ST2412 Linux Administration and Security

Lesson 1

USING ORACLE LINUX AND OTHER LINUX UTILITIES

Contents

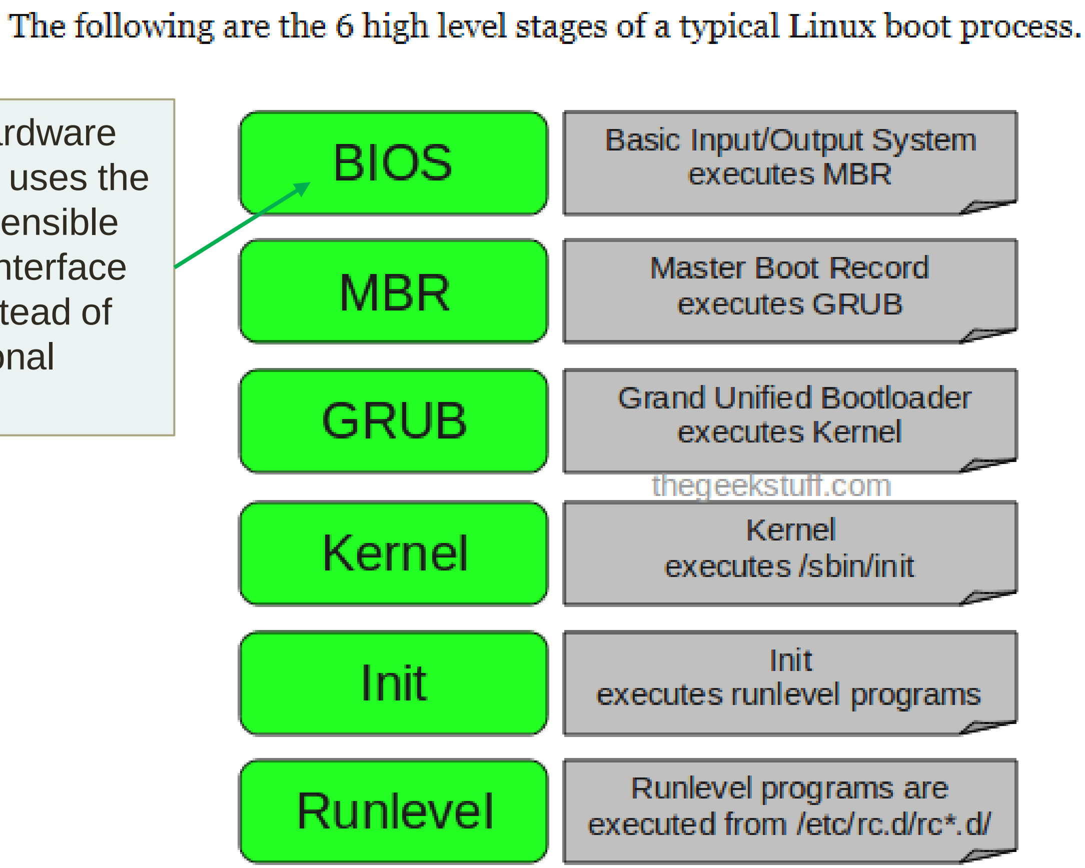
- root password recovery
- Grub Menu protection and Linux Boot Process
- Basic setup and usage of ssh, scp and sftp
- Network and Kernel configuration
- vsftpd Configurations
- SELinux
- User Process Management Basics
- find, grep, sed and awk

root password ~~Recovery~~

- Follow the step by step exercise to try out root password reset procedure
  - Useful when the root password is lost !
  - Based on interrupting the normal boot process and file system mounting/remounting techniques.
  - Impose a vulnerability when physical security is not guarantee.

Linux Boot Process

All new hardware nowadays uses the unified extensible firmware interface (UEFI) instead of the traditional BIOS.



The following are the 6 high level stages of a typical Linux boot process.

BIOS	Basic Input/Output System executes MBR
MBR	Master Boot Record executes GRUB
GRUB	Grand Unified Bootloader executes Kernel
Kernel	Kernel executes /sbin/init
Init	Init executes runlevel programs
Runlevel	Runlevel programs are executed from /etc/rc.d/rc*.d/

Ref: https://www.thegeekstuff.com/2011/02/linux-boot-process

Grub Menu Protect

- Follow the step by step exercise
  - Protect your Grub Menu with specific
    - User ID
    - Password
  - To prevent unauthorized root password reset
- Other protection method
  - Password protection on boot operation
    - Configure at BIOS/UEFI Settings
    - Note: VMWare Workstation simulates these settings too !
- What if the attacker takes away your hard disk ?
  - Can they break into your file system ?
  - You may have a chance to get your own answer in CA1 – part 1.

ssh, scp and sftp

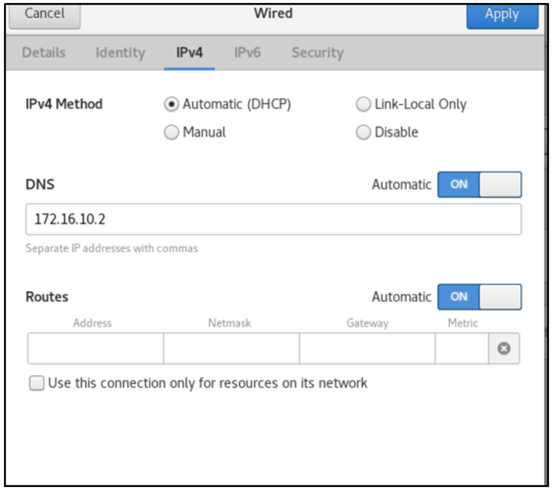
- A set of remote access utilizes that based on the same protocal.
- ssh
  - Secure shell
  - A utility/protocol to provide secured remote shell access based on encryption
  - Server / Client based protocol
    - Server – sshd service – listening on port 22
    - Client – runs ssh utility
- scp
  - Secure copy
  - Based on ssh to enable remote host file copy.
- sftp
  - SSH File Transfer Protocol
  - Technically not relate to the FTP Protocol (FTPD listening on port 21)
  - Also based on ssh to enable FTP like features.

Overview of TCP/IP ports and port number range

- Each TCP/IP Network interface support up to 64K ports
- The port number serves to uniquely identify that service on a particular host/interface.
- Outgoing traffic also needs to base on a available port.
- Well known port numbers are listed in /etc/services
- Ports from 1 to 1023 are privileged. Only root processes can bind to these ports.
- Client processes (eg web browsers – outgoing to visit a web site) are usually assigned port numbers way above 1023
- The netstat -tuna command is used to see which ports are open on a machine
- Use netstat -tunap to see the name of the processes
- Port number is one of the key attributes that a firewall may be based on to block/accept incoming/outgoing traffic.

Network Manager

- Network Manager is used to manage the network on a Linux System.
- To configure network on Oracle Linux
  - Run nmtui, a curses-based text user interface for Network Manager
  - Use nmcli, a command-line tool
  - Use the Gnome Network Settings GUI



IPv4 Method ● Automatic (DHCP) ○ Link-Local Only
○ Manual ○ Disable

DNS Automatic ON

172.16.10.2

Separate IP addresses with commas

Routes Automatic ON

Address	Netmask	Gateway	Metric

□ Use this connection only for resources on its network

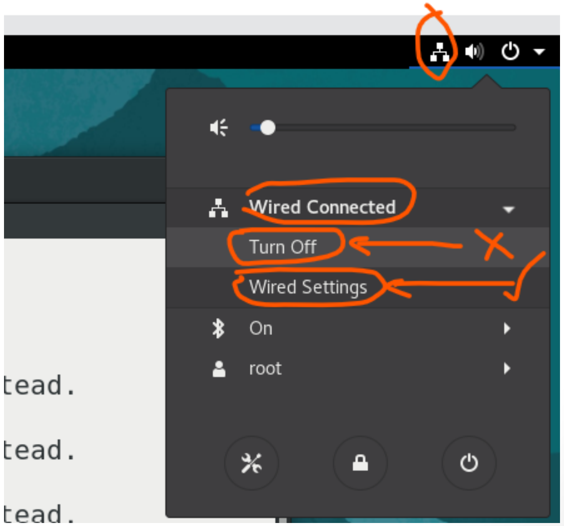
Network configuration

- The ip command can be used to show or set network configuration like addresses and routing
  - ip addr show ens160
  - ip route
- Any change made by the ip or ifconfig commands will be lost upon next reboot
- To permanently change network settings:
  - Use nmcli or Gnome Network Setting UI
    - Settings go to the config files.
  - Modify the config files manually. Example :
    - /etc/sysconfig/network-scripts/ifcfg-ens160

Network configuration

- To bring down and up a network interface*
  - `nmcli c down ens160`
  - `nmcli c up ens160`

*It is a common mistake that ST2412 students may make is accentually bring down the network connection by clicking on the Turn Off option when using the GUI to manage the Wired Settings.



Kernel tuning

- Kernel parameters allow some tuning of the Linux kernel
- The **sysctl** command can be used to display or set (temporarily) the kernel parameters
- To make changes in the kernel parameters persistent across reboots, change the config file
  - /etc/sysctl.conf

Do not login as root

- Recommended not to login as root
- When logged in as root, every process you start is run as root
- Hijack of a process or account could give attacker root-privileges
- Faulty process run as root can cause more damage to system
- Higher risk of accidentally changing system configuration

Do not log in as root

- Some Linux distributions disable root logins
- Login as normal user and use **su** or **sudo** when root privilege is required
- Members of the wheel group can do all admin tasks through sudo by default

The vsftpd service

- Very Secure File Transfer Protocol Daemon
- Config file /etc/vsftpd/vsftpd.conf
- Ftp home directory in /var/ftp
- Typically the FTP home directory contains a **`pub`** subdirectory that holds all the downloadable files

vsftpd.conf

- Some common configurations
  - ftpd_banner

    Not good practice to use default greeting banner that displays software version
  - anonymous_enable

    Allow users to connect as anonymous user, without needing a password
  - local_enable

    Allow local users to connect with their normal passwords. Remember that FTP runs on unsecure channel (No encryption), so usernames and passwords will be sent over in cleartext!

ftp chroot

- **chroot** – change root directory
- Use chroot to restrict users to a directory on the FTP server
- Without chroot enabled, users may be able to access the whole file system on the FTP server
- With chroot enabled, users can be restricted to only their home directories on the FTP server

ftp chroot

- chroot_list_enable
  - To activate or not activate chroot for local users (depends on chroot_local_users sertting)
- chroot_list_file
  - Filename of list of users to chroot or not to chroot
  - Refer to the chroot_jail_in_vsftpd.txt and the practical exercises

SELinux

- Security-Enhanced Linux
- Enhancement to the standard Linux Discretionary Access Control (DAC) for file access and program execution.
  - Linux file access permission in DAC
    - 3 user categories : owner, group, others
    - 3 permissions per category: rwx (Read, Write, Execute)
- Allows administrators to define highly-customizable security policies
- With SELinux
  - Processes are run in a SELinux domain
  - Resources (files, sockets, etc) are assigned a SELinux context
  - User / process can access to an object Only when the context of the object meets the requirement.
- Watch this video (after you have completed the practical exercises) : https://www.youtube.com/watch?v=tXNr3gOgrn8

SELinux state

- On bootup, Oracle Linux enters one of the following 3 SELinux states
  - Enforcing : Any action that violates SELinux policy is prohibited and logged
  - Permissive : Any action that violated SELinux policy is logged but allowed to continue
  - Disabled : SELinux not used
- **`getenforce`** : to display current SELinux state
- **`setenforce`** : to set the SELinux state (temporarily)

SELinux config file and log messages

- /etc/selinux/config : used upon bootup to determine SELinux state and policy

- SELINUX=permissive
- SELINUXTYPE=targeted

- SELinux violations are logged to /var/log/audit/audit.log

Viewing SELinux domains and contexts

- The SELinux domains of processes can be displayed using the '-Z' switch
  - eg. ps -axZ
- The SELinux contexts of resources can also be displayed using the '-Z' switch
  - eg. ls -aZ

Change SELinux contexts of files

- chcon : change security context of a file

- Example : (login as root)
  - [root@station]# touch /tmp/tmpfile
  - [root@station]# touch ~/homefile
  - [root@station]# mv /tmp/tmpfile /root
  - [root@station]# ls –Z /root
- To change the SELinux context of /root/tmpfile to follow /root/homefile's context
  - [root@station]# chcon --reference ~/homefile ~/tmpfile

Restore SELinux contexts of files

- restorecon : restore security context of a file based on where it resides in the filesystem.

- Example :
  - [root@station]# touch /tmp/tmpfile2
  - [root@station]# mv /tmp/tmpfile2 /root
  - [root@station]# ls -Z /root
- To restore the SELinux context of /root/tmpfile
  - [root@station]# restorecon ~/tmpfile2

Managing SELinux Booleans

- SELinux policy consists of a collection of booleans
- getsebool lists the boolean and its current setting
  - [root@station]# getsebool bluetooth_disable_trans
  - bluetooth_disable_trans --> off

- getsebool -a lists all booleans and their current settings
  - [root@station]# getsebool -a

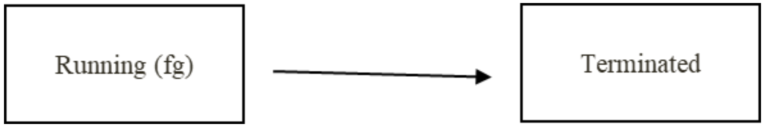
Managing SELinux Booleans

- setsebool modifies boolean setting
- [root@station]# setsebool bluetooth_disable_trans 1
- [root@station]# getsebool bluetooth_disable_trans
  bluetooth_disable_trans --> on

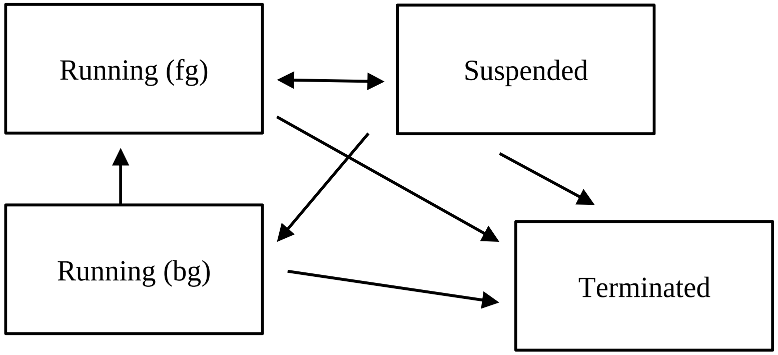
- setsebool -P causes the modification to persist across reboot
- [root@station]# setsebool -P bluetooth_disable_trans 1

User Processes Management

- Typical User Process life cycle:
  - User execute a command/application (process runs in foreground.)
  - The command has finished/application has ended (Process is terminated.)



- By using Hot-Key and commands, user process can be switched between 4 states:



find

- Help to locate a target file in the file system.
- Provide many ways to search for a (group of) target file(s).
  - By name (Partial or exact).
  - By file size range.
  - By file owner.
  - By file attributes.
- Simple example:
  - find /home -name "secret*"
- Can combine with other command too:
  - To delete all files that has the suffix of .bak
  - find / -name "*.bak" -type f -print | xargs /bin/rm -f
  - find / -name "*.bak" -type f -print0 | xargs -0 /bin/rm -f

grep

- Help to extract a line from a text file that matches a specific pattern.
- Search for a (group of) line(s) based on 'regular expressions'.
- Simple example:
  - Find the enabled repo
    - grep 'enable=1' *.repo
  - List all the non-commented out lines from a config file
    - grep -v '^#' vsftpd.conf

Sed

- Stream Editor
  - Reads from file line by line.
  - Good for batch mode text replacement.
- The sed substitution command has the following structure:

```
s/target_string/replacement_string/ input_file
```

- Only the first occurrence of the target_string in each line will be replaced.
- To do a global replace of all occurrences of the target_string

```
s/target_string/replacement_string/g
  input_file
```

Sed examples

- /tmp/test.txt

```
apple,red,$2,$2.20
```

- To replace the word “apple” with “orange”

```
sed s/apple/orange/ test.txt
```

- To replace all occurrences of “2” with “4”

```
sed s/2/4/g test.txt
```

- To replace the first occurrence of “2” in each line with “4”

```
sed s/2/4/ test.txt
```

Sed examples

- /tmp/test.txt

```
apple,red,$2,$2.20
```

- To replace all occurrences of “$” with “RM”

```
sed ‘s/\$/RM/g’ test.txt
```

  - The dollar sign has a special meaning, so it has to be escaped with a backslash
  - Put single quotes around the substitute part

Sed examples

- /tmp/test.txt

```
apple,red,$2,$2.20
```

- If you want to add the word “big” before the contents of the first column, you can use \1 to keep the contents of the first column

```
sed ‘s/\(.*,\)/big \1/’ test.txt
```

- **`(.*,)`** will match the first word till the comma sign

  `.` matches a single character (any character)

  `*` matches any multiple or no characters

  Brackets have special meaning, so they need a backslash in front of them

  \1 will have the first matched pattern

Sed examples

- /tmp/test.txt

```
apple,red,$2,$2.20
```

- To add the word “big” in front of the first column, followed by the fourth column

```
sed ‘s/\(.*,\)\(.*,\)\(.*,\)\(.*\)/big \1 \4/’
test.txt
```

- Sed has many more capabilities. You can check the Internet for more sed features.

Awk basics

- □ Awk can be used to process column-oriented text data
- □ $1, $2, etc, are the contents of the first, second, etc, columns

- □ A simple awk statement could be written this way :

```
awk -F 'pattern_to_match {action_to_do}'
input_file
```

- □ To print the second column in a file

```
awk -F ‘{print $2}’ test.txt
```

- □ To print the second and third columns in a file if the first column starts with the letter “a”

```
awk -F ‘$1 ~/^a/ {print $2, $3}’ test.txt
```

Awk basics

- To print the second column in a file if the third column is greater than 200

```
awk -F ‘$3 > 200 {print $2}’ test.txt
```

- To print the fourth and fifth columns in a file if the first column starts with the letter “a” and the second column is greater than 10

```
awk -F ‘$1 ~/^a/ && $2 > 10 {print $4, $5}’
test.txt
```

- Awk has many more capabilities. You can check the Internet for more awk features.

Summary

- Linux Boot Process and the associated vulnerability
- Network and Kernel configuration
- Using vsftpd service
- Chrooted users for vsftpd service
- SELinux
- User Processes Management Basics
- Usuful command line tools:
  - find, grep, sed and awk
- Complete Online Quiz1 for your assignment scores