IFPB
Segurança de Dados
Prof. Dênio Mariz

Exercício: Configurando um firewall no Linux usando o IPTables

Atenção: no final do exercício há instruções de como enviar sua resposta para avaliação

Procedimentos iniciais:

1. Este exercício precisará que outro host seja seu parceiro. Para tanto, você precisará de DOIS hosts (duas VM), sendo uma delas chamada de **HOST_A** e a outra de **HOST_B**. Anote abaixo o endereço IP de cada um dos hosts. Você precisará de acesso privilegiado (de root) aos hosts:

IP_HOST_B	
IP_HOST_A	

2. **Em cada host,** acessar o shell usando o login **root** ou com **sudo**
3. Vamos habilitar alguns serviços no seu host, para poder conduzir o exercício.

```
comando→ sudo su
comando→ apt-get install -y apache2 telnetd nmap curl
```

Exercício 1 – Testando o tráfego

1. Libere o tráfego de entrada no **HOST A**:

```
comando→ iptables -F INPUT
comando→ iptables -A INPUT -p all -j ACCEPT
```

2. Veja as regras do "chain" INPUT no **HOST A**:

```
comando→ iptables -L -n --line-numbers
```

3. A partir do **HOST B** acesse o serviço HTTP no **HOST A**. No **HOST B** usar o comando abaixo

```
curl http://IP_HOST_A
```

4. Observe que o tráfego está liberado, pois o curl recupera a página web

Exercício 2 – Fechando o tráfego HTTP

5. Feche o tráfego de entrada para o serviço HTTP no **HOST A**:

```
comando→ iptables -I INPUT 1 -p tcp --dport 80 -j REJECT
```

6. Veja as regras do "chain" INPUT no **HOST A**:

```
comando→ iptables -L -n --line-numbers
```

7. A partir do **HOST B**, acessar o serviço HTTP no **HOST A** com o comando abaixo:

```
curl http://IP_HOST_A
```

8. O comando conseguiu baixar a página?

Exercício 3 – Fechando o tráfego TELNET

9. A partir do **HOST B**, tentar acessar o serviço TELNET no **HOST A**. Use o seguinte comando:

```
comando→ telnet IP_HOST_A
senha: ****
exit
```

10. O acesso foi bem sucedido?
11. Feche o tráfego de entrada para o serviço TELNET no **HOST A**:
```
comando→ iptables -I INPUT 1 -p tcp --dport 23 -j REJECT
```
12. Veja as regras do "chain" INPUT no **HOST A**:
```
comando→ iptables -L -n --line-numbers
```
13. Repita o acesso telnet a partir do **HOST B** para **HOST A** usando o mesmo comando acima. O acesso foi bem sucedido?

Exercício 4 – Fechando o tráfego ICMP

14. No **HOST B**, fazer o comando abaixo:
```
comando→ ping IP_HOST_A
```
Observe que **o HOST A** responde os pacotes ICMP ECHO-REQUEST com o correspondente ICMP ECHO-REPLY. Mantenha o comando rodando no **HOST B**.
15. Agora feche o tráfego de entrada para os pacotes ICMP no **HOST A**:
```
comando→ iptables -I INPUT 1 -p icmp -j REJECT
```
16. Observe que o comando "ping" do **HOST B** começa a indicar que o seu host está "inalcançável". Isso acontece porque o **HOST A** passou a responder com pacotes do tipo DESTINATION-UNREACHABLE (ao invés de ECHO-REPLY).
17. Veja as regras do "chain" INPUT no **HOST A**:
```
comando→ iptables -L -n --line-numbers
```
18. Remova a regra que impede a entrada de ICMP no **HOST A**:
```
comando→ iptables -D INPUT 1
```
19. Observe que o comando "ping" do **HOST B** volta a obter respostas do **HOST A**.
20. Agora vamos impedir a entrada de pacotes ICMP no **HOST A**, mas de uma maneira diferente. Vamos realmente ***ignorar*** os pacotes ICMP. No **HOST A** use o comando:
```
comando→ iptables -I INPUT 1 -p icmp -j DROP
```
21. Observe que o comando "ping" do **HOST B** agora não recebe qualquer pacote como resposta do **HOST A**.
22. Veja as regras do "chain" INPUT no **HOST A**:
```
comando→ iptables -L -n --line-numbers
```
23. Agora vamos permitir a entrada de pacotes ICMP, mas apenas aqueles que vierem do **HOST B**, mantendo a negação para os demais. Temos que inserir uma regra "DROP icmp", antes da atual regra nº 1. No **HOST A** use o comando abaixo, substituindo o **IP_HOST_B** pelo IP correspondente do **HOST B**.
```
comando→ iptables -I INPUT 1 -p icmp -s IP_HOST_B -j ACCEPT
```

Exercício 5 – Finalizando

24. No **HOST A** salve suas regras
```
comando→ iptables-save > iptables-rules.txt
```
25. No **HOST A** desabilite o firewall
```
comando→ iptables -F INPUT
```
26. No **HOST A** veja que as regras foram removidas:
```
comando→ iptables -L -n --line-numbers
```
27. Caso queira restaurar as regras a qualquer momento ou no próximo boot use o comando:
```
comando→ iptables-restore < iptables-rules.txt
```

Entregando o resultado do exercício:

Faça uma cópia do arquivo **iptables-rules.txt** para outro arquivo que inclui seu nome. Exemplo:

```
comando→ cp iptables-rules.txt joao-iptables-rules.txt
```

Entregue o novo arquivo SEUNOME-iptables-rules.txt com seu nome como resultado da atividade através do upload no formulário do Classroom.