

**ALTERNATIVA GRATUITA A  
HERRAMIENTAS DE SOC Y SIEM**

**SNORT Y PFSENSE**



## COMUNICADO

### Implementación de Seguridad y Simulación de Ataques con Fines Educativos

Quiero compartir que el proyecto realizado tiene como objetivo enseñar y practicar la **implementación de medidas de seguridad** y la simulación de **ataques informáticos** en un entorno controlado y virtual. La práctica ha sido diseñada para ofrecer una visión más clara de cómo se llevan a cabo las configuraciones de seguridad y cómo responder ante amenazas reales.

Es importante destacar que este entorno es completamente **virtual**, lo que garantiza que no se expongan datos confidenciales ni personales en ningún momento. Todas las simulaciones y configuraciones se han llevado a cabo en sistemas creados específicamente con fines educativos, sin interacciones con redes o datos sensibles.

Cabe mencionar que esta práctica **no incluye todas las configuraciones posibles** ni todas las opciones avanzadas disponibles, sino que es **una introducción a cómo llevar a cabo estas implementaciones** y cómo ponerlas en práctica en un entorno controlado.

El propósito de esta práctica es proporcionar a los estudiantes y profesionales interesados en la **ciberseguridad** una oportunidad de **aprender, experimentar y poner en práctica** conceptos de defensa y ataque, sin ningún riesgo para datos reales o infraestructuras productivas.

Puedes realizar esta práctica si ya has utilizado pfSense o si deseas probar nuevas configuraciones. Además, este documento sirve como una guía para observar cómo se realizan las configuraciones.

## Recursos Necesarios para la Práctica de Implementación de Seguridad y Simulación de Ataques

Para realizar esta práctica educativa en un entorno virtualizado, se requieren los siguientes **recursos y equipos**:

### Equipos Virtuales Requeridos:

#### 1. 1 Equipo con pfSense Instalado:

- Actuarán como **firewall** dentro de la red simulada. **pfSense** se utilizará para gestionar y monitorear el tráfico de red, implementando medidas de seguridad y políticas de protección.

#### 2. 1 Equipo Atacante:

- Este equipo será utilizado para realizar **ataques simulados** hacia los sistemas protegidos por **pfSense**. En el documento, se menciona el uso de herramientas como **SSH** para llevar a cabo ataques de fuerza bruta y pruebas de vulnerabilidad.

### Configuración de Red Virtual:

- **Red interna virtual:** Se recomienda crear una **red interna** o **adaptador puente** para que los equipos puedan comunicarse entre sí dentro del entorno virtualizado, pero sin acceder a la red externa (salvo que sea necesario para ciertas pruebas).

### Requisitos de Software:

- **Sistema operativo para los equipos con pfSense:** **pfSense** debe ser instalado en la máquina virtual. Puedes descargar la ISO desde el sitio oficial de pfSense.
- **Sistema operativo para el equipo atacante:** Se puede utilizar una **distribución Linux** como **Parrot OS** o **Kali Linux**, que ofrece herramientas de **penetración** como **SSH** para realizar ataques simulados.

- **Herramientas de Seguridad:** Además de **Snort** en **pfSense**, es recomendable contar con herramientas de análisis y simulación de ataques, como **Nmap** y **Metasploit** en el equipo atacante.

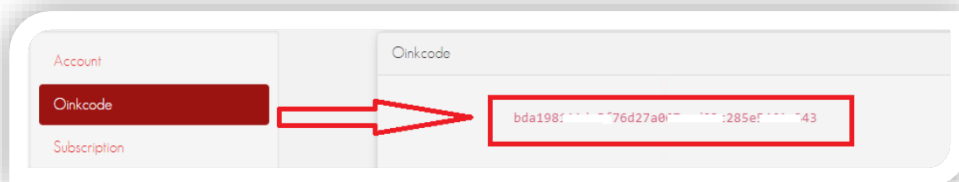
### **Pasos de Configuración del Entorno Virtual:**

1. **Crear 2 máquinas virtuales:**
  - 1 con **pfSense** para simular firewalls.
  - 1 con **Parrot OS** o cualquier distribución de tu elección para el **equipo atacante**.
2. **Conectar las máquinas virtuales** a través de una **red interna** o configurarlas con **adaptador puente** para simular un entorno de red aislado o conectado según sea necesario.

## PASOS PARA CREAR TU IDS CON SNORT EN PFSense Y MONITOREAR ATAQUES EN TIEMPO REAL

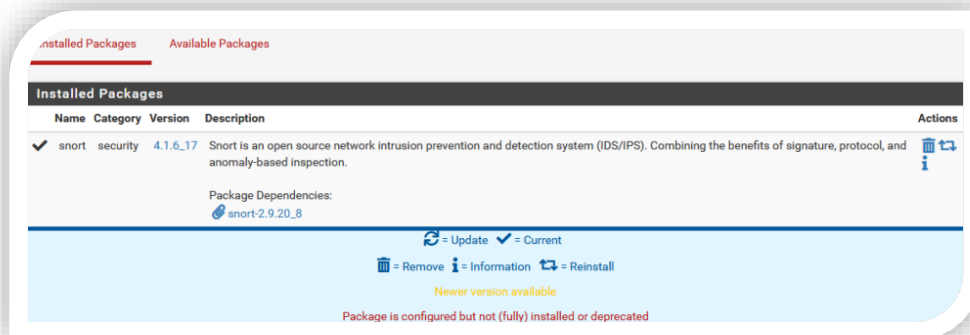
### Paso 1: Registro en Snort

1. Dirígete a la página oficial de **Snort** [aquí](#).
2. Crea una cuenta y obtén tu "**oinkcode**" (código de suscripción) para acceder a las reglas de Snort (En ajustes de tu cuenta podrás encontrar).



### Paso 2: Instalación de Snort en pfSense

1. Accede a la interfaz de administración de **pfSense** desde un navegador.
2. En **pfSense**, ve a **System > Package Manager**.
3. En la pestaña **Available Packages**, escribe "snort" en la caja de búsqueda.
4. Haz clic en **+ Install** al lado de Snort para instalarlo.
5. Una vez instalado, verifica en la pestaña **Installed Packages** que **Snort** se haya agregado correctamente.



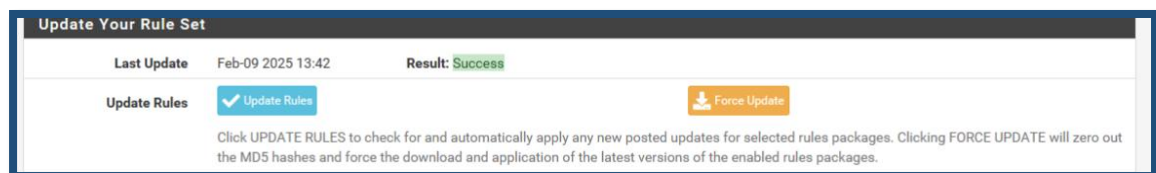
### Paso 3: Configuración Global de Snort

#### En Pfsense

1. Dirígete a **Services > Snort** y selecciona la pestaña **Global Settings**.
2. Marca la casilla **Enable Snort VRT** y, en el campo que aparece debajo, introduce tu **oinkcode**.
3. Marca la casilla **Enable Snort GPLv2** para usar las reglas comunitarias.
4. En **Rules Update Settings**, selecciona el intervalo de actualización como **12 HOURS** y establece el **Update Start Time** a **00:15**.
5. Haz clic en **Save** para guardar la configuración.

### Paso 4: Actualización de las Reglas de Snort

1. Ve a **Services > Snort** y selecciona la pestaña **Updates**.
2. Haz clic en **Update Rules** para actualizar las reglas de Snort. Este proceso puede tomar algunos minutos.
3. Una vez completada la actualización, verás el estado de la actualización como **Success**.



## Paso 5: Configuración de las Interfaces de Snort

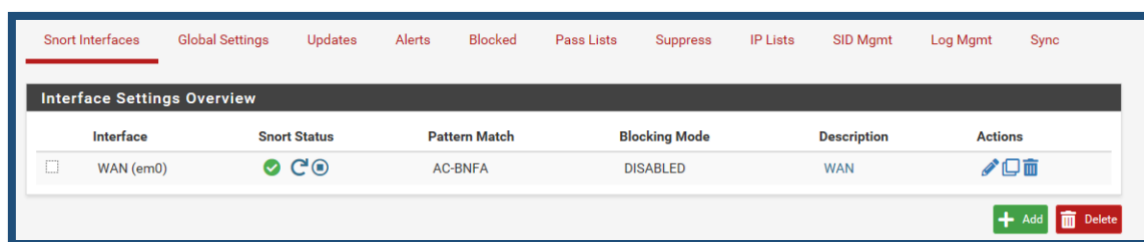
1. Ve a **Services > Snort > Snort Interfaces** y haz clic en **+Add**.
2. En **WAN Settings**, configura las opciones para la interfaz **WAN**:
  - En **Alert Settings**, marca la casilla **Send Alerts to System Log**.
  - Configura el **System Log Facility** como **LOG\_AUTH** y el **System Log Priority** como **LOG\_ALERT**.
3. **No marques** la casilla **Block Offenders** por ahora, ya que necesita una configuración más profunda de las reglas.
4. En **Detection Performance Settings**, deja la opción **Search Method** como **AC-BNFA**.
5. Haz clic en **Save** para aplicar la configuración.

## Paso 6: Configuración de Reglas

1. Dirígete a **Services > Snort > Interface Settings** y selecciona **WAN Categories**.
2. Si no tienes una suscripción de pago, selecciona las reglas de la **Community Rules**.
3. Para un buen balance, selecciona reglas como **snort\_backdoor.rules**, **snort\_browser-chrome.rules**, **snort\_browser-firefox.rules**, **snort\_ddos.rules**, entre otras.
4. Haz clic en **Save**.

## Paso 7: Activación del Interfaz WAN en Snort

1. Ve a **Services > Snort > Snort Interfaces > WAN Settings**.
2. Haz clic en el ícono de **play** para activar el interfaz **WAN**.
3. Asegúrate de que la interfaz esté activa y visible en el panel de configuración de Snort.



## Paso 8: Configuración de Pre-Procesado

1. Dentro de **Services > Snort > Interface Settings**, edita la interfaz **WAN** y ve a la pestaña **WAN Preprocs**.
2. Habilita **Portscan Detection** para todos los protocolos.
3. Habilita **ARP Spoof Detection**.
4. Haz clic en **Save** para guardar los cambios.

## Paso 9: Creación de una Regla Personalizada para Monitoreo de Ataques

1. Dirígete a **Services > Snort > WAN Rules** y selecciona la categoría **custom.rules**.
2. En el cuadro de texto **Defined Custom Rules**, escribe la siguiente regla personalizada para monitorear ataques SSH:

***alert tcp any any -> any 22 (msg: "Alerta de Ataque via SSH"; sid: 33000)***

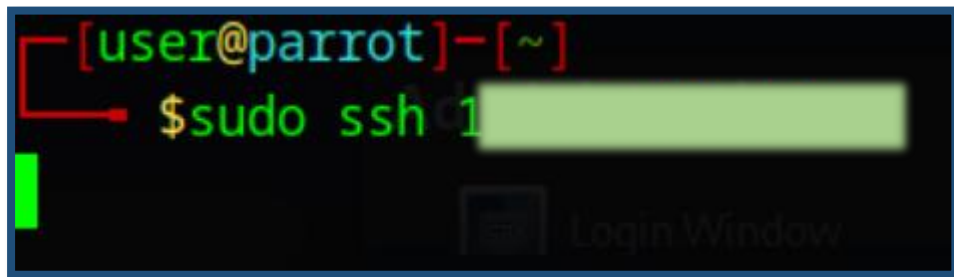
3. Haz clic en **Save** para guardar la regla.



## Paso 10: Simulación de Ataques y Monitoreo de Alertas

En mi caso estoy utilizando un red virtual en la cual tengo dos equipos (PC) en el cual ambos tienen Pfsense instalado y un equipo atacante. He utilizado el equipo atacante para atacar los equipos en la red mediante ssh y posteriormente accedi a los equipos que tienen Pfsense para monitorear y comprobar las políticas de seguridad.

Esta práctica se llevó a cabo con fines educativos, permitiendo simular ataques y aprender a responder adecuadamente ante ellos. Está diseñada para ayudar a quienes no tienen acceso a plataformas de pago, brindándoles la oportunidad de practicar con firewalls y herramientas de IDS como Snort, de manera accesible y efectiva.

A terminal window with a dark background. The prompt is `[user@parrot]-[~]` in green and red. Below it, the command `$sudo ssh 1[redacted]` is entered in green. A green cursor is at the end of the command. In the bottom right corner, there is a faint "Login Window" watermark.

```
[user@parrot]-[~]  
$sudo ssh 1[redacted]
```

Ahora iremos al equipo que tiene instalado Pfsense y veremos lo siguiente:

Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☐ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

9 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-02-09 14:23:44	⚠	0	TCP		[redacted] 5	51566	[redacted]	22	1:33000 ⊕ ✖	Alerta de ataque via SSH
2025-02-09 14:23:36	⚠	0	TCP		[redacted] 5	51566	[redacted]	22	1:33000 ⊕ ✖	Alerta de ataque via SSH
2025-02-09 14:23:32	⚠	0	TCP		[redacted] 5	51566	[redacted]	22	1:33000 ⊕ ✖	Alerta de ataque via SSH
2025-02-09 14:23:30	⚠	0	TCP		[redacted] 5	51566	[redacted]	22	1:33000 ⊕ ✖	Alerta de ataque via SSH
2025-02-09 14:23:29	⚠	0	TCP		[redacted] 5	51566	[redacted]	22	1:33000 ⊕ ✖	Alerta de ataque via SSH
2025-02-09 14:23:28	⚠	0	TCP		[redacted] 5	51566	[redacted]	22	1:33000 ⊕ ✖	Alerta de ataque via SSH
2025-02-09 14:23:27	⚠	0	TCP		[redacted] 5	51566	[redacted]	22	1:33000 ⊕ ✖	Alerta de ataque via SSH
2025-02-09 14:23:26	⚠	0	TCP		[redacted] 5	51566	[redacted]	22	1:33000 ⊕ ✖	Alerta de ataque via SSH