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 (GNS3 Y PFSENSE): CREACIÓN DE RED Y SERVIDORES VIRTUALES CON GNS3, FIREWALL PFSENSE

INTRODUCCIÓN

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

DESPLIEGUE DE VM KUBUNTU CON GNS3

- Configuración de IP Pública
- Arranque de GNS 3
- Afinamiento de la VM Kubuntu
- Configuración de tarjetas de red
- Instalación de VM Xubuntu en GNS3

INSTALACIÓN Y DESPLIEGUE DE PFSENSE 2.8.1

- Introducción a Pfsense
- Requerimientos de Hardware
- Instalación de pfSense 2.8.0 en GNS 3

- Upgrade de pfSense a 2.8.1
- Configuración de interfaces de red para LAN, WAN
- Despliegue inicial

INSTALACIÓN Y CONFIGURACIÓN DE ACTIVE DIRECTORY

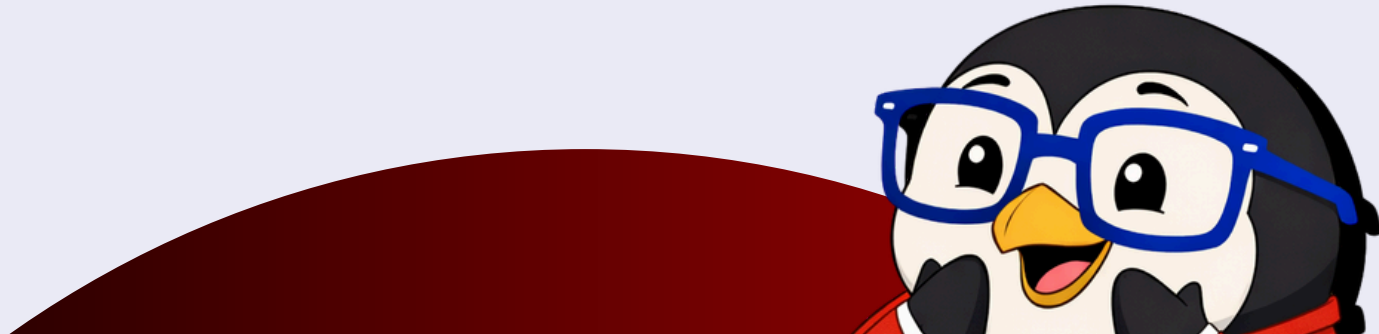
- Instalación de Windows Server 2022
- Instalación y configuración de dominio Active Directory
- Creación de usuarios y grupos
- Instalación de VM Windows 10 en GNS3
- Agregación de Windows al dominio Active Directory

PFBLOQUERNG: FILTRADO DNS E IP

- Firewall DNS e IP
- Configuración de credenciales de bases de datos
- Bloqueo de IPs por GeoIP
- Bloque de IP personalizado
- Configuración de backlist para DNS
- Habilitación de bloqueo DNS por categorías
- Reenvío de solicitudes DNS hacia Unbound
- Pruebas funcionales
- Revisión de Logs

SQUID, SQUIDGUARD: FILTRADO WEB POR CATEGORÍAS Y USUARIOS

- Squid Proxy, configuración inicial
- Instalación de SquidGuard y LigthSquid
- Creación de certificados
- Intercepción SSL (Man In The Middle)



- Proxy Autenticado con usuarios locales
- Proxy Autenticado con Active Directory
- Configuración de políticas de filtrado Web por perfil y categorías
- Creación personalizada de filtrado Web
- Proxy Transparente
- GPO para certificados y proxy en el dominio AD
- Pruebas funcionales
- Revisión de Logs y reportes con LightSquid

SNORT Y OPENAPPID: FILTRADO DE APLICACIONES

- Instalación de Snort y OpenAppId
- Intercepción SSL (dpi) con Squid
- Configuración de filtrado de aplicaciones con OpenAppId
- Reglas a medida
- Pruebas funcionales
- Revisión de Logs

VLANS CON SWITCH CISCO Y PFSENSE

- Instalación de Switch Cisco
- Configuración de VLANs para Servidores y PCs en el switch
- Configuración de VLANs en pfSense
- Reglas para VLANs en pfSense
- Pruebas funcionales
- Revisión de Logs

aulaútil

VPN CON PFSENSE: OPENVPN E IPSEC

- Instalación de sucursal en laptop con Virtualbox y pfSense
- Creación de certificados digitales
- OpenVpn Site 2 Site, reglas para VLANs y VPN
- Auteticación Active Directoy con pfSense
- OpenVpn Móvil, despliegue de clientes
- IPSec Site 2 Site
- Pruebas funcionales
- Revisión de Logs

DMZ CON PFSENSE: WEB SERVER, MAIL SERVER, SURICATA

- Creación de DMZ
- Reglas NAT para http y https
- Instalación de VM Ubuntu en DMZ para servidor Web
- Compra de dominio de internet y configuración de registros DNS
- Despliegue de http y https en Apache
- Despliegue de portal con wordpress
- Certificados letsencrypt
- Protección del Servidor Web con Suricata IPS
- Instalación de Servidor de Correo Carbonio CE en DMZ
- Registros DNS, Reglas NAT para smtp, imap y pop3
- Pruebas funcionales
- Revisión de Logs

aulaútil

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

INTRODUCCIÓN

- Definiciones y Arquitectura de zabbix
- Requerimientos de Hardware

INSTALACIÓN DE ZABBIX, BACKUP, UPGRADE Y BRANDING

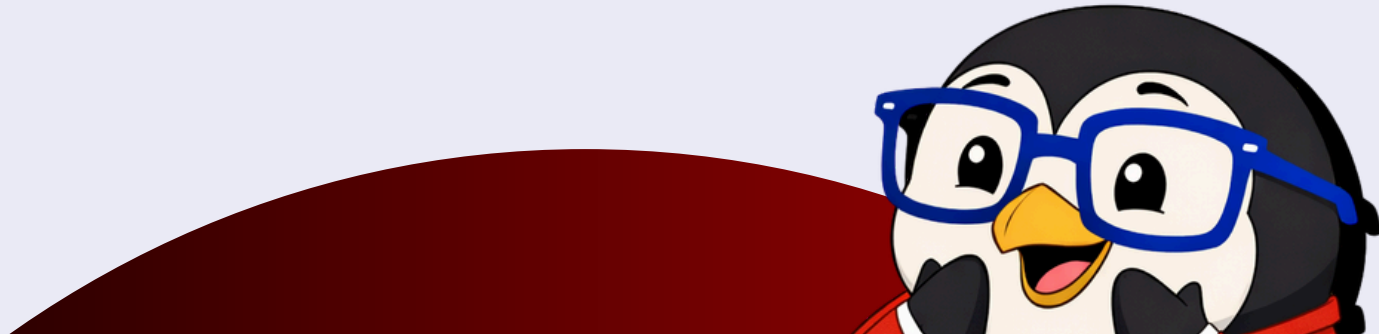
- Instalación de Zabbix 6.0 en Ubuntu 24.04
- Instalación de Zabbix 7.4 en Ubuntu 24.04 de manera distribuida
- Backup y Upgrade de Zabbix 6.0 a 7.4
- Branding de Zabbix

DESCRIPCIÓN DEL FRONTEND DE ZABBIX, HOSTS, USERS, AUTHENTICATION INTERNAL, LDAP (JIT PROVISIONING) Y MFA

- Gestión de User Groups y Users
- Gestión de User roles
- Gestión de Host Groups, Hosts y permissions

GESTIÓN DE TEMPLATES, AGENTS, ITEMS, PREPROCESSING, MACROS Y LLD

- Instalación de agentes y plugins en linux y windows
- Zabbix agent
- Zabbix agent active



- Zabbix trapper
- Calculated
- SNMP agent
- HTTP agent
- External checks
- Dependent item
- Regular expresion
- Replace
- Trim
- Rigth Trim
- Left Trim
- JSONPath
- CSV to JSON
- SNMP walk to JSON
- Custom multiplier
- Simple changue
- JavaScript
- In range
- Discard unchanged
- Discard unchanged with heartbeat
- LLD Discovery

GESTIÓN DE TRIGGERS, REMOTE COMANDS Y ACTIONS

- Triggers: min, max, avg, last, find, changue, count, between, sum y nodata
- Media types: Telegram HTML y Correo en HTML
- Remote comands
- Escalations

aulaútil

GESTIÓN DE DASHBOARDS CON WIDGETS DE ZABBIX

- Geomap
- Item navigator
- Item value
- Host navigator
- Honeycomb
- Gauge
- Graph
- Graph (classic)
- Graph prototype
- Problems by severity
- Top Hosts
- Top items
- Widgets de terceros

ZABBIX CON GRAFANA

- Instalación de Grafana 12.0.1 OSS con PostreSQL
- Integración de Zabbix 7.4 y Grafana 12.0.1
- Desarrollo de dashboard con widgets interactivos y reutilizables basado en variables en Grafana

BONUS

- Certificado SSL para Zabbix server con letsencrypt
- Certificado SSL para Grafana server con letsencrypt
- Configuración de Proxy inverso para Grafana server

aulaútil

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

INTRODUCCIÓN

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

INSTALACIÓN Y DESPLIEGUE DE BUNKERWEB WAF

- Arquitectura de BunkerWeb WAF
- Plugins gratuitos y comerciales
- Requerimientos de Hardware
- Instalación de Servidor BunkerWeb WAF
- Configuración de Ceritifcados digitales
- Configuración de Plugins
- Pruebas de ataques y análisis de Vulnerabilidades
- Logs y Reportes

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.

EVALUACIÓN FINAL

- Prueba de conocimiento de todo lo aprendido