Atividade sobre Segurança 02

(iptables)

iptables é o nome da ferramenta da interface do usuário que permite a criação de regras de *firewall* e NATs. Apesar de, tecnicamente, o iptables ser apenas uma ferramenta que controla o módulo netfilter, o nome "iptables" é frequentemente utilizado como referência ao conjunto completo de funcionalidades do Netfilter. O iptables é parte de todas as distribuições modernas do Linux.

O Netfilter representa um conjunto de ferramentas dentro do kernel do Linux, portanto, permite que os módulos do núcleo específicos para registrar as funções de retorno com a pilha de rede do kernel. Essas funções, geralmente são aplicadas ao tráfego na forma de regras de filtragem e de modificação, são chamados de volta para cada pacote que atravessa a respectiva ferramenta dentro da pilha de rede.

Há uma versão do iptables, chamado de IP6Tables que é usado para configurar, manter e inspecionar as tabelas de regras de filtragem dos pacotes IPv6 no kernel do Linux. Podem ser definidas várias tabelas diferentes. Cada uma contém uma série de cadeias embutidas e pode também conter cadeias definidas pelo usuário. Cada cadeia é uma lista de regras que podem combinar um conjunto de pacotes. Cada regra especifica o que fazer com um pacote que corresponde. Isso é chamado de 'target', que pode ser um salto para uma cadeia definida pelo usuário na mesma tabela.

Fonte: https://pt.wikipedia.org/wiki/Iptables

AS 3 PRINCIPAIS TABELAS DO IPTABLES

Dentro da estrutura do iptables podemos destacar 3 camadas (também chamadas “tabelas”) como as mais importantes para o seu funcionamento: filter, NAT e mangle.

Elas servem para organizar as regras de acordo com sua estrutura, isto é, as tabelas — e as cadeias nelas inseridas — determinarão os pacotes aos quais as regras serão aplicadas.

Quais são as diferenças entre as 3 tabelas aqui mencionadas? As tabelas possuem funções distintas, conforme veremos a seguir.

1. FILTER

As regras contidas na tabela filter determinam a aceitação (ou não) de um pacote, portanto, estamos falando da tabela básica do iptables cujas regras podem ser usadas de modo geral. Dentro dessa camada existem três cadeias:

INPUT – nele somente os pacotes destinados ao IP do computador em questão são avaliados pelas regras, caso elas existam;
OUTPUT – os pacotes avaliados dentro desta regra se limitam aos processos locais do computador;

FORWARD – aqui somente os pacotes repassados pela máquina são avaliados, ou seja, pacotes que não provém dela e nem são destinados a ela.
Quanto às ações que a tabela filter pode aplicar, temos as opções:

REJECT – é aplicada ao pacote correspondente às regras. Quando isso acontece, todas as outras eventuais regras são ignoradas e o pacote é descartado;
ACCEPT – diferentemente do REJECT, esta ação consiste em aceitar o pacote de maneira que ele não venha a ser avaliado posteriormente dentro desta mesma tabela;
DROP – esta ação se assemelha ao REJECT, porém, se diferencia por não enviar mensagem de erro ao remetente. Pode ser a estratégia ideal para quando o firewall está atuando no modo bridge (transparente), visto que o remetente (às vezes um invasor) não identifique a causa do bloqueio ou o IP que está resultando no mesmo;
LOG – a ação LOG consiste apenas em criar registros sobre um pacote, não dando término ao processo de avaliação, ou seja, os pacotes continuam sendo analisados pelas regras.

2. NAT

A tabela NAT (Network Address Translation), como a própria origem do acrônimo nos diz, realiza a tradução dos endereços que passam pelo roteador no qual ela opera.

Essa função pode trazer recursos úteis envolvendo endereços de IP, visto que as características de origem e destino dos pacotes podem ser alteradas. Da mesma forma que a tabela filter, a NAT possui 3 cadeias:

PREROUTING – aplica as regras aos pacotes que entram no firewall, independentemente do seu destino. O nome PREROUTING não se dá por acaso, pois, caso o destino tenha que ser modificado, os parâmetros devem ser ajustados antes do roteamento;
POSTROUTING – na lista PREROUTING estão inseridas as regras capazes de modificar o pacote após o roteamento, ou seja, quando estão saindo do firewall;
OUTPUT – a proposta do OUTPUT é similar a do PREROUTING, sendo a única diferença o fato deste operar pacotes oriundos de processos locais.

Assim como no filter, as ações da tabela NAT também são 4:

SNAT – realiza a troca dos endereços IP de origem;
DNAT – altera os endereços de IP de destino;
MASQUERADE – faz o mascaramento de IP;
REDIRECT – redireciona o pacote para uma porta local.

3. MANGLE

A tabela mangle, por sua vez, tem a função de especificar ações especiais que devem ser aplicadas no tráfego que passa pelas cadeias. No caso, tais ações ocorrem anteriormente aos chains das tabelas filter e NAT.

Para melhor compreendermos esse processo, vamos nos apegar ao fato de que as cadeias da tabela mangle são 5 (PREROUTING, POSTROUTING, INPUT, OUTPUT e FORWARD), isto é, correspondem às cadeias das outras camadas do iptables.

Supondo que a chain INPUT seja acionada na tabela mangle. Isso significa que regras especiais deverão ser aplicadas antes que os pacotes passem pela chain INPUT correspondente à tabela filter.

Vale salientar que a cadeia OUTPUT do mangle corresponde ao OUTPUT da tabela NAT.

CRIANDO REGRAS COM O IPTABLES NO UBUNTU

Agora que você já conheceu as camadas do iptables, vamos tornar essa lição um pouco mais prática: que tal criar uma regra básica para o firewall usando o iptables no Ubuntu? Mas pode ser utilizado em qualquer distribuição LINUX, OK?

Para começar, vamos listar as regras já existentes no iptables:

```
sudo iptables -L
.
```

CRIANDO UMA REGRA

Vamos supor que você queira bloquear o acesso remoto de forma segura usando uma conexão HTTP. Para isso, usa-se a regra:

sudo iptables -A INPUT -p tcp --dport X -j ACCEPT

O “X” no comando refere-se ao número da porta de destino para o pacote correspondente. É mais simples do que parece, não? Mas é preciso tomar cuidado com essas regras, pois elas podem tanto tornar o seu sistema mais protegido como também vulnerável.

Agora, vamos inicialmente instalar o servidor web mais utilizado no mundo, chamado Apache. Para tanto, no terminal digite *sudo apt-get install apache2.* Após a instalação do apache, peça a um colega seu para acessar o seu servidor web através do IP da sua máquina. Por exemplo: se seu ip for 10.17.10.10, ele colocará no navegador http://10.17.10.10.

Agora, crie uma regra para bloquear acessos à porta web (não sabe qual é o número? Não tem problema, você encontrará facilmente na Web). Substituir X pelo número da porta.

```
sudo iptables -A INPUT -p tcp --dport X -j DROP .
```

Agora, peça pra seu colega acessar o seu servidor web novamente.

Questão 1. O que aconteceu? Comente.

Agora, liste a regra criada anteriormente:

```
sudo iptables -L .
```

E então apague a regra criada anteriormente e confirme com os comandos abaixo:

```
sudo iptables -F .
sudo iptables -L .
```

Crie uma nova regra inserido o IP do seu colega no campo apropriado e peça pra ele e mais um colega acessar seu servidor Web.

```
sudo iptables -A INPUT -p tcp -s $IP_A_BLOQUEAR --dport 80 -j DROP .
```

Questão 2. Comente sobre o comportamento observado.

Uma das formas mais utilizadas para saber se uma determinada porta está bloqueada ou não é através do telnet. Por exemplo, peça para seus dois colegas utilizar o comando abaixo:

```
telnet $SEU_IP 80 .
```

Questão 3. Comente sobre o comportamento observado.

Agora, vamos instalar um outro pacote bastante útil no gerenciamento remoto seguro, chamado de SSH. Para tanto, no terminal digite: *sudo apt-get install openssh-server*. Agora, acesse remotamente o computador do seu colega com o comando abaixo:

```
ssh alunos@$IP_DO_SEU_COLEGA .
```

Voilá! Você está acessando remotamente o computador do seu colega e poderá realizar gerenciamento remoto sempre que necessário.

Questão 4. Além de verificar se uma porta está aberta ou não, o telnet também possibilita o acesso remoto. Quais a diferenças entre SSH e Telnet? Pesquise.

Por fim, execute o comando abaixo na sua máquina (preste atenção para não realizar este comando na máquina remota).

```
sudo iptables -A INPUT -j DROP .
```

Questão 5. O que este último comando fez com a conexão SSH? Comente.

Como você provavelmente já sabe, existem dois tipos de mensagens ICMP (echo request e echo reply). O echo request diz respeito à solicitação do ping, enquanto o reply representa a resposta). Quando você não consegue pingar para um determinado host, não significa necessariamente que este host esteja off-line. Ele pode estar simplesmente se protegendo e evitando que você se comunique diretamente com ele através do Ping. Por exemplo, o comando abaixo bloqueia o Ping. *Antes vamos excluir as regras criadas até aqui para que elas não interfiram em nossas futuras regras*.

```
sudo iptables -F .
sudo iptables -I INPUT 1 -p icmp --icmp-type echo-request -j DROP
.
```

Prática nc e Wireshark.