Ferramentas de Segurança

Professores:
Fred Sauer, D.Sc.
Guilherme Neves, M.Sc.

NP-1

Gestor: CI/ICM
Versão 1 – junho/2013

Sumário

- Ataques
  - Varredura de Vulnerabilidades
  - Sniffing
  - Hacking
  - Artefatos Maliciosos (Malware)
    - Vírus, worms, trojan horses, keyloggers, spywares
- Defesas
  - Filtro de pacotes (IP Firewall)
  - Proxy (Firewall Proxy)
  - IDS/IPS
  - Honeypots.

Varredura de Vulnerabilidades

- Técnica básica preliminar de identificação de possíveis vulnerabilidades
- Identifica portas abertas (protocolos/aplicações). Exemplos:
  - TCP 20/21 – FTP
  - TCP 22 – SSH
  - TCP 80 – HTTP (servidor WEB)
- Mais popular atual – NMAP.

Sniffing

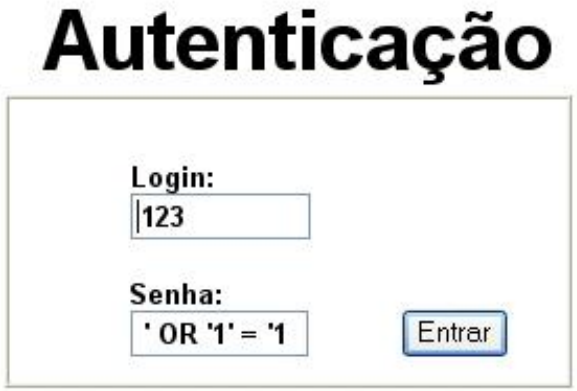
- Poderosa ferramenta criada para análise de tráfego de rede
- Há vários, mas todos fazem a mesma coisa:
  - Colocam a placa de rede em modo promíscuo;
  - Instalam um driver que desabilita o filtro L2; e
  - Levam todos os quadros recebidos na interface de rede para o *sniffer*
- O mais popular atual é o Wireshark.

Hacking

- Técnicas usadas para comprometimento da CID
- Vem sendo substituídas pela Engenharia Social, exceto na área de Guerra Cibernética, onde o elemento humano é teoricamente mais preparado
- Algumas técnicas ainda eficazes:
  - SQL *Injection*;
  - *Buffer Overflow*; e
  - *Exploits*.

SQL Injection

- Criação de *strings* que “enganam” as interfaces de controle de acesso a bancos de dados;
- Exemplo:



  - Resulta em:

- **SELECT * FROM tabela_usuarios WHERE login = '123' AND senha = ' ' or '1' = '1'**

Buffer Overflow

- Técnica que explora falhas de segurança no desenvolvimento de aplicações que possibilitam a interrupção do serviço
- Como é típico, ao ser abortado, o programa oferece um *shell* com os direitos do seu executor, que normalmente é administrador do sistema
- Técnicas como o SDL (*Secure Development Lifecycle*) e OWASP (*Open Web Application Security Project*), entre outras ações, evitam essa vulnerabilidade.

Buffer Overflow

PETROBRAS

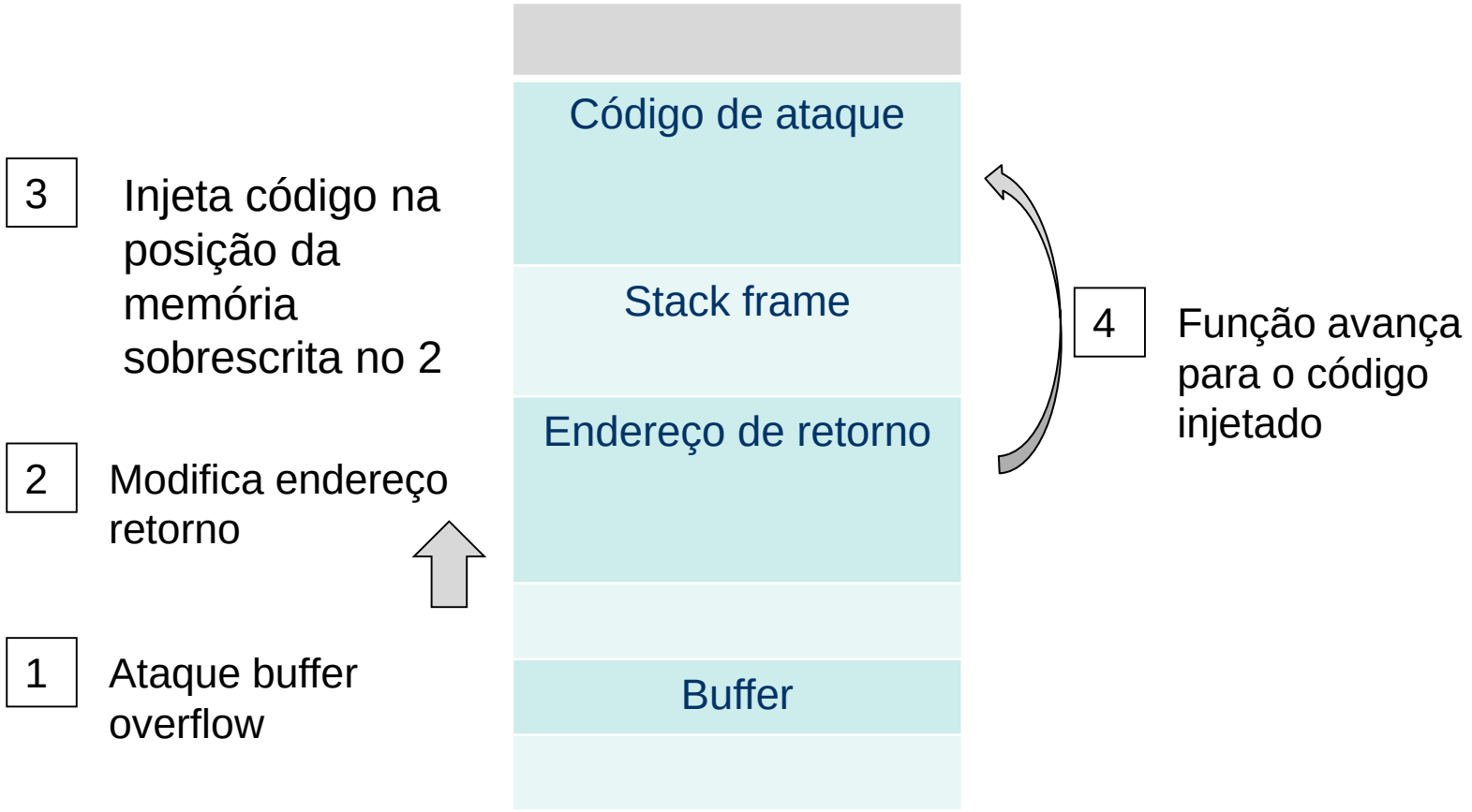
- Basicamente é um “Estouro da pilha” de memória artificialmente provocado por um *hacker*
  - São desenvolvidos especificamente para um determinado SO e hardware
- Ocorre onde o controle do buffer (memória temporária para armazenamento de dados) não é feito adequadamente
- Com isso, pode haver execução de códigos arbitrários
- Pode resultar em:
  - Sequestro do acesso ao sistema
  - Perda ou modificação de dados
  - Paralisação do sistema.

NP-1

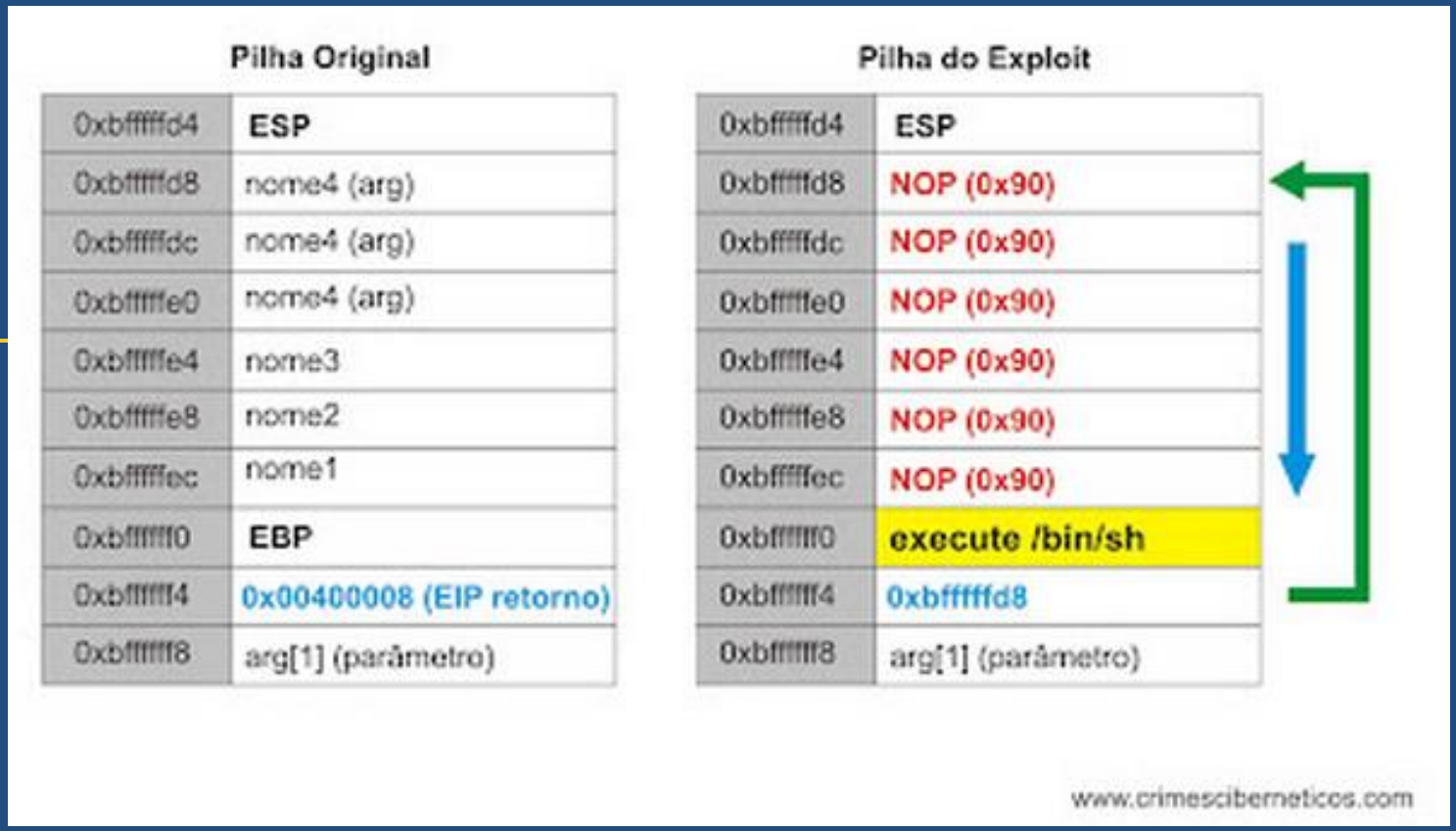
Buffer Overflow

- Técnica de exploração:
  - Descobrir uma variável do tipo buffer que esteja vulnerável
  - Verificar, no código fonte ou por tentativa/erro, os endereços onde as chamadas de função estão, bem como o endereço que marca o início do buffer da variável
  - Implementar um *exploit* que insira códigos de máquina no *buffer*, contendo instruções para abrir uma sessão *shell*, e depois encher a pilha até atingir a posição do ponteiro de retorno, lá colocando o endereço de início do buffer.

Buffer Overflow

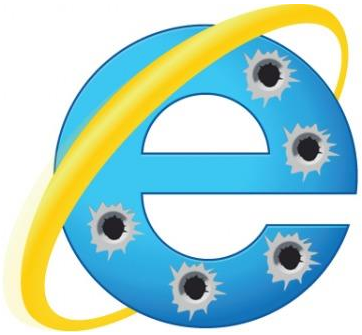


Buffer Overflow



Exploits

- Programa desenvolvido para explorar uma vulnerabilidade conhecida
- Há inúmeras vulnerabilidades não corrigidas mesmo em sistemas comercialmente regularizados, e ainda há os zero-day...
- Veja como está o seu sistema:
  - www.securityfocus.com



Artefatos Maliciosos

- Programas criados para:
  - Comprometer a Integridade e/ou a Disponibilidade
  - Em alguns casos, instalar programas para comprometer a confidencialidade
- Há tipos diferentes, com características distintas:
  - Vírus
  - Worms
  - Trojan Horses
  - Keyloggers
  - Spywares.

Vírus

- Principal característica: DEPENDE da ação humana para se propagar
- Uma vez executado, vai se replicar uma ou mais vezes, contaminando outros arquivos
- Pode destruir arquivos, consumir CPU e/ou memória, e instalar outros programas maliciosos
- Principal dificuldade para detecção: sua característica metamórfica atual

Worms

- Códigos maliciosos que se propagam SEM a ação humana, usando vulnerabilidades existentes nos sistemas
- Altíssimo potencial de propagação, é hoje a principal ferramenta de criação de redes *zombies (botnets)*

Trojan Horses

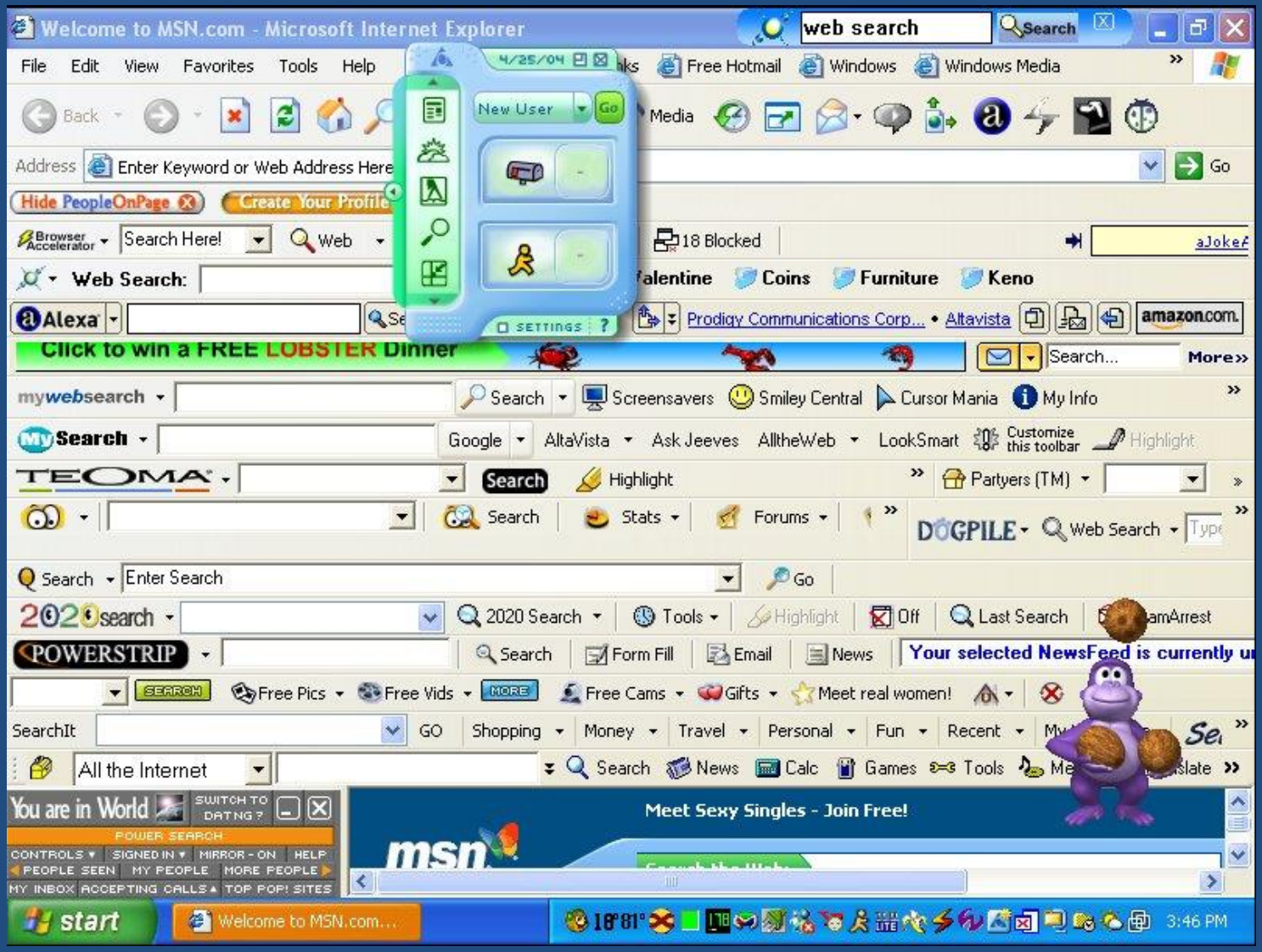
- Assim como os vírus, dependem da ação humana
- No entanto, não se propagam. Apenas realizam a tarefa para a qual foram designados
  - Instalar backdoors, rootkits, keyloggers, etc.
- São agregados a programas legítimos, passando a impressão de que não existem

Loggers

- Como o nome diz, prestam-se a capturar informações digitadas ou visualizadas
  - Senhas, credenciais de acesso, informações sigilosas
- Normalmente instalados por *trojans*
- Também podem ser físicos

NP-1

Spywares

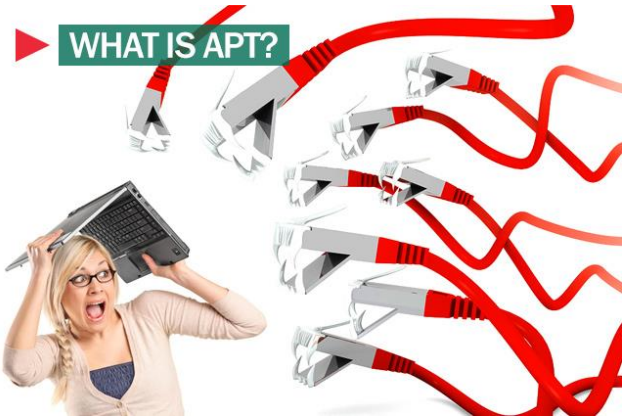

Welcome to MSN.com - Microsoft Internet Explorer
web search
Search
File Edit View Favorites Tools Help
Free Hotmail
Windows
Windows Media
Back
Media
Address
Enter Keyword or Web Address Here
Go
Hide PeopleOnPage
Create Your Profile
New User
Browser Accelerator
Search Here!
Web
18 Blocked
Web Search:
Valentine
Coins
Furniture
Keno
Alexa
Prodigy Communications Corp...
Altavista
amazon.com
Click to win a FREE LOBSTER Dinner
Search...
More»
mywebsearch
Search
Screensavers
Smiley Central
Cursor Mania
My Info
MySearch
Google
AltaVista
Ask Jeeves
AlltheWeb
LookSmart
Customize this toolbar
Highlight
TEOMA
Search
Highlight
Partyers (TM)
Search
Stats
Forums
DOGPILE
Web Search
Search
Enter Search
Go
2020search
2020 Search
Tools
Highlight
Off
Last Search
POWERSTRIP
Search
Form Fill
Email
News
Your selected NewsFeed is currently u
SEARCH
Free Pics
Free Vids
MORE
Free Cams
Gifts
Meet real women!
SearchIt
GO
Shopping
Money
Travel
Personal
Fun
Recent
All the Internet
Search
News
Calc
Games
Tools
You are in World
SWITCH TO DATING
POWER SEARCH
CONTROLS
SIGNED IN
MIRROR - ON
HELP
PEOPLE SEEN
MY PEOPLE
MORE PEOPLE
MY INBOX
ACCEPTING CALLS
TOP POP! SITES
Meet Sexy Singles - Join Free!
msn
start
Welcome to MSN.com...
3:46 PM

Spywares

BAIDU
PSAFE
AVAST
AVG
ASK
FUNMOODS
IMINENT
BABYLON
TOOLBAR
HAO123
MEU PC

Novidades...

- *APT (Advanced Persistent Threats)*
  - *Spear phishing*
- *Phish Pharm*



Defesas

- As defesas visam sempre MITIGAR os ataques
- Como há vulnerabilidades desconhecidas e/ou não-controláveis, o monitoramento contínuo é a única adoção indiscutível
- Além, do monitoramento, podemos agregar à segurança da rede os seguintes elementos:
  - Filtros de Pacotes (IP Firewall)
  - Filtros de Conteúdo (Firewall Proxy)
  - IDS/IPS (Intrusion Detection/Prevention Systems)
  - Antivírus
  - Honeypots

Filtros de Pacotes (IP Firewall)

- Camada de rede e de transporte (sockets)
- Informações básicas para permitir ou bloquear pacotes, baseados em Listas de controle de acesso (ACL – Access Control Lists)
- Filtragem com base cabeçalho do pacote TCP/IP
  - Endereço IP de origem
  - Endereço IP de destino
  - Porta de origem TCP/UDP
  - Porta de destino TCP/UDP
  - Flags do TCP (sentido das conexões)
  - Mensagens ICMP (tipos e códigos das msg)

IP Firewall

- Filtro de Pacotes:
  - Limitações de segurança
    - Serviços com características complexas (Ex.:FTP)
    - Não conseguem barrar ataques de fragmentação
    - Não verificam *payload*
    - Não guardam o estado das conexões
    - Vulnerável - IP SPOOFING
    - não oferece autenticação do usuário
  - Difíceis de configurar e administrar quando o conjunto de regras é grande
  - Dica: padrão bloquear todas as portas e deixar passar somente as que são expressamente permitidas

Firewall Proxy

- Servem para intermediar a comunicação entre cliente e servidores
- Pode trabalhar na camada de:
  - Sessão ou de transporte: ***circuit level***
    - Relay – não verifica serviços
      - Problema ! outro serviço que utilize porta 80 pode passar pelo proxy...
  - Aplicação: ***application level***
    - Payload – filtrado. Ex.: tags HTML filtradas em proxy HTTP
- Faz que o tráfego pareça ter origem no proxy, o que mascara o endereço host interno – maior segurança

Firewall Proxy de Aplicação

- Usados para armazenar caches de páginas web
- Ocultam os clientes privados (NAT)
- Podem bloquear URLs suspeitas (*blacklists*)
- Podem filtrar os *payload* antes de passá-lo ao cliente
- **Previne contra ataques de fragmentação, roteamento de origem, DoS**

- Mas...
  - Criam um ponto único de falha
  - Um proxy para cada tipo de serviço

Proxy de Aplicação

- Vantagens
  - Não permite conexões diretas entre hosts internos e externos
  - Pode implementar autenticação do usuário
  - Analisa uso de comandos no *payload* dos pacotes
  - Permite criar logs de tráfego
- Desvantagens
  - É mais lento que o filtro de pacotes
  - Requer um proxy específico para cada aplicação
  - Não trata pacotes ICMP
  - Não aceita os serviços para os quais não foi projetado
  - Requer que os clientes internos saibam sobre ele
    - Exceto proxies transparentes – redirecionam as sessões que passam pelo firewall para um serviço de proxy local de modo transparente

IDS – Intrusion Detection System

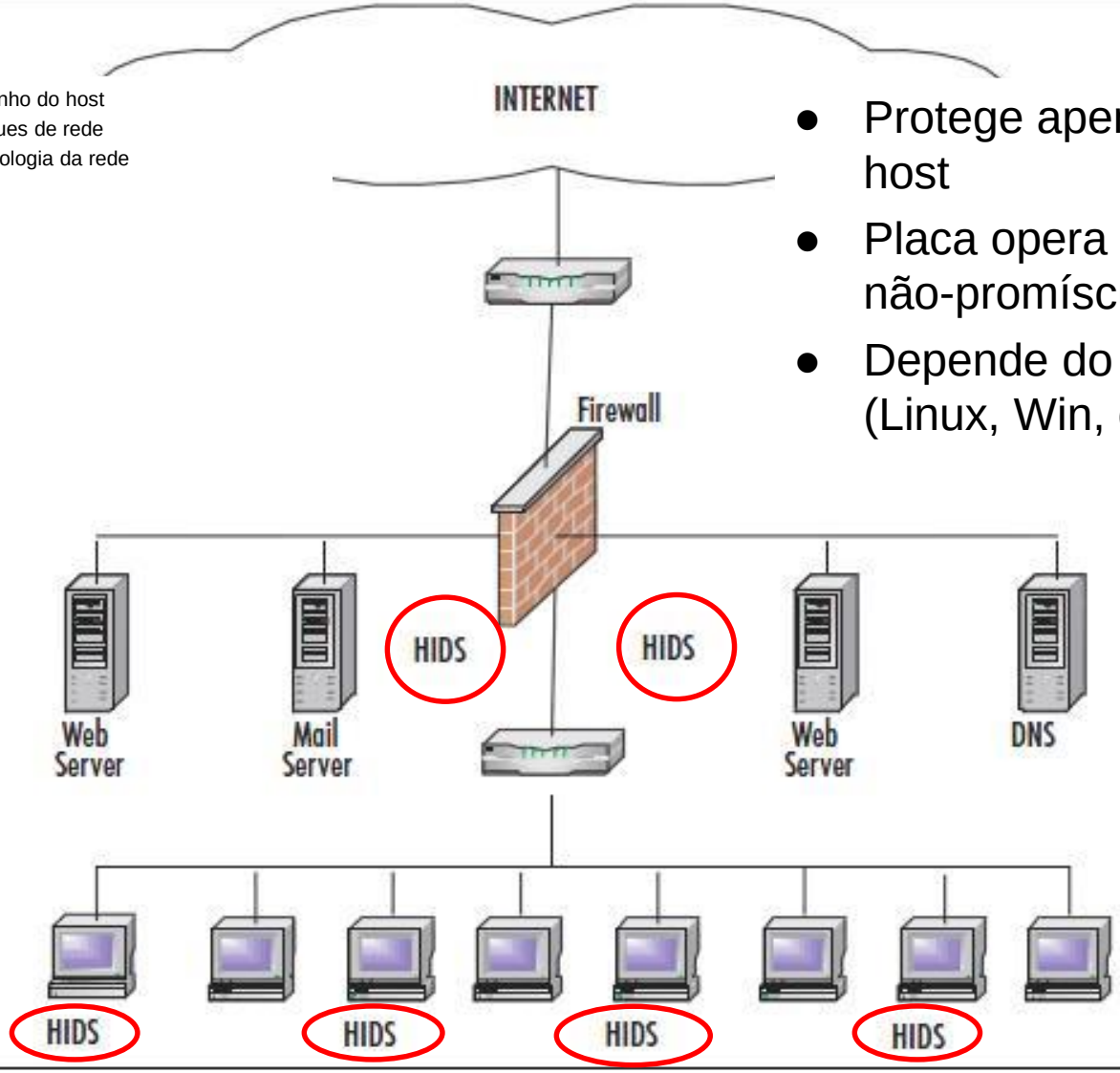
- IDS/SDI - Sistemas de **Detecção** de Intrusão
  - Ferramenta especializada que pode ler e interpretar o conteúdo de arquivos de log de roteadores, firewalls, servidores e outros dispositivos de redes (passivo)
  - Utilizam banco de dados de assinaturas de ataque conhecidas
  - Pode comparar padrões de atividade, tráfego ou comportamento no tráfego monitorado, comparando com assinaturas, emitindo alertas

SDI (IDS) - Sistemas de Detecção de Intrusão

- O SDI (IDS) pode ter a capacidade de manter o "estado" dos pacotes, remontar os fragmentos e depois fazer a análise.
- De acordo com sua localização:
  - de hosts (SDIH) (inglês: HIDS)
  - de rede (SDIR) (inglês: NIDS)
- Dois métodos de detecção ou estratégias de análise de evento:
  - Detecção de assinaturas
    - Banco de dados com assinaturas de ataques
  - Detecção de anomalia
    - Regras e conceitos pré-definidos sobre atividades "normais" e "anormais" chamadas *heurísticas.*

SDIH (HIDS) – Sistema de Detecção de Intrusão de Hosts

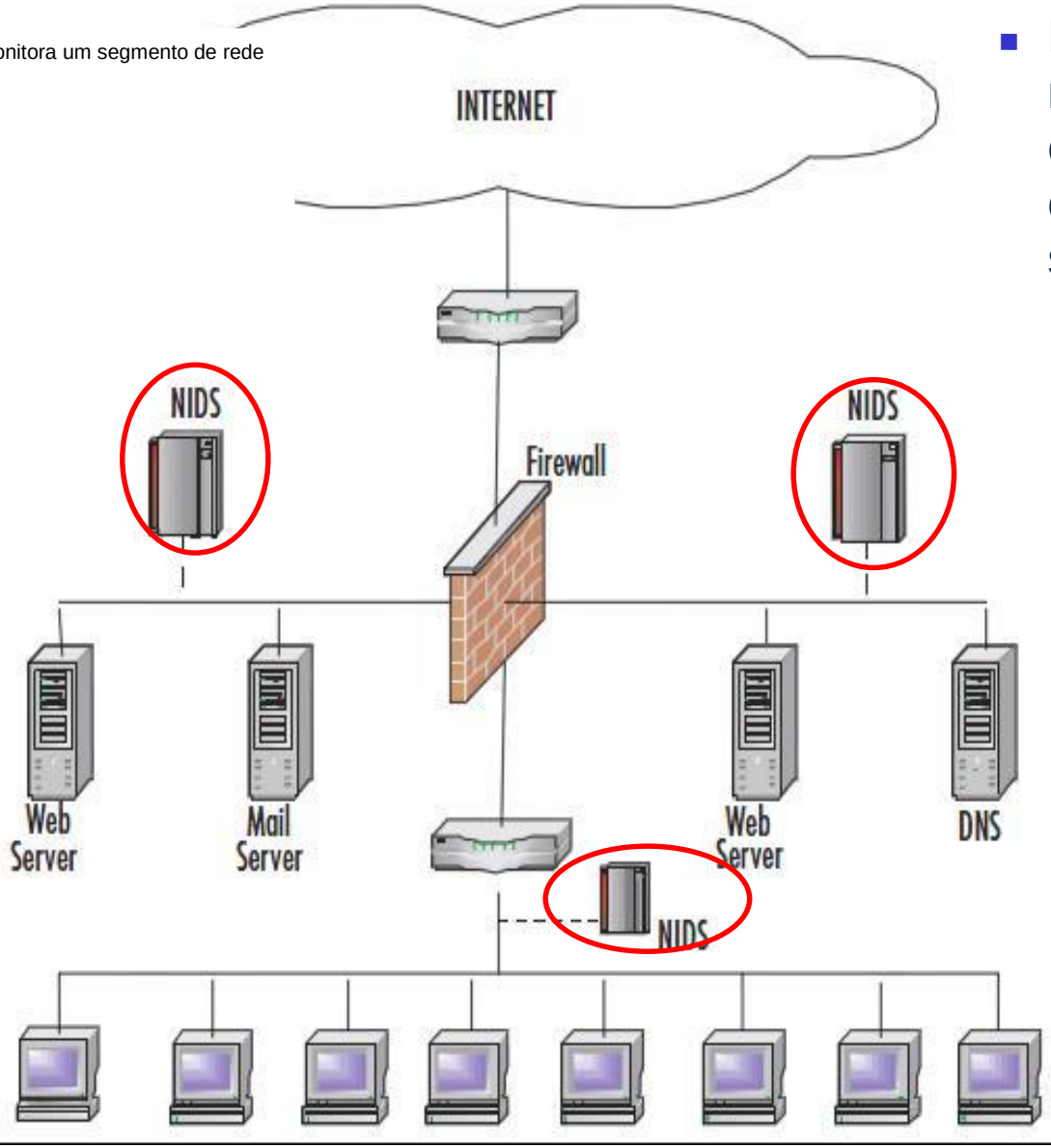
- Diminui desempenho do host
- Não detecta ataques de rede
- Independe da topologia da rede



- Protege apenas o host
- Placa opera no modo não-promíscuo
- Depende do SO (Linux, Win, etc.)

SDIR (NIDS) – Sistema de Detecção de Intrusão de Rede

- Monitora um segmento de rede



- Deve operar em modo promíscuo para captar todas as comunicações no segmento de rede

- Port scanning, ip spoofing, tear drop, podem ser detectados, pois há a analise do cabeçalho e payload

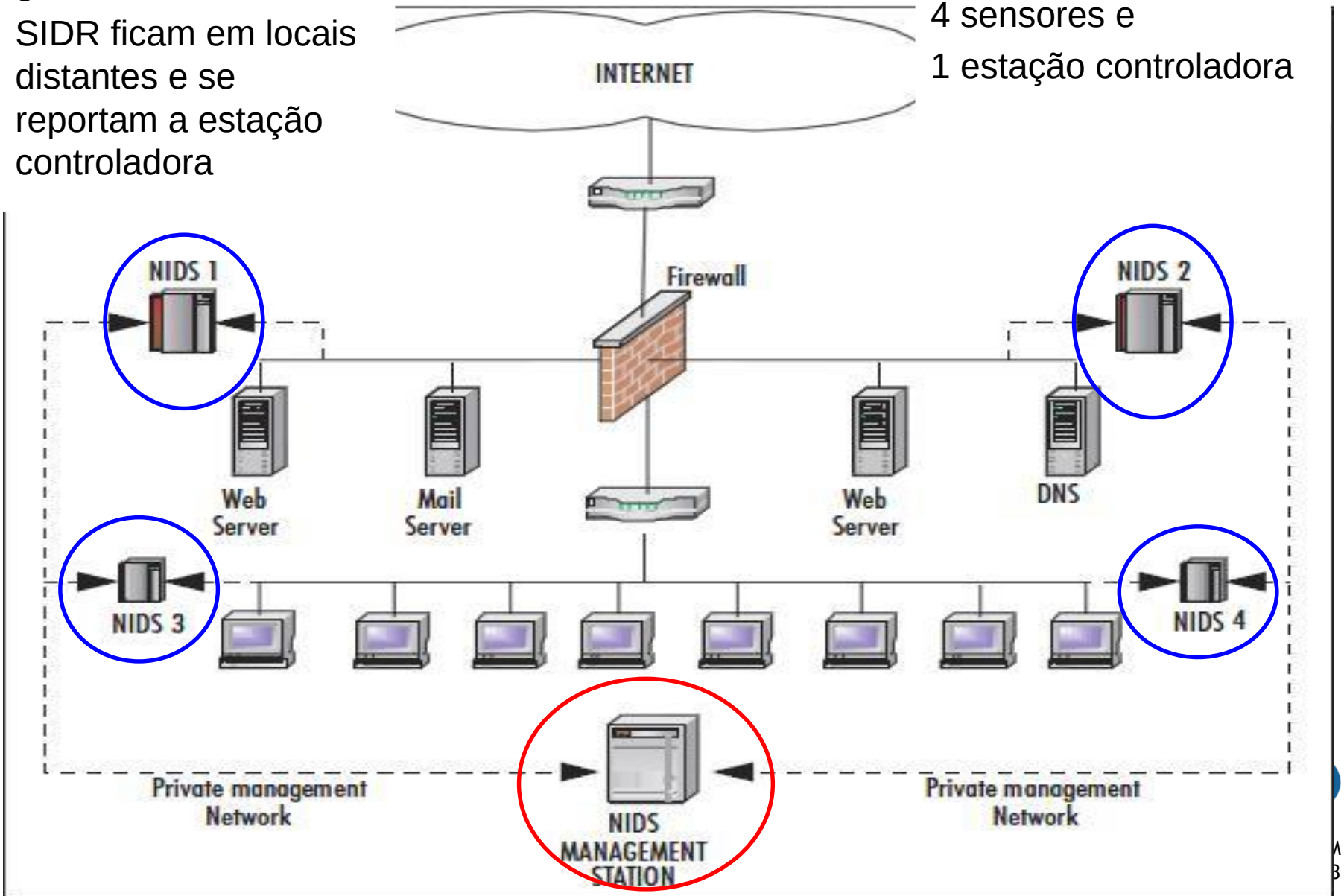
SDID – Sistema de Detecção de Intrusão Distribuídos

- Possui estação de gerenciamento
- SIDR ficam em locais distantes e se reportam a estação controladora

- Na fig. Temos:

4 sensores e

1 estação controladora



IPS – Intrusion Prevention System

- SPI (IPS) - Sistema de Prevenção de Intrusão
- Operação *in line*
  - Capaz de detectar (supor) os ataques e bloqueá-los
  - Grande problemas são os “falsos positivos” e “falsos negativos”

Honeypot x Honeynet

- Honeypot é um recurso preparado especificamente para ser sondado, atacado ou comprometido e para registrar essas atividades. Tipos:
  - De produção – adiciona segurança para organização; usado para ajudar a mitigar riscos
  - De pesquisa – não agrega segurança, usado para aprender como os atacantes estão trabalhando

- Honeynet é uma rede projetada especificamente para ser comprometida e utilizada para observar os invasores. Essa rede normalmente é composta por sistemas reais e necessita de mecanismos de contenção eficientes e transparentes, para que não seja usada como origem de ataques e também não alertar o invasor do fato dele estar em uma honeynet