Linux Installation

Prepared by:

William Zereneh

zereneh@scs.ryerson.ca

Introduction

- 1. System Installation and Customization
- 2. System Maintenance
- 3. System Performance and Monitoring

1.Installation and Customization

- Hardware compatibility
- Disk space
- Installation method
- Installation class
  - Personal Desktop Installation
  - Workstation Installation
  - Server Installation
  - Custom Installation
  - Upgrade

1. Installation and Customization

- Configuring a Dual-Boot System
  - Allocating Disk Space for Linux
    - Add a New Hard Drive
    - Use an Existing Hard Drive or Partition
    - Create a New Partition
  - Installing Linux in a Dual-Boot Environment
    - Disk Partitioning
    - Configuring the Boot Loader
    - Post-Installation
  - Partitioning with parted
    - Partitioning a Windows System

1. Installation and Customization

Debian will be installed in class.....

1. Kerberos

- Kerberos is a network authentication protocol created by MIT which uses symmetric key cryptography.
- Design goal is to eliminate the need to send passwords over the network

- Advantages
  - Conventional networks require password-based authentication schemes
  - Such schemes requires username and password
  - Transmission of authentication information for many services is unencrypted
  - KERBEROS NEVER SENDS PASSWORDS ACROSS THE NETWORK

1. Kerberos Cont.

- Disadvantages
  - Implementation is difficult
  - Account information migration from UNIX password database to a Kerberos password can be tedious
  - Partial compatibility with Pluggable Authentication Modules PAM
  - Applications need to be modified to utilize Kerberos
  - Assumes a trusted user using an untrusted host on an untrusted network, but if Key Distribution Center (KDC) is compromised, then the entire Kerberos authentication system will be at risk.
  - All or nothing solution. must use PAM or kerberized versions of all clients/server applications

1. Kerberos Cont.

- How does it work?
  - Three-way authentication, client/server and KDC
  - User authenticate to a service by sending a request to KDC
  - KDC sends a Ticket Granting Ticket (TGT) encrypted with user's key back to user
  - Services (kinit,klogin,..) on the client machine then decrypts the TGT using the user's key (which is derived from the user's password). User's key is used only on the client machine, never sent on the network.
  - If client provides correct password, then TGT will be decrypted and therefore used for subsequent request, otherwise authentication fails.
  - The TGT is set to expire after a certain period of time defined by Network Administrator

2. System Maintenance

- Update Packages – apt-get update && apt-get upgrade
- Install/Remove Packages – apt-get install/remove
- Resize Existing Partition – resize2fs
  - NOTE: boot into rescue mode
- Create New Partition - fdisk
- Mount File System
- Create Swap File/Partition
  - *dd if=/dev/zero of=/swapfile bs=1M count=512*
  - *mkswap /swapfile*
  - *swapon /swapfile*
  - *Make it Permanent: edit /etc/fstab and add:*

    /swapfile none swap defaults 0 0

2. System Maintenance

- Run levels
  - /etc/inittab
  - Change run level for system maintenance
    - Halt System: */sbin/init 0*
    - *Single User: /sbin/init 1*
    - *Multiuser: /sbin/init 2*
    - *Full Multiuser: /sbin/init 3*
    - *Graphical: /sbin/init 5*
    - *Reboot System: /sbin/init 6*
  - Debian combines runlevels 2-5 as multi-user

2. System Maintenance

- Booting Into Rescue Mode
  - Why? Forgotten root password
    - Boot from CD-ROM/ISO image
    - *Choose Advanced options*
    - *Choose Rescue mode and follow prompts*
    - *Run passwd to change root password*
  - *Why? New updated kernel is not booting*
    - *Boot from machine and select (Recovery mode)*
    - *Edit grub boot options by pressing "e"*
    - *Add "init=/bin/bash" on the Linux kernel line*
    - *Ctrl-x to boot*
    - *From root shell you could change grub configuration using an editor*

2. System Maintenance

- File system maintenance
  - Rotate /var/log files
  - Remove stale files from /tmp
- Documentation
  - Policies
  - Procedures
  - Changes
- *Network maintenance*
  - *Keep Firewall up-to-date*
  - *Keep services up-to-date*

2. System Maintenance

- Planning for Disaster
  - Disaster: Unplanned event that disrupts the normal operation of the organization
- Types of Disasters
  - Hardware failures
  - Software failures
  - Environmental failures
  - Human errors
- Backups
  - To restore individual file
  - To restore entire file system

2. System Maintenance

- Type of Backups
  - Full backup
    - Every single file is written to backup media
  - Incremental backup
    - Only modified files are written to backup media
  - Differential backup - Cumulative
    - Modified files will continue to be included in all subsequent differential backups
  - Backup Media
    - Tape
    - Disk
    - Network

2. System Maintenance

- Backup Technologies
  - tar

    tar vcf /mnt/backup/home.backup.tar /home/

    tar vzcf /mnt/backup/home.backup.tar /home/
  - cpio

    find /home/ | cpio -o > /mnt/backup/home.backup.cpio

    find /home/ -atime +365 | cpio -o > /mnt/backup/home.backup.cpio
  - RSYNC

    /usr/bin/rsync –avx –rsh="ssh " username@remote.machine:/var/log/snort /mnt/backup

3. System Performance & Monitoring

- Tuning Hard Disk Performance
  - Put swap partition near the beginning of hard drive
  - *Hard disk read timing*

    /sbin/hdparm -t /dev/hdaX

3. System Performance & Monitoring

- Network
  - Change the following TCP/IP values *edit /etc/sysctl.conf change/add*

 # Decrease the time default value for tcp_fin_timeout connection

net.ipv4.tcp_fin_timeout = 30

Decrease the time default value for tcp_keepalive_time connection

net.ipv4.tcp_keepalive_time = 1800

Turn off the tcp_window_scaling

net.ipv4.tcp_window_scaling = 0

Turn off the tcp_sack

net.ipv4.tcp_sack = 0

Turn off the tcp_timestamps

net.ipv4.tcp_timestamps = 0

- Restart network - /etc/init.d/network restart

3. System Performance & Monitoring

- File System
  - ext3 over ext2

    /bin/umount /dev/sdaX

    /sbin/tune2fs -j /dev/sdaX

    edit /etc/fstab change ext2 to ext3 for /dev/sdaX

    /bin/mount /dev/sdaX
- Maximum number of file handles allocated by the kernel - file-max parameter
  - Approx: 256 files for every 4M
  - Edit /etc/sysctl.conf add/change

    # Improve the number of open files

    fs.file-max = 8192 # for a 128M machine

3. System Performance & Monitoring

- Access Time
  - Linux records information about when files were created, last modified and last accessed
  - Highly accessed files should have *atime* attribute removed
  - /usr/bin/chattr -R +A /var/spool/
  - noatime mount parameter
  - edit /etc/fstab and add noatime option

```
/dev/hdaX       /chroot       ext3       defaults,noatime       1  2
```

3. System Performance & Monitoring

- Resource Monitoring
  - What to Monitor? Resources
    - CPU Power
    - Bandwidth
    - Memory
    - Storage
  - Utilities to use for CPU, Bandwidth and Memory
    - free
    - top
    - vmstat

3. System Performance & Monitoring

- free – The free command displays system memory utilization

  Example:

```
             total       used       free     shared    buffers     cached
Mem:        255508     240268      15240          0       7592      86188
-/+ buffers/cache:     146488     109020
Swap:       530136      26268     503868
```

  - Automate free

    /usr/bin/watch -n 1 -d free

3. System Performance & Monitoring

- top – Displays CPU utilization, process statistics, memory utilization
  - example

```
14:18:52  up 16 days, 21:37,  1 user,  load average: 0.07, 0.02, 0.00
71 processes: 70 sleeping, 1 running, 0 zombie, 0 stopped
CPU0 states:  0.0% user   0.0% system    0.0% nice   0.0% iowait 100.0% idle
CPU1 states:  2.0% user   6.0% system    0.0% nice   0.0% iowait  90.0% idle
Mem:  513232k av,  505424k used,    7808k free,      0k shrd,   66464k buff
                379364k actv,      0k in_d,   12044k in_c
Swap: 417648k av,  108724k used,  308924k free                 325384k cached

 PID USER     PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME CPU COMMAND
18866 root      20   0   984  984   788 R     6.5  0.1   0:00   1 top
```

3. System Performance & Monitoring

- vmstat – Display process, memory, swap, I/O, system and CPU activity
- example:

```
   procs                  memory     swap       io     system      cpu
 r  b  w   swpd   free   buff  cache   si   so    bi    bo   in    cs us sy id
 0  0  0 108724   6400  66452 325664    0    0     5     6   10    10  2  1  8
```

r – Runnable processes state
b – Uninterruptible sleep state
w – Swaped out, but runnable

si – swaped in

so – swaped out

3. System Performance & Monitoring

- Other monitoring tools
  - The Sysstat suite

/usr/bin/iostat

/usr/bin/mpstat

/usr/bin/sar

3. System Performance & Monitoring

- Storage
  - Utilities to use for Storage
    - smartd/smartctl
    - df
    - du
    - badblocks
  - smartd – is a daemon that monitors the Self-Monitoring, Analysis and Reporting Technology System (S.M.A.R.T.) built into ATA-3 and later IDE and SCSI-3 hard drive.

```
/usr/sbin/smartctl -i /dev/hda
Device: Maxtor 90650U2  Supports ATA Version 5
Drive supports S.M.A.R.T. and is enabled
```

3. System Performance & Monitoring

- df – Disk free

```
/bin/df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/hda5              5578804   4279424   1298180  77% /
/dev/hda1               108868     9899     93348  10% /boot
none                    256616        0    256616   0% /dev/shm
```

- du – Disk usage

```
/usr/bin/du /tmp
du /tmp/
4       /tmp/screens/S-root
8       /tmp/screens
.....
```

3. System Performance & Monitoring

- Other monitoring tools
  - smartd
  - Big Brother - bb
  - Multi Router Traffic Grapher - mrtg
  - logwatch
  - .....

References

- www.debian.org
- www.redhat.com
- www.disasterplan.com
- www.amanda.org
- www.linux-backup.net
- http://web.mit.edu/kerberos/