2.2 More Linux Security

> This article is just starting.
>
> Some topics,
>
> Email Login Events
>
> - Alert me when a sudo capable account logs in.
> - Alert me when serveradmin logs in.
> - Alert me when accounts fail sudo attempts.
>
> Integrity Check
>
> - Possibly using tripwire.
>
> File Permissions - World Writable
>
> - Possibly using to report tripwire on.

Email Login Events

On servers that are managed by only a few administrators it is often useful to know if someone has logged in.

On more larger system it is more manageable to only send notification when sudo access is attempted.

> This script can be improved,
>
> - add descriptive info to the header
> - use a code for level
> - have option to alert only for sudo enabled account
> - have option to alert only for specific group(s)

First ensure your system is setup to send emails.

Here is the start of the contents of the login notification script,

sentry-login.sh

Until the script is done simply add the email line to the end of the the global startup scripts **/etc/profile**,

```
... more stuff up here ...
umask 022

echo "User $LOGNAME logged into $HOSTNAME on $(date)" | mail
-aFrom:sentry@bonsaiframework.com -s "Sentry Alert Login
$LOGNAME@$HOSTNAME" bhitch@imagecomics.com
```

Now every login will result in an alert.

Email Sudo Events

On small systems, you will want to be emailed sudo events.

Failed Sudo Logins

Actually send an email on failed login...

Login

Email alert upon the first sudo command...

File Integrity Check

Verify that files are not modified without your knowledge...

Securing Passwd

...