Segurança no Portal UNIX

Fernanda Santoro Jannuzzi fernanda@cbpf.br
Marita Maestrelli marita@cbpf.br
Ricardo Venancio dos Santos ricardov@cbpf.br

Julho 2002
CAT – CBPF

PREFÁCIO

A idéia da criação de uma máquina única para acesso remoto á rede computacional do CBPF surgiu, com o início das atividades maliciosas de alguns usuários da grande Rede(Internet), nas máquinas alheias.

Usuários com atividades maliciosas são chamados constantemente de *hackers,* mas nós prefirimos denominá-los de intrusos.

Apoiados nas Normas de Uso da Rede computacional do CBPF de 1998, colocamos em prática o Portal do CBPF. Ele compreende uma estação de trabalho Sparc Sun, rodando o sistema operacional Unix, e permitindo acesso externo aos funcionários e pesquisadores do CBPF, nos sistemas de computadores da instituição.

Esta nota técnica explica os critérios adotados na configuração da rede e na máquina de nome *positron*.

INDICE

1 – Introdução

O portal de entrada do CBPF é uma máquina conectada na rede de computadores da instituição com função de servidor remoto único para seus usuários. O objetivo principal da criação do portal , foi para aumentar a segurança da rede.

Essa solução facilita o controle externo, pois centraliza o acesso remoto numa única máquina. A partir dela , o usuário pode se conectar aos vários sistemas que compõem a rede computacional do CBPF.

A criação desse portal envolveu os seguintes pontos:

- Política de Segurança;
- Escolha da máquina e do sistema operacional;
- Filtros de roteamento (na entrada e saída de pacotes);

Política de Segurança: é o conjunto de decisões que coletivamente determinam a postura de uma organização em relação à segurança, ou seja, ela determina os limites aceitáveis de comportamento e as medidas a serem tomadas no caso de sua violação. Uma política de segurança, basicamente define o que é permitido e o que é proibido , tanto no acesso aos dados quanto na utilização dos serviços oferecidos.

Hardware e Sistema operacional: a escolha da máquina requer muito cuidado , pois é necessário uma com arquitetura confiável e estável. Um sistema operacional sólido e com grande versatilidade , como o UNIX, também reforça essa escolha. Portanto , utilizamos uma estação de trabalho Sun Sparc com Solaris 8.

Filtros de pacotes: os filtros de pacotes constituem um mecanismo capaz de atuar sobre a entrada e saída de dados de uma rede, através de regras que permitam ou bloqueiem o tráfego com base nos endereços, portas e protocolos utilizados. No item 2 deste artigo descrevemos essa técnica.

Resumindo - com a implementação do portal, obtivemos:

- centralização do controle de acesso remoto,
- segurança na conexão do usuário coma encriptação do login e senha,
- facilidade na correção de falhas ,
- maior controle dos processos locais.

No item 3 são listadas as técnicas utilizadas no portal, assim como uma explicação detalhada de cada uma. As estatísticas de vulnerabilidades em sistemas operacionais ilustram a nossa escolha , e são colocadas no item 4. Para completar , no item Conclusão(5) , resumimos o método aplicado .

Existem muitas palavras em inglês que significam comandos ou atributos do sistema Unix, e podem ser localizadas no item 7 – Glossário.

2 - Roteador e Filtros de pacotes

Conceito:

São equipamentos que possibilitam a interligação de duas ou mais redes distintas, de forma que as estações possam se comunicar como se estivessem num mesmo ambiente. No caso do CBPF, o roteador Cisco é nossa conexão com o mundo, e isto é possível através do backbone da Rede Rio.

A segurança destes equipamentos é feita usando filtros de pacotes que constituem de um mecanismo capaz de atuar sobre a entrada e saída de dados da rede, com regras que permitem ou bloqueiam o tráfego com base em endereços, portas e protocolos utilizados. Estas regras atuam na camada de transporte garantindo a proteção contra alguns tipos de ataques.

A utilizaçãode filtros é relativamente simples, embora sua criação através das regras possa crescer em complexidade de acordo com cada caso. O uso de filtros é apenas uma medida complentar à segurança de rede.

A implementação de filtros de pacotes em roteadores CISCO é feita por meio de listas de acesso (access-list). Existem dois tipos de access-list:

1.standard: onde o controle é feito com base no endereço de origem e a identificação destas listas variam de 1 a 99.

Sintaxe: access-list <número> {deny | permit} <origem> <máscara>

2.extended: onde o controle é feito levando-se em consideração endereços, portas com algumas opções adicionais.A identificação destas listas variam de 100 a 199.

Sintaxe: access-list <número> {deny | permit} <protocolo> <origem> <máscara> <destino> <máscara> <porta> {established | log}

Access-List (extended) - Criação

Router# **access-list numero acao protocolo origem destino modificadores**

Numero = É o numero da acess-list
Ação = É o que você vai fazer com o PACOTE. (DENY - PERMIT)
Protocolo = Os protocolos (IP - TCP - UDP - ICMP)
Origem = Da onde vem o pacote (o IP origem com o endereço e NETMASK invertido
Destino = E para onde vai o pacote (O IP destino, com endereço e netmask

invertidos)

Modificadores = São opções de seleção de portas e flags de pacotes. (EQ, ESTABLISHED, entre outros).

Uma explicação mais detalhada sobre filtros de pacotes em roteadores Cisco, está no **Anexo 1**, elaborada pelo engenheiro Anderson Alves de Albuquerque.

3 – Técnicas utilizadas:

3 – 1 – Implementação de senha na EEPROM

A Eeprom , memória de leitura programável, vem sem senha . Isto quer dizer, se a máquina for ligada , ela não necessitará de senha para inicializar o sistema , e ficará vulnerável a manipulação em sua memória de configuração.

Para acionar a senha na eeprom:
eeprom security-mode=command
Changing PROM password:
New password: (digitar uma senha)

Para alterar a senha na eeprom:
eeprom security-password=

3 – 2 - Patches

Manutenção do Sistema

Os patches são arquivos para a correção de falhas no sistema. Periodicamente, a Sun disponibiliza estes pacotes para o sistema Solaris na suas mais diversas versões. Existem diversas opções de patches, inclusive os em cluster, ou seja, vários patches empacotados em um único arquivo.

Depois de trazer do site da Sun, o Recommended Patch para a versão do Solaris desejada, basta descomprimir e rodar o script de instalação do cluster de patches.

Abaixo segue a simulação da instalação deste pacote em um sistema Solaris 2.8, onde o arquivo foi colocado no /tmp da estação.

Descomprimir os arquivos usando unzip:.

unzip 8_Recommended.zip

Acessar o diretório:

cd 8_Recommended

Inicializar o script de instalação dos patches:

#./install_cluster

```
Patch cluster install script for Solaris 8 Recommended

*WARNING* SYSTEMS WITH LIMITED DISK SPACE SHOULD *NOT* INSTALL PATCHES:
With or without using the save option, the patch installation process
will still require some amount of disk space for installation and
administrative tasks in the /, /usr, /var, or /opt partitions where
patches are typically installed.  The exact amount of space will
depend on the machine's architecture, software packages already
installed, and the difference in the patched objects size.  To be
safe, it is not recommended that a patch cluster be installed on a
system with less than 4 MBytes of available space in each of these
partitions.  Running out of disk space during installation may result
in only partially loaded patches.  Check and be sure adequate disk space
is available before continuing.

Are you ready to continue with install? [y/n]:y

Determining if sufficient save space exists...
Sufficient save space exists, continuing...
Installing patches located in /tmp/8_Recommended
Using patch_order file for patch installation sequence
112396-01
108987-08
111293-04
108869-15
109326-07
109805-06

The following patches were not able to be installed:

        110387-03
        110283-05
        109277-02
        110951-02
        111234-01
        110903-04
        109320-04
        109470-02
        109783-01
        109951-01

For more installation messages refer to the installation logfile:
  /var/sadm/install_data/Solaris_8_Recommended_log

Use '/usr/bin/showrev -p' to verify installed patch-ids.
Refer to individual patch README files for more patch detail.
Rebooting the system is usually necessary after installation.
```

Quando a instalação termina aparece uma mensagem informando o número dos patches que não conseguiram ser instalados no sistema, a localização do arquivo de log e um aviso para que a estação seja reinicializada para que as correções sejam efetivadas.

Conforme o aparecimento de novos bugs ou vulnerabilidades no sistema operacional ou em algum programa em utilização, são anunciados novos patches. A observação dessas ocorrências devem ser acompanhadas diariamente.

Exemplo: Vulnerabilidade no : snmpdx/mibiisa/libssasnmp/snmplib

Patch SunOS 5.8 108869-16 : 108869-16.jar (jar – compactador em java)

jar xvf 108869-16.jar (para expandir o arquivo)

patchadd ./108869-16 (para instala-lo)

3 – 3 – Serviços de Rede

Arquivo /etc/inetd.conf:

Este arquivo define os serviços de rede e é parte do sistema Solaris.Ele contem vários serviços que devem ser desabilitados, por serem raramente utilizados e/ou facillitarem a ação de ataques maliciosos. A seguir, a descrição desses serviços:

FTP - Permite acessos de usuários remotos a máquina para a transferência de arquivos. O grande problema deste serviço é que os dados para a conexão passam sem nenhum tipo de encriptação o que facilita o roubo de senhas e logins por algum hacker que esteja "escutando" o tráfego da rede. Aconselhável desabilitar e utilizar serviços mais seguros contidos nos pacotes do SSH.

TELNET - Permite que usuários remotos acessem uma máquina. Tem a mesma limitação do ftp. Aconselhável desabilitar e instalar versões atuais do SSH.

NAME - Habilita o protocolo de serviço de nomes do TCP/IP. Aconselhável desabilitar.

SHELL - Permite ao usuário remoto rodem programas arbitrários em uma máquina. Aconselhável desabilitar.

LOGIN - Permite ao usuário remoto uma vez logado possa conectar-se a outra estação sem precisar de senha novamente. Inseguro pelos mesmos motivos do FTP e TELNET. Aconselhável desabilitar e utilizar o SSH.

EXEC - Permite que usuários remotos executem comandos em uma máquina sem precisar de

login. Expõe a senha deste usuário pela rede. Aconselhável desabilitar este serviço.

COMSAT - É o processo de notificação de e-mail. Utilizando a porta 512 este daemon fica aguardando a chegada de um mail e quando isso acontece é impresso no terminal do mail cerca de 7 linhas com o seu conteúdo excluindo o cabeçalho da mensagem. Aconselhavel desabilitar pois não é um serviço primordial ao funcionamento do sistema. Somente o habilite se realmente for utiliza-lo.

TALK - Permite que um usuário remoto possa abrir um terminal para conversação com outro usuário que também esteja conectado a mesma máquina. Aconselhável desabilitar.

UUCP - Permite que usuários remotos transfiram arquivos de/para uma máquina que utiliza o protocolo UUCP e a menos que voce utilize-o, é aconselhável desabilitar este serviço.

TFTP - Utilizado para tranfesrência de arquivos sem que seja preciso o usuário se conectar. Era muito utilizado em X_Terminals e Roteadores. Recomendável desabilitar este serviço.

FINGER - Permite que usuários remotos utilizem o comando finger para obter informações de um determinado usuário em uma certa máquina. Considerado inseguro. Aconselhável desabilitar este serviço e utilizar versões mais seguras como cfinger.

SYSTAT, NETSTAT - Permite que usuários externos a rede possam obter informacoes de outros usuários em uma máquina local. Considerado inseguro pois estas informações poderam ser utilizadas em futuros ataques. Aconselhável fechar estes serviços.

TIME - Utilizado para sincronizar o relógio com o sistema. Aconselhável desabilitar e usar outras soluções como xntp.

ECHO - Usa a porta 7 para cuidar do tráfego de tcp udp. É usado como uma ferramenta de medição e depuração de erros, mandando de volta a fonte original qualquer pacote recebido. Isso pode gerar facilmente um ataque do tipo Denial Of Service, logo, é aconselhável desabilitar o serviço.

DISCARD - Trabalha na porta 9 com o tcp e o udp. Utilizado como uma ferramenta de depuração e sua função é discartar qualquer pacote recebido. Considerado pouco necessário, logo, aconselhável desabilita-lo.

DAYTIME - Tem função similar ao time. Considerado de pouco necessidade , logo, aconselhável desabilita-lo.

CHARGEN - Trabalha com o tcp e udp na porta 19. Chargen espera uma conexão enquanto for sobre tcp, manda o fluxo continuo dos dados até que a fonte original feche a conexão. Quando for sobre udp, o serviço espera por um datagrama. Uma vez recebido, ele responde com um datagrama com caracteres que variam entre 0 e 512. É frequentemente usado para ataques do tipo Denial of Service, logo, aconselhável desabilitar o serviço.

SADMIND - Este processo tem interface do pacote Solstice Admin Suite, autorizando a administração remota através dele(criar contas, trocar senhas). Aconselhável desabilitar pois se alguma invasão ocorrer, o hacker pode facilmente manipular o sistema, criando , alterando e deletando as contas e máquinas.

RQUOTAD - Retorna a quota de um usuário no sistema desde que o mesmo utilize o NFS (Network File System). Recomendável desabilitar este serviço.

RUSERD - Retorna uma lista de usuários conectados a rede. Recomendável desabilitar este serviço.

SPRAYD - Registra os pacotes enviados por spray e manda uma resposta para o fonte original dos pacotes. Aconselhável desabilitar.

WALLD - Usado para rwall e requesições de shutdown. Recomendável desabilitar.

RSTATD - Servidor remoto de estatísticas. Gera informações do kernel e exibe um pequeno gráfico do desenvolvimento do CDE. Se não for funcional ao seu sistema e aconselhável desabilitar.

REXEC - Servidor de execução remoto. Similar ao rlogin e o rexec, permitindo que usuários executem comandos remotamente. Se for realmente necessário utilizar, as especificações de segurança podem ser feitas no arquivo pam.conf. Aconselhável desabilitar.

rpc.ttdbserverd - Habilita o serviço do SUN Tooltalk Database Server. O Tooltalk trabalha agindo como mediador entre aplicativos, permitindo a troca de dados entre eles, mesmo que sejam de tipos diferentes. É considerado inseguro pois gera ataques do tipo buffer overflow o qual dava o controle ao invasor remotamente em alguns sistemas Solaris, logo, aconselhável desabilitar.

UFSD - É uma parte incompleta do pacote add-on. No futuro poderá ser capaz de concertar problemas nos arquivos de sistemas ufs.

KCMS_SERVER - Parte do Kodak Color Management System. A função deste processo é servir perfis a uma estação de trabalho remota.

FS - Usado somente se a estação for um servidor de fontes (usado quando a rede tem clientes diskless e elas vão obter as fontes deste servidor). Aconselhável desabilitar.

CACHEFSD - Trabalha com tcp. É responsável pelo cache do sistema de arquivos, armazenando-os no diretório principal da máquina. Pode ser administrado através do utilitário cfsadmin.

KERBD - É o processo do Kerberos, responsável por validar requisições rpc usando a encriptação do Kerberus e gerando o chamandos Kerberos Tickets (chaves de autenticação) e atribuir os UID e GID correspondentes a cada usuário.

PRINTER - Habilita a estação a ser servidora de impressão. Pode ser desabilitado se o host não estiver configurado para aceitar requisições de impressão.

GSSD - É o Generic Security Service Daemon. Este processo é um nivel adicional de segurança, acoplado com o kerb para Secure RPC. É de sua responsabilidade a identificação de ambos os lados da transição, integridade dos dados, privacidade, e toda a encriptação adicional dos dados entre os pontos de transição.

DTSPC - O CDE Subprocess Control é o processo responsável por aceitar requisições de usuários externos para executar e lançar programas remotamente. Existem falhas que são exploradas frequentemente neste serviço, pois um usuário mal intencionado pode manipular os dados de maneira a criar um buffer overflow e com isso ganhar controle total da estação.É aconselhável desabilita-lo.

rpc.cmsd - É o processo do calendário usado pelo CDE. Ele permite que usuários remotos criem calendários localmente através da configuração do arquivo cmsd.conf. Este processo contém algumas vulnerabilidades, aconselhável desabilita-lo.

3 - 4 - Serviços de boot(inicialização do sistema)

Alguns serviços que são inicializados pelo sistema devem ser retirados, tais como:

NFS server - responsável pelo serviço de exportação de arquivos para outras máquinas na rede. NFS é frequentemente explorado para facilitar o acesso não autorizado a arquivos e sistemas.

```
# mv /etc/rc3.d/S15nfs.server  /etc/rc3.d/K15nfs.server
```

NFS client – para disponibilizar acesso a arquivos de outras máquinas, e como usa NFS tem os mesmos problemas do anterior.

```
# mv /etc/rc2.d/S73nfs.client  /etc/rc2.d/K73nfs.client
# mv /etc/rc2.d/S74autofs  /etc/rc2.d/K74autofs
```

RPC – serviços básicos de RPC usam muito pouco ou nada de autenticação e compartilham informações muito sensíveis. NFS , NIS, Kerberus, GUI, utilizam RPC.

```
# mv/etc/rc2.d/S71rpc  /etc/rc2.d/K71rpc
```

3 – 5 – Ajuste do Kernel

- **Desabilitar Core dumps**

Quando uma estação deixa de funcionar, é útil obter uma cópia da imagem da memória (chamada de core dumps) para identificar a causa da falha. Isto pode consumir grande espaço em disco e deixar vários dados críticos expostos. Recomenda-se a sua desabilitação.

Acrescentar ao arquivo /etc/system o limite 0(zero) para o core dumps:
cat >> /etc/system
set sys:coredumpsize = 0

- **Proteção de pilha**

A exploração de buffer overflow (estouro da memória reservada por programas), é o método mais utilizado para ataques atualmente. Habilitando a proteção de pilha previnimos certa parte de ataques desse tipo.

Acrescentar ao arquivo /etc/system os seguintes ajustes:
cat >> /etc/system
set noexec_user_stack = 1
set noexec_user_stack_log = 1

3 – 6 - Proteção do GUI

A interface gráfica do sistema solaris - CDE é baseada em X-windows, o qual tem conhecidas falhas de segurança. O serviço remoto gráfico deve ser desabilitado.

Comentar as seguintes linhas no arquivo /usr/dt/config/Xaccess
* # grant service to all remote displays
* CHOOSER BROADCAST #any indirect host can get a chooser
Ficam assim:
#* # grant service to all remote displays
#* CHOOSER BROADCAST #any indirect host can get a chooser

3 – 7 – Instalação de programas de segurança

Alguns programas extras são necessários para aumentar a segurança do sistema. Esses programas são trazidos no modo fonte , e necessitam de compilação, instalação e configuração no sistema em questão. Utilizamos o compilador C da GNU (Free Software Foundation) , **gcc** .

- ***TCPWRAPPER***

O tcpwrapper é um software que controla e monitora acesso aos serviços de FINGER, FTP, TELNET, RLOGIN, RSH, TFTP, TALK, EXEC e outros, e é um dos métodos mais comuns de controles de acesso no sistema Unix. O tcpwrapper permite criar limitações de acesso, definindo quem pode e quem não pode acessar cada serviço. Isto permite, por exemplo, que você defina que apenas usuários de determinada instituição possam acessar a sua máquina, ou então que todos os usuários podem ter acesso a alguns serviços. Os daemons originais são substituídos pelo daemon do tcpwrappers que monitora e controla o acesso.

Assim fica no /etc/inetd.conf:

```
Original:  ftp   stream  tcp6   nowait  root   /usr/sbin/in.ftpd  in.ftpd  -l
Tcpd:      ftp   stream  tcp6   nowait  root   /usr/sbin/tcpd  in.ftpd –dl –t 600
```

Proibindo a acesso de alguns hosts, no arquivo /etc/hosts.deny:

ALL: none.all.com nenhum.com.br: (/var/adm/inve %d %h %H|usr/ucb/mail -s %d-%h root@cbpf.br)&

O exemplo acima proíbe o acesso remoto das máquinas none.all.com e nenhum.com.Br , e informa , via mail , ao administrador, alguns dados gerados pelo programa inve (script privado).

A versão mais atual do tcpwrapper pode ser encontrado no link:
ftp:://ftp.porcupine.org/pub/security

- ***SSH***

Com o crescimento das redes de computadores, foi necessário criar uma forma de conexão segura, permitindo o envio de dados e execução de comandos de forma segura entre dois computadores ou mais. Foram criados vários protocolos de conexão, para substituição dos conhecidos **telnet** e **ftp**.

O ssh é uma ferramenta que utiliza o sistema criptográfico de chaves, sendo uma pública para encriptar e outra privada para decriptar os dados. Ele utiliza a técnica de túneis na qual cria-se um canal seguro entre os computadores. Quando uma requisição é feita essa máquina envia uma chave pública que será validada pela máquina que recebe o pedido. Quando um intruso tentar usar alguma de suas ferramentas para visualizar os dados de terceiros, ele somente visualizará os dados criptografados, não havendo assim problemas para os nossos usuários.

O software se encontra no http://www.openssh.org, ele também é um software livre que pode ser usado por diversos sistemas operacionais e ainda ser configurado de acordo com a suas preferências.

Caso queria saber mais sobre o programa ssh e sobre sua instalação, configuração e segurança e só entrar em contato com o CBPF, e requisitar a nota técnica feita por Anderson Alves de Albuquerque & Marita Maestrelli, sobre Segurança – Secure Shell (ssh), ou enviar um e-mail para socorro@cbpf.br ou valeria@cbpf.br

- ***Programas investigavivos***

Utilizamos outros programas, conforme a situação, para investigar determinado IP que tenha tentado nos atacar, como:
nmap – utilitário para exploração de redes e exames de segurança, tipo *portscanner*;
http://www.insecure.org/nmap/

nessus – utilitário para examinar redes quanto as vulnerabilidades existentes e / ou programas maliciosos instalados.
http://www.nessus.org/

3 – 8 - Monitoração

"Em rádio e televisão, checagem da qualidade de sons, imagens, técnicas operacionais, conteúdos do programa e etc., no momento da realização. Acompanhamento permanente da programação."(Michaelis). Relacionando esta frase com as redes de computadores, temos que a monitoração consiste num controle da rede pelo administrador utilizando ferramentas de detecção. Abaixo estão listadas as formas pelo qual o portal acompanha os *logs* para tentar evitar os possíveis ataques.

- ***IDS - snort***

As ferramentas do sistema de detecção de intrusão IDS ou "Intrusion Detection System" são as principais ferramentas para a segurança da rede. Algumas instituições colocam somente o "firewall" como proteção de sua rede, e todos nós sabemos que mesmo com um "firewall" conectado a rede, pode ainda ter algumas falhas de segurança na qual intrusos tentarão violar. O que é permitido e o que é proibido é determinado pelo administrador. A intrusão só é caracterizada por qualquer conjunto de ações que tentem comprometer a integridade, confidencialidade ou disponibilidade dos dados ou do sistema.

Existem inúmeras ferramentas de detecção de intrusão em diferentes plataformas, mas basicamente a maioria funciona da mesma forma analisando pacotes que trafegam na rede e comparando com as tentativas de ataques. Os IDS trazem informações como tentativas de ataques que sofremos por dia, qual tipo de ataque foi usado e qual origem dos ataques e destino.

Os IDS rodam constantemente em "background" verificam se alguém está tentando invadir a sua rede, ou algum usuário tentando fazer o mau uso dela. Geralmente percebe-se uma tentativa de invasão com uma anomalia na rede, como: o aumento do tráfego, usuários tentando usar serviços que normalmente não são utilizados, muitas tentativas de conectar ao servidor, entre outros.

As informações obtidas pelo IDS são comparadas com bases de padrão de ataque previamente

montadas permitindo também a configuração e a inclusão de novos parâmetros. As informações são comparadas e podem ser registradas como tentativa de invasão e qual a técnica utilizada pelo invasor.

A ferramenta utilizada no portal é o "SNORT". É uma ferramenta de detecção de intrusão muito utilizada pelos administradores de servidores que rodam Unix, devido a sua fácil instalação, configuração e ótimo desempenho. O SNORT é uma ferramenta "Open Source", na qual dá direito de ser redistribuído e modificado sem restrições. Isto quer dizer que, se você tem um software livre, você poderá alterá-lo conforme suas necessidades.

O processo de compilação e instalação do SNORT é muito parecido com os outros softwares do sistema Unix. Primeiro, trazemos do site o fonte : **http**://www.snort.org ,e até o presente momento a versão para "download" é a snort-1.8.7.tar.gz.
Existem alguns pré-requisitos para sua instalação, como a biblioteca Libcap(http://www.tcpdump.org).

Instalando o SNORT:

```
# gzip –d snort-1.8.7.tar.gz | tar xf –
# cd snort-1.8.7
# ./configure
# make
# make install
```

O executável instala no /usr/local/bin. Para configuração , alteramos o arquivo **snort.conf** de acordo com as características de sua rede.As regras são a chave da eficiência do **snort**, e devem sempre acompanhar as novas vulnerabilidades e os tipos de ataques conseqüentes.

Os IDS também são alvos de ataques, por exemplo, se um hacker souber da existência de um IDS na rede, a primeira coisa que ele faria era apagar suas "impressões digitais" com a tentativa de reconfigurar o programa que está rodando, ou até mesmo pará-lo, para que ele possa ter suas ações livres. Por esses motivos, deve-se ter cuidado na instalação, configuração e escolha de um IDS, para que não sofra ataques sem ser percebido.

Um dos maiores problemas dos IDS são com o falso positivo, o qual ocorre quando pacotes normais são caracterizados como tentativa de ataques, e o falso negativo que é mais grave, pois o software deixa de alertar os reais ataques. Para que isso possa ser minimizado, é necessário uma analise bem minuciosa dos dados gerados.

- ***SYSLOG***

O *kernel* e muitos programas do sistema produzem avisos, mensagens de erros, e outros alertas. É importante que estas mensagens possam ser lidas outra hora, mesmo que isto demore muito tempo deste o ocorrido. Para que isso seja possível elas devem ser gravadas em um arquivo. O programa responsável por este arquivamento é o **syslog**. Ele pode ser configurado para gravar as mensagens em

diferentes arquivos de acordo com o nível de importância ou origem. As mensagens do *kernel* são freqüentemente direcionadas para arquivos distintos, pois estas mensagens são normalmente mais importantes e necessitam ser lidas com mais freqüência para se evitar/sanar problemas.

Para segurança dos dados gerados pelo **syslog**, eles devem ser enviados para uma outra máquina reservada, ou seja, mantemos uma cópia dos *logs* no portal e enviamos outra para um endereço na nossa rede interna.

O **syslog** permite filtrar as mensagens de *log* por prioridade/facilidade , que podem ser divididas em diversos arquivos para facilitar a seleção de eventos . A configuração do **syslog** é feita através do arquivo **/etc/syslog.conf**. Na inclusão de uma nova facilidade/prioridade, não esquecer de usar <tab> para designar o arquivo que irá receber o *log*.

Exemplo: mail.info <tab> /var/log/maillog

Um exemplo do arquivo /etc/syslog.conf , pode ser visto no Anexo 2.

Configurando o SYSLOG:

1 – Facilidade AUTH

Os dados enviados para o canal LOG_AUTH geram importantes informações relativas a segurança, como acessos a conta root(administradora do sistema), falhas/sucessos nas tentativas de início de sessão com direitos de root(su), e outras. Para capturar essas informações , acrescente a linha abaixo, no arquivo /etc/syslog.conf:

auth.info /var/log/authlog

E não esqueça de criar o arquivo com leitura somente pelo supervisor(root):

touch /var/log/authlog

chown root:root /var/log/authlog

chmod 600 /var/log/authlog

2 – Facilidade DAEMON

Todos os programas que ficam rodando no sistema geram informações que podem ser capturadas pelo canal LOG_DAEMON.

daemon.info;daemon.debug /var/log/daemonlog

- **Outros LOGS úteis:**

1 - /var/adm/loginlog

A criação desse arquivo permite os *logs* das falhas de tentativa de acesso.

A modificação no parâmetro SYSLOG_FAILED_LOGINS permite controlar o número de

falhas aceitáveis antes do *log* ser realizado. Esse parâmetro pode ser alterado no arquivo /etc/default/login.

2 – Relatório de atividades do sistema

Dados como utilização de CPU, I/O de disco, etc podem ser armazenados utilizando os comandos sa1, sa2, sadc, sar. Descomentar no arquivo /etc/rc2.d/S21perf a linha:

/usr/bin/su sys –c "/usr/lib/as/sadc /var/adm/as/as ´date +%d´"

Acrescentar no **cron**(relógio do sistema) as seguintes linhas , para carregar os dados a cada 20 minutos, e arquivá-los por um mês:

crontab –e (editando)

0,20,20 * * * * /usr/lib/as/sa1

45 23 * * * /usr/lib/as/sa2 –s 0:00 –e 23:59 –i 1200 –A

Para acessar os dados gerados, utilize o comando **sar**.

3 – 9 – Backup

O sistema de **backup** (cópias de segurança) é simples, ou seja, diariamente , em determinado horário, o sistema é copiado para uma estação na rede interna , através do comando **tar.**

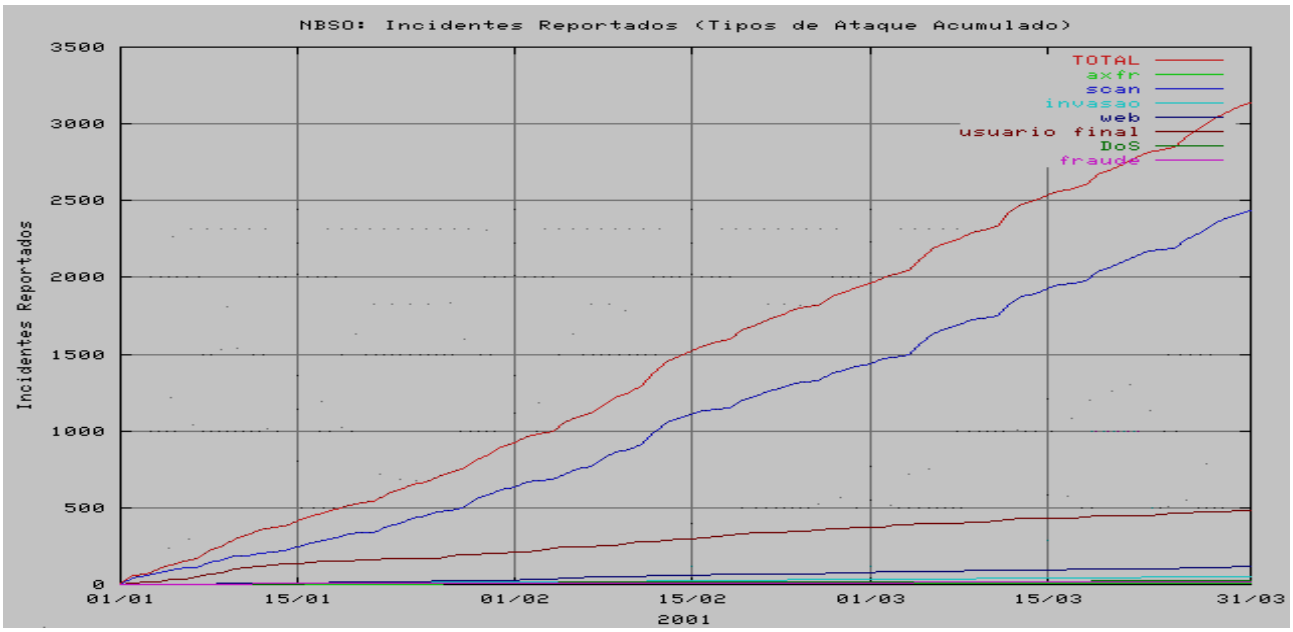
4 - Estatísticas

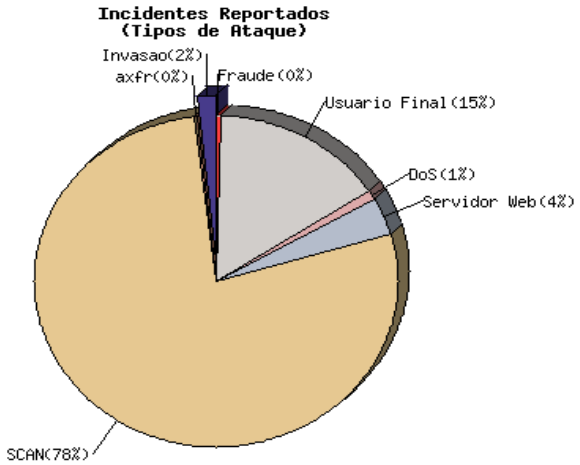
Os dados reportados abaixo, foram extraídos do site do CERT - http://www.cert.org , o qual é um centro de incidentes de segurança .

Número de Incidentes reportados.								
Ano	1988	1989	1990	1991	1992	1993	1994	1995
Incidentes	6	132	252	406	773	1334	2340	2412
Ano	1996	1997	1998	1999	2000	2001	2002	
Incidentes	2573	2134	3734	9859	21756	52658	43136	

Podemos perceber claramente o aumento de incidentes reportados ano a ano, isso devido a grande divulgação de falhas em sistemas operacionais, através da Internet. O ano de 2002 compreende o primeiro semestre.

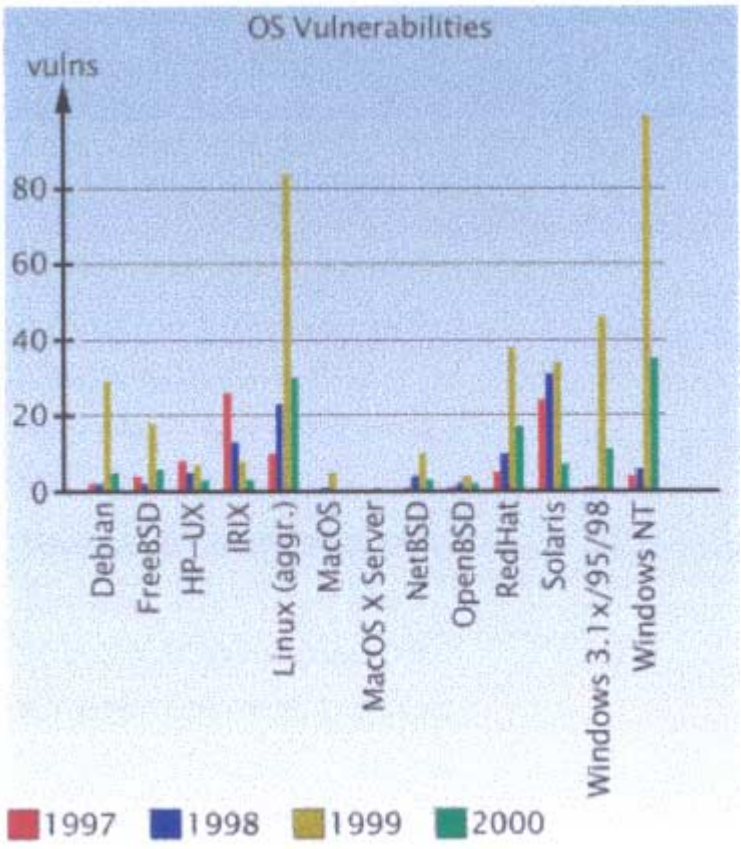
Os gráficos abaixo mostram os incidentes reportados, ao órgão de incidentes nacionais (NBSO) em 2002, por tipo de ataque:



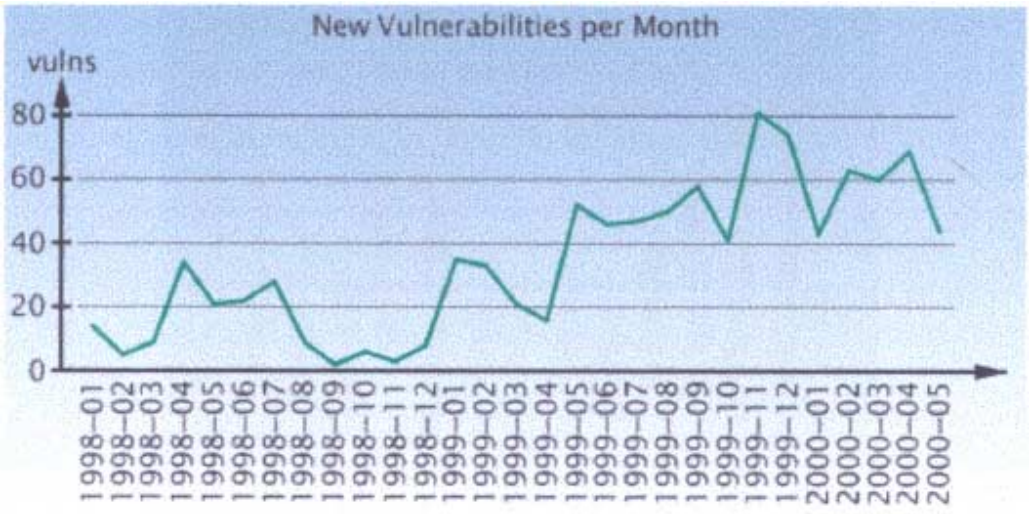


Percebemos que a maioria dos ataques é do tipo "*portscan*", o qual procura portas vulneráveis a ataques.

No gráfico abaixo, as vulnerabilidades descobertas , por sistemas operacionais , nos anos de 1997 a 2000:



Agora , as mesmas vulnerabilidades num escopo geral mês a mês:



5 – Conclusão

Com o portal seguro, os usuários e máquinas da rede interna estarão mais protegidos, mantendo o sigilo das informações e a integridade do sistema operacional.

Para isso, o administrador da rede, deverá se manter atualizado no que se refere ao sistema operacional, pois a todo instante são criados novos programas para explorar as vulnerabilidades dos sistemas, como mostram as estatísticas.

A segurança pró-ativa é a base desse projeto, visto que devemos tentar pensar antes dos intrusos(*hackers*).

Devemos lembrar, também , que não existe segurança total, só se desligarmos as máquinas. Mas mesmo assim, não estaríamos livres dos ladrões.

Boa sorte aos administradores de rede!

6 - Referências

Sites:

http://www.sunfreeware.com
http://www.cert.org/stats/
http://www.linuxsecurity.com.br
http://www.cipsga.org.br
http://www.unixsecurity.com.br
http://www.registro.br
http://www.nic.br
http://www.olinux.com.br
http://www.linux.trix.net
http://www.cbpf.br
http://www.securityfocus.com
http://www.snort.org
http://www.openssh.org
http://www.openssl.org
http://www.tcpdump.org

Notas Técnicas:

"Segurança – Secure Shell (ssh)", Anderson Alves de Albuquerque, Marita Maestrelli - Centro Brasileiro de Pesquisas Físicas (CBPF) , aaa@cbpf.br: outubro de 2001.

"Web-Server Seguro: Apache",Anderson Alves de Abuquerque, Marita Maestrelli, Centro Brasileiro de Pesquisas Físicas (CBPF) , aaa@cbpf.br: dezembro de 2000.

"Webmail Seguro", José Gracia Neto, Marita Maestrelli, Centro Brasileiro de Pesquisas Físicas (CBPF), zegracia@cbpf.br : outubro de 2001.

"Segurança na Web", Bernardo Trovão, Fernanda Jannuzzi, Marita Maestrelli, Centro Brasileiro de Pesquisas Físicas (CBPF): Outubro de 2000.

"Passwords – Segurança de Sistemas Redes UNIX", Mário Henrique de Sá Vera, Marita Maestrelli, Centro Brasileiro de Pesquisas Físicas (CBPF): Novembro de 1994.

7 – Glossário

Apache
Servidor de HTTP desenvolvida pela “The Apache Software Foundation”. Atualmente ‘eo servidor de web mas usado na internet. Suportado por plataformas Linux, Unix, OS/2, Windows e etc...

Buffer Overflow
É uma das técnicas mais usadas atualmente. Um programa que manipula dados do sistema, geralmente reserva espaços de memória(buffers) para manipulação desses dados. Quando um utilizador do programa envia mais dados do que o espaço permitido, nós temos um estouro do buffer(Buffer Overflow).

Bug
Expressão que caracteriza falha de programação em software ou em um sistema operacional.

Cache
Tem a função de armazenar dados previamente consultados em vez de busca-lo na origem.

CDE (Common Desktop Enviroment)
Ambiente Gráfico muito utilizado pelo sistema Unix.

CISCO
É uma empresa internacional que é uma das lideres em soluções de Redes Corporativas, Internetworking e Telecomunicações.

Client
Quem gera requisição ao servidor.

EEPROM
Acrônimo para memória de leitura programável e eletricamente apagável.EEPROM é um tipo especial de PROM que pode ser apagado expondo-o a uma carga elétrica. Como outros tipos de PROM, EEPROM mantem seu conteúdo, mesmo quando o computador é desligado.

Finger
Comando do Unix que procura informações dos usuários.

Firewall
Equipamento utilizado para proteger uma rede, pode ser dividido basicamente em firewall de filtro de pacotes, NAT, proxy (gateway de aplicação) e gateway de circuito.

FTP(File Transfer Protocol)
Protocolo para transferência de arquivo, porta 21-tcp.

Gateway
Equipamento responsáveis pelo roteamento de pacotes entre duas ou mais redes.

GUI (Grafical user Interface)
É uma interface gráfica alernativa para quem não quer usar CDE ou Openwindows.

Host
Qualquer computador,equipamento, de usuário final que conecta a rede.

Hostname
O nome dado ao host.

Http (Hyper Text Transfer Protocol)
Protocolo da World Wide Web.

IDS
E uma classe de programas dedicados a monitorar uma rede buscando indícios de tráfego ilegal e possíveis tentativas de invasão.

Inetd
Software que gerencia o processo de inicialização de um servidor. Chamado de super servidor.

Internet
Conjunto de Hosts, redes e roteamento que utiliza o protocolo TCP/IP unindo mais de 61 paises. Formando uma única rede. Intranet - uma Internet local.

IP
Protocolo usado para identificar os computadores com endereços ips de origem e destino.

Ip Address
Endereço com 32 bits (IPV4), este caracteriza um host na rede. Também é dividido em redes classes A,B,C,D,E

IPV4
Versão atual do IP.

Kerberos
É um protocolo de autenticação de rede. É designado para prover autenticação entre cliente e servidor.

Kernel
Módulo central de um sistema aberto.É a parte do sistema operacional que carrega primeiramente e fica na memória principal.

LDAP (Lightweight Directory Access Protocol)
É um banco de dados com informações da entidade e dos usuários.

Log
Armazenando de ocorrências para realização de auditorias.

NFS (Network file System)
Protoco que possibilita o compartilhamento de arquivos entre duas ou mais maquinas UNIX/LINUX Porta 2049/tcp e udp.

Nis
É um sistema de banco de dados distribuído pela rede, de modo que todas as máquinas tenham acesso.

Nis+
Foi feito para substituir o Nis, aumentando a segurança usando um método de autenticação adicional.

OS/2
Sistema operacional desenvolvido pela IBM voltado para o mercado coorporativo e domestico.

Protocolo
Descrição formal das regras que possibilitam a troca de informações entre os dispositivos de rede.

Patches
Arquivos para correção de falhas no sistema.

Rcp
Copia remotamente um ou mais arquivos entre dois sistemas.

Rlogin
Protocolo de acesso remoto

Root
Conta que controla o sistema (super usuário)

Roteador
São equipamentos para interconexão de duas redes que utilizam a mesma camada de transporte, porem possuem camadas de rede diferentes.

RPC (Remote Procedure Call)
RPC permite o desenvolvimento de aplicações em rede por meio de chamadas e uma biblioteca de rotinas especializadas em comunicação de rede.

Rsh
Abre um Shell em um sistema remoto.

Server
Uma máquina específica conectada a rede, geralmente 24h ao dia, que roda alguns programas na qual gera serviços para a requisição do cliente.

Sniffer
É um programa que deixa a interface de rede em modo promíscuo. Programa muito utilizado por hackers

SNMP (Simple Network Management Protocol)
O protocolo SNMP permite que administradores remotamente monitorem e configurem dispositivos como roteadores, switches e sistemas de gerenciamento de redes.

Snort
É uma ferramenta de detecção de intrusão

Solaris
É o sistema operacional UNIX fabricado pela empresa Sun Microsystems.

SSL (Secure Socks Layer)
Protocolo desenvolvido pela netscape que oferece serviço de segurança acima do protocolo tcp.

SSH (Secure Shell)
Protocolo de acesso remoto que possui um canal encriptado. Possui as versões ssh1 e ssh2 estas versões de ssh utilizam algoritmo de encriptacao RSA e DAS respectivamente. Porta 22/tcp.

TCP
Protocolo orientado a comunicação e atua na camada de transporte.

Tcpdump
É uma ferramenta que coleta dados na rede.

Tcpwrapper
É um software que monitora os serviços de rede.

Telnet
Protocolo que possibilita a emulação de terminal entre duas maquinas. Porta 23/tcp

UDP (User Datagram Protocol)
Protocolo não orientado a comunicação e atua na camada de transporte.

UNIX
É um tipo de sistema operacional com diversas distribuições no mercado. Como exemplo temos o solaris (Sun Microsystems).

Windows
Sistema Operacional desenvolvido pela Microsoft , possuidor de vários problemas de estabilidade e segurança, mas possui recursos que torne o sistema agradável.

WWW (World Wide Web)
Recurso de hipermídia para acessar a internet. Desenvolvido pelo CERN.

YP (Yellow pages)
É um banco de dados muito parecido com o Nis.

Anexo 1

Filtros de pacotes em roteadores Cisco

Anderson Alves de Albuquerque, Eng.

1 - Introdução

As regras de filtragem (filtro de pacotes - *firewall* de primeira geração) atuam apenas na camada de transporte garantindo proteção contra alguns tipos de ataques. Alguns ataques como o DOS, trojans, apple java, buffer overflow, HP com códigos javas nocivos, e vírus, os filtros de pacotes não podem proteger ou podem proteger parcialmente. Para alguns desses ataques há necessidade de um *firewall* de segunda ou terceira geração, que atuam na camada de aplicação.

2 - Desenvolvimento

As sintaxes dos filtros de pacotes sao baseadas em: protocolo, ip de origem, máscara de origem, ip de destino , máscara de destino, portas/serviços e *flags* do tcp/ip.

Existe a possibilidade enviar logs para um "servidor de logs do tipo *syslog(Unix)*".

2.1 - Exemplos de protocolos usados pelo filtro de pacotes do Cisco:

eigrp Cisco's EIGRP routing protocol
gre Cisco's GRE tunneling
icmp Internet Control Message Protocol
igmp Internet Gateway Message Protocol
igrp Cisco's IGRP routing protocol
ip Any Internet Protocol
ipinip IP in IP tunneling
nos KA9Q NOS compatible IP over IP tunneling
ospf OSPF routing protocol
tcp Transmission Control Protocol
udp User Datagram Protocol

2.2 - Descrição de serviços:

Os números de portas são agrupados em três faixas:

- Well Known Ports - 0 a 1023
- Registered Ports - 1024 a 49151

- Dynamic and/or Private Ports - 49152 a 65535

A primeira faixa está destinada a serviços bem estabelecidos e de interesse geral. Normalmente, a ativação desses serviços exige privilégios de administrador do sistema.

A segunda faixa usada para os programas de usuários(clientes) e outros serviços, que podem ser ativados sem privilégios de administrador.

Basicamente, quando um cliente conecta um serviço como o *smtp* ele o faz abrindo a conexão por uma porta maior que 1023 , enquanto o servidor escuta na porta 25.

Para a maioria dos serviços este modelo é verdadeiro. Salvo casos como NFS,X -windows, OpenWindows, portmap e outros.

2.3 - Exemplos de ataques que podem ser bloqueados:

2.3.1. Bloquear spoofing:

- proibir, na entrada, endereços originados da mesma rede

2.3.2. Bloquear pacotes com endereços inválidos:

- proibir, na entrada, endereços de redes privadas(RFC1918) que são :
  10.0.0.0/8
  192.168.0.0/16
  172.16.0.0/16

- proibir, na entrada, endereço de loopback (127.0.0.1)

- proibir, na entrada, endereços inexistentes (255.255.255.255)

2.3.3. Bloquear ataque land:

- proibir, na entrada, endereços da própria interface(origem e destino), evitando que sejam enviados para o router pacotes onde o endereco ip de origem e destino são os mesmos da interface externa e interna. Este tipo de ataque e muito usado para ataques em windows 95/98.

2.3.4. Bloquear pacotes de saída que no sejam da própria rede:

- proibir, na saída, endereços de origem que não sejam da rede. Neste tipo de ataque é caracterizado a tentativa de atacar uma rede externa, como por exemplo o ataque smurf , onde são enviados pacotes da sua rede "W" para o broadcast de uma rede "X" ,alternando a origem como se fosse uma rede "Y". Como isso a rede "X" irá enviar respos- tas para "Y".

2.3.5.Permitir acesso ao servidor Web:

- requisição cliente externo:

Permitir, na entrada, pacotes originados de portas > 1023 para a porta 80

- resposta do servidor interno:

Permitir, na saída, pacotes da porta 80 para portas > 1023 em conexões já estabelecidas .

2.3.6. Permitir acesso de clientes locais para Web:

- requisição cliente interno:

Permitir, na saída, pacotes de portas > 1023 para porta 80

- resposta do servidor externo:

Permitir, na entrada, pacotes da porta 80 para portas > 1023 em conexões já estabelecidas

2.3.7. Desvio de pacotes ip source route:

- comando para desabilitar o source route:

no ip source-route

2.3.8 Log no roteador Cisco:

- No roteador Cisco:

Adicionar "**log**" no final das regras do router por exemplo:
access-list 130 deny udp any any eq netbios-ns **log**
access-list 130 deny udp any any eq netbios-dgm **log**

cisco (config)# logging on
cisco (config)# logging x.y.z.w --> servidor de syslog
cisco (config)# logging trap 6 --> 6 = trap_number
cisco (config)# logging facility local0 --> local6 = facility_type

onde, **trap_number** pode ser:
0 = emergencies (LOG_EMERG)
1 = alerts (LOG_ALERT)
2 = critical (LOG_CRIT)
3 = errors (LOG_ERR)
4 = warnings (LOG_WARNING)
5 = notifications (LOG_NOTICE)
6 = informational (info) (LOG_INFO)
7 = debugging (LOG_DEBUG)
[default=6]

Em alguns IOS dos roteadors Cisco em vez do código (trap number) é necessário escrever o trap)

Onde, **facility_type** pode ser (algumas sugestões):
local0
local4
local6
local7

- Na servidora de logs Unix:

No /etc/syslog.conf adicione:
local0.info /var/log_do_cisco/router.log

Crie o arquivo de log:
touch /var/log_do_cisco/router.log

Reinicialize o processo do syslog:
kill -HUP syslog_pid_number

2.3.9 proibir acesso a portas de serviços que historicamente são atacados:

netbeui -> tcp/udp 137,136 e 139
X-windows -> tcp/udp 6000 ate 6011
openwindows -> tcp/udp 2000 ate 2002
bootp -> udp 67
tftp -> tcp/udp 69
rpc -> tcp/udp 111
snmp -> udp 161 ate 162
bgp -> tcp 169
talk -> tcp/udp 517
uucp -> tcp 520

nfs -> 2049
rlogins -> tcp 513
rexec -> tcp 514
lpd -> tcp 515
outros rcomandos -> tcp 512
finger -> tcp 79
router -> tcp/udp 520

Obs: alguns desses serviços pode ser necessário, e nesse caso deve -se apenas redirecionar as portas para os hosts confiáveis.

2.3.10. backdoors conhecidas:

netbus -> tcp/udp 31337
backorifice -> tcp/udp 12345
backorifice 2 -> tcp/udp 20034

2.3.11. desabilitar alguns serviços desnecessários:

Exemplo: no service finger

2.3.12. Ativar acesso criptografado ao router

Alguns IOS do roteador Cisco possuem suporte para acessos criptogra- fados por kerberos e/ou ssh.

Uma alternativa para os routers Cisco que não possuem suporte é desati- var o telnet e ter um servidor/estação Unix confiável com o *sshd* instalado ,e o cabo conectado no console do router Cisco, para acessá-lo.

Após conectar ao servidor com *ssh* basta executar:

cu -l /dev/cuaa0
(este exemplo foi usado em um servidor com sistema operacional freebsd)

2.3.13. Bloquear pacotes no *broadcast* da rede

2.3.14. Sincronizar o relógio do roteador pelo protocolo ntp(porta 123 udp)

Exemplo:
! Setup our clock environment
clock timezone PST -8
clock summer-time zone recurring
! Configure NTP
ntp authenticate
ntp authentication-key 1 md5 ntpk3y
ntp trusted-key 1
ntp access-group peer 20
ntp server ntp_server1_ip key 1 prefer
ntp server ntp_server2_ip key 1

Exemplo de um access-list :

Access-list 101

```
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny   ip any 0.0.0.255 255.255.255.0 log
access-list 101 deny   ip any 0.0.0.0 255.255.255.0 log
access-list 101 deny   ip any 0.0.0.0 255.255.255.0 log
access-list 101 permit tcp any any established
access-list 101 deny   tcp any any eq 12345 log
access-list 101 deny   udp any any eq 12345 log
access-list 101 deny   tcp any any eq 20034 log
access-list 101 deny   udp any any eq 20034 log
access-list 101 deny   tcp any any eq 31337 log
access-list 101 deny   udp any any eq 31337 log
access-list 101 deny   tcp any any range 6000 6011 log
access-list 101 deny   udp any any range 6000 6011 log
access-list 101 deny   tcp any any range 2000 2003 log
access-list 101 deny   udp any any range 2000 2003 log
access-list 101 deny   tcp any any eq 2049 log
access-list 101 deny   udp any any eq 2049 log
access-list 101 permit tcp any any range  1024 65535
access-list 101 permit udp any any range 1024 65535
```

```
access-list 101 deny   tcp any any log
access-list 101 deny   udp any any log
access-list 101 permit icmp any any
```

Anexo 2

Exemplo do arquivo /etc/syslog.conf

```
#ident  "@(#)syslog.conf        1.5     98/12/14 SMI"   /* SunOS 5.0 */
#
```

```
# Copyright (c) 1991-1998 by Sun Microsystems, Inc.
# All rights reserved.
#
# syslog configuration file.
#
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words.  Also, within ifdef's, arguments
# containing commas must be quoted.
#
*.err;kern.notice;auth.notice                   /dev/sysmsg
*.err;kern.debug;daemon.notice;mail.crit        /var/adm/messages

local0.notice                           /var/log/pop.log

*.alert;kern.err;daemon.err                     operator
*.alert                                 root

*.emerg                                 *

# if a non-loghost machine chooses to have authentication messages
# sent to the loghost machine, un-comment out the following line:
auth.notice                     ifdef(`LOGHOST', /var/log/authlog, @loghost)
mail.debug                      /var/log/syslog
daemon.notice;daemon.info;daemon.debug          /var/log/inetdlog

#
# non-loghost machines will use the following lines to cause "user"
# log messages to be logged locally.
#
ifdef(`LOGHOST', ,
user.err                                /dev/sysmsg
user.err                                /var/adm/messages
user.alert                              `root, operator'
user.emerg                              *
)
```