# Ubuntu Checklist

Read the read me file (CRITICAL!!!! This will give you your directions for each CyberPatriot Challenge!!!! Follow it with STRICT guidance)

Do forensics questions first….and then address the security issues some forensics questions open.

Make sure to empty the recycle bin

Make sure to turn Firewall back on. It sometimes gets turned off.

Make sure to install anti virus and then update it twice before running it.

Make sure to remove all media and pictures and games not explicitly asked to be kept.

To edit files, run gedit, a graphical editor akin to notepad; nano, a simple command-line editor; or vim, a powerful but less intuitive command-line editor. Note that vim may need to be installed with apt-get install vim.

|  |  |
| --- | --- |
| Update the Linux kernel | Apt-get update – gets the latest package list  Apt-get upgrade – updates current packages |
| Update Sudo |  |
| Logs | Logs o Some of the logs ♣ /var/log/messages : General log messages ♣ /var/log/boot : System boot log ♣ /var/log/debug : Debugging log messages ♣ /var/log/auth.log : User login and authentication logs ♣ /var/log/daemon.log : Running services such as squid, ntpd and others log message to this file ♣ /var/log/kern.log : Kernel log file o Viewing logs ♣ tail, more, cat, less, grep ♣ GNOME System Log Viewer |
| Install important security updates |  |
| Disable SSH root login |  |
| Manage users  Change insecure root password | o Users & Groups o Do not use root user (disabled by default) ♣ sudo passwd ♣ sudo passwd -l root o Use sudo instead of root (/etc/sudoers) ♣ sudo visudo OR sudo gedit /etc/sudoers ♣ james ALL=(ALL) ALL ♣ sudo adduser user\_name sudo o Adding users ♣ sudo adduser username o Deleting users ♣ sudo deluser username o Removing world readable permissions to home directory ♣ sudo chmod 0750 /home/username o Locking/Unlocking user ♣ sudo passwd -l username ♣ sudo passwd -u username o Passwords ♣ Expiration • sudo chage username • sudo chage –l username  Made users change password on next login |
| Enable firewall | - *sudo ufw status*  then *sudo ufw enable/disable*  All ports are blocked by default. You may need to open some up if directed. |
| Disable guest account | Go to /etc/lightdm/lightdm.conf and add the line allow-guest=false |
| Antivirus | ClamTK (under Accessories) |
| SSHD service has been installed and started |  |
| Set automatic checks for system updates - daily |  |
| Bash has been updated |  |
| Libre Office has been updated |  |
| Apache2 service has been disabled or removed |  |
| Samba service has been disabled or removed |  |
| Removed netcat backdoor |  |
| Update essential programs |  |
| Disable remote access to MySQL |  |
| IPv6 has been disabled |  |
| Prohibited files removed |  |
| Monitor Processes | ♣ ps aux or top ♣ System Monitor |
| Secure Root | set PermitRootLogin no in /etc/ssh/sshd\_config |
| Configure services | 1. Check service configuration files for required services. Usually a wrong setting in a config file for sql, apache, etc. will be a point. 2. Ensure all services are legitimate. service --status-all |
| Enable syn cookie protection | sysctl -n net.ipv4.tcp\_syncookies |
| Secure ports | 1. sudo ss -ln  2. If a port has 127.0.0.1:$port in its line, that means it's connected to loopback and isn't exposed. Otherwise, there should only be ports which are specified in the readme open (but there probably will be tons more). 3. For each open port which should be closed: 1. sudo lsof -i :$port 2. Copy the program which is listening on the port. whereis $program 3. Copy where the program is (if there is more than one location, just copy the first one). dpkg -S $location 4. This shows which package provides the file (If there is no package, that means you can probably delete it with rm $location; killall -9 $program). sudo apt-get purge $package 5. Check to make sure you aren't accidentally removing critical packages before hitting "y". 6. sudo ss -l to make sure the port actually closed. |
| Enforce Password Requirements. | 1. Add or change password expiration requirements to /etc/login.defs. 2. PASS\_MIN\_DAYS 7 3. PASS\_MAX\_DAYS 90 4. PASS\_WARN\_AGE 14 5. Add a minimum password length. 1. Open /etc/pam.d/common-password. 2. Add minlen=8 to the end of the line that has pam\_unix.so in it. 6. Implement an account lockout policy. 1. Open /etc/pam.d/common-auth. 2. Add deny=5 unlock\_time=1800 to the end of the line with pam\_tally2.so in it. 7. Change all passwords to satisfy these requirements. chpasswd is very useful for this purpose. |
| Check Users | 2. Open up /etc/passwd and check which users ▪ Are uid 0 ▪ Can login ▪ Are allowed in the readme  3. Delete unauthorized users: sudo userdel -r $user  sudo groupdel $user 4. Check /etc/sudoers.d and make sure only members of group sudo can sudo. 5. Check /etc/group and remove non-admins from sudo and admin groups. 6. Check user directories. |
| If ssh is needed | Ufw allow 22, ssh |