| DATOS DE LA ACTIVIDAD | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| No. de Actividad: | **1.10** | **Actividad** | Actividad 1.10 Amenazas de Seguridad y Tabla Comandos Seguridad | | | | |
| Unidad: | Unidad 1: Riesgos de seguridad informática en infraestructura de red | | | | | | |
| Carrera: | Tgo. en Desarrollo de Software | | | | | | |
| Materia | **Seguridad en Infraestructura de tecnologías de información** | | | | | Clave | **18MPEDS0835** |
| Profesor: | Andrés Figueroa Flores | | | | | | |
| Alumno: | Gabriel Esqueda Guzmán | | | | | Registro: | 19100076 |
| Institución: | **Centro de Enseñanza Técnica Industrial plantel Colomos** | | | | | | |
| Semestre: | 8 | Grupo: | B1 | Período: | Ago-Dic 2022 | Fecha: | 11/09/2022 |
| Compet. Genéricas | | 4.1, 4.5, 5.2, 5.5 | | Compet.. Profesional | | 12 | |

**1. Objetivo(s) de la actividad**

* Identificar los diferentes tipos de malware en el ámbito de seguridad informática.

**2. Instrucciones (Descripción) de la actividad**

1. Investiga y realiza un listado sobre las 3 metodologías de ataques: acceso, reconocimiento, denegación de servicio, clasificando los principales ataques y la descripción breve de cada uno.

Ataques de acceso

Los ataques de acceso explotan vulnerabilidades conocidas en los servicios de autenticación, servicios FTP y servicios web para obtener acceso a cuentas web, bases de datos confidenciales y otra información confidencial. Un ataque de acceso permite a las personas obtener acceso no autorizado a información que no tienen derecho a ver. Sus tipos de ataques son:

Ataques de contraseña

Los actores de amenazas pueden implementar ataques de contraseña utilizando varios métodos diferentes:

Ataques de fuerza bruta: Consiste en descifrar un nombre de usuario, contraseña o página web oculta a través de prueba y error.

Ataques de caballos de Troya: Este método permite que los atacantes oculten una carga dentro de un archivo o software, que al ser activada consiga las credenciales del usuario

Sniffers de paquetes: Permite capturar los paquetes de una red, que en este caso podrían contener información sensible y útil para el atacante.

Explotación de confianza

En un ataque de explotación de confianza, un actor de amenazas utiliza privilegios no autorizados para obtener acceso a un sistema, posiblemente comprometiendo el objetivo.

Redirección de puerto

En un ataque de redirección de puerto, un actor de amenaza utiliza un sistema comprometido como base para ataques contra otros objetivos.

Ataques de reconocimiento

Los ataques de reconocimiento se utilizan para realizar la detección y el análisis no autorizado de sistemas, servicios o vulnerabilidades. Por su naturaleza, estos ataques preceden a otros como los de acceso o los de denegación de servicio.

Consultas de internet

El actor de la amenaza está buscando información inicial sobre un objetivo. Se pueden usar varias herramientas, incluida la búsqueda de Google, los sitios web de organizaciones, whois y más.

Barrido de ping

Sencillamente esta parte del ataque consiste en saber qué direcciones IP están activadas para poder atacar posteriormente.

Escaneos de puertos

Similar al barrido de ping, sin embargo en este paso se revisan los puertos de las direcciones IP activas (encontradas previamente) para recabar información de ellas.

Denegación de servicio

Tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado. Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática. Esto puede suceder debido a que los servidores en la web tienen una capacidad limitada para recibir y procesar peticiones de los clientes, por lo que si se alcanza el número máximo el servidor puede ralentizarse y fallar.

DoS

Los ataques DoS son un riesgo importante porque interrumpen la comunicación y causan una pérdida significativa de tiempo y dinero. Estos ataques son relativamente simples de realizar, incluso por un actor de amenazas no calificado. Algo a destacar es que este ataque se realiza desde una sola fuente.

DDoS

Un DDoS es similar a un ataque DoS, pero se origina en múltiples fuentes coordinadas. Esto se logra mediante algo conocido como una botnet, que es una red de computadoras infectadas (llamadas zombies) por un software malicioso que el atacante utiliza para mandar peticiones coordinadas (Para esto se utiliza un programa de comando y control) a un servidor.

2. Retomar la información de comandos usados en la Actividad 1.4, hacer una tabla con dos columnas para identificar y describir el uso de los principales comandos de seguridad aplicados a un router CISCO en una red, (agregando los nuevos comandos usados).

| **Sintaxis** | **Descripción** |
| --- | --- |
| R1(config)#username [nombre] secret [password] | Permite configurar el username y password de un router |
| R1(config)# aaa new-model | Permite habilitar AAA en el router |
| R1(config)# aaa authentication login default local | Permite configurar AAA para que use la base de datos local para el login |
| R1(config)# line console 0 | Permite ingresar al modo de configuración de línea de la consola |
| R1(config-line)# login authentication default | Configura el inicio de sesión de la linea de la consola a usar el método default |
| R1(config)# ip domain-name [name] | Permite especificar el nombre de dominio del dispositivo. |
| R1(config)# aaa authentication login SSH-LOGIN local | O a lo mejor no s quiere llamar la atención |
| R1(config)# line vty 0 4 | Permite ingresar al modo de configuración de la líneas de terminal virtual del router. |
| R1(config-line)# transport input [protocolo] | Configura los protocolos aceptados para ser usados en la linea |
| ssh –l Admin1 192.168.1.1 | Acceder mediante telnet a un dispositivo. Se tiene que proveer una ip |
| R2(config)# tacacs-server key password | Configura el router para indicarle que contraseña tiene el servidor tacacs que va a usar. Se tiene que proveer una password. |
| R2(config)# tacacs-server host [ip] | Configura el router para indicarle que servidor tacacs va a usar |
| show running-config | Nos permite ver la configuración actual del router |
| configure terminal | Permite entrar al modo global para establecer y cambiar configuraciones del dispositivo |
| hostname name | Permite cambiar el nombre de host de un dispositivo. Name es un parametro |
| enable | Permite entrar al modo exec. Después de esto puede pedir credenciales de acceso |
| interface name\_interface | Permite entrar a la configuración de interfaz indicada |
| copy running-config startup-config | Permite guardar la configuración actual, reemplazando la configuración de startup previa |
| shutdown | Permite apagar la interfaz. Se usa en la configuración de interfaz |
| no shutdown | Permite encender la interfaz. Se usa en la configuración de interfaz |
| ping ip\_direction | Permite mandar paquetes a una dirección ip para verificar la conectividad. |
| enable secret password | Permite establecer una contraseña de acceso al modo exec. password es la contraseña que se establecerá. Se usa en el modo config. |
| ip route | Este comando define una ruta estática para una red de destino específica |

**Reflexión:** (personal, 3 a 4 renglones)

Gabriel Esqueda Guzmán

Considero que conocer de manera detallada los procesos y las diferentes formas de un ataque es importante. Tras realizar la investigación puedo entender que los ataques más importantes y dañinos son los de acceso, pues estos son el punto de origen muchas veces para otros ataques. Por lo que es necesario tener más cuidado con descargar cosas que puedan ser troyanos, y tener contraseñas de una seguridad aceptable.

**Referencias:**

*¿Qué son los ataques DoS y DDoS?* (s/f). Osi.es. Recuperado el 11 de septiembre de 2022, de https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

Walton, A. (2020a, abril 4). *Tipos de Ataques de Red*. CCNA desde Cero. https://ccnadesdecero.es/ataques-de-redes/

Walton, A. (2020b, septiembre 1). *Ataques de Red Habituales*. CCNA desde Cero. https://ccnadesdecero.es/ataques-red-comunes/