



Técnicas de elaboración de paquetes TCP y UDP utilizando HPING3

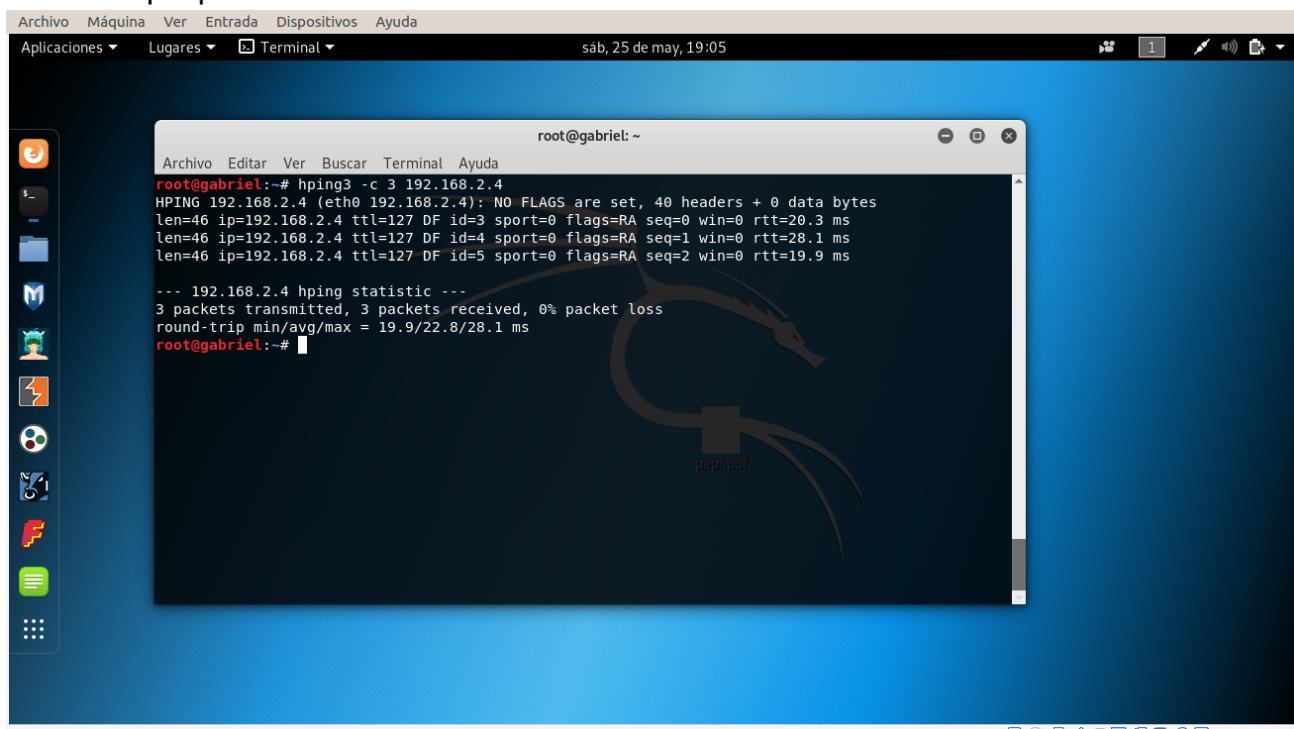
HPING3 es un programa scriptable que usa el lenguaje TCL, y los paquetes se pueden recibir y enviar a través de un binario de representación de cadenas que describe al paquete.

Objetivos del laboratorio

El objetivo de este laboratorio es ayudar a entender cómo realizar análisis de red y elaboración de paquetes utilizando los comandos de HPING3. Esta técnica fue realizada desde la máquina Kali Linux a la máquina windows_server-1.

Tareas del laboratorio

1. Abrir la consola de Kali Linux.
2. Ahora escribiremos **hping3 -c 3 <Dirección IP de la máquina objetivo>** y presionamos **Enter**. Nuestra máquina objetivo será nuestro Windows Server 2016 (192.168.2.4). -c 3 significa que solo queremos enviar tres paquetes a la máquina de destino.
3. A partir del comando anterior, la salida muestra que se recibieron y enviaron tres paquetes.

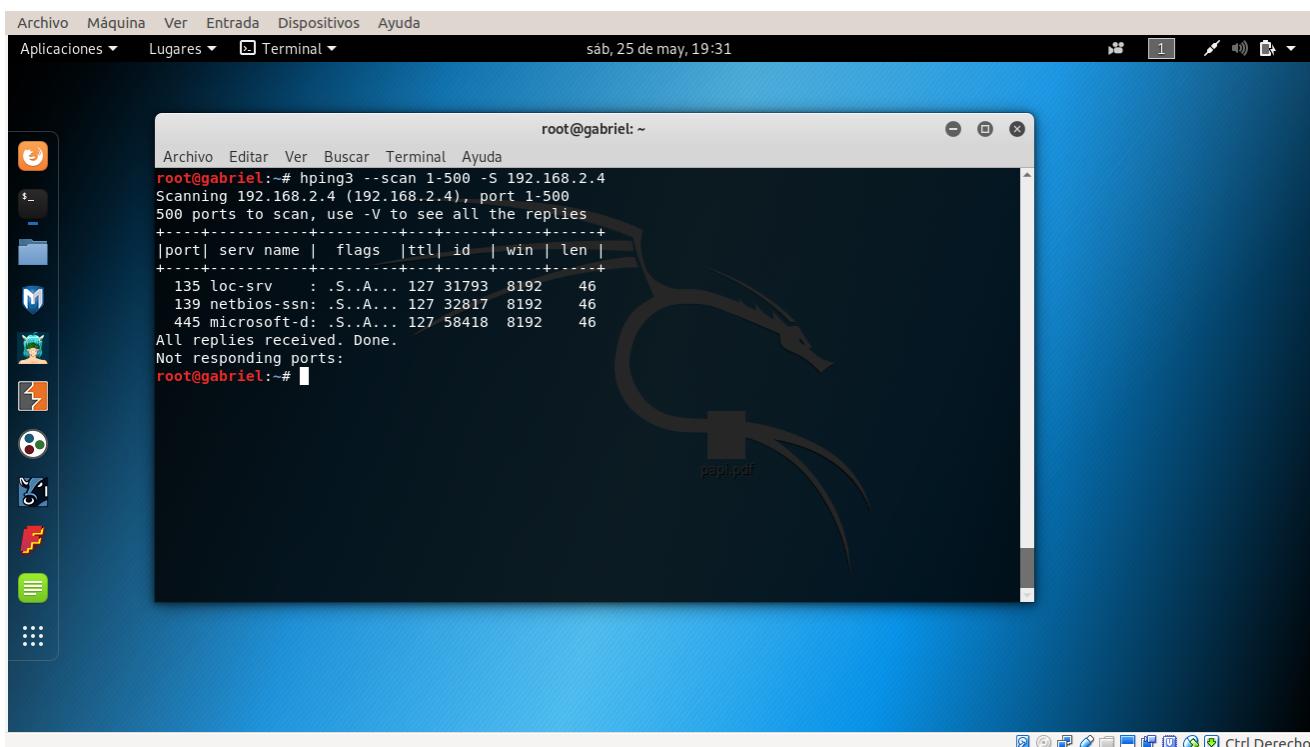


A screenshot of a Kali Linux desktop environment. The terminal window shows the command `hping3 -c 3 192.168.2.4` being run, resulting in the following output:

```
root@gabriel:~# hping3 -c 3 192.168.2.4
HPING 192.168.2.4 (eth0 192.168.2.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.2.4 ttl=127 DF id=3 sport=0 flags=RA seq=0 win=0 rtt=20.3 ms
len=46 ip=192.168.2.4 ttl=127 DF id=4 sport=0 flags=RA seq=1 win=0 rtt=28.1 ms
len=46 ip=192.168.2.4 ttl=127 DF id=5 sport=0 flags=RA seq=2 win=0 rtt=19.9 ms

--- 192.168.2.4 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 19.9/22.8/28.1 ms
root@gabriel:~#
```

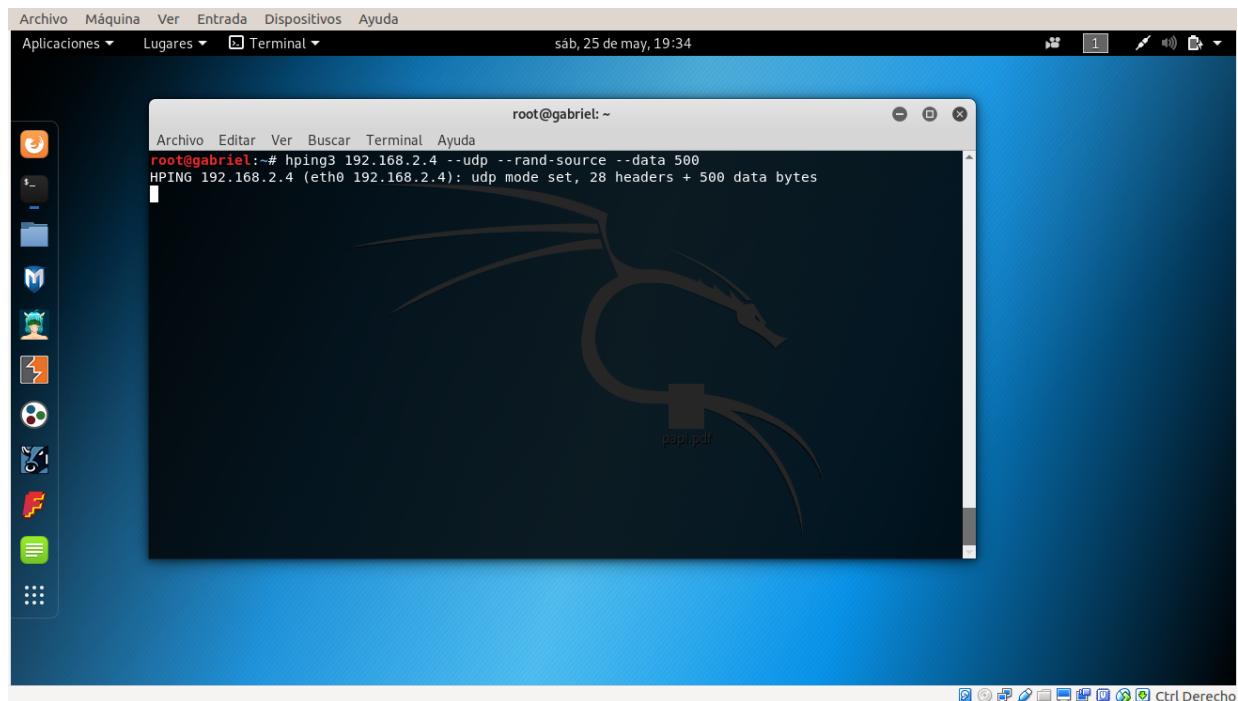
4. Vamos a escribir en la consola **hping3 -scan 1-3000 -S <dirección IP del objetivo>** y presionamos **Enter**.
5. El parámetro **-scan** define el rango de puertos a escanear en la máquina objetivo y el **-S** indica la bandera SYN.
6. La salida debe mostrar los puertos abiertos en la máquina objetivo que en este caso es Windows Server 2016.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "root@gabriel: ~". The command entered is "hping3 --scan 1-500 -S 192.168.2.4". The output shows a scan of port 1-500 on 192.168.2.4. It lists three open ports: 135 (loc-srv), 139 (netbios-ssn), and 445 (microsoft-d). The terminal window has a dark blue background with a white font. The desktop environment includes a dock at the bottom with various icons and a taskbar at the top with application icons like LibreOffice and a file manager.

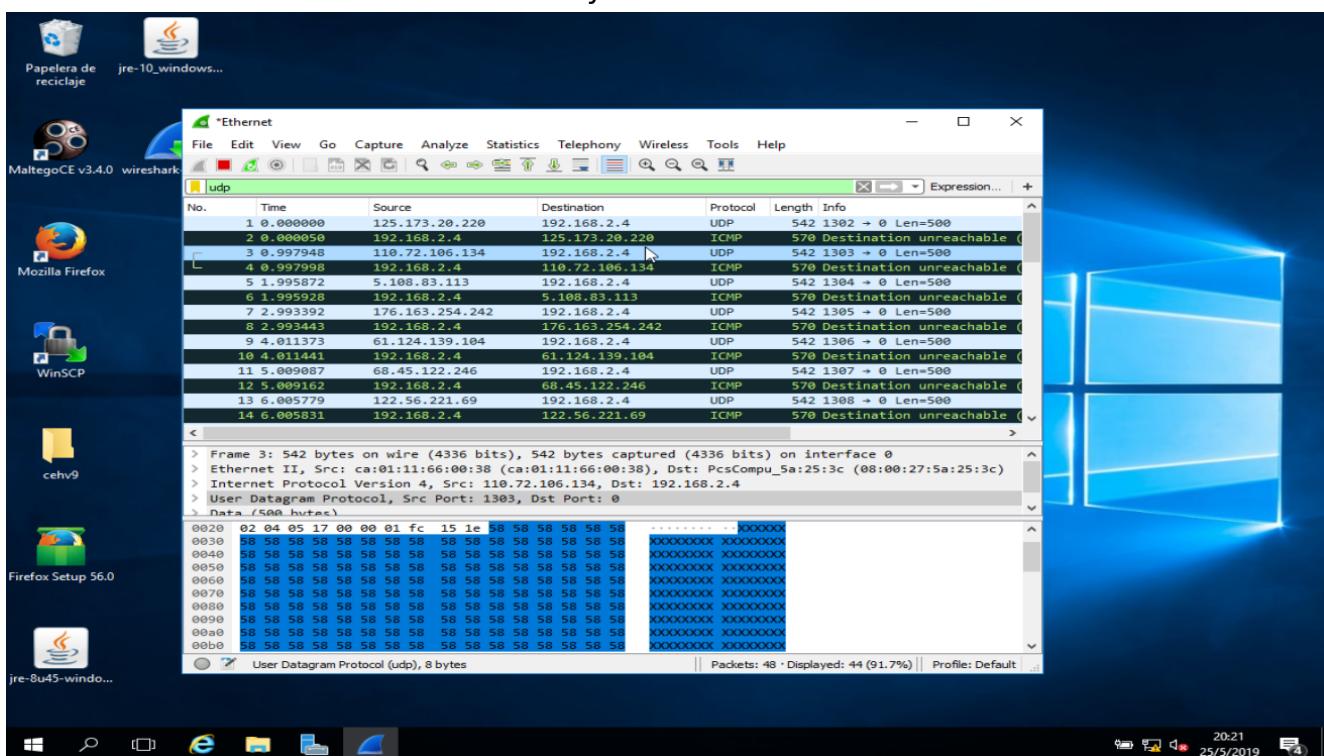
```
root@gabriel:~# hping3 --scan 1-500 -S 192.168.2.4
Scanning 192.168.2.4 (192.168.2.4), port 1-500
500 ports to scan, use -V to see all the replies
+---+-----+-----+-----+-----+
|port| serv name | flags |ttl| id | win | len |
+---+-----+-----+-----+-----+
 135 loc-srv : .S.A... 127 31793 8192 46
 139 netbios-ssn: .S.A... 127 32817 8192 46
 445 microsoft-d: .S.A... 127 58418 8192 46
All replies received. Done.
Not responding ports:
root@gabriel:~#
```

7. Ahora realizaremos la elaboración de paquetes UDP para ello escribiremos en la consola **hping3 <dirección IP del objetivo> --udp --rand-source --data 500**.
8. Aquí, la máquina de destino está ejecutando Windows Server 2016.



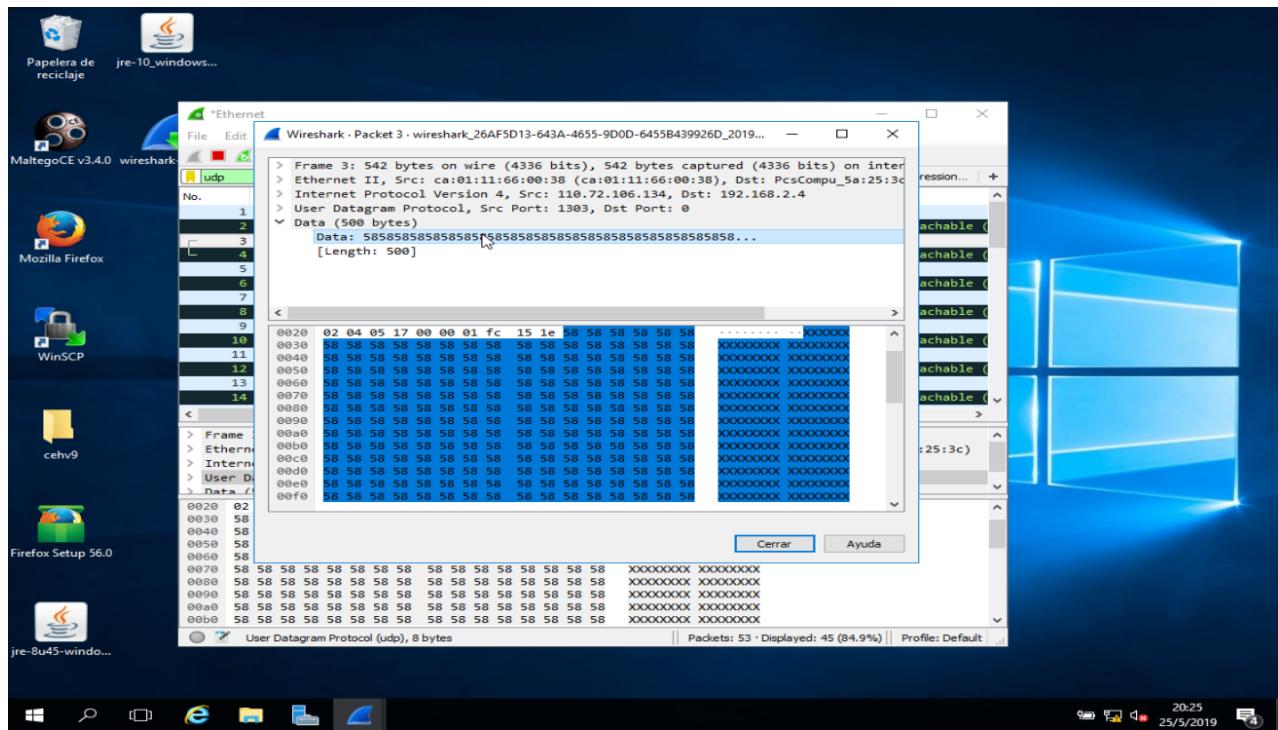
9. Entramos a esta máquina e iniciamos la captura de paquetes con **Wireshark** y observamos los paquetes UDP.

10. Damos doble clic en uno de ellos y miramos los detalles.



11. Los paquetes han sido recibidos en la maquina objetivo.

12. Cierre todas las ventanas de Wireshark. Cuando se le solicite guardar, haga clic en Salir sin guardar para cerrar Wireshark sin guardar la captura de tráfico.



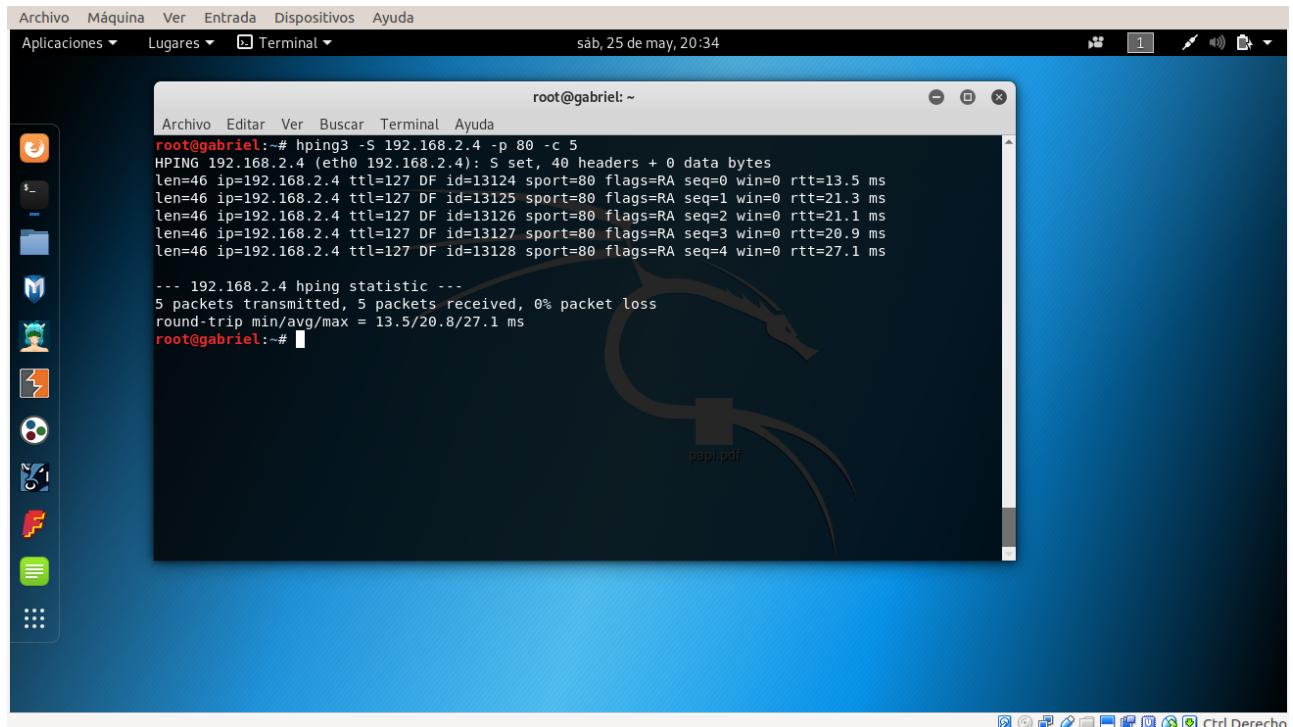
13. Antes de realizar esta tarea, inicie de nuevo Wireshark en la máquina con Windows Server 2016 (máquina de destino) y déjelo funcionando.

14. Enviaremos solicitudes TCP SYN a la maquina objetivo para ellos escribimos **hping3 -S <dirección IP de la maquina objetivo> -p 80 -c 5** y presionamos **Enter**.

15. El parámetro **-S** llevara a cabo solicitudes **TCP SYN** a la maquina objetivo, **-p** pasara traficó a través del puerto asignado y **-c** contara los paquetes enviados a la maquina objetivo.

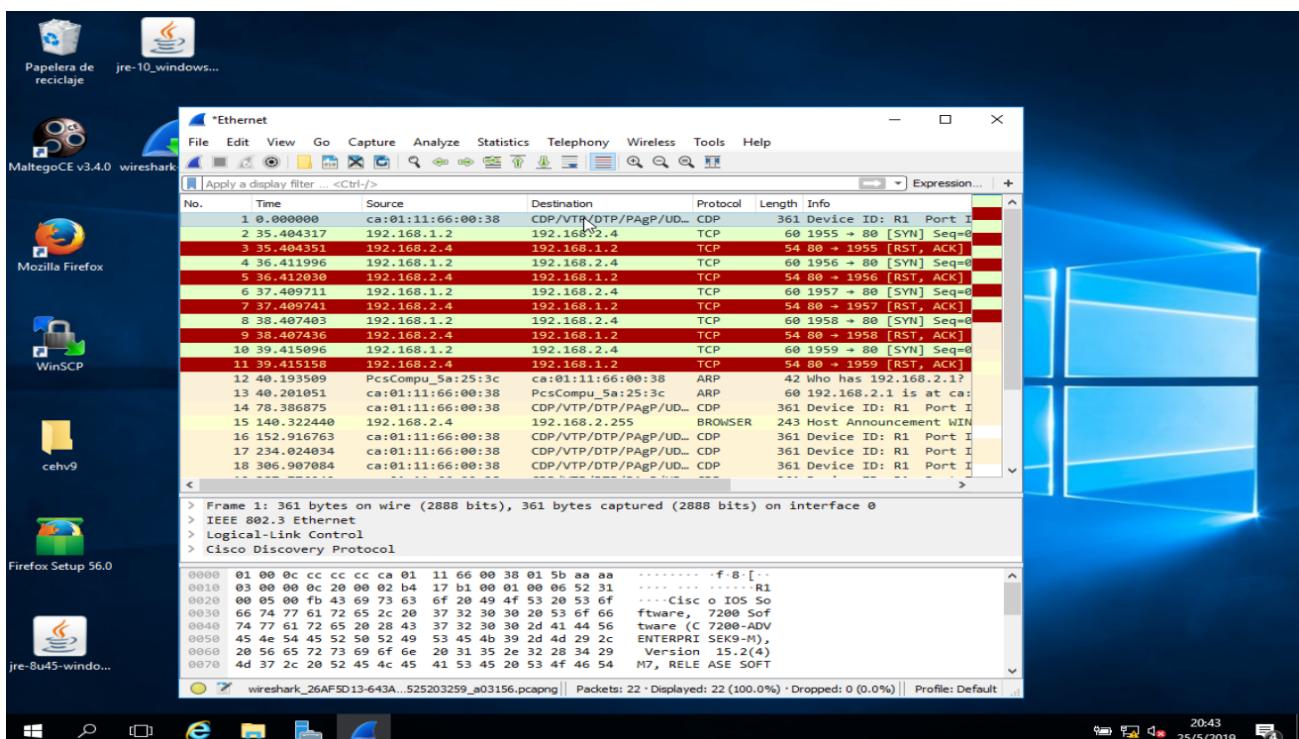
16. Aquí, la máquina de destino es Windows Server (192.168.2.4); la dirección IP puede variar en su entorno de laboratorio.

17. La siguiente captura de pantalla muestra que se enviaron cinco paquetes TCP a través del puerto 80 a la máquina de destino.



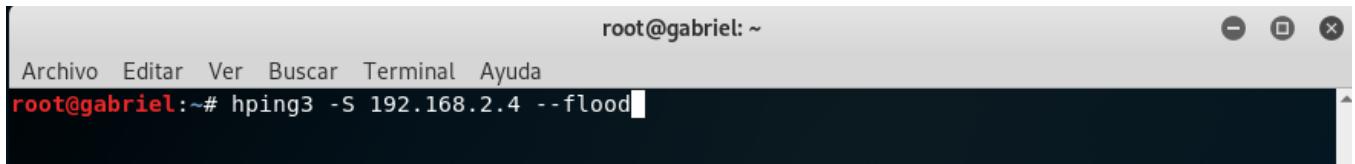
18. Ahora cambie a la máquina de destino (servidor Windows 2016) y observe los paquetes TCP capturados a través de Wireshark.

19. Iniciamos de nuevo una captura de tráfico desde la maquina objetivo.



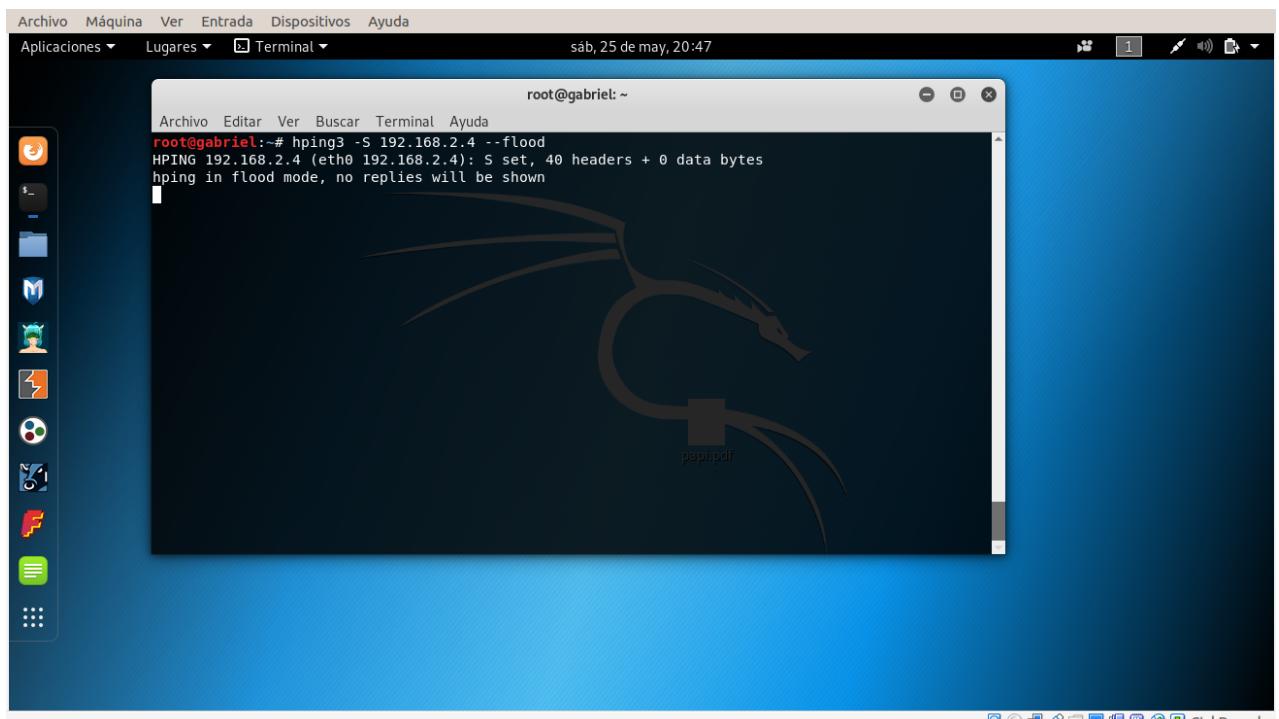
20. Cambie a la máquina de Linux Kali e intente inundar los paquetes TCP a Windows Server (máquina de destino).

21. Para realizar esto escribimos en la consola **hping3 <dirección IP del objetivo> --flood** y presionamos **Enter**.



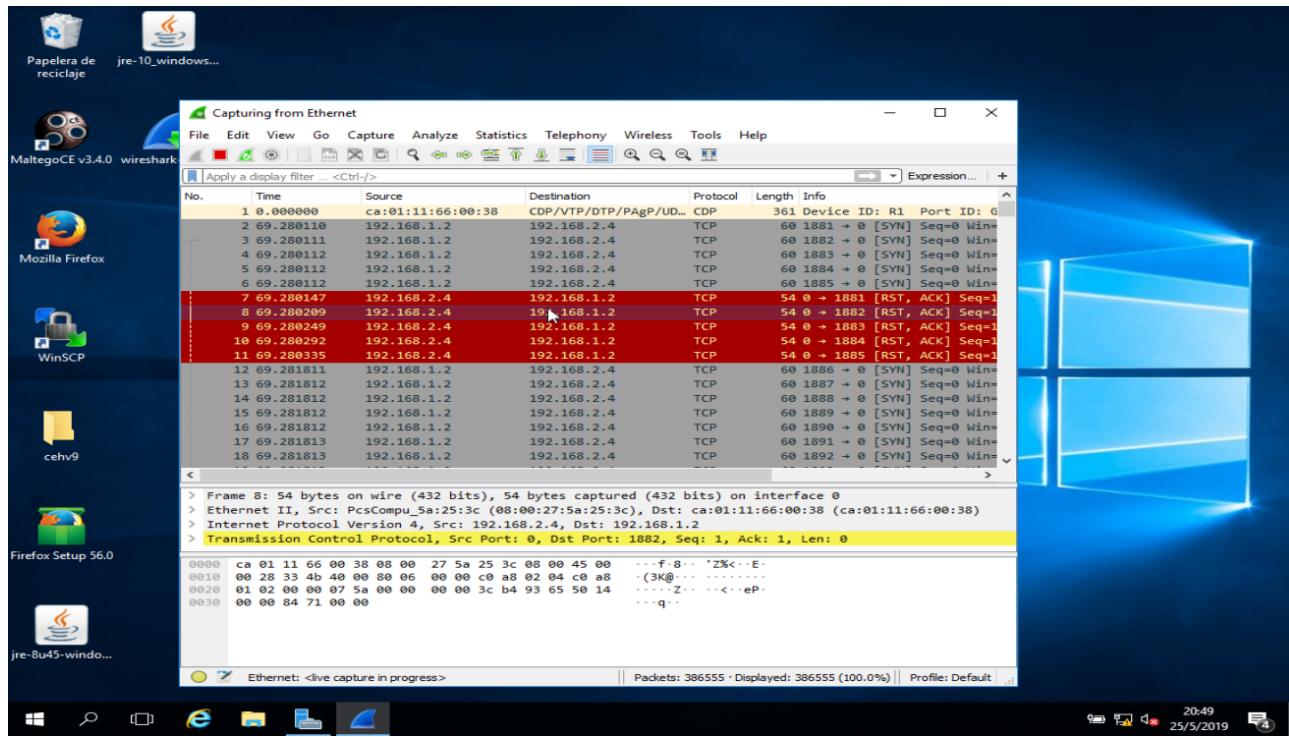
A screenshot of a terminal window titled "root@gabriel: ~". The window has a standard Linux desktop interface with a menu bar at the top. In the terminal, the command `root@gabriel:~# hping3 -S 192.168.2.4 --flood` is being typed. The terminal is running in root mode, indicated by the red text "root@gabriel". The background of the terminal window shows a faint watermark of the Kali Linux logo.

22. Una vez que se haya inundado de paquetes la maquina objetivo está responderá en la consola de Kali Linux.



23. Cambie a Windows Server (máquina de destino) y observe la ventana de Wireshark, que muestra la inundación de paquetes TCP desde la máquina atacante.

24. Damos doble clic en cualquier paquete TCP y observamos su información.



25. La secuencia de paquetes TCP muestra la información completa de los paquetes TCP transmitidos a la máquina atacante y los paquetes recibidos.

