Checkhosts

Monitoramento e Gerência de Sistemas

**Anderson Alves, Fernando Spencer, Marcelo Portes,
Márcio de Albuquerque e Marita Maestrelli**

ceo@cbpf.br

Rio de Janeiro
Dezembro de 2003

Agenda

1. Introdução

- **Crescimento da rede e da diversidade**

- Acesso fácil a informação ⇒ riscos
- Informação valiosa pode ser perdida, roubada, corrompida, mal-utilizada e/ou o sistema pode ser corrompido
- O intruso esconde as evidencias da atividade não autorizada

Preocupação de todos

Ataques – Motivações e Agentes

Motivações

- Simples curiosidade
- Notoriedade
- Lucro
- Vingança
- Investigação Legal

Agentes

- Alunos
- Espiões
- Administradores de Rede
- Amparados pela lei
- "Turista acidental"
- Kids ?

Porque investir na S.I. ?

- **Crescente número de ameaças**
  - Recursos cada vez mais complexos
  - Ferramentas de ataques mais poderosas
- **Proteger**
  - Competitividade
  - Hora de trabalho
  - Cumprimento da política de segurança
  - Imagem
- **Ações de S.I. mais comuns**
  - Firewalls
  - Sistema de detecção de intrusos (IDS)
  - Contínua troca de senhas
  - Monitoraramento dos usuários

Trancar tudo é impossível !

Técnicas de Ataques

- **Técnicas mais comuns**
  - Monitoramento / cópia de transmissões
    - Sniffing
  - Exploração de Erros de
    - Configuração de serviços e permissões
    - Programação (exploit, buffer overflow)
  - Negação de Serviço
  - Backdoor
  - Varreduras
    - Hosts e redes
    - Engenharia Social

Variedades de ferramentas

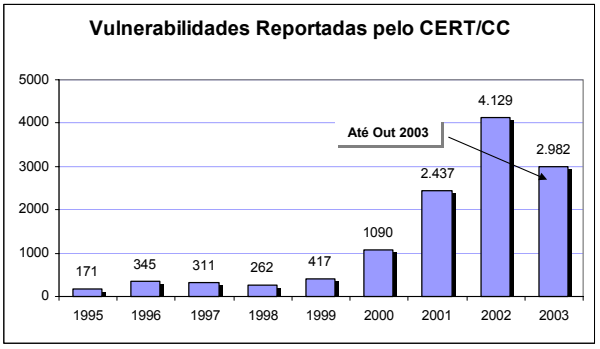
Vulnerabilidades

Vulnerabilidade:

Falha que pode ser explorada por alguém que não é autorizado a usar um recurso

Causa: erro de projetos ou falhas na implementação do sistema

- Executar comandos como outro usuário
- Acessar dados restritos
- Colocar uma entidade desconhecida no sistema
- Conduzir um "denial of service"



Fonte: Computer Emergency Response Team / Coordination Center – CERT/CC

Dados até 17 Outubro 2003

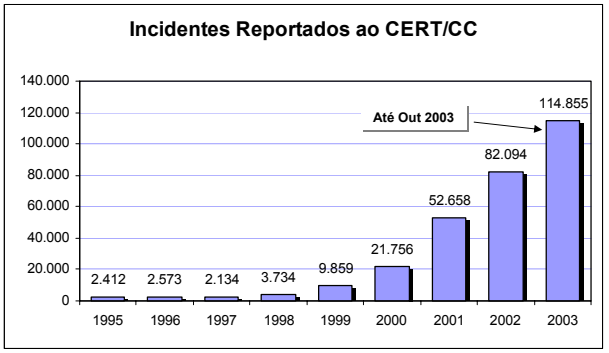
Quando uma vulnerabilidade é aproveitada comprometendo o sistema ou a informação ⇒ incidente de segurança

Incidentes

Incidentes de segurança:

- Definidos de acordo com as regras locais de uma entidade
- O que para uns é um incidente para outros pode não ser

Na prática: pode ser definido como uma atividade nas máquinas ou na rede que possa ameaçar a segurança dos sistemas computacionais.



Fonte: Computer Emergency Response Team / Coordination Center – CERT/CC

Dados até 17 Outubro 2003

Ambiente de Rede

CBPF

- Coordenação de Engenharia e Operações da Rede Rio
- Ponto de presença da RNP-RJ
- Importante ponto de troca de tráfego acadêmico
- Sistema de gerência descentralizado e redundante
- Análise e previsão de tráfego
- Monitoramento de páginas HTML
- Gerência de fluxo de tráfego no backbone

Sistema de Gerência Pró-Ativo

Painel Eletrônico

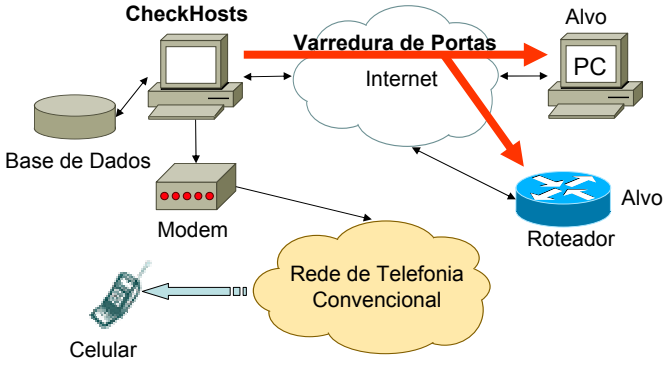
Necessidade de monitorar serviços em equipamentos

Alertar possíveis comprometimentos

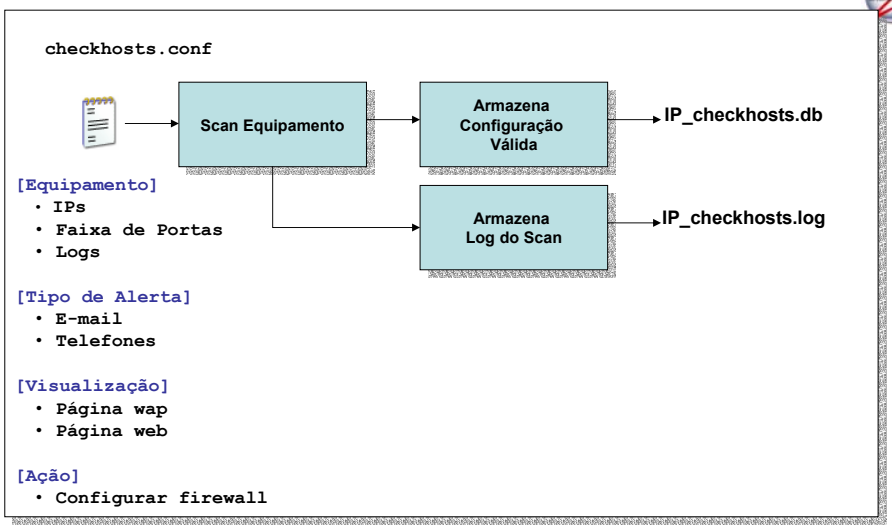
Desenvolvimento do Checkhosts

2. Sistema CheckHosts

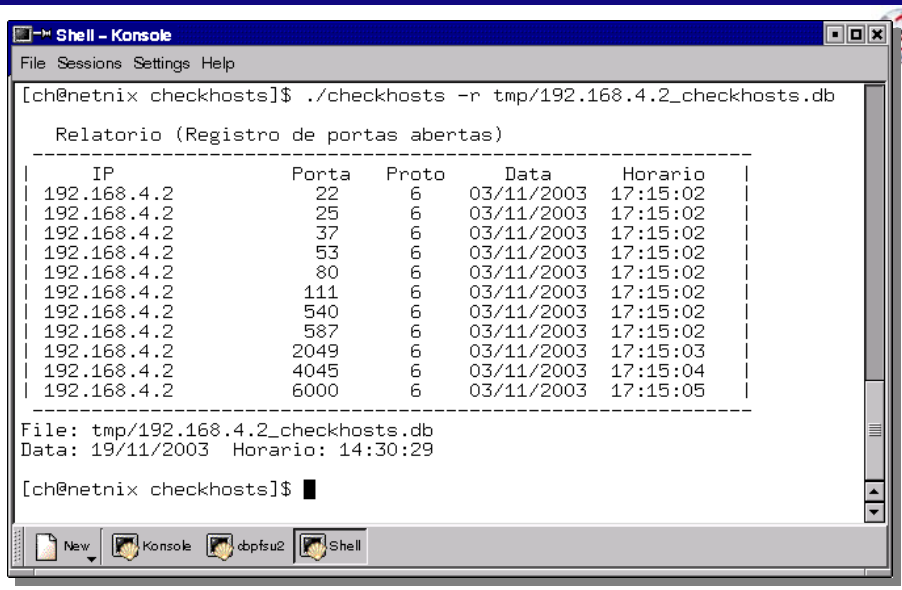
Diagrama Esquemático



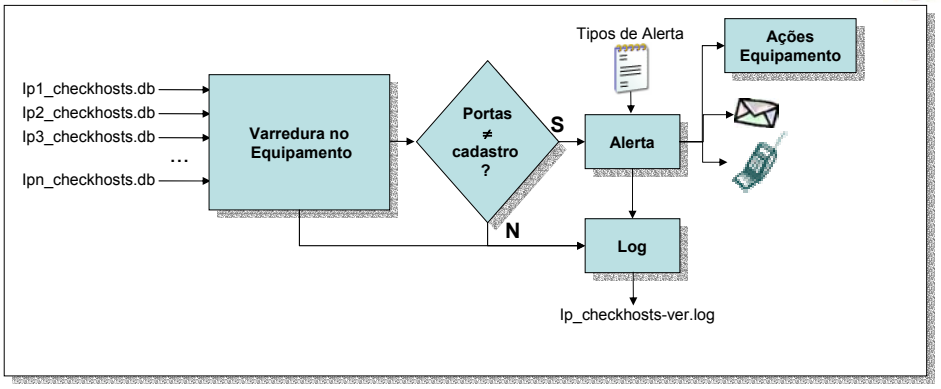
Etapa de Cadastro



Relatório do Cadastro



Etapa de Monitoramento



3. Estrutura do Sistema

Varredura de Portas TCP e UDP

O # **IP** e a **porta** permitem que **qualquer** aplicativo em uma **máquina** em rede seja **identificado** de forma exclusiva

- **Porta de Origem:** identifica o aplicativo na estação local que solicitou a transferência de dados
- **Porta de Destino:** definido pelo serviço solicitado a estação destino

A IANA (Internet Assigned Numbers Authority) define os números de portas reservados (On-line database ou antiga RFC 1700)

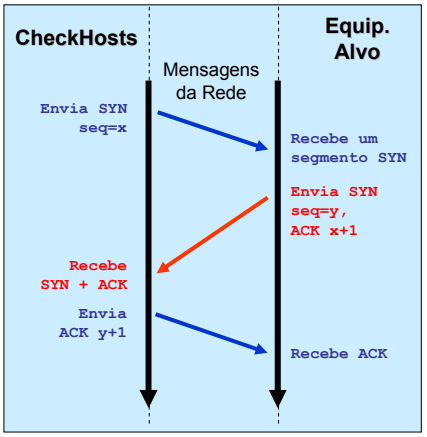
- http://www.iana.org/numbers.htm (atualizações)
- **atribuídos:** [0, 1023] (não devem ser usadas)
- **registrados:** [1024, 65535] (registrados por empresas)
- **dinâmicos :** [1024, 65535]

Portas ≥ 1024
- podem ser usadas livremente

Protocolo TCP

Como verificar se a porta TCP está em estado de escuta ?

Seqüência de mensagens em um handshake de três vias



Estabelecimento de uma conexão TCP

Handshake de três vias

- **Segmento 1:** bit SYN no campo de código
- **Segmento 2:** bits SYN e ACK confirmando o primeiro SYN e continuando o handshake
- **Segmento 3:** mensagem final de confirmação

Garante que ambas as extremidades estão prontas para transmitir dados

Checkhost encerra a conexão

Exemplo Porta TCP Aberta

TCPdump

```
# tcpdump  host 192.168.y.y -x
tcpdump: listening on eth1
```

Seqüência #1: SYN

```
11:58:47.450932 netnix.44736 > 192.168.y.y.telnet
112138132[|tcp]> (DF) [tos 0x10]
4510 003c b7b0 4000 4006 c73e c814 5e46   IP
9854 fd0d aec0 0017 377f a024 0000 0000
a002 16d0 d0bb 0000 0204 05b4 0402 080a   TCP
06af 1794 0000
```

SYN

Seqüência #2: SYN + ACK

```
11:58:47.453291 192.168.y.y.telnet > netnix.44736:
143536982 112138132,nop,[|tcp]> (DF)
4500 0040 afdb 4000 3e06 d11f 9854 fd0d   IP
c814 5e46 0017 aec0 d1b9 9b2b 377f a025
b012 6028 cc82 0000 0101 080a 088e 3356   TCP
06af 1794 0103
```

SYN ACK

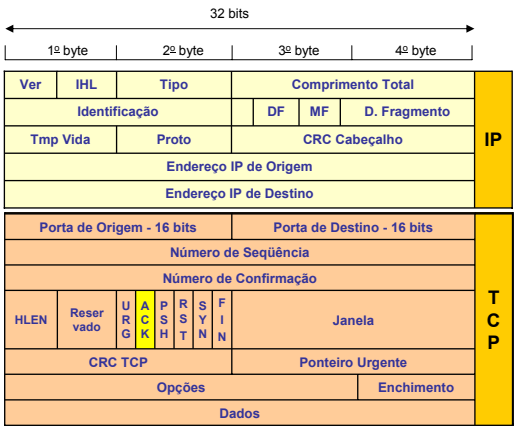
Seqüência #3: ACK

```
11:58:47.453353 netnix.44736 > 192.168.y.y. ack 1
112138133 143536982> (DF) [tos 0x10]
4510 0034 b7b1 4000 4006 c745 c814 5e46   IP
9854 fd0d aec0 0017 377f a025 d1b9 9b2c
8010 16d0 56a5 0000 0101 080a 06af 1795   TCP
088e 3356
```

ACK

Fonte: TCPDump trace

Cabeçalho IP-TCP



Fonte: Comer, D.E. – Interligação em Rede com TCP/IP

Exemplo Porta TCP Fechada

TCPdump

```
# tcpdump  host 192.168.y.y.3333  -x
tcpdump: listening on eth1
```

Seqüência #1: SYN

```
12:01:17.575821 netnix.44742 > 192.168.y.y.3333
112153145[|tcp] > (DF) [tos 0x10]
        4510 003c c585 4000 4006 2884 c814 5e46   IP
        c814 5e33 aec6 0d05 40f2 97bc 0000 0000
SYN     a002 16d0 f731 0000 0204 05b4 0402 080a   TCP
        06af 5239 0000
```

Seqüência #2: Reset + ACK

```
12:01:17.580908 192.168.y.y.3333 > netnix.44742
        4510 0028 3b43 4000 4006 b2da c814 5e33   IP
        c814 5e46 0d05 aec6 0000 0000 40f2 97bd
Reset
ACK     5014 0000 ceb2 0000 0204 05b4 0402        TCP
```

Fonte: TCPDump trace

Cabeçalho IP-TCP

32 bits

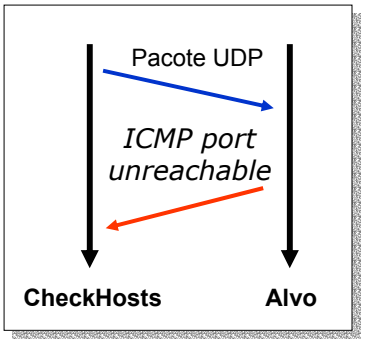
1º byte	2º byte	3º byte	4º byte	
Ver	IHL	Tipo	Comprimento Total	IP
Identificação		DF / MF	D. Fragmento	IP
Tmp Vida		Proto	CRC Cabeçalho	IP
Endereço IP de Origem				IP
Endereço IP de Destino				IP
Porta de Origem - 16 bits			Porta de Destino - 16 bits	TCP
Número de Seqüência				TCP
Número de Confirmação				TCP
HLEN	Reservado	URG ACK PSH RST SYN FIN	Janela	TCP
CRC TCP			Ponteiro Urgente	TCP
Opções			Enchimento	TCP
Dados				TCP

Fonte: Comer, D.E. – Interligação em Rede com TCP/IP

Protocolo UDP

Como saber se a porta UDP está em estado de escuta ?

- Ao receber ICMP *port unreachable,após o envio de um pacote UDP* o CheckHosts marca a porta como fechada.



Exemplo: Porta UDP

Envio de pacote UDP

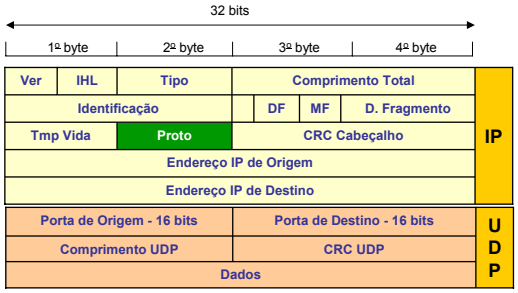
Pacote IP-UDP

UDP

```
4500 0024
0000 4000
4011 ee26
c814 5e46
c814 5e33
8349 e0e1
0010 c97a
6161 6161 ...
```

Fonte: TCPDump trace

Cabeçalho IP-UDP



Fonte: Comer, D.E. – Interligação em Rede com TCP/IP

Exemplo: Porta UDP

Exemplo UDP ⇒ ICMP *port unreachable*: porta fechada.

Pacote IP-ICMP

ICMP

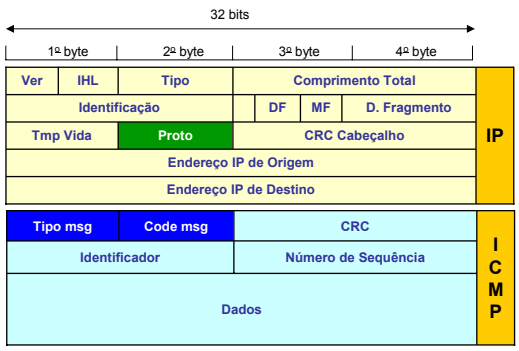
Porta destino NÃO acessível

```
4500 0040
710b 4000
ff01 be0e
c814 5e33
c814 5e46
0303 49c1
0000 0000
```

```
4500 0024 0000 4000
4011 ee26 c814 5e46
c814 5e33 8349 e0e1
                ...
```

Fonte: TCPDump trace

Cabeçalho IP-ICMP



Fonte: Comer, D.E. – Interligação em Rede com TCP/IP

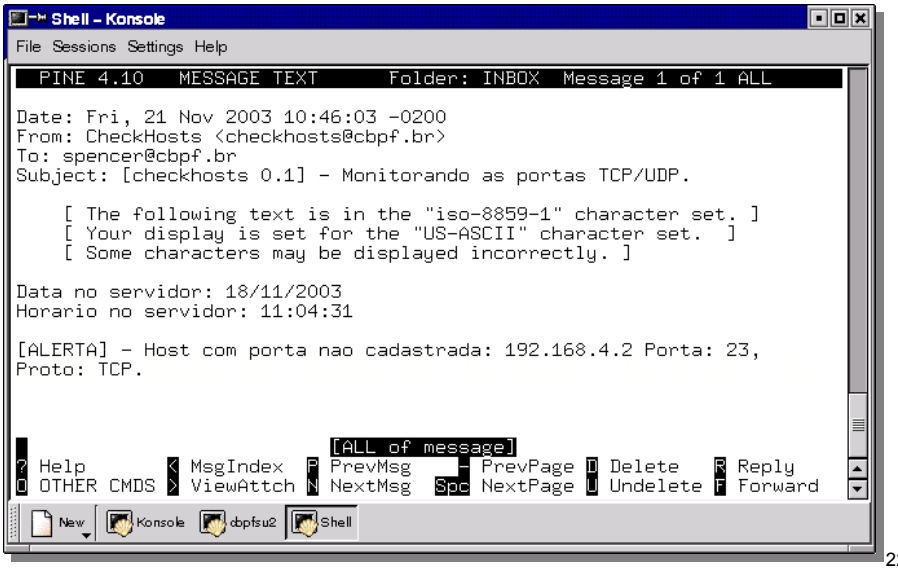
Pacote IP-UDP enviado anteriormente

Tipos de Alertas

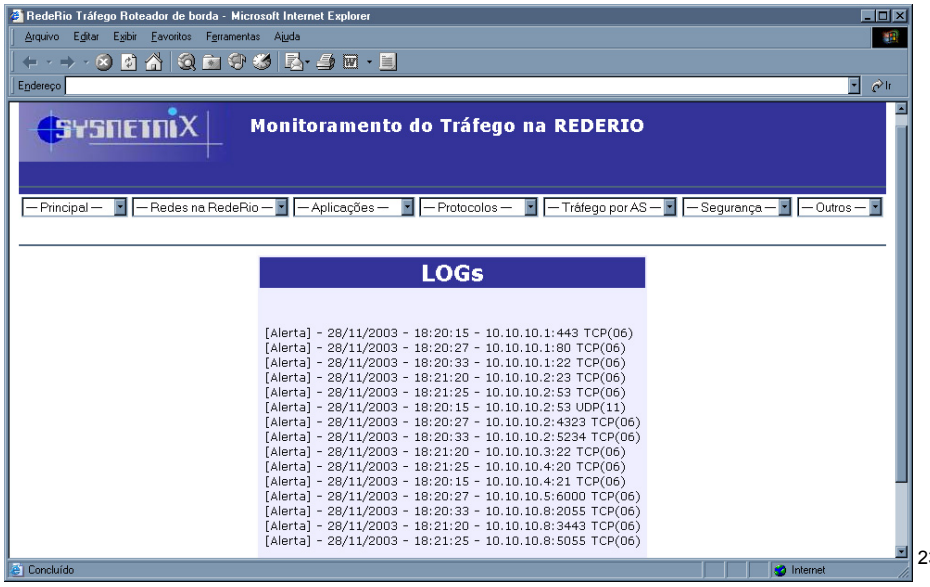
Tipos de Alerta

- Logs
- Via WEB
- Via WAP
- Via e-mail
- Ligação Celular

Exemplo de Alerta via E-mail

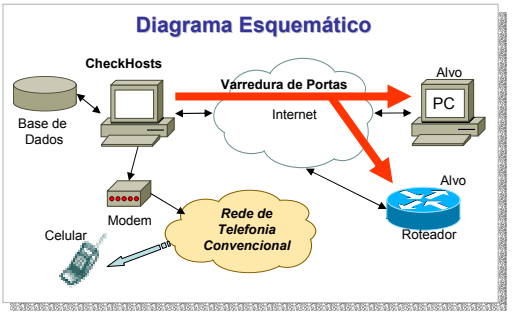


Exemplo de Histórico via Web



Alerta via Celular

Uso da tecnologia WAP



Ação do CheckHosts

- Sistema interagindo com firewall
- Bloqueio do serviço
- Ação rápida e automática
- Aumenta o tempo para intervenção humana
- Problema resolvido (temporariamente)

Segurança no CH

- **Softwares:**
  - Kernel e SO otimizados (só o necessário)
  - Verificar assinatura dos arquivos do sistema (AIDE ou Tripwire)
  - Habilitação de logs
  - Atualização periódica do SO e dos utilitários
  - Eliminar programas servidores desnecessários
  - Filtro de pacotes sem atrapalhar as varreduras de portas
- **Hardware**
  - Ponto de rede confiável e em posição estratégica
  - No Breaks
- **Acesso:**
  - Acesso restrito e criptografado (SSH)
  - Instalação de um Sistema Detecção de Intrusos (tipo snort)
    - cuidado com falsos alarmes

4. Estudo de Casos

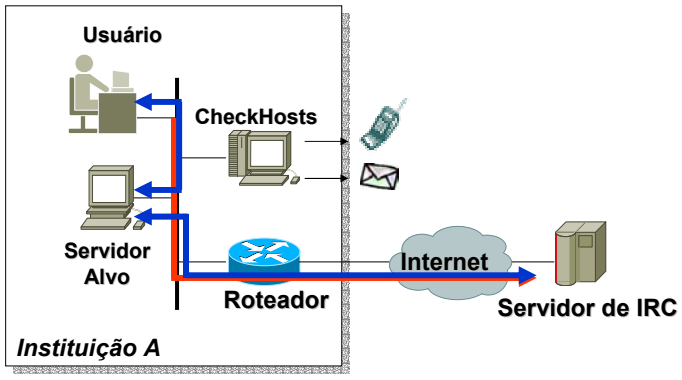
Exemplos de atuações do CheckHosts

1. Usuário local utilizando programa não autorizado

2. Invasão de um servidor

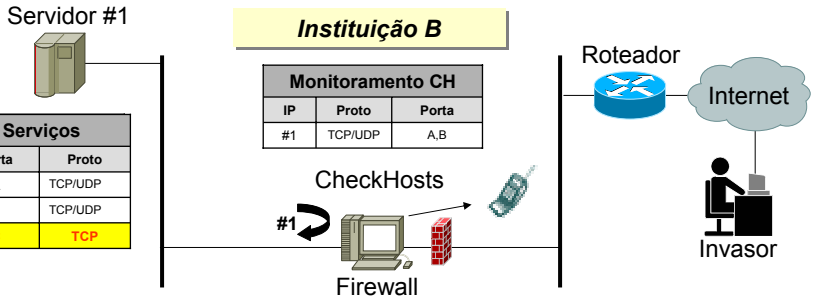
Caso 1

Usuário local utilizando programa não autorizado



Caso 2

Invasão de um servidor em rede local



t_0 – Configura o CH e o Firewall

t_1 – Invasor aproveita vulnerabilidade nos serviços de A e B e instala uma backdoor no Servidor #1

Regras do Firewall

IP	Permit/Deny	Porta	In/Out	Proto
#1	Deny	C	IN	TCP
#1	Permit	A,B	IN	TCP/UDP
#1	Permit	> R1 < R2	IN	TCP
#1	Deny	others	IN	TCP/UDP

Ação do Checkhosts bloqueia a participação do Servidor #1 no ataque

5. Perspectivas

Atualizações previstas

- Base de dados encriptada
- Alertar quando serviço é parado
- Verificar assinatura dos serviços
- Utilizar "*half-scan*" na varredura TCP
- Gerência via WEB

Conclusão

- Ferramenta para monitoramento de serviços
- Comparação dos estados de equipamentos
- Alertas gerados rapidamente
- Ações de bloqueio de serviços
- Software Livre

A Informação

"Cabe lembrar que o mais importante sempre será a informação.

A área de segurança trabalha numa tênue linha que visa proteger a informação, porém sem bloquear ou censurar"

Obrigado !!!

Checkhosts

Monitoramento e Gerência de Sistemas

Anderson Alves de Albuquerque – aaa@cbpf.br
Fernando Spencer – spencer@cbpf.br
Marcelo Portes de Albuquerque – marcelo@cbpf.br
Márcio Portes de Albuquerque – mpa@cbpf.br
Marita Maestrelli – marita@cbpf.br

Rio de Janeiro
Dezembro de 2003