Firewalls

Hackers

- Gostam de alvos fáceis.
- Podem não estar interessados nas suas informações.
- Podem invadir seu computador apenas por diversão.
- Para treinar um ataque a uma máquina relativamente segura.
- Para usar seu disco rígido como armazenamento de arquivos ilegalmente copiados.
- Para implantar um programa "zumbi" no seu disco que possa comandar sua máquina para inundar determinado *site* com dados inúteis, que é conhecido como ataque de negação de serviço.

Hackers

- Seus dados podem ser inúteis, mas seu computador em si pode ainda ser um recurso valioso.

Firewalls

- Se você não gosta da idéia de alguém tomar controle do seu computador e ter a capacidade de apagar seus dados a qualquer momento, você precisa protegê-lo com um Firewall.

Conceito de Firewall destinados à rede

- Mecanismo de segurança interposto entre a rede interna (corporativa) e a rede externa (Internet), com a finalidade de liberar ou bloquear o acesso de computadores remotos - de usuários na Internet - aos serviços que são oferecidos dentro de uma rede corporativa.

Conceito de Firewall destinados à uma Máquina

- Também, temos os Firewalls Home, destinados a uma máquina ou uma estação de trabalho (workstation).

Firewalls

- Sendo um firewall o ponto de conexão com a Internet, tudo o que chega à rede interna deve passar pelo firewall.
- É responsável pela aplicação de regras de segurança, e em alguns casos pela autenticação de usuários, por “logar” tráfego para auditoria.
- É mecanismo obrigatório num projeto de segurança.

Firewalls

- No mínimo todo computador deveria ter um firewall, o qual age como uma porta trancada para manter intrusos vindos da Internet afastados do seu computador.

Firewalls

- Não propicia 100% de proteção contra hackers,mas pode protegê-lo contra boa parte dos harckers que espreitam endereços IP, procurando um computador vulnerável.

Firewalls

- Assim que um hacker encontra um computador sem um firewall, é relativamente fácil invadí-lo.

- Suscetíveis a ataques:
  - modem ADSL,
  - acesso discado

Firewalls

- Funcionam bloqueando as comunicações de/para seu computador.
- Muitos hackers usam scanners de portas para localizar alvos potenciais.
- Um firewall pode bloqueá-los para impedir que um hacker alcance seu computador.

Firewalls

- No nível mais simples um firewall bloqueia um scanner de portas, o que informa ao hacker que o firewall existe.

Firewalls

- Num nível mais complexo, um firewall pode mascarar a existência do seu computador, tornando-o invisível para hackers que usem scanners de portas.

Firewalls

- Neste caso, o hacker não saberá se encontrou um uma máquina protegido por firewall ou um endereço IP inválido.

Firewalls

- Em ambos os casos, é provável que o hacker deixe seu computador e procure um alvo mais fácil para atacar.

Firewalls

- Permitir que o tráfego legítimo passe através de um firewall.
- Critérios para bloquear tráfego ilegal:
  - endereços IP
  - protocolos
  - portas
  - programas específicos

Endereços IP

- Um firewall pode bloquear tráfego de certos endereços IP ou, ao contrário, somente aceitar conexões de endereços IP específicos (um computador corporativo confiável)

Protocolos

- Um firewall pode permitir somente a passagem do HTTP e bloquear o FTP, UDP, ICMP, SMTP e Telnet.

Protocolos

- UDP (User Datagram Protocol)

  para transmitir informações que não requeiram uma resposta, como streaming de áudio ou vídeo.

Protocolos

- ICMP (Internet Control Message Protocol)

  Relatar erros a outros computadores.

Protocolos

- SMTP (Simple Mail Transfer Protocol)

  Para enviar e receber email.

- Telnet

  Acessar e controlar um computador remoto.

Portas

- Permitem tipos de comunicações para dentro de um computador.
- Firewalls normalmente bloqueam todas as portas, excetos a porta 80 (HTTP) e a porta 25 para enviar e receber emails.

Portas

- Fechando certas portas, um firewall pode impedir que um hacker invada o sistema através de uma porta que foi esquecida aberta, ou abra um porta obscura para transmitir informações do seu computador para o hacker.

Portas

- Fechando portas, apenas força-se os hackers direcionarem seus ataques para as portas abertas.
- Isso limita os tipos de ataques que hacker pode fazer.

Programas Específicos

- Servem para controlar o que um computador pode fazer através da Internet.
- Examinam programas que se conectam à Internet e permitem que se escolha quais terão sua permissão para se conectar. Se um firewall detecta um programa não permitido, ele o bloqueia e notifica o fato.

Bloqueando Tráfego Ilegal

- Combinando a filtragem de endereços IP, protocolos, portas ou mesmo de palavras ou frases específicas, firewalls podem bloquear a maioria das tentativas indesejadas de invadir um computador.

Firewalls em Hardware

- Netgear
  http://www.netgear.com
- TRENDware
  http://trendware.com
- D-Link
  http://www.dlink.com

Firewalls em Software

- Muitas versões do LINUX vêm com um firewall.

Problemas com Firewalls

- Só se consegue proteger conexões chegando e saindo do computador via Internet.
- Nada pode ser feito para impedir o acesso por uma linha telefônica, através de um dispositivo de acesso sem fio, ou através do teclado se alguém estiver fisicamente usando o computador.

Problemas com Firewalls

- Firewalls podem ser enganados.

  Por exemplo, um hacker poderia renomear um Cavalo de Tróia de acesso remoto, que acesse a Internet, de forma que ele tenha o mesmo nome que um programa na lista dos programas permitidos, como por exemplo, um navegador Web.

Testar a capacidade de Firewalls

- Backbox
- Backtrack
- Portscanners