Uso do iptables como ferramenta de firewall.

Rafael Rodrigues de Souza – rafael@tinfo.zzn.com
Administração em Redes Linux
Universidade Federal de Lavra – UFLA

RESUMO

O artigo pretende abordar o uso de firewalls utilizando iptables como ferramenta de implementação. O uso de firewall pode ser aplicado não apenas para proteger pequenas redes locais de ataques provenientes da internet, mas também pode ser usado para estabelecer uma boa política de segurança em uma grande rede de uma grande corporação, levando em consideração a grande quantidade de ameaças por hackers e pragas virtuais que fazem uso de diversas vulnerabilidades dos sistemas faz-se necessário o uso de um número cada vez maior de ferramentas de segurança, o que justifica este o estudo e análise das ferramentas para implementação de segurança como o iptables.

PALAVRAS-CHAVE

computador, segurança de informações, iptables, firewall, linux.

INTRODUÇÃO

Imagine o caso de uma pequena empresa que possua um baixo número de computadores conectados em rede e que esta rede esteja ligada à Internet através de um único ponto de acesso fornecido por um provedor qualquer. Esta situação já é comum, e tende a crescer cada vez mais.
Pense agora numa forma simples de proteger a rede interna desta empresa dos ataques provenientes da Internet: colocar um guarda no ponto de acesso da rede. Este guarda é comumente conhecido como firewall e a sua principal função é controlar o fluxo de informações que passam pelo ponto de acesso, e a maneira de se configurar este guarda se encontra descrito em livros e na Internet.
Porém, será que ao lidar com grandes corporações, que possuem vários computadores e grupos de usuários com privilégios e funções diferentes, a implementação do firewall simples descrito acima é suficiente para proteger toda a rede?
A complexidade da rede vai além do controle apenas do ponto de acesso. Este trabalho passa, principalmente, pelo controle do fluxo de informações dentro da própria corporação, fluxo este que é reflexo da estrutura organizacional da própria corporação. O resultado é que para atender ao fluxo de informações na corporação é necessário um modelo que inclui um firewall e serviços de uma maneira não tradicional.

IPTABLES

O FILTRO DE PACOTES do Linux funciona mediante regras estabelecidas. Todos os pacotes entram no kernel para serem analisados. As CHAINS (correntes) são as situações possíveis dentro do kernel. Quando um pacote entra no kernel, este verifica o destino do pacote e decide qual chain irá tratar do pacote. Isso se chama roteamento interno. Os tipos de chains irão depender da tabela que estaremos utilizando no momento. Existem 3 tabelas possíveis:

- filter: é a tabela default. Quando não especificarmos a tabela, a filter será utilizada. Refere-se às atividades normais de tráfego de dados, sem a ocorrência de NAT. Admite as chains INPUT, OUTPUT e FORWARD.

- nat: utilizada quando há NAT. Exemplo: passagem de dados de uma rede privada para a Internet. Admite as chains PREROUTING, OUTPUT e POSTROUTING.

- mangle: há referências de que a mesma é utilizada para alterações especiais em pacotes. Raramente utilizada.

Vejamos o funcionamento da tabela filter (default) e as suas respectivas chains:

São três, as possíveis chains:

- INPUT: utilizada quando o destino final é a própria máquina firewall;

- OUTPUT: qualquer pacote gerado na máquina firewall e que deva sair para a rede será tratado pela chain OUTPUT;

- FORWARD: qualquer pacote que atravessa o firewall, oriundo de uma máquina e direcionado a outra, será tratado pela chain FORWARD.

REGRAS DE FIREWALL

As regras (rules) de firewall, geralmente, são compostas assim:

#iptables [-t tabela] [opção] [chain] [dados] -j [ação]

Exemplo:
#iptables -A FORWARD -d 192.168.1.1 -j DROP
A linha acima determina que todos os pacotes destinados à máquina 192.168.1.1 devem ser descartados. No caso:
tabela: filter (é a default)
opção: -A
chain: FORWARD

dados: -d 192.168.1.1
ação: DROP
Existem outras possibilidades que fogem à sintaxe mostrada anteriormente. É o caso do comando #iptables -L, que mostra as regras em vigor.

OPÇÕES

As principais opções são:

-P - Policy (política). Altera a política da chain. A política inicial de cada chain é ACCEPT. Isso faz com que o firewall, inicialmente, aceite qualquer INPUT, OUTPUT ou FORWARD. A política pode ser alterada para DROP, que irá negar o serviço da chain, até que uma opção -A entre em vigor. O -P não aceita REJECT ou LOG.

Exemplos:
#iptables -P FORWARD DROP
#iptables -P INPUT ACCEPT

-A - Append (anexar). Acresce uma nova regra à chain. Tem prioridade sobre o -P. Geralmente, como buscamos segurança máxima, colocamos todas as chains em política DROP, com o -P e, depois, abrimos o que é necessário com o -A.

Exemplos:
#iptables -A OUTPUT -d 172.20.5.10 -j ACCEPT
#iptables -A FORWARD -s 10.0.0.1 -j DROP
#iptables -A FORWARD -d www.chat.com.br -j DROP

-D - Delete (apagar). Apaga uma regra. A regra deve ser escrita novamente, trocando-se a opção para -D.

Exemplos:
Para apagar as regras anteriores, usa-se:
#iptables -D OUTPUT -d 172.20.5.10 -j ACCEPT
#iptables -D FORWARD -s 10.0.0.1 -j DROP
#iptables -D FORWARD -d www.chat.com.br -j DROP
Também é possível apagar a regra pelo seu número de ordem. Pode-se utilizar o -L para verificar o número de ordem. Verificado esse número, basta citar a chain e o número de ordem. Exemplo:
#iptables -D FORWARD 4
Isso deleta a regra número 4 de forward.

-L - List (listar). Lista as regras existentes.

Exemplos:
#iptables -L
#iptables -L FORWARD

-F - Flush (esvaziar). Remove todas as regras existentes. No entanto, não altera a política (-P). Exemplos:
#iptables -F
#iptables -F FORWARD

CHAINS

As chains já são conhecidas:

INPUT --> Refere-se a todos os pacotes destinados à máquina firewall.

OUTPUT --> Refere-se a todos os pacotes gerados na máquina firewall.

FORWARD --> Refere-se a todos os pacotes oriundos de uma máquina e destinados a outra. São pacotes que atravessam a máquina firewall, mas não são destinados a ela.

DADOS

Os elementos mais comuns para se gerar dados são os seguintes:

-s --> Source (origem). Estabelece a origem do pacote. Geralmente é uma combinação do endereço IP com a máscara de sub-rede, separados por uma barra.

Exemplo:
-s 172.20.0.0/255.255.0.0

No caso, vimos a sub-rede 172.20.0.0. Para hosts, a máscara sempre será 255.255.255.255.

Exemplo:
-s 172.20.5.10/255.255.255.255

Agora vimos o host 172.20.5.10. Ainda no caso de hosts, a máscara pode ser omitida. Caso isso ocorra, o iptables considera a máscara como 255.255.255.255.

Exemplo:
-s 172.20.5.10

Isso corresponde ao host 172.20.5.10. Há um recurso para simplificar a utilização da máscara de sub-rede. Basta utilizar a quantidade de bits 1 existentes na máscara. Assim, a máscara 255.255.0.0 vira 16. A utilização fica assim:
-s 172.20.0.0/16

Outra possibilidade é a designação de hosts pelo nome. Exemplo:
-s www.chat.com.br

Para especificar qualquer origem, utilize a rota default, ou seja, 0.0.0.0/0.0.0.0, também admitindo 0/0.

-d - Destination (destino). Estabelece o destino do pacote. Funciona exatamente como o -s, incluindo a sintaxe.

-p - Protocol (protocolo). Especifica o protocolo a ser filtrado. O protocolo IP pode ser especificado pelo seu número (vide /etc/protocols) ou pelo nome. Os protocolos mais utilizados são udp, tcp e icmp.

Exemplo:
-p icmp

-i - In-Interface (interface de entrada). Especifica a interface de entrada. As interfaces existentes podem ser vistas com o comando #ifconfig. O -i não pode ser utilizado com a chain OUTPUT.

Exemplo:
-i ppp0

O sinal + pode ser utilizado para simbolizar várias interfaces.

Exemplo:
-i eth+
eth+ refere-se à eth0, eth1, eth2 etc.

-o - Out-Interface (interface de saída). Especifica a interface de saída. Similar a -i, inclusive nas flexibilidades. O -o não pode ser utilizado com a chain INPUT.
! --> Exclusão. Utilizado com -s, -d, -p, -i, -o e outros, para excluir o argumento.

Exemplo:
-s ! 10.0.0.1
Isso refere-se a qualquer endereço de entrada, exceto o 10.0.0.1.

-p ! tcp
Todos os protocolos, exceto o TCP.

--sport --> Source Port. Porta de origem. Só funciona com as opções -p udp e -p tcp.

Exemplo:
-p tcp --sport 80
Refere-se à porta 80 sobre protocolo TCP.

--dport --> Destination Port. Porta de destino. Só funciona com as opções -p udp e -p tcp. Similar a --sport.

AÇÕES

As principais ações são:

ACCEPT --> Aceitar. Permite a passagem do pacote.

DROP --> Abandonar. Não permite a passagem do pacote, descartando-o. Não avisa a origem sobre o ocorrido.

REJECT --> Igual ao DROP, mas avisa a origem sobre o ocorrido (envia pacote icmp unreachable).

LOG --> Cria um log referente à regra, em /var/log/messages. Usar antes de outras ações.

CONCLUSÃO

Apesar de serem extremamente fácil de serem implementados, os firewalls não oferecem sozinhos a segurança absoluta do sistema, seu uso é recomendado, porém como uma ferramenta de segurança adicional e não como a única ferramenta.

BIBLIOGRAFIA

MACHADO , Marcio Pereira. Análise e estudo de segurança de corporações utilizando firewalls, URL: `http://www.modulo.com.br`

MOTA F., João Eriberto. Firewall no Linux, http://www.iptablesbr.cjb.net/