

Securing Linux Internet Server

Arnon Rungsawang

fenganr@ku.ac.th

Massive Information & Knowledge Engineering

Department of Computer Engineering

Faculty of Engineering

Kasetsart University, Bangkok, Thailand.

Outline

- Any computer connected to the internet will require steps and precautions to be taken to reduce the exposure to hacker threats. Web, mail and DNS servers are especially vulnerable.
- This tutorial covers steps and tools which can be used to monitor and counteract hacker threats.
 - Basic security steps.
 - SSH (Secure Shell) and OpenSSH.
 - PortSentry.
 - Nmap.
 - Tripwire.

Basic security steps (1)

- See distribution [errata and security fixes](#), and update your system where appropriate.
- Reduce the number of network services exposed. The more services exposed, the greater your vulnerability.
 - Reduce the number of network services accessible through the `inetd` or `xinetd` daemon.
 - Turning of an `inetd` service: `/etc/inetd.conf`

```
# /etc/inetd.conf
```

```
...
```

```
# Pop and imap mail services et al
```

```
#pop-2 stream tcp nowait root /usr/sbin/tcpd ipop2d
```

```
#pop-3 stream tcp nowait root /usr/sbin/tcpd ipop3d
```

```
#imap stream tcp nowait root /usr/sbin/tcpd imapd
```

```
# The Internet UUCP service.
```

```
#uucp stream tcp nowait uucp /usr/sbin/tcpd /usr/lib/uucp/uucico -l
```

```
# Tftp service is provided primarily for booting. Most sites
```

```
# run this only on machines acting as "boot servers." Do not uncomment
```

```
# this unless you *need* it.
```

```
#tftp dgram udp wait root /usr/sbin/tcpd in.tftpd
```

```
#bootps dgram udp wait root /usr/sbin/tcpd bootpd
```

- Turning on/off an xinetd service: `/etc/xinetd.d/`

```
[root@tutu]$ less /etc/xinetd.d/tftp
# default: off
# description: The tftp server serves files using the trivial file transfer \
#      protocol. The tftp protocol is often used to boot diskless \
#      workstations, download configuration files to network-aware printers, \
#      and to start the installation process for some operating systems.
service tftp
{
    disable = yes
    socket_type          = dgram
    protocol             = udp
    wait                 = yes
    user                 = root
    server               = /usr/sbin/in.tftpd
    server_args          = -s /tftpboot
}
```

- We can also use the command **chkconfig wu-ftp on** and **chkconfig wu-ftp off** that will edit appropriate file (/etc/xinetd.d/wu-ftp) and restart the xinetd process.
- List init settings including all xinted controlled services, use command **chkconfig --list**

```
[root@tutu]$ chkconfig --list
```

```
...  
lpd          0:off 1:off 2:on 3:off 4:on 5:on 6:off  
xfs          0:off 1:off 2:on 3:off 4:on 5:on 6:off  
ntpd        0:off 1:off 2:off 3:off 4:off 5:off 6:off  
nfs         0:off 1:off 2:off 3:on 4:off 5:off 6:off  
nfslock     0:off 1:off 2:off 3:on 4:on 5:on 6:off  
identd     0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

```
xinetd based services:
```

```
...  
finger:      off  
rexec:       off  
rlogin:      on  
rsh:         on  
ntalk:       off  
talk:        off  
telnet:      on  
wu-ftp:      on
```

Basic security Steps (2)

- Reduce the number of non-inetd network services that have been started by scripts in /etc/rc.d/rc*.d/ directories.
 - There may be no need to run sendmail (mail server), portmap (RPC listener required by NFS), lpd (line printer server daemon), innd (news server), linuxconf etc.

```
[root@tutu]$ ls /etc/rc.d/init.d/
```

```
amd      gated      kadmin     mcscrv     portmap    rstatd    ups
anacron  gpm        kdcrotate  mysqld    postgresql rusersd   vncserver
apmd     halt       keytable   named     pxe        rwalld    wine
arpwatch httpd      killall    netfs     radvd      rhod      xfs
atd      identd    kprop      network   random     sendmail  xinetd
autofs   innd      krb524     nfs       rarpd      single    ypbind
bcm5820  ipchains  krb5kdc    nfslock   rawdevices smb        yppasswdd
bgpd     iptables  kudzu      nscd      reconfig   snmpd     ypserv
bootparamd irda      ldap       ntpd      rhnsd      squid     ypxfrd
cron     iscsi     linuxconf  ospf6d    ripd       sshd      zebra
dhcpd    isdn      lpd        ospfd     ripngd     syslog
functions junkbuster mars-nwe   pcmcia    routed     tux
```

- Terminate the service using a command:

```
[root@tutu]$ /etc/rc.d/init.d/sendmail stop
Shutting down sendmail: [ OK ]
[root@tutu]$ chkconfig --level 3 sendmail off
[root@tutu]$
```

- To see what daemons are configured to be operable after boot-up using a command:

```
[root@tutu]$ chkconfig --list
...
lpd      0:off  1:off  2:on   3:off  4:on   5:on   6:off
xfs      0:off  1:off  2:on   3:off  4:on   5:on   6:off
ntpd     0:off  1:off  2:off  3:off  4:off  5:off  6:off
nfs      0:off  1:off  2:off  3:on   4:off  5:off  6:off
xinetd based services:
...
finger:      off
rexec:       off
rlogin:      on
rsh:         on
talk:        off
telnet:      on
wu-ftpd:     on
```

Basic security Steps (3)

- Verify your configuration. List the open ports and processes which hold them.

```
[root@tutu]$ netstat -pnta
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:32768	0.0.0.0:*	LISTEN	690/rpc.statd
tcp	0	0	0.0.0.0:513	0.0.0.0:*	LISTEN	915/xinetd
tcp	0	0	0.0.0.0:32769	0.0.0.0:*	LISTEN	951/rpc.mountd
tcp	0	0	0.0.0.0:514	0.0.0.0:*	LISTEN	915/xinetd
tcp	0	0	0.0.0.0:111	0.0.0.0:*	LISTEN	662/portmap
tcp	0	0	0.0.0.0:1009	0.0.0.0:*	LISTEN	828/ypbind
tcp	0	0	0.0.0.0:21	0.0.0.0:*	LISTEN	915/xinetd
tcp	0	0	0.0.0.0:23	0.0.0.0:*	LISTEN	915/xinetd
tcp	0	0	0.0.0.0:702	0.0.0.0:*	LISTEN	946/rpc.rquotad
tcp	0	0	192.168.33.123:23	192.168.33.97:40378	ESTABLISHED	21209/in.telnetd: m
tcp	0	0	192.168.33.123:824	192.168.33.115:992	TIME_WAIT	-
tcp	0	158	192.168.33.123:23	192.168.33.174:3727	ESTABLISHED	21022/in.telnetd: l
udp	0	0	0.0.0.0:32768	0.0.0.0:*		690/rpc.statd
udp	0	0	0.0.0.0:32769	0.0.0.0:*		951/rpc.mountd
udp	0	0	0.0.0.0:699	0.0.0.0:*		946/rpc.rquotad
udp	0	0	0.0.0.0:837	0.0.0.0:*		828/ypbind
udp	0	0	0.0.0.0:866	0.0.0.0:*		690/rpc.statd
udp	0	0	0.0.0.0:1006	0.0.0.0:*		828/ypbind
udp	0	0	0.0.0.0:111	0.0.0.0:*		662/portmap

Basic security Steps (4)

- Configure FTP server with great care.
 - There are three kinds of FTP logins that wu-ftpd provides:
 - **anonymous FTP** - one logs in with the username 'anonymous'.
 - **real FTP** - log in with a real username and password and **has access to the entire disk structure**.
 - **guest FTP** - one logs in with a real user name and password, but the user is chroot'ed to his home directory and cannot escape from it.
 - They are constrained to their home directory which also means that they don't have access to /bin/lis and other commands on the server.
 - Thus a local minimalist environment must be set up.

Disable anonymous FTP

- anonymous FTP allows users to ftp to your server and log in with the login anonymous and use an email address as the password.
 - To turn of this feature, edit the file `/etc/ftpaccess` and change:

```
class all real,guest,anonymous *  
to  
class all real,guest *
```

Basic security Steps (5)

- Use the **find** command to locate vulnerabilities.
 - Find suid and guid files as well as world writable files and directories.
 - Search and list all files from current directory and down for the string *ABC*:
find ./ -name "*" -exec grep -H ABC {} \;
 - Find all files of a given type from current directory on down:
find ./ -name "*.conf" -print
 - Find all user files larger than 5Mb:
find /home -size +500000c -print
 - Find all files owned by a user (defined by user id number. see /etc/passwd) on the system: (could take a very long time)
find / -user 501 -print
 - Find all suid and setgid executables:
find / \(-perm -4000 -o -perm -2000 \) -type f -exec ls -ldb {} \;
find / -type f -perm +6000 -ls
 - ...

Basic security Steps (6)

- Use the command `chattr` and `lsattr` to make a file unmodifiable over and above the usual permissions.
 - Make a file unmodifiable:
 - `chattr +i /bin/l`
 - Make directories unmodifiable:
 - `chattr -R +i /bin /sbin`
 - Make a file append only:
 - `chattr +a /var/log/messages`
- Use `tripwire` to monitor your system for signs of unauthorized file changes.
 - “Tripwire for Servers software assures the security and integrity of data on your servers by notifying users if, when, and how files have changed.” (<http://www.tripwiresecurity.com>)

Basic security Steps (7)

- Watch your log files frequently, especially `/var/log/message` and `/var/log/secure`.
- Avoid generic account names such as **guest**.
- Use PAM to disallow passwords which can be found easily by crack or other hacking programs.

```
# /etc/pam.d/login
# (This is a fairly minimal 'login' configuration)
#
auth      requisite pam_securetty.so
auth      requisite pam_nologin.so
auth      required pam_unix.so nullok
account   required pam_unix.so
session   required pam_unix.so
password  required pam_cracklib.so retry=3 minlen=9
password  required pam_unix.so use_authok nullok obscure
```

Basic security Steps (8)

- Use /proc file setting for defending against attack, i.e. SYN flood, syncookie attack,...

```
#/etc/sysctl.conf
...
#Enable Ignoring Ping Request
net.ipv4.icmp_echo_ignore_all=1
#Enable Ignoring Ping Broadcast
net.ipv4.icmp_echo_ignore_broadcasts=1
#Enable TCP SYN Cookie Protection
net.ipv4.tcp_syncookies=1
#Disable IP Source Routing
net.ipv4.conf.all.accept_source_route=0
#Disable ICMP Redirect Acceptance
net.ipv4.conf.all.accept_redirects=0
#Enable IP Spoofing Protection
net.ipv4.conf.all.rp_filter=1
...
```

Basic security Steps (9)

- Use Linux firewall rules to protect against attacks.

```
#Allow loopback access. This rule must come before the rules denying port access!!  
#This rule is essential if you want your own computer to be able to access itself through  
#the loopback interface.
```

```
ipchains -A input -s 0/0 -d 0/0 -i lo -j ACCEPT
```

```
ipchains -A input -p tcp -s 0/0 -d 0/0 2049 -y -j REJECT # Block NFS
```

```
ipchains -A input -p udp -s 0/0 -d 0/0 2049 -j REJECT # Block NFS
```

```
ipchains -A input -p tcp -s 0/0 -d 0/0 6000:6009 -y -j REJECT # Block X-Windows
```

```
ipchains -A input -p tcp -s 0/0 -d 0/0 7100 -y -j REJECT # Block X-Windows font server
```

```
ipchains -A input -p tcp -s 0/0 -d 0/0 515 -y -j REJECT # Block printer port
```

```
ipchains -A input -p udp -s 0/0 -d 0/0 515 -j REJECT # Block printer port
```

```
ipchains -A input -p tcp -s 0/0 -d 0/0 111 -y -j REJECT # Block Sun rpc/NFS
```

```
ipchains -A input -p udp -s 0/0 -d 0/0 111 -j REJECT # Block Sun rpc/NFS
```

```
#Deny and log (option -l) outside packets from internet which claim to be from your  
#loopback interface.
```

```
ipchains -A input -j REJECT -p all -s localhost -i eth0 -l
```

Lokkit firewall tool



Securing Linux Internet Server

Basic security step (9)

Lokkit firewall tool

```
root@tutu:~  
lokkit 0.50 (C) 2001 Red Hat, Inc.  
----- Firewall Configuration - Customize -----  
  
You can customize your firewall in two ways. First, you can select to  
allow all traffic from certain network interfaces. Second, you can allow  
certain protocols explicitly through the firewall. Specify additional  
ports in the form 'service:protocol', such as 'imap:tcp'.  
  
Trusted Devices: [*] eth0 [ ] irlan0  
  
Allow incoming: [ ] DHCP [*] SSH [ ] Telnet  
[*] WWW (HTTP) [*] Mail (SMTP) [ ] FTP  
Other ports domain:tcp, domain:udp  
  
OK  
  
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen
```

Securing Linux Internet Server

Basic security step (9)

Lokkit firewall tool

```
[root@tutu]# cat /etc/sysconfig/ipchains
# Firewall configuration written by lokkit
# Manual customization of this file is not recommended.
# Note: ifup-post will punch the current nameservers through the
#       firewall; such entries will *not* be listed here.
:input ACCEPT
:forward ACCEPT
:output ACCEPT
-A input -s 0/0 -d 0/0 53 -p tcp -y -j ACCEPT
-A input -s 0/0 -d 0/0 53 -p udp -j ACCEPT
-A input -s 0/0 -d 0/0 22 -p tcp -y -j ACCEPT
-A input -s 0/0 -d 0/0 25 -p tcp -y -j ACCEPT
-A input -s 0/0 -d 0/0 80 -p tcp -y -j ACCEPT
-A input -s 0/0 -d 0/0 -i lo -j ACCEPT
-A input -s 0/0 -d 0/0 -i eth0 -j ACCEPT
-A input -p tcp -s 0/0 -d 0/0 0:1023 -y -j REJECT
-A input -p udp -s 0/0 -d 0/0 0:1023 -j REJECT
-A input -p tcp -s 0/0 -d 0/0 6000:6009 -y -j REJECT
-A input -p tcp -s 0/0 -d 0/0 7100 -y -j REJECT
[root@tutu]# /etc/rc.d/init.d/ipchains restart
Flushing all current rules and user defined chains:      [ OK ]
Clearing all current rules and user defined chains:      [ OK ]
Applying ipchains firewall rules:                        [ OK ]
[root@tutu]#
```

Basic security Steps (10)

- Remote access should NOT be done with clear text telnet but with an encrypted connection using `ssh`.
- Use `portsentry` to monitor network hacker attacks.
- A minimal and monolithic kernel might also provide a small bit of protection (avoid trojan modules) as well as running on less common hardware (MIPS, Alpha, etc... so buffer overflow instructions will not run.)

Basic security Steps (11)

- DDoS (Distributed Denial of Service) attacks.
 - The only thing you can do is have gobs of bandwidth and processing power/firewall.
 - Lots of processing power or a firewall are useless without gobs of bandwidth as the network can get so overloaded from a distributed attack.
 - Block icmp and invisible to ping using ipchains:
ipchains -A output -p icmp -d 0/0 -j DENY
 - Or set tunable kernel parameters in `/etc/sysctl.conf`
`#Enable Ignoring Ping Request`
`net.ipv4.icmp_echo_ignore_all=1`
- A minimal and monolithic kernel might also provide a small bit of protection (avoid trojan modules) as well as running on less common hardware (Sun, Alpha, ...).

Securing Linux Internet Server

SSH & OpenSSH

OpenSSH - Microsoft Internet Explorer

File Edit View Favorites Tools Help


Address <http://www.openssh.org/> Go Links >>

Language: [en]
[de] [es] [fr]
[hu] [ja] [ru]

About OpenSSH

[Project Goals](#)
[History and Credits](#)
[Features](#)
[Security](#)
[Press Coverage](#)
[Systems using OpenSSH](#)
[Usage Statistics](#)

Resources



**OpenSSH 3.0.2 released December 3, 2001.
Contains support for SSH1 and SSH2 protocols.**

OpenSSH is a **FREE** version of the SSH protocol suite of network connectivity tools that increasing numbers of people on the Internet are coming to rely on. Many users of telnet, rlogin, ftp, and other such programs might not realize that their password is transmitted across the Internet unencrypted, but it is. OpenSSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks. Additionally, OpenSSH provides a myriad of secure tunneling capabilities, as well as a variety of authentication methods.

Internet

SSH & OpenSSH

- SSH protocol suite of network connectivity tools:
 - Encrypt connections across the Internet.
 - Encrypt all traffic including logins and passwords to eliminate network sniffing, connection hijacking, and other network-level attacks.
- SSH is a commercial product but available freely for non-commercial use at <http://www.ssh.com>
- OpenSSH, compatible with SSH1 and SSH2, relies on the OpenSSL project for the encrypted communication layer.

Client config /etc/ssh/ssh_config

```
# $OpenBSD: ssh_config,v 1.10 2001/04/03 21:19:38 todd Exp $
# This is ssh client systemwide configuration file.  See ssh(1) for more
# information.  This file provides defaults for users, and the values can
# be changed in per-user configuration files or on the command line.
...
# Site-wide defaults for various options
# Host *
#   ForwardAgent no
#   ForwardX11 no
#   RhostsAuthentication no
#   RhostsRSAAuthentication yes
...
#   CheckHostIP yes
#   StrictHostKeyChecking yes
#   IdentityFile ~/.ssh/identity
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_rsa
#   Port 22
#   Protocol 2,1
Protocol 2
#   Cipher blowfish
#   EscapeChar ~
Host *
    ForwardX11 yes
```

Server config /etc/ssh/sshd_config

```
# $OpenBSD: sshd_config,v 1.38 2001/04/15 21:41:29 deraadt Exp $
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin
# This is the sshd server system-wide configuration file. See sshd(8)
# for more information.
```

Port 22

#Protocol 2,1

Protocol 2

#ListenAddress 0.0.0.0

#ListenAddress ::

HostKey /etc/ssh/ssh_host_key

HostKey /etc/ssh/ssh_host_rsa_key

HostKey /etc/ssh/ssh_host_dsa_key

ServerKeyBits 768

LoginGraceTime 600

KeyRegenerationInterval 3600

PermitRootLogin no

#

Don't read ~/.rhosts and ~/.shosts files

IgnoreRhosts yes

Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication

#IgnoreUserKnownHosts yes

StrictModes yes

X11Forwarding yes

...

Start/stop sshd daemon, usage

- To start/stop a sshd daemon server:

```
[root@mike]# /etc/rc.d/init.d/sshd start
Starting sshd: [ OK ]
[root@mike]# /etc/rc.d/init.d/sshd stop
Stopping sshd: [ OK ]
[root@mike]#
```

- To connect to another server:

```
[arnon@merlin]$ ssh arnon@mozilla
The authenticity of host 'mozilla (192.168.33.65)' can't be established.
DSA key fingerprint is 1b:9e:27:ed:8a:b1:54:1d:aa:20:c6:ef:42:e3:5d:89.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mozilla,192.168.33.65' (DSA) to the list of known hosts.
arnon@mozilla's password:
Last login: Thu Mar 07 2002 11:31:42 +0700 from 192.168.33.174
[arnon@mozilla]$
```

SSH notes

- The sshd should not be started using xinetd/inetd due to time necessary to perform calculations when it is initialized.
- ssh client will suid to root. sshd on the server is run as root. Root privileges are required to communicate on ports lower than 1024. The -p option may be used to run SSH on a different port.
- RSA is used for key exchange, and a conventional cipher (default Blowfish) is used for encrypting the session.
- Encryption is started before authentication, and no passwords or other information is transmitted in the clear.

SSH notes (2)

- Authentication:
 - Login is invoked by the user. The client tells the server the public key that the user wishes to use for authentication.
 - Server then checks if this public key is admissible. If yes then random number is generated and encrypts it with the public key and sends the value to the client.
 - The client then decrypts the number with its private key and computes a checksum. The checksum is sent back to the server.
 - The server computes a checksum from the data and compares the checksums.
 - Authentication is accepted if the checksums match.
- To establish a secure network connection on another TCP port, use "tunneling" options with the ssh command:
 - Forward TCP local port to hostport on the remote-host:
ssh remote-host -L port:localhost:hostport command

Securing Linux Internet Server

Psionic Technologies™ is a provider of intelligent security tools and services. With our [TriSentry™](#) suite ([PortSentry™](#), [HostSentry™](#), and [LogSentry™](#)) of intrusion protection tools you can protect your network-computing environment from attack. This intelligent security solution enhances the security of your

PortSentry

- Monitor the network probes and attacks against your server in real-time.
 - A log indicating the incident is made via `syslog()`.
 - Target host is automatically dropped into `/etc/hosts.deny` for TCP Wrappers.
 - Local host can be configured to route all traffic to the target to a dead host to make the target system disappear.
 - Local host can be configured to drop all packets from the target via a local packet filter.

PortSentry (2)

- Steps to install and configure PortSentry.
 - Download and unzip source code.
 - Edit include file and compile.
 - Start PortSentry.
 - Read logs.

PortSentry (3)

- Download and unzip source code.
 - Download: <http://www.psionic.com/products/port Sentry.html>
 - Move to your source directory and unzip:
tar -xzf portsentry-1.1.tar.gz
- Edit include file and compile:
 - Edit `portsentry_config.h`
 - `CONFIG_FILE` – PortSentry runtime configuration file.
 - `WRAPPER_HOST_DENY` – The path and name of TCP wrapper `host.deny` file.
 - `LOG_DAEMON` will log messages to the `/var/log/messages` file.

```
#define CONFIG_FILE "/etc/portsentry/portsentry.conf"  
/* The location of Wietse Venema's TCP Wrapper hosts.deny file */  
#define WRAPPER_HOSTS_DENY "/etc/hosts.deny"  
/* The default syslog is as daemon.notice. You can also use */  
/* any of the facilities from syslog.h to send messages to (LOCAL0, etc) */  
#define SYSLOG_FACILITY    LOG_DAEMON  
#define SYSLOG_LEVEL      LOG_NOTICE
```

PortSentry (4)

- Add logging directives to syslogd configuration file:
`/etc/syslog.conf`
 - Change the following line to reflect that portsentry messages are not going to be logged to the regular syslog output file `/var/log/messages` (Note that you must use tab not spaces in the syslog configuration file).
`*.info;mail.none;news.none;authpriv.none;local6.none /var/log/messages`
- Add the following line to assign a portsentry log facility:
`local6.* /var/log/portsentry.log`
 - Restart syslogd
`/etc/rc.d/init.d/syslog restart`
 - Set portsentry_config.h entry to new log facility:
`#define SYSLOG_FACILITY LOG_LOCAL6`

Options for the SYSLOG_FACILITY are defined in /usr/include/sys/syslog.h

SYSLOG_FACILITY	Facility Name	Description
LOG_LOCAL0	local0	reserved for local use
LOG_LOCAL1	local1	reserved for local use
LOG_LOCAL2	local2	reserved for local use
LOG_LOCAL3	local3	reserved for local use
LOG_LOCAL4	local4	reserved for local use
LOG_LOCAL5	local5	reserved for local use
LOG_LOCAL6	local6	reserved for local use
LOG_LOCAL7	local7	reserved for local use
LOG_USER	user	random user-level messages
LOG_MAIL	mail	mail system
LOG_DAEMON	daemon	system daemons
LOG_SYSLOG	syslog	messages generated internally by syslogd
LOG_LPR	lpr	line printer subsystem
LOG_NEWS	news	network news subsystem
LOG_UUCP	uucp	UUCP subsystem
LOG_CRON	cron	clock daemon
LOG_AUTHPRIV	authpriv	security/authorization messages (private)
LOG_FTP	ftp	ftp daemon

Options for the SYSLOG_LEVEL include:

SYSLOG_LEVEL	Priority	Description
LOG_EMERG	0	system is unusable
LOG_ALERT	1	action must be taken immediately
LOG_CRIT	2	critical conditions
LOG_ERR	3	error conditions
LOG_WARNING	4	warning conditions
LOG_NOTICE	5	normal but significant condition
LOG_INFO	6	informational
LOG_DEBUG	7	debug-level messages

PortSentry (5)

■ Edit `portsentry.conf`

- Set paths for configuration files and ports to monitor.

```
# Hosts to ignore
IGNORE_FILE="/etc/portsentry/portsentry.ignore"
# Hosts that have been denied (running history)
HISTORY_FILE="/etc/portsentry/portsentry.history"
# Hosts that have been denied this session only (temporary until next restart)
BLOCKED_FILE="/etc/portsentry/portsentry.blocked"
...
KILL_ROUTE="/sbin/route add -host $TARGET$ reject"
...
# Default TCP ident and NetBIOS service
#ADVANCED_EXCLUDE_TCP="113,139"
ADVANCED_EXCLUDE_TCP="21,22,25,53,80,119,113,139"
# Default UDP route (RIP), NetBIOS, bootp broadcasts.
#ADVANCED_EXCLUDE_UDP="520,138,137,67"
ADVANCED_EXCLUDE_UDP="21,22,53,520,138,137,67"
...
KILL_HOSTS_DENY="ALL: $TARGET$"
...
```

PortSentry (6)

- Route deny options: network “`route`” or firewall command “`ipchains`”.
 - Simple method to drop network return routes if ipchains are not compiled into your kernel:

```
KILL_ROUTE="/sbin/route add -host $TARGET$ reject"
```

- For Linux 2.2.x kernels using ipchains:

```
KILL_ROUTE="/sbin/ipchains -I input -s $TARGET$ -j DENY -I"
```

- Edit `portsentry.ignore` to contain ip address to be ignored.

```
127.0.0.1/32
```

```
0.0.0.0
```

```
158.108.33.99
```

PortSentry (7)

- Edit the Makefile:

```
#CC = cc
# GNU..
CC = gcc
# Normal systems flags
CFLAGS = -O -Wall
# Debug mode for portsentry
#CFLAGS = -Wall -g -DNODAEMON -DDEBUG
#CFLAGS = -Wall -g -DNODAEMON
#CFLAGS = -Wall -g -DDEBUG
# Profiler mode for portsentry
#CFLAGS = -pg -O -Wall -DNODAEMON
#LIBS = /usr/lib/libefence.a
```

```
INSTALLDIR = /etc
CHILDDIR=/portsentry
```

- Compile and install PortSentry:

make linux; make install

PortSentry (8)

- Run PortSentry for advanced UDP/TCP stealth scan detection:
 - `portsentry -atcp`
 - `portsentry -audp`
 - Or use init scripts!
- Check logfile for hacker attacks.
 - See `/var/log/portsentry`
 - Check `/var/hosts.deny` to see a list of IP address that PortSentry has deemed attackers.
 - Check the history file `/etc/portsentry/portsentry.history`

PortSentry (9)

- Notes on DoS (Denial of Service) possibility.
 - If PortSentry is configured to shut down an attack with firewall rules, an attacker may use this feature to slow down your machine over time by creating a huge set of firewall rules. In this case, it would require the hacker to use (or spoof) a new IP address each time.
 - It is probably a good idea to monitor or even clear the firewall rules from time to time.
 - ipchains
 - list firewall rules: **ipchains -L**
 - clear firewall rules: **ipchains -F**
 - Or create a clean-up script `/etc/cron.weekly/reset-chainrules` which will be run automatically once a week by cron.

/etc/cron.weekly/reset-chainrules

```
#!/bin/bash

# An example of reset-chainrules
# Purge and re-assign chain rules
ipchains -F
ipchains -A input -p tcp -s 0/0 -d 0/0 2049 -y -j REJECT
ipchains -A input -p udp -s 0/0 -d 0/0 2049 -j REJECT
ipchains -A input -p tcp -s 0/0 -d 0/0 6000:6009 -y -j REJECT
ipchains -A input -p tcp -s 0/0 -d 0/0 7100 -y -j REJECT
ipchains -A input -p tcp -s 0/0 -d 0/0 515 -y -j REJECT
ipchains -A input -p udp -s 0/0 -d 0/0 515 -j REJECT
ipchains -A input -p tcp -s 0/0 -d 0/0 111 -y -j REJECT
ipchains -A input -p udp -s 0/0 -d 0/0 111 -j REJECT
ipchains -A input -j REJECT -p all -s localhost -i eth0 -l
```

PortSentry (10)

- Configure logrotate for portsentry.
 - `/etc/logrotate.d/portsentry`

```
/var/log/portsentry.log {  
    rotate 12  
    monthly  
    errors root@localhost  
    missingok  
    postrotate  
        /usr/bin/killall -HUP portsentry 2> /dev/null || true  
    endscript  
}
```

Securing Linux Internet Server

FREE KEVIN
Welcome to
Insecure.Org
GNU

Last modified: Monday, 12-Nov-2001 11:10:03 PST
WHAT IS YOUR OPERATING SYSTEM LETTING OTHERS DO? *Nmap now!*

Nmap stealth port scanner

- [Intro](#)
- [Download](#)
- [OS Detect](#)

Security

Tools

Good Reading

Security Lists

- [Nmap-hackers](#)
- [Nmap-dev](#)
- [Bugtraq](#)

NMAP Free Security Scanner
Audit Your Network Now!
www.insecure.org/NMAP

Introduction	Documentation	Propaganda
Download	OS Detection	Portability
In The News	Related Projects	Thanks To

Introduction

Nmap ("Network Mapper") is an open source utility for network exploration c
It was designed to rapidly scan large networks, although it works fine agains
Nmap uses raw IP packets in novel ways to determine what hosts are availat

Nmap

- A hacker tool responsible for many of the portscans you may be receiving.

`nmap -sT -F IP-address` **Scan**

`nmap -sS -F IP-address` **SYN Scan**

`nmap -sU -F IP-address` **Scan UPD ports**

`nmap -sF -F IP-address` **FIN Scan**

`nmap -O -F IP-address` **Determine OS**

`nmap -p22 -F -O IP-address`

`nmap -p 1-30,40-65535 IP-Address` **Scan given port ranges**

- Add the option `-v` (verbose) or `-vv` (super verbose) for more info.
- The ports will be determined to be open, filtered or firewalled.

Nmap (2)

```
[root@mike root]# nmap -sS -F -O mozilla.cpe.ku.ac.th
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on mozilla.cpe.ku.ac.th (158.108.33.105):
(The 1079 ports scanned but not shown below are in state: closed)
```

Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
98/tcp	open	linuxconf
111/tcp	open	sunrpc
113/tcp	open	auth
513/tcp	open	login
1024/tcp	open	kdm

```
Remote operating system guess: Linux 2.1.122 - 2.2.16
Uptime 3.108 days (since Mon Mar 4 21:17:44 2002)
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 29 seconds
[root@mike root]#
```

Nmap (3)

```
[root@mike root]# nmap -sS -F -O mike.cpe.ku.ac.th
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on mike.cpe.ku.ac.th (158.108.33.97):
(The 1077 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp    open      ssh
37/tcp    open      time
80/tcp    open      http
111/tcp   open      sunrpc
443/tcp   open      https
3128/tcp  open      squid-http
3306/tcp  open      mysql

No exact OS matches for host (If you know what OS is running on it, see http://www...
TCP/IP fingerprint:
SInfo(V=2.54BETA22%P=i386-redhat-linux-gnu%D=3/7%Time=3C879BB3%O=22%C=1)
T1(Resp=Y%DF=Y%W=7FFF%ACK=S++%Flags=AS%Ops=MNNTNW)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=7FFF%ACK=S++%Flags=AS%Ops=MNNTNW)
T4(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=C0%IPLen=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=...
```

Uptime 19.116 days (since Sat Feb 16 21:09:45 2002)
Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds
[root@mike root]#

TRIPWIRE

Data Integrity Assurance

Tripwire establishes a baseline of data in its desired state, detects and reports any changes to the baseline, and enables fast discovery and remediation when an undesired change occurs.

Tripwire for Routers and Switches	Tripwire for Servers	Tripwire Manager
Tripwire for Routers and Switches reduces network downtime through immediate detection and notification of changes to Cisco routers or switches. more	Tripwire for Servers software assures the security and integrity of data on your servers by notifying users if, when, and how files have changed. more	Tripwire Manager is a cross-platform management console for managing up to 2,500 Tripwire for Servers installations. more

New Integrity Alert Posted
Use Tripwire Software to Detect a Backdoor Trojan Caused by the W32.Gibe@mm Worm Virus

FREE posters!
Vulnerability Matrix and new "Servers Under Siege"

Sign Up for **Tripwire Newsletters**

- General
- Linux
- Unix/Solaris
- NT/2000
- Routers & Network Devices

Enter E-mail:

[Register >>](#)

Tripwire

- Integrity checking of system files:
 - Create a database of system files, and a compact digital “snapshot” of the system.
 - Detect and report any additions, deletions, or changes to system outside of the specified boundary.
 - If the change is valid, admin can update the baseline database with the new information.
 - If malicious changes are found, admin can instantly know which parts of which components of the system have been affected.

Tripwire (2)

- Installation instructions assume that:
 - Command are Unix-compatible.
 - The source path is /var/tmp
 - All steps will happen in super-user account “root”.
 - Tripwire version number 1.3.1-1 download at <http://www.tripwiresecurity.com/>

Compilation Tripwire-1.3.1-1

- Decompress the tarball (tar.gz)

```
[root@godzilla]$ cp Tripwire-version.tar.gz /var/tmp
[root@godzilla]$ cd /var/tmp; tar xzpf Tripwire-version.tar.gz
[root@godzilla]$
```

- Compile and optimize

- Move into the new tripwire directory and type the following on your terminal:

- Edit the `utils.c` (src/utils.c) and change the line:

```
else if (iscntrl(*pcin)) {
to read
```

```
else if (!(*pcin&0x80) && iscntrl(*pcin)) {
```

- Edit the `config.parse.c` (src/config.parse.c) and change the line:

```
rewind(fpout);
```

```
to read
```

```
else {
    rewind(fpin);
}
```

Compilation Tripwire-1.3.1-1(2)

- Edit the `config.h` (include/config.h) and change the line:
`#define CONFIG_PATH "/usr/local/bin/tw"`
`#define DATABASE_PATH "/var/tripwire"`
to read
`#define CONFIG_PATH "/etc"`
`#define DATABASE_PATH "/var/spool/tripwire"`
- Edit the `config.h` (include/config.h) and change the line:
`#define TEMPFILE_TEMPLATE "/tmp/twzxxxxxx"`
to read
`#define TEMPFILE_TEMPLATE "/var/tmp/twzxxxxxx"`
- Edit the `config.pre.y` (src/config.pre.y) and change the line:
`#ifdef TW_LINUX`
to read
`#ifdef TW_LINUX_UNDEF`

Compilation Tripwire-1.3.1-1(3)

- Edit the **Makefile** (Makefile) and change the line:
DESTDIR=/usr/local/bin/tw
to read
DESTDIR= /usr/sbin

DATADIR=/var/tripwire
to read
DATADIR= /var/spool/tripwire

LEX=lex
to read
LEX=flex

CC=gcc
to read
CC=egcs

CFLAGS=-O
to read
**CFLAGS=-O9 -funroll-loops -ffast-math -malign-double
-mcpu=pentiumpro -march=pentiumpro -fomit-frame-
pointer -fno-exceptions**

Compilation Tripwire-1.3.1-1(4)

- Compile and install all binaries and supporting files into appropriate locations.
 - **make;make install**
 - **chmod 700 /var/spool/tripwire/**
 - **chmod 500 /usr/sbin/tripwire**
 - **chmod 500 /usr/sbin/siggen**
 - **rm -rf /usr/sbin/tw.config**

- Cleanup after work.
 - **cd /var/tmp**
 - **rm -rf tw_ASR_version/ Tripwire-version.tar.gz**

Tripwire configuration

- Set which system files and directories to be monitored in the `/etc/tw.config` file:

```
#/etc/tw.config
# First, root's "home"
/root R
!/root/.bash_history
/ R
# OS itself
/boot/vmlinuz R
# critical boot resources
/boot R
# Critical directories and files
/chroot R
/etc R /etc/inetd.conf R
/etc/nsswitch.conf R
/etc/rc.d R
/etc/mtab L
/etc/motd L
/etc/group R
/etc/passwd L
# other popular filesystems
/usr R /usr/local R
/dev L-am
/usr/etc R
# truncate home
=/home R
# var tree
=/var/spool L
/var/log L
/var/lib L
/var/spool/cron L
!/var/lock
# unusual directories
=/proc E
=/tmp
=/mnt/cdrom
=/mnt/floppy
```

- Run a command: **chmod 600 /etc/tw.config**

Tripwire's interactive checking mode

- Verify files or directories that have been added or deleted, or changed from the original database.
- Ask user whether the database entry should be updated.

- To create the Tripwire file information database:

```
[root@godzilla]$ cd /var/spool/tripwire  
[root@godzilla]$ /usr/sbin/tripwire --initialize
```

- To run Tripwire in interactive mode:

```
[root@godzilla]$ cd /var/spool/tripwire/database  
[root@godzilla]$ cp tw.db_myserverhostname /var/spool/tripwire  
[root@godzilla]$ cd ..
```

Tripwire's interactive checking mode (2)

```
[root@godzilla]$ /usr/sbin/tripwire -interactive
Tripwire(tm) ASR (Academic Source Release) 1.3.1
File Integrity Assessment Software (c) 1992
Purdue Research Foundation, (c) 1997, 1999
Tripwire Security Systems, Inc.
All Rights Reserved. Use Restricted to Authorized Licensees.
### Phase 1: Reading configuration file
### Phase 2: Generating file list
### Phase 3: Creating file information database
### Phase 4: Searching for inconsistencies
### ### Total files scanned:          15722
### ### Files added:                  34
### ### Files deleted:                42
### ### Files changed:                321
### ### Total file violations:        397
### added: -rwx----- root 22706 Dec 31 06:25:02 1999 /root/tmp/firewall
---> File: '/root/tmp/firewall'
---> Update entry? [YN(y)nh?]
```

Tripwire's database update mode

- If a single file has changed:

```
[root@godzilla]$ tripwire -update /etc/newly.installed.file
```

- If a single file has changed:

```
[root@godzilla]$ tripwire -update /usr/lib/Package_directory
```

- In either case above, Tripwire will regenerate the database entries for every specified file. A backup of the old database is created in the `./databases` directory.

