**Securing a LAMP server**

**LINUX**

1. Update the machine
   1. *apt-get update*
   2. *apt-get upgrade*
   3. *apt-get dist-upgrade*
2. Install clamtk
   1. *apt-get install clamtk*
   2. Run the scan
      1. *freshclam*
3. Set automatic Updates
   1. System settings>software & updates>Updates
      1. *Automatically check for updates*
      2. *Important security updates*
4. Search for all prohibited files
   1. *find / -name “\*.{extension}” –type f*
5. Configure the firewall
   1. *apt-get install ufw / yum install ufw*
   2. *ufw enable*
   3. *ufw status*
6. Edit the lightdm.conf file
   1. Ubuntu
      1. Edit */etc/lightdm/lightdm.conf or /usr/share/lightdm/lightdm.conf/50-ubuntu.conf*
      2. *allow-guest=false*
      3. *greeter0hide-users=true*
      4. *greeter-show-manual-login=true*
      5. *autologin-user=none*
   2. Debian
      1. Edit */etc/lightdm/lightdm.conf* 
         1. *Greeter-hide-users=true*
         2. *Greeter-allow-guest=false*
         3. *Greeter-show-manual-login=true*
         4. *Allow-guest=false*
         5. *Autologin-user=none*
      2. Edit */etc/gdm3/greeter.dconf-defaults*
         1. *Disable-user-list=true*
         2. *Disable-restart-buttons=true*
         3. *AutomaticLoginEnable = false*
7. Create any missing users
   1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
8. Change all the user passwords to “Cyb3rPatr!0t$”
9. Edit the */etc/login.defs*
   1. *FAILLOG\_ENAB YES*
   2. *LOG\_UNKFAIL\_ENAB YES*
   3. *SYSLOG\_SU\_ENAB YES*
   4. *SYSLOG\_SG\_ENAB YES*
   5. *PASS\_MAX\_DAYS 90*
   6. *PASS\_MIN\_DAYS 10*
   7. *PASS\_WARN\_AGE 7*
      1. Add the following to the line that ends in difok=3 to /etc/pam.d/common-password
      2. *ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1*
10. Delete any users
    1. *\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_*
    2. *\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_*
    3. *\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_*
11. Check the /etc/passwd file
    1. Look for any repeating UID or GID
    2. Make sure no programs have *a /bin/sh or /bin/bash*
    3. Only root should have a UID and GID of 0
12. Check the */etc/group* file and manage the groups
    1. Add all the admins to the *sudo* and *adm* group.
13. Disable the root accounts
    1. *passwd –l root*
14. secure SSH if required
    1. *edit /etc/ssh/sshd\_config*
       1. *LoginGraceTime 60*
       2. *PermitRootLogin no*
       3. *Protocol 2*
       4. *PermitEmptyPasswords no*
       5. *PasswordAuthentication yes*
       6. *X11Fowarding no*
       7. *UsePAM yes*
       8. *UsePrivilegeSeparation yes*
15. Secure the */etc/shadow* file
    1. *chmod 640 /etc/shadow*
16. Look for any bad programs
    1. *dpkg –l | grep {PACKAGE}*
       1. *John The Ripper (JTR)*
       2. *Hydra*
       3. *Nginx*
       4. *Samba*
       5. *Bind9*
       6. *Vsftpd/ftp*
          1. If required then secure the */etc/vsftpd.conf*
             1. *anonymous\_enable=ON*
             2. *local\_enable=YES*
             3. *write\_enable=YES*
             4. *chroot\_local\_user=YES*
       7. *Tftpd*
       8. *X11vnc/tightvncserver*
       9. *Snmp*
       10. *Nfs*
       11. *Sendmail/postfix*
       12. *Xinetd*
17. *Configure /etc/sysctl.conf*
    1. *Sysctl -p*
    2. Add this to the bottom of the */etc/sysctl.conf file*
       1. Disable ICMP redirects
          1. *net.ipv4.conf.all.accept\_redirects = 0*
       2. Disable IP redirecting
          1. *net.ipv4.ip\_forward = 0*
          2. *net.ipv4.conf.all.send\_redirects = 0*
          3. *net.ipv4.conf.default.send\_redirects = 0*
       3. Disable IP spoofing
          1. *net.ipv4.conf.all.rp\_filter=1*
       4. Disable IP source routing
          1. *net.ipv4.conf.all.accept\_source\_route=0*
       5. SYN Flood Protection
          1. *net.ipv4.tcp\_max\_syn\_backlog = 2048*
          2. *net.ipv4.tcp\_synack\_retries = 2*
          3. *net.ipv4.tcp\_syn\_retries = 5*
          4. *net.ipv4.tcp\_syncookies = 1*
       6. Disable IPV6
          1. *net.ipv6.conf.all.disable\_ipv6 = 1*
          2. *net.ipv6.conf.default.disable\_ipv6*
          3. *net.ipv6.conf.lo.disable\_ipv6*
18. Check cronjobs
    1. Check these folders
       1. */etc/cron.\**
       2. */etc/crontab*
       3. */var/spool/cron/crontabs*
    2. Check the init files
       1. */etc/init*
       2. */etc/init.d*
    3. Check for each user
       1. *crontab –u {USER} -l*
19. Check sudoers
    1. When using the *sudo su* command it should always ask for a password, if not
       1. Check */etc/sudoers*
       2. Or */etc/sudoers.d*
    2. Make sure that there are no *NOPASSWD* values set
       1. Change all of them to *ALL=(ALL:ALL) ALL*

*20. Check the runlevels if unable to boot into GUI*

* + - 1. To check the run level
         1. *runlevel*
      2. Runlevels
         1. *0-System halt;No activity*
         2. *1-Single user*
         3. *2-Multi-user, no filesystem*
         4. *3-Multi-user, commandline only*
         5. *4-user defineable*
         6. *5-multi-users,GUI*
         7. *6-Reboot*
      3. *To change the run level* 
         1. *Telinit {level}*

**APACHE**

1. Hide Apache Version number.
   1. Add the following lines to the bottom of /etc/apache2/apache2.conf
      1. *ServerSignature Off*
      2. *ServerTokens Prod*
2. Make sure Apache is running under its own user account and group.
   1. Add a separate user “apache”
   2. Edit the /etc/apache2/apache2.conf file
      1. *User apache*
      2. *Group apache*
3. Ensure that file outside the web root directory are not accessed. /etc/apache2/apache2.conf
   1. *<Directory />*

*Order Deny,Allow*

*Dent from all*

*Options -Indexes*

*AllowOverride None*

*</Directory>*

*<Directory /html>*

*Order Allow,Deny*

*Allow from all*

*</Directory>*

1. Turn off directory browsing, Follow symbolic links and CGI execution
   1. Add *Options None* to a *<Directory /html>* tag
2. Install modsecurity
   1. *apt-get install mod\_security*
   2. *service httpd restart*
3. Lower the Timeout value in */etc/apache2/apache2.conf*
   1. *Timeout 45*

**MySQL**

1. Restrict remote MySQL access
   1. Edit */etc/mysql/my.cnf*
      1. *Bind-address=127.0.0.1*
2. Disable use of LOCAL INFILE
   1. Edit */etc/mysql/my.cnf*
      1. *[mysqld]*
      2. *local-infile=0*
3. Create Application Specific user
   1. *root@Ubuntu:~# mysql –u root –p*
   2. *mysql> CREATE USER ‘myusr’@’localhost’ IDENTIFIED BY ‘password’;*
   3. *mysql> GRANT SELECT,INSERT,UPDATE,DELETE ON mydb.\* TO ‘myusr’@’localhost’ IDENTIFIED BY ‘password’;*
   4. *mysql> FLUSH PRIVILEGES;*
4. Improve Security with *mysql\_secure-installation*
   1. *root@Ubuntu:~# mysql\_secure\_installation*
      1. *change the root password?: y*
      2. *Remove anonymous users?: y*
      3. *Disallow root login remotely?: y*
      4. *Remove test database and access to it?: y*
      5. *Reload privilege tables now?: y*

**PHP**

1. Restrict PHP Information Leakage
   1. Edit */etc/php5/apaceh2/php.ini*
      1. *expose\_php = off*
2. Disable Remote Code Execution
   1. Edit */etc/php5/apache2/php.ini*
      1. *allow\_url\_fopen=Off*
      2. *allow\_url\_include=Off*
3. Disable dangerous PHP Functions
   1. Edit */etc/php5/apache2/php.ini*
      1. *disable\_functions=exec,shell\_exec,passthru,system,popen,curl\_exec,curl\_multi\_exec,parse\_ini\_file,show\_source,proc\_open,pcntl\_exec*
4. Enable Limits in PHP
   1. Edit */etc/php5/apache2/php.ini*
      1. *upload\_max\_filesize = 2M*
      2. *max\_execution\_time = 30*
      3. *max\_input\_time = 60*