

2º Projeto Prático - Segurança da Informação

Projeto realizado no programa Desenvolve Boticário em parceria com a Alura.

JOÃO LUCAS GOMES PINHEIRO

Este projeto propõe o desenvolvimento e execução de uma segurança de rede, incluindo como componentes principais o firewall, WAF com Nginx, e um SIEM.

Ferramentas e programas utilizados no projeto:

1. Virtualbox;
2. PfSense;
3. Debian;
4. Graylog;
5. Nginx ModSecurity;
6. Snort;
7. Netfilter(iptables)

Planejamento de Segurança:

- **Definir Requisitos de Segurança:**

- **Firewall:** Utilizaremos o Pfsense como firewall para proteger a rede.
- **Zonas Militarizadas e Desmilitarizadas:** Definiremos as zonas DMZ (Demilitarized Zone) para separar os serviços internos e externos da nossa aplicação.
- **WAF:** O WAF deverá ser configurado corretamente para evitar ataque de SQL Injection e XSS(Cross-Site Scripting).

- **Definir Políticas de Segurança Básica para a rede:**

- **Política de Senhas:**
 - **Complexidade:** Senhas devem ter um mínimo de caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais.
 - **Expiração:** Senhas devem ser trocadas periodicamente (ex: a cada 90 dias).
 - **Reutilização:** Proibir a reutilização das últimas senhas usadas.
- **Política de Acesso à Rede:** Implementar através do Firewall recursos que limitem o acesso a certas dependências da aplicação que possa comprometer a integridade da segurança e acesso a dados restritos.
- **Política de Segurança quanto ao monitoramento:** Implementar ferramentas para monitoramento de logs e tentativas de logs para prever ataques de força bruta, ou, qualquer ataque semelhante.

- **Definir Objetivo de Segurança:**

- **Desenvolver e Manter uma Rede Segura:** Garantir que todos os componentes da rede sejam configurados e mantidos de acordo. Isso inclui a implementação de firewalls, sistemas de detecção e prevenção de intrusões, e políticas de acesso rigorosas para minimizar riscos e proteger contra ameaças.

Implementação do Firewall:

Após a preparação do ambiente que inclui baixar e instalar o VirtualBox e importar no VirtualBox os arquivos do PFSense.iso, Debian, configure o IP em cada máquina virtual da seguinte forma:

- Internet: IPv4 DHCP (placa em modo Bridge);
- Server_Web: IPv4 estático: 172.16.10.10/24;
- Graylog: IPv4 estático: 172.16.10.12/24;
- WAF: IPv4 estático: 172.16.20.12/24;

Você pode verificar na máquina virtual do seu firewall PFSense se está de acordo cada IP em sua devida máquina assim que abrir ele:

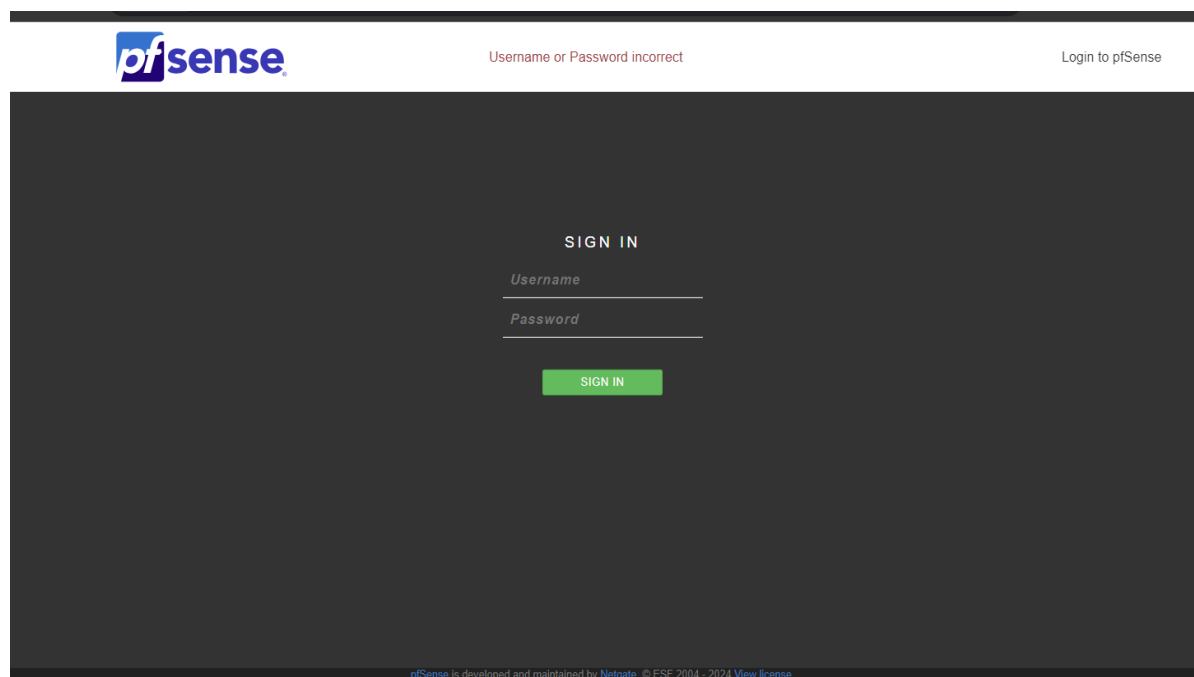
```
Enter an option:
FreeBSD/amd64 (lab.local) (ttyv0)
VM Guest - Netgate Device ID: 7f18f677bfcc3745827e
** Welcome to pfSense 2.7.0-RELEASE (amd64) on lab ***

INTERNET (wan)  -> em0          -> v4/DHCP4:
INTRANET (lan)  -> em1          -> v4: 192.168.56.10/24
DMZ (opt1)      -> em2          -> v4: 172.100.1.10/24
DMZEXT (opt2)   -> em3          -> v4: 172.100.2.10/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Disable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Após a configuração escreva o endereço IP do seu firewall na barra do seu navegador: <http://192.168.56.2>



Informe o usuário e a senha, que vem por padrão usuário: “admin”, senha: “pfsense”.

Configure o firewall:



Regra inicial: É recomendado criar uma regra inicial para bloquear todo o tráfego e, depois, adicionar regras para permitir tráfegos específicos.

- Clicaremos em **Firewall e Rules**. Em cada uma das interfaces, clique em **Add**, altere o campo Action de Pass para Block e o campo Protocol de TCP para Any.
- Clique em **Save** e em **Apply Changes**.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> 	0/22 KIB	IPv4 *	*	*	*	*	*	none		BLOCK GERAL	   

Neste projeto, para simplificar a criação de regras, foram criados aliases para os IPs da interface DMZ e as portas WEB e SSH.

- Navegue até **Firewall, Aliases e IP** e clique em **Add**. Adicione um nome e uma descrição correspondente nos campos **Name** e **Description**, e não altere o campo **Type**. Adicione os seguintes IPs em **Hosts**:
 172.100.1.101 GrayLog
 172.100.1.100 Web
- Clique em **Save** e confirme clicando em **Apply Changes**.

Firewall Aliases IP				
Name	Type	Values	Description	Actions
Update_DMZ	Host(s)	172.100.1.101, 172.100.1.100	Hosts DMZ com liberação para UPDATE	 

* Repita o mesmo processo em **Firewall > Aliases > Ports**, adicionando as portas em **Ports**:

80 HTTP
 443 HTTPS
 22 SSH

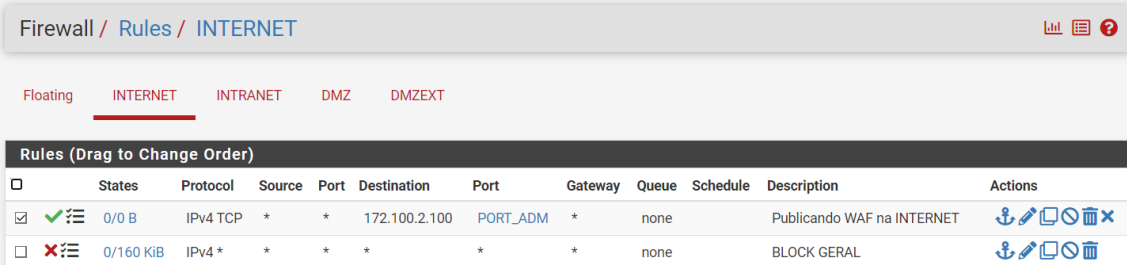
Salve e confirme

Crie regras para permitir o tráfego:

Interface INTERNET

Para que o WAF seja acessível pela internet quando configurado futuramente, siga os passos abaixo para adicionar uma regra na interface INTERNET:

1. Clique em "Add" para criar uma nova regra.
2. No campo "Destination", altere a opção para "Address or Alias".
3. No campo "Destination address", insira o IP 172.100.2.100.
4. Abaixo, no campo "Destination Port Range", insira as portas "WEB 80" e "443".
5. Adicione uma descrição para a regra.
6. Clique em "Save" e depois em "Apply Changes" para salvar e aplicar as alterações.



Firewall / Rules / INTERNET											
Floating INTERNET INTRANET DMZ DMZEXT											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	172.100.2.100	PORT_ADM	*	none		Publicando WAF na INTERNET	
<input type="checkbox"/>	0/160 KiB	IPv4 *	*	*	*	*	*	none		BLOCK GERAL	

Interface INTRANET

Por padrão, o pfSense adiciona uma regra de Anti-lockout na interface INTRANET. Neste projeto, optamos por substituir essa regra por uma personalizada para fins de estudo, embora isso não seja obrigatório. Para replicar essa configuração, siga estes passos:

1. Crie uma nova regra e posicione-a acima da regra de bloqueio existente.
2. No campo "Source", selecione a opção "INTRANET subnets".
3. No campo "Destination", escolha "INTRANET address".

4. No campo "Destination Port Range", insira as portas WEB ou o alias correspondente.
5. Adicione uma descrição para a regra.
6. Clique em "Save" para salvar as alterações.

Para garantir que o firewall não bloqueie o acesso ao WAF, siga os passos abaixo para adicionar uma nova regra:

1. Clique em "Add" para criar uma nova regra.
2. No campo "Source", selecione "INTRANET subnets".
3. No campo "Destination", escolha "Address or Alias" e insira o IP 172.100.1.101 no campo "Destination address".
4. No campo "Destination Port Range", insira a porta 9000.
5. Adicione uma descrição para a regra.
6. Clique em "Save" para salvar as alterações.
7. Confirme as mudanças clicando em "Apply Changes".

Firewall / Rules / INTRANET

Floating

INTERNET

INTRANET

DMZ

DMZEXT

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<div><div></div><div>0/0 B</div></div>	IPv4 TCP	INTRANET subnets	*	172.100.1.101	9000	*	none		Acesso da administração ao Graylog	<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div></div><div>4/2.84 MiB</div></div>	IPv4 TCP	INTRANET subnets	*	INTRANET address	PORT_ADM	*	none		Acesso administrativo do firewall	<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div></div><div>0/0 B</div></div>	IPv4 *	*	*	*	*	*	none		BLOCK GERAL	<div><div></div><div></div><div></div><div></div><div></div></div>

Interface DMZ

Para habilitar atualizações de pacotes e configurações no Graylog e no Server, siga os passos abaixo:

1. Adicione uma nova regra clicando em "Add".
2. No campo "Source", selecione "Address or Alias" e insira o IP do Graylog ou do Server no campo "Source address". Se não houver um alias criado para esses IPs, será necessário criar duas regras separadas. Caso contrário, insira o nome do alias. Neste projeto, o alias é "UPDATE_DMZ".
3. No campo "Destination Port Range", insira as portas WEB ou o alias correspondente.
4. Adicione uma descrição para a regra.
5. Clique em "Save" para salvar as alterações.

Para adicionar uma nova regra para consultas DNS:

1. Clique em "Add".
2. Altere o campo "Protocol" de TCP para UDP.

3. No campo "Source", selecione "DMZ subnets".
4. No campo "Destination", escolha "DNS (53)".
5. Adicione uma descrição para a regra.
6. Clique em "Save" para salvar as alterações.
7. Confirme as mudanças clicando em "Apply Changes".

Firewall / Rules / DMZ

Floating

INTERNET

INTRANET

DMZ

DMZEXT

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>		0/28 KiB	IPv4 UDP	DMZ subnets	*	*	53 (DNS)	*	none	Consulta DNS	
<input type="checkbox"/>		1/411 KiB	IPv4 TCP	Update_DMZ	*	*	PORT_ADM	*	none	Acesso para atualização de pacotes	
<input type="checkbox"/>		0/19 KiB	IPv4 *	*	*	*	*	none		BLOCK GERAL	

Interface DMZEXT

Para habilitar a atualização de pacotes e a configuração no WAF, execute os seguintes passos para adicionar duas regras:

1. Adicione uma nova regra clicando em "Add".
2. No campo "Source", selecione "Address or Alias" e insira o IP 172.100.2.100 no campo "Source address".
3. No campo "Destination", defina as portas WEB ou o alias correspondente no campo "Destination Port Range".
4. Insira uma descrição apropriada para a regra.
5. Clique em "Save" para salvar a regra.

Para permitir consultas DNS, adicione outra regra:

1. Crie uma nova regra clicando em "Add".
2. Alterar o campo "Protocol" de TCP para UDP.
3. No campo "Source", escolha "DMZEXT subnets".
4. No campo "Destination", selecione "DNS (53)".
5. Adicione uma descrição para esta regra e clique em "Save" para salvá-la.

Como o Graylog será usado para coletar logs do WAF, é necessário liberar o tráfego de logs. Para isso, adicione uma nova regra:

1. Clique em "Add" para adicionar a regra.
2. Modifique o campo "Protocol" para UDP.
3. No campo "Source", escolha "Address or Alias" e insira o IP 172.100.2.100 no campo "Source address".
4. No campo "Destination", selecione "Address or Alias" e insira o IP 172.100.1.101 no campo "Destination address".
5. No campo "Destination Port Range", insira a porta 1514.
6. Insira uma descrição para a regra e clique em "Save".

Por fim, para permitir que o WAF envie requisições ao servidor, adicione uma regra adicional:

1. Clique em "Add" para criar a nova regra.
2. No campo "Source", selecione "Address or Alias" e insira o IP 172.100.2.100 no campo "Source address".
3. No campo "Destination", escolha "Address or Alias" e insira o IP 172.100.1.100 no campo "Destination address".
4. No campo "Destination Port Range", selecione "HTTP (80)".
5. Adicione uma descrição para esta regra e clique em "Save" para salvar.

Após adicionar todas as regras, confirme as alterações clicando em "Apply Changes".

Traduza os IPs:

Configuração de NAT

Para garantir que os IPs do Graylog e do WAF sejam reconhecidos na rede, é necessário configurar a tradução de endereços de IP usando o NAT (Network Address Translation). Siga os passos abaixo:

1. Navegue para **Firewall > NAT > 1:1** e adicione dois novos mapeamentos clicando em "Add".
2. **Configuração do Graylog:**
 - Selecione a interface **INTRANET** no campo "Interface".
 - No campo "External subnet IP", defina o "Address" como 192.168.56.11.
 - No campo "Internal IP", defina o "Address" como 172.100.1.101.
 - Insira uma descrição para a regra.
 - Clique em "Save" para salvar as alterações.
3. **Configuração do WAF:**
 - Escolha um IP que esteja na mesma rede da INTERNET e que não esteja em uso. Para verificar a disponibilidade, execute o comando no terminal CMD usando o IP desejado. Neste projeto, o IP selecionado é 192.168.0.110:

```
ping 192.168.0.110
```

- Se não houver resposta, o IP está disponível. Adicione um mapeamento para o WAF mantendo a interface como **INTERNET**.
- No campo "External subnet IP", defina o "Address" para o IP escolhido, 192.168.0.110.
- No campo "Internal IP", defina o "Address" como 172.100.2.100.
- Adicione uma descrição e clique em "Save" para salvar a configuração.

4. Após adicionar ambos os mapeamentos, confirme as alterações clicando em "Apply Changes".

Crie IPs virtuais:

Para garantir o acesso às interfaces do Graylog e do WAF, siga os passos abaixo para adicionar IPs virtuais correspondentes aos IPs traduzidos:

1. **Adicionar IPs Virtuais:**
 - No pfSense, navegue para **Firewall > Virtual IPs**.
 - Clique em "Add" para criar dois novos IPs virtuais.
2. **Configuração do Graylog:**
 - Selecione "IP Alias" como o tipo de IP.
 - Defina a Interface como **INTRANET**.
 - No campo "Address(es)", insira o IP 192.168.56.11/24.
 - Adicione uma descrição apropriada e salve as configurações clicando em "Save".
3. **Configuração do WAF:**
 - Repita o processo para configurar o IP do WAF, mantendo a Interface como **INTERNET**.
 - No campo "Address(es)", insira o IP 192.168.0.110/24, conforme definido anteriormente.
 - Adicione uma descrição para o IP e salve a configuração clicando em "Save".
4. **Aplicação das Alterações:**
 - Após configurar ambos os IPs, aplique as mudanças clicando em "Apply Changes".

Configure os sistemas de detecção e prevenção de intrusões:

1. Instalar o Snort:

- No pfSense, acesse **System > Package Manager > Available Packages**.
- Encontre o pacote **Snort** e instale a versão mais recente disponível.

2. Configuração do Snort:

- Após a instalação, vá para **Services > Snort > Interfaces** e adicione uma nova interface clicando em "Add".
- Selecione **INTERNET (em0)** como a interface e forneça uma descrição.
- Na seção **Alert Settings**, ative as opções **Send Alerts to System Log** para enviar alertas ao Graylog e **Enable Packet Captures** para iniciar a captura de tráfego.
- Salve as configurações clicando em "Save".

3. Ativar o Snort:

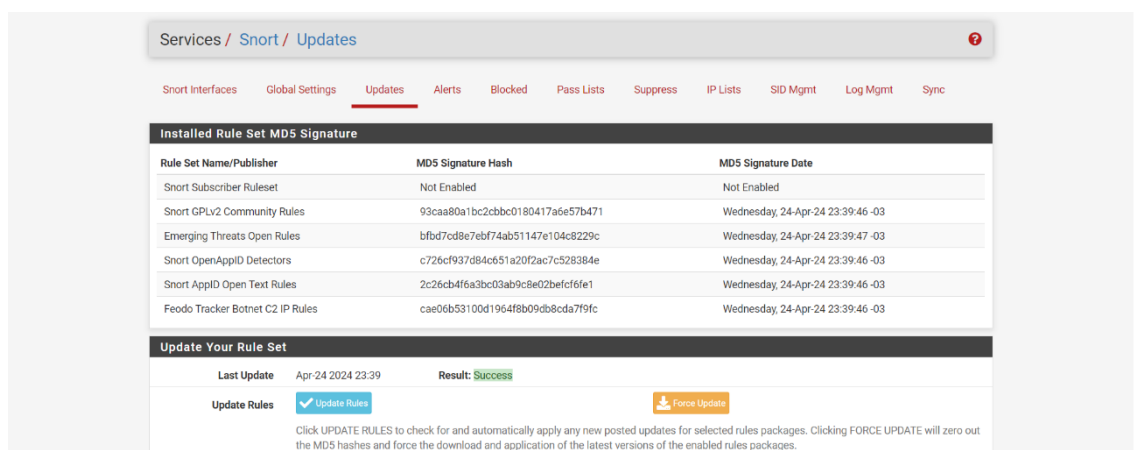
- Habilite o Snort na interface configurada clicando no ícone de "Iniciar" ao lado do status do Snort.

4. Configurar Opções Globais:

- Ajuste as configurações globais conforme necessário em **Services > Snort > Global Settings**.

5. Atualizar Configurações:

- As configurações do Snort podem ser baixadas e atualizadas navegando até **Services > Snort > Updates**.



Services / Snort / Updates

Short Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	93caa80a1bc2cbbc0180417a6e57b471	Wednesday, 24-Apr-24 23:39:46 -03
Emerging Threats Open Rules	bfb7cd8e7ebf74ab51147e104c8229c	Wednesday, 24-Apr-24 23:39:47 -03
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Wednesday, 24-Apr-24 23:39:46 -03
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Wednesday, 24-Apr-24 23:39:46 -03
Feodo Tracker Botnet C2 IP Rules	cae06b53100d1964f8b09db8cda7f9fc	Wednesday, 24-Apr-24 23:39:46 -03

Update Your Rule Set

Last Update: Apr-24 2024 23:39 Result: Success

Update Rules [Update Rules](#) [Force Update](#)

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Configure o Server:

Criação da Máquina Virtual:

- No VirtualBox, crie uma nova máquina virtual com o nome "server" utilizando o arquivo .iso do Debian que você baixou previamente.

Configuração da Rede:

- Após a criação, ajuste as configurações de rede da máquina virtual:
 - **Adaptador 1:**
 - Conectado a: Rede interna
 - Nome: DMZ

Instalação do Debian:

- Inicie a máquina virtual e siga o processo de instalação do Debian. Durante a instalação, desconsidere as configurações de rede.

Configuração do Nome do Host:

- Após a instalação, abra o terminal e execute o seguinte comando para alterar o nome do host:

```
bash  
nano /etc/hostname
```

- Substitua o conteúdo do arquivo por:

```
server
```

- Salve as alterações pressionando Ctrl + O.

Configuração do Servidor DNS:

- Para configurar o servidor DNS, edite o arquivo com:

```
bash  
nano /etc/resolv.conf
```

- Substitua o conteúdo por:

```
nameserver 1.1.1.1
nameserver 1.0.0.1
```

- Salve as alterações pressionando Ctrl + O.

Configuração dos Hosts:

- Edite o arquivo de hosts com:

```
bash
nano /etc/hosts
```

- Substitua o conteúdo por:

```
makefile
127.0.0.1    localhost
172.0.1.1    server.lab    server

# The following lines are desirable for IPv6 capable hosts
::1    localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

- Salve as alterações pressionando Ctrl + O.

Configuração da Rede:

- Configure os IPs editando o arquivo com:

```
bash
nano /etc/network/interfaces
```

- Substitua o conteúdo por:

```
bash
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
```

address 172.100.1.100/24
gateway 172.100.1.10

- Salve as alterações pressionando Ctrl + O.

Atualização e Reinício:

- Atualize as configurações e reinicie o sistema com os seguintes comandos:

```
sql  
update-grub  
reboot
```

Instalação e Ativação do NGINX:

- Para instalar e ativar o servidor NGINX, execute os comandos:

```
bash  
apt update  
apt install nginx  
systemctl enable nginx  
systemctl restart nginx
```

Configure o SIEM:

Criação da Máquina Virtual:

- No VirtualBox, crie uma nova máquina virtual com o nome "Graylog" usando o arquivo .iso do Debian que você já baixou.

Configuração da Rede:

- Após a criação da máquina virtual, ajuste as configurações de rede:
 - **Adaptador 1:**
 - Conectado a: Rede interna
 - Nome: DMZ

Instalação do Debian:

- Inicie a máquina virtual e siga o processo de instalação do Debian. Durante a instalação, ignore as configurações de rede.

Alteração do Nome do Host:

- Após a instalação, abra o terminal e execute o seguinte comando para modificar o nome do host:

```
bash
nano /etc/hostname
```

- Substitua o conteúdo do arquivo por:

```
graylog
```

- Salve as alterações pressionando Ctrl + O.

Configuração do Servidor DNS:

- Configure o servidor DNS editando o arquivo com:

```
bash
nano /etc/resolv.conf
```

- Substitua o conteúdo por:

```
nameserver 1.1.1.1
nameserver 1.0.0.1
```

- Salve as alterações pressionando Ctrl + O.

Configuração dos Hosts:

- Edite o arquivo de hosts com:

```
bash
nano /etc/hosts
```

- Substitua o conteúdo por:

```
makefile
127.0.0.1    localhost
172.0.1.1    graylog.lab  graylog

# The following lines are desirable for IPv6 capable hosts
::1    localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

- Salve as alterações pressionando Ctrl + O.

Configuração da Rede:

- Configure os IPs editando o arquivo com:

```
bash
nano /etc/network/interfaces
```

- Substitua o conteúdo por:

```
bash
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
```

```
source /etc/network/interfaces.d/*
```

```
# The loopback network interface
auto lo
iface lo inet loopback
```

```
# The primary network interface
auto enp0s3
iface enp0s3 inet static
address 172.100.1.101/24
gateway 172.100.1.10
```

- Salve as alterações pressionando Ctrl + O.

Atualização e Reinício:

- Atualize as configurações e reinicie o sistema com os comandos:

```
sql
update-grub
reboot
```

Instalação e Configuração do Graylog:

- Instale o Graylog conforme as instruções fornecidas.
- **Aviso:** Neste projeto, o Debian foi alterado para a versão 11, MongoDB foi instalado na versão 4.2.21 e o Graylog na versão 4.3.
- Acesse a interface do Graylog em <http://192.168.56.11:9000> e faça o login com a senha configurada.
- Para configurar o Graylog como um servidor Syslog, siga as diretrizes da documentação e defina o campo Port como 1514.

Configuração no pfSense:

- No pfSense, vá para o menu Status > System Logs > Settings.

- No campo Remote Logging Options, habilite a opção Send log messages to remote syslog server.
- Defina o Source address como DMZ e adicione o IP 172.100.1.101:1514 em Remote log servers.
- Selecione apenas a opção Firewall Events e clique em Save.

Verificação dos Logs:

- Volte para a interface do Graylog e atualize a página para verificar se os logs do pfSense estão sendo recebidos.

Configure o WAF:

Criação da Máquina Virtual:

- No VirtualBox, crie uma nova máquina virtual com o nome "WAF" usando o arquivo .iso do Debian previamente baixado.

Configuração da Rede:

- Após criar a máquina virtual, ajuste as configurações de rede:
 - **Adaptador 1:**
 - Conectado a: Rede interna
 - Nome: DMZEXT

Instalação do Debian:

- Inicie a máquina virtual e siga o processo de instalação do Debian, ignorando as configurações de rede.

Alteração do Nome do Host:

- Após a instalação, abra o terminal e altere o nome do host com o comando:

```
bash
nano /etc/hostname
```

- Substitua o conteúdo por:

```
waf
```

- Salve as alterações pressionando Ctrl + O.

Configuração do Servidor DNS:

- Configure o servidor DNS editando o arquivo com:

```
bash
nano /etc/resolv.conf
```

- Substitua o conteúdo por:

```
nameserver 1.0.0.1
nameserver 1.1.1.1
```

- Salve as alterações pressionando Ctrl + O.

Configuração dos Hosts:

- Edite o arquivo de hosts com:

```
bash
nano /etc/hosts
```

- Substitua o conteúdo por:

```
makefile
127.0.0.1    localhost
172.100.2.100 waf.lab waf

# The following lines are desirable for IPv6 capable hosts
::1    localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

- Salve as alterações pressionando Ctrl + O.

Configuração da Rede:

- Configure os IPs editando o arquivo com:

```
bash
nano /etc/network/interfaces
```

- Substitua o conteúdo por:

```
bash
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
```

```
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
address 172.100.2.100/24
gateway 172.100.2.10
```

- Salve as alterações pressionando Ctrl + O.

Atualização e Reinício:

- Atualize as configurações e reinicie o sistema com os comandos:

```
sql
update-grub
reboot
```

Instalação e Configuração do ModSecurity + NGINX:

- Instale e configure o ModSecurity e o NGINX seguindo as instruções fornecidas.

Configuração do Envio de Logs para o Graylog:

- Para enviar os logs do WAF para o Graylog, edite o arquivo de configuração do NGINX com:

```
bash
nano /usr/local/nginx/conf/nginx.conf
```

- Adicione as seguintes linhas logo abaixo de `error_log /var/log/nginx/error.log;`:

```
css
access_log syslog:server=172.100.1.101:1514;
error_log syslog:server=172.100.1.101:1514;
```

- Salve as alterações pressionando Ctrl + O.

Verificação da Configuração:

- Confira se a configuração foi adicionada corretamente com o comando:

```
nginx -t
```

- Recarregue o NGINX para aplicar as novas configurações com:

```
nginx -s reload
```

Testes Finais:

- Verifique se o WAF está funcionando corretamente e se os logs estão sendo enviados para o Graylog acessando a interface do WAF através do IP configurado. Realize um teste de ataque, por exemplo:

```
perl  
http://192.168.0.110/?exec=/bin/bash
```