|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DATOS DE LA ACTIVIDAD | | | | | | | |
| No. de Actividad: | **1.10** | **Investigación** | Cuadro Sinóptico 1: 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 ITI** | | | | | Clave | **MPF3608DSO** |
| Profesor: | Andrés Figueroa Flores | | | | | | |
| Alumno: | David Alejandro López Torres | | | | | Registro: | 17300155 |
| Institución: | **Centro de Enseñanza Técnica Industrial plantel Colomos** | | | | | | |
| Semestre: | 8 | Grupo: | D1 | Período: | Feb-Jun 2021 | Fecha: | 12/03/2021 |
| Compet. Genéricas | | 4.1, 4.5, 5.2, 5.5 | | Competencia Profesional | | CP1-1 | |

**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. Realizar un diagrama o cuadro sinóptico sobre las 3 metodologías de ataques: acceso, reconocimiento, denegación de servicio, clasificando los principales ataques y la descripción breve de cada uno (Puedes usar herramientas como Lucidchart para desarrollar tu diagrama).

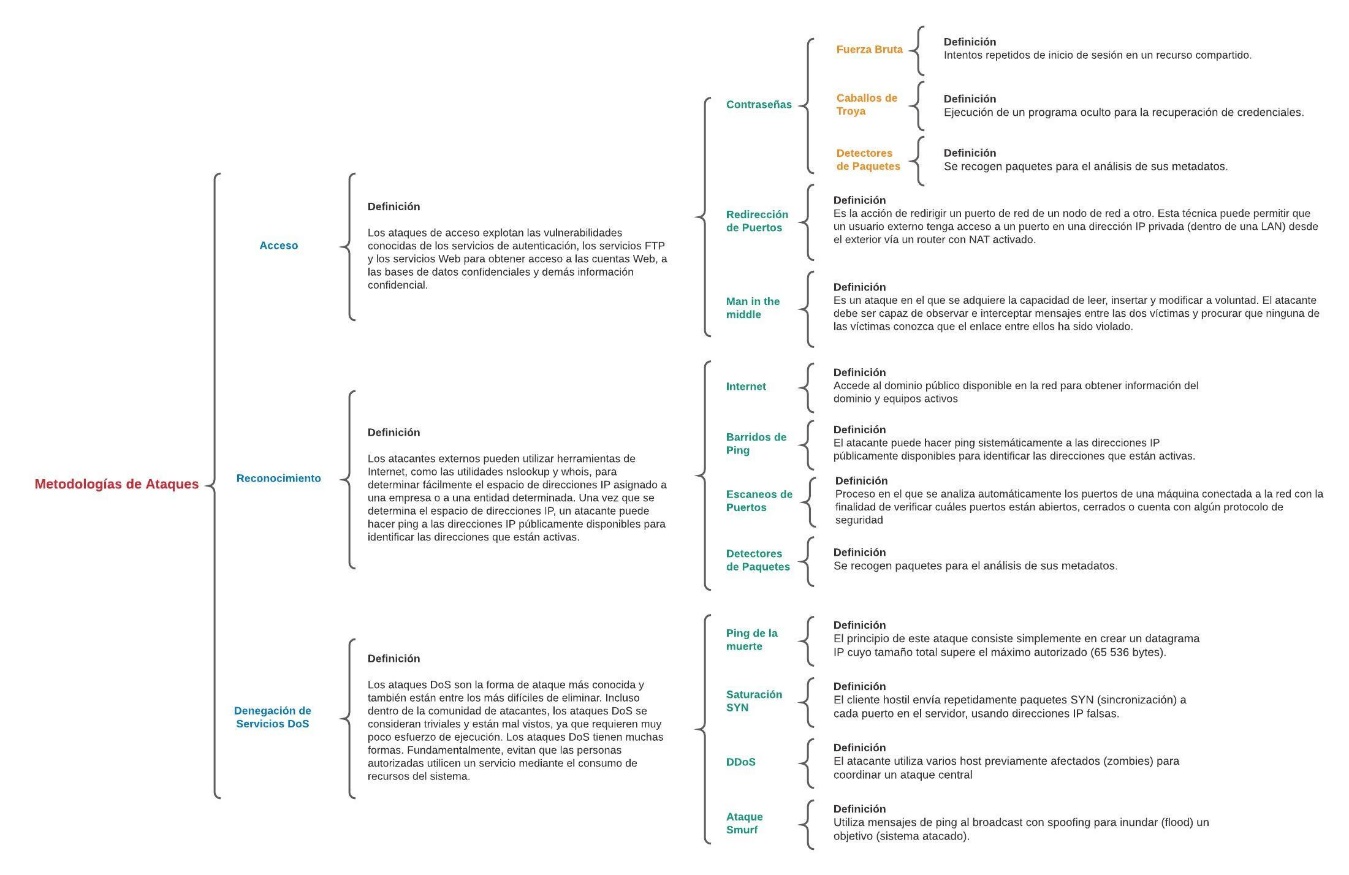
2. Retomar la información de comandos usados en la Actividad 1.4, hacer una tabla con dos columnas para identificar y describir el uso de los principales comandos de seguridad aplicados a un Router CISCO en una red, (agregando los nuevos comandos usados).

3. Usar el archivo de ejemplo de actividades, completar todos los datos del encabezado identificando si es Actividad, Investigación o Práctica, así como las competencias a desarrollar para esta actividad.

4. Subir el archivo terminado, no se te olvide, la reflexión, agregar la bibliografía en formato APA y dar clic para marcar como entregada la actividad.

**3. Desarrollo de la actividad**

**Cuadro Sinóptico de Metodologías de Ataque**

****

**Tabla de comandos de seguridad**

|  |  |
| --- | --- |
| 1 | $(domain) |
| Sirve para obtener el nombre del dominio actual |
| 2 | $(hostname) |
| Sirve para obtener el nombre del host actual |
| 3 | $(line) |
| Sirve para obtener el nombre de la línea que actualmente se configura |
| 4 | $(line-desc) |
| Genera una descripción de la línea con la que se configura |
| 5 | banner {exec | incoming | login | motd | slip-ppp} d message d |
| Genera un mensaje a manera de banner al inicializar el equipo |
| 6 | commands parser-mode {include | include- exclusive | exclude} [all] [interface interface-name| command] |
| Sirve para cambiar el modo con el se interpretan los comandos de una interfaz |
| 7 | config-register 0x2102 |
| Sirve para acceder a la configuración de un registro en específico (0x2102 en este caso) |
| 8 | configure terminal |
| Sirve para acceder al modo de configuración de la terminal |
| 9 | copy running-config startup-config |
| Sirve para guardar la configuración actual en el archivo de inicialización del equipo (guardar cambios) |
| 10 | copy startup-config running-config |
| Sirve para cargar la configuración inicial en el archivo de configuración actual (deshacer cambios) |
| 11 | crypto key generate rsa general-keys módulo modulus-size |
| Sirve para generar un par de llaves de encriptación RSA |
| 12 | crypto key zeroize rsa. |
| Sirve para eliminar las configuraciones de llaves de RSA que se hayan realizado previamente |
| 13 | enable nivel |
| Sirve para activar la configuración con un determinado nivel de privilegio |
| 14 | enable secret |
| Sirve para activar la configuración de un determinado nivel de privilegio |
| 15 | enable secret password |
| Sirve para activar y configurar una contraseña |
| 16 | enable secret level 5 cisco5 |
| Sirve para activar y configurar una contraseña para un determinado nivel de privilegio |
| 17 | enable view |
| Sirve para activar y configurar el modo de visualización del dispositivo fuera del modo de configuración |
| 18 | enable view root |
| Sirve para activar y configurar el modo de visualización del dispositivo fuera del modo de configuración |
| 19 | exec privilegiado enable view |
| Sirve para activar y configurar el modo de visualización del dispositivo fuera del modo de configuración para un determinado nivel de privilegio |
| 20 | exit |
| Sirve para cerrar el modo de configuración actual |
| 21 | line aux |
| Sirve para acceder al modo de configuración de la línea auxiliar |
| 22 | login block-for segundos attempts intentos within segundos |
| Sirve para configurar el inicio de sesión y sus parámetros de tiempos e intentos |
| 23 | login delay segundos |
| Sirve para establecer el tiempo que debe esperar para el login antes de lanzar un error de tiempo de espera |
| 24 | login delay. |
| Sirve para configurar el tiempo de espera durante el login |
| 25 | login local |
| Sirve para especificar el inicio de sesión de manera local en el dispositivo |
| 26 | login on-failure log [every login] |
| Sirve para configurar las acciones posteriores a un error en el inicio de sesión |
| 27 | login on-success log [every login] |
| Sirve para configurar las acciones posteriores a un inicio de sesión adecuado |
| 28 | login quiet-mode access-class {acl-nombre | acl-número} |
| Sirve para configurar el modo de acceso y la manera en la que se revisan las credenciales del usuario |
| 29 | no service password-recovery |
| Sirve para eliminar el servicio de guardar contraseñas |
| 30 | parser view nombre-vista superview |
| Sirve para configurar el nombre de una vista determinada y que pueda ser interpretada correctamente |
| 31 | privilege exec level 5 ping |
| Sirve para conceder el privilegio de realizar un ping de nivel 5 |
| 32 | privilege modo {level nivel de comando | reset} comando |
| Sirve para establecer el privilegio de realizar un determinado comando de cierto nivel a un usuario |
| 33 | secret contraseña-cifrada. |
| Sirve para establecer y configurar la contraseña de manera que permanezca encriptada |
| 34 | secure boot- config restore nombre-archivo. |
| Sirve para reestablecer un archivo determinado en la configuración de inicio |
| 35 | secure boot-config |
| Sirve para configurar las rutinas y ficheros de arranque del equipo |
| 36 | secure boot-image |
| Sirve para configurar una imagen (copia) de la configuración de inicio |
| 37 | security authentication failure rate tasa umbral log |
| Sirve para configurar una imagen (copia) de la configuración de inicio |
| 38 | service password-encryption |
| Sirve para habilitar el servicio de encriptación de contraseñas por defecto |
| 39 | router ospf 1 |
| Configuración del protocolo OSPF |
| 40 | area 0 authentication message-digest |
| Autenticación por MD5 en OSPF |
| 41 | ip ospf message-digest-key 1 md5 MD5pa55 |
| Configuración del protocolo OSPF |
| 42 | ntp authenticate |
| Configuración de autenticación ntp en Router |
| 43 | ntp authentication-key 1 md5 NTPpa55 |
| Configuración de llave MD5 ntp en Router |
| 44 | show logging |
| Información sobre el estado de los mensajes log en Router |
| 45 | username SSHadmin privilege 15 secret ciscosshpa55 |
| Crea un usuario SSHadmin con el nivel más alto de privilegio y establece password |
| 46 | crypto key generate rsa |
| Genera una llave RSA en Router |
| 47 | show ip ssh |
| Verifica la configuración SSH en Router |
| 48 | ssh –v 2 –l SSHadmin 10.2.2.1 |
| Conecta con una dirección en particular utilizando conexión SSH |
| 49 | username Admin1 secret admin1pa55 |
| Crear un usuario local con su respectivo nombre y contraseña |
| 50 | aaa new-model |
| Aplica inmediatamente la autenticación local a todas las líneas e interfaces (excepto la línea estafa 0 de la línea de la consola). Si se abre una sesión Telnet hacia el Router después de habilitar este comando (o si una conexión caduca y debe volver a conectarse), entonces el usuario debe autenticarse usando la base de datos local del Router. |
| 51 | aaa authentication login default local |
| Indica que la autenticación por default es la base de datos local |
| 52 | aaa authentication login default group radius local |
| La autenticación de todos los usuarios se hace usando el servidor Radius (el primer método). Si no responde el servidor de RADIUS, después se utiliza la base de datos local del Router (el segundo método). |
| 53 | login authentication default |
| Configurar la consola para usarla como el método de listado por default. |
| 54 | ip domain-name ccnasecurity.com |
| Establecer el nombre de dominio para una dirección ip |
| 55 | aaa authentication login SSH-LOGIN local |
| Configurar una lista llamada SSH-LOGIN para autenticar los inicios de sesión que usan el AAA local. |
| 56 | transport input shh |
| Únicamente acceso remoto a SSH |
| 57 | tacacs-server host 192.168.2.2 |
| Configurar la ip del servidor Tatacs |
| 58 | tacacs-server key tacacspa55 |
| Configurar la llave de acceso secreto en el servidor Tacacs |

**4. Reflexión**

Es de gran importancia conocer las diferentes metodologías que pueden ser empleadas para llevar a cabo un ciberataque, así como conocer las principales características de cada uno de los tipos que podrían darse en un sistema informático real, ya que nos permiten tomar medidas de prevención y de atención para cuando estas situaciones puedan ocurrir, lo que a su vez aumenta la seguridad de la red. Para proteger a la red, es necesario conocer las vulnerabilidades de la misma pero también es sumamente importante conocer las diferentes herramientas que tenemos para mejorar la seguridad de la red; de ahí la importancia de conocer los diferentes comandos de configuración que nos brindan los equipos de CISCO para llevar a cabo acciones que tengan por fin auxiliar en la seguridad de la red

**Referencias:**

* CISCO NETACAD (2021). Ataques de Reconocimiento. Recuperado desde: <http://itroque.edu.mx/cisco/cisco1/course/module11/#11.2.2.2>
* CISCO NETACAD (2021). Ataques con Acceso. Recuperado desde: <http://itroque.edu.mx/cisco/cisco1/course/module11/#11.2.2.3>
* CISCO NETACAD (2021). Ataques en DoS. Recuperado desde: <http://itroque.edu.mx/cisco/cisco1/course/module11/#11.2.2.4>