

Securing Linux

Yeak Nai Siew
system consultant, ceo

16 Jan 2006

We Support:



Novell.



fedora^f_{TM}

CentOS

OBJECTIVES

- To share the experience of Linux security and our ways to securing it.
- Outline:
 - About Us
 - Some Experiences
 - Hacker mindset
 - Securing Linux
 - Tools

ABOUT MY DIRECTORY

- Established in 1999 to focus in Internet Solutions and Linux.
- A subsidiary of CCC Holdings Sdn Bhd (a construction company).
- Short name “MD”.
- Major Portfolios:
 - SMJK Dindings
 - AirAsia

ABOUT YEAK NAI SIEW

- Interests in general security stuffs...
- (Assist in) Hacking one major ISP's web site in 1997
- Integrate SecureID, PKI and Password (3-factor authentication for APEC2000
- System hardening on Solaris and Linux

SOME EXPERIENCE



Web site deface

- What
 - Changing the normal web site to something else like “defaced by XXX”.
- How
 - Commonly done via SQL or PHP remote code injection due to bugs in web application.
 - It is carried out by a mass deface tool with opportunistic scan.
- Why
 - Competition among hacker peers.
- Risk
 - High risk to the site owner and its data.
 - Very common.
 - We always have this because we are providing web hosting services to about 200 customers.

Sending junk mails

- What
 - Sending out junk mails or relaying junk mails.
- How
 - Weakness in OS that allow installation of external program as web user or root user by hacker.
- Why
 - Sending junk mail is a business to do!
- Risk
 - High risk and consuming bandwidth.
 - Hard to detect without special attention.
 - Very common, for example, ebay scam

Data lost

- What
 - Hack and destroy the data by wiping out the server.
- How
 - Remotely attack and once gain access, wipe it.
- Why
 - Possible revenge
 - Mostly “by accident”! Work of Amateur Hacker...
 - Hacking tools are easily available.
 - Normally happen when hacker tried to install backdoor programs but screwed up everybody.
- Risk factor
 - High risk
 - Not common

COMMON SYNDROME OF HACKED SERVERS

- Strange startup with lots of errors or failed services.
- Hang when booting up – stuck at starting up services.
- Some command could not perform tasks that you desired: ls, ps, netstat
- Files are locked with “chattr”. Try “lsattr {/bin,/usr/bin,/sbin,/usr/sbin} | less” to check
- Strange folder found in /dev/shm, /tmp, /var/tmp with name “...<space>” and alike.

HACKER MINDSET AND OBJECTIVES

- Was
 - Showing off their skills by leaving their marks.
 - Try to behave as “big brother” who concern about security and warn you to be more alert.
- Now
 - You don't care, do you?
 - So turn into business. Hack your server and sell it underground, or keep it for future use.
- Most hackers are well educated.
 - They are professional, aren't they?
 - They point out problem and they want attention.
 - We should thank them and acknowledge them.

SECURING LINUX

- Scope of security:
 - Server – concerning OS
 - Network – wireless, vlan, hub/switch
 - Application – software bugs
 - User – weak password, chain letter, spyware
- Almost everything has to do with security!
- But our focus: Server

PREVENTION COME FIRST

- Beef up your defenses (firewall, hardening)
- Know your threats (snort)
- Use good security tools (on reporting)
- Backup your data daily and weekly
- Practice to restore from backup
- Keeping the crime scene
- Know a list of who can help you (MYCERT)

KNOWING SOME FACTS



HOW HACKERS FOUND YOUR PROBLEM?

- Spread virus
 - Virus only succeed in hacking servers/workstations that were not patched.
- Spyware with automated probe
 - Users behavior is going to be a major problem.
 - Too many “aunty” “uncle” are now going online without proper “protection”.
 - Their PC affected by spyware and they help hackers to discover you!

WHAT THEY DO WITH YOUR COMPUTER?

- Install rootkits
 - a program that is designed to be hard to find once installed and it opens a backdoor for future entry.
- Sell or trade in underground market
- Hack deeper into your network
- Stealing confidential data by sniffing

OUR SECURITY POLICY



ON PEOPLE

- Differentiate system administrator (SA) and users
- Shell access given to SA only
- Keep /etc/passwd for system use only
- Avoid using /etc/passwd for Applications
- Keep the number of SA low
- SA must have proper training on Linux and System Administration
- SA should be Certified Engineers
- How about "Super Admin"?
 - You may have multiple level of SA and control them by "sudo"

ON SERVER

- Install firewall
- Harden server
- Keep “hot” and “warm” backup of the data
- Install monitoring software to watch logs and do statistic.

SECURING SSH

- What
 - SSH is Secured SHell. It has replaced telnet for remote access.
 - SSH added other good features such as SCP, SFTP, SSH Agent.
- Why
 - Denial of service to SSH is possible.
 - Lots of trial and error with easy password guessing.

SECURING SSH: HOW

- Harden SSHD config.
 - Protocol 2
 - PermitRootLogin no
 - PermitEmptyPassword no
 - Banner /etc/ssh/banner
- Get DenyHosts from <http://denyhosts.sourceforge.net>
 - It watched failed login attempt in /var/log/secure.
 - Jan 9 01:02:00 pepe sshd[24538]: Invalid user fluffy from ::ffff:211.91.163.150
 - Jan 9 01:02:02 pepe sshd[24541]: Invalid user admin from ::ffff:211.91.163.150
 - Then it configures /etc/hosts.deny file to block repeated failure attempts.

USING SHOREWALL

- What
 - Shorewall makes iptables easy!
 - Let you focus on your rules, not other little nifty details.
 - Design like CheckPoint with zones and simple rules.
- Why
 - It is quite difficult to fully understand iptables.
 - You can easily make mistake in iptables.
 - Shorewall let you easily maintain and updates rules in future.

USING SHOREWALL: HOW

- Download from <http://www.shorewall.net>
- Get the latest “production” RPM release.
- Get the contributed “Samples” for one-interface, two-interfaces and three-interfaces for really quick start.
- Read the docs, if you are not familiar.
- Sample easy rules:
 - AllowDNS net fw
 - AllowSSH net:202.71.97.155 fw
 - ACCEPT dmz net tcp smtp,http
 - DNAT net loc:192.168.1.3 tcp ssh,http

USING BASTILLE-LINUX

- What
 - The Bastille Hardening program "locks down" an operating system, proactively configuring the system for increased security and decreasing its susceptibility to compromise. Bastille can also assess a system's current state of hardening, granularly reporting on each of the security settings with which it works.
- Why
 - Quite and easy way to harden the system
 - Easy maintenance in future.
- How
 - Download from <http://www.bastille-linux.org/>
 - We just discovered this 2 weeks ago... currently studying it and will deploy once ready.

USING SELINUX

- What
 - Developed by NSA for Linux community to provide similar things like Trusted Solaris. It runs at kernel level.
 - It added extra 3 modes of security control besides standard User, Group, Read, Write, Execute.
 - It is quite new. Only introduced commercially in Red Hat Enterprise Linux version 4.
- Why
 - Standard Linux security is not comprehensive enough.
 - “root” is too powerful. SELinux will make root like an ordinary user.

USING SELINUX: HOW

- Use Red Hat Enterprise Linux 4 or Fedora Core 4 or CentOS 4.
- Read about SE-Linux guide:
 - <http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/selinux-guide/>
- Quick config and exploration:
 - Edit `/etc/sysconfig/selinux` to enable it. Reboot to take effect.
 - Watch selinux violation and check problem: `“dmesg | grep avc”`.
 - Understand and fix each violation.
 - Configure SE-Linux:
 - `ls -Z`
 - `ps axwf -Z`
 - `chcon`

USING VPN

- What
 - VPN let you login to your office virtually as if you are in office. Thus you can access to office's resources (depending on your firewall rules)
 - There is net-to-net and net-to-roadwarrior VPN.
- Why
 - While SSH remote management is secure, but we may limit it to come from certain fixed hosts.
 - Using VPN let us switch to the trusted network and start to work as usual.
- How
 - Setting up VPN on Linux is not discussed here!
 - We recommend it to be setup on separate box or router.
 - Look at:
 - Monowall – <http://www.m0n0.ch>
 - Linux PPTPd – <http://www.poptop.org>

KEEPING SYSTEM UP-TO-DATE

- What
 - Update your OS and program to the latest copy usually fix the security problem.
- Why
 - There is no “suddenly-everyone-at-risk” kind of event (yet).
 - Most problem are first discussed/reported to bugtraq and alert come CAN or MYCERT...
 - The fix for Open Source Software can come out in hours as opposed to days for commercial.
 - Program like Virus and Spyware make use of known exploits and attack unpatched system.
- How
 - Use supported Linux distribution and rely on their expertise to fix the problem with updates.

ON DATA

- The only things that is precious to you is Your Data!
- Repeat: The only things that is precious to you is Your Data!
- Backup to disk or to tape drive?
 - Disk: fast, cheap, SAN over iSCSI
 - Tape: still quite expensive and limited storage
- Confusion over "RAID-1" mirroring
 - RAID-1 is for system redundancy, not data backup.
- We have our way of doing data backup.

DAILY BACKUP

- What
 - Keep a copy of day-to-day data.
 - Usually is incremental backup.
- Why
 - To reduce the amount of data lost.
- How
 - We only select those data we want to keep daily, i.e. web, email, db, important configuration.
 - We keep for 3 to 7 days or copies

backup-daily.sh

```
#!/bin/sh

# This backup script should be run daily.

# number of backup?
BACKUP=4

export PATH=/usr/bin:/bin:/sbin:/usr/sbin

TIMENOW=`date +%s`
NUM=`echo $((($TIMENOW/86400*$BACKUP))`

# Define where you want to backup.
DEST=/net/nas/backup/pepe/DAILY

# Check for NFS mount to ensure we got the mount point
ls /net/nas/backup > /dev/null 2>&1
if [ ! -d $DEST ]; then
    echo "Directory not found: $DEST"
    exit 1
fi

function copythis () {
    RSOPTS="-ax --numeric-ids --delete-excluded --bwlimit=30000"
    FROM="$1"
    shift
    TO="$1"
    shift
    XOPTS="$*"
    echo $FROM to $TO
    rsync $RSOPTS $XOPTS $FROM $TO
}

function dbdump () {
    TABLE="$1"
    DBUSER="root"
    DBPASSWD="SECRET"
    mysqldump -u$DBUSER -p$DBPASSWD -q -S /var/lib/mysql/mysql.sock $TABLE | \
        bzip2 - > $DEST/mysql/$TABLE.sql.$NUM.bz2
}

copythis /etc $DEST/

# backup mysql databases

umask 077
dbdump cerberus
dbdump dotproject
dbdump intranet
dbdump mysql
dbdump phpmyadmin
dbdump wikidb
```

WEEKLY BACKUP

- What
 - Keep a copy of full data backup.
- Why
 - To have a complete backup of the system on another partition so that recovery is fast.
- How
 - Do full backup by filesystem
 - One copy only.
 - See “note” on our script.

backup-weekly.sh

```
#!/bin/sh

# This backup script should be run weekly.

export PATH=/usr/bin:/bin:/sbin:/usr/sbin

# Define where you want to backup.
DEST=/net/nas/backup/pepe

# Check for NFS mount to ensure we got the mount point
ls /net/nas/backup > /dev/null 2>&1
if [ ! -d $DEST ]; then
    echo "Directory not found: $DEST"
    exit 1
fi

function copythis () {
    RSOPTS="-ax --delete --numeric-ids --delete-excluded --bwlimit=30000"
    FROM="$1"
    shift
    TO="$1"
    shift
    XOPTS="$*"
    echo $FROM to $TO
    rsync $RSOPTS $XOPTS $FROM $TO
}

copythis /home/bb $DEST/home/
copythis /root $DEST/
copythis /var/lib/mysql $DEST/
copythis /var/named $DEST/
copythis /var/www $DEST/
copythis /etc $DEST/
```

REMOTE BACKUP

- What
 - Keep a copy of weekly data in a remote server.
- Why
 - To allow us to restore the service quickly.
 - Used for Disaster Recovery.
- How
 - Write a script to do this task automatically.
 - (email me to request for the script)

SECURITY MONITORING

- It is almost impossible to monitoring all traffics or data.
- We need automated software that produce statistics and reports for:
 - Usage – whether your system is operating correctly.
 - Problem – why your system fail to grant Usage.

MAKING USE OF LOGWATCH

- What
 - Logwatch read and parse your log files and find out interesting problem and email you daily as a report.
 - It is enable by default in Red Hat Enterprise Linux.
- Why
 - Time is short, we need reports that make sense.
- How
 - Configure `/etc/log.d/logwatch.conf` to specify the email to send the report to.
 - Read `/usr/share/doc/logwatch-*/` to learn about how to create your own log analyzer.

MAKING USE OF RPM

- What
 - RPM is a package management tool that keep track of everything that it is installed in your system.
 - “Everything?” Yes, “Everything!”.
- Why
 - To allow you to identify what you installed in your system – check the installation date, pre and post install script, changelog, original file status and so on.
- How
 - One security feature of RPM is that it keep track of your installed files with a md5 checksum.
 - Any change to the file/folder will be indicated when you type “rpm -Va” or “rpm -Vf /path/to/file”.

MAKING USE OF TRIPWIRE

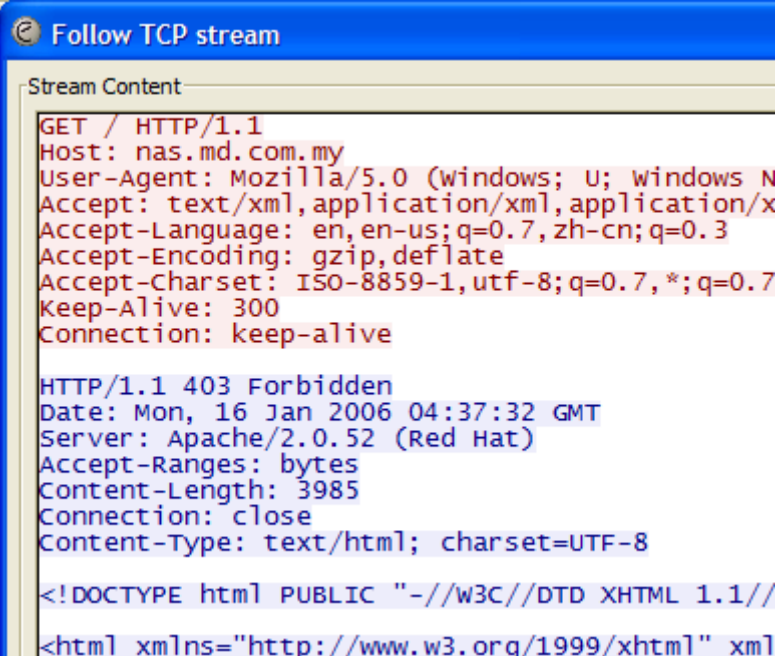
- What
 - Tripwire can tell you any specific file that you want to monitor had changed. It is on-going basis.
- Why
 - The tripwire database can be updated whenever needed with the current changes and start to compare from that point onward.
 - It is particular useful for a web server that you allow many users to login with shell access.
- How
 - Download from <http://tripwire.sourceforge.net/>

MAKING USE OF SNORT

- What
 - Snort is known as Intrusion Detection Software. It sniffs the network packet to find interesting things and do reporting.
 - Snort_inline can do Prevention as well.
- Why
 - It is extremely popular among network integrators to provide network layer security system.
- How
 - Not really describe here...
 - Please visit <http://www.snort.org/>
 - Download RPMS from <http://dag.wieers.com/packages/snort/>

BE A CASUAL HACKER

- Seeing is believing!
- You can setup your notebook that run Windows XP with 2 NICs, bridge the interfaces, and run Ethereal.
- Get ethereal:
<http://www.ethereal.com/>
- We often use this technique to locate computers affected by virus that jammed our Internet access.



```
Follow TCP stream
Stream Content
GET / HTTP/1.1
Host: nas.md.com.my
User-Agent: Mozilla/5.0 (windows; U; windows N
Accept: text/xml,application/xml,application/x
Accept-Language: en,en-us;q=0.7,zh-cn;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive

HTTP/1.1 403 Forbidden
Date: Mon, 16 Jan 2006 04:37:32 GMT
Server: Apache/2.0.52 (Red Hat)
Accept-Ranges: bytes
Content-Length: 3985
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//
<html xmlns="http://www.w3.org/1999/xhtml" xml
```

THANK YOU

Questions & Answers