Alonso Eduardo
Caballero Quezada
(ReYDeS)

Curso IDS / IPS con Suricata 2026

2	6	En vivo, Virtual, o Personalizado
Sesiones	Horas	



Alonso Eduardo Caballero Quezada

Tengo más de veintidós años de experiencia, y desde hace dieciocho años realizo capacitaciones y consultorías en Hacking, Forense, OSINT, CiberSeguridad, y GNU/Linux

Redes Sociales

LinkedIn

X (Twitter)

YouTube

Facebook

Sitio Web

e-mail

WhatsApp

Presentación

En el ecosistema de ciberseguridad actual, los endpoints y las aplicaciones web no son los únicos puntos expuestos; la red de una empresa constituye la principal vía crítica donde fluyen las comunicaciones de la misma, como datos sensibles y accesos remotos. Consecuentemente proteger el perímetro y la infraestructura interna exige tener visibilidad en tiempo real, además de una capacidad avanzada para intercepción, superando así las limitaciones de los sistemas pasivos tradicionales.

Este curso intensivo está diseñado y orientado específicamente para administradores de sistemas, ingenieros de redes, y analistas en ciberseguridad, quienes buscan dominar uno de los motores para detección y prevención de intrusiones de fuente abierta más potentes del mercado.

Durante el desarrollo de este curso se aprenderá a desplegar y configurar Suricata en entornos GNU/Linux, aprovechando arquitecturas de alta velocidad basadas en hilos (multithreading), y captura optimizada con AF_PACKET. Se explorará la gestión profesional de fuentes de amenazas mediante suricata-update, integrando bases de firmas líderes como Emerging Threats para la detección temprana de anomalías, escaneos de puertos, y cargas maliciosas.

Se profundiza también en la creación de reglas personalizadas en texto plano, la interpretación de logs estructurados en formato JSON (eve.json) y el diseño de políticas de afinamiento para reducir drásticamente los falsos positivos, utilizando archivos de umbrales y supresión. Finalmente se realizará un salto operativo hacia la prevención activa (Modo IPS Inline), aplicando reglas para descarte de paquetes (drop), con el propósito de contener amenazas en tiempo real.

Al finalizar el curso se tendrá la capacidad técnica indispensable para blindar la red de cualquier organización, automatizar respuestas defensivas, y elevar la postura de ciberseguridad, sin depender de licencias de alto costo.

Alonso Eduardo
Caballero Quezada
(ReYDeS)

Curso IDS / IPS con Suricata 2026

Temario

- ¿Porqué la Seguridad Perimetral Tradicional no Basta?
- Detección Pasiva (IDS) vs. Prevención Activa (IPS)
- Suricata
- Características de Suricata
- Arquitectura Multiprocesamiento de Suricata
- Motores de Captura de Alta Velocidad
- Estructura del Log Unificado
- Prerrequisitos de Red e Infraestructura
- Instalación de Suricata desde Repositorio Oficial (PPA)
- Configuración Inicial de suricata.yaml
- Verificación y Estado del Servicio
- Ecosistema de Reglas: ET Open vs. ET Pro vs. Snort Rules
- La Herramienta suricata-update
- Inspección de Fuentes de Reglas
- Habilitar Fuentes y Actualización de Firmas
- Desactivación y Modificación Automática de Reglas
- Automatización de Actualizaciones mediante Cron Job
- Anatomía de una Regla de Suricata
- Opciones de Regla: Identificadores y Mensajes
- Inspección de Capa de Aplicación: Palabras Clave de Contenido
- Detección de Escaneos de Red y Reconocimiento
- Vigilancia de Alertas en Tiempo Real
- Simulación de Escaneo de Puertos con Nmap
- Detección de Malware y Descargas Inseguras
- Simulación de Descarga de Payload de Prueba
- Declaración e Inclusión de Reglas Locales
- Regla Personalizada 1: Detección de Intento de Exfiltración en Texto Plano
- Regla Personalizada 2: Detección de Agentes de Usuario Maliciosos
- El Desafío de Falsos Positivos en Tráfico de Red
- El Archivo threshold.config (Supresión y Umbrales)
- Configuración Paso a Paso de Exclusiones y Umbrales
- Optimización de Rendimiento del Motor
- Transición del Modo IDS al Modo IPS
- Configuración de IPS mediante AF_PACKET Inline
- Configuración de Reglas con Acción drop
- Simulación de Ataque de Fuerza Bruta SSH y Bloqueo Efectivo

Beneficios

- Acceso al aula virtual por sesenta (60) días
- Acceso a las sesiones en vivo
- Videos de las dos (2) sesiones
- Acceso libre a las sesiones en vivo de los siguientes cursos a dictarse
- Material utilizado durante el desarrollo del curso
- Asesoría personalizada y permanente
- Certificado digital de participación
- Certificado digital de aprobación por una duración total de 16 horas

Inversión

Perú: S/. 225 Soles

- Depósito o transferencia interbancaria a Scotiabank
- Pago mediante YAPE o PLIN

Otros países: $ 75 Dólares

- Pago mediante PayPal

Escriba un mensaje al WhatsApp https://wa.me/reydes para proporcionarle los datos pertinentes.

Información

Para obtener más información sobre este curso tiene a su disposición los siguientes mecanismos de contacto.

WhatsApp: https://wa.me/reydes

Correo electrónico: reydes@gmail.com