Prova 1 - Parte SEGURANÇA DE REDES – Prof. Bosco – 03/05/2013

Questão 1 (Firewall e NAT) 1,0/5,0

Entregue, impressa, no dia da prova.

Leia com atenção a tarefa e responda os itens (a), (b), (c) e (d), valendo cada 0,25.

A máquina virtual Ubuntu Server 11.10 na rede virtual para tarefas da disciplina, funciona como um servidor-gateway, que estabelece um Firewall Iptables (Linux) nesta máquina.

Os seguintes comandos na VM Ubuntu Server 11.10 são usados:

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 existente no kernel do Linux, que permite a configuração e manipulação dos pacotes na camada de rede ou de transporte. Assim os protocolos IP, ICMP, TCP, UDP são utilizados, e para pacotes deste protocolos, que chegam numa placa de rede, digamos eth0, o firewall pode verificar ou alterar os cabeçalhos de endereçamento desses pacotes e realizar ações. Uma configuração completa do Iptables não pode ser abordada em poucas páginas, sendo que existem livros especializados para sua configuração.

Em resumo, cada comando no **iptables** define uma regra que pode ser alocada em uma das suas três tabelas: **filter**, **NAT** e **mangle**. Cada destas tabelas possui, alguns conjuntos de regras, chamados **chains,** que são consultadas na medida que pacotes passam (entrando ou saindo) no firewall. Cada **chain** define um conjunto de regras que são aplicadas em determinadas situações específicas. O próprio administrador do servidor pode criar suas **chains**, dependendo de sua necessidade., com uma regra:

$iptables –n <nome\_chain\_criada>

 A tabela **filter** é a padrão, e possui as regras para os pacotes nas camadas de rede e transporte. Seus **chains** são: INPUT, FORWARD e OUTPUT. A tabela **nat** tem regras para a tradução de endereços. Seus **chains** são: PREROUNTING, POSTROUTING e OUTPUT. A tabela **mangle** contém regras especiais para pacotes IPv4, quanto ao campo Type Of Service (TOS). Suas **chains** sãoOUTPUT (saída) e PREROUTING. (entrada).

Quando um pacote entra na placa de rede (interface eth0) ou está para sair para a rede, o **iptables** analisa o pacote e verifica se ele coincide com uma das regras de algum **chain** constante na regra. Ele executará as regras na ordem que elas aparecerem na lista de regras e ações como (ACCEPT, DROP, REJECT) são tomadas sobre os pacotes.

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.

a) O quarto comando, é como segue,

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

Explique o que se passa quando esta regra é executada.

<espaço para resposta>

b) Tente imaginar a execução de um comando ping, a partir do computador Backtrack 5, para a Internet (150.162.65.x)

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

O que você espera de resultado, após a execução do deste comando ping.

<espaço para resposta>

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

**$ iptables -t nat -A PREROUTING -p tcp –i eth0 --dport 21 -j DNAT --to 192.168.1.254**

O que acontece quando a regra acima é executada ?

<espaço para resposta>

d) A porta 21 é a padrão para FTP. Supondo que se tenha configurada a porta 20 para FTP no Ubuntu Server 11.10, e que um cliente faça uma tentativa de FTP nesta porta 20, e que no firewall exista a regra a seguir:

Execute o comando no SERVIDOR (VM Ubuntu Server 11.10):
$ iptables -A INPUT -p tcp --dport 20 -j REJECT

Explique o que acontecerá quando a regra acima for executada.

<espaço para resposta>

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.

Também, é uma prática comum usar o comando abaixo.

$ 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 comandos “ping”.

Comentários: Aqui você pode deixar seus comentários sobre a tarefa.