

## Engenharia de Segurança

Profa. Dra. Kalinka Regina Lucas Jaquie Castelo Branco  
[kalinka@icmc.usp.br](mailto:kalinka@icmc.usp.br)

Slides baseados nas transparências de diversos professores e autores de livros (prof. Edward David Moreno, Márcio H. C. d'Ávila, Tannenbaum, Kurose, Adriano Cansian, Luciana Martimiano entre outros)

## FIREWALLS

### SEGURANÇA COMPUTACIONAL FERRAMENTAS - FIREWALLS

- Dispositivo de hardware ou software designado para controlar o tráfego de entrada e saída em uma rede de computadores.
- Comumente utilizado para prevenção de ataques.
- Protege intervalos de endereços IP contra rastreamentos e ataques de uma maneira geral.
- Capaz de bloquear ataques às máquinas mesmo que essas estejam vulneráveis.

### SEGURANÇA COMPUTACIONAL FERRAMENTAS - FIREWALLS

- É primeira linha de defesa, mas não deve ser a única.
- Comumente firewalls passam uma falsa impressão de segurança.
- Serviços legítimos não bloqueados pelo firewall e com vulnerabilidades não corrigidas ainda podem ser explorados.

### SEGURANÇA COMPUTACIONAL FERRAMENTAS - FIREWALLS

- ◆ Bloqueio de pacotes baseado em:
  - Endereço IP de origem ou intervalo de endereços
  - Porta de origem
  - Endereço IP de destino ou intervalo de endereços
  - Porta de destino
  - Protocolo

### PORQUE?

- Proteção contra vazamento interno de informações;
- Proteção para serviços vulneráveis (malwares);
- Proteção contra acesso externo.

### SEGURANÇA COMPUTACIONAL FERRAMENTAS - FIREWALLS

- Portas padrão
  - 80 HTTP
  - 443 HTTPS
  - 20 & 21 FTP
  - 23 Telnet
  - 22 SSH
  - 25 SMTP
  - 110 POP3
  - 143 IMAP

### PRIMEIRA GERAÇÃO

- Controle de portas TCP/UDP
- Controle de acesso (IP)

- 1988 AT&T
- Maioria das soluções Windows

### SEGUNDA GERAÇÃO

- Proteção para início de conexão
- Restrições de tráfego externo
- Controle de sequência
  - Firewall statefull
- Anos 90 – Bell Labs

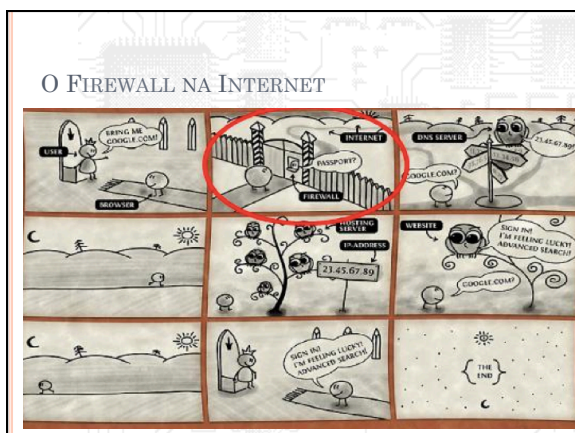
### TERCEIRA GERAÇÃO

- Firewall + Proxy
  - Controle FTP
  - Controle HTTP
- 21 – Seal da DEC
  - Firewall Comercial

### QUARTA GERAÇÃO

- Statefull Inspection
- Deep Packet Inspection
- Prevenção de Intrusão
- Anos 200
  - Juniper, Cisco...

### ONDE ESTÁ O IPTABLES



### FIREWALLS - EXEMPLO DE REGRAS

Servidor a proteger: 134.71.1.25  
 Sub-rede a proteger: 134.71.1.\*

Supondo \$internal ser a placa de rede conectada à rede interna da instituição  
 Supondo \$external ser a placa de rede conectada à rede externa da instituição

### FIREWALLS

#### EXEMPLO DE REGRAS

(quando o pacote combina com determinada regra, então o processamento termina)

Pass in on \$external from any proto tcp to 134.71.1.25 port = 80  
 Pass in on \$external from any proto tcp to 134.71.1.25 port = 53  
 Pass in on \$external from any proto udp to 134.71.1.25 port = 53  
 Pass in on \$external from any proto tcp to 134.71.1.25 port = 25  
 Block in log on \$external from any to 134.71.1.25  
 Block in on \$external from any to 134.71.1.0/24  
 Pass in on \$external from any proto tcp to 134.71.1.25 port = 22  
 Pass out on \$internal from 134.71.1.0/24 to any keep state

### FIREWALLS

#### REGISTRO DE INFORMAÇÕES

- O registro (log) de pacotes que passam pela rede pode ser positivo ou negativo.
  - Se as regras resultarem em muitas informações registradas, os logs certamente não serão armazenados.
  - Se resultarem em poucas informações, não serão suficientes.
  - Se não houver log, não haverá informações de como o *firewall* está se comportando e que tipo de tráfego tem passado pela rede.

### EXEMPLO DE LOG

```

May 30 08:03:01 antrak kernel: IN=eth1 OUT= MAC=00:0b:6a:0c:18:79:00:0a:e6:1c:4d:d3:08:00
SRC=192.168.0.17 DST=192.168.0.10 LEN=152 TOS=0x00 PREC=0x00 TTL=64 ID=53304 DF PROTO=TCP SPT=797
DPT=2049 WINDOW=63712 RES=0x00 ACK FSH URG=0
May 30 08:03:01 antrak kernel: IN=eth1 OUT= MAC=00:0b:6a:0c:18:79:00:0a:e6:1c:4d:d3:08:00
SRC=192.168.0.17 DST=192.168.0.10 LEN=172 TOS=0x00 PREC=0x00 TTL=64 ID=53305 DF PROTO=TCP SPT=797
DPT=2049 WINDOW=63712 RES=0x00 ACK FSH URG=0
May 30 08:03:01 antrak kernel: IN=eth1 OUT= MAC=00:0b:6a:0c:18:79:00:0a:e6:1c:4d:d3:08:00
SRC=192.168.0.17 DST=192.168.0.10 LEN=152 TOS=0x00 PREC=0x00 TTL=64 ID=53306 DF PROTO=TCP SPT=797
DPT=2049 WINDOW=63712 RES=0x00 ACK FSH URG=0
May 30 08:03:01 antrak kernel: IN=eth1 OUT= MAC=00:0b:6a:0c:18:79:00:0a:e6:1c:4d:d3:08:00
SRC=192.168.0.17 DST=192.168.0.10 LEN=160 TOS=0x00 PREC=0x00 TTL=64 ID=53307 DF PROTO=TCP SPT=797
DPT=2049 WINDOW=63712 RES=0x00 ACK FSH URG=0
May 30 08:03:01 antrak kernel: IN=eth1 OUT= MAC=00:0b:6a:0c:18:79:00:0a:e6:1c:4d:d3:08:00
SRC=192.168.0.17 DST=192.168.0.10 LEN=150 TOS=0x00 PREC=0x00 TTL=64 ID=53308 DF PROTO=TCP SPT=797
DPT=2049 WINDOW=63712 RES=0x00 ACK FSH URG=0
May 30 08:03:01 antrak kernel: IN=eth1 OUT= MAC=00:0b:6a:0c:18:79:00:0a:e6:1c:4d:d3:08:00
SRC=192.168.0.17 DST=192.168.0.10 LEN=164 TOS=0x00 PREC=0x00 TTL=64 ID=53309 DF PROTO=TCP SPT=797
DPT=2049 WINDOW=63712 RES=0x00 ACK FSH URG=0
May 30 08:03:01 antrak kernel: IN=eth1 OUT= MAC=00:0b:6a:0c:18:79:00:0a:e6:1c:4d:d3:08:00
SRC=192.168.0.17 DST=192.168.0.10 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=53310 DF PROTO=TCP SPT=797 DPT=2049
WINDOW=63712 RES=0x00 ACK URG=0
    
```

### EXEMPLO DE LOG

```

May 30 08:03:02 antrak kernel: IN=eth1 OUT= MAC=00:0b:6a:0c:18:79:00:0a:e6:1c:4d:d3:08:00
08:00 SRC=192.168.0.18 DST=200.245.158.146 LEN=120 TOS=0x00 PREC=0x00 TTL=128
ID=40282 DF PROTO=TCP SPT=1032 DPT=507 WINDOW=8616 RES=0x00 ACK FSH URG=0
May 30 08:03:02 antrak kernel: IN=eth1 OUT= MAC=00:0b:6a:0c:18:79:00:0a:e6:1c:4d:d3:08:00
08:00 SRC=192.168.0.18 DST=200.245.158.146 LEN=40 TOS=0x00 PREC=0x00 TTL=128
ID=40538 DF PROTO=TCP SPT=1032 DPT=507 WINDOW=8536 RES=0x00 ACK URG=0
May 30 08:03:02 antrak kernel: IN=eth1 OUT= MAC=00:0b:6a:0c:18:79:00:0a:e6:1c:4d:d3:08:00
08:00 SRC=192.168.0.18 DST=200.245.158.146 LEN=120 TOS=0x00 PREC=0x00 TTL=128
ID=40794 DF PROTO=TCP SPT=1032 DPT=507 WINDOW=8536 RES=0x00 ACK FSH URG=0
May 30 08:03:02 antrak kernel: IN=eth1 OUT= MAC=00:0b:6a:0c:18:79:00:0a:e6:1c:4d:d3:08:00
08:00 SRC=192.168.0.18 DST=200.245.158.146 LEN=40 TOS=0x00 PREC=0x00 TTL=128
ID=41050 DF PROTO=TCP SPT=1032 DPT=507 WINDOW=8472 RES=0x00 ACK URG=0
May 30 08:03:02 antrak kernel: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:00:00:00:00:00:00:00
08:00 SRC=192.168.0.18 DST=192.168.0.255 LEN=219 TOS=0x00 PREC=0x00 TTL=128
ID=41306 PROTO=UDP SPT=138 DPT=138 LEN=199
    
```

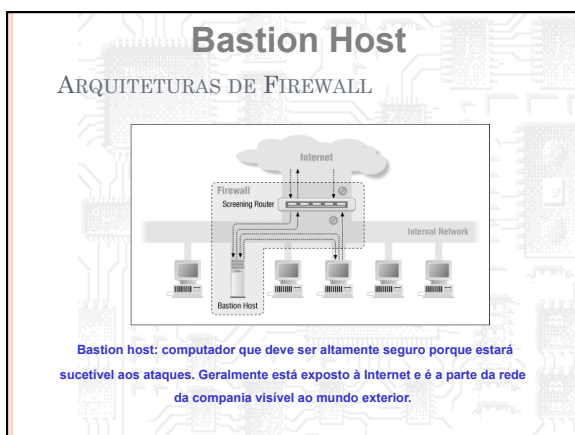
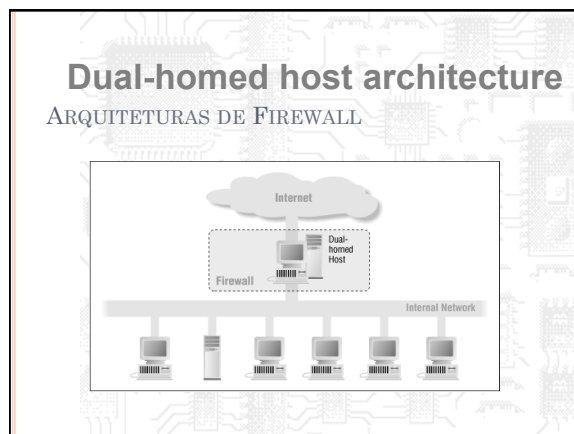
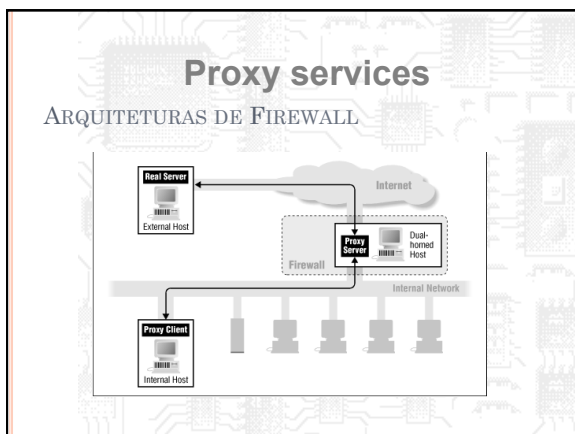
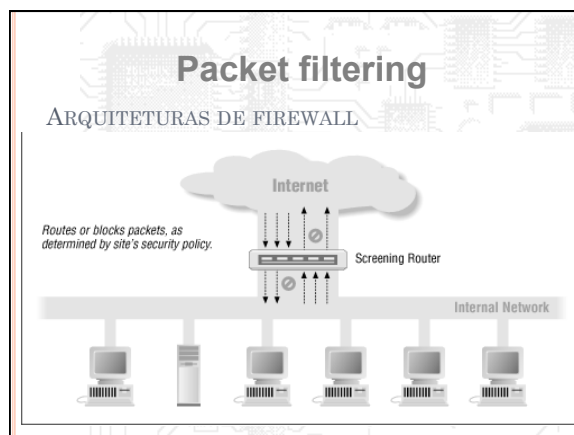
## SERVIÇOS DO FIREWALL

Network Address Translation (NAT)

Filtro de pacotes

Filtro de pacotes baseado em estados

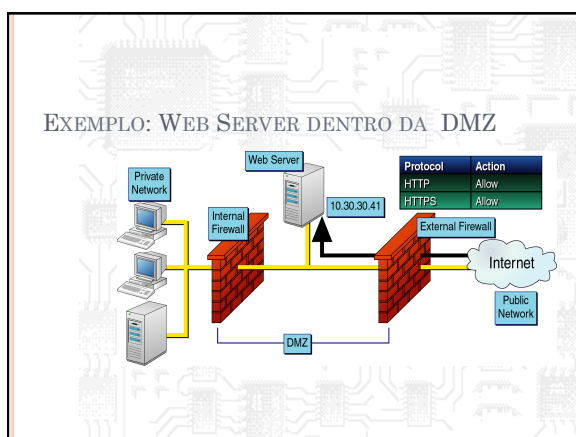
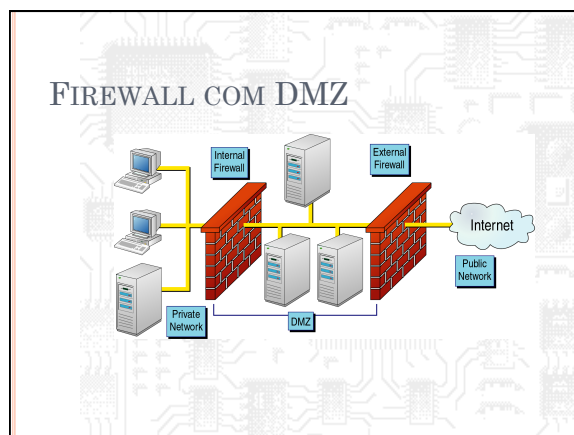
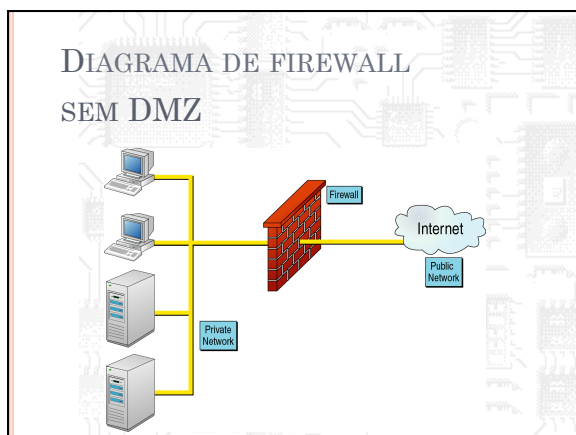
Funcionalidades avançadas



## DMZ

- ▣ Zona desmilitarizada.
- ▣ Área separada da rede interna, onde são colocados os servidores.
- ▣ Protegida de ataques internos e externos.
- ▣ Evita que seja necessário permitir o tráfego da rede externa (Internet) para a rede interna.





### FUNCIONALIDADES AVANÇADAS DOS FIREWALLS

- Time-out no estabelecimento de conexões
  - Habilita o firewall a desconectar sessões antes que a fila de pacotes de sincronização (SYN) estoure.
  - Impede ataques do tipo SYN flood, que objetivam travar computadores pelo envio de sucessivas aberturas de sessões TCP.

### FUNCIONALIDADES AVANÇADAS DOS FIREWALLS

- Filtro de conteúdo
  - Habilita o firewall a inspecionar o conteúdo (payload) transmitido nas sessões
    - Virus
    - Sites pornográficos
    - Vazamento de informações confidenciais

### FUNCIONALIDADES AVANÇADAS DOS FIREWALLS

- LIMIT
  - Limitar a frequência de determinados pacotes na rede.
- RECENT
  - Bloquear host a partir de padrões e conexões anteriores
  - Port Scan, por exemplo.

## ESTRATÉGIAS PARA FIREWALLS

- ◆ Para configuração de firewalls, geralmente escolhe-se:
  1. Especificar pacotes proibidos e liberar o restante
  2. Especificar pacotes permitidos e negar o restante
- ◆ Qual estratégia é mais segura?

## CRIAÇÃO DAS REGRAS

### BLOQUEAR TUDO

- ◆ Bloquear tudo provê maior segurança, porém maior inconveniência.
- ◆ Funcionalidades são perdidas e usuários reclamam.
- ◆ Dificuldades adicionais: descobrir como determinadas aplicações funcionam, então liberar o funcionamento no firewall.

## Criação das regras

### Não bloquear nada

- ◆ **A ESTRATÉGIA DE PARTIR DA LIBERAÇÃO TOTAL DO TRÁFEGO PARA ENTÃO NEGAR EXPLICITAMENTE DETERMINADOS PACOTES PROVÊ MENOR SEGURANÇA.**
- ◆ **OCORRE MENOR INCONVENIÊNCIA COM USUÁRIOS.**
- ◆ **DIFICULDADES ADICIONAIS: TEMPO GASTO EM DESCOBRIR OS PADRÕES A SEREM BLOQUEADOS E O QUE DEVE SER PROTEGIDO, PARA ENTÃO NEGAR NO *FIREWALL*.**

## “BURACO NEGRO” OU RST

(QUE RESPOSTA ENVIAR AOS PACOTES NEGADOS)

- Ao bloquear um pacote, duas estratégias existem:
  - Silenciosamente rejeitá-lo
  - Avisar o remetente que o pacote foi bloqueado (envio de RST)
- Para alguns casos, é indicado deixar o remetente sem a resposta. Isto pode atrasar os ataques.
- Em outros casos, convém avisar o remetente que o tráfego foi bloqueado. Por exemplo, usuários que utilizam portas ou hosts errados.

## LINUX FIREWALLS

## LINUX FIREWALL

- **Ipfwadm** : Linux kernel 2.0.34
- **Ipchains** : Linux kernel 2.2.\*
- **Iptables** : Linux kernel > 2.4.\*

## FIREWALL NO LINUX

- O que é iptables?
  - Firewall carregado diretamente ao kernel do Linux.
- O que pode ser feito com iptables?
  - Efetuar filtro de pacotes baseados em estados.
  - Executar NAT para compartilhamento de acesso à Internet.
  - Executar NAT para proxy transparente.
  - Modificações arbitrárias no cabeçalho dos pacotes IP.

## CHAINS

- O método utilizado pelo iptables para organizar as regras de filtragens
- Facilita o entendimento e gerenciamento das regras
- O Linux utiliza 3 chains principais:
  1. INPUT – pacotes que chegam para a máquina
  2. OUTPUT – pacotes saindo da máquina
  3. FORWARD – pacotes são roteados (repassados) pela máquina

## SINTAXE BÁSICA

- -F limpa as regras
- -P seta a política padrão
- -I insere uma regra
- -A adiciona uma regra
- -L lista regras

## SINTAXE BÁSICA

- -s seleciona pacote pelo IP de origem
- -d seleciona pacote pelo IP de destino
- --sport seleciona pela porta de origem
- --dport seleciona pela porta de destino
- -p seleciona pelo protocolo

## DESTINOS

- ACCEPT
  - Aceita o pacote
- DROP
  - Rejeita o pacote silenciosamente (buraco negro)
- REJECT
  - Rejeita o pacote e avisa o emissor
- LOG
  - Registra a ocorrência do pacote

## SINTAXE BÁSICA

- iptables -F
- iptables -I INPUT -s 192.168.0.0/24 -j REJECT
- iptables -A INPUT -i lo -j ACCEPT
- iptables -A OUTPUT -o lo -j ACCEPT
- iptables -P INPUT DROP
- iptables -P OUTPUT DROP
- iptables -P FORWARD DROP

### DICAS DE OTIMIZAÇÃO

- Inserir regras para rotas locais no início.
- Inserir regras de repasse (*forward*) no início.
- Se possível combinar diversas regras em uma, especificando endereços de entrada, saída, portas...
- Regras com previsão de maior tráfego devem ser inseridas antes.

### TRATAMENTO DE ESTADOS NO IPTABLES

- Iptables utiliza 4 estados básicos:
  - NEW
  - ESTABLISHED
  - RELATED
  - INVALID

### TRATAMENTO DE ESTADOS NO IPTABLES

- **NEW**
  - Pacotes que coincidirem com esse estado são novos na conexão. Isto é, representam o primeiro pacote.
  - Trata-se da abertura da conexão.

### Tratamento de estados no iptables

- **ESTABLISHED**
  - Representa pacotes referentes à conexões estabelecidas, tanto no tráfego em uma direção como em outra.
  - A regra básica para que o pacote se encaixe neste estado é que ele seja resposta à alguma requisição previamente enviada.

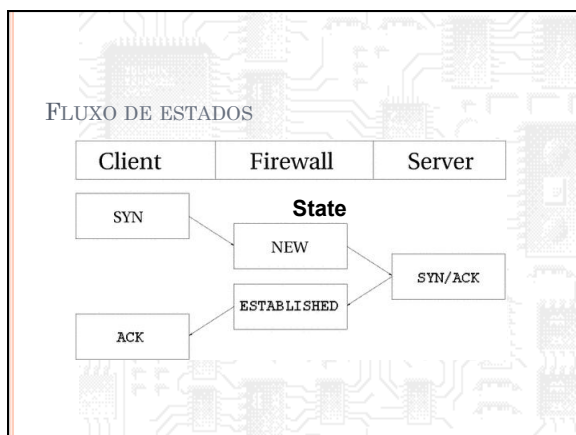
### Tratamento de estados no iptables

- **RELATED**
  - Representam pacotes relacionados à uma conexão já em andamento (ESTABLISHED).
  - Por exemplo, uma conexão FTP-DATA (porta 20) é RELATED com a conexão FTP control (porta 21).

### Tratamento de estados no iptables

- **INVALID**
  - Representa pacotes que não puderam ser identificados ou que não tiveram nenhum estado associado.
  - Devem sempre ser barrados.





## Tratamento de estados no iptables

### • EXEMPLO DE USO DE ESTADOS EM IPTABLES:

```
– iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
```

```
– iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
```

## IPTABLES – OUTRAS OPÇÕES

- Bloqueio por string:
  - iptables -A OUTPUT -m string --string "conta" -j LOG --log-prefix "ALERTA: dado confidencial "
  - iptables -A OUTPUT -m string --string "conta" -j DROP
- Conferindo o tipo de pacote e especificando o limite de fluxo
  - iptables -A FORWARD -i eth0 -o eth0 -m pkttype --pkt-type broadcast -m limit --limit 5/s -j ACCEPT

## IPTABLES – OUTRAS OPÇÕES

- Verificando o usuário que gerou o pacote:
  - iptables -A OUTPUT -m owner --gid-owner 100 -p udp -j DROP
- Limitando o número de conexões simultâneas de um mesmo IP:
  - iptables -A INPUT -p tcp -m state --state NEW --dport http -m iplimit --iplimit-above 5 -j DROP

## IPTABLES – OUTRAS OPÇÕES

- Bloqueando usuários por determinado período, devido à determinadas conexões
  - iptables -I FORWARD -d www.playboy.com.br -m recent --name bloqueado --set -j DROP
  - iptables -A FORWARD -m recent --name bloqueado -rcheck --seconds 300 -j DROP
  - iptables -I FORWARD -d www.vatican.va -m recent --name bloqueado --remove -j ACCEPT

## TABELA NAT

- Implementa Network Address Translation
- Permite fazer tradução de endereços IP
- Permite compartilhar Internet
- Permite efetuar redirecionamento de portas

### TABELA NAT

- Possui as seguintes CHAINS:
  - PREROUTING (para mudar o destino dos pacotes) – Antes do roteamento, usado para DNAT (port forwarding)
  - POSTROUTING (para mudar a origem dos pacotes) – depois do roteamento, usado pelo SNAT
  - OUTPUT (para mudar o destino) – tradução no firewall.

### TABELA NAT

- Reescrita de origem
  - `iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 200.20.0.1`
- Reescrita de destino
  - `iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 172.20.0.1`
- Redirecionando conexões para máquina onde roda o iptables
  - `iptables -t nat -A PREROUTING -s 10.0.0.0/8 -p udp --dport 53 -j REDIRECT --to-port 53`

### TABELA NAT

- Proxy transparente:
  - `iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128`
- Inserir na configuração do squid:
 

```
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

### TABELA NAT

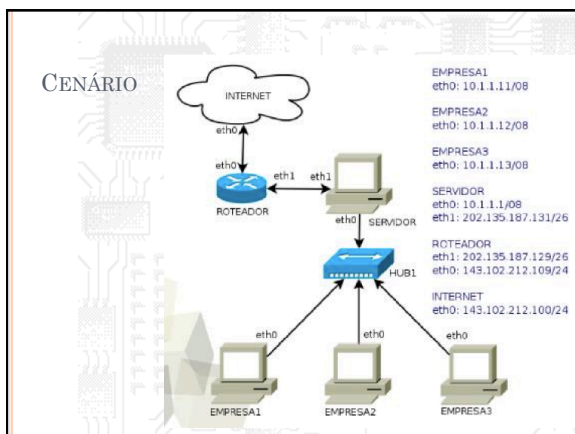
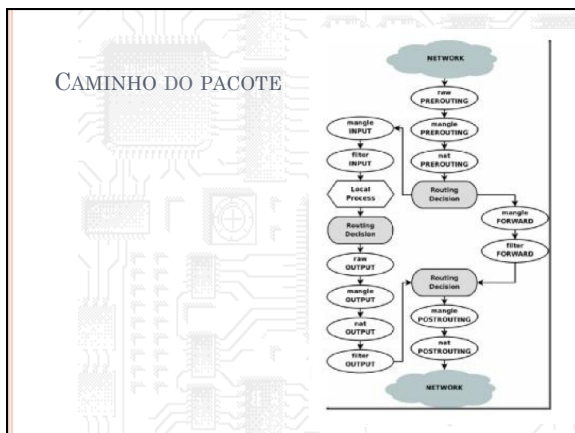
- Compartilhamento da Internet (Mascaramento)
  - `iptables -I POSTROUTING -s 192.168.0.0/24 -o eth1 -j MASQUERADE`
  - `echo 1 > /proc/sys/net/ipv4/ip_forward`
- Balanceamento de carga
  - `iptables -t nat -A PREROUTING -i eth0 -d 10.0.0.1 -j DNAT --to 10.0.0.1-10.0.0.3`

### TABELA NAT

- Balanceamento de carga
  - `iptables -A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m random --average 50 -j DNAT --to-destination 192.168.0.5:80`
  - `-A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m random --average 50 -j DNAT --to-destination 192.168.0.6:80`

### TABELA MANGLE

- Todas as chains anteriores.



- ### NMAP
- o Famosa ferramenta de varredura de redes
  - o Capaz de buscar grande número de máquinas em poucos segundos
  - o Implementa diversos tipos de ataques/scans do TCP

### NMAP

```

    [root@antrax root]# nmap 192.168.0.34
    Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-03-23 18:53
    BRT
    Interesting ports on learning1-04 (192.168.0.34):
    (The 1658 ports scanned but not shown below are in state: closed)
    PORT      STATE SERVICE
    22/tcp    open  ssh
    25/tcp    filtered smtp
    111/tcp   open  rpcbind
    614/tcp   open  unknown
    32770/tcp open  sometimes-rpc3
    MAC Address: 00:0D:87:A6:95:EE (Elitegroup Computer System Co. (ECS))

    Nmap run completed -- 1 IP address (1 host up) scanned in 3.010 seconds
  
```

## NMAP

- Opções de scan
  - P0 não pinga o host
  - sP efetua somente ping scan
  - sT faz conexão completa para o scan
  - sS faz syn SCAN
  - sX christmas tree scan
  - O identifica o SO da máquina de destino
  - v verbose
  - p porta (-p 22,25,110)

## NMAP

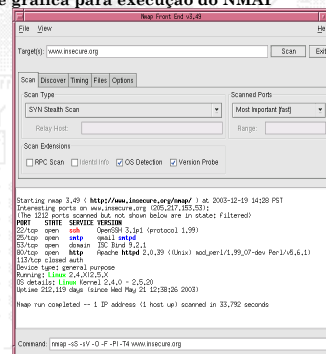
- Opções de scan
  - v verbose
  - p especifica as portas a serem rastreadas (-p 22,25,110)
- Arquivos de Registro
  - oN <logfile> formato humano
  - oX <logfile> formato xml
  - oM <logfile> formato de máquina
  - oS <logfile> th1s 10gz th3 r3su1tS of YouR resume <logfile>

## NMAP

- Opções gerais
  - iL <inputfilename> lê hosts de destino do arquivo
  - iR <num hosts> escolhe aleatoriamente os hosts de destino
  - D <decoy1 [,decoy2][,ME],...> utiliza ips falsos na origem do scan
  - S <IP\_Address> utiliza determinado ip como origem do scan
  - ttl <value> valor do ttl
- Velocidade do SCAN
  - T <Paranoid | Sneaky | Polite | Normal | Aggressive | Insane>

## NMAP-FRONTEND

- Interface gráfica para execução do NMAP



## NESSUS

- Principal ferramenta open-source de busca de vulnerabilidades
- Cliente – servidor
- Servidor para Linux
- Cliente para Linux ou Windows
  - <http://www.nessus.org>
- Gera relatórios

## NESSUS



# SISTEMAS DE DETECÇÃO DE INTRUSÃO

## O QUE É UM SDI (IDS)

Arte de detectar atividades incorretas, inapropriadas ou anômalas.

Podem ser executados em uma máquina (host) para detectar atividade maliciosa nesta máquina (HIDS).

Podem ser executados em uma rede, observando o tráfego, para detectar atividade maliciosa nesta rede (NIDS).

## FALSOS POSITIVOS E FALSO NEGATIVOS

- Falso positivo: SDI incorretamente detecta uma atividade como anômala
- Falso negativo: SDI incorretamente deixa de detectar uma atividade anômala
- Acuidade do SDI reflete a o número de falsos positivos
- Completitude do SDI reflete o número de falsos negativos

## HIDS vs. NIDS

- HIDS
  - Geralmente software instalado em uma máquina
  - Monitora diversas fontes de dados: logs, arquivos de sistema, dados de processamento, usuários atualmente logados, etc...

## HIDS vs. NIDS

- NIDS
  - Monitora o tráfego em uma rede
  - Reporta o tráfego considerado não-normal
    - Baseados em anomalia
      - Traça padrão de pacotes, destinos, protocolos, distribuição dos dados, etc.
      - Gera alerta quando este padrão é alterado.
    - Baseados em assinatura (ou abuso)
      - Dispara alertas quando determinados padrões são encontrados

## SIGNATURE-BASED NIDS

- Vantagens do NIDS baseado em assinatura
  - Não apresenta curva de aprendizado (você coloca para funcionar e pronto!)
  - Funciona muito bem para ataques já conhecidos
- Desvantagens do NIDS baseado em assinatura
  - Novos ataques não podem ser detectados
  - Falsos positivos
  - Atualização constante da base de ataques.

### ONDE INSERIR O SDI?

- Dentro do firewall
  - Limita falsos positivos (dados já foram limpos pelo firewall)
- Fora do firewall
  - Mostra todos os dados

### ONDE INSERIR O SDI?

- Como coletar todos os dados?
  - Switch com porta de captura
  - HUB
- Dificuldades em redes muito rápidas (>300Mbps)
  - Processamento da máquina SDI pode não suportar tratar todas as informações

### SDI – RESPOSTA ATIVA

- SDI passivo
  - Apenas monitora o tráfego
  - Não interfere no fluxo de informações
- Resposta ativa
  - Atividade de efetuar contra-medidas às atividades detectadas
  - Possui prós e contras

### RESPOSTA ATIVA

- Alguns pontos importantes:
  - Timing
    - Aplicam-se filtros de tempo para driblar os ataques
  - Alarmes falsos - spoofados
    - Pode causar auto-DOS no sistema alvo
  - Falta de padronização nas respostas gera dificuldade para integração de ferramentas
    - CVE

### SDIs GRATUITOS E OPEN SOURCE

- Snort
  - Baseado em rede
  - Open-source
  - Tornando-se padrão para SDI
  - Versões para windows e Unix
  - Trabalha com regras que disparam alertas em diferentes formatos (conforme o plugin)
- ACID
  - Interface web para acesso aos logs do snort

### SDIs GRATUITOS E OPEN SOURCE

- Porsentry
  - SDI baseado em host
  - Escuta por conexões em portas chaves
  - Gera alertas conforme conexões correm nestas portas
  - Capaz de detectar 'half-connections' (conexões incompletas, geradas por ferramentas como o nmap)
  - Capaz de efetuar respostas ativas e integras com iptables para bloquear acesso à máquina

### SDIS GRATUITOS E OPEN SOURCE

- Advanced Intrusion Detection Environment (AIDE)
    - SDI baseado em host
    - Versão gratuita do tripwire
    - Analisa arquivos do sistema operacional e gera assinatura digital dos mesmos
    - Execuções periódicas verificam se os arquivos foram modificados
    - Modificações podem representar ataques ocorridos
- ◇ <http://www.cs.tut.fi/~rammer/aide.html>

### TCPDUMP

- Ferramenta que utiliza a interface de rede em modo promíscuo para monitorar pacotes que trafegam pelo barramento (Sniffer)
- Pode ser utilizada para o “bem” ou para o “mal”

### EXEMPLOS: TCPDUMP

- `tcpdump -r tcpdump.out not port 22`
- `tcpdump -r tcpdump.out not port ssh`
- `tcpdump -r tcpdump.out host 192.168.101.73 not port 22`
- `tcpdump -r tcpdump.out host 10.0.1.100 and port 8080`

### TCPDUMP

```
[root@antrax root]# tcpdump -i eth2 host www.ig.com.br
08:16:02.447073 IP intra.virgos.com.br.50957 > www.ig.com.br.http: S
3204060569:3204060569(0) win 5840 <mss
1460,sackOK,timestamp 900705683 0,nop,wscale 2>
08:16:02.531589 IP www.ig.com.br.http > intra.virgos.com.br.50957: S
2242226452:2242226452(0) ack 3204060570 win 17520 <mss
1460,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK>
```

### REFERÊNCIAS

- <http://www.rnp.br/cais>
- <http://www.cert.org/>
- <http://www.modulo.com.br/>
- <http://www.nbso.nic.br/>
- <http://www.first.org/>
- <http://www.sans.org/>
- <http://www.snort.org/>

### REFERÊNCIAS

- Iptables connection tracking; *James C. Stephens*. <http://www.netfilter.org>
- Iptables Tutorial 1.1.11; *Oskar Andreasson*. <http://iptables-tutorial.haringstad.com/iptables-tutorial.html>
- Netfilter Hacking HOWTO. <http://www.netfilter.org>