**Do First:**

* Complete Forensic Questions

**Updates:**

* Update system and other applications
* Setup automatic updates
* Install Windows Service Packs (Not for Windows 8/10)

**Files:**

* Delete Unrelated Media Files
* Find and Delete Plain Text Password File
* Delete hacking and other unrelated software
* Disable file sharing on the C Drive and any hidden drives

**Security Policies:**

* Setup Audit Policy
* Disable Login without CTRL+ALT+DEL
* Disable Last names on login page
* Disable anonymous SID/Name translation
* Do not allow Anonymous Enumeration of SAM accounts (enable)
* Do not allow Anonymous Enumeration of SAM accounts and shares (enable)
* Digitally encrypt or sign secure channel data (always)
* Place the University warning banner in the Message Text for Users Attempting to log on.
* Disable the sending of unencrypted password to connect to Third-Party SMB Servers.
* Do not allow Ev*e*ryone permissions to apply to anonymous users.
* Do not allow any named pipes to be accessed anonymously.
* Restrict anonymous access to Named Pipes and Shares.
* Do not store LAN Manager hash values
* Choose "Classic" as the sharing and security model for local accounts. (Default)
* Set LAN Manager Authentication level to NTLMv2 only
* Ensure that no shares can be accessed anonymously.
* Enable Windows Action Centre

**Users:**

* Remove unauthorised users
* Make sure only authorised admins have privileges
* Make sure all users have secure passwords
* Turn on User Access Control

**Account Policies:**

* Password Policy
* Lockout Policy
* Disable guest account
* Disable Admin Account
* Rename Guest Account
* Rename Admin Account

**Firewall and Network Settings:**

* Enable Firewall
* Disable unnecessary services e.g. FTP (services)
* Disable unnecessary services e.g. Telnet (Windows features)
* Install anti-virus
* Clean host file
* Secure internet connections controls