Networking Academy

Seguridad en Equipos Terminales

Alcance y la secuencia

1.0

Contents

Público Objetivo

El curso Seguridad en Equipos Terminales (Endpoint Security) es apropiado para estudiantes con competencia en lectura de escuela secundaria, conocimientos básicos de computación e interesados en buscar un trabajo de nivel de entrada en el campo de la seguridad cibernética.

Prerrequisitos

No hay requisitos previos para este curso, aunque los alumnos deben tener las siguientes habilidades básicas:

- Habilidades básicas de navegación del sistema operativo de PC
- Conocimiento de las redes TCP/IP, incluidos los protocolos, servicios y procesos de red.

Si bien no es obligatorio, se recomienda que los alumnos completen los siguientes cursos dentro de la ruta de aprendizaje de seguridad cibernética:

- Introducción a la Ciberseguridad
- Fundamentos de la red

Alineación de Certificación

Este curso, de la Carrera Profesional de Analista de Ciberseguridad Junior, se alinea con la certificación de CCST Cybersecurity.

Descripción del Curso

Seguridad en Equipos Terminales tiene muchas funciones para ayudar a los alumnos a comprender los conceptos de seguridad. El diseño del curso incluye:

- Diez módulos compuestos por temas clave.
- Los módulos enfatizan el pensamiento crítico, la resolución de problemas, la colaboración y la aplicación práctica de las habilidades.
- Cada módulo contiene actividades de práctica y evaluación, como una actividad de Verifique su comprensión, un laboratorio o una actividad utilizando nuestra herramienta de simulación de red, Cisco® Packet Tracer.
- Las actividades de nivel de tema están diseñadas para indicar el dominio de un alumno de las habilidades del curso, lo que permite a los alumnos medir la comprensión antes de realizar un cuestionario o examen calificado.
- El lenguaje que describe los conceptos está diseñado para que los estudiantes de nivel secundario lo entiendan fácilmente.
- Las evaluaciones y las actividades de práctica se enfocan en competencias específicas y están diseñadas para aumentar la retención y proporcionar flexibilidad en el camino del aprendizaje.
- Las herramientas de aprendizaje multimedia, incluidos videos y cuestionarios, abordan una variedad de estilos de aprendizaje, estimulan el aprendizaje y promueven la retención de conocimientos.
- Las actividades basadas en simulación de laboratorios y Packet Tracer ayudan a los estudiantes a desarrollar el pensamiento crítico y habilidades para resolver problemas complejos.
- Las evaluaciones innovadoras brindan retroalimentación inmediata para respaldar la evaluación de conocimientos y habilidades.
- Los conceptos técnicos se explican utilizando un lenguaje de nivel introductorio.

- Las actividades interactivas integradas dividen la lectura de grandes bloques de contenido y refuerzan la comprensión.
- El curso enfatiza las habilidades aplicadas y las experiencias prácticas, al tiempo que alienta a los alumnos a considerar la educación adicional en Tecnología de la Información (TI).

Objetivos del Curso

Seguridad en Equipos Terminales presenta importantes conceptos fundamentales en ciberseguridad, como ataques y atacantes comunes, amenazas, vulnerabilidades y riesgos, tendencias actuales en ciberseguridad, vulnerabilidades de servicios y protocolos de red, puntos finales de Windows y Linux, y mitigación y defensa de amenazas. Al final del curso, los alumnos pueden identificar amenazas comunes y técnicas de mitigación, comprender los conceptos de amenaza, vulnerabilidad y riesgo, y adquirir experiencia en el análisis de ataques comunes, operación y seguridad de equipos terminales y malware.

El material del curso lo ayudará a desarrollar las habilidades de los alumnos, que incluyen:

- Explicar cómo los actores de amenazas ejecutan algunos de los tipos más comunes de ciberataques.
- Explicar los principios de seguridad de la red.
- Explicar cómo las vulnerabilidades de TCP.IP permiten ataques a la red.
- Recomendar medidas para mitigar las amenazas.
- Solucionar problemas de una red inalámbrica.
- Explicar cómo se utilizan los dispositivos y servicios para mejorar la seguridad de la red.
- Usar herramientas administrativas de Windows.
- Implementar la seguridad básica de Linux.
- Evaluar la protección de equipos terminales y el impacto del malware.
- Utilizar las mejores prácticas de ciberseguridad para mejorar la confidencialidad, la integridad y la disponibilidad.

Requisitos del equipo

Los laboratorios prácticos de Seguridad en Equipos Terminales requieren equipos que se encuentran en la mayoría de las redes domésticas. Cualquier laboratorio que requiera un entorno de red más complejo utiliza Packet Tracer, la herramienta de simulación de red.

Software

- Oracle Virtual Box
- Archivos OVA de máquina virtual de laboratorio
- Packet Tracer 8.0.1 or mayor

Equipo de laboratorio opcional

- PC con Microsoft Windows

Esquema del curso

La Tabla 1 a continuación detalla los módulos y sus competencias asociadas. Cada módulo es una unidad integrada de aprendizaje que consta de contenido, actividades y evaluaciones que apuntan a un conjunto específico de

competencias. El tamaño del módulo depende de la profundidad del conocimiento y la habilidad necesarios para dominar la competencia.

Tabla 1: Título y objetivo del módulo

Título del módulo/Título del tema	Objectivo
Módulo 1: Amenazas, vulnerabilidades y ataques a la ciberseguridad	
1.0 Amenazas, vulnerabilidades y ataques a la ciberseguridad	Explicar cómo los actores de amenazas ejecutan algunos de los tipos más comunes de ciberataques.
1.1 Amenazas comunes	Explicar las amenazas, vulnerabilidades y ataques que ocurren en los distintos dominios.
1.2 Engaño	Identificar los diferentes métodos de engaño utilizados por los atacantes para engañar a sus víctimas.
1.3 Ataques cibernéticos	Describir algunos tipos comunes de ataques a la red.
1.4 Ataques a dispositivos inalámbricos y móviles	Describir los tipos comunes de ataques a dispositivos inalámbricos y móviles.
1.5 Ataques de aplicaciones	Describir los tipos de ataques a aplicaciones.
Módulo 2: Protección de redes	
2.0 Protección de redes	Explicar los principios de seguridad de la red.
2.1 Acceso al IOS de Cisco	Explicar cómo acceder a un dispositivo Cisco IOS para fines de configuración.
2.2 Navegación IOS	Explicar cómo navegar por Cisco IOS para configurar dispositivos de red.
2.3 La estructura de mando	Describir la estructura de comandos del software Cisco IOS.
2.4 Configuración básica del dispositivo	Configure un dispositivo Cisco IOS usando CLI.
2.5 Guardar configuraciones	Utilice los comandos de IOS para guardar la configuración en ejecución.
2.6 Puertos y Direcciones	Explicar cómo se comunican los dispositivos a través de los medios de red.
2.7 Configurar el direccionamiento IP	Configure un dispositivo host con una dirección IP.
2.8 Verificar la conectividad	Verifique la conectividad entre dos dispositivos finales.
Módulo 3: Atacar a la Fundación	
3.0 Atacando a la Fundación	Explicar cómo las vulnerabilidades de TCP/IP permiten los ataques a la red.
3.1 Detalles de IP PDU	Explicar la estructura de encabezado de IPv4 e IPv6.
3.2 Vulnerabilidades de IP	Explicar cómo las vulnerabilidades de IP permiten los ataques a la red.
3.3 Vulnerabilidades de TCP y UDP	Explicar cómo las vulnerabilidades de TCP y UDP permiten ataques a la red.
Módulo 4: Atacar lo que hacemos	
4.0 Atacar lo que hacemos	Recomendar medidas para mitigar las amenazas.
4.1 Servicios de PI	Explicar las vulnerabilidades del servicio IP.
4.2 Servicios empresariales	Explicar cómo las vulnerabilidades de las aplicaciones de red permiten los ataques a la red.
4.3 Mitigación de ataques de red comunes	Recomendar medidas básicas de mitigación de amenazas.
Módulo 5: Dispositivos de comunicación de red inalámbrica	
5.0 Dispositivos de comunicación de red inalámbrica	Solucionar problemas de una red inalámbrica.
5.1 Comunicaciones inalámbricas	Explicar cómo los dispositivos inalámbricos permiten la comunicación en red.
5.2 Amenazas WLAN	Describir las amenazas a las WLAN.
5.3 WLAN seguras	Solucionar problemas de una conexión inalámbrica.
Módulo 6: Infraestructura de seguridad de red	
6.0 Infraestructura de seguridad de red	Explicar cómo se utilizan los dispositivos y servicios para mejorar la seguridad de la red.

6.0 Cortafuegos de política basados en zonas	Implemente el cortafuegos de política basado en zonas mediante la CLI.
6.1 Dispositivos de seguridad	Explicar cómo se utilizan dispositivos especializados para mejorar la seguridad de la red.
6.2 Servicios de seguridad	Explicar cómo los servicios mejoran la seguridad de la red.
Módulo 7: El Sistema Operativo Windows	
7.0 El sistema operativo Windows	Utilice las herramientas administrativas de Windows.
7.1 Historial de Windows	Describa la historia del sistema operativo Windows.
7.2 Arquitectura y operaciones de Windows	Explique la arquitectura de Windows y su funcionamiento.
7.3 Configuración y Monitoreo de Windows	Use las herramientas administrativas de Windows para configurar, monitorear y administrar los recursos del sistema.
7.4 Seguridad de Windows	Explique cómo se puede mantener seguro Windows.
Módulo 8: Descripción general de Linux	
8.0 Descripción general de Linux	Implemente la seguridad básica de Linux.
8.1 Fundamentos de Linux	Explique por qué las habilidades de Linux son esenciales para el monitoreo y la investigación de la seguridad de la red.
8.2 Trabajar en el shell de Linux	Use el shell de Linux para manipular archivos de texto.
8.3 Servidores y Clientes Linux	Utilice la línea de comandos de Linux para identificar los servidores que se ejecutan en una computadora.
8.4 Administración básica del servidor	Use comandos para ubicar y monitorear archivos de registro.
8.5 El sistema de archivos de Linux	Use comandos para administrar el sistema de archivos y los permisos de Linux.
8.6 Trabajar con la GUI de Linux	Explicar los componentes básicos de la GUI de Linux.
8.7 Trabajar en un host Linux	Use herramientas para detectar malware en un host Linux.
Módulo 9: Protección de sistemas y terminales	
9.1 Sistemas y dispositivos de defensa	Utilice procesos y procedimientos para proteger los sistemas.
9.2 Protección antimalware	Explicar los métodos para mitigar el malware.
9.3 Prevención de intrusiones basada en host	Recomendar medidas de seguridad de punto final.
9.4 Seguridad de la aplicación	Use herramientas de investigación de malware para conocer las características del malware.
9.1 Sistemas y dispositivos de defensa	Utilice procesos y procedimientos para proteger los sistemas.
Módulo 10: Principios, prácticas y procesos de ciberseguridad	
10.0 Principios, prácticas y procesos de ciberseguridad	Utilice las mejores prácticas de ciberseguridad para mejorar la confidencialidad, la integridad y la disponibilidad.
10.1 Las tres dimensiones	Use hashes para verificar la integridad de los archivos.
10.2 Estados de los datos	Compare los tres estados de los datos.
10.3 Contramedidas de ciberseguridad	Compare los tipos de contramedidas de ciberseguridad.