E2: PRUEBA PRÁCTICA

Instalar IDS-IPS Suricata

Denominación del curso	IFCT0109. Seguridad Informática	**Código curso:**	23-38/002065
Denominación del MF/ UF	MF0488_3: Gestión de incidentes de seguridad informática	**Fecha:**	19/09/2024
		Duración:	120 minutos
Nombre Docente Examinador	Benito Manuel González Rodríguez	**Firma Docente**	
Nombre y apellido del alumno/a **DNI**		**Firma Alumno**	
		Nota Obtenida	

INTRUCCIONES PARA EL/LA ALUMNO/A

⇨ **DESCRIPCIÓN GENERAL DE LA PRÁCTICA:**

Suricata es un motor de red de alto rendimiento IDS (Intrusion Detection System), IPS y seguridad de red, desarrollado por el OISF, esta es una aplicación de código abierto multiplataforma y es propiedad de una fundación sin ánimo de lucro de la comunidad Open Information Security Foundation (OISF).

1. Descargar e instalar Suricata
2. Configurar la interface de red, directorios y ficheros de reglas.
3. Crea una alerta para detectar paquetes ICMP

Los alumnos deberán realizar correctamente las siguientes tareas:

- Utilizar los parámetros correctos de la herramienta SURICATA.

⇨ **INSTRUCCIONES ESPECÍFICAS:**

TAREA 1.- Descargar e instalar Suricata. Configurar la interface de red, directorios y ficheros de reglas. Crea una alerta para detectar paquetes ICMP.

TAREA 2.- Desarrollar una memoria en procesador de textos en la que se desarrollen los apartados solicitados.

TAREA 3.- Subir la memoria a la plataforma

⇨ **EQUIPO Y MATERIAL:**

En el aula homologada ordenador con conexión a Internet y suite ofimática

⇨ **DURACIÓN DE LA PRUEBA:**

El tiempo estimado de la prueba es de 120 minutos