CyberPatriot Round 3 Linux Checklist (AMP Stack Edition)

1. USERS & PASSWORDS

- deluser
- passwd
- usermod -s /bin/bash

Check: /etc/passwd, /etc/group, /etc/shadow, /etc/sudoers

2. PASSWORD POLICY

Edit /etc/login.defs:

```
PASS_MAX_DAYS 90
PASS_MIN_DAYS 1
PASS_WARN_AGE 14
```

3. SUDO POLICY

- visudo

Remove NOPASSWD and unauthorized users.

4. FIREWALL (UFW)

```
ufw reset
ufw allow 22
ufw allow 80
ufw allow 443
ufw enable
```

5. SYSTEM HARDENING

Disable SysRq:

```
kernel.sysrq = 0
```

Hardlinks/symlinks protections:

```
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
```

6. SERVICE DISABLING

Disable unnecessary services:

postfix, avahi-daemon, cups, ircd, telnet.socket

7. UPDATES

```
apt update && apt upgrade -y
```

```
apt autoremove -y
```

Remove harmful tools (xprobe, cmospwd, ftpscan, etc.)

8. FILE SEARCH

```
find / -name '*.bak'
```

```
find /var/www -perm 777
```

Remove suspicious files.

9. CRON & SYSTEMD BACKDOORS

Check crontab, /etc/crontab, /etc/cron.*

Check systemd services, timers.

10. APACHE2 HARDENING

Disable autoindex, cgi, dav, status

```
ServerSignature Off
```

```
ServerTokens Prod
```

Permissions on /var/www

Remove backup files

11. PHP HARDENING

Edit php.ini:

```
disable_functions = exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,show_source
```

```
display_errors = Off
```

```
expose_php = Off
```

12. MYSQL HARDENING

Bind address 127.0.0.1

```
mysql_secure_installation
```

Drop anonymous users

Enable error log

13. LOGGING

Check auth.log, apache2/error.log, mysql/error.log

14. WEB APP CONFIGS

Permissions on config.php

Remove exposed backups

15. FINAL CHECKS

```
ss -tulpn
```

```
systemctl --failed
```

```
dpkg -l
```

```
ufw status
```

```
apache2ctl configtest
```