Do First:

- ☐ Complete Forensic Questions

Updates:

- ☐ Update system and other applications
- ☐ Setup automatic updates
- ☐ Update Firefox

Files:

- ☐ Delete Unrelated Media Files
- ☐ Find and Delete Plain Text Password File
- ☐ Delete hacking and other unrelated software

File Permissions:

- ☐ /etc/fstab: make sure the owner & group are set to root.root and the permissions are set to 0644 (-rw-r--r--)
- ☐ verify that /etc/passwd, /etc/shadow & /etc/group are all owned by 'root'
- ☐ verify that permissions on /etc/passwd & /etc/group are rw-r--r-- (644)
- ☐ verify that permissions on /etc/shadow are r-------- (400)
- ☐ Only allow root to access cron

Security Policies:

- ☐ Setup Audit Policy
- ☐ Disable auto-login
- ☐ Disable usernames on the login page
- ☐ Disable SSH root login (if applicable)
- ☐ Disable plain text FTP authentication (if applicable)
- ☐ Secure sudo file (/etc/sudoers)
- ☐ Secure user crontabs

Users:

- ☐ Remove unauthorised users
- ☐ Make sure only authorised admins have privileges
- ☐ Make sure all users have secure passwords

Account Policies:

- ☐ Password Policy (common-password)
- ☐ Password Policy (common-auth)
- ☐ Password Policy (login.defs)
- ☐ Disable guest account
- ☐ Disable root login

Firewall and Network Settings:

- ☐ Enforce security settings on Firefox
- ☐ Firefox Pop-up Blocker Enabled
- ☐ Update firewall
- ☐ Enable firewall
- ☐ Enable syn cookie protection
- ☐ Disable IPv6
- ☐ Disable IP Forwarding
- ☐ Clean hosts files (/etc/hosts)
- ☐ Disable unnecessary services e.g. FTP, Apache and Samba
- ☐ Install anti-virus (clamav)
- ☐ Install anti-virus (clamtk)
- ☐ Search for and remove any backdoor