

Após instanciar o Netkit e antes de executar o roteiro do lab, **modifique os endereços MAC eth0 do SERVIDOR e EMPRESAS1** para validar a sua prática. Utilize o seguinte formato, por exemplo:

Se seu R.A. é 123456789 e o MAC eth0 é 3D:6F:00:23:A1:E8, altere o MAC para 3D:6F:00:45:67:89. Faça o mesmo com outra interface usando o R.A. da sua dupla.

Laboratório V - NAT e Firewall

OBJETIVOS DO LABORATÓRIO

- Conhecer o ipables em aplicações de firewall e nat
- Entender as implicações das redes inseguras
- Entender como a internet pode ser distribuída dentro de uma empresa

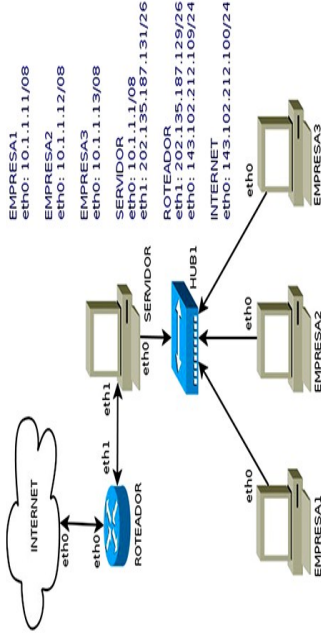
CENÁRIO SENDO REPRODUZIDO

A figura abaixo representa a topologia de rede sendo estudada. A CosmoBooks é uma livraria fundada em 2009 e conta com um acervo local de 1500 títulos de diversos gêneros literários, com disponibilidade de encomendas de títulos que não estão em seu estoque, mas são encomendados e retirados na loja.

Para atender o movimento crescente, o Sr. Joaquim informatizou sua loja e o técnico montou a topologia de rede mostrada na figura a seguir. O computador EMPRESAS1 é o ponto de venda principal, seguido do terminal de consulta EMPRESAS2 disponível aos visitantes. No fundo, existe um terceiro computador, EMPRESAS3, utilizado para a gerência e para a administração do negócio.

Para o compartilhamento da internet, foi utilizado um servidor montado numa velha máquina do proprietário, um K6-II 500 Mhz com 64Mb de RAM, o qual denominamos SERVIDOR. Esta máquina é ligada à internet pelo provedor Festy. Os computadores são ligados em rede por um hub de 8 portas de 100Mbps e cabos categoria 5, devidamente dimensionados. Os possíveis usuários são joaquim, manuel, maria e comprador.


Em nosso laboratório virtual, o provedor é representado pelo “ROTEADOR” e os números de IPs são mostrados. Ao iniciar o laboratório virtual, SERVIDOR e INTERNET se comunicam à vontade.




CONHECIMENTOS DE REDE QUE VOCÊ IRÁ ADQUIRIR

Você irá entender que a segurança de uma rede começa com a escolha de uma topologia e do equipamento adequado e que descuidos podem levar ao vazamento de informações sensíveis.

Iremos entender o que é um firewall e sua configuração básica. Aprenderemos também a criar NATs para que, pela internet, seja possível acessar serviços que estão hospedados em máquinas que não possuem um IP público.




ANTES DE continuar, é importante lembrar que você deve ter feito a instalação do software Wireshark que será utilizado neste lab, portanto use os comandos apt-get install wireshark (distribuições debian) ou rpmi wireshark (mandriva) para instalar este software, caso o mesmo não esteja instalado.



DEVEMOS LEMBRAR que, os comandos marcados com a tag [real] deverão ser executados no console real. Os demais comandos serão executados dentro das máquinas virtuais. Sempre que exigido, a instrução pedirá uma máquina virtual específica.

EXECUÇÃO DO LABORATÓRIO



IMPORTANTE: ANTES de executar este lab, você desejará se preparar com os seguintes requisitos: Este lab requer diversas janelas. Use um ambiente de trabalho com vários espaços, preferencialmente 4 deles. Gnome, Kde, Xfce têm quatro espaços por padrão. Use um deles ou configure seu ambiente preferido para quatro espaços.

1. [real] Salve o arquivo netkit_lab05.tar.gz na sua pasta de labs.
(/home/ seu_nome /nklabs).
 2. [real] Acesse a pasta nklabs a partir do terminal.
[seu_nome @suamaquina ~]\$ cd /home/ seu_nome /nklabs
 3. [real] Use o comando:
[seu_nome @suamaquina ~]\$ tar -xf netkit_lab05.tar.gz
- Será criada a pasta lab05 dentro da sua pasta nklabs.
4. [real] Use o comando a seguir:
[seu_nome @suamaquina ~]\$ **lstart -d /home/ seu_nome /nklabs /lab05**

As seis máquinas virtuais serão iniciadas com as interfaces de rede devidamente configuradas. A internet não está distribuída para os computadores da empresa e os serviços de rede ainda não estão inicializados.

5. [real] Organize suas janelas de modo a localizar qualquer uma delas rapidamente.
6. Tente executar um ping de INTERNET para o SERVIDOR.
INTERNET: ~\$ **ping 202.135.187.131**

O resultado esperado é sucesso na comunicação. Para interromper o ping utilize as teclas Ctrl+C.

7. Tente executar um ping de INTERNET para EMPRESAS2.
INTERNET: ~\$ **ping 10.1.1.12**

O resultado esperado é que a rede não pode ser alcançada.

8. Tente executar um ping a partir do SERVIDOR para INTERNET.
SERVIDOR: ~\$ **ping 143.102.212.100**

O resultado esperado é sucesso na comunicação.

9. Tente fazer o mesmo da EMPRESAS1 para a INTERNET.
EMPRESAS1: ~\$ **ping 143.102.212.100**

O resultado esperado é que os pacotes sejam perdidos. Nada será exibido até que você pressione Ctrl+C para interromper o comando ping.

Devemos lembrar que cada computador permite o acesso de 4 usuários, maria, joaquim, manuel e comprador. As senhas são 123mar, 123joa, 123man e 123com respectivamente.

10. No computador SERVIDOR, use o comando **/etc/init.d/proftpd start**. Isso irá iniciar o servidor de FTP que nesta máquina está configurado para a porta 20.

11. No computador EMPRESAS3, use o comando **/etc/init.d/proftpd start**. Isso irá iniciar o servidor de FTP que nesta máquina está configurado para a porta 21.

12. No computador EMPRESAS1, use o comando **/etc/init.d/ssh start**. Isso irá iniciar o servidor SSH que nesta máquina está configurado para a porta 22.

13. A partir da máquina INTERNET, use o comando **ftp 202.135.187.131 21**. Atenção ao espaço entre 131 e 21.

Isso irá tentar iniciar uma comunicação com o servidor ftp na porta 21 do computador conectado à internet pelo ip acima. Não há serviço na porta 21 deste ip (que é do SERVIDOR) e por este motivo a conexão será recusada. Para sair do programa de ftp, use o comando quit. A conexão com ssh, também na porta 22, também será recusada.

14. A partir da máquina INTERNET, use o comando **ftp 202.135.187.131 20**. Atenção ao espaço entre 131 e 20. No usuário, use manuel e na senha use 123man. Ao conectar, use o comando ls para ver os arquivos disponíveis. Use o comando quit para encerrar o ftp.

Você pode usar help e testar comandos de FTP neste momento se desejar. Essa comunicação poderia ser feita usando um front-end gráfico como o filezilla no entanto.



A PORTA padrão para a comunicação ftp é 21 e ssh 22. A porta do servidor foi modificada para 20 para que seja possível, se desejar, acessar tanto o ftp do servidor, como o do computador EMPRESAS3.

15. No computador SERVIDOR, use o seguinte comando:

```
SERVIDOR:~$ echo 1 > /proc/sys/net/ipv4/ip_forward
```

Este comando irá habilitar o encaminhamento de pacotes ip entre diferentes interfaces de rede. A maioria das principais distribuições não exigem este passo, mas precisamos mostrá-lo. Vai que você se depara com uma que está desativada?

O próximo passo consiste na configuração do firewall iptables do servidor.

16. Use os seguintes comandos no SERVIDOR:

```
SERVIDOR:~$ iptables -F
```

```
SERVIDOR:~$ iptables -F -t nat
```

```
SERVIDOR:~$ iptables -F -t mangle
```

```
SERVIDOR:~$ iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

O iptables é um dos firewalls mais poderosos existentes. Permite a configuração e manipulação dos pacotes na camada de rede ou de transporte, alterando seus headers ou definindo ações. Sua configuração é complexa para ser abordada em poucas páginas, sendo que existem livros especializados em sua configuração.

Em resumo, cada comando no iptables gera uma regra que pode ser alocada em uma das três tabelas. A tabela filter, padrão, que possui as regras de controle sobre os pacotes nas camadas de rede e transporte. A tabela nat regras para a tradução de endereços e a tabela especial mangle para regras especiais.

Quando um pacote entra ou sai da rede, o iptables analisa o pacote e verifica se ele coincide com uma das regras. Ele executará as ações na ordem que elas aparecerem na lista de regras.

O comando “iptables -F” elimina todas as entradas de uma tabela. Se -t não for especificado, ele usará a tabela filter.

Caso contrário usará a tabela especificada. O quarto comando, inclui uma ação “máscarar” na tabela nat para o filtro de pós-roteamento na saída do pacote pela interface eth1. Ou seja, quando o pacote está quase saindo para a internet, ele irá

trocar os ips internos pelo externo, para que o retorno seja efetuado. Quando a resposta volta, o ip é trocado novamente para o ip interno, como se o servidor não existisse no meio do caminho.

17. Tente executar um ping a partir do computador EMPRESAS1 para INTERNET.

```
EMPRESA1:~$ ping 143.102.212.100
```

O resultado agora é sucesso na transmissão. A internet está compartilhada e todas as máquinas da empresa podem acessar páginas disponíveis na internet.

18. Execute os comandos no SERVIDOR:

```
$ iptables -t nat -A PREROUTING -p tcp --dport 21 -j DNAT --to 10.1.1.13
```

```
$ iptables -t nat -A PREROUTING -p tcp --dport 22 -j DNAT --to 10.1.1.11
```

As regras acima acrescentam, cada, uma entrada na tabela nat para que os pacotes enviados para as portas 21 e 22 do endereço público da empresa sejam redirecionadas para os servidores FTP no computador EMPRESAS3 e SSH no computador EMPRESAS1.

19. Execute o comando no SERVIDOR:

```
$ iptables -A INPUT -p tcp --dport 20 -j REJECT
```

Este comando instrui o kernel do sistema operacional para que todo pacote enviado por tcp para a porta 20 seja rejeitado. A ação DROP poderia ser utilizada, ao invés de REJECT para que o pacote fosse descartado silenciosamente sem avisar o remetente do erro de modo que o mesmo não tivesse certeza se o serviço explorado está online.

É uma prática comum usar o comando (não faça agora!!) iptables -A INPUT -s 0.0.0.0/0 -j DROP como última regra, forçando o firewall a descartar tudo que não foi autorizado por regras anteriores. Esta instrução impedia o computador até mesmo de responder ao “ping”.

20. No computador EMPRESAS2 que estava sem uso até agora, ative o tcpdump com o comando:

```
tcpdump -i eth0 -v -n -s 1600 -w /home/lab5.pcap.
```

21. Na máquina INTERNET, use agora o comando **ftp 202.135.187.131** para conectar ao ftp na porta default (21). Utilize o usuário joaquim e a senha 123joa. Faça um comando ls para exibir a lista de arquivos de joaquim e posteriormente um quit encerrando o ftp.

22. Na máquina INTERNET, use agora o comando **ssh manuel@202.135.187.131** para conectar ao ssh na porta default (22). A senha é 123man. Faça um comando ls para exibir a lista de arquivos de Manuel e posteriormente um exit encerrando o ssh.

23. Vá ao computador EMPRESAS2 e use as teclas Ctrl+C para interromper a captura.

24. Estude atentamente o pacote no wireshark. Ele está em sua pasta home com o nome de lab5.pcap.

25. [real] Use o comando a seguir para encerrar a execução do laboratório:

```
[seu_nome@suamaquina ~]$ 1halt -d /home/seu_nome/nk1labs/lab05
```

26. [real] Use o comando a seguir para apagar os enormes arquivos.disk:

```
[seu_nome@suamaquina ~]$ 1c1ean -d /home/seu_nome/nk1labs/lab05
```

Entregue no moodle o arquivo lab5-pcap com o nome no seguinte formato: Firewall-RA-Aluno1-RA-Aluno2-pcap. Cada aluno deve entregar uma cópia do arquivo.

REFERÊNCIA

P. Gurgel, K. R. L. C. Branco, L. H. C. Branco, F. E. Barbosa, and M. M. Teixeira. Redes de

Computadores Da teoria à prática com Netkit. Elsevier, 1ed, 2015.