Operating System Hardening Guide

Host Configuration

HUBzero software needs to be installed on a secured base: hardened OS and services. The following is a description of most of what we do at Purdue to harden the HUBs we manage.

- Software updates. Debian 6 will have security updates until May 2014. Look for patches and apply them daily:

  ```
  aptitude update;  aptitude upgrade
  ```

  Check for failed or incomplete package updates in a cron job running daily. We once have had a compromise due to a failed package security update which would have been detected by this check. Since then we've run it every day:

  ```
  dpkg --audit
  ```

  Check for any deviations from packages in a cron job running at least weekly:

  ```
  debsums | grep FAILED
  ```

  Make sure that the HUBzero repository is configured as a source of updates. Our updates also modify and fix issues with Joomla! itself. We provide support for Joomla! 1.5 through this repository. Even though it was EOL by the original authors, we effectively forked it and are maintaining it until the next HUBzero release.
- Configure Apache with the suhosin application firewall (package php5-suhosin), or mod-security. An application firewall is to PHP and the HUBzero CMS what a network firewall is to an operating system. They can block attacks targetting an existing code vulnerability, even if only the attacker is aware of the vulnerability. They can also limit or mitigate abuse. Suhosin is known to have protected against so-called "0-day" attacks. In addition, log messages from suhosin can be used as a basis for a fail2ban jail (see fail2ban paragraph)
- Configure Apache with mod-spamhaus (package libapache2-mod-spamhaus). The Spamhaus organization is very effective in finding IP addresses used for spamming. Blocking those from submitting content to the web site, while still allowing affected users to browse, will decrease spam questions and other forms of spam. In addition, it alerts users effectively that their machine is likely compromised. This is the message we show when someone is blocked:

  ```
   Access Denied! Your address is blacklisted. It could be because
  your computer is infected and participates in a spam botnet. If y
  ou're using a shared access point (e.g., wireless), it's possible
   that the IP address of that access point has been banned because
   someone else's computer is infected.  You can find the IP addres
  s of that device by going to http://whatismyipaddress.com/ .  You
  ```

```
 can find the reason for blacklisting the address by going to htt
p://www.spamhaus.org/lookup/  You will regain full access after c
orrecting the situation and removing the IP address from the blac
klist.
```

Note that commercial users need to obtain a datafeed from Spamhaus.

- Configure Apache to redirect all plain HTTP connections to HTTPS. This will mitigate issues such as pages presenting mixed HTTP and HTTPS content, or accepting plain HTTP connections to areas that require a login.
- Install Dshield's blocklist in the firewall iptables. dshield.org's blacklist is available at:

  ```
  http://dshield.org/block.txt
  ```

  and the signature used to verify its integrity is at:

  ```
  http://dshield.org/block.txt.asc
  ```

- Install spamassassin and tune it.
- Install an antivirus like ClamAV and make sure that HUBzero is configured to use it to scan all uploads on the fly. Use the EICAR test file to verify that it is operating properly:

  ```
  http://www.eicar.org/86-0-Intended-use.html
  ```

  and keep a copy on the web site. Scan the entire web site with ClamAV at least weekly. Make sure the "fresh-clam" daemon is running all the time and restart it as necessary (we do it every day to make sure) to get the most up-to-date malware definitions.
- Install fail2ban and configure it with jails for WebDAV, SSH, Apache errors, Apache suhosin messages, HUBzero CMS logins (in /var/log/hubzero/cmsauth.log), exim4, and spamassassin logs. We permanently ban anyone trying to login as root and some other key accounts. SSH is configured to deny root logins with passwords, but we let them try anyway so we can better ban attackers.
- Run a configuration management software that will automatically detect and report any unauthorized configuration changes. We run something called "Ogre" every hour. The Ogre core engine itself is open-source, but it needs meta-data and file templates to be useful. Those are not open-source at this time.
- Configure file system permissions such that the Apache user (www-data) can't modify the HUBzero and Joomla! code directories, by setting ownership to a different user. We're currently testing and deploying this.
- Run the auditing tool "Lynis" (package "lynis") and obtain a hardening score of at least 72.
- Run "rkhunter" at least every day to detect suspicious changes.
- Add firewall rules to block IPv6 on all interfaces but local, unless you also deploy an IPv6 equivalent for fail2ban and dshield. Due to the large address space of IPv6 and its privacy extension, blocking individual IPs is pointless. Any blocking tool worth using must have the capability to block networks. Blocking networks may also block innocent users, so it is important that the tool scales the size of the block, from individual IPs to

large networks, depending on the number of failures. We do not accept IPv6 traffic due to this connundrum; blocking misbehaving IP addresses is too useful a security measure to consider offering service without that capability. Tools that offer IPv6 address blocking capabilities all seem to be attempting to block individual IPs or fixed network sizes at this time; we believe that they are not useful.
- Consider recommendations from the PHP auditor to change php.ini settings. It's very easy to install, but some recommendations aren't practical and are incompatible with HUBzero functionality. You can get it, and see screenshots, from https://www.idontplaydarts.com/2011/02/hardening-and-securing-php-on-linux/

External Hardening Tools

- Run network-based vulnerability scans periodically. Note that Debian doesn't increase the version numbers in banners when applying security patches. This makes it very difficult to draw any conclusions from a vulnerability scanning engine like Nessus, using default settings. Most results are false positives. However, the scan can be useful to detect new open ports and some configuration issues.
- Make sure that the site is rated "A" by the Qualys SSL Labs server test at:

  `https://www.ssllabs.com/ssltest/index.html`