Syllabus del Curso de Monitoreo y SOC Open Source con Zabbix, Grafana, Pfsense, Security Onion y Wazuh (Videoconferencia)

Módulo 1: Despliegue inicial de infraestructura de red y servidores con GNS3 y PfSense

Introducción
- Herramientas de Monitoreo Open Source
- Herramientas de SOC Open Source
- Arquitectura propuesta

Despliegue de VM Kubuntu con GNS3
- Configuración de IP Pública
- Arranque de GNS 3
- Afinamiento de la VM
- Script de Iptables

Instalación y despliegue de PfSense 2.8
- Introducción a Pfsense
- Requerimientos de Hardware
- Instalación de PfSense en GNS 3
- Configuración de interfaces de red para LAN, WAN, DMZ
- Configuración de VLANs
- Reglas iniciales de salida a internet para LAN y DMZ
- Reglas de NAT para Web Server y Mail Server

Configuración de Servicios en PfSense
- Configuración de Kea DHCP
- Squid Proxy
- PfBlockerNG
- OpenVPN
- Wireguard

Módulo 2: Despliegue de Zabbix y Grafana como solución de Monitoreo de infraestructura

Introducción
- Definiciones y procesos zabbix
- Arquitectura de Zabbix
- Requerimientos de Hardware

Instalación y Despliegue de Zabbix
- Instalación de zabbix en Ubuntu 24.04
- Instalación de zabbix en Ubuntu 24.04 de manera distribuida
- Configuración de zabbix en alta disponibilidad para el web server y demonio zabbix-server

Gestión de Usuarios
- Gestion de usuariosy grupos
- Creación de roles
- Permisos y autenticaciones

Gestion de Agentes y protocolos de monitoreo
- Zabbix agent
- Zabbix agent active
- Templates de monitoreo
- SNMP agent
- SNMP trap
- HTTP agent
- External checks
- Calculated
- SSH checks

- Database monitor
- Zabbix trapper
- Zabbix internal

Gestion de Triggers y Acciones

- min, max, avg, last, changue, find, forecast y timeleft
- Media types
- Comandos remotos
- Trigger alerts
- Escalations

Gestion de mapas y Dashboards

- Creación de mapas de monitoreo
- Creación de dashboards dinámicos principal y por hosts en zabbix con widgets
- Geomap, Item History, Item navigator, Item value, Host navigator, Honeycomb, Gauge,
- Graph, Pie charts, Problems, Top Hosts, Top items, maps y widgets de terceros

Zabbix con Grafana

- Instalación de grafana
- integración de desarrollo de dashboard dinámico
- Casos de uso

Monitoreo con zabbix de plataformas

- Monitoreo de Proxmox
- Monitoreo de Carbonio
- Monitoreo de Zimbra
- Monitoreo de base de datos PostgreSQL
- Monitoreo de Issabel
- Monitoreo de nginx
- Monitoreo de active directory
- Monitoteo de FW pfsense
- Monitoreo de switch cisco

Módulo 3: SOC Open Source con Wazuh, Security Onion y Zabbix

Introducción

- Soluciones Open Source de Seguridad
- SIEM, IDS, HIDS, NIDS,
- Escanners, Análisis de Vulnerabilidades
- Herramientas de explotación

Instalación y Despliegue de Wazuh

- Arquitectura de Wazuh
- Requerimientos de Hardware
- Instalación de Servidor Wazuh
- Elastic Stack
- Instalación del Agente Wazuh

Administración y configuración de Wazuh

- Reglas y decodificaciones en Wazuh
- Opciones para la configuración de reglas en Wazuh
- Sintaxis y niveles de clasificación de reglas en Wazuh
- Decodificaciones y opciones de codificadores en Wazuh
- Descodificadores y personalización de reglas de estos en Wazuh
- Alertas y respuestas activas en Wazuh
- Respuestas activas en Wazuh - opciones, funcionamientos y respuestas por defecto

Instalación y Despliegue de Security Onion

- Historia y arquitectura de Security Onion
- Requerimientos de Hardware
- Instalación y despliegue de Security Onion en diferentes arquitecturas de servidor.

Administración y configuración de Security Onion

- Análisis de tráfico: Explorar el sniffing y la reproducción de tráfico para la detección de amenazas.
- Gestión de registros y casos: Aprender a utilizar las herramientas de registro y gestión de casos de Security Onion.
- Visibilidad de red y host: Obtener información sobre la visibilidad que ofrece Security

Onion para la red y los hosts.
- Honeypots y detección de intrusiones: Aprender a utilizar honeypots para detectar y analizar intrusiones.

Zabbix con funciones de SOC

- Integración con wazuh
- Configuración de integrator de wazuh
- Dashobard para wasuh
- Integración con netflow
- Instalación de Collector mode
- Dashboard para netflow con grafana
- Integración con netbox
- Registro de hosts automáticos desde netbox
- Envio de alerta de nuevo host registrado