# Laboratorio 5 Redes de Computadores

*Integrantes: Vicente Henríquez 202051507-7 | Nelson Sepúlveda 202004610-7*

## Preguntas Generales

1. Realice un diagrama de la interacción realizada en el laboratorio, incluya en el diagrama las etiquetas con las direcciones IP y puertos que conozca, agregue al diagrama tanto al servidor, router, cliente y un atacante. No es necesario incluir al atacante con su IP sino solo incluirlo para entender la interacción correspondiente

Imagen que contiene Mapa

Descripción generada automáticamente

2. ¿En qué consisten los ataques de inundación (Flooding)? Si bien en la experiencia se realizó una inundación por UDP, ¿Qué otros tipos de inundaciones pueden realizarse? ¿En qué consisten dichos tipos? ¿Qué podemos hacer para mitigar cada tipo de inundación?

Los ataques de inundación (Flooding) consisten en saturar un sistema o red enviando un alto volumen de paquetes maliciosos, agotando los recursos de estos para causar una denegación de servicio (DoS). Otros tipos de Floodins que podrían realizarse son: TCP SYN Flooding, que explota el proceso de handshake del protocolo TCP enviando solicitudes SYN sin completarlas, lo que consume recursos del servidor; el ICMP Flooding (Ping Flood), que genera un volumen masivo de paquetes ICMP (pings) para saturar ancho de banda y procesamiento; y el HTTP Flooding, que realiza numerosas solicitudes HTTP legítimas para sobrecargar servidores web. Para evitar o minimizar estos ataques se pueden habilitar reglas específicas del firewall como por ejemplo para filtrar tráfico sospechoso y sistemas de prevención de intrusos (IPS) para detectar y bloquear ataques, entre otros.

3. ¿Qué cambios realizarían para mejorar la seguridad y eficiencia de la red? ¿Realizaría o implementaría algún cambio al cliente, servidor o configuración de red para mejorar dichos aspectos? Argumente a partir de lo visto en las diferentes unidades de la asignatura

En el cliente lo ideal sería configurar un firewall robusto y solo permitir conexiones hacia el puerto del servidor necesario. En el servidor se podría limitar el número de conexiones simultáneas desde una misma IP; además se podría hacer una segmentación del tráfico del servidor utilizando VLANs. En el Router también se podrían hacer algunas acciones como habilitar protecciones para este tipo de ataques como podría ser Unicast Reverse Path Forwarding para prevenir los spoofing de IP y Rate Limiting en puertos clave para limitar la tasa de solicitudes por cliente. Por último, respecto a la configuración de red se podría implementar un sistema de detección y bloqueo de ataques en tiempo real y configurar un DNS seguro para evitar un posible DNS spoofing.

## Preguntas para atacantes

1. ¿En qué consiste la suplantación de IP? ¿Qué protocolos vistos durante la asignatura influyen o permiten este tipo de ataques? ¿Qué se puede usar para proteger los sistemas de este tipo de ataques?

La suplantación de IP consiste en falsificar la dirección IP de origen en los paquetes enviados, permitiendo al atacante ocultar su identidad o desviar las respuestas a otro sistema. Protocolos como IPv4, debido a la ausencia de mecanismos de autenticación, y ARP, por su uso en la resolución de direcciones dentro de subredes, facilitan este tipo de ataques. Para protegerse, es recomendado usar listas de control de acceso (ACL) en routers, establecer inspección de tráfico con mecanismos DPI y emplear autenticación basada en certificados. También, herramientas como detección de ARP spoofing y filtros estrictos en firewalls son clave para minimizar este riesgo​​​.

2. En el caso que el sistema a atacar estuviera dentro de una subred, ¿Qué técnicas podrían utilizarse para alcanzar los mismos resultados? ¿Qué otros tipos de vulnerabilidades o protocolos se podrían explotar en la red?

En el caso de que el sistema a atacar estuviese en una subred, una de las técnicas que se podría emplear es el ARP spoofing, el cual redirige el tráfico hacia el atacante, otro sería el escaneo de puertos para identificar servicios vulnerables y por último el DNS poisoning para manipular las resoluciones de nombres y redirigir tráfico a servidores controlados por el atacante. La falta de segmentación de red y la ausencia de políticas de seguridad como firewalls internos son vulnerabilidades que podrían estar presentes, facilitando los ataques.

## Imágenes del Laboratorio

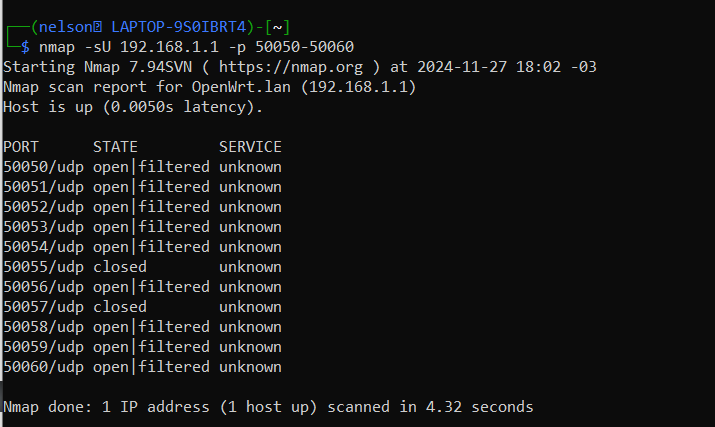


Imagen 1: nmap de puertos 50050 a 50060

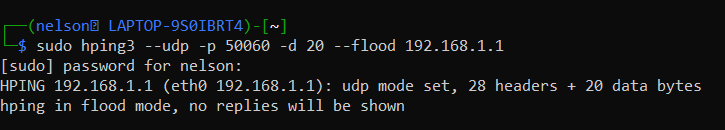


Imagen 2: hping3 a 192.168.1.11 (en imagen se ve 1.1, pero fue a 1.11)

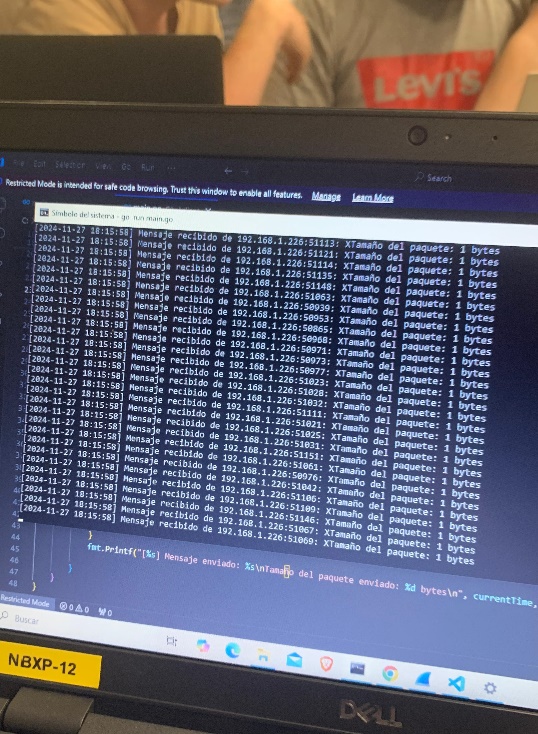


Imagen 4: Defensores siendo atacados

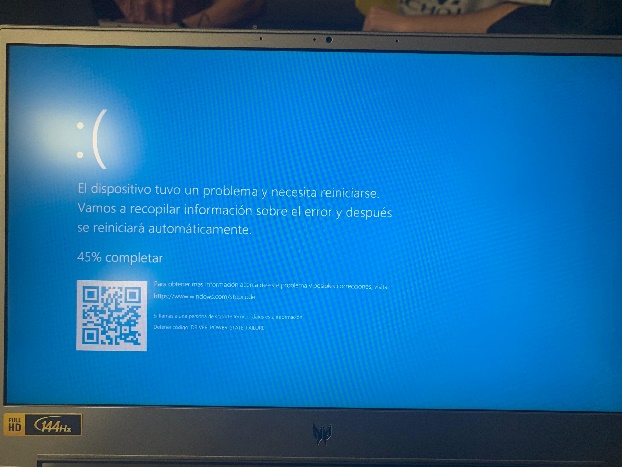


Imagen 3: Pantallazo azul (parte de la experiencia)