



# MDC

## CyberPatriot Categorized Checklist

Team Number \_\_\_\_\_

Round # \_\_\_\_ Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

Operating System \_\_\_\_\_

### Securing a LAMP server

#### LINUX

1. Update the machine
  - a. `apt-get update`
  - b. `apt-get upgrade`
  - c. `apt-get dist-upgrade`
2. Install clamtk
  - a. `apt-get install clamtk`
  - b. Run the scan
    - i. `freshclam`
3. Set automatic Updates
  - a. System settings>software & updates>Updates
    - i. Automatically check for updates
    - ii. Important security updates
4. Search for all prohibited files
  - a. `find / -name "*.{extension}" -type f`
5. Configure the firewall
  - a. `apt-get install ufw / yum install ufw`
  - b. `ufw enable`
  - c. `ufw status`
6. Edit the lightdm.conf file
  - a. Ubuntu
    - i. Edit `/etc/lightdm/lightdm.conf` or `/usr/share/lightdm/lightdm.conf/50-ubuntu.conf`
    - ii. `allow-guest=false`
    - iii. `greeter-hide-users=true`
    - iv. `greeter-show-manual-login=true`
    - v. `autologin-user=none`
  - b. Debian
    - i. 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`
    - ii. Edit `/etc/gdm3/greeter.dconf-defaults`
      1. `Disable-user-list=true`
      2. `Disable-restart-buttons=true`
      3. `AutomaticLoginEnable = false`
7. Create any missing users
  - a. \_\_\_\_\_
  - b. \_\_\_\_\_
8. Change all the user passwords to "Cyb3rPatr!0t\$"
9. Edit the `/etc/login.defs`
  - a. `FAILLOG_ENAB YES`
  - b. `LOG_UNKFAIL_ENAB YES`
  - c. `SYSLOG_SU_ENAB YES`
  - d. `SYSLOG_SG_ENAB YES`
  - e. `PASS_MAX_DAYS 90`
  - f. `PASS_MIN_DAYS 10`
  - g. `PASS_WARN_AGE 7`
    - i. Add the following to the line that ends in difok=3 to `/etc/pam.d/common-password`
    - ii. `ucred=-1 lcredit=-1 dcredit=-1 ocredit=-1`



# MDC

Team Number \_\_\_\_\_

Round # \_\_\_\_ Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

Operating System \_\_\_\_\_

## CyberPatriot Categorized Checklist

10. Delete any users

- a. \_\_\_\_\_
- b. \_\_\_\_\_
- c. \_\_\_\_\_

11. Check the /etc/passwd file

- a. Look for any repeating UID or GID
- b. Make sure no programs have a /bin/sh or /bin/bash
- c. Only root should have a UID and GID of 0

12. Check the /etc/group file and manage the groups

- a. Add all the admins to the sudo and adm group.

13. Disable the root accounts

- a. *passwd -l root*

14. secure SSH if required

- a. *edit /etc/ssh/sshd\_config*
  - i. *LoginGraceTime 60*
  - ii. *PermitRootLogin no*
  - iii. *Protocol 2*
  - iv. *PermitEmptyPasswords no*
  - v. *PasswordAuthentication yes*
  - vi. *X11Forwarding no*
  - vii. *UsePAM yes*
  - viii. *UsePrivilegeSeparation yes*

15. Secure the /etc/shadow file

- a. *chmod 640 /etc/shadow*

16. Look for any bad programs

- a. *dpkg -l | grep {PACKAGE}*
  - i. *John The Ripper (JTR)*
  - ii. *Hydra*
  - iii. *Nginx*
  - iv. *Samba*
  - v. *Bind9*
  - vi. *Vsftpd/ftp*
    - 1. If required then secure the /etc/vsftpd.conf
      - a. *anonymous\_enable=ON*
      - b. *local\_enable=YES*
      - c. *write\_enable=YES*
      - d. *chroot\_local\_user=YES*
    - vii. *Tftpd*
    - viii. *X11vnc/tightvncserver*
    - ix. *Snmp*
    - x. *Nfs*
    - xi. *Sendmail/postfix*
    - xii. *Xinetd*

17. Configure /etc/.conf

- a. *Sysctl -p*
- b. Add this to the bottom of the /etc/sysctl.conf file
  - i. Disable ICMP redirects
    - 1. *net.ipv4.conf.all.accept\_redirects = 0*
  - ii. 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*
  - iii. Disable IP spoofing



# MDC

Team Number \_\_\_\_\_

Round # \_\_\_\_ Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

Operating System \_\_\_\_\_

## CyberPatriot Categorized Checklist

1. *net.ipv4.conf.all.rp\_filter=1*
- iv. Disable IP source routing
  1. *net.ipv4.conf.all.accept\_source\_route=0*
- v. 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*
- vi. 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

- a. Check these folders
  - i. */etc/cron.\**
  - ii. */etc/crontab*
  - iii. */var/spool/cron/crontabs*
- b. Check the init files
  - i. */etc/init*
  - ii. */etc/init.d*
- c. Check for each user
  - i. *crontab -u {USER} -l*

19. Check sudoers

- a. When using the *sudo su* command it should always ask for a password, if not
  - i. Check */etc/sudoers*
  - ii. Or */etc/sudoers.d*
- b. Make sure that there are no *NOPASSWD* values set
  - i. Change all of them to *ALL=(ALL:ALL) ALL*

20. Check the runlevels if unable to boot into GUI

- a. To check the run level
  - i. *runlevel*
- b. Runlevels
  - i. *0-System halt;No activity*
  - ii. *1-Single user*
  - iii. *2-Multi-user, no filesystem*
  - iv. *3-Multi-user, commandline only*
  - v. *4-user definable*
  - vi. *5-multi-users, GUI*
  - vii. *6-Reboot*
- c. To change the run level
  - i. *Telinit {level}*

### APACHE

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



# MDC

Team Number \_\_\_\_\_

Round # \_\_\_\_ Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

Operating System \_\_\_\_\_

## CyberPatriot Categorized Checklist

```
Order Deny,Allow  
Deny from all  
Options -Indexes  
AllowOverride None  
</Directory>  
<Directory /html>  
Order Allow,Deny  
Allow from all  
</Directory>
```

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

### MySQL

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

### PHP

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



# MDC

Team Number \_\_\_\_\_

Round # \_\_\_\_ Date: \_\_\_ / \_\_\_ / \_\_\_

Operating System \_\_\_\_\_

## CyberPatriot Categorized Checklist

---