Engenharia de Segurança (SSC -0747)

São Carlos, 26 de Maio de 2010

Prática 6 – Firewall

1. Introdução

Firewalls são dispositivos em uma rede capazes de aplicarem determinadas regras de segurança a mesma, restringindo determinados tipos de tráfego que podem ser considerados nocivos a rede.

Nesta prática configuraremos o IPTables do Linux aplicando algumas regras de filtragem de pacotes.

2. Materiais

Utilizaremos os seguintes materiais:

- Computadores na rede local
- Apache Web Server
- SSH Server

3. Descrição da Prática

Os alunos se dividirão em grupos de 4 pessoas, e cada grupo escolherá um computador do lab conectado a rede interna para configurar e testar o IPTables.

3.1 Listando as Regras do IPTables

Com o usuário 'root' digite o comando

- iptables -L

Para listar as regras de CHAIN INPUT, por exemplo, digite

- iptables -L INPUT

O mesmo pode ser feito com as CHAINS OUTPUT e FORWARD.

3.2 Adicionando Regras

O comando abaixo adiciona uma regra que rejeita pacotes IP na INPUT CHAIN com endereço de destino 192.168.0.10

- iptables -t filter -A INPUT -d 192.168.0.10 -j DROP

Para bloquear o tráfego proveniente da rede 200.100.200.* utilizamos o comando

- iptables -A INPUT -s 200.100.200.0/24 -j DROP

Para bloquear conexões com o destino 10.1.2.3 utilizaremos o comando

- iptables -A OUTPUT -d 10.1.2.3 -j DROP

Para bloquear um protocolo (TCP, UDP, ICMP) utilizaremos a opção -p. O exemplo abaixo ilustra o bloqueio de pacotes udp provenientes do host 200.100.200.123.

- Iptables -A INPUT -s 200.100.200.123 -p udp -j DROP

Para bloquear portas utilizaremos a opção -dport. O exemplo abaixo ilustra o bloqueio da porta 80 dos pacotes provenientes do IP 200.100.200.123 e protocolo tcp.

- iptables -A INPUT -s 200.100.200.123 -p tcp --dport 80 -j DROP

Vale ressaltar que podemos especificar múltiplas portas através de virgula.

Também é possível adicionar uma exceção a regra. O comando abaixo bloqueia todos os pacotes, exceto os que chegam do endereço 200.100.200.100

- iptables -t filter -A INPUT ! -s 200.100.200.100 -j DROP

3.3 Removendo Regras

Para removermos a regra criada anteriormente que rejeita pacotes na INPUT CHAIN com destinatário 192.168.0.10 da tabela do IPTables utilizamos o comando

- iptables -D INPUT -d 192.168.0.10 -j DROP

Engenharia de Segurança (SSC -0747)

São Carlos, 26 de Maio de 1010

Provinha 6 – Firewall

Elaborar os comandos para as seguintes operações, e anotar no relatório.

Anexar a imagem das telas com o teste do SSH e APACHE.

1. Bloquear conexões ICMP de entrada.

2. Bloquear conexões TELNET e FTP de entrada.

3. Liberar o servidor do APACHE rodando na porta default.

4. Liberar o ssh apenas para um IP específico (preferenciamente a máquina ao lado do servidor com o firewall com a finalidade de testes).

5. Bloquear quaisquer conexões com endereço de fonte (source) fora da rede 192.168.181.*