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 what little Joomla! code remains in HUBzero software. At some point there will be no Joolma! code being run at all.
- 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://feeds.dshield.org/block.txt
  ```

  and the signature used to verify its integrity is at:

  ```
  http://feeds.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 configuration management software. It should automatically detect and report any unauthorized configuration changes. Ansible is a popular one. We also 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.
- IPv6 support is becoming more and more necessary, but IP blocking, effective with IPv4, is less so with IPv6. Due to the large address space of IPv6 and its privacy extension, blocking individual IPs not very effective and other methods must be given more weight. Make sure to configure the CMS options on the number of allowed password login attempts, and at which point accounts presumably under attack should be disabled. However, this exposes accounts to "prank blocking" by someone purposefully failing login attempts for someone else's account. Allowing other login methods than passwords may mitigate this; HUBzero supports many other authentication mechanisms. If you deploy IPv6, password login limits may need to be tightened.
- We are in the process of developing Content Security Policies so web browsers can participate in securing Hub usage; however they are not mature at this time.

External Hardening Tools

- Run network-based vulnerability scans periodically. Note that Debian doesn't increase the version numbers that software uses to identify itself, when applying security patches. This makes it 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`