Completo: Curso em vídeo com exemplos práticos + Material de referência exclusivo

H4CK3R

Especial Firewall

Essencial para carreira em TI

Inédito: Mais de uma hora de vídeo ensinando:

* Conceitos gerais de Segurança *Técnicas de Defesa *Programação de Regras *Uso de Patches *Mascaramento e Tabelas NAT *Comandos avançados do Iptables *Utilização de Filtros



Firewall em casa

Pacote de segurança para proteger PCs com Windows e evitar invasões e vírus.

Proteção Invisível

Aprenda a usar um Firewall bridge e reforce a segurança da sua rede ou PC

Tech Bugs

Um guia revelador mostrando as fraquezas dos sistemas de Firewall

Tudo sobre Iptables

Aprenda a usar a melhor ferramenta de segurança para redes Linux

R$ 11,90 Ano III #2
www.digerati.com
ISSN 1677-1680

::curso de segurança digital básico e avançado

universidade H4CK3R

::curso ministrado

Exercícios de defesa e ataque de servidores Linux e Windows

Ideal para administradores de redes e profissionais que desejam trabalhar com segurança digital

Estruturado em hackerismo básico e hackerismo avançado

Curso baseado no livro de informática mais vendido dos últimos 6 meses

Grupos reduzidos para maior interação com o instrutor

Material didático exclusivo

100% PRÁTICO

últimas vagas

*preço promocional: 2xR$180,00

Sobre o instrutor:
Henrique César Ulbrich, autor do livro Universidade H4CK3R, é um profissional com mais de 15 anos de experiência na área de informática, incluindo passagens por empresas como Siemens, Conectiva e Positivo. Foi também sub-editor técnico da revista Info Exame, editor da revista do Linux e dos livros Dossiê Vírus e Dossiê Hardware, da Digerati Books.



Duração: 32horas/aulas
Início: A partir de março de 2004
Horário: 18 às 22 horas
Turmas: (seg, quar e sex) e (ter e qui)

Inscrições por telefone (11) 3217-2600
ou via e-mail para cursos@digerati.com.br
com seus dados para contato
A inscrição será confirmada mediante contato telefônico feito pelo nosso departamento comercial

DIGERATI
education center

Rua Haddock Lobo, 347 – 13º andar
01414-001 – Cerqueira César
São Paulo – SP

*válido somente para as duas primeiras turmas.

ÍNDICE

04 Teoria do Firewall

06 Firewall Anônimo

08 Estratégias para Firewall

11 Tech Bugs

14 IPTables

18 Firewall for Windows

22 Firewall Externo

26 Guia do CD

30 Expediente

Será que o Brasil está virando realmente um laboratório do cybercrime? Esse é o título da matéria que saiu no jornal New York Times, citando inclusive a nossa revista. É realmente difícil acreditar na imprensa não-especializada (na especializada também) quando a discussão é hackerismo e conhecimento avançado em computação. Como as pessoas não conseguem entender a cultura digital, partem para os estereótipos fáceis. Para o NYT, o Brasil é um grande celeiro de criminosos digitais. Por outro lado, para a revista de uma emissora "jovem" de São Paulo, geeks são os tarados pela Rede. São mais estereótipos para um geek: moleque com problemas de relacionamentos pessoais, cheio de espinhas e meio doido. Nada mais longe da realidade.

A diferença está na relação com o conhecimento. A revista H4ck3r não se preocupa em ensinar coisas ilegais, mas também não evita assuntos porque alguém pode usar o conhecimento para coisas ilegais. Então, o negócio é evitar os estereótipos e partir para o estudo sistemático. E nada de se dedicar somente à computação. Há diversos outros assuntos desafiadores esperando respostas.

O Editor

Teoria do fire

Tá certo. Você entende de IP, conhece um ataque DoS e até mesmo sabe como driblar as normas de segurança de um firewall, mas, na hora de explicar, não consegue traduzir em palavras como ou por que a coisa funciona daquela maneira? No problem. Nós, da H4CK3R, explicamos na teoria o que você já sabe na prática - ou ainda vai aprender, ao longo desta edição especial.

Uma rápida evolução

Em primeiro lugar, é preciso entender o que é um firewall e como surgiu essa idéia aplicada a informática. O conceito tem origem na construção civil. No sentido tradicional, é literalmente uma parede não-inflamável ou pouco inflamável sem janelas e colocada entre dois cômodos cuja função é impedir ou dificultar o alastramento do fogo em um incêndio, dando tempo para a atuação dos bombeiros.

Na informática, o termo foi adaptado para designar uma barreira lógica (formada por um único componente ou por um conjunto de componentes) entre duas redes: uma particular e interna, chamada *LAN* (Local Area Network), e outra externa, normalmente a Internet ou o extrato superior de uma rede corporativa. A idéia é proteger a rede local de ataques ("fires") oriundos da rede externa.

Os primeiros firewalls, que eram do tipo network layer firewall (veja mais abaixo o que isso significa), surgiram no final da década de 80. Seu funcionamento, semelhante ao de um roteador atual, tinha como objetivo separar a network em LANs menores. A idéia era evitar que problemas encontrados em uma LAN se propagassem e interferissem no funcionamento de toda a rede.

No início dos anos 90, surgiram os firewalls que atuavam na área de segurança. Um fato, ocorrido no dia 2 de novembro de 1988, parece estar por trás dessa guinada na manutenção das redes. Naquele dia, Peter Yee, da NASA Ames Research Center, enviou uma nota para seu mailing informando sobre o aparecimento, na Internet, do que mais tarde ficou conhecido como o worm Morris. A Web, que em sua infância havia sido confiável, lotada de universidades e pesquisadores, já não era um lugar seguro. Listas de discussão sobre segurança e bugs começaram a surgir e marcam o ciberespaço até hoje.

Esses primeiros firewalls de segurança também eram do tipo network layer. Eles trabalhavam, basicamente, filtrando pacotes IP. Aplicando regras de predefinidas, permitiam que os pacotes seguissem ou não para seus destinatários. Ainda hoje, é mais ou menos como funcionam os firewalls que atuam apenas na camada TCP/IP da informação.

A geração seguinte tornou-se ainda mais flexível e elaborada. Eram firewalls que faziam o papel de *bastion hosts*, ou seja, nós de rede com duas mãos de fluxo que têm a função de *choke points* (pontos através dos quais passa todo o tráfego de uma rede, tanto de entrada quanto de saída). Provavelmente o primeiro firewall comercial desse tipo foi desenvolvido pela Digital Equipment Corporation (DEL) em 1991, e recebeu o nome de SEAL (Secure External Access Link), tendo sido baseado no firewall corporativo da própria empresa. O SEAL usava filtros e proxies.

Em 1993, pelas mãos da Trusted Information Systems (TIS), surgia o Firewall Toolkit (FWTK), que forneceu a base para boa parte das tecnologias usadas hoje na área. Cerca de um ano depois, a Check Point inaugurava, com o Firewall-1, a primeira interface amigável para auxiliar o usuário na configuração, que, antes, era diretamente feita em arquivos ASCII.

Tipificação dos firewalls

Depois dessa rápida olhada na história, resta saber um pouco mais sobre o funcionamento dos diferentes firewalls.

Quanto ao público-alvo:

Firewall "tradicional": software ou hardware que normalmente fica em dispositivo dedicado e que é posicionado entre duas ou mais redes. Estas podem ser, por exemplo, a rede interna (LAN) e a externa ou uma delas e uma terceira camada de rede destinada a aumentar a segurança, a que chamamos *DMZ* (Demilitarized zone).

Personal firewall: um software que normalmente filtra o tráfego que sai ou entra de um único computador.

Quanto à operação:

Packet filtering: a função principal é rotear pacotes baseando-se em endereços e opções dos próprios pacotes via protocolo TCP/IP. Dessa forma, pode bloquear ou permitir a passagem de

ewall

Por João Marinho
joao@digerati.com.br

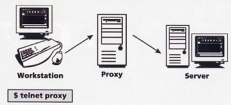
Entenda o conceito por trás do funcionamento desses importantes dispositivos

pacotes IP, refletindo a política de segurança programada pelo administrador. Há três subtipos: static filtering, que contém regras de filtragem que devem, todas, ser mudadas manualmente; dynamic filtering, no qual as regras são alteradas dinamicamente, de acordo com eventos observados pelo componente; stateful inspection, similar à dynamic filtering, mas com um exame mais acurado dos dados dos pacotes. São também chamados de network layer firewalls.

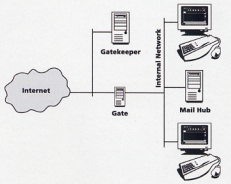
Application gateways (ou application layer firewalls): operam no nível das aplicações, ou seja, no tráfego dos browsers, Telnet e/ou FTP. Interceptam e investigam as requisições provenientes dos diferentes aplicativos e verificam se elas estão de acordo com as regras de segurança antes de passá-los (ou não) para os serviços de fato. São também chamados de proxy-based firewalls ou proxy services. O nome advém do fato que firewalls desse tipo provêm novas conexões em substituição às antigas, atuando como "procuradores" ("proxies") das máquinas protegidas que requisitaram os serviços externos.

Circuit gateways: atuam na camada de transporte da rede e são uma espécie de variação dos application gateways. Enquanto os primeiros interpretam os comandos das aplicações e sabem a quais estão atendendo, estes criam circuitos entre máquinas clientes e servidores sem interpretar os protocolos dos vários aplicativos. Dessa forma, um circuit gateway pode atender a diversos protocolos, enquanto deve existir um proxy-based firewall para cada tipo de serviço que se queira proteger.

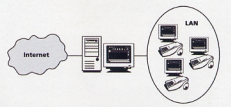
Hybrid firewalls: firewalls que somam duas ou mais características dos tipos anteriores.



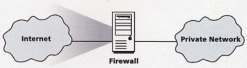
Como atua um circuit gateway



Esquema de funcionamento do DEC SEAL, primeiro firewall comercial (Fonte: Avolio Consulting)



Esquema simplificado da relação entre uma LAN e a Internet



Funcionamento genérico de um firewall

Para saber mais:

www.cisco.com/warp/public/759/ipj_2-2/ipj_2-2_fis1.html
Excelente artigo sobre evolução do firewall

www.dcc.ufmg.br/~mlbc/cursos/internet/firewall/index.html
trabalho contendo conceitos básicos

www.securityfocus.com/infocus/1716
outro artigo sobre evolução dos firewalls e sobre o futuro desses componentes

www.avolio.com/pres/FirewallsHistory_files/frame.html
série de slides que conta a história dos firewalls

Firewall bridg

Como construir um firewall anônimo na rede

Neste artigo, vai ser discutido o princípio de um firewall utilizando o conceito de bridge, para que exista a possibilidade de inserirmos um elemento "secreto" em nossas redes, ou seja, este firewall não vai possuir um endereço de entrada ou saída, sendo praticamente invisível, a não ser por métodos mais avançados. É como aquela velha idéia: você não pega o que não vê, por isso as chances de ter curiosos em nosso firewall serão bem diminuídas, caso ele não possua um endereço visível e constante nas rotas de acesso à nossa rede.

Para começarmos, vamos esclarecer alguns termos :

Firewall, a grosso modo, é um sistema de controle de acesso, mas também de distribuição e proteção.

Bridge pode tanto ser encontrado na forma de hardware, quanto na de software. Hoje em dia, não é tão divulgado quanto há algum tempo atrás, em que protocolos como IPX/SPX das redes netware não podiam ser roteados e quando havia a necessidade de se comunicar entre duas redes ou dois barramentos. Uma bridge basicamente copia um pacote de uma interface para a outra, sem análise ou distinção.

Endereço é o identificador de uma interface, o endereço IP de uma máquina indica a sua localização e é uma das formas de acesso a serviços.

Rotas são artifícios utilizados para organizar os endereços e distribuir as redes que os contém.

Gateway é o computador ou dispositivo que será a entrada/saída padrão de nossa rede. Toda máquina que acessa a Internet tem um gateway padrão e uma rota para ele que vão receber os pacotes destinados para fora da rede. Também chamado de **default gateway**, é geralmente apresentado com o endereço de **0.0.0.0** na tabela de rotas.

Modo promíscuo de uma interface é quando o hardware recebe e aceita todos os pacotes apresentados em seu barramento, sejam direcionados para ela ou não. De modo geral, as interfaces de rede só aceitam o que for direcionado a elas, tendo um filtro em seu hardware para bloquear o resto, já que ela recebe sinais elétricos do barramento todo. Neste caso, mandamos a interface aceitar tudo. Este recurso é usado nos programas do tipo **sniffer** que monitoram e gravam pacotes na rede.

Alguns conceitos já são familiares, mas esta introdução serve para pensarmos neles apenas no aspecto de significado e não de produtos, um erro que pode impedir-nos de criar soluções criativas ou que atendam as necessidades apresentadas. Se pensarmos apenas em termos de produtos, comerciais ou não, vamos esbarrar em nosso conhecimento do produto ou em suas limitações.

A idéia básica de um firewall "invisível" (o invisível vai entre aspas, pois como foi dito anteriormente, existem maneiras de detectá-lo) é termos entre a entrada de nossa rede e o gateway de distribuição, ou até mesmo diretamente entre o roteador e os outros computadores, um dispositivo que filtrará os pacotes, podendo até fazer um proxy transparente de algum protocolo (tal como http), mas sem apresentar um endereço de entrada e um de saída, como estamos acostumados:

(web) -> roteador ->(ip) firewall (ip)-> rede local

A proposta é utilizarmos o conceito de bridge para que nossa máquina copie os pacotes de um lado ao outro (da interface de entrada para a de saída), mas sem a necessidade de novas rotas, sub-redes ou endereços.

(web) -> roteador -> firewall/bridge -> rede local

A desvantagem deste sistema é que não teremos o acesso remoto a não ser que seja incluída uma interface de rede especial para isto, colocada em uma rede à parte. O acesso para a configuração deve ser local.

Claro que existem maneiras de implementar este acesso por qualquer interface, mesmo a de entrada e saída, mas nosso objetivo é um sistema básico, sem muitas complicações para o funcionamento inicial. Fica como sugestão de estudo posterior a implementação deste modo de acesso remoto. O fato de não termos endereços nas interfaces não vai caracterizá-lo como um gateway.

Nosso firewall bridge vai copiar os pacotes de uma entrada à outra, mas aplicando os filtros normais do iptables a cada pacote. O princípio é tão simples, que pode ser executado em outras plataformas, tal como freebsd e openbsd, que possuem este recurso há muito tempo e bem estáveis. O recurso de bridge no Linux começou como um projeto simples e hoje contém drivers no

e "invisível"

Por Gleicon S. Moraes
gsmoraes@terra.com.br

kernel e um programa de configuração.

Além das características que comentamos, esta solução é ideal para quem quer "economizar" endereços IPs ou não quer usar muitas sub-redes apenas para um firewall.

A idéia é setar as duas interfaces em modo promiscuo, de forma que aceitem todos os pacotes presentes em sua entrada e habilitar o bridge, para que estes pacotes sejam copiados. Para isso, devemos ter o forwarding habilitado em nosso kernel e com o iptables, podemos definir regras para este tráfego.

Inicialmente, vamos precisar recompilar o kernel, caso as opções necessárias não estejam disponíveis. São elas:

CONFIG_BRIDGE=y ("802.1d Ethernet bridging") e ("netfilter (firewalling) support")
CONFIG_FIREWALL=y
CONFIG_NET_ALIAS=y
CONFIG_INET=y
CONFIG_IP_FORWARD=y
CONFIG_IP_MULTICAST=y
CONFIG_IP_FIREWALL=y
CONFIG_IP_FIREWALL_VERBOSE=y
CONFIG_IP_MASQUERADE=y

Antes de compilar o kernel, deve-se aplicar o patch bridge-nf, encontrado na URL *http://bridge.sourceforge.net* para acrescentar as funções necessárias.

Todas essas opções estão na sessão Networking da compilação do kernel. Nas documentações das distribuições, geralmente constam os nomes dos pacotes que contêm módulos já prontos e/ou kernel já compilado com estas opções. Consulte-a!

Após esta configuração, tendo certeza de que as placas de rede estão reconhecidas pelo sistema, basta ativar o forwarding no kernel:

```
# echo "1" > /proc/sys/net/ipv4/ip_forward
```

Setar as interfaces para modo promiscuo:

```
# ifconfig eth0 promisc
# ifconfig eth1 promisc
```

E com o programa brcfg:

```
# brcfg -enable
# brcfg -port 0 -enable
# brcfg -port 1 -enable
```

Assim, a bridge estará funcionando e transmitindo. Resta utilizar o iptables para montar suas regras como de costume. Uma sugestão nova é o **ebtables**, que trabalha em um nível mais baixo que o iptables, com opções mais especializadas para estes protocolos (requer patch no kernel também).

Um exemplo de regra:

```
# iptables -I FORWARD -p tcp -s 0.0.0.0/0 -d 10.0.0.1 —dport 22 -j DROP
```

(Bloqueia acessos externos à porta 22 do host 10.0.0.1)

Como não temos interface e a bridge está copiando pacotes, a regra vai no chain FORWARD.

De resto, é só experimentar e testar com o seu setup. Alguns detalhes podem variar de uma distribuição para outra, mas o objetivo deste artigo foi explicar o conceito, podendo ser aplicado diretamente em outras plataformas. Com o FreeBSD, por exemplo, uma vez compilada as opções no kernel (options BRIDGE), basta utilizar o comando sysctl (ou adicionar no /etc/sysctl.conf) :

```
# sysctl -w net.link.ether.bridge=1
# sysctl -w net.link.ether.bridge_cfg=if1,if2
# sysctl net.link.ether.bridge_ipfw=1
```

e seguir utilizando o ipfw para moldar as regras.

Procure na documentação do seu sistema operacional e para entender mais, pesquise em um bom livro sobre redes. Lembrando que mais vale o conceito do que a receita de bolo de um produto.

>> Referências:

http://bridge.sourceforge.net - brcfg, patch para o kernel 2.4.x
http://www.tldp.org/HOWTO/Bridge+Firewall-3.html
http://ebtables.sourceforge.net/
http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/bridging.html - Freebsd handbook

Estratégias para u

Proteger sua rede não é algo difícil

Antes de decidir implementar um firewall, é importante ter o conhecimento de algumas estratégias básicas empregadas na construção destes. Visando uma maior segurança e confiabilidade de seu firewall, resolvi escrever sobre estes métodos que podem e devem ser analisados.

Menor privilégio

O princípio do menor privilégio é aquele que preza por delegar somente os privilégios necessários para que um determinado objeto possa realizar sua função na organização, mas é preciso tomar cuidado para não atribuir privilégios menores que o necessário, pois desta forma, tal objeto não conseguirá realizar suas tarefas. Este método é largamente utilizado, sendo importante para eliminar ou amenizar os danos causados por pessoas mal intencionadas.

"Alguns fabricantes de automóveis configuram suas fechaduras de forma que uma única chave sirva para as portas e a ignição e uma chave diferente sirva para o porta-luvas e o porta-malas, isto é, você pode impor o menor privilégio dando ao manobrista do estacionamento a possibilidade de estacionar o carro sem ter acesso ao que está guardado no porta-malas. Muitas pessoas utilizam chaveiros separados pela mesma razão. Você também pode impor o menor privilégio dando a alguém a chave do seu carro, mas não a chave da sua casa".

Um sistema de filtragem de pacotes projetado para permitir apenas a entrada de pacotes para os serviços necessários é outro exemplo do princípio do menor privilégio. Ele é muito utilizado em grande escala, por sua simplicidade e eficiência.

No contexto de Internet, existem vários exemplos:

- Todo usuário não precisa acessar todos os serviços de Internet existentes;
- Todo usuário não precisa modificar todos os arquivos em seu sistema;
- Todo usuário não precisa saber a senha de root (administrador) da máquina;
- Todo administrador de sistema não precisa conhecer as senhas de root de todos os sistemas;
- Todo sistema não precisa acessar todos os arquivos de outro sistema.

O princípio do menor privilégio sugere que você deve explorar meios para reduzir os privilégios necessários para diversas operações. Por exemplo:

- Não dê a um usuário direitos administrativos de um sistema, se tudo que ele precisa é executar o Apache;
- Não faça um programa ser executado como membro de um grupo altamente privilegiado, se tudo que

m bom firewall

Por: Clayton Kendy Nakahara Passos
netstart@brturbo.com

ele precisa fazer é gravar em um arquivo. Em vez disso, agrupe o arquivo em um grupo e faça o programa ser executado como um membro deste grupo;

- Não faça sua rede interna confiar em um dos firewalls. Em vez disso, faça o firewall confiar na sua rede interna.

Muitos dos problemas de segurança comuns na Internet podem ser evitados com a utilização deste princípio. Por exemplo, o Sendmail é um alvo muito visado pelos atacantes, devido ao fato de que funcionar acoplado ao root e de seu alto nível de complexidade, que aumenta a ocorrência de bugs. Por isso, programas privilegiados devem ser tão simples quanto possíveis. Caso um programa complexo exija privilégios acentuados, devemos procurar meios de separar e isolar as partes que n ecessitam destes privilégios das que não precisam.

Defesa em profundidade

Este princípio de segurança é destinado à prevenção dos acidentes e a minimização das respectivas conseqüências, evitando que um problema isolado se alastre pelo sistema, instituindo múltiplos, redundantes e independentes níveis de proteção. A idéia aqui é não depender de um único método de defesa, instalando vários níveis de proteção, tornando a tentativa de invasão arriscada ou cansativa demais para os atacantes. Isto porque as chances de violar um nível de proteção do sistema são muito maiores do que as chances de violar um sistema com vários níveis de segurança.

Este método já foi utilizado em Salvador no século XVIII, onde as preocupações de defesa se voltaram para o mar, de onde os corsários estrangeiros ameaçavam a cidade. Inútil contra a artilharia da época, a velha muralha (feita de taipa e barro e depois reforçada em pedra e sal) deu lugar a um eficiente sistema de defesa em profundidade, com trincheiras, muralhas e fortificações construídas em lugares estratégicos e armadas de acordo com a evolução da arte da guerra.

Ponto de estrangulamento

Existem muitos exemplos fáceis de citar para se entender este princípio: o guichê de pedágio, o caixa de supermercado ou do banco. O ponto de estrangulamento (choke point) força as pessoas a usarem um meio estreito, para que você possa monitorar o que está ocorrendo.

Normalmente, o firewall em sua rede é esse ponto de estrangulamento; qualquer atacante que desejar entrar em sua rede deve passar obrigatoriamente pelo firewall. Você deve estar preparado para responder a tais ataques.

O planejamento e utilização deste método não compensam se houver outra maneira de um atacante acessar sua rede, que não seja o ponto de estrangulamento. Afinal de contas, de que adianta travar uma batalha contra o firewall se podemos dar a volta, buscando outra maneira de acessar a sua rede? Por isto, garanta um ponto de estrangulamento eficiente.

Simplicidade

Simplicidade é uma estratégia de segurança, pois, manter as coisas mais simples, as torna mais fáceis de se entender. Se algo não é compreendido, não se pode realmente saber se o mesmo é ou não seguro. Programas complexos têm mais bugs, sendo que cada um deles pode constituir um problema de segurança.

Cuidado, não se deve sacrificar a segurança para conseguir simplicidade. A segurança efetiva é complexa por natureza. O importante é manter um sistema que se possa compreender sem perder a segurança e a confiabilidade.

Obscuridade

Manter a segurança através da obscuridade é um princípio nada confiável, pois consiste unicamente em ocultar coisas. Exemplos práticos deste método são:

- Colocar uma máquina na Internet e achar que ninguém tentará invadi-la, simplesmente porque você não contou a ninguém sobre ela;
- Abrir um servidor Apache em uma porta diferente para que ninguém o utilize, a não ser as pessoas que você informou sobre sua existência;
- Configurar sua rede de forma que usuários internos vejam as informações de uma maneira e usuários externos (Internet) não consigam ver tais informações, como portas e serviços prestados em seus servidores.

Observe alguns pontos:

- Sempre utilize esta técnica em conjunto de outras, pois manter a segurança apenas através da obscuridade é muito ruim;
- Não anunciar algo não é o mesmo que ocultá-lo;
- Utilizar um sistema de criptografia desconhecido não garante segurança nenhuma.

Conclusão

Apenas implementar um firewall, por mais consistente que este seja, não é suficiente para dizermos que toda a rede está segura. Por este motivo, apresentei neste material algumas técnicas que podem ser utilizadas para tornar a segurança de sua rede mais eficiente. Uma boa solução é utilizar várias destas técnicas e não apenas uma delas. Dê preferência à simplicidade, mas lembre-se: sem sacrifícios!

Referência

[1] Elizabeth D. Zwicky, Simon Cooper e D. Brent Chapman. **Internet e segurança na Web** - Construindo Firewalls Para a Internet. O'REILLY & Associated, Inc., 2000.

[2] Garfinkel, Simson and Spafford, Gene. **Practical UNIX and Internet Security**. O'Reilly & Associated, Inc., 1996.

[3] B. Fraser, SITE SECURITY HANDBOOK, RFC 2196, set. 1997. Disponível em: <http://www.ietf.org/rfc/rfc2196.txt?number=2196>

[4] <http://www.rnp.br/newsgen/9811/ipfw.shtml>

[5] <http://www.gta.ufrj.br/~jaime/trabalhos/firewall/firewall.htm>

[6] <http://www.academia.org.br/2000/artigo170.htm>

[7] <http://www.hackinglinuxexposed.com/articles/20020312.html>

Por Bruno Cesar
bruno@mundoerva.com.br

Tech Bugs Firewalls

Vulnerabilidades expostas



Dando continuidade à série sobre vulnerabilidades ocorridas nos mais diversos softwares, nesta edição da H4CK3R Especial Firewall vamos listar as principais falhas encontradas em firewalls pessoais, muito utilizados por usuários domésticos, que não têm a proteção disponível em outros servidores (que já possuem um firewall configurado em uma rede interna). Na maioria das vezes, esses softwares são de fácil instalação e utilização para qualquer usuário, acarretando na configuração de um sistema de segurança pessoal sem grandes problemas. Na maioria das vezes, essas configurações padrões executadas pelo usuário são feitas com o intuito de precaver os principais ataques descritos na Internet, como worms, trojans e vulnerabilidades no sistema operacional. Mas com o objetivo de proteger seu PC, muitas vezes o usuário está colocando em risco sua privacidade ao utilizar um software mal configurado ou que contenha algum bug que não foi corrigido. Abaixo, confira os alertas sobre as principais ocorrências de segurança mais recentes encontradas nos softwares mais utilizados nos últimos tempos pelos mais variados usuários. Com certeza, se você já utilizou um firewall pessoal para Windows, ele estará na lista, porém nem sempre com a mesma versão.

ZoneAlarm Random UDP Flood Denial Of Service Vulnerability

O ZoneAlarm é um dos personais firewalls mais utilizados em sistemas operacionais rodando o Windows. Desde suas primeiras versões, o software sempre colocou em prática a facilidade na hora de sua configuração. Até mesmo a sua utilização não tem muitas frescuras, oferecendo ao usuário diversas opções de configurações adicionais não disponíveis em outros firewalls do mesmo gênero.
Um ataque muito conhecido entre o meio da segurança digital foi encontrado em algumas versões do software. É possível efetuar um DoS (Denial of Service) ou negação de serviço em sistemas rodando o software. Em certas circunstâncias, é possível emitir um número elevado de pacotes UDP de tamanhos aleatórios.

Versões Afetadas:

Zone Labs ZoneAlarm 3.7 .202
Zone Labs ZoneAlarm Pro 4.0

Exploit:

http://www.securityfocus.com/data/vulnerabilities/exploits/zonealarm-udp-dos.pl
http://www.securityfocus.com/data/vulnerabilities/exploits/augustiner.c
http://www.securityfocus.com/data/vulnerabilities/exploits/zados.asm
http://www.securityfocus.com/data/vulnerabilities/exploits/zados.makefile

Correção:

Até o momento, a ZoneLabs, desenvolvedora do software, ainda não publicou uma correção ou patch para o bug.

SyGate Insecure UDP Source Port Firewall Bypass Weak Default Configuration Vulnerability

Por ter fácil utilização e, em algumas versões, ser "freeware", o SyGate Personal Firewall é um método barato e rápido de proteger um computador conectado à Internet.
Foi relatado que o SyGate Personal Firewall Pro permite o acesso às portas 137 ou 138 UDP, facilitando invasões sem problemas algum.

Versões Afetadas:

Sygate Personal Firewall Pro 5.0

Exploit:

nmap -vv -P0 -sU %victims_ip_address% -g 137

Solução:

Bloquear qualquer acesso às portas 137 e 138 UPD pelo firewall. Adicionar e setar na opção Advanced Rule Editor.

Multiple Vendor PC Firewall Auto Block Denial Of Service Weakness

Como se já não bastasse um bug (por mais insignificante que seja) tornar um software vulnerável, imagine outro que torna não somente um, mas vários softwares vulneráveis. Este bug pode fazer com que os firewalls pessoais fiquem totalmente estáveis a ataques do tipo DoS (ou negação de serviço). O problema está na manipulação do tráfego spoofed. Sob algumas circunstâncias, é possível para usuários remotos negar o serviço em vários locais.

Versões Vulneráveis:

Internet Security Systems BlackICE Defender 2.9 cap
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Terminal Services

- Microsoft Windows 2000 Terminal Services SP1
- Microsoft Windows 2000 Terminal Services SP2
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows 98SE
- Microsoft Windows ME
- Microsoft Windows NT Enterprise Server 4.0
- Microsoft Windows NT Enterprise Server 4.0 SP1
- Microsoft Windows NT Enterprise Server 4.0 SP2
- Microsoft Windows NT Enterprise Server 4.0 SP3
- Microsoft Windows NT Enterprise Server 4.0 SP4
- Microsoft Windows NT Enterprise Server 4.0 SP5
- Microsoft Windows NT Enterprise Server 4.0 SP6
- Microsoft Windows NT Enterprise Server 4.0 SP6a
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0 SP1
- Microsoft Windows NT Server 4.0 SP2
- Microsoft Windows NT Server 4.0 SP3
- Microsoft Windows NT Server 4.0 SP4
- Microsoft Windows NT Server 4.0 SP5
- Microsoft Windows NT Server 4.0 SP6
- Microsoft Windows NT Server 4.0 SP6a
- Microsoft Windows NT Terminal Server 4.0
- Microsoft Windows NT Terminal Server 4.0 alpha
- Microsoft Windows NT Terminal Server 4.0 SP1
- Microsoft Windows NT Terminal Server 4.0 SP2
- Microsoft Windows NT Terminal Server 4.0 SP3
- Microsoft Windows NT Terminal Server 4.0 SP4
- Microsoft Windows NT Terminal Server 4.0 SP5
- Microsoft Windows NT Terminal Server 4.0 SP6
- Microsoft Windows NT Workstation 4.0
- Microsoft Windows NT Workstation 4.0 SP1
- Microsoft Windows NT Workstation 4.0 SP2
- Microsoft Windows NT Workstation 4.0 SP3
- Microsoft Windows NT Workstation 4.0 SP4
- Microsoft Windows NT Workstation 4.0 SP5
- Microsoft Windows NT Workstation 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP6a
- Microsoft Windows XP Home
- Microsoft Windows XP Professional

Internet Security Systems Blackice Server Protection 3.5 cdf
Kaspersky Labs Anti-Hacker 1.0
Symantec Norton Personal Firewall 2002

Exploit:

Esta vulnerabilidade pode ser explorada com diversas ferramentas disponíveis. Um exemplo é:

hping -e 13 -d 2 -s 6000 -p 2140 -2 host1.example.com -c 2 -a host2.example.com

Solução:

Até o momento, nenhum dos desenvolvedores dos softwares publicou uma correção ou patch para os bugs.
Symantec Norton Personal Firewall/Internet Security 2001 Buffer Overflow Vulnerability
A vulnerabilidade, apesar de um pouco antiga, afeta outro software muito utilizado por diversos usuários, causando um grande impacto no sistema. O bug reportado é um buffer overflow no HTTP Proxy. Pode ser possível executar códigos arbitrários nesse contexto para comprometer o sistema.

Versões Afetadas:

Symantec Norton Internet Security 2001
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 98
- Microsoft Windows ME
- Microsoft Windows NT Workstation 4.0 SP6a
- Microsoft Windows XP Home
- Microsoft Windows XP Professional

Symantec Norton Personal Firewall 2001 3.0.4 .91
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 95
- Microsoft Windows 95 SR2
- Microsoft Windows 98
- Microsoft Windows 98SE
- Microsoft Windows ME
- Microsoft Windows NT Workstation 4.0
- Microsoft Windows NT Workstation 4.0 SP1
- Microsoft Windows NT Workstation 4.0 SP2
- Microsoft Windows NT Workstation 4.0 SP3
- Microsoft Windows NT Workstation 4.0 SP4
- Microsoft Windows NT Workstation 4.0 SP5
- Microsoft Windows NT Workstation 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP6a

Exploit:

Não divulgado

Solução:

A Symantec disponibilizou o patch pelo seu software LiveUpdate

Netfilter : mu um

A solução livre para proteger servidores e redes

Hoje, falar de firewalls nos Kernel 2.4 e 2.6 é falar de um software que é uma das ferramentas mais poderosas de segurança existentes; o Netfilter Iptables. Muitos administradores, usuários e curiosos do mundo Linux perguntam como é o firewall do Linux, como funciona e que programa coordena estas funções.

A resposta é o próprio kernel do Linux, que contém uma série de funções de filtragem de pacotes TCP/IP e que são manipuladas pelo iptables. Este programa foi o substituto do velho Ipchains e do jurássico Ipfwadm, respectivamente responsáveis por estas funções nos kernels 2.2 e 2.0.

Um filtro de pacotes é um software que tem como função analisar o cabeçalho (header) dos pacotes TCP durante o seu tráfego e decidir o seu destino como um todo. Podem ser tomadas decisões de descartar e aceitar um pacote (DROP e ACCEPT respectivamente), entre outras funções.

No Linux, como já dissemos antes, o processo de filtragem de pacotes está implementado diretamente no kernel, de maneira modular (LKMs) ou monolítica (diretamente compilado) e existem várias funções interessantes que podem ser feitas com os pacotes, mas a principal idéia é sua análise e tomada de decisões sobre o destino dos mesmos.

Desde a antiga série 1.1, os kernels do Linux têm tido filtros de pacotes, nos quais a primeira geração foi totalmente baseada no ipfw do BSD (ou melhor, "portada" por Alan Cox em 1994). Essa primeira implementação foi melhorada por Jos Vos e outros membros para o kernel 2.0 dando origem ao ipfwadm. Em 1998, para o kernel 2.2, Michael Neuling e Rusty Russel reescreveram uma série de novas funções melhorando e facilitando as regras de filtragem, dando origem ao ipchains. Em 1999, com o kernel 2.4, o iptables nasceu nas mãos do próprio Rusty Russel com uma equipe de colaboradores, introduzindo uma série de novas características importantes.

Hoje o iptables é uma ferramenta muito poderosa que pode rivalizar e até ultrapassar soluções proprietárias de mercado que custam milhares de dólares.

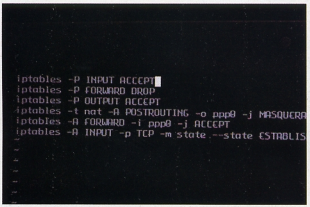
Características do Iptables

Para o iptables ser funcional, é necessário que a função de netfilter esteja implementada no kernel. Isto é feito durante o processo de compilação. É necessário acionar a opção Network Options —> Networ Packet Filterin (Replace Ipchains).

O netfilter é um framework dentro do kernel do Linux com as funções de manipular as filtragens dos pacotes, só que existe uma ferramenta para manipular estas regras: o iptables, que

ito mais do que filtro de pacotes...

Por Antonio Marcelo
amarcelo@plebe.com.br



"conversa" com o kernel e "fala" quais são os pacotes que deverão sofrer o processo de filtragem. Desta maneira é que o processo de filtros é realizado no Linux.

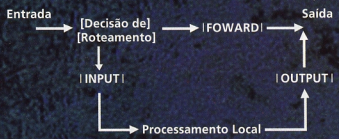
O iptables incorporou uma série de funções importantes como :

- stateless packet filtering (IPv4 and IPv6), stateful packet filtering (também chamada "Dynamic Packet Filtering e Context Based Access Control" (CBAC), filtragem dinâmica de pacotes e acesso baseado em contexto, verifica o estado/fluxo das conexões gravando informações em uma tabela e o estado de uma conexão);
- Suporte a NAT e a NAPT (network address and port translation);
- Infra-estrutura flexível e extensível ;
- Uma série de novos recursos extensíveis com o patch-o-matic;
- Interação com outros aplicativos.

O iptables trabalha com o conceito de regras que serão guardadas no kernel (nas chamadas tabelas). Logo, toda vez que uma máquina for reiniciada, as mesmas serão perdidas, por isso é muito comum colocarmos as regras em um script. Todo firewall Linux inicia sempre os famosos scripts rc.firewall, rc.fir, etc. É muito importante que este detalhe seja lembrado, mas para os mais comodistas, existem os programas iptables-save e o iptables-restore, que permitem gerar scripts e recuperar os mesmos na inicialização.

Como é o funcionamento do iptables :

Como falamos anteriormente, o kernel guarda as regras em tabelas. Uma delas em especial, a filter, armazena estas regras em listas, que são conhecidas como firewall chains ou simplesmente chains. Existem três chains na tabela filter: INPUT, OUTPUT e FORWARD. Cada vez que um pacote chega numa máquina-destino, o mesmo é analisado e encaminhado de acordo com a regra criada. Isto é feito consultando cada chain desta, sucessivamente até que seja decidido o que fazer. Temos um exemplo muito bom disto no excelente packet-filtering-HOWTO de Rusty Russel, do qual tomamos a liberdade de copiar o esquema a seguir:



1. Quando o pacote chega (por uma placa de rede, por exemplo), o kernel executa a análise do destino do pacote, realizando o que chamamos de roteamento (routing).

2. Se o pacote tem como destino a própria máquina, é direcionado desce a chain INPUT. Se passar pela chain INPUT, então a máquina recebe o pacote.

3. Se o kernel não tem suporte a forwarding ou não sabe como repassar (forward) o pacote, este é descartado. Se há suporte a forwarding e o pacote é destinado à outra interface de rede (caso exista outra), o pacote vai para a chain FORWARD. Se o mesmo for aceito (ACCEPT), ele será enviado.

4. Finalmente, um programa rodando na máquina firewall pode enviar pacotes. Esses pacotes passam pela chain OUTPUT imediatamente: se ela aceitar o pacote, ele continua seu caminho, caso contrário, ele é descartado (DROP).

O iptables possui uma série de funcionalidades, mas vamos nos ater aqui a alguns exemplos práticos como podemos criar algumas regras. Basicamente as regras de um firewall são criadas da seguinte maneira :

iptables -t (tabela) (opção) (chain) (parâmetros) -j (ação)

Por exemplo :

iptables -A INPUT -s 10.0.0.1 -j ACCEPT

A regra acima determina que todos os pacotes que vierem do endereço 10.0.0.1 devem ser aceitos. Traduzindo:

tabela: filter - não aparece por ser padrão, e logo não é necessário declará-la.

opção: -A

chain: INPUT

dados: -s 10.0.0.1

ação: ACCEPT

Um script de firewall poderia ter uma série de linhas como esta a serem executadas no momento da inicialização do microcomputador. Mas como já falamos antes, as regras são armazenadas em memória e podem ser salvas com o comando iptables-save. Por exemplo, coloque a regra acima e em seguida, digite o comando:

iptables-save > regras.txt

Será gravado um arquivo com o seguinte conteúdo:

```
# Generated by iptables-save v1.2.9 on Fri Jan 9 12:51:43 2004
*nat
:PREROUTING ACCEPT [10688:2267227]
:POSTROUTING ACCEPT [173:12340]
:OUTPUT ACCEPT [173:12340]
COMMIT
# Completed on Fri Jan 9 12:51:43 2004
# Generated by iptables-save v1.2.9 on Fri Jan 9 12:51:43 2004
*mangle
:PREROUTING ACCEPT [53753:11883864]
:INPUT ACCEPT [52821:11776460]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [26441:4620512]
:POSTROUTING ACCEPT [26441:4620512]
COMMIT
# Completed on Fri Jan 9 12:51:43 2004
# Generated by iptables-save v1.2.9 on Fri Jan 9 12:51:43 2004
*filter
:INPUT ACCEPT [52803:11761120]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [26441:4620512]
-A INPUT -s 10.1.0.20 -j DROP
COMMIT
# Completed on Fri Jan 9 12:51:43 20
```

Para a recuperação da configuração, basta apenas executarmos o comando:

iptables-restore

E teremos assim a restauração das regras do iptables.

O NAT / Mascaramento

Um outro recurso importante seria o NAT e o mascaramento. O I mascaramento está disponível desde as antigas versões 1.2.x do kernel. Esta técnica, que também é conhecida como 1:N ou um para vários, faz um

simples firewall traduzir toda uma rede através de um endereço IP. Resumindo: todas as estações que estão numa Intranet protegida pelo firewall sairão para a Web através de um único IP, propiciando economia de IPs e segurança. Já o NAT (Network Address Translator) é a técnica pela qual roteadores traduzem um endereço falso dentro de uma rede (por exemplo, uma classe A com endereços 10.0.0.X, para um endereço válido para a Internet) para uma outra rede.



Estas técnicas estão suportadas pelo iptables e, por exemplo, o conjunto de regras para a realização do mascaramento para uma interface PPP0 pode ser visto abaixo:

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

iptables -t nat -A POSTROUTING -o ppp0 -j
MASQUERADE
iptables -A FORWARD -i ppp0 -j ACCEPT
iptables -A INPUT -p TCP -m state –state
ESTABLISHED,RELATED -j ACCEPT
```

O patch-o-matic

Eis um dos recursos mais poderosos do iptables que o torna totalmente compatível e em muitos casos, superior a muitos firewalls comerciais: o patch-o-matic ou simplesmente, p-o-m. Trata-se de um conjunto de módulos/plug-ins que inserem uma quantidade enorme de recursos ao iptables, que são desenvolvidos por vários programadores que inserem no Kernel estas facilidades e que permitem realizar tarefas distintas.

O p-o-m executa uma atualização no Kernel por patches que podem ser obtidos diretamente do site da netfilter através de download no site (no final do artigo) ou dos comandos cvs abaixo :

cvs -d :pserver:cvs@pserver.netfilter.org:/cvspublic login (senha cvs)
cvs -d :pserver:cvs@pserver.netfilter.org:/cvspublic co netfilter/userspace netfilter/patch-o-matic

Em seguida, o kernel terá uma série de novas opções disponíveis no netfilter como, por exemplo, análise de strings, que é ideal para evitar conexões de usuários a sites como o KaZaA e TARPIT, para diminuição de tráfego causado por worms, além de vários outros muito interessantes (fuzzy logic, controle de tráfego por hora, etc.).

O p-o-m é desconhecido pela maioria dos administradores e é capaz de levar o iptables a um nível de recursos encontrado somente em firewalls de milhares de dólares. É recomendado que para o seu uso, seja utilizada a última versão do iptables disponível e seja bem testada antes de ser colocado em produção.

Conclusões

O netfilter é sem sombra de dúvida uma ferramenta extremamente poderosa e que compete de igual para igual com qualquer produto proprietário no mercado . É muito importante lembrar que trata-se de um recurso disponível no próprio sistema operacional e que pode ser manipulado para os mais diferentes resultados em termos de segurança. Mas, lembramos que somente um firewall não é seguro, temos uma série de outras ferramentas complementares no sistema. Queria, no entanto, ressaltar que apesar disso, o principal fator para que possamos operar cada vez melhor este tipo de ambiente é o próprio ser humano.

Sem administradores preparados e devidamente treinados, tudo o que mostramos aqui com esta poderosa ferramenta, não serve de nada. É muito importante o esclarecimento constante para que possamos levar cada vez mais o Linux ao ambiente de segurança das empresas.

Links :

Site oficial do iptables/netfilter - *http://www.netfilter.org*
Documento oficial do p-o-m - *http://www.netfilter.org/documentation/HOWTO//netfilter-extensions-HOWTO.txt*
Documentação geral do iptables e do netfilter - *http://www.netfilter.org/documentation/index.html#documentation-howto*

Antonio Marcelo Ferreira da Fonseca é autor de 12 livros sobre Linux e mantenedor dos projetos HoneypotBR (*http://www.honeypot.com.br*), FREERP (*http://www.freerp.com.br*) e da Certificação Brasileira em GNU/Linux (*http://www.cblinux.com.bn*). É diretor da Associação Brasileira de Software Livre (*http://www.abrasol.org*) na área de segurança de dados e articulador das revistas H4ck3r e GeeK. Mandem suas críticas sugestões e até mesmo um alô para amarcelo@plebe.com.br.

Firewalls & Cia

Alternativas e informações sobre firewalls para Windows

por Fernando Giannaccari

Como vocês sabem, o firewall é a parte crucial de uma rede e da segurança de computadores. Com este artigo, os usuários do Windows terão uma boa visão – apesar de básica – de como funciona e de como obter o melhor firewall

Para você encontrar o firewall mais adequado, aqui vão cinco perguntas a se considerar:

. Que opções são importantes para mim?
. Tenho histórico de vírus ou worms?
. Que outras práticas de segurança eu emprego?
. Quanto eu estou disposto a gastar em um firewall?
. Eu uso muitos programas que acessam a Internet automaticamente?

O usuário comum tem vários programas que acessam a Internet regularmente (saiba ele ou não), alguns problemas com vírus, e interesse em uma solução barata ou grátis com dificuldades mínimas de configuração e manutenção. Opções avançadas, como criptografia, bloqueio de ads e filtragem de cookies oferecem melhor privacidade, mas exigem mais da parte do usuário. Existem exceções, claro, mas a maioria dos firewalls – no caso – possui interface de uso simples que pode ser monitorada por qualquer usuário. Resumindo, os firewalls não são mais exclusividade dos administradores de rede – somos todos operadores qualificados. :]

O que temos que levar em conta é o tráfego de entrada vs. o tráfego de saída, a integridade da aplicação e notificação ao usuário – que serão discutidos a seguir.

Os firewalls funcionam examinando pacotes de dados por meio de uma variedade de filtros. Eles analisam as portas usadas pelos dados, o endereço pelo qual corre os dados, suas características e os protocolos e tipos de dados.

Filtragem de tráfego de entrada vs. Filtragem de tráfego de saída (Inbound vs. Outbound filtering)

O termo Inbound filtering (tráfego de entrada) refere-se a qualquer dado que você recebe. Isso é o que a maioria das pessoas atribui ao trabalho do firewall. O outbound filtering (tráfego de saída), entretanto, pode ser ainda mais importante para a segurança de um sistema. Por exemplo, depois de instalar um firewall como o Zone Alarm pela primeira vez, muitos usuários notarão programas estranhos tentando acesso à Internet através de portas incomuns. Estes podem ser sinais de um programa malicioso que se infiltrou no sistema sob várias possibilidades. Muitas pessoas não sabem que possuem esses programas instalados e, possivelmente, por muito tempo. No pior caso, pode ser que o computador atue como um "zumbi" e esteja sob controle de um terceiro em qualquer lugar da Internet. Como este tipo de programa não é normalmente detectado por um programa antivírus, o propósito da filtragem dos tráfegos de entrada e saída é detectá-los e prevenir o sistema de ataques. Além do mais, a filtragem do tráfego de saída avisará ao usuário sobre outras tentativas de acesso à Internet vindas de programas como spybots e spywares. Com isso, preverá a perda de dados pessoais para a Internet.

Integridade do aplicativo

A verificação da integridade do aplicativo é só um eufemismo para observar mudanças de dados. Os dermatologistas aconselham observar variações de cor e tamanho, e basicamente o mesmo é empregado aqui. Se um aplicativo muda desde sua última utilização e nenhum usuário ou administrador aplicou patches ou fez upgrade, é taxada a bandeira vermelha ao firewall, o que significa que o aplicativo pode estar infectado. Em muitos casos, o alerta se dá ao fato de você ter dado upgrade no aplicativo em particular. Em outros casos, entretanto, são detectados programas maliciosos que o manipularam e alteraram para algo perigoso ou promíscuo sem seu conhecimento.

Notificação ao usuário

Alguns firewalls têm a notificação em janela específica ou pop-ups que alertam o usuário sobre requerimentos de entrada/saída. É possível assistir a todas transações e logá-las, mas após os primeiros 15 minutos pós-instalação do firewall, o usuário se estressa. Configurar regras automáticas de aceitação ou negação de certos serviços nos previne de tal incômodo.

Quem faz os softwares de firewall pessoais?

Em primeiro lugar, sistemas operacionais como o Windows XP e o MacOS X já vêm com seu próprio firewall integrado, então, se você tem um dos dois sistemas rodando, você já tem um firewall básico instalado (não necessariamente ligado). Se eles suprirem sua necessidade (discutida acima), tudo o que precisa é de uma configuração mínima para funcionar. Já em sistemas UNIX, como o Linux, existem os filtros de pacotes.

Alguns dos firewalls populares são o Zone Alarm, o Kerio Personal Firewall2 e o Outpost.

Outros firewalls que são igualmente baratos/trial incluem o Norton Personal Firewall, o Black ICE PC Protection, o McAfee Personal Firewall e o Tiny Personal Firewall.

As informações para cada um dos firewalls listados foram compiladas por fontes confiáveis para testes. Algumas das ofertas comerciais requerem uma taxa anual, mas vale o gasto porque elas te garantem updates automáticos que mantêm seu firewall sempre em dia para um nível maior de segurança.

Firewall nativo em Sistemas Operacionais (SO)

> Windows Internet Connection Firewall:

A capacidade do firewall nativo do Windows XP é fraca, mas é melhor do que nada. É importante notar que não há filtro de tráfego de saída ou qualquer opção adicional. Por padrão, ele é desligado, mas é legal você checar antes de instalar outro software. Para localizá-lo/ligá-lo, vá em "Meus locais de rede" (My network places), clique em "Ver minhas conexões de rede" (View my network connections), selecione a conexão que trabalha com o firewall, clique com o botão direito do mouse em "Propriedades", depois em "Avançado", e marque "Proteger meu computador e a rede limitando ou impedindo o acesso a este computador por meio da Internet" (Protect My Computer And Network By Limiting Or Preventing Access To This Computer From The Internet). Voilá, você tem um firewall básico! :]

Tenha em mente que você nunca deve usar mais de um software firewall ao mesmo tempo!

> Mac OS X Firewall:

O firewall nativo do Mac OS X é como todos os outros SO baseados na plataforma UNIX, possuindo uma forma avançada de monitoramento. É fácil de entender e configurar, mas também é desligado por padrão, como no Windows XP. Vá em "System Preferences", "Sharing", "Firewall" e se entenda com ele por lá. São também necessários alguns cliques na janela "Sharing" para habilitá-lo, mas é só ler a própria instrução. Não existem opções avançadas no firewall nativo, mas vale falar que a mais nova versão do MacOSX, a Panther, inclui o novo browser da Apple, Safari, que tem seu próprio sistema de bloquear adware, pop-ups e filtragem de cookies.

Firewalls populares (e grátis)

> Kerio Personal Firewall 2

Livre para uso doméstico e vendido por 39 dólares para uso corporativo, o Kerio possui regras para download além da habilidade de criar regras definidas pelo usuário. Uma coisa única do Keria e do Tiny – ambos dividem a mesma arquitetura – é a autenticação de arquivos via assinatura digital. Os arquivos não são criptografados pelo firewall, mas possuem criptografia para fins de monitoramento de integridade do aplicativo. Ele é um firewall relativamente novo, mas recebeu boas críticas.

> Outpost Firewall

É um bom e sólido freeware que, de alguma forma, não obteve muita atenção. É fácil de usar, bloqueia ads e vírus, além de controlar cookies.

> Zone Alarm

Provavelmente é o firewall mais conhecido de todos. É fácil de instalar e configurar. Como todos os outros produtos, filtra tanto o tráfego de entrada como o de saída. O Zone Alarm é reconhecido como o líder dos firewalls pessoais grátis já por alguns anos, mas alguns dos listados a seguir têm se tornado bastante competitivos.

Firewalls de mercado

> Black ICE PC Protection

O Black ICE parece ter menos audiência do que alguns dos outros líderes, provavelmente pela sua interface simples e

limitada área de configuração. Mas ele tem boa detecção de invasão, um log simples e claro, e uma ótima aparência. O usuário pode rastrear o atacante através dos logs do ataque. É uma opção barata, mas aparentemente proporciona o mesmo que muitos outros firewalls.

> Norton Personal Firewall 2004

A Norton-Symantec tem boa reputação em relação à qualidade seus produtos e este não é exceção. Versões do Norton Personal Firewall 2004 e Norton Internet Security estão também disponíveis para Mac. Os programas são bons tanto para novatos quanto para experts. O Norton é totalmente configurável, existem regras pré-programadas e sua instalação é simples. O Norton Internet Security inclui antivírus e controle de usuários. O "problema" é que comprar produtos dos grandes chefes custa um pouco mais caro. Os produtos da Norton e McAfee custam acima de 50 dólares, enquanto os outros todos giram abaixo desse valor.

> McAfee Personal Firewall

O firewall da McAfee tem uma interface agradável ao usuário, mas um processo chato de configuração. Alguns críticos o colocam acima do Norton, mas como é um produto bem mais novo, geralmente vem em segundo lugar. A versão básica do firewall custa 30 dólares, e o Internet Security já aumenta para US$70, incluindo salas de chat para crianças, proteção antivírus e bloqueio de ads.

> Outpost Firewall PRO

A versão comercial deste firewall da Agnitum adiciona à versão grátis verificação de integridade do aplicativo, entre muitas outras opções. O preço é razoável e licenças-família estão disponíveis para uma rede doméstica. É fácil de usar, bloqueia ads, vírus e filtra cookies. Definitivamente, vale a pena para uma casa cheia! ;]

> Tiny Personal Firewall

As versões anteriores eram grátis, entretanto no presente momento o Tiny está se tornando trial somente. A Tiny ganhou grande reputação rivalizando com a ZoneLabs pelo número um no ranking do software grátis. É de fácil instalação, possui uma infinidade de opções para experts, como controle detalhado do programa, e os dialogs contêm também muitos detalhes. A modificação das regras pode ser um processo tedioso, mas muitos experts gostam dessa opção.

> Zone Alarm Plus ou Zone Alarm Pro

É um pouco confusa a infinidade de opções disponíveis pela Zone Labs (Zone Alarm, Zone Alarm Trial, Zone Alarm Plus 4.0 e Zone Alarm Pro 4 com Web Filtering), mas tudo se resume a isso: de graça, você só tem um firewall simples. Pague 40 dólares e adicione interface de proteção de usuário e vírus, ou pague 50 dólares e adicione as opções citadas,o limpador de cache, bloqueio de ads e controle de cookies. O Zone Alarm é um firewall robusto, mas seu revés é que seu mecanismo de filtragem de tráfego de saída é extremamente chato e te incomoda em extremos com centenas de alert pop-ups.

>> Uma comparação

A tabela abaixo compara os firewalls destacados acima. (Os custos são em dólares)

Firewalls básicos

Programa	Custo para versão básica	Configuração & modificaçãoion de regras	Interface com usuário	Filtragem de tráfego de entrada	Filtragem de tráfego de saída	Monitoramento de integridade do aplicativo	Notificação & logs
Black ICE PC Protection	US$40 com renovação de US$20 por ano	simples	Baseada no WinXP	Avançado	Avançado	Avançado	Claro e conciso
Kerio Personal Firewall 4	De graça para uso doméstico	robusta	Básica	Avançado	Avançado	Avançado	Claro e conciso
Mac OS X Firewall	Incluído em todas as versões do MacOSX	simples	Mac OSX	Básico	Nenhum	Básico	Claro e conciso
McAfee Personal Firewall Plus 4.1	US$30	robusta	Boa	Avançado	Limitado (3 níveis básicos)	Avançado	Avisos confusos
Norton Personal Firewall 2004	US$50 para PC, US$70 para versão pra Mac	robusta	Boa	Avançado	Avançado	Avançado	Claro e conciso, log completo de pacotes
Outpost Firewall FREE	Versão gratuita	simples	Boa	Avançado	Avançado	nenhum	Claro e conciso, log completo de pacotes
Tiny Personal Firewall 3	Somente 30 dias de trial	robusta	Boa	Avançado	Avançado	Avançado	Avisos detalhados
Windows Internet Connection Firewall	Incluso no sitema operacional Windows XP	simples	WinXP	Básico	Básico	nenhum	nenhum
Zone Alarm	Versão gratuita	simples	Boa	Avançado	Limitado	Avançado	Avisos detalhados, log completo de pacotes

Parecida com a tabela acima, a próxima compara os softwares que nos oferecem opções mais avançadas. Com todas essas análises, você não tem como se enganar quanto aos softwares. :]

Firewalls avançados

Programa	Custo	Proteção antivírus	Criptografia	Disfarce	Bloqueio de pop-up e ads	Proteção contra spywares	Filtragem de cookies	Proteção laptop	Capacidade multiusuário
Black ICE PC Protection	US$40 com renovação de US$20 por ano	Não	Não	Não	Não	Não	Não	Não	Não
Kerio Personal Firewall 4 (for businesses)	US$45 usuário único; US$22 inscrição	Não	Somente para propósitos de autenticação	Não	Sim	Sim	Sim	Sim	Sim
McAfee Internet Security Suite 5.0	US$75	Sim (McAfee VirusScan)	Não	Não	Sim	Sim	Não	Não	Não
Norton Internet Security 2004	US$70 para PC, US$100 para versão Mac	Sim (Opção adicional-Norton Anti-Virus)	Não	Sim	Sim	Sim	Sim	Sim	Sim
Outpost Firewall PRO 2	US$50	Sim	Não	Sim	Sim	Não	Sim	Não	Não
Tiny Personal Firewall 5	US$50	Não	Somente para propósitos de autenticação	Não	Não	Sim	Não	Não	Sim
Zone Alarm Plus & Pro 4	US$40; US$50	Sim	Sim	Sim (Somente na versão Pro)	Sim (Somente na versão Pro)	Sim (Somente na versão Pro)	Sim (Somente na versão Pro)	Sim	Sim

Manutenção do firewall

A instalação e a configuração de qualquer um desses firewalls deve ser extremamente fácil. A maioria deles usa linguagem clara, como "Paranóico", "Nervoso", "Confiável" do BlackICE, por exemplo. O uso diário e o monitoramento podem ser tão detalhados quanto o software permita, mas a maioria dos usuários prefere menos detalhes. Todos os firewalls não-nativos possuem logs enquanto o programa é rodado. Esses logs podem ser complicados de ler, mas normalmente contam muito sobre o tráfego no sistema e na rede, e podem ser bastante efetivos alertando o usuário sobre ameaças comuns.

1,2,3, Testando!

Ainda bem que existem alguns sites que servem para escanear e testar firewalls pessoais. Aqui vão alguns dos melhores:

> HackerWhacker

Períodos grátis estão disponíveis aqui para fins de scans e testes.

> ShieldsUp! Internet Vulnerability Profiling e Leak Test

Com interface web, os serviços de identificação de portas/serviços do ShieldsUp! são justamente acrescidos de boa reputação.

> Security Space: Desktop Audit

Por 10 dólares por ano, esta companhia oferece consultas de segurança em interface web com duração de 30 minutos a uma hora.

Conclusão

Por causa do grande aumento de tráfego e ameaças mais sofisticadas surgindo na Internet, a necessidade do firewall pessoal aumentou bastante e, hoje em dia, se torna até necessária ao usuário doméstico. Investindo um pouco de tempo e dinheiro, é uma estratégia inteligente para sua segurança e privacidade pessoal no PC.

Firewalls Routers

Funções e informações

A busca por segurança na Internet é constante: novos projetos e sistemas são desenvolvidos diariamente. Atualmente, podemos considerar que o mercado da segurança da informação (não somente na Internet, mas também em outros meios) é um negócio muito lucrativo e interessante. Por esse motivo, existem diversas tecnologias voltadas e desenvolvidas especificamente para essa área. Podemos citar como exemplo o conhecido firewall, que pode ser descrito e utilizado em sistemas Linux, Windows, MAC, entre outros *nix. O que diversos usuários ligados à informática e Internet não sabem é que um firewall não é somente voltado a um software de qualquer sistema operacional, que você instala no sistema, faz as configurações e ele já está rodando livre, leve e solto. A busca por novas tendências de Internet Security fez com que o firewall em modo software não fosse totalmente aplicável em grandes servidores, rooters e outros sistemas de grande porte que necessitavam de uma tecnologia mais amigável e segura. Com isso, foi necessário o uso do firewall baseado em hardware, com dispositivos alocados especificamente para essa função. Ele está fisicamente ligado às duas redes em questão: a privada e a pública. Possui a vantagem da obtenção de uma melhor proteção do que os firewalls baseados em software, além de poder proteger mais de um sistema de cada vez. Outro ponto positivo são que eles não afetam a performance do sistema, já que, como estão separados, não interferem no seu desempenho. Além disso, são independentes do sistema operacional e das aplicações que você vá utilizar ou utiliza no sistema atual. A desvantagem é que é necessário alocar mais energia e espaço na sua rede de computadores – que já pode estar saturada –, além de os firewalls baseados em hardware tenderem a ser mais caros.

Os principais componentes de um firewall não incluem o software ou mesmo o hardware, mas sim o objetivo que está em mente de quem irá aplicá-lo ou configurá-lo, seja por software ou hardware em um router. Podemos considerar a configuração de um firewall um conceito básico, porém difícil de ser aplicado corretamente se não houver um bom senso e um conhecimento apropriados. Uma estratégia tecnológica sempre utilizada na hora de construir e configurar um firewall é a seguinte: o administrador deve definir corretamente tudo aquilo que convém para o bom uso e a segurança do servidor. De nada adianta ter o melhor carro se você não sabe dirigir. O mesmo se aplica a um projeto de segurança: pode ser o melhor produto do mercado, mas você deve saber utilizar o que tem em mãos, saber qual o objetivo da sua aplicação, e o que ele pode gerar de bom e ruim a seu servidor. Antes de implementar um sistema de segurança deste em sua rede, primeiramente pergunte-se:

- O que eu quero que o firewall faça?
- Qual será o nível de controle desejado?
- Quanto pretendo gastar para conseguir esses resultados?
- O que vai manter o custo?

Dessa forma, um estudo aprimorado do sistema que possui em mãos é essencial.

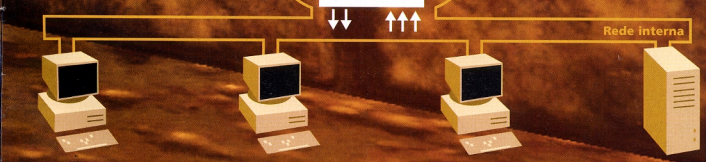
Com os constantes ataques gerados pelos mais variados motivos com o objetivo de proteger sua rede, muitas vezes, o administrador acaba pecando em pontos estratégicos cruciais em seu projeto de segurança em um servidor. Muitas pessoas acham que, se utilizarem somente um firewall em sua rede, ela ficará segura pela vida inteira. Isso é uma ilusão que ocorre constantemente em nosso meio. Devemos saber que um firewall se torna inútil quando o problema vem de dentro do servidor, ou seja, quando ocorre uma simples vulnerabilidade no sistema, como um Daemon não-atualizado. Tudo isso pode gerar uma invasão que passará pelo firewall normalmente, sem problema algum para o invasor. Assim, o administrador se pergunta: como minha rede rodando Linux foi invadida se meu iptables está corretamente configurado? Simples, o invasor utilizou um exploit remoto e explorou uma falha no SSH, por exemplo, que deu acesso root a esse mesmo invasor. Como a porta SSH no caso está liberada para o acesso de outras pessoas, o firewall não barrou o acesso a esse Daemon.

Packet Filters e Screening Router

Vejamos um exemplo da implementação de um projeto básico de um firewall baseado em um router, cuja função é simplesmente formar uma barreira de segurança em uma rede qualquer. Na Internet, devemos saber antes de qualquer coisa que existem diversos protocolos, tais como TCP, ICMP e UDP. Esses são os principais protocolos referentes a transporte e rede considerados e examinados assim que são estabelecidas regras de filtragem num packet filter.

O mecanismo de filtragem de um router (que é e pode ser considerado um "hardware firewall") possibilita que o controle de tráfego de rede e do tipo de serviços que comprometam a segurança do sistema possa ser restringido.

O packet filter não é responsável por examinar nenhum protocolo de nível superior ao de transporte como, por exemplo, o nível de aplicação que fica como tarefa dos application gateways. Portanto, qualquer falha de segurança relacionada a software não pode ser evitada utilizando somente esse projeto de firewall. Neste caso, o componente que realiza a filtragem de pacotes geralmente é um router dedicado, mas também pode ser um host de propósito geral, configurado como router, podendo receber a denominação de Screening Router. Vejamos no cronograma abaixo um exemplo básico:



Se já temos a idéia de que a filtragem dos pacotes não considera protocolos acima do nível de transporte, não é tomada nenhuma decisão baseada no conteúdo dos pacotes, ou seja, nos dados dos pacotes propriamente ditos. A filtragem que a maioria dos screening routers realiza é baseada nas seguintes informações:

- Endereço IP fonte
- Endereço IP destino
- Protocolo: se o pacote é TCP, UDP ou ICMP
- Portas TCP ou UDP fontes
- Portas TCP ou UDP destino
- Tipo de mensagem ICMP

No protocolo TCP existe uma flag denominada ACK, que é utilizada para a confirmação de pacotes e para detectar se o pacote é o primeiro de uma solicitação de conexão. Quando a flag não estiver acionada, significa que o pacote se refere a uma solicitação de conexão e, caso contrário, ele corresponde a alguma conexão já existente. Assim, o packet filter pode bloquear um serviço inbound (que vem de fora para dentro) apenas não permitindo o fluxo de pacotes com o ACK acionado, destinado a um servidor interno e associado a uma porta qualquer do serviço bloqueado.

Antes de qualquer coisa, é importante que o router tenha facilidades de filtragem por interfaces de rede. Ou seja, todas as interfaces disponíveis no router são submetidas às regras de filtragem, possibilitando que elas sejam aplicadas considerando as seguintes informações:

- A interface em que o pacote chega
- A interface da qual o pacote sai

Regras de filtragem em um screening router

- Bloquear todas as solicitações de conexão de hosts da rede externa com a sub-rede "X.X.8" conectada em alguma interface do router, exceto conexões SMTP

- Bloquear todas as conexões (para e de) daqueles que sejam considerados "não confiáveis" pelo administrador

- Desabilitar o source routing, que é o roteamento de uma máquina para outra máquina destino especificada no pacote

- Bloquear totalmente os serviços que são considerados inseguros, tais como X-Windows, RPC, NFS, TFTP, SNMP, NIS, entre outros

Um exemplo importante de ataque muito utilizado na Internet por hackers e entre outros invasores que pode ser evitado com a aplicação deste projeto de firewall é o IP Spoofing, que no caso é um ataque em que o intruso tenta se passar por um host interno (considerado um host confiável por qualquer firewall ao utilizar o endereço IP interno como endereço fonte). Pois bem, se a filtragem é realizada por interface em ambos os sentidos, este ataque não irá funcionar porque jamais um pacote pode vir de fora tendo como endereço fonte o endereço de uma máquina que está na rede interna.

A síntese dessas regras de filtragem depende muito do router ou firewall utilizado porque, atualmente, não existe uma norma de síntese. É aconselhável montar uma tabela com as possibilidades de pacotes para cada serviço a ser fornecido.

- Direction: é a direção do pacote (in: entrada no router; out: saída do router)
- Source address: é o endereço fonte
- Destination address: é o endereço destino
- Protocol: é o protocolo utilizado
- Source port: é a porta fonte
- Destination port: é a porta destino
- ACK set: indica se a flag ACK está acionada

Ações Screening Router

O router encarregado da filtragem dos pacotes pode executar uma série de atividades que servem, entre outras coisas, para monitorar o sistema, como podemos ver em alguns exemplos abaixo:

- Realizar logs de acordo com a configuração especificada pelo administrador. Com isso, será possível analisar detalhadamente eventuais tentativas de ataques, bem como verificar a correta operação do sistema.

- Retorno de mensagens de erros ICMP. Caso um pacote seja barrado, existe a possibilidade de enviar ao endereço fonte alguma mensagem com o código de erro ICMP do tipo host unreachable ou host administratively unreachable. Tais mensagens, entretanto, além de causarem um overhead, podem fornecer ao invasor algumas informações sobre o packet filter, pois dessa forma ele poderia descobrir quais os protocolos que estão barrados e quais estão disponíveis. É recomendável que não se retorne nenhum código ICMP de erro para os hosts externos.

Abaixo listamos algumas vantagens e desvantagens dos Packet Filters

Vantagens:

- Podem ajudar a proteger uma rede inteira, principalmente se este é o único router que conecta a rede interna ou a Internet

- A filtragem de pacotes é transparente e não requer tanto conhecimento

- Estão disponíveis em diversos routers e podem ser aplicados sem problemas

Desvantagens:

- As ferramentas de filtragem atualmente disponíveis não são 100% perfeitas

- Alguns protocolos não são bem adaptados a cada tipo de filtragem

- Algumas políticas não podem ser aplicadas somente com a filtragem de pacotes

Alguns Riscos na filtragem

A filtragem por endereço fonte pode apresentar alguns riscos que podem gerar ataques ao sistema. São eles:

- Source address: o invasor forja o endereço fonte utilizando o endereço de uma máquina, seja ela externa ou interna, considerada confiável pelo firewall. Este ataque pode ser bem-sucedido principalmente se o invasor não precisar capturar nenhum pacote e quando – caso a máquina forjada seja interna – não houver mecanismos de filtragem que impeçam o ip ipoofing. A resposta ao ataque poderia ser o envio de algumas informações via e-mail diretamente ao invasor.

Man in the middle: além de forjar o endereço, neste ataque o invasor deve estar no caminho entre o firewall e o host confiável porque ele tem de capturar os pacotes que são, na realidade, enviados ao host confiável.

Conclusão

Procuramos no artigo apenas citar um exemplo básico de um firewall baseado em hardware (router) e seus tipos de filtragem. É claro que hoje no mercado existem diversas tecnologias voltadas a essa área (routers e meios de filtragem). O que deve ser feito é um projeto rede para saber qual é a sua necessidade.

O funcionamento de qualquer firewall só será bem-sucedido a partir do memento em que a sua utilização for realizada com outros aplicativos do sistema, tal como um IDS, e principalmente se o servidor estiver atualizado e configurado corretamente. Este é e sempre foi o grande segredo do firewall perfeito.

Guia do CD

O PALESTRANTE

O carioca Antonio Marcelo, que apresenta o curso de Firewalls no CD desta edição, é diretor da Área de Segurança da Associação Brasileira de Software Livre (ABRASOL) e já escreveu mais de 12 livros sobre Linux e Segurança. Profissional formado no Politécnico de Redes da UNESA - RJ, Antonio é Professor Conferencista da Cadeira de Segurança da pós-graduação em Redes de Computadores da UNESA-RJ e também escreve regularmente para as revistas H4ck3r e GeeK. Além do vídeo, você também encontrará no CD desta revista dois capítulos completos do livro Segurança em Linux e uma apresentação com os tópicos do curso resumidos.

Resumo do Capítulo VI:

Neste capítulo, você vai conhecer os conceitos básicos de um firewall e suas principais características. Também verá algumas técnicas básicas, como o mascaramento, as configurações de preparação de uma máquina e muito mais. No CD estão disponíveis versões para Word e OpenOffice.

Resumo do Capítulo VII:

Neste capítulo, você verá exemplos práticos de uso do IPtables e as regras e implementações de um firewall rodando no Kernel 2.4.X do Linux. Além disso, você vai saber mais sobre as tabelas NAT, o bloqueio e filtragem de pacotes e outras importantes funções de um firewall. No CD estão disponíveis versões para Word e OpenOffice.

Os tópicos do curso

Para melhor assimilação das informações, o curso de Firewalls foi dividido em quatro partes e 13 capítulos. Conheça um pouco mais sobre cada um deles.

>>>Rodando o CD

Qualquer micro com 32 MB de RAM e um Pentium pode rodar o CD da Geek. Muitos programas, porém, exigirão muito mais da sua máquina, ao serem instalados. O CD deverá rodar automaticamente ao ser colocado no drive. Se tiver problemas, é só entrar no Gerenciador de Arquivos, no qual você também poderá acessar cada programa individualmente, sem usar a interface.

>>>Para pedir socorro...

Se você não conseguir instalar algum software do CD ou se tiver alguma dúvida, entre em contato com nosso serviço de atendimento ao leitor, de segunda a sexta, em horário comercial.

Por e-mail: *atendimento@digerati.com.br*
Por telefone: (11) 3217-2626

CONCEITOS BÁSICOS

Na introdução do curso, os diferentes tipos de atacantes e técnicas de ataque são mostrados um a um. A intenção é iniciar falando sobre segurança de uma forma mais ampla e menos específica, discutindo assim os conceitos de privacidade, confiabilidade, integridade e autenticação. Assuntos como as definições básicas de um Firewall e suas funções também são abordados.

TIPOS DE FIREWALL

Neste tópico, o assunto principal são as diferenças entre os tipos de firewall, como e quando eles são usados, além de exemplos práticos. Outro assunto abordado é a filtragem de pacotes e aplicativos feita por softwares como o Ipfwadm, o Ipchains e o Iptbales.

H4CK3R Especial

REGRAS E OPERACIONALIZAÇÃO

Com ênfase na parte prática do assunto, este tópico mostra a aplicação de filtros e regras gerais. Com exemplos reais do uso de Iptables, o palestrante realiza diversas técnicas de utilização e dá um exemplo de mascaramento.

CONSELHOS E DICAS

No encerramento do curso, Antonio Marcelo faz comentários a respeito da profissão de especialista em Segurança e dá dicas para se aperfeiçoar no ramo.

CATEGORIA FIREWALLS PARA LINUX

Além do Iptables...
Os sistemas baseados em GNU/Linux também têm muitas opções competentes de firewall. A vantagem de tanta variedade é poder contar com versões personalizadas para cada tipo de necessidade. Existem distribuições que rodam a partir de disquetes, e outras que exigem muito pouco da máquina para funcionar, possibilitando assim o uso de computadores antigos como firewall físico. A seguir, confira os destaques desta categoria:

Coyote Linux 2.02 - Distribuição Linux especialmente desenvolvida para compartilhar conexão e firewall. Cabe em apenas um disquete e roda diretamente por ele. Pode-se criar o disquete bootável tanto no Windows como no Linux

Adamantix - O projeto Adamantix (formalmente conhecido como o Debian Confiável) tem como alvo criar uma segurança de alto nível e com facilidades para os usuários. Traz soluções de segurança, incluindo: kernel patches, patches para os compiladores, programas relacionados à segurança e outras opções

Paranoia Firewall 1.53 - Firewall projetado especificamente para computadores autônomos em redes inseguras. É empregado um bom mecanismo para IP/port-based ACLs e é requerido um arquivo que lista as conexões permitidas para cada porta/portrange aberta

BBlagent Router - Imagem de uma distribuição Linux que roda por meio de um simples disquete para o compartilhamento de conexão de banda larga. Também serve como firewall para evitar o acesso de intrusos na sua LAN. Você pode criar o seu próprio BBlagent router software, baseado na sua configuração de hardware (NICs) e protocolo de conexão



Ipmkchains 0.17 - Este software lê um conjunto de regras e as compara com as regras que estão sendo utilizadas. Executa os comandos necessários para as regras em uso combinarem com as regras que estão em arquivos, usando diff e ipchains

Guarddog 2.2.0 - Recomendado para usuários novatos e intermediários que queiram configurar um firewall sem precisar conhecer a fundo TCP/IP e nem configurar ipchains, etc. Suporta FTP, SSH, Telnet, Linuxconf, Corba, SMTP, DNS, Finger, HTTP, HTTPS, NFS, POP2, POP3, SUN RPC, Auth, NNTP, NETBIOS, IMAP, além de outras opções

Adcfw-log 0.9 - Ferramenta para a análise de logs de firewalls em ordem de extração de informações válidas para os usuários. Desenvolvido para ser um script stand-alone com poucos requerimentos que podem gerar diversos tipos de relatórios, inclusive mais detalhados. Também possui opções para filtrar entrada de dados por data, protocolo, etc.

Alfandega Firewall 2.2 - Um firewall com filtro de pacotes. É como uma alfândega por onde os pacotes devem passar para serem analisados e poder separar os nocivos dos úteis. Utilizando o Netfilter, filtro de pacotes que acompanha as versões 2.4 acima do kernel do Linux, o software faz uma barreira para evitar a chegada ou saída de pacotes nocivos

BBStatus 2.08 - Contador de pacotes de IP e SNMP e ferramenta de monitoração para o Linux. Coleta, resume e mostra os valores. Pode ser usado para a contagem de IPs (permitindo que você tenha vários filtros de contagem), monitoramento de SNMP (coleta dados fazendo requisições SNMP), monitoramento ICMP, além de outras opções

Firewall by Jim 1.30 - Este firewall obtém vantagens das informações do tcp_wrappers para bloquear usuários. Também separa arquivos para fácil configuração, trabalha com a eth0 para a Internet e a eth1 para a rede

Mason 0.13.9 - Ferramenta interativa que cria um firewall usando o ipfwadm ou o ipchains. O Mason lhe dá uma lista de regras de firewall para permitir e bloquear conexões de acordo com as regras definidas pelo usuário

Firewall Builder 1.1.2 - Uma interface gráfica e um conjunto de compiladores para várias plataformas de firewalls. Ajuda os usuários a manter um conjunto de regras e permissões. Suporta iptables, ipfilter e OpenBSD pf

Turtle Firewall 1.27 - Projeto de configuração de firewalls baseado no kernel 2.4.x e iptables. Possui uma interface web com um módulo webmin

TBFirewall 3.1 - Projetado para conectar uma ou mais redes locais a outras redes, dando forma a uma rede interna e em outros modelos da rede. Também controla as regras de firewall graças à arquitetura de seus arquivos de configuração

Firewall Linuxman 0.4 - Shellscript que utiliza iptables para configurar suas regras de forma semi-automatizada. Conta com as seguintes funções: inserir automaticamente os módulos necessários ao iptables, fazer NAT de uma ou várias redes, fazer DNAT para um ou vários servidores em uma ou várias portas, eliminar pacotes estranhos e/ou spoofados, utilizar proxy transparente, definir porta específica para o squid, bloquear P2P e Instant Messengers

Firestarter 0.9.2 - Firewall que utiliza o GNOME. O usuário pode utilizar o wizard para criar um sistema de proteção básico, podendo utilizar regras dinâmicas, além de poder abrir e fechar portas com apenas alguns cliques e selecionar os programas que poderão ter acesso às portas

Floppyfw - Um firewall para Linux que roda a partir de um disquete. Usa as capacidades básicas do Linux, em relação aos firewalls, e ainda possui um sistema básico de compactação. Ótimo para compartilhar conexões em banda larga

CONFIRA TAMBÉM...

A categoria especial Iptables, na qual você vai encontrar scripts e patches de configuração para transformar seu firewall em uma barreira intransponível

CATEGORIA: FIREWALLS PARA WINDOWS

Janelas com proteção extra

O curso, que é o principal destaque desta edição

especial, fala apenas de firewalls desenvolvidos para sistemas baseados em GNU\Linux, pois eles são os melhores e mais confiáveis do mercado. Quem lida com Windows, porém, também pode proteger seu PC ou sua rede com programas de alta qualidade. Confira alguns deles a seguir:

ZoneAlarm 4.5.538 - Protege contra ataques e acessos não-autorizados ao PC, monitorando as portas do sistema, bloqueando ataques e controlando programas do computador (Obs.: É limitado ao uso em uma máquina)

PeerGuardian 1.99.12.29.2003 - Protege usuários de programas P2P do monitoramento das gravadoras. Ele trabalha basicamente como um firewall que impede conexões dos IPs suspeitos de monitorar o download e o compartilhamento de arquivos

Omniquad Personal Firewall 1.1- Sistema de segurança para proteger o computador de acesso desautorizado à LAN/Internet. Com ele, pode ser especificado o período em que será fechado automaticamente o acesso à Web

Kerio Personal Firewall 4.0.10 - Protege contra ataques hacker, identificando o IP do invasor e não permitindo que ele entre no computador. Funciona durante 30 dias

Tiny Personal Firewall 5.5.1288 - Faz uma busca em uma conexão com a Internet procurando por atividades hackers, assim como os antivírus procuram por vírus, sem afetar a conexão. Ele detecta o ataque e bloqueia as ações de hackers, escaneia cada pacote da conexão e bloqueia portas vulneráveis. Roda em Windows 2000 ou XP

ProPort 2.2 - Monitora portas locais para evitar invasão de hacker e trojans. As características incluem: monitoração ilimitada das portas, autodesconexão, edição das listas de portas, registro de ataque, filtro remoto, gerente de processo, entre outras funções

Securepoint Intrusion Detection System 2.0 - Analisa a rede em busca de invasores e pacotes maliciosos. Ele trabalha sempre de encontro ao tráfego diferente na rede, avisando-lhe quando há algum pacote ilegal querendo entrar na rede

Sygate Personal Firewall 5.5 - Possui um sistema de segurança contra intrusos, ataques hackers e trojans. Quando detecta um port scanning ou tentativa de invasão, ele automaticamente bloqueia a conexão e avisa a você sobre o problema, antes que o hacker roube dados do computador (Obs.: Versão para uso pessoal)

BartWare Personal Firewall 1.3.4 - Permite bloquear as portas de entrada do PC. Pode especificar quais portas se quer bloquear e escolher entre permitir ou não que o número de IP seja visto. Bloqueia trojans, worms, entre outros

SecureIIS 2.0.4 Personal Edition - Para a defesa do IIS 4.0, 5.0 ou 6.0. Utiliza a tecnologia CHAM (Common Hacking Attack Methods) para analisar e bloquear todas as tentativas de ataques ao servidor. Possui defesa contra o CodeRed e o CodeRed II. Requer Windows NT 4.0 e Service Pack 6 ou Windows 2000, IIS 5.0 e Service Pack 1 ou mais recente, ou ainda Windows 2003 e IIS 6.0 (Obs.: Esta versão protege um site por servidor)

AlertWall Personal Firewall 1.2.1- Evite os hackers e outros invasores com este firewall. Permite bloquear a entrada de hackers e spywares para que não enviem nada pela Internet. O computador ficará protegido de trojans, vírus, hackers, entre outros (Obs.: Expira em 21 dias e funciona em Windows nas versões NT/2000/XP)

Armor2net Personal Firewall 3.12 - Proteja-se dos ataques de hackers e arquivos maliciosos, como worms, trojans e spywares. Possui uma série de recursos interessantes que garantem a privacidade e segurança, incluindo um antipop-up. Funciona durante 30 dias

Norman Personal Firewall 1.2 - Protege contra ataques de hackers ao computador. Ele é um firewall de aplicação e de pacotes. Usa técnicas que são compatíveis com a tecnologia TDI, fazendo com que o upgrade do sistema, assim como aplicação de "service packs", não deixem o sistema instável, o que acontece com a maioria dos firewalls

NOVA LOJA DIGERATI

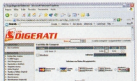
Muito mais fácil, muito mais completa

busca rápida



Arquivo completo atualizado constantemente

compra facilitada



Diversas formas de pagamento

superlista

Listagem completa com todas revistas, livros, pockets, camisetas, jogos, etc.



segurança

A loja dispõe de um dos certificados de segurança SSL mais confiáveis do mundo. Você faz suas compras e seus dados são todos cifrados para sua total segurança



www.lojadigerati.com.br

H4CK3R Especial

Atendimento ao leitor
Fone: (11) 3217-2626 (9h às 21h) — suporte@digerati.com.br
Marcos Raul, Wallace Freitas, Rodrigo França, Thiago Sobrinho, Willian Jeeves
Atendimento de vendas
Fone: (11) 3217-2600 — vendas@digerati.com.br
Luana Aguiar, Helby Campos e Samara Assi

Hacker Especial

Editor
Marcelo Barbão (mbarbao@digerati.com.br)
Redatores
Bruno Cesar, João Marinho e Fernando Wiek
Arte
Helber Bimbo, Andreza S. Francisco e Andressa Nozue
Colaboradores
Gleicon S. Moraes, Fernando Giannaccari, Clayton Kenchy Nakahara Passos
Antonio Marcelo
Revisão
Silvia Almeida e Eliane Escobar
Departamento Multimídia
Design e Programação: Alexandre Diniz
Conteúdo: Juliano Barreto, João Henrique e Cleber Farias
Vídeo: Felipe Madureira
Departamento de Internet
Tarcila Broder, Carlos Sawilli Ignatti e Aleksandro Botelho

Os artigos assinados não refletem necessariamente a opinião da revista, e sim de seus autores.

Mais uma publicação da DIGERATI especialista na comunidade digital digerati.com

Digerati Comunicação e Tecnologia Ltda
Rua Haddock Lobo, 347 — 12º Andar
CEP 01414-001 São Paulo SP
Fone: (11) 3217-2600 Fax: (11) 3217-2617
www.digerati.com

Diretores
Alessandro Gerardi — (gerardi@digerati.com.br)
Luis Afonso G. Neira — (afonso@digerati.com.br)
Alexsio Fon Meloze — (alexsio@digerati.com.br)
Diretor Comercial
René Luiz Cassettari — (rene@digerati.com.br)
Representante Comercial no E.U.A.
Multimedia, Inc. Tel. + 1-407-903-5000 Ext.222 Fax + 1-407-363-9809
Fernando Mariano — (info@multimediausa.com)
Marketing
Érica V. Cunha, Simone Siman, Carlos Ignatti, José Antonio Martins
Assessoria de imprensa
Simone Siman — (simon@digerati.com.br)
Recursos Humanos
Viviane Cardoso — (viviane@digerati.com.br)
Logística de Produção
Pierre Afonso — (pierre@digerati.com.br)
Tecnologia da Informação
Tadeu Carmona — (tadeu@digerati.com.br)

Impressão e Acabamento
Cromosete Indústria Gráfica Ltda.
Fone: (11) 4446-6544
Distribuidor Exclusivo para bancas de todo o Brasil
Fernando Chinaglia Distribuidora SA
Fone: (21) 3879-7766

ANER IVC
www.aner.org.br


José sonha em conhecer a Internet
Juntos podemos realizar este sonho
Como José, milhares de pessoas no Brasil ainda não tiveram a oportunidade de conhecer o mundo digital. A Digerati conta com a sua ajuda para realizar este sonho. Se você tiver um computador ou equipamentos que não usa mais, entre em contato conosco. Buscamos tudo em sua casa, encaminhamos para uma entidade em sua cidade e financiamos o material didático para ela.
Inclusão digital: nós podemos realizar este sonho.
Mais informações pelo telefone (11) 3217-2605
DIGERATI
especialista na comunidade digital

H4CK3R Especial Firewall

Exclusivo

CURSO COMPLETO EM VÍDEO

13 capítulos apresentados por Antonio Marcelo, diretor da ABRASOL e autor de mais de 12 livros sobre o assunto. Confira os destaques do conteúdo:

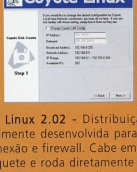
CONCEITOS BÁSICOS
*Conheça os diferentes tipos de atacantes e técnicas de ataque um a um.
*Aprenda a trabalhar com de privacidade, confiabilidade, integridade e autenticação de forma prática.

TIPOS DE FIREWALL
*As diferenças entre os tipos de firewall e como eles são usados
*Exemplos práticos de Iptables e a história dos aplicativos de segurança Ipfwadm e Ipchains

REGRAS E OPERACIONALIZAÇÃO
*Com ênfase na parte prática do assunto, veja a aplicação de filtros e regras gerais
*Confira exemplos reais de Mascaramento usando o Iptables

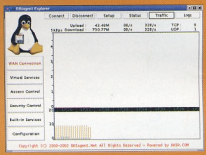
E MAIS:
Saiba mais sobre: tabelas NAT, bloqueio e filtragem de pacotes e configurações de preparação de uma máquina

Firewall de bolso



Coyote Linux 2.02 - Distribuição Linux especialmente desenvolvida para compartilhar conexão e firewall. Cabe em apenas um disquete e roda diretamente por ele. Com opção para criar o disquete no Windows e no Linux

BBlagent Router - Distro. Linux que roda por disquete e serve como firewall para evitar o acesso de intrusos na sua LAN. É possível criar o seu próprio BBlagent router software, baseado na sua configuração de hardware (NICs) e protocolo de conexão. Também compartilha conexão de banda larga



Janelas com proteção extra

Pacote para segurança de PCs domésticos e redes baseadas em sistemas Windows

ZoneAlarm 4.5.538 - Protege contra ataques e acessos não-autorizados ao PC, monitorando as portas do sistema, bloqueando ataques e controlando programas do computador (Obs.: É limitado ao uso em uma máquina)

PeerGuardian 1.99.12.29.2003 - Protege usuários de programas P2P do monitoramento das gravadoras. Ele trabalha basicamente como um firewall que impede conexões dos IPs suspeitos de monitorar o download e o compartilhamento de arquivos

Kerio Personal Firewall 4.0.10 - Protege contra ataques hacker, identificando o IP do invasor e não permitindo que ele entre no computador. Funciona durante 30 dias

Tiny Personal Firewall 5.5.1288 - Faz uma busca em uma conexão com a Internet procurando por atividades hackers, assim como os antivirus procuram por vírus sem afetar a conexão. Ele detecta o ataque e bloqueia as ações de hackers, escaneia cada pacote da conexão e bloqueia portas vulneráveis. Roda em Windows 2000 ou XP

Sygate Personal Firewall 5.5 - Possui um sistema de segurança contra intrusos, ataques hackers e trojans. Quando detecta um port scanning ou tentativa de invasão, ele automaticamente bloqueia a conexão e avisa a você sobre o problema antes que o hacker roube dados do computador

Atenção! Este CD-ROM contém softwares que podem danificar computadores. Eles foram incluídos nesse CD exclusivamente para estudo e desenvolvimento técnico. Não nos responsabilizamos por seu uso indevido. O uso destes softwares para prejudicar terceiros é crime, passível de punição.

PARENTAL ADVISORY EXPLICIT SOFTWARE

Configuração mínima do equipamento: PC Pentium 233 com 32 MB de RAM e drive de CD com velocidade dupla. Os requisitos podem variar de programa para programa

O conteúdo do CD-ROM é formado por softwares freeware e versões de demonstração