Linux-RHEL

There are numerous distributions for Linux operating systems. Below are a few items to review and implement when deploying a Linux system on the UT network. Some examples reference configurations for a specific Linux distribution (e.g. RHEL/CentOS), but should translate to other distributions with some slight modifications. For specific questions for certain distributions, please email it@bme.utexas.edu.

Anti-Virus Considerations

According to the ISO...
There are few viruses that infect Linux computers; therefore, it is understandable for most Linux servers to have an exception to this rule. See the Operations Manual for information on the exception process.
You may choose any proven anti-virus product. One option is ClamAV.

Applying Security Updates

CentOS (command line):

Install and use the yum-security plugin.
To install the plugin run:

```
sudo yum install yum-security
```

To list all updates that are security relevant, and get a return code on whether there are security updates use:

```
sudo yum --security check-update
```

To apply updates that are security relevant use:

```
sudo yum --security update
```

Ubuntu (command line):

Update the Package Index: The APT package index is essentially a database of available packages from the repositories defined in the **/etc/apt/sources.list** file.

```
sudo apt-get update
```

Upgrade Packages: updated versions of packages (security updates).

```
sudo apt-get upgrade
```

Change SSH Default Port

Depending on your Linux distribution, the configuration file for SSH may reside in different locations. Please perform a simple web search for instructions on how to change the port used by SSH on your specific Linux distribution. Below is an example that may guide you through the process.

- As root, use your favorite text editor to edit the sshd configuration file.

```
vi /etc/ssh/sshd_config
```

- Edit the line which states **Port 22**. Choose a port that is not currently used on the system.

```
# What ports, IPs and protocols we listen for

Port 49152
```

It is recommended that a commonly known port number or a port number currently in use by another application is not selected. This may cause technical issues with port allocation in the future. A good secure range of ports you may want to use are ports from 49152 through 65535.

- Switch over to the new port by restarting SSH.

```
/etc/init.d/ssh restart
```

- Verify SSH is listening on the new port by connecting to it. Note how the port number now needs to be declared

```
ssh username@hostname -p 49152
```

Configure NTP Server

The Information Security Office (ISO) has been proactively scanning systems on the UT wired network for outdated versions of the NTP (Network Time Protocol) service running. Systems running a vulnerable version of NTP can be compromised, thus begin participation in NTP-based distributed denial of service (DDOS) attacks targeting various endpoints across the internet. This ultimately leads to an inordinate amount of network usage from the system, and it will be identified from the ISO and the ITS-Networking group.

The Prevention
----
1. If you plan to continue running NTP, ensure it is upgraded to 4.2.6, or later. ITS Networking operates two NTPv4 (NTP version 4) free of charge: 128.83.185.40 (ntp1.utexas.edu) or 128.83.185.41 (ntp2.utexas.edu)
2. Review NTP access restrictions and adjust as needed. Refer to the following resources: http://support.ntp.org/bin/view/Support/AccessRestrictions
   Example:

```
edit /etc/inet/ntp.client -> ntp.conf
added:

#added for DDoS prevention - don't allow any machine, except those w/o flags
restrict default notrust nomodify noquery
restrict 127.0.0.1
restrict 146.6.177.21
restrict 128.83.185.40
restrict 128.83.185.41
```

Implement Deny Hosts

DenyHosts is a script intended to be run by Linux system administrators to help prevent SSH server attacks (also known as dictionary based attacks and brute force attacks) **- http://denyhosts.sourceforge.net/**

Configuration example: set /etc/hosts for specific restrictions. in this example, allowing *.utexas.edu domain hosts, and restricting everything else.

/etc/hosts./allow
ALL: .utexas.edu
and /etc/hosts.deny
ALL:PARANOID

/etc/hosts.allow is checked 1st, then /etc/hosts.deny.

Particular services can also be allowed to only particular machines, e.g:

/etc/hosts.allow
sshd:hostname **(allowed name of machine or IP address)**
and /etc/hosts.deny
sshd:ALL

Limit SSH Access to Campus Network

Example of IP Tables configuration that will only allow UT campus networks to access a system remotely via SSH. The networks listed below include various wired, wireless, and VPN networks.

Note: To access these systems from off-campus, users will need to utilize the UT VPN client available at https://vpn.utexas.edu

```
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -s 128.62.0.0/16 -j ACCEPT
-A INPUT -s 128.83.0.0/16 -j ACCEPT
-A INPUT -s 129.114.0.0/16 -j ACCEPT
-A INPUT -s 129.116.0.0/16 -j ACCEPT
-A INPUT -s 146.6.0.0/16 -j ACCEPT
-A INPUT -s 172.29.0.0/16 -j ACCEPT
-A INPUT -s 198.213.192.0/18 -j ACCEPT
-A INPUT -s 206.76.64.0/18 -j ACCEPT
-A INPUT -s 10.144.0.0/12 -j ACCEPT
-A INPUT -s 146.6.248.0/21 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -j DROP
COMMIT
```

Password Complexity

On most Linux systems, you can use PAM to enforce password complexity. If you have a file in RHEL/CentOS named **/etc/pam.d/system-auth-ac**

Example: Modify pam passwd requirements, length of 10 with special, upper, and lower cases plus a number:

/etc/pam.d/system-auth-ac

```
#password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    requisite     pam_cracklib.so try_first_pass retry=3 minlen=10 ucredit=-1 dcredit=-1 ocredit=-1 lcredit=-1
```

/etc/login.defs

```
PASS_MAX_DAYS   9999999
PASS_MIN_DAYS   0
PASS_MIN_LEN    10
PASS_WARN_AGE   7
```

To change some of the defaults at user creation time

/etc/default/useradd

GROUP=1000   <-setting a default group doesn't seem to work. specify with useradd -g <groupname> <username>

```
#HOME=/home
HOME=/group/users
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
#CREATE_MAIL_SPOOL=yes
CREATE_MAIL_SPOOL=no
```

System Accounts

Files/Directory Permissions/Access

- Enable system accounting (install package sysstat).
- Integrity checking of system accounts, group memberships, and their associated privileges should be enabled and tested.
  - Check in /etc/sudoers to see who has sudo rights
  - Check in /etc/groups to see what groups your users belong to
  - Check in /etc/passwd and/or /etc/shadow for blank passwords
- All administrator or root access must be logged.

System Access, Authentication, and Authorization

- Enable the terminal security file to restrict root logins to system console **only**. **Do not** allow root logins via SSH.
- Ensure the following are set in /etc/pam.d/other:

```
auth  required pam_deny.so
auth   required pam_warn.so
account  required pam_deny.so
account  required pam_warn.so
password  required pam_deny.so
password  required pam_warn.so
session  required pam_deny.so
session  required pam_warn.so
session  required pam_deny.so
```

Warn will report alerts to syslog.