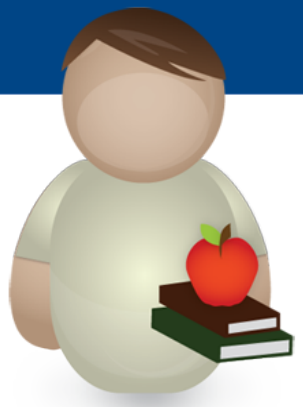


Disciplina:
Segurança de Redes

Professor:
Roitier Campos

Aula 04

Introdução ao Hardening de Servidores

Introdução

O termo Hardening é utilizado em redes de computadores quando se faz necessário estabelecer parametros de configuração que visam proteger o Sistema Operacional, utilizando de ferramentas específicas para cada tipo de ação.

O Hardenig de Servidores é a aplicação dessas configurações em um Servidor de Rede, visando proteger o Servidor e tudo o que o servidor, eventualmente controla e, quando for o caso, protege.

O portal DevMedia.com.br traz a seguinte definição:

Hardening, ou blindagem de sistemas, consiste na utilização de técnicas para prover mais segurança a servidores que disponibilizam serviços externos, como servidores Web, ou até mesmo serviços internos, como servidores de banco de dados, de arquivos, entre outros.

Caracteristicas dos serviços da rede

De forma geral, um servidor é um computador da rede que dispões de serviços para outros computadores.

Um serviço de rede estar:

- Acessível a qualquer máquina;
- Acessível a apenas algumas máquinas;
- Não estar acessível.

Obs: Para cada serviço há pelo menos um processo (daemon) associado

Run Level

Runlevel é o nível de inicialização do sistema. Este nível decide qual serviço vai inicializar ou não com o sistema.

Após o carregamento do sistema, o kernel é carregado na memória, junto com os dispositivos que estão no /etc/fstab e no /etc/dev.

Temos então, o carregamento do sistema. Este acontece no /etc/init.d, onde ficam todos os ***daemons*** que são iniciados como sistema, todos os scripts responsáveis por parar ou iniciar um serviço estão no /etc/init.d.

Daemons

Daemon é um script que é utilizado para dar start, stop ou restart em um serviço. Quando o sistema é ativado, o primeiro arquivo a ser lido é o **/etc/inittab**, que armazena o runlevel do sistema na seguinte linha **id:x:initdefault,** onde x é o runlevel padrão.

As opções que podemos colocar no inittab são:

- 0 → Logo após iniciar o sistema o mesmo já finaliza todos os serviços e desliga.
- 1 → Temos ao iniciar o modo monousuário.
- 2-5 → Temos os modos multiusuários que podem ser tanto gráfico como no modo texto.
- 6 → Modo que reinicia a máquina.

Iniciando e Parando serviços

Sintaxe: /etc/init.d/(serviço) start/stop

Ex: /etc/init.d/apache start

Obs: Para cada run-level são executados os scripts do /etc/rcN.d;

- S20shh (inicia o serviço SSH com prioridade 20;
- K20sssh (interrompe o serviço SSH com prioridade 20);

Inicie apenas quando precisar

Uma das regras básicas da segurança de redes de computadores é:

- Não oferecer serviços desnecessários;
- Um servidor nunca deve conter programas “clientes”;
- telnet, rshd, rlogind, rwhod, ftpd, sendmail, identd, wget, dentre outros, deverão ser removidos

OBS: Serviços pouco utilizados costumam ser menos monitorados. Este pode ser uma porta para os atacantes.

Ex real: Porta para cachorros.

RCCONF

O rcconf é um front-end para o update-rc.d, e normalmente precisa ser instalado:

#apt-get install rcconf

O rcconf permite você controlar que serviços são iniciados quando o sistema inicia (:S), ele irá mostrar uma tela onde você poderá ver o status de cada serviço [*] ou [ ].

#rcconf

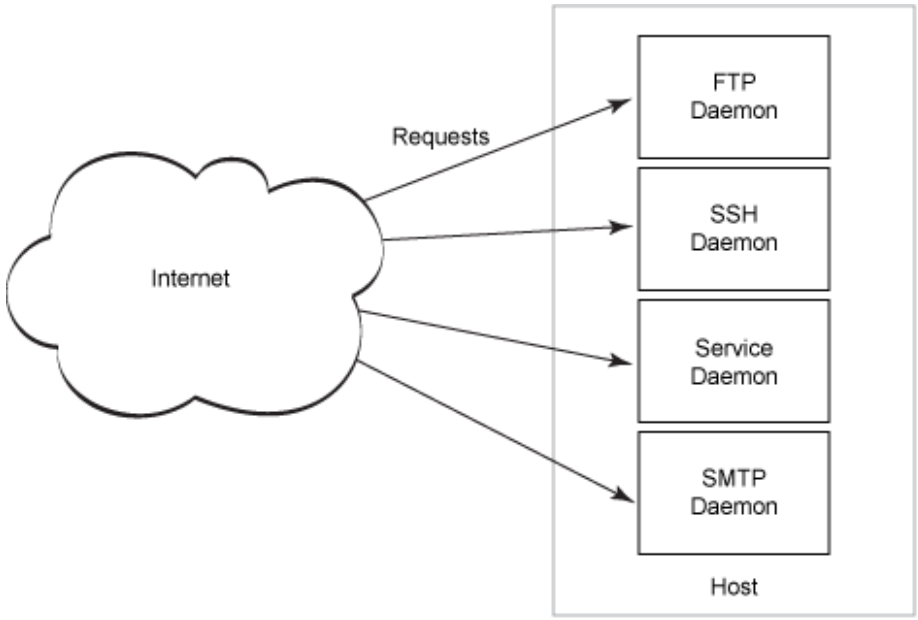
Atividade sugerida

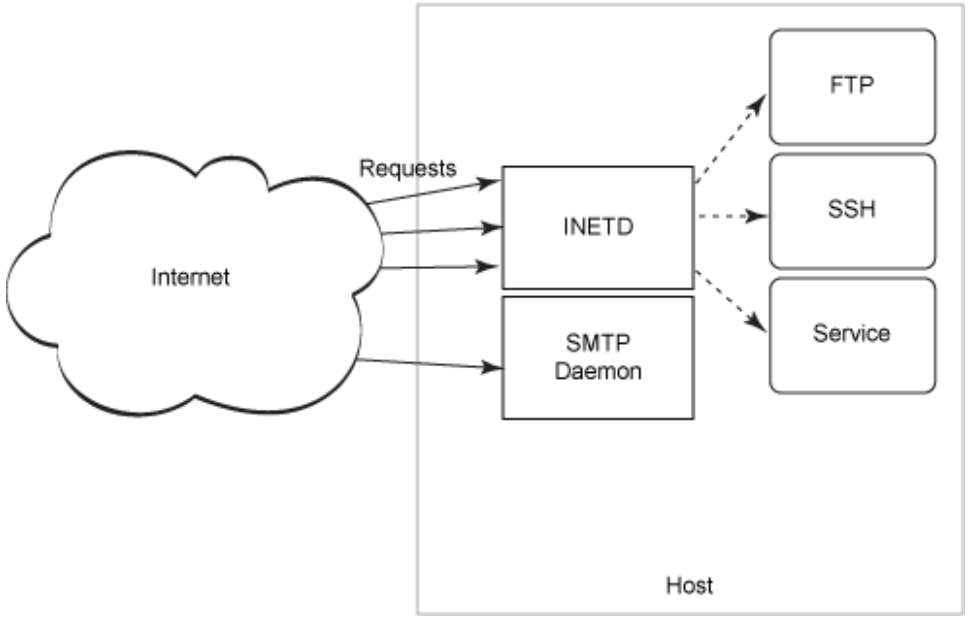
Instale e utilize o RCCONF para iniciar a parar serviços no seu Sistema Operacional

Daemon xinetd

O xinetd carrega seu arquivo de configuração e passa a “ouvir” por conexões em portas específicas.

Quando uma conexão é solicitada, o xinetd executa o programa servidor correspondente para manipular o serviço solicitado. Então, desta forma, existirá apenas um servidor em memória esperando por uma solicitação.





/etc/xinetd.conf)

Defaults – sessão com configurações referentes a todos os serviços monitorados pelo xinetd:

```
Defaults

{

Instances = 25  #controla o número de conexões simultâneas em um serviço

per_source = 10 #Controla o número máximo de conexões originadas de uma mesma máquina.

log_type = SYSLOG authpriv #Indica como o xinetd irá logar as requisições.

log_on_success = HOST PID USERID #Informa ao xinetd quais informações ele deverá capturar do usuário que conseguir logar.

log_on_failure = HOST RECORD USERID #Indica quais informações deverão ser capturadas dos usuários que não conseguirem logar.

}
```

/etc/xinetd.conf

O superservidor ou xinetd é configurado para iniciar a sua execução quando o sistema é inicializado, recebendo a lista de serviços a serem monitorados a partir de um arquivo denominado /etc/xinetd.conf ou através de uma arquivo por serviço.

Neste ultimo caso, o xinetd.conf tem que conhecer a localização dos arquivo individuais de cada serviço. Para isso, inclua a linha a seguir no arquivo /etc/xinetd.conf

```
includedir /etc/xinetd.d
```

/etc/xinetd.d (arquivos por serviço)

- Utiliza-se sempre um arquivo para cada serviço;
- Recomenda-se nomear o arquivo com o nome do serviço;
- Dois arquivos para um mesmo serviço gera inconsistência;

Exemplo:

root@roitier-C400-G-BC23P1:/etc/xinetd.d# ls

chargen daytime discard echo telnet time

/etc/xinetd.d/telnet

```
service telnet
{
flags = REUSE
log_type = FILE /var/log/telnet.log
socket_type = stream
protocol = tcp
wait = no
user = root
server = /usr/sbin/in.telnetd
bind = 200.1.1.20
redirect = 192.168.1.111 23
only_from = 192.168.1.0/24
}
```

/etc/xinetd.d/ssh

```
service ssh
{
  disable          = no
  socket_type      = stream
  port             = 22
  wait             = no
  user             = root
  server           = /usr/sbin/sshd
  server_args      = -i
 }
```

Detalhes do arquivo do serviço

flags: Recebe as opções passadas em linha de comando para o daemon.

socket_type: Especifica o tipo de socket usado, como: dgram, stream ou raw.

protocol: Indica o protocolo usado pelo serviço.

wait: Diz ao xinetd se ele deve chamar o serviço sobre demanda ou não.

user: Usuário que executará o serviço.

server: Localização do daemon do serviço.

bind: O IP ou host especificado aqui será origem quando um serviço for redirecionado com o uso da opção redirect.

redirect: Host ou IP da máquina que receberá a requisição do serviço.

only_from: Limita os endereços de IP que terão acesso a determinado serviço

Localizando o daemon do serviço

O comando **which** é utilizado para mostrar a localização do daemon de um determinado serviço.

Exemplos

- root@roitier-C400-G-BC23P1:/# which telnet

  /usr/bin/telnet

- root@roitier-C400-G-BC23P1:/# which telnet

  /usr/bin/telnet

Desativando portas desnecessárias

Com a utilização do xinetd, as portas do servidor deverão ficar todas fechadas. Isso porque o xinetd fará requisições às portas à medida que forem ocorrendo requisições aos xinetd.

Para isso, será necessário scannear todas as portas do computador através de um Scanner de portas. Neste caso utilizaremos o **nmap**. Outras opções como: *Advanced Port Scanner, NetView Scanner e Free Port Scanner.*

NMAP

Segudo o Wikipédia, o Nmap é um software livre que realiza port scan desenvolvido pelo Gordon Lyon, autoproclamado hacker "Fyodor". É muito utilizado para avaliar a segurança dos computadores, e para descobrir serviços ou servidores em uma rede de computadores.

#apt-get install nmap

Alternativa com interface gráfica: Zenmap

Scaneando o localhost (127.0.0.1)

root@roitier-C400-G-BC23P1:/etc/xinetd.d# nmap 127.0.0.1

Starting Nmap 6.40 (http://nmap.org) at 2014-08-29 10:17 BRT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000024s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
631/tcp open ipp
3306/tcp open mysql
9050/tcp open tor-socks

Nmap done: 1 IP address (1 host up) scanned in 2.52 second

Fechando uma porta

Depois de scannear o servidor, feche a porta desejada e mate o processo que abriu essa porta com os comandos:

- fuser -v 9050/tcp #fecha a porta 9050
- Kill -9 1470 #mata o processo que chama a porta

Obs: Para que o serviço não inicialize após a reinicialização do sistema retire-o do boot através do RCCONF. Haverá caso que matar a porta não resolverá. Retirar do Boot é necessário. (ex: 22/tcp)

Testando a configuração do xinetd

Restart do servidor:

- # service xinetd restart
- # /etc/rc.d/init.d/xinetd restart

Deverá surgir a seguinte informação dizendo que o servidor está sendo paralisado e re-iniciado.

- Stopping xinetd: [OK]
- Starting xinetd: [OK]

Cópia de arquivos com SSH (scp)

O SSH é um protocolo que permite o acesso remoto criptografado a sistemas operacionais através da porta 22/tcp.

É possível realizar cópias de arquivos, em rede, através do protocolo SSH. Para isso, utiliza-se o comando scp, que é o tradicional comando "cp" + ssh.

Exemplo:

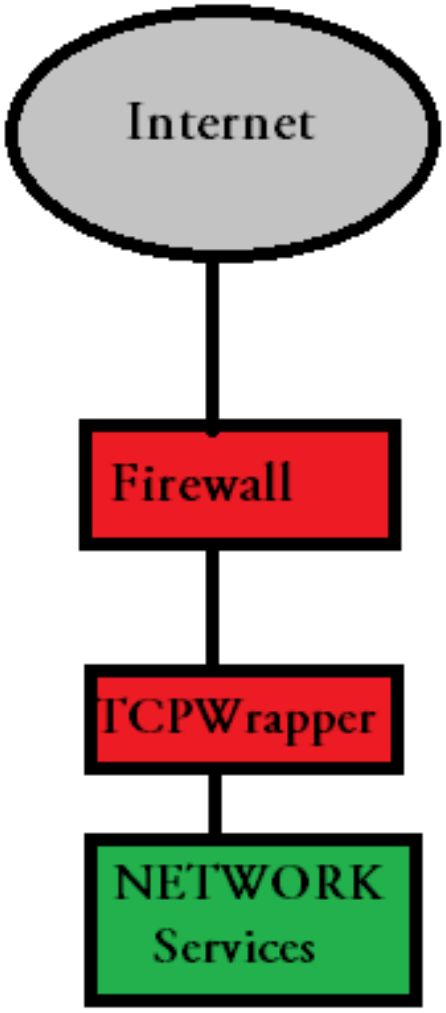
- **scp roitier@127.0.0.1:/home/roitier/testescp /home**

Algumas variações do ''scp''

- scp tux@192.168.254.156:/home/roitier/Images/teste /home/roitier/dir_teste/
- scp arquivo.txt roitier@192.168.254.92
- scp megaupload roitier@192.168.254.156:/home/roitier/Public
- scp -P 6969 megaupload roitier@192.168.254.156:/home/roitier/Public

TCPWrapper

- TCP Wrapper é visto como uma camada adicionl de proteção;
- Utiliza ACL's específicas para cada serviço;
- TCP Wrapper basea-se no em host/rede (host-based);
- O executável /usr/sbin/tcpd (TCP Wrapper Daemon) é instalado através pelo **tcpd** e a biblioteca libwrap pelo pacote **libwrap0;**



Verificação de Suporte

Para saber se um serviço oferece suporte para **libwrap** utilizamos o comando **ldd**.

#type -P sshd | xargs ldd | fgrep libwrap

Arquivos Hosts (allow e deny)

As configurações do TCPwrapper podem sem manipuladas através dos arquivos:

- /etc/hosts.allow
- /etc/hosts.deny

Arquivos

- tftpd: 192.168.0.1 # permite acesso ao computador 192.168.0.1 acessar o serviço tftp
- tftpd: 192.168.0. # permite acesso a todos os computadores da rede 192.168.0.0 acessar o serviço tftp
- ALL: ALL # permite acesso a todos os computadores acessar todos os serviços
- ALL: LOCAL # permite acesso a todos os computadores da rede local acessar todos os serviços
- tftpd: .linuxbrasil.org.br # permite acesso a todos os computadores do domínio linuxbrasil.org.br acessar o serviço tftp
- ALL 192.168.1. EXCEPT sshd: 192.168.1.2 # permite acesso a todos os computadores da rede 192.168.1.0 acessar todos os serviços, exceto o serviço sshd para o host 192.168.1.2
- ALL: .linuxbrasil.org.br EXCEPT pc01.linuxbrasil.org.br # permite acesso a todos os computadores do domínio linuxbrasil.org.br

Atividade Complementar

1) Interrompa o ssh;

2) Remova-o da inicialização do sistema (rcconf);

3) Configure o seu xinetd;

4) Teste serviços aleatóriamente em duplas;

5) Desabilite os serviços configurados no xinetd da inicialização do Sistema.

6) Configure o Tcpwrapper (definição de permissões) hosts.allow e hosts.deny

7) Teste com o comando scp;