PRÁCTICA 7: Seguridad Perimetral

Seguridad en la Información

Lenguajes y Ciencias de la Computación.
ETSI Informática, Universidad de Málaga

EJERCICIO 1: Análisis de la configuración de un cortafuegos

En el Campus Virtual tienes un script dentro de `Configuración IPtables` que se utiliza para la configuración del cortafuegos un determinado equipo que cuenta con tres interfaces de red

- eth0: 192.168.1.2 (a Internet)
- eth1: 192.168.10.1
- eth2: 192.168.3.1

En el script encontrarás 7 líneas que empiezan con el símbolo '#', que sirven para escribir comentarios. Debes **indicar de manera clara y concisa** para qué sirven los comandos que aparecen a continuación de cada comentario.

Además, debes responder a las siguientes preguntas argumentando tus respuestas indicando claramente los comandos del script relacionados:

1. ¿Qué servicios pueden ser accedidos desde Internet?
2. ¿Existe una zona desmilitarizada (DMZ) en la red?
3. ¿Los hosts de la red 192.168.10.0/24 pueden acceder a Internet?
4. ¿Pueden los hosts de la red 192.168.10.0/24 recibir conexiones desde Internet?
5. ¿Pueden los hosts de la red 192.168.10.0/24 recibir conexiones desde la red 192.168.3.0/24?

EJERCICIO 2: Bloqueo de servicios con IPtables

Monta algún servidor en la máquina virtual Linux (p.ej., FTP, telnet/nc , HTTP, …), para ello puedes basarte en alguna de las prácticas realizadas anteriormente donde montábamos diferentes servicios con el propósito de atacar o simplemente para analizar las comunicaciones.

Una vez lanzado el servicio, comprueba con la herramienta `netstat` o con `nmap` que el puerto asociado al servicio está a la escucha y, por tanto, puedes tratar de establecer una conexión. A continuación, utiliza el comando `iptables` para comprobar la configuración del cortafuegos del sistema.

Si la configuración del cortafuegos lo permite (política por defecto y reglas) establece una conexión con el servicio que acabas de lanzar. Cambia la configuración para que la política por defecto sea denegar todo el tráfico entrante y añade reglas que permitan las conexiones desde equipos que se encuentren en la misma red de área local.

Una vez comprobado que el servicio está accesible, utiliza la herramienta `hping` (disponible en Kali Linux) para lanzar un ataque SYN flood al servicio que acabas

de montar. Utiliza la herramienta `iptables` para bloquear los intentos de conexión a tu servicio desde la dirección IP y puerto que te está atacando. De manera que puedas seguir accediendo al servicio desde otros puertos.

Busca la forma de evadir la regla que acabas de montar en el cortafuegos con `hping`. Para ello, busca en la documentación qué posibilidades te ofrece esta herramienta.

EJERCICIO 3: Detección de intrusiones

En este ejercicio vamos a instalar y configurar Snort para detectar potenciales ataques que se realicen contra nuestro equipo, como un escaneo de puertos utilizando `nmap`.

NOTA: Este ejercicio se realizará con la máquina virtual CIA_ubuntu22.04 disponible en el equipo del laboratorio
RECORDATORIO: Sólo debe utilizarse nmap con el equipo localhost

Una vez instalado, Snort viene pre-configurado con una serie de reglas (/etc/snort/rules). Abre este directorio y observa alguno de los ficheros que hay disponibles. Además, Snort también nos permite crear nuestras propias reglas de monitorización. Para indicar a Snort que haga uso de nuestras reglas, debemos indicárselo a través del fichero de configuración por defecto (/etc/snort/snort.conf). Echa un vistazo a este fichero.

Por defecto, Snort ya nos permite detectar ataques de escaneo de puertos contra nuestro equipo. Por lo tanto, los pasos para realizar el ejercicio es el siguiente:

Instalar tanto Snort como `nmap` en la máquina virtual Ubuntu.

- Lanzar Snort sacando información a través de la consola (opción -a PARAM1) usando el interfaz "loopback" (localhost) del equipo (-i PARAM2) y proporcionando el fichero de configuración por defecto (-c PARAM3)
    - PARAM1 se obtiene a través de la documentación oficial (URL)
    - PARAM2 se obtiene ejecutando el comando ip address en consola, y extrayendo el nombre del interfaz "LOOPBACK".
    - PARAM3 es el nombre del fichero de configuración por defecto, mencionado en este enunciado.
- Lanzar un ataque de análisis de puertos contra el equipo, usando el comando `nmap` de la práctica 6.
    - La inmensa mayoría de las alertas que vemos por consola no son alertas relacionadas con nmap, sino alertas relacionadas con tráfico cuyo origen y destino es local. Encuentra el fichero de configuración de estas reglas ("bad traffic" dentro de /etc/snort/rules) y coméntalas usando el carácter "#". Posteriormente, reinicia Snort (usando `ps -a` y `kill -9`) y vuelve a ejecutar `nmap`.

INFORMACIÓN COMPLEMENTARIA

HPING/NPING

La herramienta hping [1] permite la composición y envío de diferentes tipos de paquetes (ICMP, TCP, UDP, IP) para comprobar la seguridad de un sistema en red. Entre otros usos, sirve para detectar posibles agujeros de seguridad en firewalls o su capacidad para resistir ataque de denegación de servicio.

Hping está desarrollada para ser utilizada en sistemas basados en Unix. En la mayoría de sistemas Linux puede instalarse desde un gestor de paquetes como aptitude.

Una alternativa a hping es nping [2]. Desarrollada por Nmap Project y más moderna, aunque similar.

SNORT

Para instalar Snort [3] utilizando la herramienta `apt` en algunos sistemas Linux puede ser necesario editar el fichero de fuentes apt y añadir la URL desde dónde descargar Snort. No obstante, en Ubuntu no deberías tener problema para instalarlo sin necesidad de tocar los fuentes – aunque la versión instalada será Snort 2.X.

Durante la instalación de Snort, se preguntará cual es la red local. Ésta puede obtenerse mediante el comando `ip address`.

Referencias:

[1] https://linux.die.net/man/8/hping3
[2] https://nmap.org/nping/
[3] https://www.snort.org/