Uma Ferramenta para Monitoramento de Serviços de Rede

Anderson Alves de Albuquerque
Fernando Spencer
Marcelo Portes de Albuquerque
Marcio Portes de Albuquerque
Marita Maestrelli

{aaa, spencer, marcelo, mpa, marita}@cbpf.br

CAT / CBPF

Abstract

Despite the increase of security of computers and network we are still observing and reporting a great number of new types of attacks and intruder tools. In this article we present a network detection system, Checkhost, which periodically checks for new TCP/UDP ports and vulnerability in equipments of a network. New services are commonly enabled after exploiting network vulnerabilities. In a situation where new unauthorized services as backdoors, worms or scripts are detected, this monitoring tool can automatically reconfigure the system firewall and generate different types of alerts. The system was developed in ANSI C and is available for UNIX platforms.

Resumo

Apesar do aumento na segurança dos computadores e das redes na Internet, estes continuam sendo alvos de constantes invasões. A presença de falhas na segurança criou a necessidade de um monitoramento permanente dos serviços disponíveis. Este artigo descreve um sistema denominado Checkhosts que procura periodicamente alterações nas portas TCP/UDP de equipamentos definidos pelo administrador de rede. Em casos de comprometimento através da instalação de um *backdoor*, *worms* ou de programas não autorizados, é usual a adição de novos serviços. Ao detectar um desses casos, uma reconfiguração do sistema de firewall é realizada e vários tipos de alerta são gerados. O sistema foi desenvolvido em ANSI C para ambiente UNIX.

INDICE

1. Introdução

O crescimento e popularização das redes IP trouxe também insegurança para os usuários. A diversidade de sistemas operacionais, hardwares, fabricantes e softwares trazem uma incerteza do que está realmente funcionando em nossos computadores. De acordo com as estatísticas do CERT ("*Computer Emergency Response Team*" [1], órgão que atua na prevenção de incidentes de segurança na rede) foram notificados mais de cem mil incidentes de segurança no ano 2003 contra oitenta mil no ano anterior. A segurança da rede passou a ser uma preocupação de todos, não apenas dos administradores de redes, mas também dos usuários que recebem correspondências eletrônicas infectadas com vírus e *worms* [2, 3]. Diversos especialistas têm se preocupado em construir ferramentas que permitam aos gerentes de sistemas computacionais verificar a segurança e a integridade de suas redes, equipamentos e dados, tais como: nmap, nagios, nessus etc [4, 5, 6]. No entanto, essa é uma tarefa complexa, pois exige uma constante vigilância de serviços disponibilizados pelos recursos computacionais e pelos usuários.

Este trabalho partiu da necessidade que temos na Rede-Rio e no CBPF de monitorar a infra-estrutura de rede (local e metropolitana) a fim de garantir os serviços atualmente oferecidos. O CBPF é hoje um importante ponto de troca de tráfego nacional, regional e metropolitano abrigando os pontos de troca de tráfego das redes acadêmicas brasileiras (Rede Nacional de Ensino e Pesquisa - RNP) e metropolitana (Rede-Rio de Computadores). As necessidades de monitoramento e garantias dos serviços é hoje uma peça fundamental para a estabilidade dessas redes. Além disso, a diversidade de usuários encontrados na área acadêmica faz com que os problemas sejam freqüentes, diversos e complexos. Em busca de uma ferramenta de uso simples fomos motivados a desenvolver um sistema capaz de monitorar periodicamente os principais servidores da rede e alertar os gerentes de possíveis comprometimentos aos equipamentos.

2. Funcionamento da Ferramenta

A ferramenta em utilização no CBPF recebe o nome de Sistema Checkhosts.

A Figura 1 apresenta um diagrama esquemático do Sistema Checkhosts, que é composto dos seguintes dispositivos:
i) um microcomputador conectado a Internet e a um modem com acesso a linha telefônica, sistema operacional Unix e executando o programa Checkhosts;
ii) um ou vários equipamentos alvos (roteadores, servidores, impressoras, etc) no qual estarão sendo verificados periodicamente os serviços de rede disponíveis;

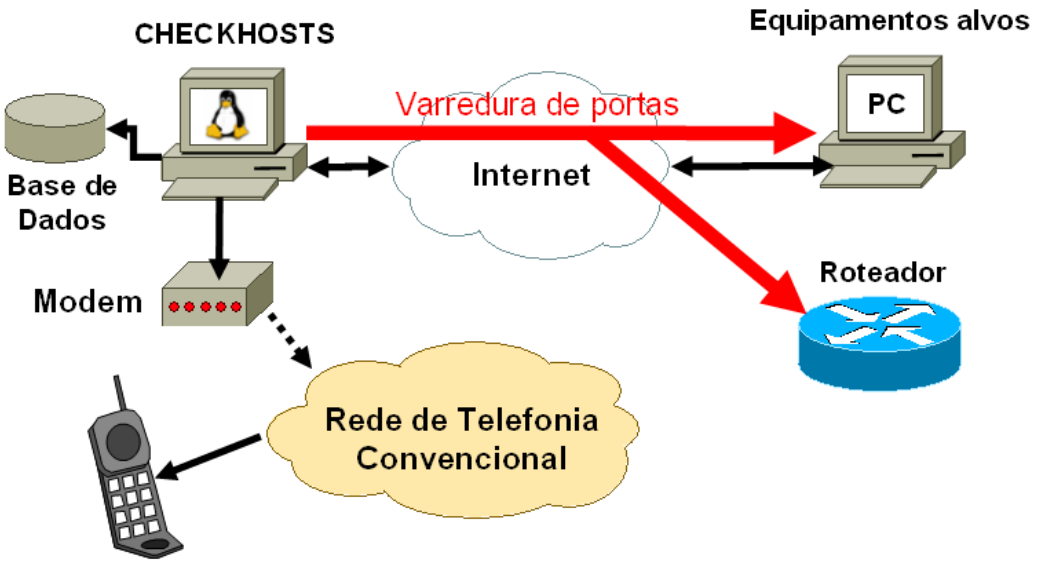


Figura 1 – Arquitetura do Sistema Checkhosts: o programa de monitoramento está situado no microcomputador à esquerda que varre o equipamento alvo em busca de modificações nos serviços por ele disponibilizado. O resultado será comparado com o estado armazenado previamente. No caso de modificação um alerta pode ser enviado via telefonia celular.

O Checkhosts está dividido em duas partes, cadastro e monitoramento. Na primeira parte o sistema varre os equipamentos alvos cadastrando os serviços disponíveis e gera a base de dados em formato binário, contendo as informações referentes aos serviços oferecidos. Esta etapa é realizada na inicialização do sistema ou nos instantes em que o administrador modificar os serviços. Nesta parte, o administrador deve também configurar, utilizando um arquivo texto, os tipos de alerta que devem ser gerados para cada equipamento alvo: relatório (*logs*), e-mail, ligação telefônica e/ou bloqueio da porta. A opção de bloqueio da porta só pode ser realizada no caso do Checkhosts estar sendo executado no mesmo computador que realiza o serviço de "*firewall*". Neste caso, o Checkhosts reconfigura a permissão de acesso bloqueando a porta TCP/UDP no "*firewall*" para a máquina alvo, que não está em conformidade com as regras da base de dados.

O conjunto de dados coletados pelo programa armazena as informações necessárias para efetuar a comparação, e segue a seguinte estrutura:

```
struct _reg{
   unsigned int IP_N[4];      // Endereço IP do equipamento alvo
   unsigned int porta;        // Portas TCP ou UDP
   char protocolo;            // TCP ou UDP
   unsigned int data[3];      // Formato DD/MM/YYYY
   unsigned char horario[3];          // Formato: HH:MM:SS
}reg;
```

O esquema do cadastramento é visto na Figura 1.1.

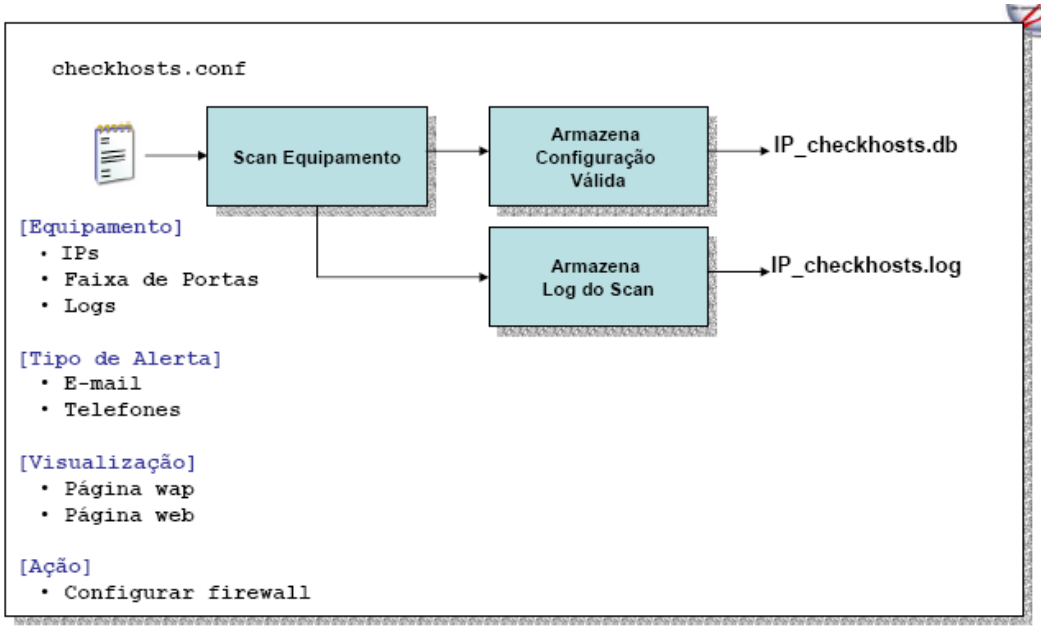


Figura 1.1 – Esquema do cadastramento

Após o cadastramento é possível verificar os serviços disponíveis nos equipamentos alvos, i.e. o estado que deve ser comparado periodicamente pela etapa de monitoramento, Figura 2.

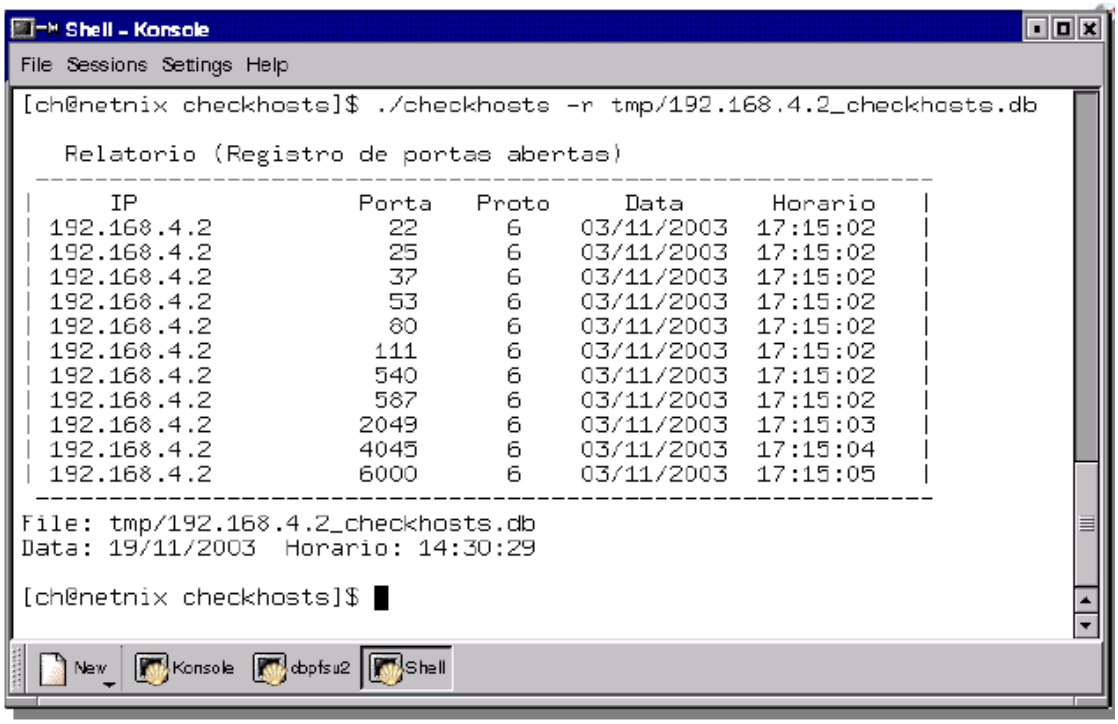


Figura 2 – Exemplo de uma auditoria realizada em um equipamento alvo. A listagem corresponde as portas disponíveis em um servidor oferecendo serviços de SSH, SMTP, TIME, DNS, PORTMAP, UUCP, NFS E X11.

Na etapa de monitoramento, o Checkhosts questiona periodicamente os equipamentos alvos verificando os serviços que eles estão disponibilizando e os compara com aqueles obtidos na fase de cadastro (Figura 3).

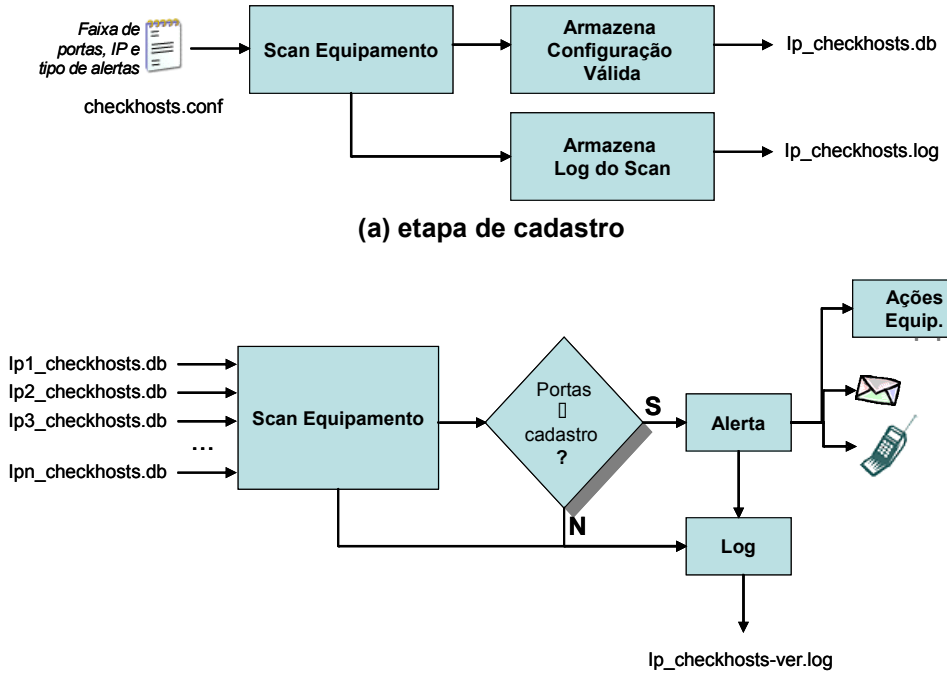


Figura 3 – Diagrama de funcionamento do sistema Checkhosts. (a) etapa de cadastro do equipamento alvo. (b) etapa de monitoramento do equipamento alvo.

3. Estrutura

Para a construção da ferramenta fomos motivados ao desenvolvimento próprio da função de varredura (*scan*). Isto permitiu garantir a independência de um programa externo e ter um formato com um padrão simples e estático [7].

A função "*scan*" tem a finalidade de realizar a varredura das portas a fim de detectar os serviços ativos. Este procedimento é efetuado através do envio de um pacote a porta de destino (TCP/UDP). O procedimento que estabelece a conexão utiliza o *flag* de controle de sincronização (SYN) e envolve a troca de três mensagens. Este procedimento é conhecido como "*three-way handshake*"[1]. Esse procedimento é repetido para todas as portas a serem verificadas. No caso do protocolo TCP será realizado um "*three-way handshake*" (a estrutura gráfica pode ser observada na Figura 3.1) completo,

[1] O procedimento "*three-way handshake*" é voltado para o estabelecimento de uma conexão TCP entre equipamentos A e B. Esse inicia com o envio de um pacote com o *flag* de sincronização (SYN) de A para B a fim de checar se este último está pronto para o estabelecimento da conexão TCP. Uma vez o equipamento B pronto para estabelecer a conexão TCP, ele responde por meio de um único pacote com os *flags* SYN e ACK. Por fim, A envia de volta para B um novo pacote com o *flag* de controle ACK ativo, concluindo as três etapas do procedimento [8, 11].

e caso os equipamentos envolvidos na comunicação finalizem este processo a porta será considerada aberta para conexão. Para a verificação de serviços utilizando o protocolo UDP o Checkhosts envia um pacote UDP para a porta destino, e verifica a ausência de serviços por meio do recebimento da resposta "*ICMP port unreachable*" [7].

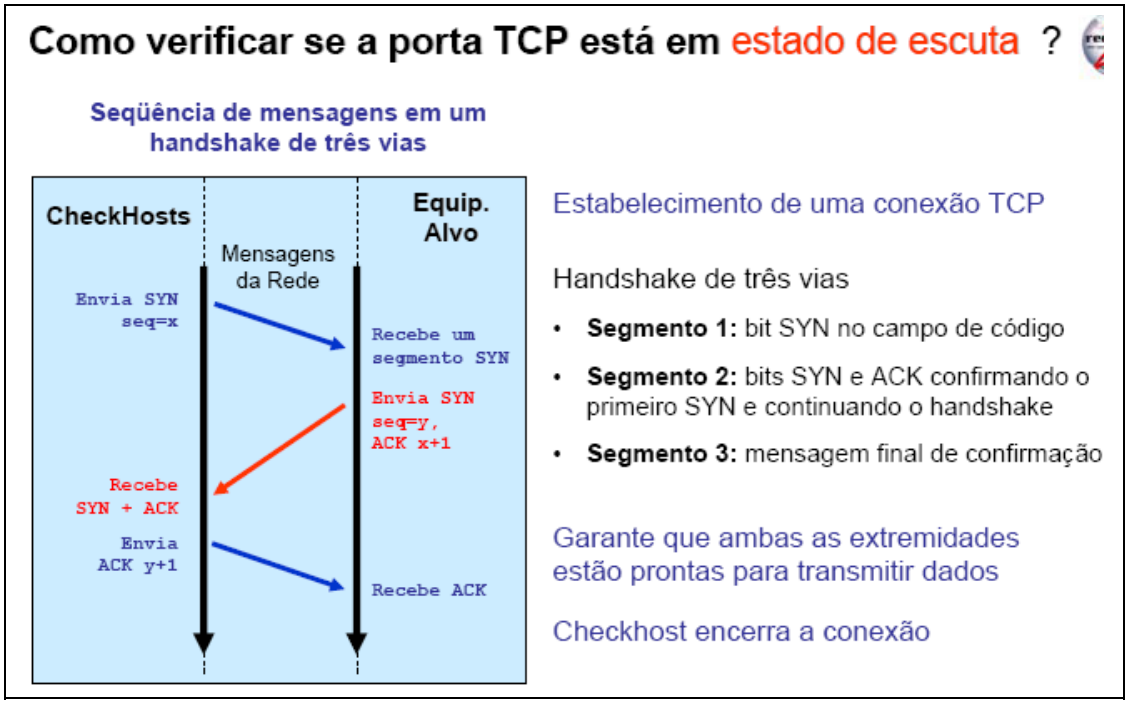


Figura 3.1 - Handshake de 3 vias

No caso da modificação das portas TCP/UDP dos equipamentos alvos cadastrados na base de dados, o sistema envia um aviso segundo a configuração de alerta definida previamente: relatórios, e-mail, chamada telefônica e bloqueio do serviço via "firewall".

Dois relatórios são gerados, um em formato HTML e o outro em WML (*Wireless Markup Language*). O primeiro apresenta o histórico (*log*) das atividades permitindo assim uma análise detalhada *a posteriori* de todos os eventos, Figura 4. As informações exibidas são: i) data e hora do momento que foi identificada a inclusão de um serviço não autorizado em um determinado equipamento alvo; ii) número da porta e do protocolo utilizado (TCP/UDP); iii) tipo de alerta executado. O acesso a esta página é restrito ao administrador da rede. O segundo relatório (WAP) disponibiliza o estado atualizado dos equipamentos monitorados.

23/10/2005 08:03:01 [ALERTA] - Host xx.xx.xx.10 Porta não cadastrada: 23, Proto: TCP
23/10/2005 08:03:01 E-mail de alerta enviado para admin@domain.br.
23/10/2005 08:03:03 Iniciando scan em xx.xx.xx.50
23/10/2005 08:03:44 Iniciando scan em xx.xx.xx.51
23/10/2005 12:03:00 Iniciando scan em xx.xx.xx.1

Figura 4: Exemplo do relatório apresentado em uma página HTML contendo o histórico dos eventos monitorados.

Um dos serviços disponíveis pelo sistema Checkhost é o envio de uma

mensagem de alerta (Figura 5) para o administrador, contendo o endereço IP do equipamento alvo, a porta do novo serviço, o protocolo utilizado e a hora em que a verificação foi realizada. Na troca de mensagens com o servidor SMTP o sistema verifica possíveis erros e caso algo inesperado impeça a transmissão da mensagem um relato do acontecimento é armazenado no arquivo "log".

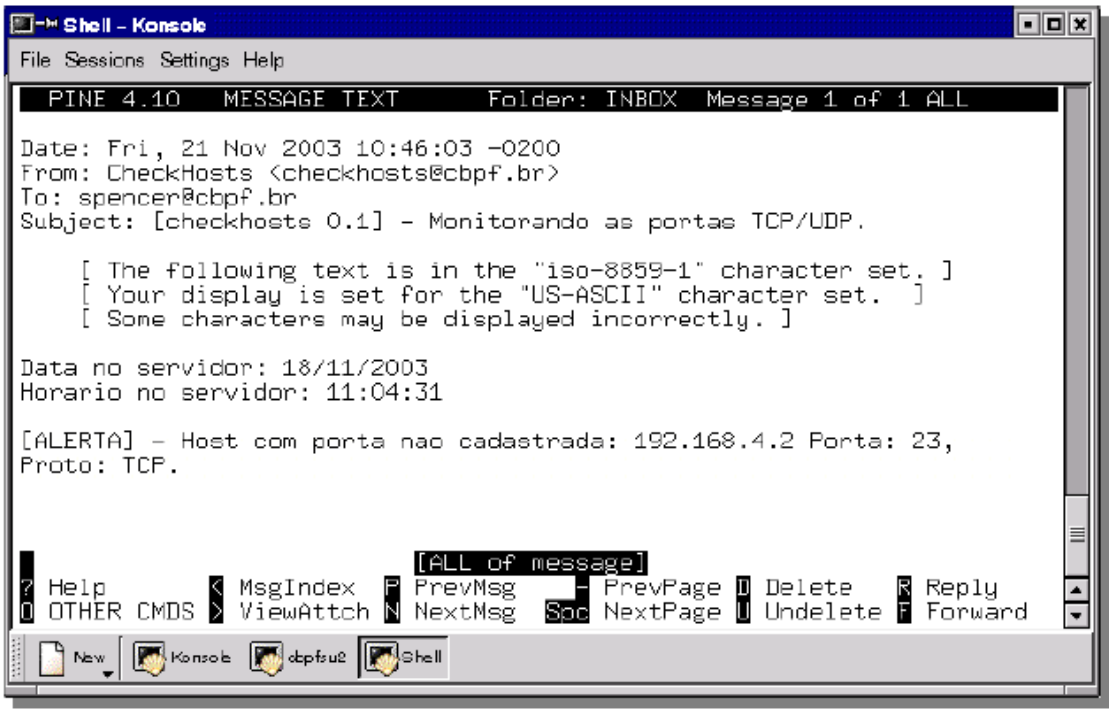


Figura 5 – exemplo de um alerta via mensagem eletrônica

Um outro recurso disponível do sistema de monitoramento é a chamada via telefone. Nesse caso o Checkhosts realiza uma ligação para os telefones celulares dos administradores cadastrados no arquivo de configuração, utilizando um modem conectado a estação de monitoramento. Do mesmo modo, em caso de erro, um relato do sucesso ou não da chamada é armazenado no arquivo de "log".

Por fim, o serviço de bloqueio completa as facilidades do sistema de monitoramento. Esta opção permite uma ação rápida por parte do sistema impedindo que o(s) serviço(s) não autorizado(s) continue(m) sendo oferecido(s). Para isso, é preciso que o Checkhosts esteja funcionando no mesmo computador que realiza o serviço de "firewall". O Checkhosts foi desenvolvido para operar com o programa de "firewall" iptables [9, 10] versão 1.2.7a. Através de comandos de definições de regras do iptables é possível negar a entrada ou a saída de pacotes para o equipamento comprometido.

Um problema freqüente encontrado em redes acadêmicas é a utilização de um Proxy de aplicação como o IRC, onde o usuário tem o objetivo de ocultar seu endereço IP real. Algumas instituições acadêmicas tem normas específicas para o uso de seus endereços IPs proibindo o acesso a pessoas não autorizadas, i.e., aqueles que não são usuários efetivos da rede. Com o

Checkhosts foi possível detectar este Proxy de aplicação IRC. Esse Proxy foi colocado em uma porta acima da porta 1023 usando o protocolo TCP. A varredura de portas promovida pelo sistema de monitoramento detectou imediatamente a nova porta aberta e enviou um sinal de alerta aos gerentes da rede. Posteriormente os detalhes foram verificados por meio de programas utilitários lsof, netstat e ps do Unix/Linux. Rapidamente o usuário que havia instalado o Proxy IRC foi localizado e o serviço normalizado.

Para o desenvolvimento deste sistema foi utilizado um microcomputador PC com o Sistema Operacional Linux Mandrake versão 9.1 e servidor web Apache versão 2.0.47**.** Seu funcionamento periódico é garantido através do processo de agendamento de tarefas do sistema unix (*cron*). O sistema foi completamente desenvolvido em linguagem C ANSI, dentro do conceito de software livre e licenciado nos termos da GNU Licença Pública Geral (*General Public License – GPL/GNU*). O código fonte e manual de utilização estão disponíveis para "*download*" e utilização a partir da Home-Page http://www.cbpf.br/cat/checkhosts.

A segurança na máquina que roda o sistema compreende o seguinte:

- **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. Conclusão

Neste trabalho apresentamos a ferramenta Checkhosts para monitoramento de serviços disponibilizados por equipamentos em rede. Esse sistema funciona por meio da comparação do estado de um equipamento monitorado com um estado previamente armazenado. Em caso de diferença entre os dois estados é gerada uma série de alertas para os gerentes responsáveis avisando-os da mudança nos serviços rapidamente por meio do telefone celular. Além disso, uma ação pode ser executada bloqueando o serviço não autorizado.

As limitações que podem comprometer sua eficiência no monitoramento são: a existência de um "*firewall*" ou de filtros entre o Checkhosts e os equipamentos alvos, ou ainda a incerteza com relação aos serviços indevidos em portas padronizadas.

Algumas expansões desse sistema estão atualmente em andamento, como: a gerência integrada via uma página web permitindo a descentralização ao seu acesso; a utilização de técnicas de criptografia do arquivo binário (base cadastrada); a utilização da comunicação TCP (*three-way handshake*) segura; certificação da aplicação que está efetivamente respondendo na porta solicitada.

Este sistema está hoje em funcionamento na Rede-Rio de Computadores e no CBPF e tem nos auxiliado a garantir os serviços oferecidos pelas estações servidoras de rede de ambas as instituições. Ele foi apresentado no GTS 02/03 – Grupo de Trabalho em Segurança de Redes, do Comitê Gestor da Internet no Brasil, em dezembro de 2003. O link da apresentação pode ser visto no site do Registro.br : ftp://ftp.registro.br/pub/gts/gts0203/

5. Glossário

ACID – Analysis Console for Intrusion Databases – Programa que proporciona uma interface via web para gerenciamento de alertas gerados por IDSs.

ACL Access Control List – Lista de controle de acesso é o meio usual pelo qual o acesso e a negação de serviços são controlados. É simplesmente uma lista que contém os host que podem acessar ou não determinados serviços.

Ataque de negação de serviço – Ocorre quando alguém maliciosamente direciona em um servidor intensas requisições de seu serviço ou gera condições de intenso tráfego fazendo com que o mesmo trave devido a sobrecarga.

Apache – Servidor web base linux gratuito.

Bridge – Dispositivo que repassa o tráfego entre segmentos de rede, baseado na camada de enlaçe do modelo OSI. Estes segmentos podem ser de uma mesma rede ou não.

Uma grande utilidade deste dispositivo, é usá-lo como filtro de pacotes, sem necessitar de alterações na configuração já estabelecida nos dispositivos de rede.

Criptografia – São os meios e métodos de se transformar informações legíveis em ilegíveis e a partir dessas mensagens ilegíveis poder retornar à informação original por meio de uma chave, como uma espécie de senha.

Dispositivo de controle – Software ou hardware que dita as regras com relação à permissão de um dado tráfego de rede.

Firewall – Combinação de hardware e software cujo papel é filtrar o tráfego de informações entre redes privadas e a Internet. Uma de suas inúmeras aplicações é o bloqueio do acesso a serviços ou dados de uma rede interna por meio de usuários externos não autorizados.

Host – Computador conectado a uma rede.

IDS Intrusion Detection Sistem – Sistemas de Detecção de Intrusos são programas que monitoram uma rede ou um host a procura de sinais padrões de comportamento que sejam considerados maliciosos, ou seja, podem constituir um ataque ou uma outra atividade não permitida.

Interfaces de rede - Dispositivo que permite a um computador conectar-se a uma rede (LAN, WAN, internet etc).

IP Internet Protocol – É um protocolo desenvolvido para uso em sistemas de comunicação por comutação de pacotes. Este protocolo especifica o formato dos pacotes (também chamados datagramas) e o esquema de endereçamento.

LSOF – programa para listagem de processos com várias informações

MySQL – Programa para criação e manipulação de banco de dados

Política de segurança – Conjunto de normas que ditam o que é e o que não é permitido em um rede, como por exemplo, que tipo de serviços podem estar ativos (ftp, http), que hosts podem ser acessados diretamente da internet, etc. Essas normas após definidas são implementadas no sistema por meio de firewalls, IDSs e outros dispositivos que se façam necessários.

Roteador – Dispositivo que usa uma ou mais medidas para determinar o melhor caminho por onde o tráfego de rede deve transitar. Roteadores repassam pacotes de uma rede para outra baseando-se na informação da camada de rede.

Scanner de vulnerabilidade – Programa que investiga um host, na maioria das vezes remotamente, para ver se este está vulnerável á um conjunto de tipos ataques. Muito útil para corrigir vulnerabilidades bem como para atacar um sistema.

Segmento de rede – Parte de uma rede, onde o trafego de mensagens é comum a todos os nós.

SNMP Simple Network Management Protocol – É um conjunto de protocolos para gerenciar redes complexas.

Switch – Dispositivo que filtra e repassa pacotes entre segmentos de uma LAN. Switches operam na camada de enlace do modelo de referência OSI.

Tráfego de rede – Conjunto de dados que transitam pelos dispositivos de uma rede de computadores.

VPN Virtual Private Networks – Rede privada virtual é uma rede privada construída sobre um meio público para conectar nós de uma rede. Tipicamente as redes envolvidas são redes IP, sendo a internet o exemplo mais comum. Para manter a privacidade da rede usa-se túneis encritados e outros mecanismos de segurança, de modo a garantir que somente usuários autorizados possam acessar a rede e que os dados não possam ser interceptados.

6. Referências

[1]. Sítio Web do "*Computer Emergency Response Team*" – CERT – http://www.cert.org - 2003.

[2]. Rufino, N. M. de O. – "*Segurança Nacional"* – Editora Novatec – Rio de Janeiro – 2001.

[3]. Scambray. J, McClure S., Kurtz, G. – "*Hacking Exposed*" – Editora: McGraw-Hill Osborne Media – 2000.

[4]. Sítio Web do software NMAP – "*Network mapper port scanning*" - http://www.insecure.org/nmap/ - 2003.

[5]. Sítio Web do software Nagios – "*Nagios host and service monitor program*", http://www.nagios.org/ - 2003.

[6]. Sítio Web do software Nessus - http://www.nessus.org/intro.html - 2003.

[7]. Stevens, W. – "*Unix Networking Programming*" – Editora: Prentice Hall; 2nd edition – 1998.

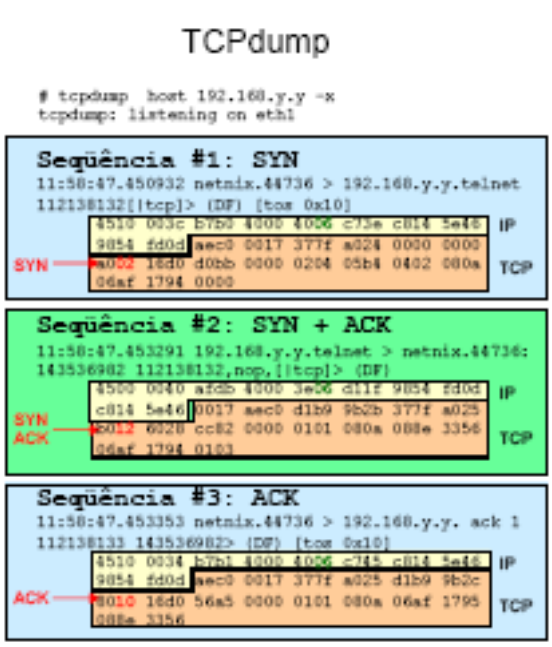
[8]. RFC 793 – Postel, J.; "*Transmission Control Protocol"*; DARPA Internet Program Protocol Specification - Information Sciences Institute - University of Southern California - http://www.faqs.org/rfcs/rfc793.html - 1981.

[9]. Sítio Web "*Introduction to Iptables Tutorial"* Andreasson, Oskar- http://www.faqs.org/docs/iptables/ - 2003.

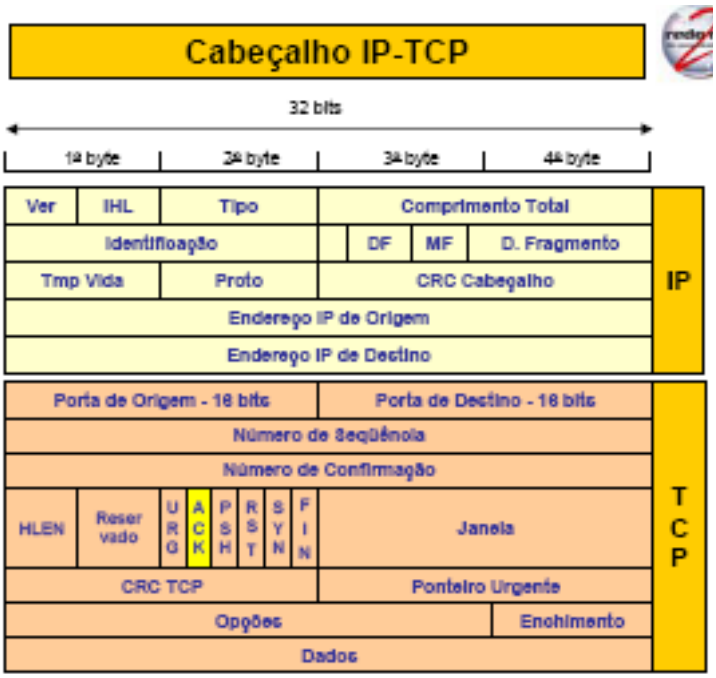
[10]. Cheswick, W. R. – "*Firewalls and Internet Security: Repelling the Wily Hacker*", 2ª Edição; Editora: Addison Wesley – 2003.

[11]. A. A. de Albuquerque, B. M. Amaral, F. C. Bento, F. S. Jannuzzi, F. Spencer, M. E. de Amorim, M. R. Felippe e M. Maestrelli – "*Tópicos sobre Protocolos de Comunicação*", Nota Técnica CBPF NT006/03 – 2003.

Anexo 1 – Exemplo de porta TCP aberta

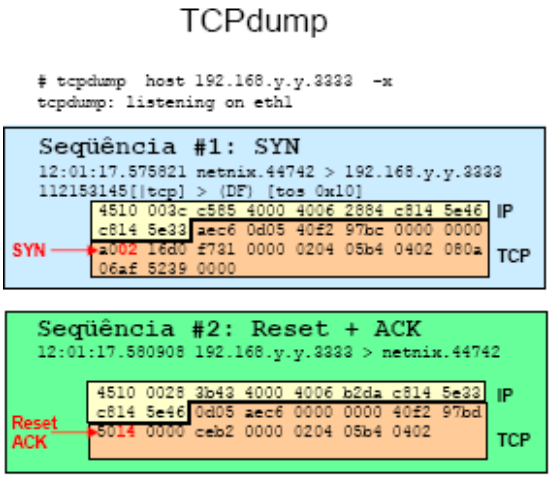


Fonte: TCPDump trace

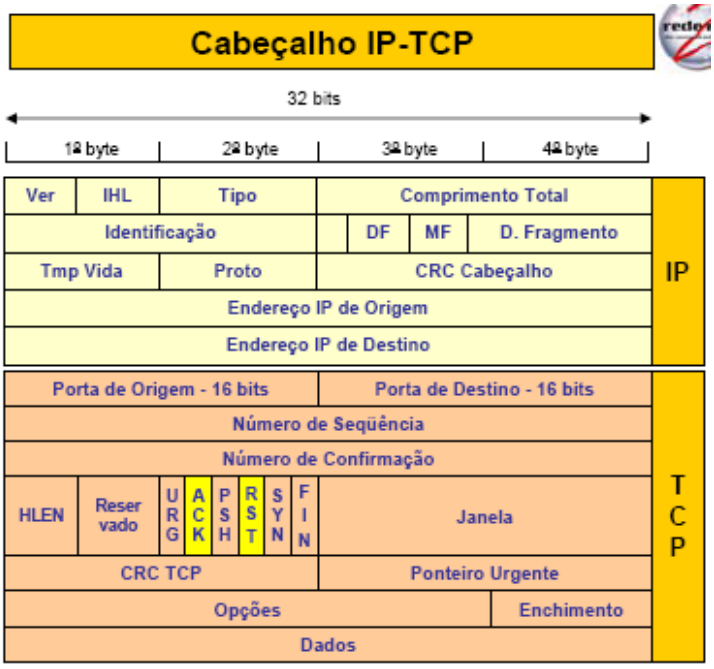


Fonte: Comer, D.E. – Interligação em Rede com TCP/IP

Anexo 2 – Exemplo de porta TCP fechada



Fonte: TCPDump trace

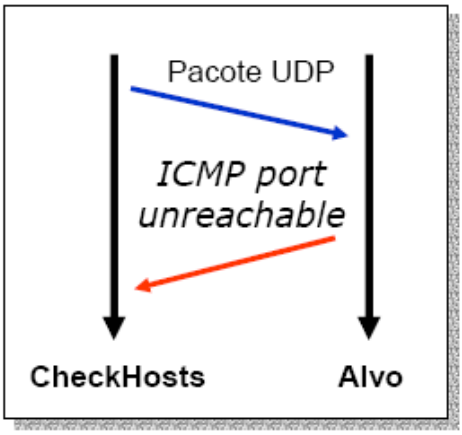


Fonte: Comer, D.E. – Interligação em Rede com TCP/IP

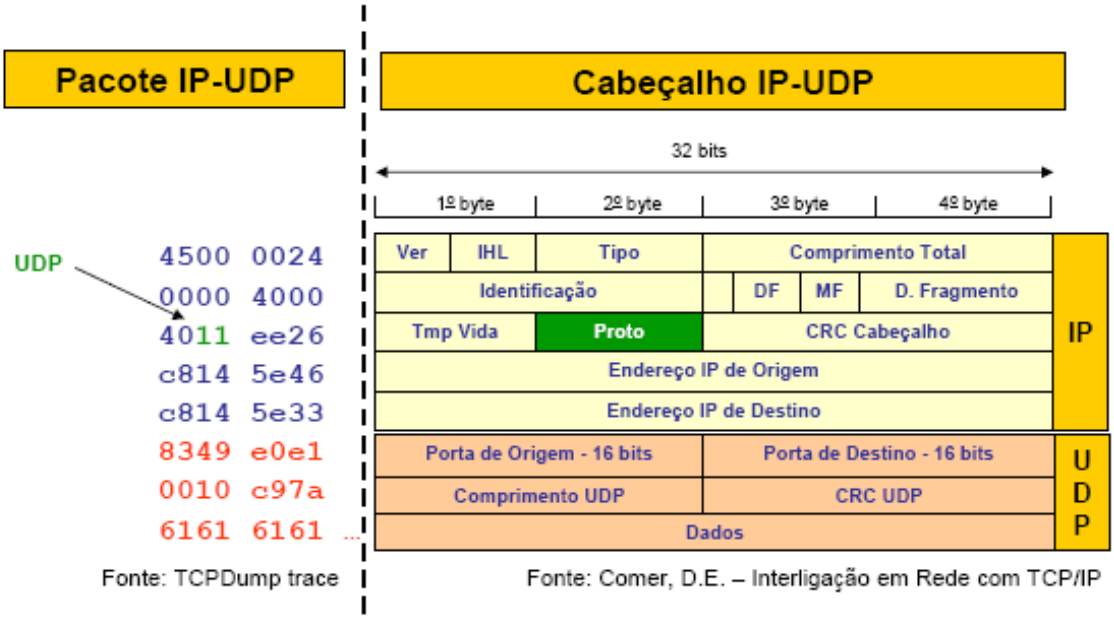
Anexo 3 – Porta UDP em estado de escuta

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.

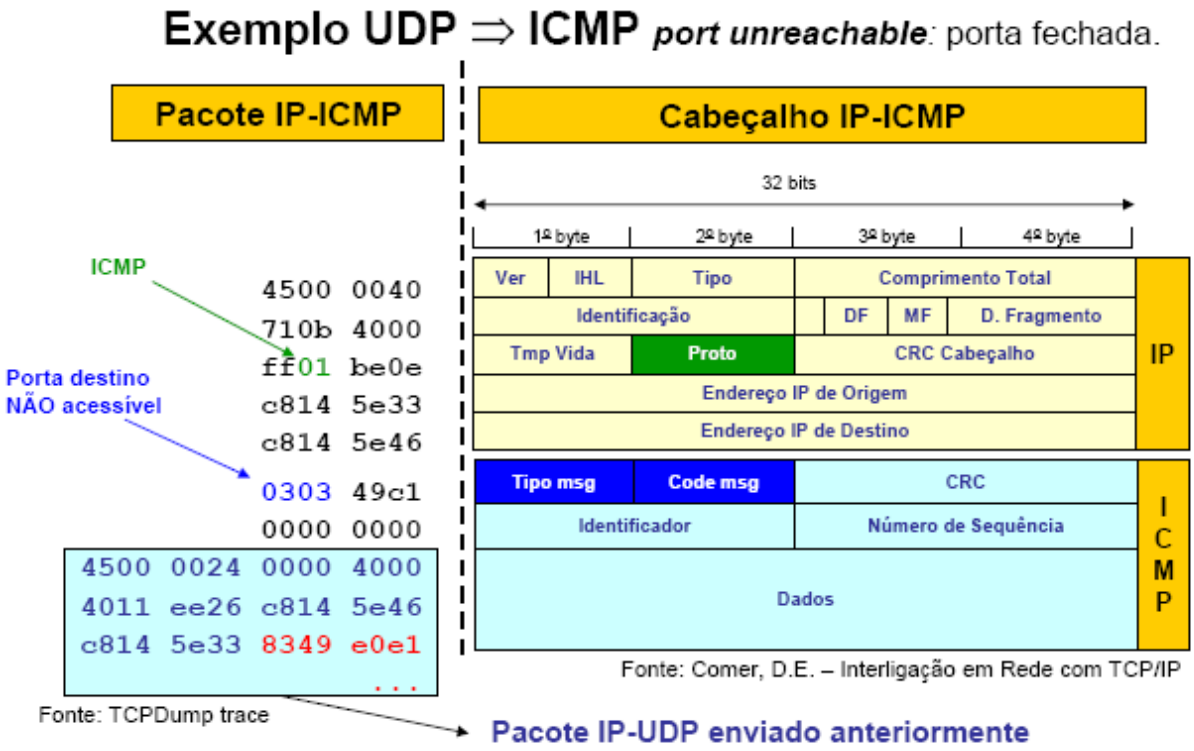


Envio de pacote UDP



Fonte: TCPDump trace

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


Exemplo UDP ⇒ ICMP port unreachable: porta fechada.
Pacote IP-ICMP
Cabeçalho IP-ICMP
32 bits
1º byte
2º byte
3º byte
4º byte
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
...
Ver
IHL
Tipo
Comprimento Total
Identificação
DF
MF
D. Fragmento
Tmp Vida
Proto
CRC Cabeçalho
Endereço IP de Origem
Endereço IP de Destino
IP
Tipo msg
Code msg
CRC
Identificador
Número de Sequência
Dados
ICMP
Fonte: Comer, D.E. – Interligação em Rede com TCP/IP
Fonte: TCPDump trace
Pacote IP-UDP enviado anteriormente