Firewall

Sumário

Índice de tabelas

Índice de Figuras

Capítulo 1

Firewall

- Historia do Firewall,
- Tipos de Firewall;
- Firewall no Linux.

1.1. Mãos a obra

A segurança é um ponto fundamental que o administrador de redes deve-se preocupar hoje em dia. A liberação e bloqueios de acessos, serviços e rotas podem ser feitos através de um Firewall. O muro corta-fogo é uma boa tradução para a palavra “Firewall”, já que a ideia é evitar o alastramento de acessos nocivos dentro de uma rede de computadores. É possível trabalhar com Firewall na forma de software, hardware ou ambos, dependendo do cenário e politica de segurança de sua empresa.

Como o Firewall nasceu?

Final do anos 80 → Com a necessidade de criar restrição de acesso entre as redes existentes, e com a popularização de computadores interligados (Arpanet – Internet);

1988 → Administradores de rede identificaram o que se tornou a primeira grande infestação de vírus de computador e que ficou conhecido como Internet Worm;

1988 → Foi através de pesquisa sustentada pela DEC (Digital Equipment Corporation) que a primeira geração de Firewall (Filtro de pacotes) foi disseminada. O Firewall filtro de pacotes é responsável pela avaliação de pacotes do conjunto de protocolos TCP/IP;

Começo dos anos 90 → Foi através de estudos desenvolvidos pelo Bell Labs (Bell Telephone Laboratories) que a segunda geração de Firewall (Filtro de estado de sessão) foi disseminada. Este tipo de Firewall é responsável por filtrar novas conexões (NEW), conexões já estabelecidas (ESTABLISHED) e conexões relacionadas a outras existentes (RELATED);

1991 → Foi lançado o primeiro Firewall como produto comercial, sendo considerado a terceira geração de Firewall (Gateway de aplicação). Diversos produtos comerciais surgiram e se popularizaram na década de 90;

Inicio do ano 2000 → Considerado como a quarta geração de Firewall, o Firewall pessoal foi aperfeiçoado para ser aplicado em estacões de trabalho. Também temos o surgimento de soluções de Firewall dedicado a servidores e aplicações específicas, como por exemplo servidores Web e banco de dados.

Vamos conhecer os tipos de Firewall

Filtros de Pacotes

Um filtro de pacotes pode elevar o nível de segurança de uma rede por fazer a filtragem nas camadas 3 e 4 do protocolo TCP/IP, ou seja, nos cabeçalhos do IP e dos protocolos da camada de transporte utilizados (TCP, UDP, ICMP e outros)

Proxy Firewall ou Gateways de Aplicação

Os gateways de aplicações conectam as redes corporativas à Internet através de estações seguras (chamadas de bastion hosts) rodando aplicativos especializados para tratar e filtrar os dados (os proxy firewalls).

Stateful Firewall (Firewall de Estado de Sessão)

Firewall que realiza a inspeção total de todas as camadas do modelo ISO/OSI. Esta tecnologia permite decodificar o pacote, interpretando o tráfego sob a perspectiva do cliente/servidor, incluindo técnicas específicas de identificação de ataques.

Firewall de Aplicação

Tipo de Firewall que analisa as particularidades de cada protocolo e toma decisões para evitar ataques maliciosos contra uma rede.

Adm-Firewall

Este tipo de Firewall é usado para o gerecimento da rede da empresa, permitindo inúmeras configurações de acesso, como por exemplo o controle de consumo de banda, regras de acesso a porta, liberação e bloqueios.

Firewall no Linux

Através do Netfilter que é uma funcionalidade do Kernel, podemos controlar o acesso a nossa rede através das “Chains” encontrada em tabelas. O iptables é um binário que funciona como uma especie de Front-End para a manipulação das “Chains” em cada tabela do Netfilter. Conforme a atualização do Kernel este binário também se atualizou.

Kernel versão 2.0 → IPFWADM;

Kernel versão 2.2 → IPCHAINS;

Kernel versão 2.4/2.6 → IPTABLES.

Descrição dos comandos iptables

iptables → Aplicativo principal para protocolos IPV4;

ip6tables → Aplicativo principal para protocolos IPV4;

iptables-save → Usado para salvar as regras inseridas na sessão e ainda na memoria;

iptables-retore → Usado para restaurar as regras salvas pelo comando iptables-save.

Veja abaixo a tabela de parâmetros do iptables

Parâmetros do iptables		**Descrição do parâmetro**
-P	--policy	Estabelece a politica de acesso de uma chain.
-t	--table	Seleciona uma tabela
-A	--append	Adiciona como ultima regra da sequencia de uma chain
-I	--insert	Insere como primeira regra da sequencia de uma chain
-N	--new-chain	Cria uma nova chain
-D	--delete	Remove uma regra
-X	--delete-chain	Elimina todas as regras presentes em chains de usuário
-F	--flush	Elimina todas as regras presentes em uma chain padrão
-s	-source	Determina a origem do pacote
-d	--destination	Determina o destino do pacote
--dport	--destination-port	Define a porta de destino
--sport	--source-port	Define a porta de origem
-i	--in-interface	Define a interface de entrada
-o	--out-interface	Define a interface de saida
-p	--protocol	Seleciona o protocolo (tcp, udp, icmp)
Alvo (target)		**Descrição do alvo**
ACCEPT		O pacote é aceito
REJECT		O pacote é rejeitado imediatamento
DROP		O pacote é negado silenciosamente

Capítulo 2

Gerenciando

2.1. Objetivos

•Trobleshooting: Logs do Firewall .

2.1. Troubleshooting

Como posso configurar a exibição de log com iptables?

Através de um recurso no próprio iptables de nome “LOG”, que quando ativado ativa o “kernel logging” dos pacotes que são submetidos.

Quando esta opção está definida para uma regra, o Kernel irá mostrar algumas informações sobre todos os enquadramento de pacotes da correspondência, através do log do kernel onde pode ser lido através do comando mesg ou uma configuração feita no Rsyslog. Vamos a prática:

Rsyslog

Antes de começar a logar o que acontece no iptables, abra o arquivo de configuração do Rsyslog e adicione um linha para resgistrar os logs no arquivo firewall.log.

```
# vim /etc/rsyslog.conf
```

```
kern.=info                      -/var/log/firewall.log
```

Grave o arquivo e reinicie o Rsyslog

```
# invoke-rc.d rsyslog restart
```

Iptables

Agora vamos criar regras no iptables para registrar no log. Antes de começar a logar o que acontece no iptables, modifique a política padrão para DROP

```
# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
# iptables -P FORWARD DROP
```

Libere o acesso de saída e entrada apenas para a loopback

```
# iptables -A OUTPUT -d 127.0.0.1 -j ACCEPT
# iptables -A INPUT -d 127.0.0.1 -j ACCEPT
```

Libere o acesso de saída e entrada para icmp apenas para sua interface de rede

```
# iptables -A OUTPUT -p icmp --icmp-type 8 -s 192.168.200.10 -d 0/0 -j ACCEPT
# iptables -A INPUT -p icmp --icmp-type 0 -s 0/0 -d 192.168.200.10 -j ACCEPT
```

Vamos registrar no log do iptables tudo o que for informação com DROP para entrada e saída

```
# iptables -A INPUT -j LOG --log-level info --log-prefix "DROP: "
# iptables -A OUTPUT -j LOG --log-level info --log-prefix "DROP: "
```

Em uma outra maquina tente acessar o servidor via ssh, telnet, etc. No servidor acompanhe os logs com o comando tail

```
# tail -f /var/log/firewall.log
```

```
Jan 13 00:55:13 server kernel: [ 2018.418633] DROPIN=eth0 OUT= MAC=08:00:27:66:3
e:ba:00:0f:ea:de:15:e2:08:00 SRC=192.168.200.254 DST=192.168.200.10 LEN=60 TOS=0
x00 PREC=0x00 TTL=64 ID=26880 DF PROTO=TCP SPT=55414 DPT=22 WINDOW=5840 RES=0x00
 SYN URGP=0
```

No Exemplo acima a maquina de origem (SRC) tem sua conexão recusada na porta do SSH (DTP=22) da maquina de destino (DST)