Basic Security Checklist – Ubuntu Linux 12.04 Focus

READ THE SCENARIO, AND THEN READ THE SCENARIO AGAIN!

- ✓ A more familiar Interface
    - sudo apt-get install gnome-session-fallback
- ✓ Updates
    - Applications > System Tools > Administration > Update Manager
    - Enabling automatic security updates
        - Update Manager -> Settings
- ✓ Firewall
    - In Ubuntu all ports are blocked by default
    - Default firewall – ufw (turned off by default)
        - sudo ufw status
        - sudo ufw enable/disable
    - Firestarter for graphical interface (recommended)
        - sudo apt-get install firestarter
        - Preferences
- ✓ User Accounts
    - Users & Groups
    - Do not use root user (disabled by default)
        - sudo passwd
        - sudo passwd -l root
    - Use sudo instead of root (/etc/sudoers)
        - sudo visudo OR sudo gedit /etc/sudoers
        - james   ALL=(ALL) ALL
        - sudo adduser user_name sudo
    - Adding users
        - sudo adduser username
    - Deleting users
        - sudo deluser username
    - Removing world readable permissions to home directory
        - sudo chmod 0750 /home/username
    - Locking/Unlocking user
        - sudo passwd -l username
        - sudo passwd -u username
    - Passwords
        - Expiration
            - sudo chage username
            - sudo chage –l username

- ✓ Antivirus
    - ClamTK (under Accessories)
- ✓ Uninstall Applications
    - Applications → Ubuntu Software Center
    - Installed Software section
    - Select application and click Remove
- ✓ Processes
    - To see processes
        - ps aux or top
        - System Monitor
    - Know what default processes are (screen shot/snip)
- ✓ Logs
    - 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
    - Viewing logs
        - tail, more, cat, less, grep
        - GNOME System Log Viewer