Networking Academy

Defensa de la Red

Alcance y secuencia

Versión 1.0

Contenido

Público Objetivo

El curso Defensa de la Red (Network Defense) es apropiado para estudiantes con competencias en lectura de escuela secundaria, conocimientos básicos de informática e interesados en conseguir un trabajo de nivel inicial en el campo de la ciberseguridad.

Requisitos Previos

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

- Conocimientos básicos de navegación en sistemas operativos 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 estudiantes completen los siguientes cursos dentro de la ruta de aprendizaje de ciberseguridad:

- Introducción a la Ciberseguridad (Introduction to Cybersecurity)
- Fundamentos de Redes (Networking Essentials)
- Seguridad en Equipos Terminales (Endpoint Security)

Alineación de la Certificación

Este curso es parte de Cybersecurity Career Path, que se alinea con la certificación CCST Cybersecurity.

Descripción del Curso

Defensa de la Red tiene muchas características para ayudar a los estudiantes a entender los conceptos de defensa de la red. El diseño del curso incluye:

- Once módulos compuestos por temas clave.
- Los módulos enfatizan el pensamiento crítico, la resolución de problemas, la colaboración y la aplicación práctica de habilidades.
- Cada módulo contiene actividades de práctica y evaluación tales como una actividad de Verifique su Comprensión, una práctica de laboratorio o una actividad utilizando nuestra herramienta de simulación de red, Cisco® Packet Tracer.
- Las actividades a nivel de tema están diseñadas para reflejar el dominio de las habilidades del curso por parte del estudiante, lo que le permite evaluar su comprensión antes de realizar un cuestionario o examen calificado.
- El lenguaje que describe los conceptos está diseñado para que los estudiantes de secundaria lo entiendan fácilmente.
- Las evaluaciones y las actividades de práctica se centran en competencias específicas y están diseñadas para aumentar la retención y proporcionar flexibilidad en el camino de 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 prácticas de laboratorio y las actividades basadas en simulación de Packet Tracer ayudan a los estudiantes a desarrollar el pensamiento crítico y la capacidad de resolución de problemas complejos.
- Las evaluaciones innovadoras brindan retroalimentación inmediata para apoyar la evaluación del conocimiento y las 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 anima a los estudiantes a considerar educación adicional en Tecnologías de la Información (TI).

Objetivos del Curso

Defensa de la Red presenta importantes conceptos básicos de ciberseguridad, tales como la defensa del sistema y de la red, el control de acceso, los firewalls, la seguridad en la nube, las aplicaciones de criptografía, los datos de seguridad de la red y la evaluación de las alertas de seguridad. Al final del curso los alumnos pueden implementar medidas defensivas y de control de acceso, configurar un firewall simulado, utilizar diferentes tipos de datos de red y evaluar las alertas de seguridad.

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

- Explicar los enfoques para la defensa de la seguridad de la red.
- Implementar algunos de los diversos aspectos del sistema y la defensa de la red.
- Configurar el control de acceso local y basado en servidor.
- Implementar listas de control de acceso (ACL) para filtrar el tráfico y mitigar los ataques a la red.
- Comprender cómo se implementan los firewalls para proporcionar seguridad en la red.
- Implementar un firewall de política basado en zonas mediante la CLI.
- Recomendar requisitos de seguridad en la nube en función de un escenario de nube determinado.
- Determinar las técnicas criptográficas que se requieren para garantizar la confidencialidad, la integridad y la autenticidad.
- Explicar cómo las tecnologías de seguridad afectan el monitoreo de seguridad.
- Usar diferentes tipos de registros para almacenar información sobre los hosts y la red.
- Explicar el proceso de evaluación de alertas.

Requisitos de Equipamiento

Defensa de la Red requiere 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 la máquina virtual de laboratorio
- Packet Tracer 8.0.1 o superior

Equipo de laboratorio opcional

- Host 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	Objetivo
Módulo 1: Comprendiendo la Defensa	
1.0 Comprender la Defensa	Explicar los enfoques para la defensa de la seguridad de la red.
1.1 Defensa en Profundidad	Explicar cómo se utiliza la estrategia de defensa en profundidad para proteger las redes.
1.2 Gestión de Operaciones de Ciberseguridad	Explicar cómo una organización monitorea las amenazas de ciberseguridad.
1.3 Políticas, Reglamentos y Normas de Seguridad	Explicar las políticas, regulaciones y estándares de seguridad.
Módulo 2: Defensa de Sistemas y Redes	
2.0 Sistema y Defensa de la Red	Implementar algunos de los diversos aspectos del sistema y la defensa de la red.
2.1 Seguridad Física	Explicar cómo se implementan las medidas de seguridad física para proteger los equipos de red.
2.2 Seguridad de la Aplicación	Explicar cómo aplicar las medidas de seguridad de las aplicaciones.
2.3 Fortalecimiento de la Red: Servicios y Protocolos	Explicar cómo fortalecer los servicios y protocolos de red.
2.4 Fortalecimiento de la Red: Segmentación	Explicar cómo la segmentación de la red puede ayudarlo a fortalecer la red.
2.5 Fortalecimiento de Dispositivos Inalámbricos y Móviles	Configurar el fortalecimiento y la seguridad del router inalámbrico.
2.6 Resiliencia de la Ciberseguridad	Explicar la seguridad física con dispositivos IoT.
2.7 Sistemas Embebidos y Especializados	Implementar seguridad física con dispositivos IoT.
Módulo 3: Control de Acceso	
3.0 Control de Acceso	Configurar el control de acceso local y basado en servidor.
3.1 Controles de Acceso	Configurar el acceso seguro en un host.
3.2 Conceptos de Control de Acceso	Explicar cómo el control de acceso protege los datos de la red.
3.3 Gestión de Cuentas	Explicar la necesidad de estrategias de administración de cuentas y control de acceso.

Módulo 4: Listas de Control de Acceso	
4.1 Introducción a las Listas de Control de Acceso (ACL)	Describir las ACL estándar y extendidas de IPv4.
4.2 Enmascaramiento de Comodines (Wildcard)	Explicar cómo las ACL usan máscaras wildcard.
4.3 Configurar ACL	Explicar cómo configurar las ACL.
4.4 Sintaxis de ACL de IPv4 Estándar con Nombre	Usar números de secuencia para editar las ACL de IPv4 estándar existentes.
4.5 Implementar ACL	Implementar ACL.
4.6 Mitigar Ataques con ACL	Usar ACL para mitigar los ataques de red comunes.
4.7 ACL de IPv6	Configurar las ACL de IPv6 mediante la CLI.
Módulo 5: Tecnologías de Firewall	
5.0 Tecnologías de Firewall	Explicar cómo se implementan los firewalls para proporcionar seguridad en la red.
5.1 Redes Seguras con Firewall	Explicar cómo se utilizan los firewalls para ayudar a proteger las redes.
5.2 Firewall en el Diseño de Redes	Explicar las consideraciones de diseño para implementar tecnologías de firewall.
Módulo 6: Firewalls de Política Basados en Zonas	
6.0 Firewall de Política Basado en Zonas	Implementar el firewall de política basado en zonas mediante la CLI.
6.1 Descripción general de ZPF	Explicar cómo se utilizan los firewalls de políticas basados en zonas para ayudar a proteger una red.
6.2 Operación ZPF	Explicar el funcionamiento de un firewall de política basado en zonas.
Módulo 7: Seguridad en la Nube	
7.0 Seguridad en la Nube	Recomendar los requisitos de seguridad de la nube en función de un escenario de nube determinado.
7.1 Virtualización y Computación en la Nube	Describir formas de gestionar las amenazas a la nube pública y privada.
7.2 Los Dominios de la Seguridad en la Nube	Explicar los dominios de la seguridad en la nube.
7.3 Seguridad de la Infraestructura en la Nube	Explicar la mitigación de las amenazas a la infraestructura de la plataforma en la nube.
7.4 Seguridad de las Aplicaciones en la Nube	Recomendar aplicaciones de seguridad en la nube.
7.5 Seguridad de Datos en la Nube	Explicar cómo proteger los datos en la nube.

7.6 Protección de Máquinas Virtuales (VM)	Explicar cómo proteger las instancias de VM.
Módulo 8: Criptografía	
8.0 Criptografía	Determinar las técnicas criptográficas que se requieren para garantizar la confidencialidad, la integridad y la autenticidad.
8.1 Confidencialidad	Determinar el algoritmo de cifrado a utilizar según los requisitos.
8.2 Ocultamiento de Datos	Utilizar una técnica para ocultar datos.
8.3 Integridad y Autenticidad	Explicar el papel de la criptografía para garantizar la integridad y autenticidad de los datos.
8.4 Hashing	Explicar cómo usar las herramientas de hash.
8.5 Criptografía de Clave Pública	Utilizar una firma digital.
8.6 Autoridades y el Sistema de Confianza de PKI	Utilizar hashing para detectar la intercepción de la red.
8.7 Aplicaciones e Impactos de la Criptografía	Explicar cómo afecta el uso de la criptografía a las operaciones de ciberseguridad.
Módulo 9: Tecnologías y Protocolos	
9.0 Tecnologías y Protocolos	Explicar cómo las tecnologías de seguridad afectan el monitoreo de seguridad.
9.1 Supervisión de Protocolos Comunes	Explicar el comportamiento de los protocolos de red comunes en el contexto de la supervisión de la seguridad.
9.2 Tecnologías de Seguridad	Explicar cómo las tecnologías de seguridad afectan la capacidad de monitorear los protocolos de red comunes.
Módulo 10: Datos de Seguridad de la Red	
10.0 Datos de Seguridad de la Red	Usar diferentes tipos de registros para almacenar información sobre los hosts y la red.
10.1 Tipos de Datos de Seguridad	Describir los tipos de datos utilizados en la supervisión de la seguridad.
10.2 Registros de Dispositivos Finales	Describir los elementos de un archivo de registro de dispositivo final.
10.3 Registros de Red	Utilizar diferentes tipos de servicios para recopilar datos de red.
Módulo 11: Evaluación de Alertas	
11.0 Evaluación de Alertas	Explicar el proceso de evaluación de alertas.
11.1 Origen de las Alertas	Identificar la estructura de las alertas.

11.2 Descripción General de la Evaluación de Alertas	Explicar cómo se clasifican las alertas.