Laboratorio 3: Redes de Computadores

Profesor: Jorge Díaz
Ayudantes: Juan Cucurrella & Nicolás Rodríguez

Noviembre 2024

Objetivos del laboratorio

- Entender y experimentar el reenvío de puertos a través de Routers
- Entender y ejecutar ataques de denegación de servicio a través del protocolo UDP y redes Wi-Fi
- Mitigar ataques a través del uso de reglas de Firewall

Introducción

Un problema común en redes de computadores y sistemas en general son los intentos de uso malicioso o ataques a la infraestructura tecnológica, asegurar las redes correctamente y entender como configurar ciertas defensas para evitar posibles ataques es clave para implementar cualquier tipo de red o conexión en el mundo real y entornos de producción.
Algunos ataques a los que pueden estar expuestos los dispositivos y redes son los ataques de *denegación de servicios*, los cuales consisten en interrumpir el normal funcionamiento de redes, servicios o plataformas para impedir el acceso a estos a través de la saturación con solicitudes o tráfico excesivo. Una forma de asegurar sistemas contra este tipo de ataques consiste en el uso de un Firewall, el cual permite establecer reglas para filtrar el tráfico tanto desde fuera como dentro de la red, dentro de estas existen ciertas reglas especiales en el Firewall de un router para permitir a los dispositivos externos (ya sea de manera general o específica) conectarse con dispositivos en una red interna a través de los puertos del router, dicha técnica es conocida como *Reenvío de puertos* (también llamado *Port Forwarding*)

Laboratorio

Dadas las experiencias anteriores, se pondrán en práctica los diversos conceptos aprendidos en las sesiones de cátedra y laboratorio para simular un entorno cliente-servidor bajo ataques de inundación, su deber, dependiendo de su rol, es intentar atacar e interrumpir la actividad del servidor y cliente a través de inundación de red o desviar el tráfico a través de reglas de firewall para evitar la saturación e interrupción de los servicios correspondientes.

Pre-Laboratorio

A lo largo de esta experiencia se les otorgarán roles dentro del sistema, ya sea como atacante o como defensor de la infraestructura, independiente de estos roles, deben conectarse a la red del laboratorio que se les asignará al llegar a la experiencia, dependiendo de su rol se definen los siguientes requisitos previos:

Atacantes

Para la presente experiencia es necesario contar con un sistema Linux que permita el uso de las herramientas **NMap** y **Hping3**, dicho sistema puede ser nativo, a través de una máquina virtual o subsistema que permita a la máquina conectarse a la red del laboratorio. Se recomienda la instalación del subsistema de Windows para Linux (si su sistema operativo es Windows 10 u 11) con la distribución Kali Linux, el cuál permite instalar de manera más rápida las herramientas que se utilizarán. Se incluyen a continuación Links para la instalación de las diversas herramientas en distintos sistemas operativos:

1. Nmap MacOS: MacOS Nmap installation
2. Hping3 MacOS: hping3 MacOS installation
3. Instalación WSL: Microsoft Windows WSL installation

Instalación hping3 y nmap para Kali:

- Ejecutar los comandos:

  $ sudo apt-get install nmap

  $ sudo apt-get install hping3

Defensores

Para la presente experiencia es necesario contar con el lenguaje Go instalado en su sistema, de manera que puedan ejecutar los códigos proporcionados en Aula para el cliente y servidor, dichos códigos deben ser adaptados según la red, dirección IP y puerto que se les asignará al llegar al laboratorio. Utilizando el comando *ipconfig* (o *ifconfig* en Linux o Mac), deben proporcionar su dirección IP asignada por el router a los ayudantes.

Deben asegurarse de tener acceso a la interfaz del router (192.168.1.1) y configurar la regla de Port Forwarding a través del apartado "Firewall" en la interfaz correspondiente:

Una vez configurada la regla de Port Forwarding deben levantar el servidor y el cliente para realizar la interacción posterior.

Sección presencial

Atacantes

Una vez se les otorgue la autorización para el ataque, deben conectarse a alguna de las redes WiFi proporcionadas para el laboratorio y escanear la red para encontrar los puertos abiertos o filtrados del router, para esto, se utilizará la herramienta Nmap.

1) Dentro de su sistema, abra una terminal y ejecute el comando:

- $ nmap -h

Dicho comando le permitirá visualizar las opciones que recibe la herramienta y los tipos de escaneos que puede realizar:

2) Ejecute un escaneo de tipo UDP a los puertos 50050 a 50060 sobre el router principal y tome una fotografía a los resultados correspondientes, entre estos resultados deben encontrar los puertos abiertos y/o filtrados, interprete los resultados.

3) A partir de la información encontrada, ejecute la herramienta hping3 a partir del siguiente comando:

- $ hping3 -h

A partir de este comando se visualizan las opciones posibles de la herramienta:

4) Ejecute un ataque de inundación al router en alguno de los puertos expuestos y encontrados eligiendo algún tamaño de paquete arbitrario (se recomienda que no sean de tamaño mayor a 50), utilizando el siguiente comando:

1. $ hping3 −− udp -p [port] -d [tamaño] –flood [IP objetivo]

Ejecute el ataque hasta que se le dé alguna señal de parte de los ayudantes para finalizar, tome fotografía a la terminal.

5) Dado que los pares defensores filtrarán su tráfico, intente suplantar al cliente utilizando la herramienta Hping3 y ejecute el ataque nuevamente, tome fotografía a la terminal. *Hint: usar la flag spoof mostrada por la ayuda de la herramienta.*

Defensores

1) Ejecute el servidor en un equipo y el cliente en otro equipo diferente, conecte el cliente apuntando a la IP del router y al puerto correspondiente al puerto de reenvío previamente configurado

2) Envíe mensajes de cliente al servidor de manera constante, los mensajes enviados serán reflejados en la terminal donde se ejecuta el servidor, tome una fotografía de la ejecución del cliente y la llegada de mensajes al servidor

3) Una vez se otorgue la señal, comenzará a recibir ataques de parte de los atacantes, los paquetes del ataque se verán reflejados en los mensajes del servidor, tome una fotografía o grabe un video de la interacción. *Nota: puede apoyarse a través del uso de WireShark para visualizar el ataque en ejecución, siendo esto totalmente opcional para esta experiencia*

4) Configure el reenvío de puertos previamente configurado para su servidor para aceptar tráfico únicamente desde la IP de su cliente, tome una fotografía a la nueva configuración del reenvío de puertos.
5) Verifique si la interacción con el servidor se normaliza o cambia, tome una fotografía a los mensajes recibidos de parte del cliente.

Post-Laboratorio: Informe

Una vez terminado el laboratorio, cuentan con aproximadamente 4 días para responder las siguientes preguntas generales y correspondientes a su rol en un informe de experiencia, debe adjuntar las imágenes tomadas durante la experiencia.

Preguntas Generales

Independiente de su rol, responda las siguientes preguntas:

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*

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?

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

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?

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?

Preguntas para defensores

1. ¿En qué consiste y qué funciones cumple el reenvío de puertos? ¿Para que suele ocuparse? Apoye sus ideas planteando y explicando un escenario diferente al visto en la experiencia de laboratorio

2. ¿Qué tipos de reglas de firewall pueden configurarse (aparte de Port Forwarding) para proteger las redes ante ataques de inundación? ¿Qué otros enfoques y/o herramientas se pueden utilizar para prevenir, evitar, mitigar o resolver este tipo de incidentes?

Consideraciones

- Se proporcionarán códigos base para realizar la experiencia, con el objetivo que puedan configurar las partes orientadas a la experiencia.
- Solo una persona del grupo debe entregar los archivos correspondientes
- **Todo lo aprendido en esta experiencia tiene un objetivo meramente educativo, ninguna técnica ofensiva aprendida en este laboratorio debe aplicarse sin debida y explícita autorización, la disrupción de comunicaciones de manera no autorizada es considerada un delito**

Reglas

- El laboratorio se realiza en parejas seleccionadas en Aula.
- **La actividad en la red será monitoreada y registrada**, por lo cual se recomienda no ejecutar actividades potencialmente maliciosas o dañinas para la infraestructura del laboratorio y/o equipos de compañeros a menos que exista una autorización previa y explícita (Ataques de denegación de servicios, intentos de acceso no autorizados, escalada de privilegios, instalación de malware, entre otros), en caso de detectar actividad maliciosa, será notificada debidamente al profesor y se evaluará el laboratorio con nota 0, además de seguir las medidas pertinentes acorde al reglamento de la universidad.
- La fecha de entrega es el día **Sábado 30 de Noviembre** a las 23:59 hrs para los grupos del día martes y el día **Domingo 1 de Diciembre** para los grupos asignados al día miércoles.
- Toda la parte de código debe ser realizado en Go.
- La entrega la debe realizar un solo estudiante a través de Aula, en un archivo comprimido .zip, indicando el número de Laboratorio y grupo en el siguiente formato: L2-Grupo[Nº Grupo].zip, Ejemplo: L2-Grupo01.zip.
- Cada hora de retraso penalizará el laboratorio, descontando 30 ptos.
- Cualquier sospecha de copia será notificada debidamente al profesor y evaluada con nota 0. Siendo tomado en cuenta también cualquier copia directa de algún sitio web o foro. Se tendrá un software a mano para realizar dichas comparaciones.

- No respetar el formato de entrega o indicaciones del laboratorio aplica descuento a la nota de la presente experiencia
- En caso de emergencias o situaciones específicas que pongan en riesgo la correcta realización del laboratorio (cortes de luz, desconfiguración de la infraestructura del laboratorio, entre otros) se informarán medidas y resoluciones a través del panel de avisos de laboratorio en la plataforma aula luego de realizar los análisis correspondientes.
- Debe entregar todos los archivos fuente necesarios para la correcta ejecución de la entrega. Teniendo al menos un archivo para el cliente y un archivo para el servidor en carpetas diferentes. Con el código bien identado, comentado, sin warnings ni errores.
- Debe entregar un README con nombre y rol de cada integrante del grupo, además de las instrucciones necesarias para ejecutar correctamente el laboratorio. (ADVERTENCIA: Si no se entrega dicha información, se colocará un cero a la entrega y posteriormente se tendrá que coordinar una sesión de apelación.)