CURSO : Seguridad Defensiva para BlueTeam
Duración : 30 horas

I. DESCRIPCIÓN

Este curso tiene un nivel intermedio y está dirigido para profesionales y administradores de red que quieran especializarse en Seguridad Defensiva para la integración y despliegue de infraestructura de ciberseguridad enfocada a identificar, proteger y detectar amenazas, utilizando como base las últimas tecnologías de protección y detección utilizadas en ciberseguridad.

Durante el desarrollo de los diferentes módulos del Programa desarrollaremos los conceptos de Implementación de Soluciones Integrales basado en Next Generation Firewall, UTM, IPS, protección de páginas web, implementación de WAF (Firewall de Aplicaciones Web), implementación de Proxy reverso, control de tráfico malicioso, Implementación de soluciones como ClearOS, Wazuh, Security Onion, OSSIM y más, aprendiendo a implementar soluciones multimarca como Cisco System, Fortinet, OpenSource, Endian, Linux entre otras marcas.

II. METODOLOGÍA

El curso contará con sesiones teórico-prácticas. Se empleará material audiovisual con la finalidad de facilitar los procesos de adquisición y evaluación del aprendizaje. Durante las clases se buscará la participación activa de los alumnos mediante el desarrollo de ejercicios y discusión en clase. Se trabaja con equipos reales y maquinas virtuales.

III. REQUISITOS

- Conocimientos de Redes de Datos y Protocolos TCP/IP.
- Conocimientos básicos de Redes LAN

IV. MATERIALES

- Manual impreso por cada Módulo, Guía de Laboratorios.
- Los Laboratorios se realizarán con equipos reales y máquinas virtuales.

CERTIFICADO: Se emite un certificado

- Certificado como Curso de Seguridad Defensiva para BlueTeam

V. PLAN DE TEMAS

El programa incluye los siguientes módulos

Módulo 1 : Sistemas de Protección Perimetral LAN
Módulo 2 : Implementación y Gestión de Firewall y UTM
Módulo 3 : Herramientas de Detección de comportamiento Malicioso
Módulo 4 : Gestión de Vulnerabilidades
Módulo 5 : Gestión de LOGS y Registros de Incidentes

Detalle de cada Módulo:

Módulo 1 : Sistemas de Protección Perimetral LAN

Seguridad de las Redes LAN

- Segmentación de Redes LAN, Troncales, vlans
- Enrutamiento en Capa 3
- Seguridad de Capa 3, ACL , políticas de Seguridad

Protección contra ataque en la Red LAN

- Seguridad de Capa 3, ACL , políticas de Seguridad
- Port Security , Dhcp Snooping, Vlan Attack, MAC Flooding, Spanning Tree Attack, Dhcp Starvation, Arp Spoofing

Auditoria de Redes LAN

- Auditoria detalla de Router y Switches.
- Escáner de Vulnerabilidades en equipos de Red
- Identificación de Vulnerabilidades
- Vulnerabilidad de SNMP v2c ,v3
- Bechmark en Dispositivos de Red - CIS

Módulo 2 : Implementación y Gestión de Firewall y UTM

Implementación de UTM Open Source

- Implementación de Firewall OpenSource
- Configuración de Interfaces y Servicios
- Firewall Linux iptables y Firewalld
- Configuración de Políticas de Seguridad
- Habilitación de SNAT y DNAT

Implementación de UTM Fortigate

- Habilitación del Appliance Fortigate
- Upgrade de OS y Backup
- Configuración de Políticas de Seguridad
- Nateo Dinámico y Estático VIP
- Configuración de Reglas de Navegación
- Manejo de Log y Eventos

Implementación y Administración de ClearOS

- Conceptos básicos de ClearOS
- Funcionalidades de ClearOS
- Implementación de ClearOS
- Configuración de Administración
- Habilitación de Servicios

Módulo 3 : Herramientas de Detección de comportamiento Malicioso

Análisis de Código malicioso

- Análisis de infecciones por malware
- Comportamiento de código malicioso persistente
- Análisis estático de malware
- Análisis Dinámico de malware
- Identificación de Firmas de malware

Análisis de trafico de Red

- Análisis de trafico de Red
- Analizadores de protocolo
- Herramientas para Análisis de trafico de Red

Herramientas de Detección y Gestión de Ciberataques

- Sistemas de detección de intrusos (HIDS)
- Herramienta OSSED y Vigilancia de logs
- Implementación de Stack Wazuh
- Implementación de Security Onion en producción

Módulo 4 : Gestión de Vulnerabilidades

Gestión de Vulnerabilidades y Cumplimiento (Compliance)

- Proceso de Gestión de Vulnerabilidades
- Score de vulnerabilidades basado en CVSS
- Diferencia entre vulnerabilidades y Benchmark
- Auditoria de Hardening y BenchMark basado CIS

Análisis de Vulnerabilidades de Infraestructura

- Análisis de Vulnerabilidades de Infraestructura
- Métodos de Ataques y Explotación de Servidores
- Implementación de Escaner de Vulnerabilidades para Infraestructura

Análisis de Vulnerabilidades de Aplicaciones Web

- Análisis de Vulnerabilidades de Aplicaciones Web
- Vulnerabilidades Web tipicas
- Herramientas de Análisis de Vulnerabilidades web

Modulo 5 : Gestión de LOGS y Registros de Incidentes

Gestión de Log y Registros

- Gestión de Logs en equipos de Red y Servidores
- Servidores de Gestión de Log y SNMP.
- Implementación de Servidor de Gestión de Log

Herramientas de Gestión de Incidentes

- Equipo de Respuesta a Incidentes
- Herramientas de Gestión de Incidentes
- Implementación de una Herramienta de Gestión de Incidentes

Correlacionador de Eventos y Alarmas de Seguridad

- Como funciona un correlacionador de eventos - SIEM
- Descubrimiento de Activos
- Análisis de Vulnerabilidades
- Detección de intrusos
- Monitoreo de comportamiento
- Correlación de eventos SIEM
- Analizando OSSIM