

Linux Security

Benchmarking, Security Tools,
Syslog Implementation, Incident
Handling

CERT-In Guidelines

- Security Template By CERT-In
 - A guide to configure Redhat Linux 9.0 as web server
- Central Syslog server guide
 - A guide to setup central syslog server with syslog-ng, mysql, apache, php

Tools

- CISecurity
 - Benchmark security configuration
- Bastile
 - Automated security setup tool

CISecurity

- www.cisecurity.com
 - Benchmark security configuration
 - ./cis-scan

Bastille

- Bastille is an open source program that facilitates the hardening of a Linux system.
- The administrator answers a series of “Yes” and “No” questions through an interactive textbased interface.

Currently available for various Linux distros

- SuSE
- TurboLinux Mandrake (several versions)
- RedHat (several versions)
- Debian
- Also available on MacOS X and HP/UX

Installation

The Bastille Linux package can be downloaded from <http://www.bastille-linux.org/>.

```
$ cd /usr/local/src
```

```
$ wget http://osdn.dl.sourceforge.net/sourceforge /bastille-linux/Bastille-2.0.4-1.0.i386.rpm
```

We also have to download the Perl Curses package:

```
$ wget http://www.bastille-linux.org/perl-Curses-1.06-4mdk.i386.rpm
```

To start the installation. Log in as root:

```
# rpm --nodeps -ivh perl-Curses-1.06-4mdk.i386.rpm
```

```
warning: perl-Curses-1.06-4mdk.i386.rpm: V3 DSA signature: NOKEY, key ID 70771ff3
```

```
Preparing. . .      ###      [100%]
```

```
# rpm -ivh Bastille-2.0.4-1.0.i386.rpm
```

```
preparing...###      [100%]
```

```
!Bastille  ###      [100%]
```

Run Bastille with the -c option:

```
# bastille -c
```

After typing Accept on a couple of screens we'll be presented with a set of 18 screens.

Bastille Text Interface Screen	Option	Our selection
1	Title screen (introduction to Bastille)	Select Next
2	Would you like to set more restrictive permissions on the administration utilities?	Select Yes, and then Next
	<p>Only root user will be able to access these utilities like <code>ifconfig</code>, <code>runlevel</code>, <code>portmap</code>, <code>fsck</code>, <code>linuxconf</code>.</p> <p>Disabling SUID status permission for the following programs. Only user with root privilege will be able to run these programs.</p> <p>Would you like to disable sum status for <code>Mountlumount</code>, <code>at</code>, <code>r-tools</code> (like <code>rsh</code> and <code>rcp</code>), <code>usernetctl</code>, <code>XFree86</code>? (<code>ping</code>, <code>traceroute</code>, <code>XFree86</code> programs will have SUID status enabled)</p>	Yes
3	<p>Should Bastille disable clear-text r-protocols that use IP-based authentication?</p> <p>Would you like to enforce password aging?</p> <p>Would you like to restrict the use of <code>crontab</code> to administrative accounts?</p> <p>Do you want to set a default <code>umask</code>?</p> <p>What <code>umask</code> would you like to set <i>for</i> users on the system?</p> <p>Should we disallow root login on tty's 1-6?</p>	<p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>077</p> <p>No</p>
4	<p>Would you like to password-protect the GRUB prompt?</p> <p>Would you like to disable <code>CTRL-ALT-DELETE</code> rebooting?</p> <p>Would you like to password protect single-user mode?</p>	<p>No</p> <p>Yes</p> <p>Yes</p>

5	<p>Would you like to set a default-deny on TCP Wrappers and xinetd?</p> <p>Should Bastille ensure the telnet service does not run on this system?</p> <p>Should Bastille ensure the FTP service does not run on this system?</p> <p>Would you like to display "Authorized <i>Use</i>" messages at log-in time? Now you will get a chance to customize the display message.</p> <p>Who is responsible <i>for</i> granting authorization to use this machine?</p>	<p>No</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Input administrator now</p>
6	<p>Would you like to disable the gcc compiler?</p>	<p>No</p>
7	<p>Would you like to put limits on system resource usage?</p> <p>Should we restrict console access to a small group of user accounts?</p>	<p>No</p> <p>No</p>
8	<p>Would you like to add additional logging?</p> <p>This script is adding additional logging files: /var/log/kernel - kernel messages /var/log/syslog- messages of severity 'warning' and 'error'</p> <p>Also, if you check the 7th and 8th TTYs, by hitting ALT-F7 or ALT-F8, you'll find that we are now logging to virtual TTY s as well. If you try this, remember that you can use ALT-F1 to get back to the first virtual TTY.</p> <p>Do you have a remote logging host? (Will configure it manually)</p>	<p>Yes</p>
9	<p>Would you like to disable apmd?</p> <p>Would you like to disable GPM?</p> <p>Would you like to deactivate NIS server programs?</p>	<p>Yes</p> <p>No</p> <p>Yes</p>

10	Do you want to stop sendmail from running in daemon mode?	No
11	Would you like to chroot named and set it to run as a non-root user?	No
12	<p>Would you like to bind the web server to listen only to the localhost?</p> <p>Would you like to bind the web server to a particular interface? (Will be doing Apache configuration manually)</p> <p>Would you like to deactivate the following of symbolic links? (Will be doing Apache configuration manually)</p> <p>Would you like to deactivate server-side includes? (Will be doing Apache configuration manually)</p> <p>Would you like to disable CGI scripts, at least for now? (Will be doing Apache configuration manually)</p> <p>Would you like to disable indexes? (Will be doing Apache configuration manually)</p>	<p>No</p> <p>No</p> <p>No</p> <p>No</p> <p>No</p>
13	Would you like to disable printing?	Yes
14	Would you like to install TMPDIR/TMP scripts?	No
15	Would you like to run the packet filtering script?	No

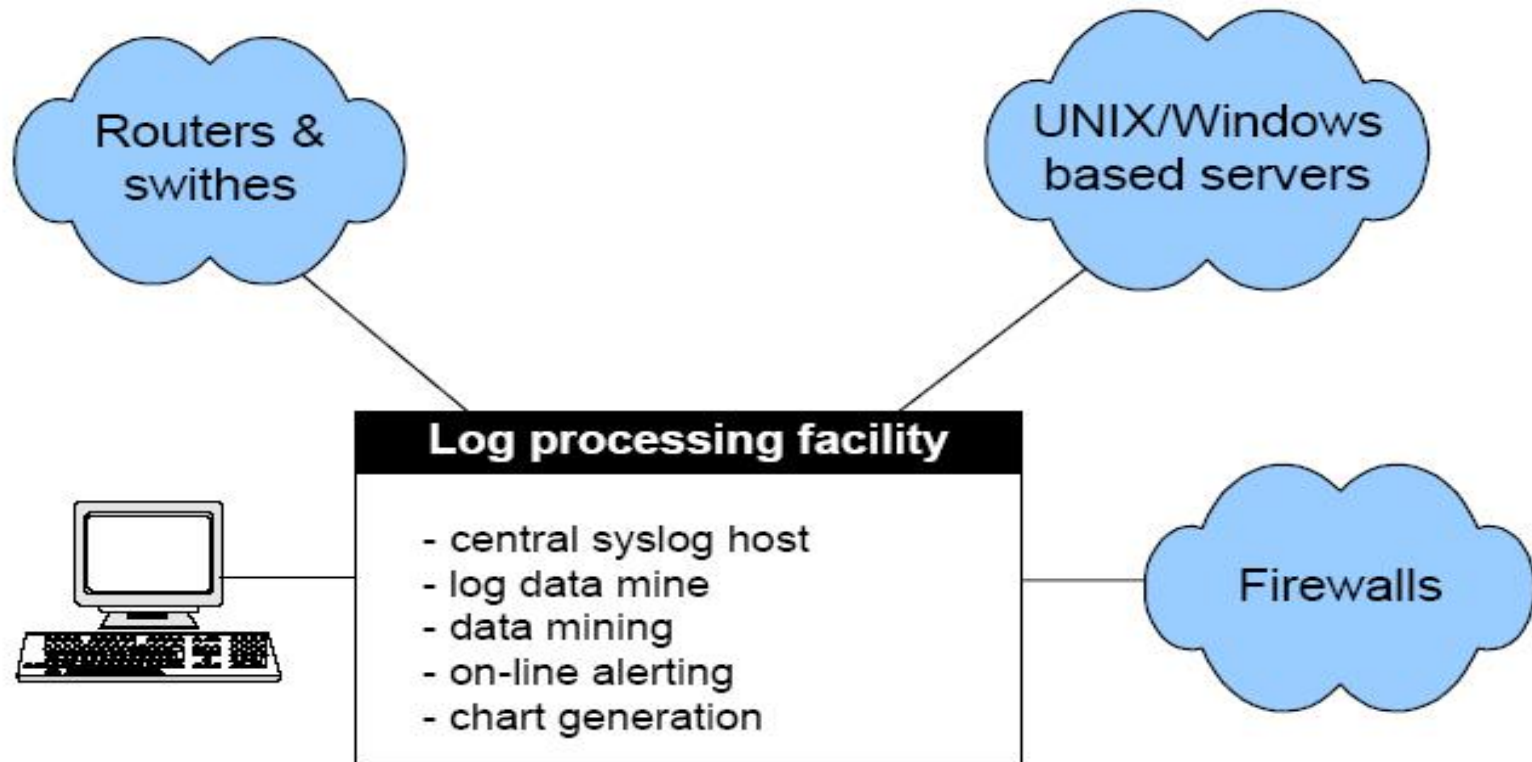
Tripwire

- Install tripwire
 - <http://www.redhat.com/swr/i386/tripwire-2.3.1-17.i386.html>
- Configure tripwire
 - /etc/tripwire/twinstall.sh
 - /etc/tripwire/twpol.txt
- Build database
 - tripwire --init
- Run Integrity check
 - tripwire --check > report.txt

Vulnerability Scanner

- Nessus
- Nikto

Centralized Syslog server



Log levels

LOG_EMERG	A panic condition. This is normally broadcast to all users
LOG_ALERT	A condition that should be corrected immediately, such as a corrupted system database.
LOG_CRIT	Critical conditions, e.g., hard device errors.
LOG_ERR	Error conditions.
LOG_WARNING	Warning messages.
LOG_NOTICE	Normal, but significant Conditions that should possibly be handled specially.
LOG_INFO	Informational messages.
LOG_DEBUG	Debug-level Messages

Log facility

LOG_AUTH	security/authorization messages (DEPRECATED Use LOG_AUTHPRIV instead)
LOG_AUTHPRIV	security/authorization messages (private)
LOG_CRON	clock daemon (cron and at)
LOG_DAEMON	system daemons without separate facility value
LOG_FTP	ftp daemon
LOG_KERN	kernel messages
LOG_LOCAL0 through LOG_LOCAL7	reserved for local use.
LOG_LPR	line printer subsystem
LOG_MAIL	mail subsystem
LOG_NEWS	USENET news subsystem
LOG_SYSLOG	messages generated internally by syslogd
LOG_USER (default)	generic user-level messages
LOG_UUCP	UUCP subsystem

Advantages of centralized syslogging:

- Hacker won't be able to delete logs after breaking into a system.
- The Central syslog can be put on a different segment with higher security.
- Log messages from all machines could allow for better co-relation of attacks on different machines.
- Easier Backup Policy, File permission

Logs: Central log Server

- Default syslogd
 - Server
 - /etc/sysconfig/syslog
 - SYSLOGD_OPTIONS="-m 0 -r -x"
 - Client
 - /etc/syslog.conf
 - *.* @loghost_server

Syslog-NG

The advantages of Syslog-NG over Syslog are :

- ability to transport syslog messages over TCP
- filtering based on message contents
- logging of complete chain of forwarding loghosts (unlike regular syslog which will only record the name of last step)
- support digital signatures and encryption.
- Can be run in a chrooted environment

Syslog-NG

- Configuration component
 - Syslog-ng+MySQL+Apache+php
- Log Analysis
 - Swatch
 - logsurfer

Linux Incident Handling

- Identify Incident Type
 - DOS
 - Unauthorized access
 - Malicious code
 - Combination of any of the above

Incident Handling DOS

- SYN attack
 - monitoring number of TCP Connection in a `syn_rcvd` state.
 - `netstat -an -f |grep SYN_RCVD |wc -l`
- Watch the value of the `TcpHalfOpenDrop` parameter
 - `netstat -s -P | grep tcpHalfOpenDrop`

Incident Handling (contd..)

Preparing toolkit

- shared libraries
- static system libraries
- netstat
- lsof
- gdb / nm
- ps
- ls
- su
- passwd
- netcat
- strace / ltrace
- MD5-generator
- fdisk / cfdisk
- who / finger / w
- dig
- find

Incident Handling (contd..)

Information collection

cat /proc/version	Version of the operating system
cat /proc/sys/kernel/name	Host name
cat /proc/sys/kernel/domainname	Domain name
cat /proc/cpuinfo	Information about hardware
cat /proc/swaps	All swap partitions
cat /proc/partitions	All local file systems
cat /proc/self/mounts	Mounted file systems
cat /proc/uptime	Uptime
cat /proc/modules	List of modules loaded to kernel memory
last, w, who	Get listings of logged in users, prior logins, etc.
Date -u	Current Date
arp -an	Current ARP Cache
Route -Cn	Current routing Table

Incident Handling

- Look for change in permission
 - World writable permissions
 - `find / -perm -2 -type f -print`
 - Find SUID root files
 - `find / -type f -perm -04000 -ls`
 - Find GUID root files
 - `find / -type f -perm -02000 -ls`
 - Time stamp
 - Find files access for last 1 day, 1 hr etc
 - `Find -- atime`
 - `Ls -lautR`

Incident Handling

- Check for promiscuous mode.
 - Ifconfig -a
- Check for new user existence.
 - /etc/passwd
- Find list of open ports
 - nmap scan
 - Netstat -l
- Current processes
 - Ps -aux
- system calls by an executable. (Trojanoid Binaries)
 - ltrace, strace, trussCheck

Incident Handling

- Compare checksum
 - Tripwire --check
- Check for traffic in out
 - Ethereal, tcpdump etc
- Examine suspicious binaries
 - strings

Incident Handling

- Presence of malicious code
 - Chkrootkit
 - Checks for presence of rootkits
 - Tripwire
 - Compare checksum
- The Coroners tool kit
 - Collection of different forensics tollkits

The Coroners tool kit

- TCT is a collection of tools written with the specific goal of gathering or analyzing forensic information on a Un*x machine...
- Four major parts of TCT:
 - grave-robber
 - the C tools (ils, icat, pcat, file, etc.)
 - unrm & lazarus
 - mactime

The Coroners tool kit

grave-robber -v /

- Automated way of collecting forensic info
- Gathers, in order -
 - Memory
 - Unallocated filesystem
 - netstat, route, arp, etc.
 - ps/lsof, capture all process data
 - stat & MD5 on all files, strings on directories
 - Config, log, interesting files (cron, at, etc.)

grave-robber

- data capturing tool at the heart of TCT
- runs various commands and records the output
- captures by order of volatility
- most effectively used when run as root over an entire filesystem

- pcat Process CAT
- ils Inode LS
- icat Inode CAT
- shell commands

Thank You

www.cert-in.org.in