PPF: PRUEBA PRÁCTICA FINAL

Denominación del curso	IFCT0109. Seguridad Informática	**Código curso:**	23-38/002065
Denominación del MF/ UF	MF0488_3 Gestión de incidentes de seguridad informática	**Fecha:**	27/09/2024
		Duración:	180 minutos
Nombre Docente Examinador	Benito Manuel González Rodríguez	**Firma Docente**	
Nombre y apellido del alumno/a	Jorge Escobar Viñuales	**Firma Alumno**	Jorge Escobar Viñuales
DNI	43835997K	**Nota Obtenida**	

INTRUCCIONES PARA EL/LA ALUMNO/A

⇨ **DESCRIPCIÓN GENERAL DE LA PRÁCTICA:**

Esta actividad evaluable consiste en cuatro apartados. En el primero se solicita el uso de la herramienta Suricata como IDS e IPS. En el segundo utilizar el visor de eventos de Windows para localizar eventos de seguridad y del sistema. En la tercera se trata del uso de la herramienta de firewall OPNsense y en la cuarta sobre las fases de un Plan de incidentes de seguridad.

⇨ **INSTRUCCIONES ESPECÍFICAS:**

La actividad consta de 4 apartados.

1. **Con la herramienta Suricata como IDS/IPS, realizar las siguientes pruebas:**
   a) Detectar conexiones a Facebook
   b) Detectar peticiones GET de Http
   c) Detectar peticiones conexiones SSH
   d) Bloquear acceso a Facebook
   e) bloquear uso de SSH
2. **En Windows comprueba y muestra los registros de seguridad con el visor de eventos, mostrando los detalles de algún evento (**1074. Apagar reiniciar equipo, 4624. Inicio de sesión, 4625. Intento fallido de sesión, 4720. Creación de un usuario, 4657. modificación de valor en el registro, 6008. Cierre inesperado sistema, etc.**).**
3. **Configura la herramienta OPNsense para que, desde una red interna, permita el acceso a la navegación web Internet a un equipo y lo prohíba a otro.**
4. **Nombrar y describir las fases de un Plan de Gestión de Incidentes de Seguridad para una organización**

⇨ **EQUIPO Y MATERIAL:**

En el aula homologada Ordenador con conexión a Internet, navegador y procesador de textos.

⇨ **DURACIÓN DE LA PRUEBA:**

El tiempo estimado de la prueba es de 180 minutos