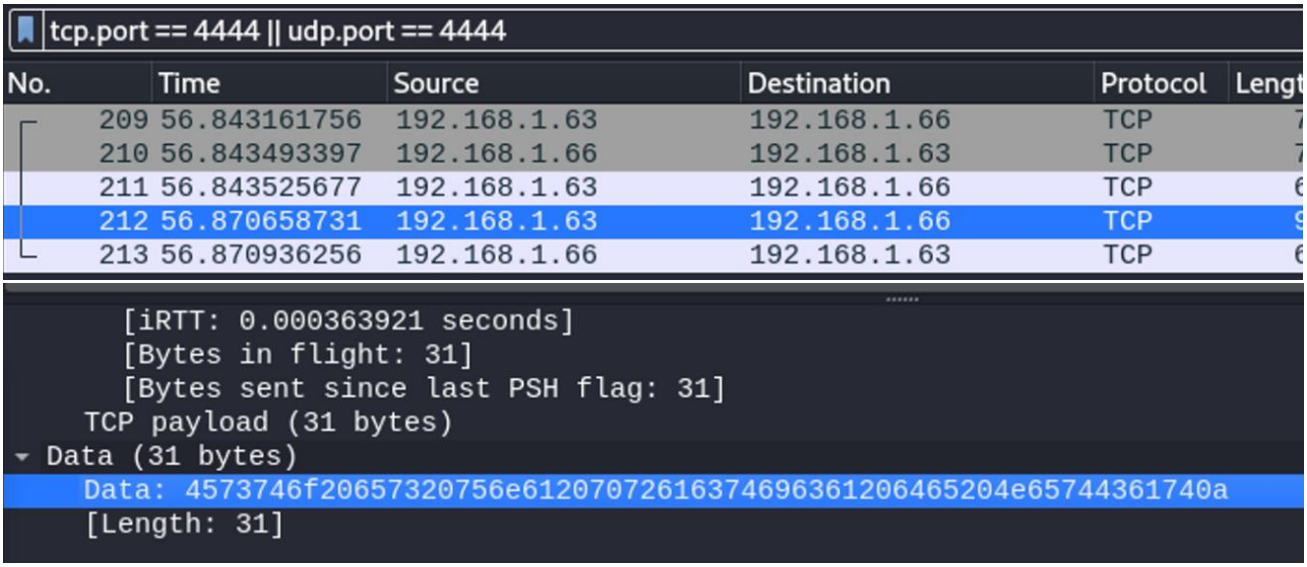
En la máquina atacante lo primero que hice fue crear un archivo de texto para después mandarlo a la máquina atacada, con el comando touch se crea, con el comando nano se abre para escribir en el y con el cat se imprime en la terminal el contenido del fichero, en el que escribí 'Esto es una práctica de NetCat'.

Para pasarlo a la máquina atacada escribí nc para abrir NetCat, la ip de la máquina atacada, el puerto al que nos vamos a conectar y con el símbolo '<' indicamos que vamos a mandar el archivo 'atacante.txt'.



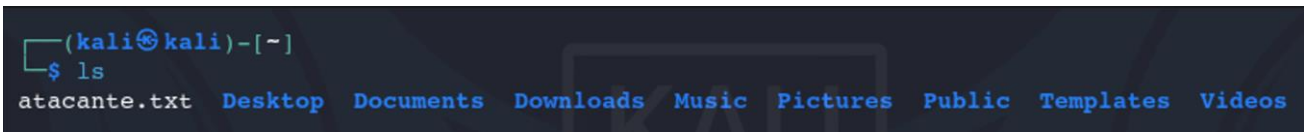
Comprobación WireShark:

Siguiendo el mismo procedimiento para abrir WireShark y filtrar por el puerto 4444 antes de trasferir el archivo, grabe todo el tráfico del puerto. Tras enviar el archivo busqué el interior del contenido del txt que es lo que más interesa mirar.



En data salió un mensaje en Hexadecimal que pase Ascii en el que sale el mensaje que escribí anteriormente en el txt desde la máquina atacante

Por último, comprobé en la máquina atacada si se ha pasado correctamente el archivo. Para ello en la terminal puse ls para ver todos los archivos y carpetas en la cual estaba el archivo.

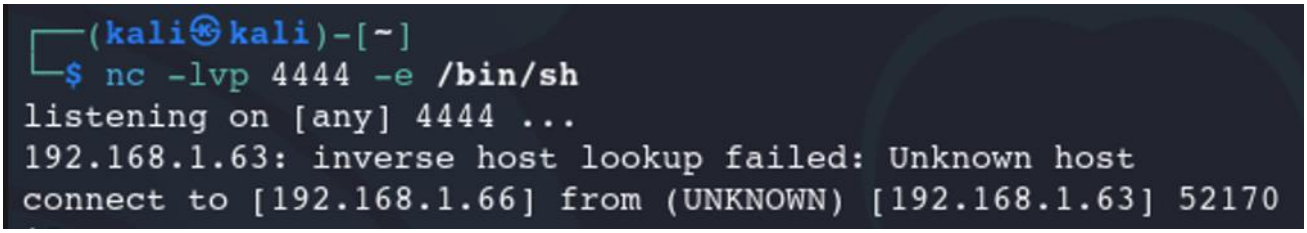


5. Bind Shell

Es una técnica utilizada que permite a un atacante obtener acceso a una computadora remota. El usuario el cual proporciona la Shell (el atacado), espera una conexión en un puerto en específico. Cuando un cliente (el atacante) se conecta a este puerto, se entabla una comunicación, en la cual todo lo que envía el usuario se considera un comando que se inserta en la shell del usuario.

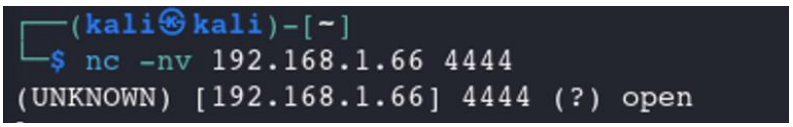
Máquina atacada:

Como en los anteriores la máquina atacada es la que abre la conexión para que la atacante se una a ella. En la terminal con nc abrí NetCat y le dí las opciones -l (escucha) -v (detallado) y -p (puerto) seguido del puerto 4444 que será al que nos conectemos con la máquina atacante, -e para indicar que archivo ejecutaremos tras la conexión y a continuación el enlace al archivo en cuestión que en este caso será a la terminal del sistema.



Máquina atacante:

Para conectarme la máquina atacante escribí nc para abrir NetCat, incluí las opciones -n(evita que NetCat realice consultas DNS y la exposición de nombres de host en el registro de actividad) y -v (verbose o detallado, lo que significa que netcat mostrará más información adicional sobre las conexiones), a continuación la IP de la máquina atacada y el puerto al que se va a conectar.



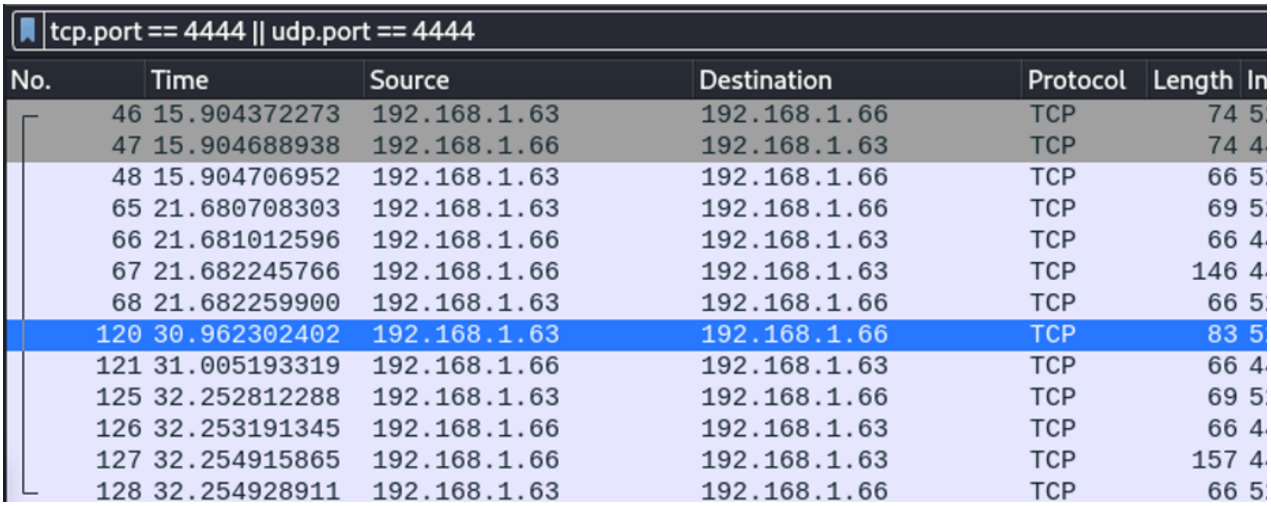
A partir de ahí se podrán hacer comandos en la máquina atacada desde la máquina atacante.

Probé a escribir un ls y mostrar las carpetas y archivos, un touch para crear un archivo prueba.txt y otra vez un ls para comprobar que se ha creado el archivo

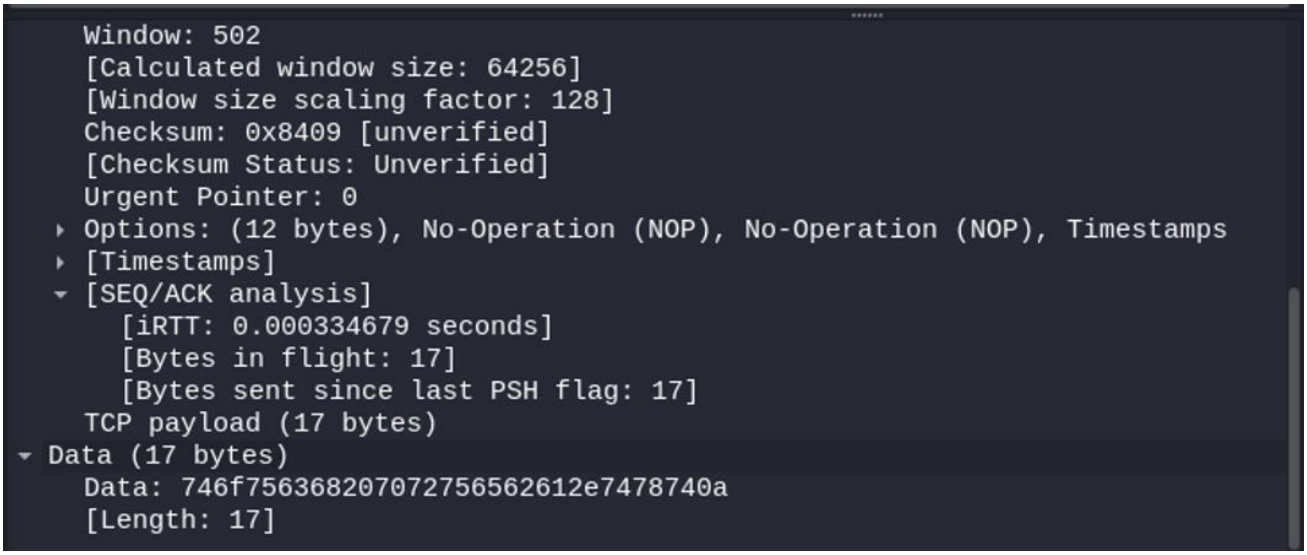
```
ls
atacante.txt
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
touch prueba.txt
ls
atacante.txt
Desktop
Documents
Downloads
Music
Pictures
prueba.txt
Public
Templates
Videos
```

Comprobación WireShark:

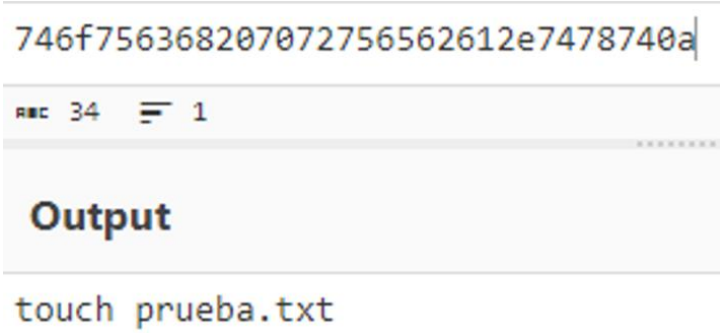
Siguiendo el mismo procedimiento para abrir WireShark que en los anteriores casos, filtré por el puerto 4444 y grabé todo el tráfico del puerto. Una vez que terminé de hacer todos los comandos busqué en los paquetes los comandos que ejecuté desde la máquina atacante.



No.	Time	Source	Destination	Protocol	Length	In
46	15.904372273	192.168.1.63	192.168.1.66	TCP	74	5
47	15.904688938	192.168.1.66	192.168.1.63	TCP	74	4
48	15.904706952	192.168.1.63	192.168.1.66	TCP	66	5
65	21.680708303	192.168.1.63	192.168.1.66	TCP	69	5
66	21.681012596	192.168.1.66	192.168.1.63	TCP	66	4
67	21.682245766	192.168.1.66	192.168.1.63	TCP	146	4
68	21.682259900	192.168.1.63	192.168.1.66	TCP	66	5
120	30.962302402	192.168.1.63	192.168.1.66	TCP	83	5
121	31.005193319	192.168.1.66	192.168.1.63	TCP	66	4
125	32.252812288	192.168.1.63	192.168.1.66	TCP	69	5
126	32.253191345	192.168.1.66	192.168.1.63	TCP	66	4
127	32.254915865	192.168.1.66	192.168.1.63	TCP	157	4
128	32.254928911	192.168.1.63	192.168.1.66	TCP	66	5



En uno de los paquetes en la parte de data salió un mensaje en Hexadecimal que pase Ascii en el que aparece uno de los comandos que realice.

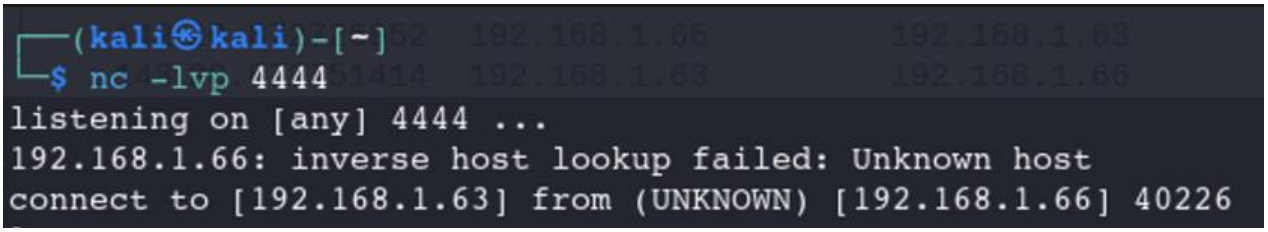


6. Reverse Shell

Es una técnica utilizada que permite a un atacante obtener acceso a una computadora remota. Al contrario que el Bind Shell en este caso el atacante es el que proporciona la Shell y espera una conexión en un puerto en específico hasta que el atacado se conecta a este puerto y se entabla una comunicación en la cual todo lo que envía el atacante se considera un comando que se inserta en la shell del atacado.

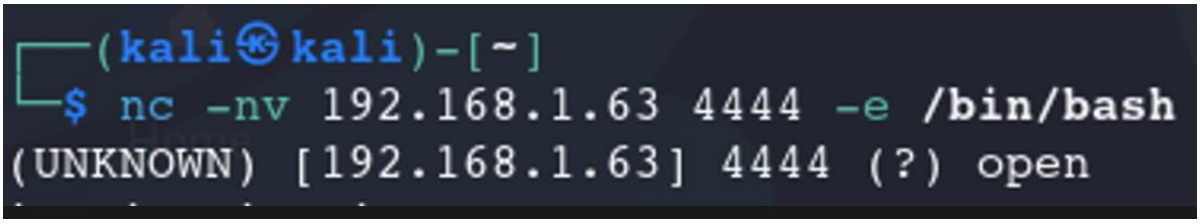
Máquina atacante:

En este caso a diferencia de los anteriores la máquina atacante es la que abre la conexión. Se hace mediante un nc para abrir NetCat y las opciones -l (escucha) -v (detallado) y -p (puerto) seguido del puerto 4444 que será al que nos conectemos con la máquina atacada



Máquina atacada:

Ahora la máquina atacada será la que se conecte a la máquina atacante mediante el siguiente comando. Como siempre nc para abrir NetCat como opciones escribimos -n(evita que NetCat realice consultas DNS y la exposición de nombres de host en el registro de actividad) y -v (verbose o detallado, lo que significa que netcat mostrará más información adicional sobre las conexiones), a continuación al IP de la máquina atacada, el puerto al que se va a conectar, -e para indicar que archivo ejecutaré tras la conexión y a continuación el enlace al archivo que en este caso será a la terminal del sistema.

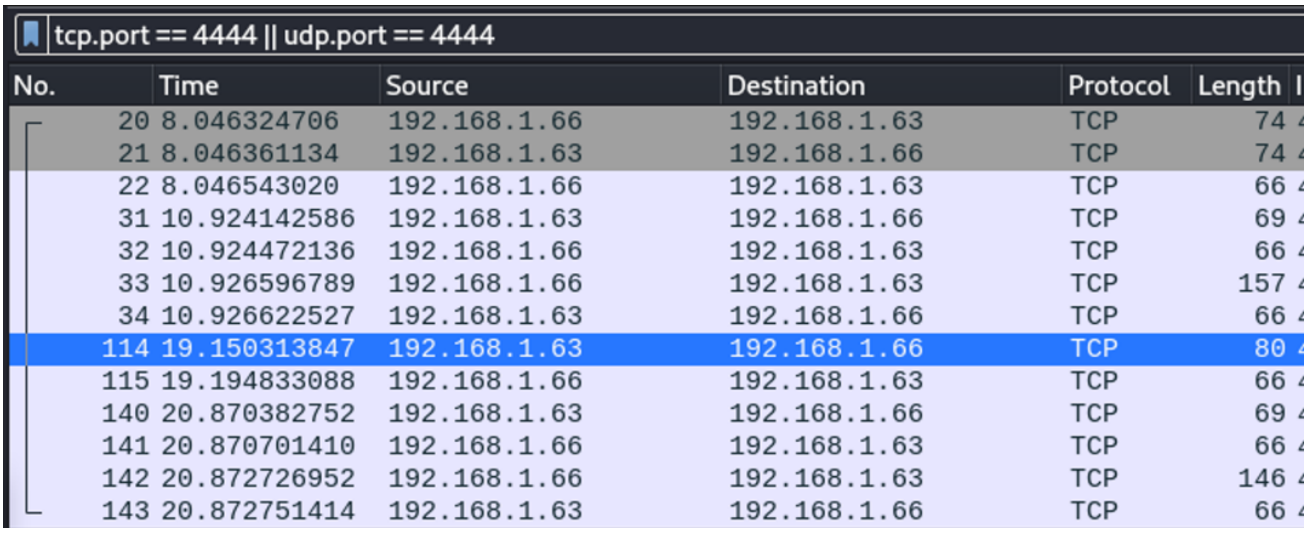


Desde la terminal del atacante comprobamos que se puedan ejecutar comandos. Ejecuto un ls para mostrar carpetas y archivos, hago un rm prueba.txt para eliminar el archivo de texto prueba y repito un ls para verificar que efectivamente se ha eliminado de la máquina atacada.

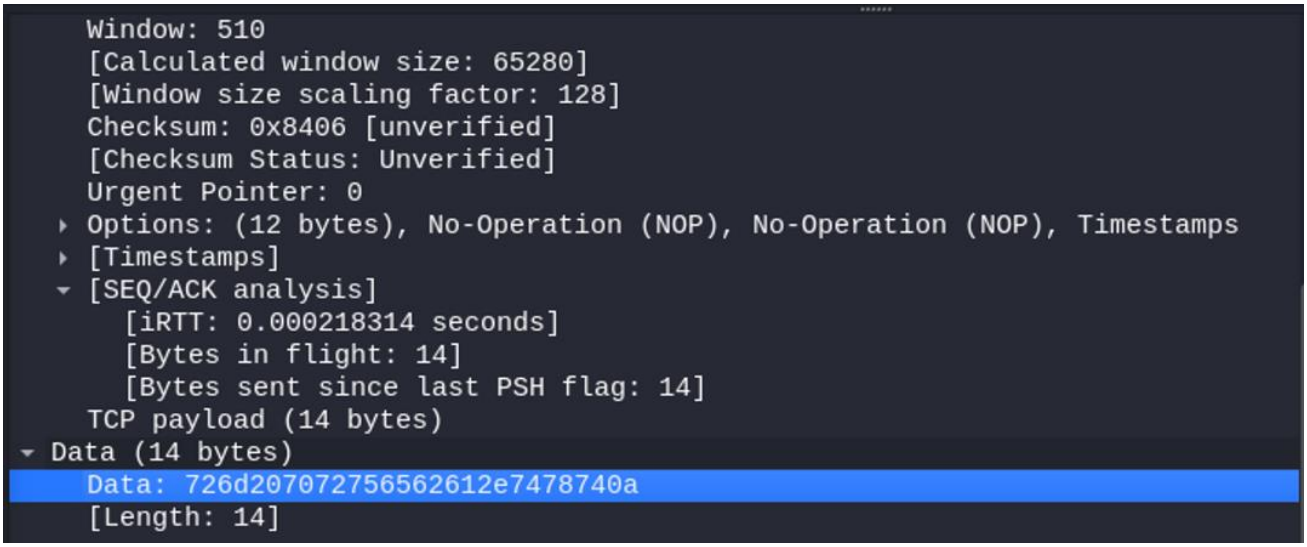
```
ls
atacante.txt
Desktop
Documents
Downloads
Music
Pictures
prueba.txt
Public
Templates
Videos
rm prueba.txt
ls
atacante.txt
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
```

Comprobación WireShark:

Siguiendo el mismo procedimiento para abrir WireShark que en los anteriores casos, filtré por el puerto 4444 y grabé todo el tráfico del puerto. Una vez que terminé de hacer todos los comandos busqué en los paquetes los comandos que ejecuté desde la máquina atacante.



No.	Time	Source	Destination	Protocol	Length
20	8.046324706	192.168.1.66	192.168.1.63	TCP	74
21	8.046361134	192.168.1.63	192.168.1.66	TCP	74
22	8.046543020	192.168.1.66	192.168.1.63	TCP	66
31	10.924142586	192.168.1.63	192.168.1.66	TCP	69
32	10.924472136	192.168.1.66	192.168.1.63	TCP	66
33	10.926596789	192.168.1.66	192.168.1.63	TCP	157
34	10.926622527	192.168.1.63	192.168.1.66	TCP	66
114	19.150313847	192.168.1.63	192.168.1.66	TCP	80
115	19.194833088	192.168.1.66	192.168.1.63	TCP	66
140	20.870382752	192.168.1.63	192.168.1.66	TCP	69
141	20.870701410	192.168.1.66	192.168.1.63	TCP	66
142	20.872726952	192.168.1.66	192.168.1.63	TCP	146
143	20.872751414	192.168.1.63	192.168.1.66	TCP	66



En uno de los paquetes en la parte de data salió un mensaje en Hexadecimal que pase Ascii en el que aparece uno de los comandos que realice.

Conclusiones

La práctica consiste en comenzar a familiarizarnos con la herramienta NetCat y WireShark en la que se incluyen varios ejercicios. En el primero, se verifica la disponibilidad de NetCat en ambas máquinas (atacante y atacada). En el segundo, se exploran las opciones y capacidades de NetCat utilizando el comando "nc -h". En el tercero, se utiliza NetCat para establecer una comunicación bidireccional en tiempo real entre la máquina atacante y la máquina atacada, demostrando cómo NetCat puede funcionar como una herramienta de chat. En el cuarto, se realiza la transferencia de archivos desde la máquina atacante a la máquina atacada, lo que muestra la capacidad de NetCat para enviar datos entre sistemas. En el quinto se usa la herramienta "Bind Shell" para ejecutar comandos remotos en la máquina atacada, y en el sexto se usa una "Reverse Shell" que invierte la dirección de la conexión, permitiendo que la máquina atacante controle la máquina atacada lo cual es una herramienta muy importante en el pentesting.