**Tarefa 5 – NAT e Firewall   
  
A preparação vale 1 ponto na prova 1 (parte Bosco)**

Aluno: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Objetivos do laboratório*

• Conhecer um firewall, utilizando o **iptables** em aplicações de firewall e NAT.

• Entender as implicações das redes inseguras.

• Entender como a Internet pode ser distribuída entre várias máquinas de uma   
 rede local.

*Cenário*

Um ambiente pode ser definido, representando a topologia de rede sendo estudada.   
  
Em nosso laboratório virtual, os números de IPs são mostrados.

Ubuntu Server 11.10 eth0=10.1.1.11 / eth1=192.168.1.254 (Gateway)  
  
Backtrack 5 eth0=10.1.1.13 / eth1=192.168.1.113

Debian 6.0.7 eth0=10.1.1.15 / eth1=192.168.1.115

Windows Server 2008 eth0=10.1.1.16 / eth1=192.168.1.116

O computador Ubuntu faz o papel de um gateway, isto é a máquina por onde se pode entrada e saída para a Internet.

Existe um computador, Backtrack 5, utilizado para a gerência para a administração da segurança da rede.

As máquinas Debian e Windows 2008 são servidores na rede.

Portanto, todas as máquinas estão sujeitas a ataques oriundos da Internet. Neste caso, não estamos supondo ataques internos, provenientes de dentro da própria rede. Imaginaremos um firewall configurado na máquina gateway Ubuntu Server 11.10.

A Internet não está distribuída para todos os computadores e os serviços de rede ainda não estão inicializados.

Para o compartilhamento da Internet, foi utilizado um servidor chamado SERVIDOR, que faz o papel de um ***gateway*** Esta máquina é ligada à Internet

Imagine que os computadores estão ligados em rede por um switch, que no caso é um switch virtual, proporcionado pelo Virtualbox, que você não vê.

Ao iniciar o laboratório virtual, o SERVIDOR Ubuntu 11.10 e a NTERNET se comunicam a vontade.

*Etapas da tarefa*

1. [real] Use Windows 7, o qual contém instalado o Virtualbox com quarto máquinas virtuais (Ubuntu Server 11.10, Backtrack 5, Debian 6.0.7 e Windows Server 2008.

2. [real] Execute o Virtualbox. Visualize as máquinas virtuais.

3. [real] Execute, no Virtualbox cada uma dessas máquinas virtuais.

As quatro máquinas virtuais serão iniciadas com as interfaces de rede devidamente configuradas, no Virtualbox, com seus IPs privados, conforme segue, para os computadores de uma empresa:

4. [real] Você pode organizar quatro janelas de modo a localizar qualquer uma delas rapidamente.

5. Tente executar um ping de INTERNET para o SERVIDOR Ubuntu Server 11.10.

INTERNET:~$ **ping 10.1.1.11 (eth0 em Ubuntu 11.10)**

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

7. Tente executar um ping da INTERNET para Backtrack 5.

**INTERNET:~$ ping 10.1.1.13**

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

8. Tente executar um ping à partir do SERVIDOR Ubuntu 11.10 para a INTERNET

**Ubuntu:~$ ping 150.162.65.42 (esta é a máquina real do professor)**

O resultado esperado é sucesso na comunicação ?

O resultado esperado é nenhum sucesso na comunicação ?

9. Tente fazer o mesmo da Backtrack 5 para a INTERNET

**Backtrack5:~$** **ping 150.162.65.42 (máquina do professor)**

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 máquina virtual permite o acesso de usuários, mas, que, por enquanto, somente 1 usuário está cadastrado com senha. O user name é bosco e sua senhas são: bosco/01031978 ou root/toor, quando for preciso. Você pode usar estas para sua experiência.

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 EMPRESA3, 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 EMPRESA1, 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 a 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 ***bosco*** e na senha use

***01031978***. 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.

 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 EMPRESA3.

No computador SERVIDOR (a VM Ubuntu Server 11.10), use o seguinte comando:

10. **Ubuntu Server 11.10:~$ echo 1 > /proc/sys/net/ipv4/ip\_forward**

Este comando irá habilitar o encaminhamento (redirecionamento) de pacotes IP entre diferentes interfaces de rede das máquinas virtuais.   
  
O próximo passo consiste na configuração do firewall **iptables** no servidor Ubuntu 11.10 (VM1)

11. Estabelecendo o Firewall no servidor Ubuntu Server 11.10

Use os seguintes comandos na VM Ubuntu Server 11.10:

Ubuntu Server 11.10:~$ **iptables -F**

Ubuntu Server 11.10:**~**$ **iptables -F -t nat**

Ubuntu Server 11.10:~$ **iptables -F -t mangle**

Ubuntu Server 11.10**:~**$ **iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**

O **iptables** é um firewall que permite a configuração e manipulação dos pacotes na camada de rede ou de transporte. Assim os protocolos IP, TCP, UDP e ICMP são utilizados, podendo verificar ou alterar os cabeçalhos de endereçamento dos pacotes e definindo ações. Sua configuração é complexa para ser abordada em poucas páginas, sendo que existem livros especializados para sua configuração.

Em resumo, cada comando no **iptables** gera uma regra que pode ser alocada em uma das três tabelas: **filter**, **NAT** e **mangle**. Cada destas tabelas possui, assim, um conjunto de regras, que são consultadas na medida que pacotes passam pelo firewall.

A tabela **filter**, é a padrão, e possui as regras de controle sobre os pacotes nas camadas de rede e transporte. A tabela **nat** tem 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, como segue,

**Ubuntu Server 11.10:~$ iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**

inclui uma ação “**mascarar**” na tabela **nat** para o filtro de pós-roteamento (POSROUTING) na saída do pacote pela interface eth0.   
  
Ou seja, quando o pacote está quase saindo para à Internet, na chain POSTROUTING, ele irá trocar o IP internos privado pelo IP externo, para que o retorno seja efetuado. Quando a resposta volta, o IP é trocado novamente para o IP interno, como se o servidor Ubuntu 11.10 não existisse no meio do caminho.

12. Tente executar um ping partir do computador Backtrack 5, para a Internet (150.162.65.x)

**Backtrack5:~$ ping 150.162.65.x**

O resultado agora deve ser sucesso na transmissão.

A Internet deve ser acessada, através do servidor-gateway Ubuntu 11.10, por qualquer das máquinas virtuais da rede interna, as quais podem acessar páginas disponíveis na Internet. Para tal: estar compartilhada

13. Execute os comandos no SERVIDOR (VM Ubuntu Server 11.10):

**$ iptables -t nat -A PREROUTING -p tcp –i eth0 --dport 21 -j DNAT --to 192.168.1.113**

**$ iptables -t nat -A PREROUTING -p tcp –i eth0 --dport 22 -j DNAT --to 10.1.1.11**

Cada uma das regras acima acrescenta 1 entrada na tabela **nat** para que os pacotes enviados para as portas 21 e 22 sejam redirecionadas para os servidores FTP e SSH no computador Ubuntu.

Não é necessário fazer a **POSTROUTING** via de regra, já que existe a regra de mascaramento no **POSTROUTING** que faz este papel, como regra a seguir:

Ubuntu Server 11.10**:~**$ **iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**

19.Execute o comando no SERVIDOR (VM Ubuntu Server 11.10):

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

Este comando vai instruir 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, poderia ser usada,   
  
$ iptables -A INPUT -p tcp --dport 20 -j DROP

para que o pacote fosse descartado silenciosamente sem avisar o remetente sobre o erro, de modo que o mesmo não tivesse certeza se o serviço explorado está online.

É uma prática comum usar o comando abaixo. Mas, **não faça agora !**$ iptables -A INPUT -s 0.0.0.0/0 -j DROPcomo última regra, forçando o firewall a descartar tudo que não foi autorizado porregras anteriores. Esta instrução impediria o computador até mesmo de responder ao “ping”.

***Formule o que aprendeu***

Lembrando seus conhecimentos sobre NAT, Firewall e segurança.

1. Monte um arquivo com os comandos que executou na tarefa 1 submeta no Moodle, até o final da aula.

1. Como os pacotes são modificados em cada regra do iptables nos comandos

executados neste laboratório?

2. O que aconteceu com o ftp do SERVIDOR ao criar uma regra bloqueando a porta 20?

***Conclusão:***

Usamos algumas regras simples para permitir ou bloquear o acesso de acordo com as portas desejadas e fizemos também bloqueio e compartilhamento na Internet com poucos comandos do iptables.   
  
Um script de firewall, típico, teria muitas linhas a mais para outros serviços que pudessem ser executados, públicos ou privados, e regras para bloqueio para vários ataques conhecidos.

Um ponto forte do uso do firewall linux com iptables é a possibilidade de criar um poderoso firewall, com baixo custo, aproveitando uma máquina obsoleta que rode Linux.