# Linux OS Hardening Baseline

| **S.No** | **Control** | **Expected O/P** |
| --- | --- | --- |
|  | NTP Configuration | Server ntp1.bankofabyssinia.com iburst  Server ntp2.bankofabyssinia.com iburst |
| Synchronized |
|  | Password Complexity | minlen=14  dcredit=-1  ucredit=-1  ocredit=-1  lcredit=-1 |
|  | Password age | PASS\_MAX\_DAYS 90  PASS\_WARN\_AGE 7 |
|  | Set login faillock | auth required pam\_faillock.so preauth audit silent deny=5 unlock\_time=1800  auth [default=die] pam\_faillock.so authfail audit deny=5 unlock\_time=1800 |
|  | Password history | password requisite pam\_pwhistory.so debug use\_authtok remember=4 retry=3 |
|  | Harden SSH | ClientAliveInterval 15m  ClientAliveCountMax 0 |
| Ciphers aes256-ctr,aes192-ctr,aes128-ctr  MACs hmac-sha2-256-etm@openssh.com |
| Protocol 2 |
| PermitRootSSH no |
| PermitEmptyPassword no |
|  | Antivirus installation and configuration | Antivirus installed |
| Automatic update configure |
| Periodic scan configured |
| Generates logs |
|  | Server shall have FIM agent installed | FIM agent installed |
| Send alerts to central server (OSSEC) |
| Required files being monitored   * /opt * /usr/bin * /usr/sbin * /var/ossec/ |
|  | Server shall have SIEM agent installed | SIEM agent installed |
| Sending logs to central server |
|  | Ensure syslog service (rsyslog, syslog, syslog-ng) is running on the server, for logging of events | rsyslog<package version> |
|  |  |  |
|  | Find and remove unwanted packages | package telnet-­server is not installed  package rsh-server is not installed  package rlogin-server is not installed  package rcp-server is not installed  package ypserv-server is not installed  package ypbind-server is not installed  package tftp-server is not installed  package tftp-­server is not installed  package talk-server is not installed  package talk-server is not installed |
|  | Find and stop unwanted services and ports | view the open/closed ports and services |
|  | Enable SELinux | SELINUX=enforcing |
| SELINUXTYPE=targeted |
|  | Enable Firewall | Active and running |
|  | Use the Linux iptables to configure policies | enabled |
|  | Set “sticky bit” on all world writable directories [this is during the installation of the OS]; Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them | Enabled |
|  | Configure access restriction to specific IP(s) that is allowed to access the server, the vendor. [You may use Tcp Wrappers of Linux, for implementation of this]; | tcp\_wrappers<package version> |
|  | Restrict the use of the “cron” utility. If required, this needs sufficient justification and approval; | disabled |