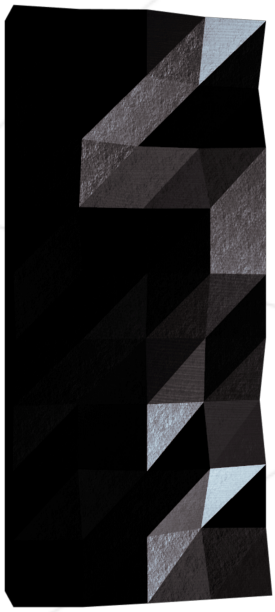

Bootcamp Ciberseguridad | 42 Madrid

Inquisitor

Resumen: Envenenamiento de la tabla ARP.

Versión: 1

Índice general

Capítulo I

Prólogo

Una víctima de envenenamiento ARP.

Capítulo II

Introducción

`Inquisitor`

El llamado, *modelo OSI* es la arquitectura que siguen las redes informáticas de todo el planeta. Consta de 7 capas, cada una de las cuales entraña riesgos y está expuesta a diferentes tipos de vulnerabilidades y formas de explotación.

En el nivel de red, hay elementos encargados de decidir hacia dónde direccionar el tráfico. Toda red local cuenta con una puerta de enlace predeterminada, que recibe el tráfico exterior y lo distribuye entre sus nodos. Esta puerta de enlace es la que se conoce como *gateway* o *router*.

Si un nodo de la red se hace pasar por dicha puerta, puede tomar el control del tráfico, interceptarlo y decidir a quién reenviarlo, además de poder modificarlo o bloquearlo.

La suplantación de ARP también se puede utilizar de manera legítima, por ejemplo, para redirigir las nuevas conexiones a una página de registro antes de usar una red, como es común en las redes abiertas de aeropuertos, cafeterías y otros sitios públicos.

Capítulo III

Parte Obligatoria

III.1. Inquisitor

Dado que para trabajar con *raw sockets* es necesario contar con permisos de bajo nivel, en este proyecto trabajaras dentro de un contendor o máquina virtual.

En caso de usar una máquina virtual, en el repositorio de entrega solo incluirás un archivo `signature.txt` con la suma de verificación del .vdi de tu máquina. Durante la corrección, se compararán la firma del repositorio con la firma real de tu máquina, y si no coinciden, tu nota será un 0.

En caso de trabajar con uno o varios contenedores, además del código de tu programa incluirás los Dockerfile o docker-compose.yaml así como un script de Bash llamado `start.sh` que inicie todo el entorno sin intervención del usuario.

Crearás un programa llamado `inquisitor` con las siguientes características:

- Recibirá cuatro parámetros: <IP-src><MAC-src><IP-target><MAC-target>
- Será capaz de realizar el envenenamiento ARP en ambos sentidos (full duplex)
- A la hora de detener el ataque (CTRL+C), se restaurarán las tablas ARP.
- Solo operará con direcciones IPv4.
- El programa será capaz de interceptar el tráfico resultante del inicio de sesión en un servidor FTP.
- Se visualizará en tiempo real el los nombres de los archivos intercambiados entre el cliente y el servidor FTP.
- El programa jamás se detendrá de forma inesperada y gestionará todos los errores de input.

Utilizarás la librería `libpcap` para capturar los paquetes. Por lo tanto, puedes utilizar cualquier lenguaje de programación que la implemente (C, C++, Python...).

Capítulo IV

Parte Bonus

La evaluación de los bonus se hará `SI Y SOLO SI` la parte obligatoria es `PERFECTA`. De lo contrario, los bonus serán totalmente `IGNORADOS`.

Puedes mejorar tu proyecto con las siguientes características:

- Modo "verbose"(-v) que muestre todo el tráfico FTP y no solo los nombres de archivo.

Capítulo V

Evaluación por pares

Este proyecto será corregido por tus compañeros. Entrega los archivos en el repositorio Git y asegúrate de que todo funciona como se espera.