

DATOS DE LA ACTIVIDAD							
No. de Actividad:	1.11	Investigación	Conceptos Ataques de 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 conceptos y diferentes tipos de ataques en el ámbito de seguridad informática.

2. Instrucciones (Descripción) de la actividad

1. Responde el ejercicio , acceda a la siguiente liga y relaciona las columnas:
https://es.educaplay.com/juego/6888491-conceptos_de_seguridad.html

2. Una vez que tengas resuelto el ejercicio, usar el archivo de ejemplo de actividades, para pegar la(s) impresión(es) de pantalla completa de tus respuestas, completar todos los datos del encabezado identificando si es Actividad, Investigación o Practica, así como las competencias a desarrollar para esta actividad.

3. Subir el archivo terminado, no se te olvide, la reflexión, dar clic para marcar como entregada la actividad.

3. Desarrollo de la actividad

Relacionar Columnas: Conceptos de Seguridad

ENHORABUENA, HAS SUPERADO LA ACTIVIDAD

Conceptos de Seguridad

Confidencialidad	→	Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
Integridad	→	Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.
Disponibilidad	→	Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
CERT	→	Computer Emergency Response Team Coordination Center
ISO/IEC 27001	→	Information technology - Security techniques - Information security management systems - Requirements
PHVA	→	Planificar-Hacer-Verificar-Actuar
Impacto de ataques de red a un negocio	→	Reducción de la productividad
Amenaza	→	Potencial peligro que representa una vulnerabilidad
Riesgo	→	Probabilidad de que un agente de amenaza aproveche una vulnerabilidad y genere un impacto en el negocio
Virus	→	Software malicioso que se une a otro programa para ejecutar una función específica no deseada en un ordenador.
Gusano	→	Ejecuta código arbitrario e instala copias de sí mismo en la memoria del ordenador infectado, el cual infecta a otros hosts.
Caballo de Troya	→	Aplicación escrita para que parezca otra cosa. Cuando se descarga y se abre, ataca al equipo del usuario final desde dentro.
Fases básicas de ataque de un gusano.	→	Prueba Penetración Persistencia propagación Paralización
Componentes principales de un gusano	→	-Habilitación de vulnerabilidad -mecanismo de propagación- Acción maliciosa.
Antivirus	→	Ayuda a prevenir una infección y propagación de código malicioso.
Fases para tratar infección del gusano	→	Contención Inoculación Cuarentena Tratamiento
Ataques de reconocimiento	→	Involucran el descubrimiento no autorizado y el mapeo de los sistemas, servicios o vulnerabilidades. Emplean el uso de analizadores de paquetes y analizadores de puertos.

David Alejandro López Torres
17300155 BD1

100 PUNTOS

08:06 TIEMPO

1er NUM. INTENTOS

Compartir resultado:

Volver a jugar

Relacionar Columnas: Conceptos de Seguridad

ENHORABUENA, HAS SUPERADO LA ACTIVIDAD

Conceptos de Seguridad

Caballo de Troya	→	Aplicación escrita para que parezca otra cosa. Cuando se descarga y se abre, ataca al equipo del usuario final desde dentro.
Fases básicas de ataque de un gusano.	→	Prueba Penetración Persistencia propagación Paralización
Componentes principales de un gusano	→	-Habilitación de vulnerabilidad -mecanismo de propagación- Acción maliciosa.
Antivirus	→	Ayuda a prevenir una infección y propagación de código malicioso.
Fases para tratar infección del gusano	→	Contención Inoculación Cuarentena Tratamiento
Ataques de reconocimiento	→	Involucran el descubrimiento no autorizado y el mapeo de los sistemas, servicios o vulnerabilidades. Emplean el uso de analizadores de paquetes y analizadores de puertos.
Métodos para ataques de reconocimiento	→	-Analizadores de paquetes -Barridos de ping -Análisis de puertos -Consultas de información de Internet
Ataques de acceso	→	Explotan vulnerabilidades conocidas en los servicios de autenticación, servicios FTP y servicios web para entrar en cuentas web, bases de datos confidenciales, y otra información sensible.
Ataques de Denegación de Servicio	→	Envían un gran número de solicitudes a través de una red o de Internet.
Métodos para Ataques de acceso	→	Ataques de fuerza bruta, Caballo de Troya, IP spoofing analizadores de paquetes.
Ataque de Contraseña	→	Un atacante intenta adivinar las contraseñas del sistema. Ataque de diccionario.
Puerto de redirección	→	Un sistema comprometido se utiliza como punto de salto para los ataques contra otros objetivos.
Ataque de confianza	→	Un atacante utiliza privilegios concedidos a un sistema de una manera no autorizada, que posiblemente lleve a comprometer el objetivo.
Man-in-the-middle	→	Un atacante se coloca en el medio de comunicación entre dos entidades legales con el fin de leer o modificar los datos.
Desbordamiento de buffer	→	Un programa que escribe datos más allá de la memoria buffer asignada.
DDoS	→	El ataque se origina a partir de múltiples fuentes coordinadas, además de aumentar la cantidad de tráfico de red desde múltiples atacantes.

David Alejandro López Torres
17300155 BD1

1045 a.m.
12/09/2021

4. Reflexión

Con el desarrollo de esta actividad fue posible repasar los diferentes conceptos que se trabajaron durante la sesión matutina del martes acerca de diferentes ataques de seguridad. Podemos apreciar la diversidad que existe entre los tipos de ataques y las técnicas con las que se implementan, dejando ver la importancia de implementar una gran cantidad de alternativas de seguridad en la infraestructura de las redes para disminuir en la medida de lo posible los riesgos que podrían representar algunas de estas estrategias de ataques informáticos.

Referencias:

Cisco NETACAD. (2021). Cybersecurity Essentials. Retrieved from:
<https://static-course-assets.s3.amazonaws.com/CyberEss/es/index.html#3.0.1.1>