Exercícios UFW vs. iptables

Para cada exercício abaixo, forneça os dois comandos:

1. O comando usando UFW
2. O comando (ou comandos) equivalente usando iptables

Parte 1: Verificação e Políticas Padrão (Exercícios 1-4)

1. Verificar Status:

Como verificar o status atual do firewall e quais regras estão ativas? (em UFW e iptables).

2. Habilitar e Desabilitar:

Como habilitar o UFW? E como desabilitar?

Por que iptables não tem um comando enable/disable simples? O que fazer em vez disso?

3. Política Padrão (Entrada):

Como configurar a política padrão para negar (DROP/DENY) todo o tráfego que entra (INPUT)?

4. Política Padrão (Saída):

Como configurar a política padrão para permitir (ALLOW) todo o tráfego que sai (OUTPUT)?

Parte 2: Liberação Básica por Porta/Protocolo (Exercícios 5-9)

5. Liberar SSH (TCP):

Como permitir conexões de entrada na porta 22/tcp (SSH)?

6. Liberar HTTP (TCP):

Como permitir conexões de entrada na porta 80/tcp (HTTP)?

7. Liberar TCP Porta Alta:

Como permitir conexões de entrada na porta 8080/tcp (uma porta comum para aplicações web/API)?

8. Liberar DNS (UDP):

Como permitir conexões de entrada na porta 53/udp (DNS)?

9. Regras Essenciais (iptables):

Como permitir todo o tráfego na interface de loopback (lo)?

Como permitir o tráfego de conexões já estabelecidas (ESTABLISHED,RELATED)?

Parte 3: Bloqueio e Rejeição (Exercícios 10-12)

10. Bloquear Porta (Deny/Drop):

Como negar (DENY/DROP) explicitamente o tráfego de entrada na porta 3306/tcp (MySQL), fazendo o pacote desaparecer?

11. Rejeitar Porta (Reject):

Como rejeitar (REJECT) explicitamente o tráfego de entrada na porta 5432/tcp (PostgreSQL), informando ativamente ao remetente que a porta está fechada?

12. Bloquear um IP:

Como bloquear todo o tráfego de entrada vindo do endereço IP 1.2.3.4?

Parte 4: Regras Contextuais (IP, Interface) (Exercícios 13-15)

13. Liberar Porta para um IP Específico:

Como permitir o acesso à porta 22/tcp (SSH) apenas para o endereço IP 192.168.1.100?

14. Liberar Porta para uma Interface Específica:

Como permitir o acesso à porta 3306 (MySQL) apenas se a conexão vier da sua rede interna (interface eth1)?

15. Bloquear Pacotes Inválidos (iptables):

Como bloquear pacotes que são considerados INVALID

Parte 5: Gerenciamento de Regras (Exercícios 16-18)

16. Listar Regras com Números:

Como listar todas as regras de entrada (INPUT) com seus respectivos números de linha?

17. Deletar uma Regra por Número:

Usando a lista numerada do exercício anterior, como deletar a regra de número 5 da cadeia de entrada?

18. Resetar Tudo (Flush):

Como resetar o firewall ao seu estado original (limpa todas as regras, contadores e zera as políticas)?

Parte 6: Nível Intermediário (Relevante para Devs) (Exercícios 19-21)

19. Rate Limiting (Proteção contra Força Bruta):

Como proteger o SSH (porta 22) limitando o número de novas tentativas de conexão de um mesmo IP?

20. Logging (Registro de Tentativas):

Como criar uma regra que registra (LOG) todas as tentativas de conexão na porta do seu banco de dados (ex: 5432/tcp) antes de bloqueá-las?

21. NAT / Redirecionamento de Porta (Port Forwarding):

(Cenário de Dev: rodar app na porta 8080, expor na 80)

Como direcionar todo o tráfego que chega na porta 80 do servidor para a porta 8080 local? (Dica: iptables usa a tabela nat).