Segurança Básica

Grupo de Comunicações por Computador

Departamento de Informática
Universidade do Minho

27 de Maio de 2004

Segurança Básica (Conteúdo)

1. Ameaça
   - Vulnerabilidade
   - Ataques
2. Prevenção de Intrusões
   - Firewalls
3. Detecção de Intrusões
   - Sistemas de Detecção de Intrusões

Ameaça sobre os sistemas informáticos

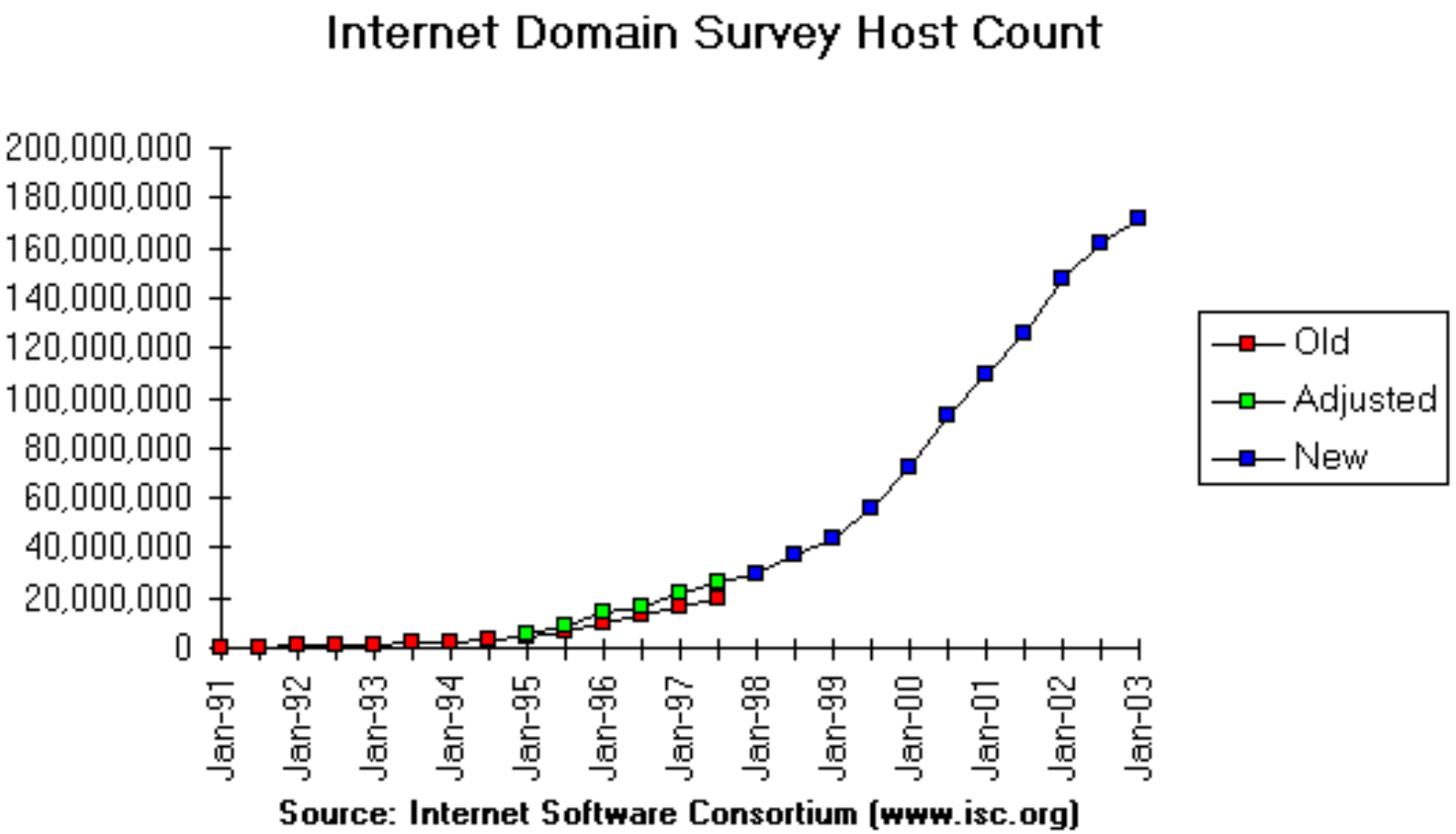

Figura: Crescimento da internet (ISC-Internet Software Consortium)

Ameaça

Caraterização da ameaça

- O crescimento exponencial da Internet
- Divulgação das falhas e vulnerabilidades do software
- Ataques cada vez mais sofisticados (Virus, Worms)
- Terrorismo informático - Ciberterrorismo

Vulnerabilidade

Principais causas

- Deficiências na concepção dos sistemas
- Deficiencias na implementação dos sistemas
- Má configuração dos sistemas

Ataques

Definição de ataque ou intrusão

Conjunto de eventos desencadeados com o objectivo de resultar em algo não autorizado.

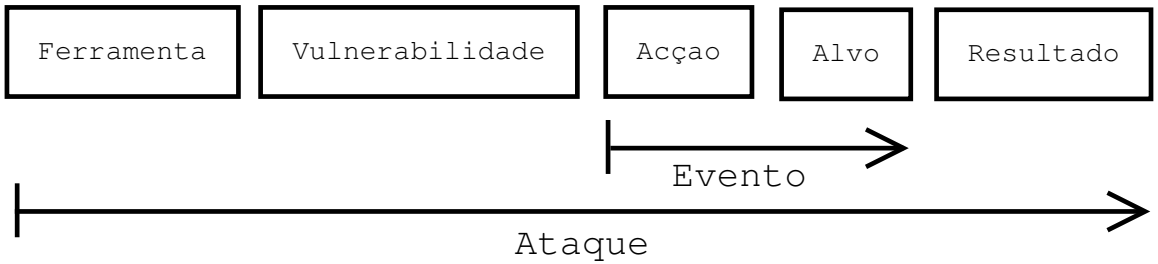

Figura: Ataque

Tipos de Ataques

Negação de Serviço (Denial of Service DOS/DDoS)

Os ataques do tipo negação de serviço visam perturbar o funcionamento normal dos serviços disponibilizados pelos sistemas informáticos. Quando estes ataque assumem a forma distribuída dá-se-lhe o nome de DDoS (Distributed DoS). Os ataques DDoS pressupõem que existem hosts comprometidos "Zombies" que serão usados para lançar o ataques DoS a partir de várias origens em simultâneo.

Tipos de Ataques

Back doors ou Troianos

Qualquer forma de usar o sistema sem que os responsáveis saibam da sua existência. As vezes são criados pelos próprios criadores do Software.
Exemplos: Back Orifice, Net Bus, etc...

Spoofing

Spoofing é uma técnica que consistem em forjar os endereços de origem de forma que um determinado host considere o tráfego gerado pelo intruso como sendo legitimo.

Tipos de Ataques

Man in the middle

Este tipo de ataque ocorre quando o intruso é capaz de interceptar tráfego colocando-se no meio de uma conversação. A técnica consiste em interceptar o tráfego, modificar o endereço de origem para que seja o host do intruso a receber a resposta. Depois, a resposta e reenviada para o host legitimo.

Replay

É um ataque do tipo "Man in the middle" que pressupõe a utilização de um sniffer para extrair informação do tráfego e reproduzi-la com o intuito de conseguir acesso ao sistema.

Tipos de Ataques

TCP Session Hijacking

É um ataque do tipo “Man in the middle” que consiste em controlar sessões TCP. O intruso pode, por exemplo, terminar sessões TCP através do envio de mensagens com a flag RST activa.

DNS Poisoning

Este ataque consiste em alterar as configurações dos servidores DNS com intuítos maliciosos. Por exemplo alterar a entrada do tipo A correspondente à tradução de um nome num endereço IP de forma a que o endereço traduzido corresponda a uma máquina que não existe, ou pior ainda, que corresponda a uma máquina que existe e que contém um site falso (por exemplo para apanhar números de cartões de crédito).

Tipos de Ataques

Ataques a Passwords

Os ataques a passwords podem ser feitos recorrendo à exploração de vulnerabilidades de algumas cifras, podem ser feitos recorrendo a palavras de dicionário (listas de passwords mais usadas), recorrendo à força bruta (geração automática de passwords) ou através do recurso à “Engenharia Social”, isto é, procurando conseguir informação junto dos utilizadores com o intuíto de obter acesso através dos processos de autenticação/autorização.

Tipos de Ataques

Ataques que recorrem à exploração do Software

Estes ataques recorrem às vulnerabilidades do Software para conseguir acesso ilegítimo aos sistemas.

Buffer Overflow

É uma das formas mais comuns de explorar falhas de segurança no Software. A técnica usada é tirar partido de código que não verifica o tamanho de strings. Quando o tamanho limite é ultrapassado os bytes excedentes vão sobrepor o código do próprio programa sendo desta forma possível conseguir reprogramar as aplicações remotamente de forma a que elas permitam o acesso ilegítimo dos intrusos.

Tipos de Ataques

Ataques baseados na vulnerabilidade dos protocolos

São ataques que exploram vulnerabilidades nos protocolos de comunicações.

SYN Flood

Este ataque explora uma vulnerabilidade no estabelecimento de conecções TCP. Este processo é desencadeado em três fases. Se um número elevado de conecções são tentadas mas não terminadas (são alocados recursos), pode tornar um serviço inutilizável. É um ataque de DoS.

Tipos de Ataques

Smurf

O Smurf consiste em enviar um broadcast para várias redes de um ou vários pacote ICMP ECHO (Ping) com o endereço de origem forjado com o endereço da vítima. Todas os hosts que receberem o Ping vão responder para o endereço da vítima.

Ping of death

Consiste em enviar pocotes ICMP com um tamanho demasiado grande. Se for enviado para um host que corra o Windows 95 um ICMP ECHO com um tamnho de 65550, o Windows irá produzir um erro do sistema (the bluescreen of death). A este tipo de ataques por vezes classificados sob a categoria de “Unexpected data”.

Tipos de Ataques

Port Scans

São ataques de reconhecimento. Podem ser aplicadas várias técnicas para se obter informação sobre que portas estão abertas no sistema (ferramenta Nmap).

```
[pedro@dhcp-7 pedro]$ nmap 193.136.9.157
Starting nmap 3.50 ( http://www.insecure.org/nmap/ )
at 2004-05-25 19:05 WEST Interesting ports on dhcp-7.uminho.pt (193.136.9.157):
(The 1654 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
32771/tcp open  sometimes-rpc5
Nmap run completed -- 1 IP address (1 host up) scanned in 0.763 seconds
```

Firewalls

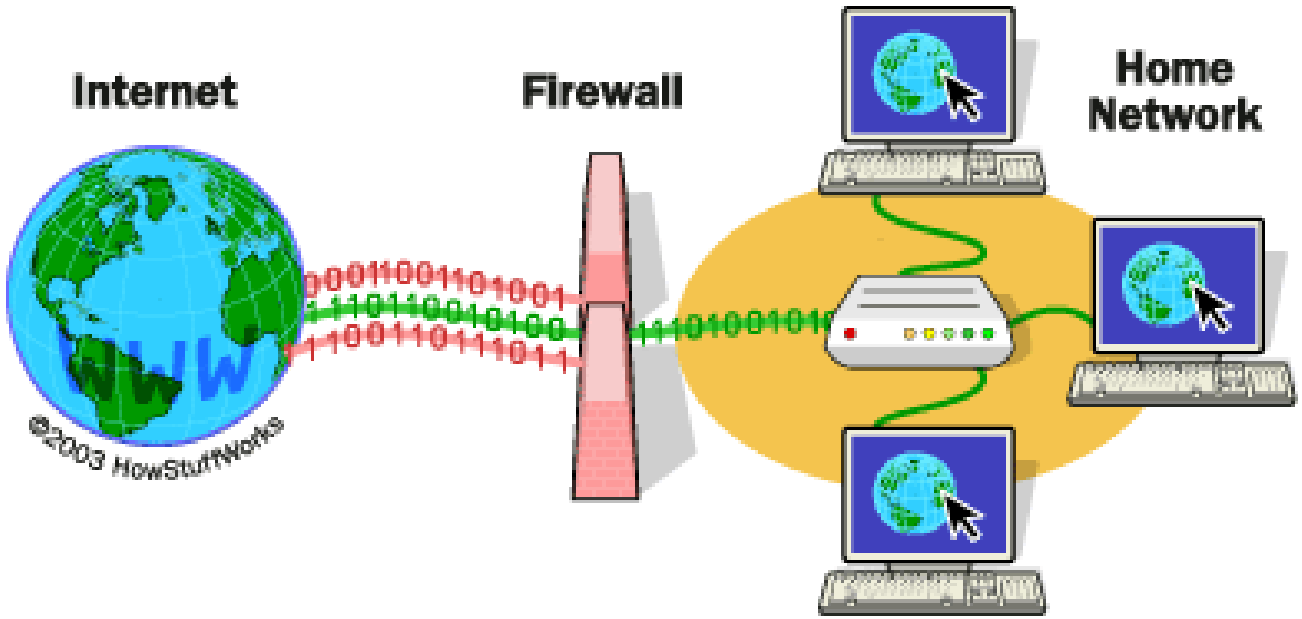

Figura: Firewall

Tipos de Firewalls

- Filtragem de pacotes (Packet filtering) - Os cabeçalhos dos pacotes são analisados e todos aqueles que não respeitam um determinado critério (policy-regras) são descartados;
- Proxy - O firewall funciona como um gateway ao nivel da aplicação, isto é, os protocolos das aplicações são emulados pelo firewall. Isto permite ter um controlo sobre as operações que os utilizadores podem efectuar. Por exemplo um proxy do serviço telnet pode limitar os utilizadores a executarem um determinado conjunto de comandos;

Tipos de Firewalls

- Stateful Inspection - Este tipo de firewalls não se limita a ter regras que filtrem com base no conteúdo dos campos dos cabeçalhos das unidades de tráfego, possui um módulo de inspecção que analisa também o conteúdo de payload (nível de aplicação). Além disso, compreende o conceito de sessão. Por exemplo respostas a pedidos que não tenham sido feitos podem ser descartados.

Packet Filters

Vantagens:

- Têm muito bom desempenho porque só verificam campos dos cabeçalhos das unidades de tráfego;
- Como o payload dos pacotes é ignorado são independentes das aplicações
- As regras são relativamente fáceis de criar

Packet Filters

Desvantagens:

- Permitem conecções fim-a-fim (sem usar NAT) comprometendo a segurança de algumas aplicações;
- Como não é possível aplicar regras ao conteúdo das unidades de tráfego não é possível, por exemplo, bloquear o acesso dos utilizadores sites com determinado conteúdo;
- A autenticação é apenas feita baseada em endereços IP e não em utilizadores;
- Pouca informação nos registos de actividade (Logs);
- Endereços dinâmicos (DHCP) podem dificultar a escrita de regras.

Stateful inspection

Vantagens:

- Mais segurança que os packet filters porque examina a totalidade das unidades de tráfego;
- Existe alguma independencia face às aplicações embora dependa do nível da inspecção;
- Mais informação nos registos de actividade do Firewall;
- Bom desempenho.

Stateful inspection

Desvantagens:

- Permitem conecções directas fim-a-fim (sem NAT);
- Não é possível ocultar hosts privados (sem NAT);
- As escrita das regras é mais complexa;
- Não permite autenticação ao nível do utilizador;
- Menor desempenho que os Firewalls packet filter.

Proxies

Vantagens:

- Por não permitirem conecções fim-a-fim e por controlarem a actividade dos utilizadores no uso das aplicações, são considerados os Firewalls que garantem maior segurança;
- Permitem a melhor filtragem por conteúdos;
- Escondem sistemas privados (o NAT também);
- Autenticação por utilizador;
- A escrita de regras é mais simples;
- Produzem registos mais exaustivos.

Cenários de Utilização

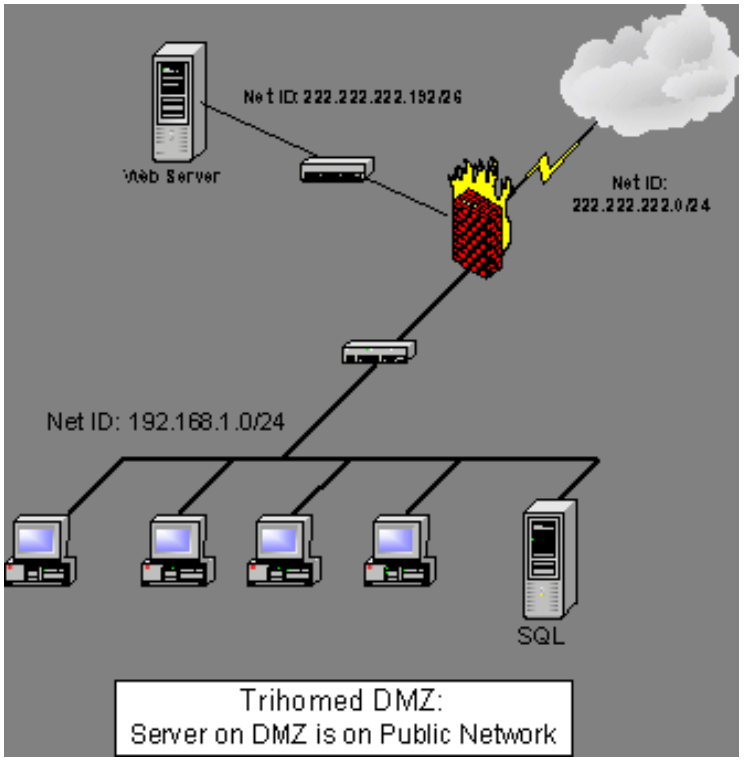

Figura: DMZ (Zona desmilitarizada) na rede pública.

Cenários de Utilização

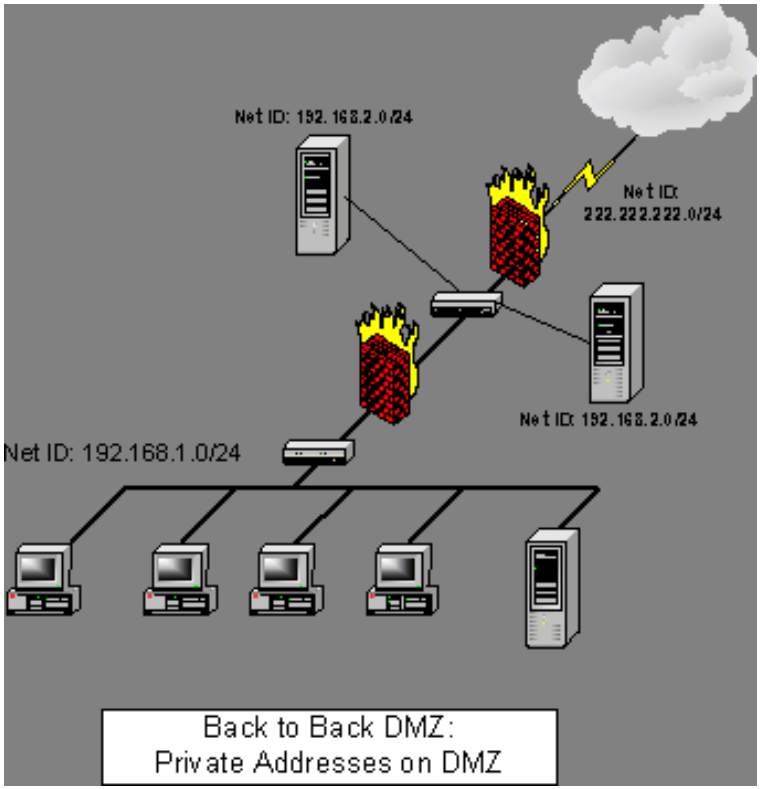

Figura: DMZ com endereços privados.

Exemplos de Firewalls

IPTables:

- Usa kernel space - os pacotes são filtrados pelo Sistema Operativo, desta forma podem ser evitados ataques que explorem vulnerabilidades da implementação da pilha TCP/IP;
- Statefull inspection
- Free software (GNU)

Exemplo de Firewalls

```
# Apaga as regras
iptables -F
#  Permite o acesso ao interface loopback
iptables -A INPUT -i lo -p all -j ACCEPT
iptables -A OUTPUT -o lo -p all -j ACCEPT
#  Permite a saida a todos os pacotes
iptables -A OUTPUT -o eth0 -p all -j ACCEPT
#  Aceita pacotes de conecções estabelecidas
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
#  rejeita pacotes tcp com a flag rst
iptables -A INPUT -p tcp --tcp-option ! 2 -j REJECT
#  Abre a porta ftp
iptables -A INPUT -p tcp -i eth0 --dport 21 -j ACCEPT
iptables -A INPUT -p udp -i eth0 --dport 21 -j ACCEPT
# Abre a porta SSH
iptables -A INPUT -p tcp -i eth0 --dport 22 -j ACCEPT
iptables -A INPUT -p udp -i eth0 --dport 22 -j ACCEPT
#  Abre a port HTTP
iptables -A INPUT -p tcp -i eth0 --dport 80 -j ACCEPT
iptables -A INPUT -p udp -i eth0 --dport 80 -j ACCEPT
#  Aceita conecções SAMBA locais
iptables -A INPUT -p tcp --syn -s 192.168.10.0/24 --destination-port 139 -j ACCEPT
iptables -P INPUT DROP
```

Sistemas de Detecção de Intrusões

O que são Sistemas de Detecção de Intrusões?

- A principal diferença entre um Sistema de Detecção de Intrusões baseado na análise do tráfego da rede e um Firewall é que os Sistemas de Detecção de Intrusões não são gateways;
- Procuram detectar e não prevenir intrusões;
- Os firewalls têm regras mais simples em que as acções associadas são normalmente aceitar ou recusar pacotes;
- Muitos dos ataques são feitos através da porta 80 (HTTP), normalmente as Firewalls deixam passar o tráfego para esta porta, sendo necessário vigiar o que passa nos fluxos de dados;
- Os firewall não detectam se alguém está a fazer um ataque composto por vários eventos, não tem a

Tipos de Sistemas de Detecção de Intrusões

Tipos de Sistemas de Detecção de Intrusões

- Fontes de informação - Rede, Hosts, Aplicações;
- Tempo - Batch, Tempo-Real;
- Resposta - Activa, Passiva;
- Técnicas de detecção - Pattern matching, Heurísticas, Expert-Systems, Redes Neuronais Artificiais, Redes de Petri, etc...
- Localização - Centralizado, parcialmente distribuído, totalmente distribuído (baseado em agentes)

Cenário de utilização

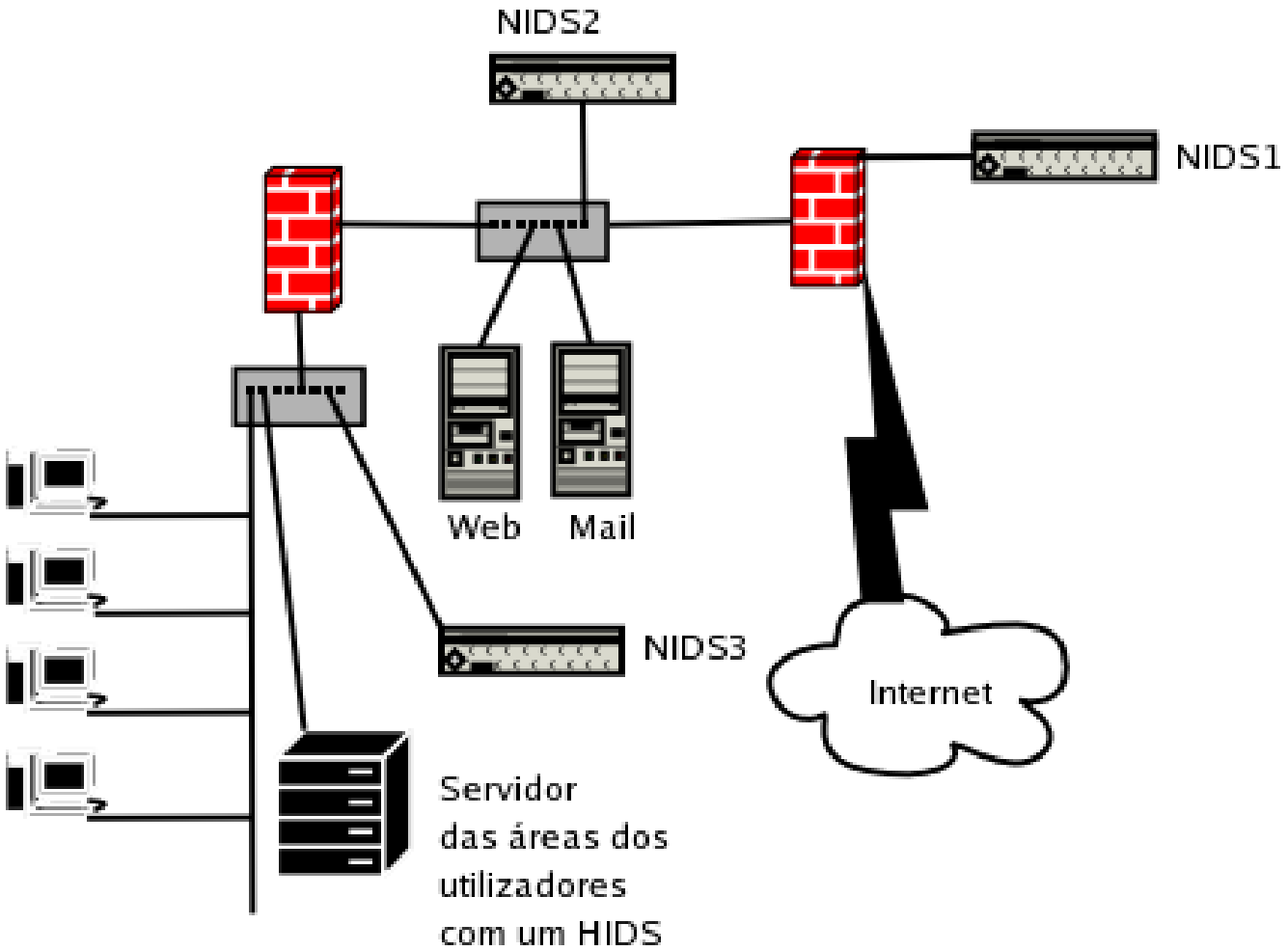

Figura: Cenário de utilização de IDSs (Intrusion Detection Systems)

Snort

Snort - Lightweight Intrusion Detection

- Carga computacional mínima
- Várias plataformas (*nix, Linux, Solaris, Mac, Windows)
- Arquitectura muito simples
- Fácil aplicação em situações específicas num curto espaço de tempo

Snort

Arquitectura

- Dois módulos principais: Sniffer e Logger;
- Regras de detecção mantidas numa lista ligada bidimensional composta por chain-headers (elementos comuns a todas as regras) com um apontador para um lista de chain-options (elementos opcionais das regras)
- Plugins: Chain-options, pré-processamento e pós-processamento.

Exemplo

Ping of Death

```
alert ICMP $EXTERNAL any -> $INTERNAL any
(msg: "IDS246/dos_dos-large-icmp"; dsize: >800;
classtype: denialofservice; reference: arachnids,246;)
```

Telnet - login falhado

```
alert TCP $INTERNAL 23 -> $EXTERNAL any
(msg: "IDS127/telnet_telnet-login-incorrect"; flags: A+;
content: "Login incorrect"; depth: 16; nocase;
classtype: system-failed; reference: arachnids,127;)
```

SNMP - NT User List

```
alert UDP $EXTERNAL any -> $INTERNAL 161
(msg: "IDS333/snmp_snmp-nt_userlist";
content: "|2b 06 10 40 14 d1 02 19|";
classtype: info-attempt; reference: arachnids,333;)
```