DATOS DE LA ACTIVIDAD							
No. de Actividad:	**1.10**	**Investigación**	**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:	Esmeralda Itzel Rodríguez Guareño					Registro:	19100256
Institución:	**Centro de Enseñanza Técnica Industrial plantel Colomos**						
Semestre:	8	Grupo:	B1	Período:	Ago-Dic 2022	Fecha:	09/09/2022
Compet. Genéricas	4.1, 4.5, 5.2, 5.5			Compet.. Profesional		12	

Propósito u objetivo:

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

Instrucciones:

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.

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 ó Practica, 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.

1.-

Acceso:

Los ataques de acceso explotan las vulnerabilidades conocidas de los servicios de autenticación, los servicios de FTP y los servicios Web para obtener acceso a cuentas Web, bases de datos y otra información confidencial. Estos ataques se clasifican en 4 tipos y a continuación se muestra ejemplo de ellos. El más común es el ataque a las contraseñas.

Ataques a las contraseñas: Pueden implementarse mediante un programa detector de paquetes para proporcionar cuentas de usuarios y contraseñas que se transmiten como texto sin cifrar.

Explotación de confianza: El objetivo de un ataque de explotación de confianza es comprometer un host de confianza, mediante su uso, con el fin de llevar a cabo ataques en otros hosts de una red.

Redirección de puertos: Es un tipo de ataque de explotación de confianza que utiliza un host comprometido para pasar tráfico a través de un firewall que, de lo contrario, estaría bloqueado.

Ataque man-in-the-middle: Son realizados por agresores que logran ubicarse entre dos hosts legítimos. El agresor puede permitir que se realicen transacciones normales entre hosts, y manipular la conversación entre ambos sólo periódicamente.

Reconocimiento:

Un ataque de reconocimiento se refiere a la fase de preparación donde el atacante obtiene toda la información necesaria de su objetivo y/o victima antes de lanzar un ataque.

los ataques de reconocimiento a menudo emplean el uso de rastreadores de paquetes y analizadores de puertos, que están ampliamente disponibles como descargas gratuitas en internet.

Los atacantes externos pueden utilizar herramientas de Internet para determinar fácilmente el espacio de direcciones IP asignado a una empresa o a una entidad determinada.

Una vez que se determina el espacio de direcciones IP, un atacante puede hacer ping a las direcciones IP públicamente disponibles para identificar las direcciones que están activas

algunos ejemplos de ataques de reconocimientos:

Consultas a través de internet
tiene como finalidad acceder a los servicios e información de la red logrando como objetivo el robo de contraseñas, redirección de servicios, técnica del hombre en medio, ip spoofing.

Denegación de servicio:

Un ataque de 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.
Los servidores web poseen la capacidad de resolver un número determinado de peticiones o conexiones de usuarios de forma simultánea, en caso de superar ese número, el servidor comienza a ralentizarse o incluso puede llegar a no ofrecer respuesta a las peticiones o directamente bloquearse y desconectarse de la red.
Existen dos técnicas de este tipo de ataques: la denegación de servicio o DoS (por sus siglas en inglés Denial of Service) y la denegación de servicio distribuido o DDoS (por sus siglas en inglés Destributed Denial of Service). La diferencia entre ambos es el número de ordenadores o IP´s que realizan el ataque.
Los ataques DoS son la forma de ataque más conocida y también están entre los más difíciles de eliminar. Incluso dentro de la comunidad de atacantes, los ataques DoS se consideran triviales y están mal vistos, ya que requieren muy poco esfuerzo de ejecución.

2.-

Comando	Descripción
show running-config	Muestra la configuración completa del equipo
configure	Opciones de configuración.
configure terminal	Accede al Modo de configuración global
interface	Accede al Modo de configuración de la interfaz seleccionada.
clock	Configura el reloj de la interfaz serie, en bits por segundo.

ip	Comandos de configuración de IP.
ip address dirección_IP máscara	Asignación de dirección IP
shutdown	Deshabilita la interfaz seleccionada.
no shutdown	Habilita la interfaz seleccionada
Enable secret _____	Este comando es para establecer una contraseña para pasar de consola a usuario al igual que para las sesiones de terminal virtual.
Line console 0	Ingresa al modo de configuración de línea de la consola. El 0 se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola
Line vty 0 4	Las líneas vty permiten el acceso a un dispositivo Cisco a través de Telnet. De manera predeterminada, muchos switches Cisco admiten hasta 16 líneas vty que se numeran del 0 al 15.
Line aux 0	Permite crear un acceso auxiliar a un dispositivo de cisco, para crear una interfaz de consola nueva que se puede modificar y adaptar al gusto del administrador de la red.
Username secret	Encripta todos los nombres de usuario existentes en el dispositivo usando el algoritmo MD5.
Login Block-for attempts within	Controla los intentos de inicio de sesión de las sesiones existentes dentro de un dispositivo. Luego de los intentos establecidos, bloquea el acceso.
SSH	Ofrece comunicación encriptada y segura entre dos sistemas sobre una red no segura.
Username privilege	Establece los privilegios de acceso de un usuario dentro de un dispositivo.
ntp authenticate	Sirve para poder configurar la autenticación del servicio NTP en un router, seguido de un identificador y una contraseña.
crypto key generate rsa	Se usa para poder crear identificadores RSA para intercambio de datos SSH cifrados, esto va seguido del número de módulos deseado.

ssh –l SSHadmin IP	Se usa para poder conectar un dispositivo con otro para poder hacer uso del ssh, en este caso fue nuestro computador PC-C con un Router
aaa authentication login default *methodname*	Realiza una lista de autenticación local predeterminada.
login authentication default	Asigna una lista de autenticación a un conjunto de líneas.
(tacacs/radius)-server host *host-ip*	Permite asignar las IP pertenecientes a un servidor TACACS/RADIUS.
(tacacs/radius)-server key *key*	Establece una contraseña de encriptación coincidente con el Daemon del server indicado TACACS/RADIUS.
aaa authentication login default group (tacacs/radius)+ local	Este comando establece métodos de autenticación, estos son EXEC para el tipo de servidor indicado.

Reflexión: Es muy importante saber sobre las 3 metodologías de ataques: ataques de acceso, reconocimiento y denegación de servicio. Ya que para saber como prevenirlos debemos saber en qué consiste. También saber cuales son los más comunes. En este caso el ataque más común es el de acceso específicamente el de las contraseñas y el ataque más conocido es de denegación de servicio.

Bibliografía

Dejo, R. A. (22 de 02 de 2017). *Ataques de Reconocimiento*. Obtenido de Tech club: https://techclub.tajamar.es/ataques-de-reconocimiento/

Guille, E. (27 de 10 de 2017). *Ataques de reconocimiento, Ataques con acceso y Ataques en DoS - CCNA1 V5 - CISCO C11*. Obtenido de Ingeniería Systems: http://www.ingenieriasystems.com/2017/10/Ataques-de-reconocimiento-Ataques-con-acceso-y-Ataques-en-DoS-CCNA1-V5-CISCO-C11.html

IBM. (05 de 03 de 2021). *Ataques de acceso no autorizado y denegación de servicio*. Obtenido de IBM: https://www.ibm.com/docs/es/msam/7.6.0.1?topic=SSG2D3_7.6.0.1/com.ibm.mbs.doc/securgroup/c_security_hacker_attacks.html