**Desafío – Creación y Manipulación de Paquetes**

Documento de Respuestas y Evidencias

Alumno: Bladimir Alejandro Burgos Conejeros

# Punto 1 – Generación de tráfico con hping3

Se ejecutó la herramienta hping3 para generar tráfico TCP SYN hacia 127.0.0.1 en el puerto 80, modificando parámetros de TTL y dirección IP de origen.

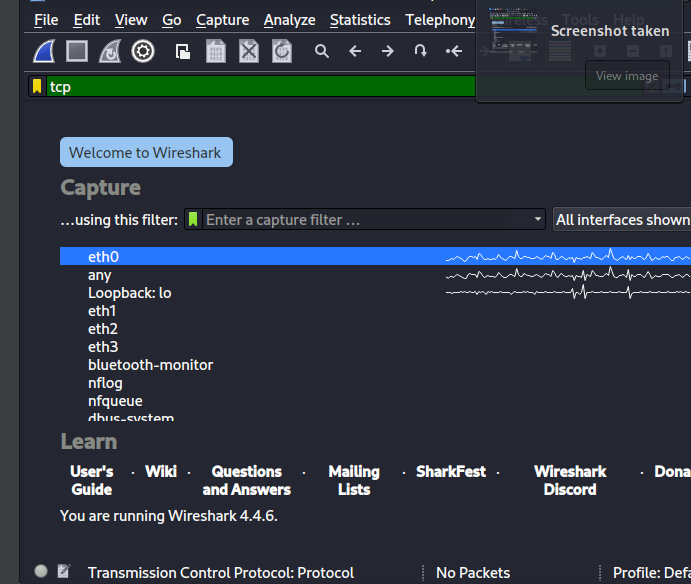
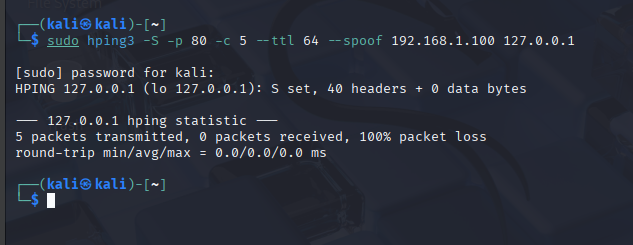
Comando utilizado:

sudo hping3 -S -p 80 -c 5 --ttl 64 --spoof 192.168.1.100 127.0.0.1

Resultados: Se transmitieron 5 paquetes TCP SYN sin recibir respuesta (100% packet loss), lo cual es normal al no existir un servicio en el puerto 80 de localhost.

Evidencias: Capturas de la terminal mostrando la ejecución de hping3 y capturas de Wireshark con filtro tcp mostrando los paquetes SYN.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

# Punto 2 – Creación de paquetes con Scapy

Se utilizó Scapy en Python para crear paquetes personalizados. Se envió un paquete ICMP con payload 'Hola Mundo' hacia 8.8.8.8 y un paquete TCP SYN con payload 'Test' hacia 127.0.0.1.

Código utilizado en Python:

from scapy.all import \*  
send(IP(dst='8.8.8.8')/ICMP()/b'Hola Mundo')  
send(IP(dst='127.0.0.1')/TCP(dport=80, flags='S')/b'Test')

Resultados: Se observaron en Wireshark los paquetes ICMP (Echo Request y Echo Reply) y los paquetes TCP SYN generados por Scapy.

Evidencias: Capturas de la consola de Python ejecutando los comandos y capturas de Wireshark mostrando los paquetes ICMP y TCP.

Texto

El contenido generado por IA puede ser incorrecto.Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.Texto

El contenido generado por IA puede ser incorrecto.

# Punto 3 – Ataque con Syn Flood

Se realizó un ataque Syn Flood con hping3 hacia 127.0.0.1 en el puerto 80, enviando una gran cantidad de paquetes SYN de forma continua para simular un ataque de denegación de servicio.

Comando utilizado:

sudo hping3 -S --flood -p 80 127.0.0.1

Resultados: En Wireshark, con el filtro 'tcp.flags.syn==1 && tcp.flags.ack==0', se observaron múltiples paquetes SYN enviados sin respuesta.

Evidencias: Captura de la terminal con el ataque en ejecución y captura de Wireshark mostrando el tráfico SYN flood.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

# Punto 4 – Mitigación con iptables

Se configuraron reglas en iptables para mitigar el ataque Syn Flood. Se estableció un límite de 1 paquete SYN por segundo y se bloqueó la IP atacante.

Comandos utilizados:

sudo iptables -A INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT  
sudo iptables -A INPUT -p tcp --syn -j DROP  
sudo iptables -A INPUT -s 127.0.0.1 -j DROP  
sudo iptables -L -v

Resultados: La salida de iptables confirmó la aplicación de reglas, mostrando el límite configurado y los paquetes descartados.

Evidencias: Capturas de la consola ejecutando los comandos y la salida de iptables -L -v.

Pantalla de computadora

El contenido generado por IA puede ser incorrecto.

# Punto 5 – Análisis del ataque y acciones correctivas

Se ejecutó un ataque Syn Flood enviando múltiples paquetes SYN al puerto 80 de 127.0.0.1. En Wireshark se evidenció el flujo de paquetes SYN masivos, característicos de este tipo de ataque.

Efectos observados: El sistema objetivo recibió los paquetes, pero no respondió con ACK. En un entorno real, este comportamiento puede saturar recursos del servidor.

Medidas aplicadas: Se utilizaron reglas en iptables para limitar el tráfico SYN y bloquear la IP atacante, mitigando efectivamente el ataque.

Vulnerabilidades identificadas: TCP es susceptible a Syn Flood, lo que puede agotar recursos del sistema si no existen defensas adecuadas.

Acciones correctivas propuestas:

1. Implementar IDS/IPS (ej. Snort, Suricata) para detección temprana.  
2. Configurar firewalls avanzados con protección DoS/DDoS.  
3. Habilitar SYN Cookies en servidores.  
4. Monitorear tráfico con SIEM (ej. Wazuh, Splunk).  
5. Segmentar la red y aplicar políticas de seguridad más estrictas.