

Computer Security

The integrity of your server is an ongoing challenge, and as hackers evolve, you will also have to do your best to stay on top of the latest methods for keeping hackers at bay. By following some of the steps below you will set yourself on the right path to shutting down some of the simpler ways for hackers to get into your system. If you make it difficult enough to get in, they will hopefully move on to an easier target.

MAINTAIN ACCESS LISTS (users and groups)

One key job of a system administrator is maintaining the list of people who may access the system. Your machine is pre-configured with several system accounts that are locked or disabled by default. These system accounts do not require additional maintenance.

Accounts may be created by the administrator over time that have served their purpose and are no longer required. It is recommended to remove, or at least disable, accounts that will not be used in the short term. A disabled account can always be re-enabled when required.

Commands are as follows:

passwd -l username: Locks the password for a user's account

passwd -u username: Unlocks the password for a user's account

userdel username: Removes the user's account from the system

APPLICATION SECURITY

Many database-driven Content Management Systems (CMS) such as PHPBB, PostNuke, WordPress, Mambo, Joomla, and others recommend or require additional access to areas of your system's hard drive to store content, images, or even scripts. These applications, even when patched, may have undiscovered security issues that open these areas to intruders.

Rather than revoking your users' permissions outright and constantly policing their applications, you may consider purchasing a separate system for blogging use or even offer managed blog accounts. If you control the application you can upgrade it for your customers on a moment's notice when a new vulnerability is discovered.

The command '**find / -perm +2**' will find any files or directories designated as world-writable. The command '**find / -user apache**' will find files and directories created by web applications that may be considered world-writable as well. You can expect to find system directories such as /tmp, /var/tmp, and /dev/shm with world-writable permissions by default. Permissions in Linux may be set using the '**chmod**' command or through FTP. Several descriptions may be found online by searching Google for "unix permissions".

TRACK SUID/SGID SOFTWARE

Minor errors in SUID-root programs (files owned by root with the Set User ID execution-bit set) can possibly lead to root compromise of your system. Intruders are known to leverage existing bugs to gain additional privileges leading to further damage. Unfortunately some software requires SUID-root privileges to operate.

You can find SUID/SGID files with the command '**find / -type f -perm +06000**'. Files in /bin, /sbin, or /usr are normal; be suspicious of files within a world-writable location though. SUID-root files in

unexpected places almost always indicate a system compromise. Know what and where your SUID files are so you can at least compare a listing of them on a regular basis.

(ADVANCED) KERNEL SECURITY

Red Hat Enterprise Linux Enterprise Server 4 (RHEL ES 4) includes features donated by the U.S. National Security Agency (NSA) called "Security Enhanced (SE) Linux". SE Linux adds mandatory application security mechanisms to Linux that prevents software from operating outside of its normal parameters. A high-level description and documentation may be found at <http://www.nsa.gov/selinux>.

Without appropriate security policies, SE Linux will prevent many applications from running. For this reason we set 'SELINUX=disabled' on all PEER 1 Dedicated Hosting servers by default. If you would like to experiment with SE Linux, we recommend using a test server and setting the option to "permissive" in /etc/selinux/config so that it will only warn about errors. You will need to read the documentation on the NSA's website on how to set the appropriate policies and security contexts for your applications.

MONITOR APPLICATION AND SYSTEM LOGS

Administrators usually read logs in response to an incident and ignore them in-between. In fact, the amount of information can often be too much to deal with and isn't usually in a usable form. Enabling SE Linux will only increase the amount of logs you must go through daily.

Intrusion attempts may be logged hours, days, or even weeks in advance. One example is the brute-force attempts against the Secure Shell (SSH) service: "sshd: Failed login from user 'test'". If you've removed or disabled your test accounts you may be safe; if you're thinking about that account just now...

Red Hat includes a utility called "logwatch" that does some simple log processing. All you need to do is give it an email address in the form "MailTo = user@host" (cat "/etc/logwatch/conf/logwatch.conf" for more information). Once it's been configured you should expect an email every morning.

Splunk (<http://www.splunk.com>) offers a free log processing server that can process up to 500 megabytes of logs per day. Please see their website for more information.

THE CONCLUSION

While there are many things you may consider to increase the security of your system, please remember that you are an integral component. By staying on top of your system's security, taking the precautions mentioned above, being alert to new intrusion methods and the availability of new patches, you should be well on your way to maintaining a relatively secure system.