aulaútil

CURSO DE SOC Y MONITOREO

CON SERVIDORES VPS PARA CADA ALUMNO

CENTRO DE CAPACITACIÓN ESPECIALIZADO EN CURSOS DE INFORMÁTICA

CURSOS ALTAMENTE ESPECIALIZADOS EN LINUX, OPEN SOURCE, CLOUD COMPUTING, PROGRAMACIÓN, SEGURIDAD, IA Y TELEFONÍA IP

aulaútil

MG. CLEVER FLORES

MASTER EN PLATAFORMAS OPEN SOURCE

Docente especialista en plataformas Open Source, con amplia experiencia en el diseño, implementación y administración de infraestructuras basadas en tecnologías Linux.

Cuenta con un máster en plataformas Open Source y sólidos conocimientos en soluciones empresariales como Linux, Zimbra, Carbonio, Proxmox y Nextcloud, orientadas a entornos de alta disponibilidad, virtualización y servicios colaborativos.

Posee certificaciones internacionales de alto nivel como LPIC-3, RHCE y CPTE, que respaldan su dominio técnico en administración avanzada de sistemas, seguridad y entornos empresariales.

Su enfoque combina fundamento teórico, buenas prácticas y aplicación práctica en escenarios reales, facilitando un aprendizaje claro, estructurado y alineado a las necesidades actuales del sector tecnológico.

aulaútil

CURSO DE SOC Y MONITOREO OPEN SOURCE CON PFSENSE, GNS 3, ZABBIX, GRAFANA, BUNKERWEB WAF, SECURITY ONION Y WAZUH (72 HORAS)

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

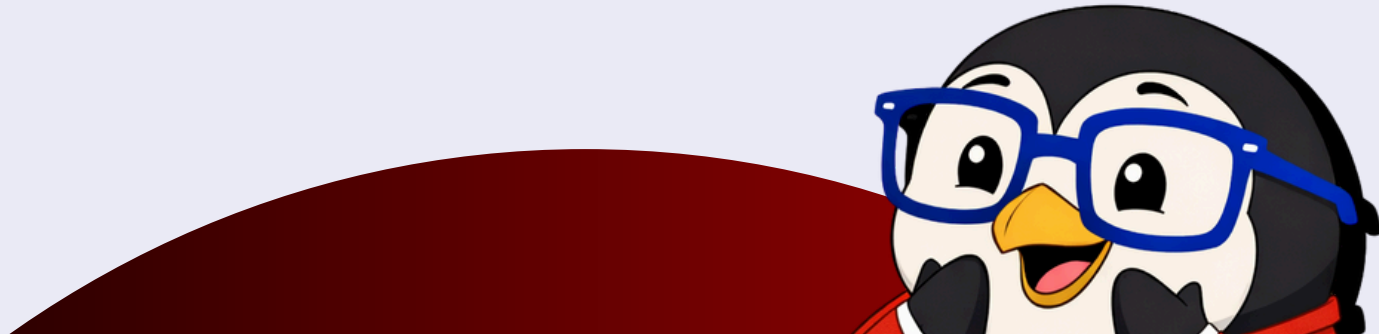
MÓDULO 2: DESPLIEGUE DE ZABBIX Y GRAFANA COMO SOLUCIÓN DE MONITOREO DE INFRAESTRUCTURA

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



aulaútil

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

aulaútil

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

aulaútil

MÓDULO 3: SOC OPEN SOURCE CON WAZUH, SECURITY ONION Y ZABBIX

INTRODUCCIÓN

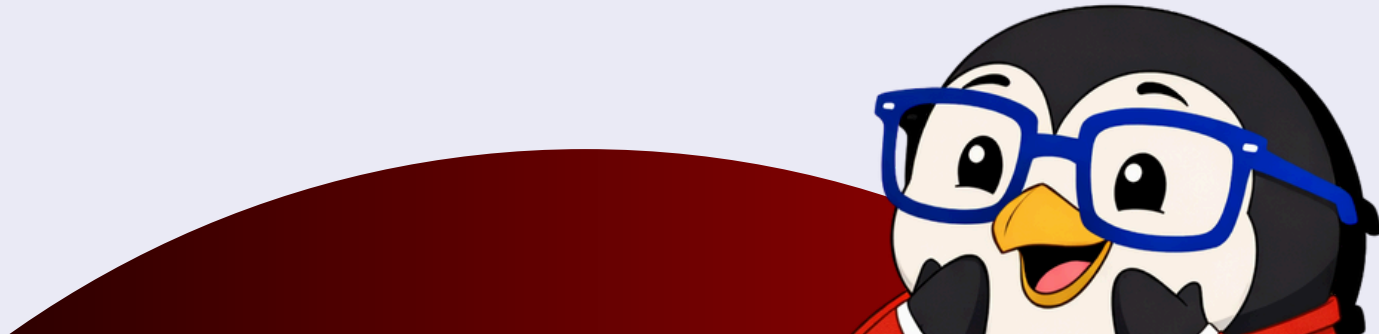
- Soluciones Open Source de Seguridad
- SIEM, IDS, HIDS, NIDS,
- Escanners, Análisis de Vulnerabilidades
- Herramientas de explotación

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



aulaútil

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

EVALUACIÓN FINAL

- Prueba de conocimiento de todo lo aprendido