- **User Account**
  - User account naming convention
  - User account user IDs
  - User password policies –

    chage –l username

    chage –help

    /etc/shadow

    vi /etc/login.defs
  - Disable old password

    cd /etc/pam.d/system-auth
  - User or service account files and directories permission
- **Remove un-wanted packages**
  - Install what you need
  - Remove packages no longer in use
- **Stop un-used Services**
  - List all running services

    systemctl (List only running service)

    systemctl –a (List every service running or not)

    telnet, ftp, NFS etc.
- **Check on Listening Ports**
  - netstat -tunlp
- **Secure SSH Configuration**
  - Disable direct root login
  - Change SSH port
- **Enable Firewall (iptables/firewalld)**
  - Older version = iptables
  - New version = firewalld

    firewall-config (GUI)

    firewall-cmd

    iptables

    older version = /etc/sysconfig/iptables-config

    new version = /etc/firewalld/
- **Enable SELinux**

  Security-Enhanced Linux (SELinux) is a security architecture integrated into the 2.6.x kernel using the Linux Security Modules (LSM). It is a project of the United States National Security Agency (NSA) and the SELinux community. SELinux integration into Red Hat Enterprise Linux was a joint effort between the NSA and Red Hat.

SELinux defines the access and transition rights of every user, application, process, and file on the system

/etc/sysconfig/selinux
enforcing — The SELinux security policy is enforced.
permissive — The SELinux system prints warnings but does not enforce policy.
This is useful for debugging and troubleshooting purposes.
disabled — SELinux is fully disabled. SELinux hooks are disengaged from the kernel and the pseudo-file system is unregistered.

Commands = sestatus
Find status of a file = stat filename
Other commands = chcon, checkpolicy, newrole, getsebool, setsebool, fixfiles, semanage
Documentation attached within the hand-out section

- Change Listening Services Port Numbers
- Keep your OS up to date (patching)