

Operating System Security

#06 - Securing Linux System



Herman Kabetta

hermanka.github.io



Message of The Day

- When you first login to a terminal on a Linux system, you are usually greeted by the system's message of the day(MOTD). The message of the day, gives you important information about the system or just messages from the system admin
- It is important for a system administrator to setup the MOTD which will alert users to be careful as their activity is being monitored
- A simple text message can be added to the following file
 - **/etc/motd**

```
dev@dev: ~  
File Edit View Search Terminal Help  
  
/ Just because the message may never be received does not mean it is \  
\  
not worth sending. /  
-----  
  \  ^  ^  
   \ (@@)\_____  
    ( _)\_____) \/  
        ||----w |  
        ||      ||  
  
dev@dev:~$
```



Customize MoTD

- Once again, message of the day is the first message users will see when they login to the Linux machine
- Steps:
 - Create a new file in `/etc/profile.d/motd.sh`
 - Add desired commands in motd.sh file
 - Modify the `/etc/ssh/sshd_config` file to edit `#PrintMotd yes` to `PrintMotd no`
 - Restart sshd service
 - `systemctl restart sshd.service`

```
1  #!/bin/bash
2
3  HOSTNAME=`uname -n`
4  KERNEL=`uname -r`
5  CPU=`uname -p`
6
7  figlet -f digital Welcome to $HOSTNAME!
8  echo "You're running $KERNEL on $CPU"
```



Remove Un-necessary or Orphan Packages

The first rule is to keep your server lean and mean. Install only those packages that you really needed. If there are unwanted packages, delete them. The fewer the packages the less chance of unpatched code

Guidelines:

- Do not install packages that you do not need during the initial installation
- Pay close attention to the add-on packages

To get a list of all packages

```
# rpm -qa (CentOS)
```

```
# apt list -installed (Ubuntu)
```

Remove packages

```
# rpm -e package_name
```

```
# apt-get remove package_name
```

Orphaned Packages:

The objective is to remove all orphaned packages from CentOS Linux. By orphaned packages we mean all packages which no longer serve a purpose of package dependencies.

For example, package A is depended on package B, thus, in order to install package A the package B must also be installed. Once the package A is removed the package B might still be installed, hence the package B is now orphaned package



Remove Un-necessary or Orphan Packages

- A built-in utility which allows you to check for orphaned packages

`yum-utils`

- Check if that exist in your system

```
# rpm -qa | grep yum-utils
```

- If not then install

```
# yum install yum-utils
```

- Get a list of all orphaned packages

```
# package-cleanup -leaves
```

- Remove

```
# yum remove `package-cleanup -leaves`
```

```
# apt-get autoremove
```



Keep Kernel and System Up to Date

- Register to OS providers websites such as Redhat, CentOS, Ubuntu, Debian etc.
- Stay connected with the technical news feeds and OS community
- Run package management software such as Redhat Satellite or Ubuntu Landscape

Commands:

```
# yum update or upgrade
```

```
# apt-get update
```





System Upgrade/Patch Management

- Two type of upgrades

Major version = 5, 6, 7

Minor version = 7.3 to 7.4

Major version = yum  command


Minor version = yum update 

Example:

yum update -y

yum update vs. upgrade

upgrade = delete packages 

update = preserve 



Stop and Disable Unwanted Services

- What is a Service?
- Difference between a service and a package?
- Before you can decide which services are unnecessary, you need to know which services are running. To find out, run
 - `netstat -l`
 - `netstat -tulpn`
 - `systemctl`
 - `chkconfig --list` (older version of CentOS)
 - `service --status-all | grep running` (CentOS or Ubuntu)
 - `ps -ef`

Disabling through PAM files

- Looking at the files in `/etc/pam.d/`, you'll probably see configuration files for a number of programs you don't use and maybe even a few you've never heard of. The best way to disable PAM authentication for these programs is to rename these files. Not finding the file named after the service requesting authentication, PAM will fallback to the (hopefully) very secure `/etc/pam.d/other`
- If you later find that you need one of these programs, you can simply rename the file to its original name and everything will work as it was intended.



Stop and Disable Unwanted Services

- To stop a service
 - `chkconfig httpd off`
 - `chkconfig httpd disable`

 - `systemctl stop httpd`
 - `systemctl disable httpd`
- Example of `httpd` package and service
 - `rpm -qa | grep httpd`
 - `yum install httpd`
 - `systemctl start httpd`
 - `ps -ef | grep http`
 - OR
 - `netstat -tulpn`
 - `systemctl stop httpd`
 - `systemctl disable httpd`



Separate Disk Partitions

- What is disk partitioning?
- A disk in Linux should be partition into the following mounts
 - /
 - /boot
 - /usr
 - /home
 - /tmp
 - /var
 - /opt.

How disk partitioning can help?

- Partitioning your drive can also keep your data safer from malware attacks. If ransomware lands on your Linux partition, it would have a lesser chance of locking your personal or critical files on another partition
- If a partition gets full it can be easily extended using LVM and it won't impact other partitions
- Disk partitioning can enhance your system or application performance
- Utilize other filesystems for each partition (e.g. ext4, XFS etc.).



Disable Ctrl+Alt+Del

- What is Alt+Ctrl+Del?
- Command to check the status of alt+ctrl+del

```
# systemctl status ctrl-alt-del.target
```

(CentOS and Ubuntu)
- Command to disable alt+ctrl+del

```
# systemctl disable ctrl-alt-del.target
```
- For earlier version like CentOS/RHEL 6 the file that handles Ctrl-Alt-Del

```
#/etc/init/control-alt-delete.conf
```
- The above steps will not disable "ctrl+Alt+delete" key combination in GUI mode. To disable it in GUI change keyboard settings

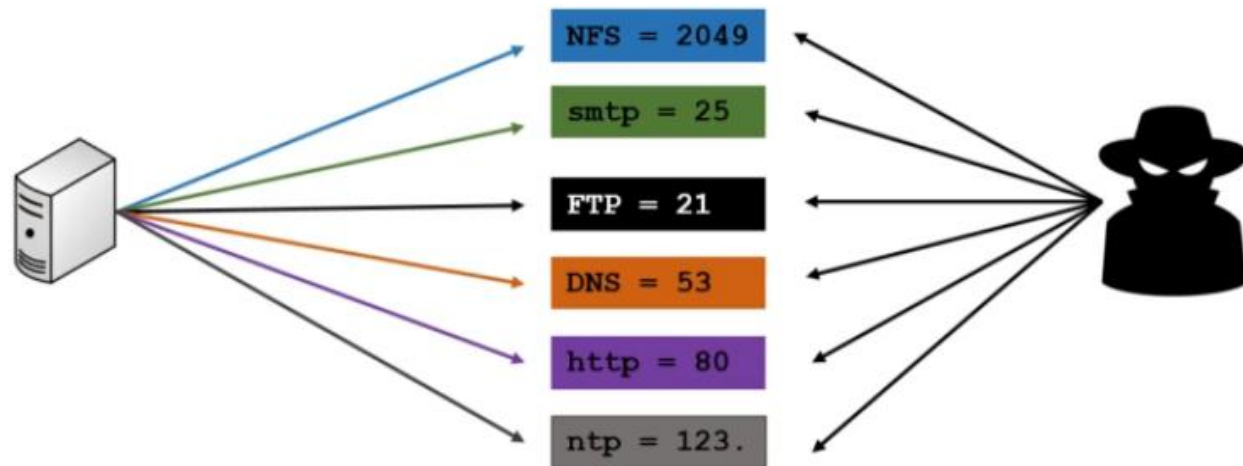
Go to your Linux Console as root → Navigate to Applications → System Tools → Settings → Devices → Keyboard → Keyboard Shortcuts → System → Logout → Enter

- Set value of "Logout" as Disabled by hit Backspace → Set



One Service Per Server

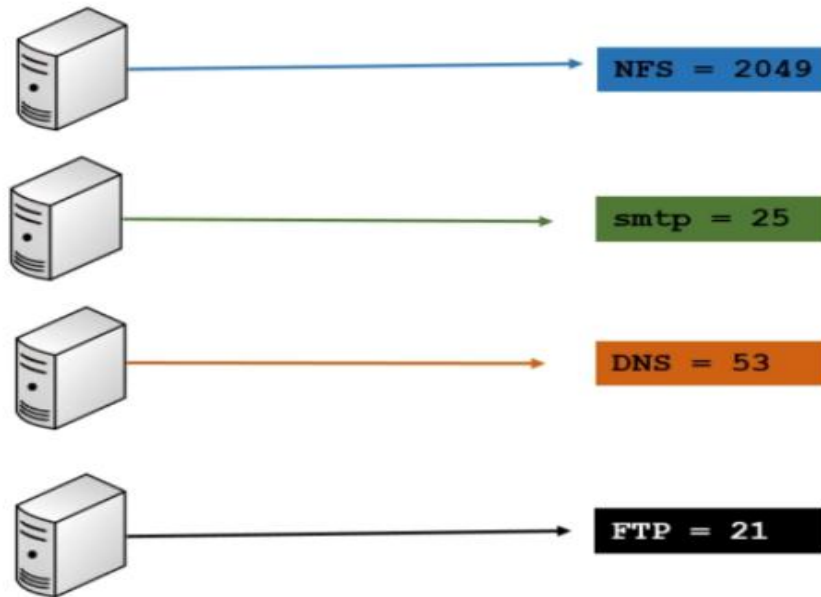
- What is Service or a Program?
- Example of Services:
 - **NFS**, **DNS**, **WebServer**, **FTP**, **sendmail** etc.





One Service Per Server

- Best architecture would be:





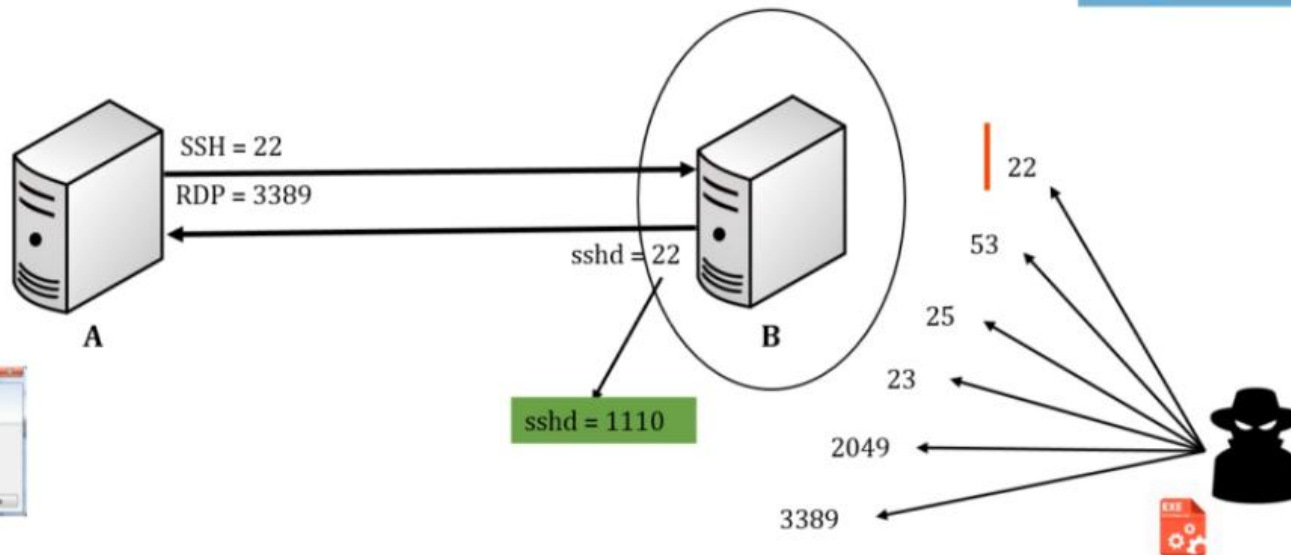
Disable USB Stick Detection

- Many times we want to restrict users from using USB stick in systems to protect and secure data from stealing
- To disable USB stick detection
 - Create a file `/etc/modprobe.d/no-usb` and add the following line
 - `install usb-storage /bin/true`



Change SSH Port

- How server to server connection works? = IP to IP
- Every server runs services to listen on pre-defined ports
- SSH port = 22?
- Listing of ports = `/etc/services`





Change SSH Port

- Make a backup of
`/etc/ssh/sshd_config`
- Modify config file
`/etc/ssh/sshd_config`
- Change
`Port 22 = Port 1110`
- Restart the server
`#systemctl restart sshd"`
- From Unix like OS connect using command syntax
`ssh username@IP -p 1110`



Etc.

1. Backups Management
2. Enable Network Time Protocol (NTP or Chronyd)
3. Lockdown Cronjobs
4. Secure Enhanced Linux (SELinux)
5. Firewall Configurations
6. Auditing System using Auditd
7. Intrusion Detection using AIDE
8. Scanning for Rootkits
9. Configuring Rsyslog