
# Curso Bônus

# Planejando Sua Carreira Para as Profissões do Futuro

# Lab 11 - Configuração de Firewall, Regras de Acesso e SSH


Neste ponto do curso você já tem condições de trabalhar sozinho(a) com Linux, Docker e Kubernetes.

O Lab 11 (que é um bônus dentro do curso de bônus) é para você praticar a configuração de firewall, regras de acesso e SSH no Linux.

Para começar execute os comandos abaixo para criar um container com permissão de uso da rede (NET_ADMIN), instalação do iptables e criação de um usuário com permissão de sudo (admin). O iptables é o principal software de firewall no Linux.

```
docker run -dit --name lab11 --cap-add=NET_ADMIN ubuntu
```

```
apt update -y
```

```
apt-get install iptables openssh-server vim sudo -y
```

```
adduser userdsa
```

```
adduser userdsa sudo
```

su - user1

sudo iptables -L -n

Abaixo estão alguns comandos úteis para configuração de firewall, regras de acesso e SSH no Linux. Vamos abordar o iptables para gerenciamento de firewall, já que é uma ferramenta comum e amplamente utilizada para esse propósito, e os comandos relacionados ao SSH.

**Configuração de Firewall com iptables (execute os comandos com o usuário userdsa e sudo):**

iptables -L: Lista as regras de firewall existentes.

iptables -A INPUT -p [protocolo] --dport [porta] -j ACCEPT: Adiciona uma regra para permitir tráfego para a porta especificada usando o protocolo especificado (por exemplo, tcp ou udp).

iptables -A INPUT -p [protocolo] -s [IP_origem] --dport [porta] -j ACCEPT: Adiciona uma regra para permitir tráfego de um IP específico para a porta especificada usando o protocolo especificado.

iptables -A INPUT -p [protocolo] --dport [porta] -j DROP: Adiciona uma regra para bloquear tráfego para a porta especificada usando o protocolo especificado.

iptables -A INPUT -p [protocolo] -s [IP_origem] --dport [porta] -j DROP: Adiciona uma regra para bloquear tráfego de um IP específico para a porta especificada usando o protocolo especificado.

iptables -D INPUT -p [protocolo] --dport [porta] -j [ação]: Remove uma regra de firewall específica.

iptables-save: Salva as regras de firewall atuais.

iptables-restore: Restaura as regras de firewall salvas.

**Regras de Acesso e SSH (execute os comandos com o usuário userdsa e sudo):**

Para gerenciar regras de acesso e configurações SSH, você precisará editar o arquivo de configuração do SSH, geralmente localizado em /etc/ssh/sshd_config. Aqui estão algumas diretivas comuns que você pode modificar:

Port [número]: Altera a porta padrão do SSH (padrão: 22).

PermitRootLogin [yes/no]: Define se o login como root é permitido via SSH (não recomendado).

PasswordAuthentication [yes/no]: Define se a autenticação por senha é permitida.

PermitEmptyPasswords [yes/no]: Define se senhas vazias são permitidas (não recomendado).

PubkeyAuthentication [yes/no]: Define se a autenticação por chave pública é permitida.

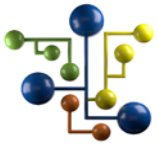
AllowUsers [usuário1] [usuário2] ...: Lista de usuários permitidos para se conectar via SSH.

DenyUsers [usuário1] [usuário2] ...: Lista de usuários negados para se conectar via SSH.

AllowGroups [grupo1] [grupo2] ...: Lista de grupos de usuários permitidos para se conectar via SSH.

DenyGroups [grupo1] [grupo2] ...: Lista de grupos de usuários negados para se conectar via SSH.

Após fazer as alterações desejadas no arquivo /etc/ssh/sshd_config, você precisa reiniciar o serviço SSH para que as alterações entrem em vigor. O Lab 12 a seguir traz os comandos necessários para isso.



**Equipe DSA**

Muito Obrigado!
Continue Trilhando Uma Excelente Jornada de Aprendizagem.