4. Prepare for Intrusion Detection

4.1 Establish Policy and Procedure
4.2 Build an archive of OS installation media and patches
4.3 Maintain required hardware and software tools.
4.4 Create Baseline
4.5 Check and enforce backup procedures
4.6 Maintain contact information.
4.7 Ensure IDS systems are properly configured.

4.4.1 Determine User Profile
4.4.2 Create Baseline of System Files
4.4.3 Create baseline of network traffic
4.4.4 Backup Baseline

4.4.1.1 Monitor Software Usage
4.4.1.2 Monitor CPU and memory Utilization.
4.4.1.3 Monitor Logs Generated
4.4.1.4 Monitor network usage.