

66th Cyber Patriot Team

Ubuntu Checklist

Ubuntu Checklist (CyberPatriot)

1. Input team ID
2. Read the Read me
 - a. Read the readme VERY carefully- could give you hints, ex. if the readme says “no media files allowed” it would be wise to search for media files.
3. Install Gnome, a more familiar Interface
 - a. `sudo apt-get install gnome-session-fallback`
4. Updates
 1. Applications > System Tools > Administration > Update Manager
 2. enabling automatic security updates
 - i. Update Manager -> Settings
5. Firewall
 1. In Ubuntu all ports are blocked by default
 2. Default firewall – ufw (turned off by default)
 1. `sudo ufw status`
 2. `sudo ufw enable/disable`
 3. Firestarter for graphical interface (recommended)
 1. `sudo apt-get install Firestarter`
 2. Preferences
6. User Accounts
 1. Users & Groups
 2. Do not use root user (disabled by default)
 1. `sudo passwd`
 2. `sudo passwd -l root`
 3. Use sudo instead of root (/etc/sudoers)
 1. `sudo visudo` OR `sudo gedit /etc/sudoers`

2. james ALL=(ALL) ALL
3. sudo adduser user_name sudo
4. Adding users
 - i. sudo adduser username
 - e. Deleting users
 - i. sudo deluser username
 - f. Removing world readable permissions to home directory
 - i. sudo chmod 0750 /home/username
7. Locking/Unlocking user
 1. sudo passwd -l username
 2. sudo passwd -u username
8. Passwords
 - i. Expiration
 1. sudo chage username
 2. sudo chage -l username
7. Antivirus
 - a. ClamTK (under Accessories)
8. Uninstall Applications
 1. Applications → Ubuntu Software Center
 2. Installed Software section
 3. Select application and click Remove
9. Processes
 - a. To see processes
 1. ps aux or top
 2. System Monitor
- b. Know
10. Logs
 1. Some
 2. /var/log/boot : System boot log
 3. /var/log/debug : Debugging log messages
 4. /var/log/auth.log : User login and authentication logs
 5. /var/log/daemon.log : Running services such as squid, ntpd and others log message to this file
 6. /var/log/kern.log : Kernel log file
 2. Viewing logs
 1. tail, more, cat, less, grep
 2. GNOME System Log Viewer

