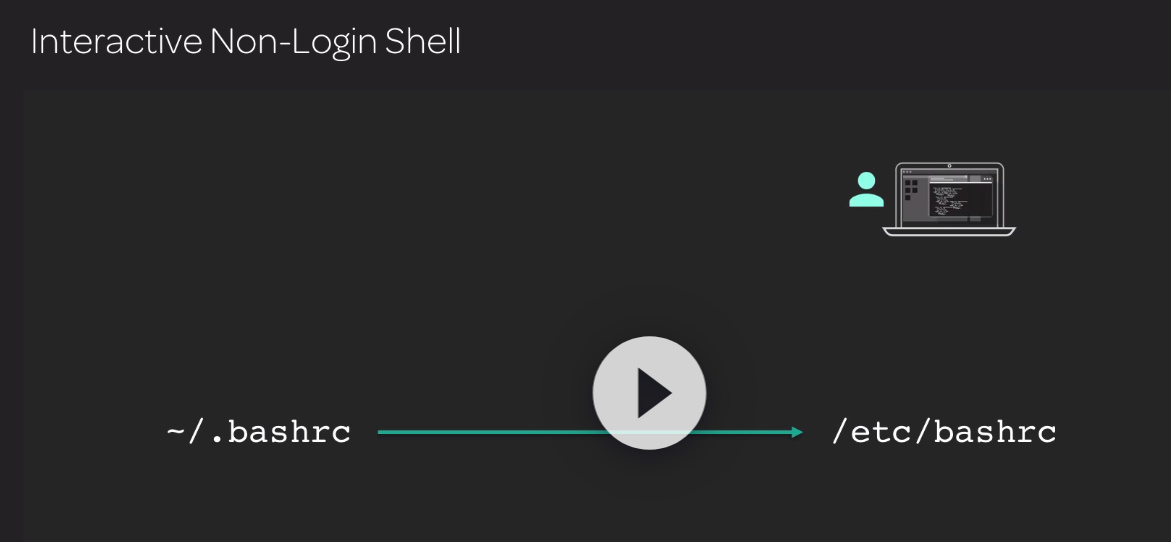
# LPIC-1: System Administrator – Exam 102

**Chapter 2**

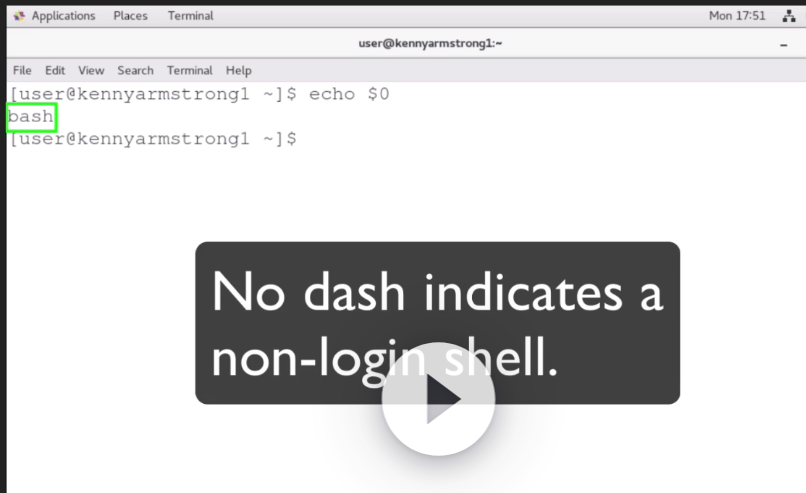
105.1 Customize and Use the Shell Environment

Setting up the shell Environment:









/etc/profile : this first file read on a login session. Sets up system-wide environment variables. Unmask values, bash history controls, etc.

/etc/profile.d/ : the directory that contains extra script configuration files for Bash.

The /etc/profile file will read in the contents of this directory.

/etc/bashrc : you can configure system-wide functions and aliases here.

/etc/skel : the directory that contains the default .bash\_profile, .bashrc, and other files that are added to a user’s home directory when an account is created on the system.

~/.bash\_profile : this file can contain a user’s modified PATH environment variable and will source the ~/.bashrc file. This file can also be named ~/.profile on some distributions.

~/.bashrc : local user command aliases and functions are Defines here. This file sources the /etc/bashrc file.

~/.bash\_logout : this file gets called on user logout and can be used to shut down applications, display a message , or to perform other environment cleanup tasks.

~/.bash\_login : this file gets called on a user login. Typically, .bash\_profile and .bashrc are used instead of this file.

Customizing the shell envionment:

Alias : the alias command is used to create a shortcut to a longer command, typically with optiona.

Function: A Bash keyword used to indicate that a new bash function follow. A bash function is any custom command that a user can use in a Bash shell.

.(dot) : the dot command is used to source or apply functions from a file into the current Bash session or a shell script.

Source : same as above. The dot command is an alias to the source command.

PATH : An environment variable that defines where applications can be found by the Bash shell without specifying their full path.

**Chapter 3**

## 105.2 Customize or Write Simple Scripts

Basic shell scripts:

#! : character sequence (known as the ‘shebang’ ) that can be used at the beginning of the any perl, python or Bash script. This sequence tells the system that the file is a script. The actual script interpreter follows the shebang sequence.

# (comment) : this character indicates that what follows is a comment

<< comment\_name

comment\_name : to multi line comment

**Chapter 5**

## 106.2 Graphical Desktops

The primary linux Desktop Environments

GTK+Based Desktops: GTK+ is primarily a ‘C’ language library. Desktops that use this library include:

GNOME

XFCE

Qt based Desktops: Qt is a ‘c++’ language library used for graphical applications. Desktops that use this library include: KDE

**Chapter 7**

## 107.1 Manage User and Group Accounts and Related System Files

Adding and removing user:

Useradd : To add the user

Passwd : to change the password

Userdel: to delete the user

Adding and removing group:

groupadd : To add the user

groupdel: to delete the user

Groups: to see the groups

User and group configuration files:

/etc/passwd: it contains information about user and system accounts

/etc/shadow: it contains encrypted passwords for account listed in /etc/passwd file

$1$ : md5

$2a$ , $2y$ : blowfish

$5$ : SHA-256

$6$ :SHA-512

/etc/group: it contain group definitions along with what user belong to each group.

/etc/skel : it contains item that will automatically get added to a new user’s home directory when the account is created.

/etc/default/useradd : this configuration file in referenced by the useradd command when a new user account is created.

getent: this command is used to query a database for information about a user or group.

User and group modification :

usermod: this command is used to modify an existing user account setings

chage : this command can list and modify the aging parameters of a user’s password.

groupmod : this command can modify attributes of an existing group.

**Chapter 8**

## 107.2 Automate System Administration Tasks by Scheduling Jobs

Cron:

crontab used to view and edit user's cron table file.  
 /etc/cron.hourly,daily,weekly,monthly  
 pre-existing drirectories that will run script files a set intervals such as ho,w,d,m

/etc/cron.d  
 containts cron jobs for system

/etc/cron.deny users listed in this file will be prevented from using contabs.

man 4 crontabs

crontab -l, -r, -e

At:

at command will let you schedule a one time job at a specific time. at 4:00 AM tomorrow  
  
 atq  
 les you view your job queue.  
  
 atrm 3   
 remove a scheduled job u

Systemd timer unit files:

monotonic

realtime

**Chapter 9**

## 107.3 Localization and Internationalization

Working with the system’s Locale

Locale: command that displays loacale information

Localectl : set the defult system language and character encoding

UTF-8 : this is the dominant character encoding type for character on computers. This character encoding is part of the unicode standard.

ISO-8859: character encoding format used throughout the world, however UTF-8 is much more prominent.

Iconv: utiliy that can be used to convert files from one character encoding to another

To set the diffenent language command is : LANG=lan\_name.encoding

Ex: LANG=pl\_PL.utf8

To know the file encoding command is : file -I filename

Time and Date on the Linux system:

Date: this command will display the current date and time in multiple formates and to set the date and time.

Timedatectl: this command will display the current date and time setting and will alow the updating of the system time and RTC clock.

Tzselect: this is a menu driven command that will assist in finding a region’s time zone

TZ : enviroment variable for a time zone that can be used in a script or a user’s bash profile.

/etc/localtime : on red hat based distributiond this is a symbolic link that points back to /user/share/zoneinfo/<time zone> as the system’s time zone setting

/etc/timezone : on debian based distributions, this file contains a system’s configured time zone setting

/user/share/zoneinfo : the directory that contains all of the available time zones that a computer could potentially use for its settings.

**Chapter 10**

## 108.1 Maintain System Time

Working with remote time severs:

Ntpd: the network time protocol daemon. This is the service that checks upstream time servers for the correct time.

Ntpdate: command that can query a specified NTP server anf receive a new time. Make sure that ntpd is not runniing prior to using this command.

/etc/ntp.conf : primary configuration file for the ntpd daemon

Ntpd: this command can query the ntpd daemon for various bits of information.

Timedatectl : the status of the system’s configuration with an NTP server can be checked with this command. To enable NTP synchronization use the ‘set-ntp on’ switch

Chronyd: the modern NTP daemon used on computrers that utilize systemd.

/etc/chrony/chrony.conf : configuration file for the chronyd daemon. This file has a very similar syntax to the ntpd.conf file

Chroyc : this command is used tp query the chronyd daemon for information on upsteam NTP servers.

Chapter 11

## 108.2 System Logging

[Legacy Logging Systems](https://learn.acloud.guru/course/17fdc90a-5a2f-406d-b221-097e881b46bc/learn/b1d582ae-4434-42f7-9130-0e825caa5457/7744c980-3757-4fea-979e-40034ebf6f18/watch)

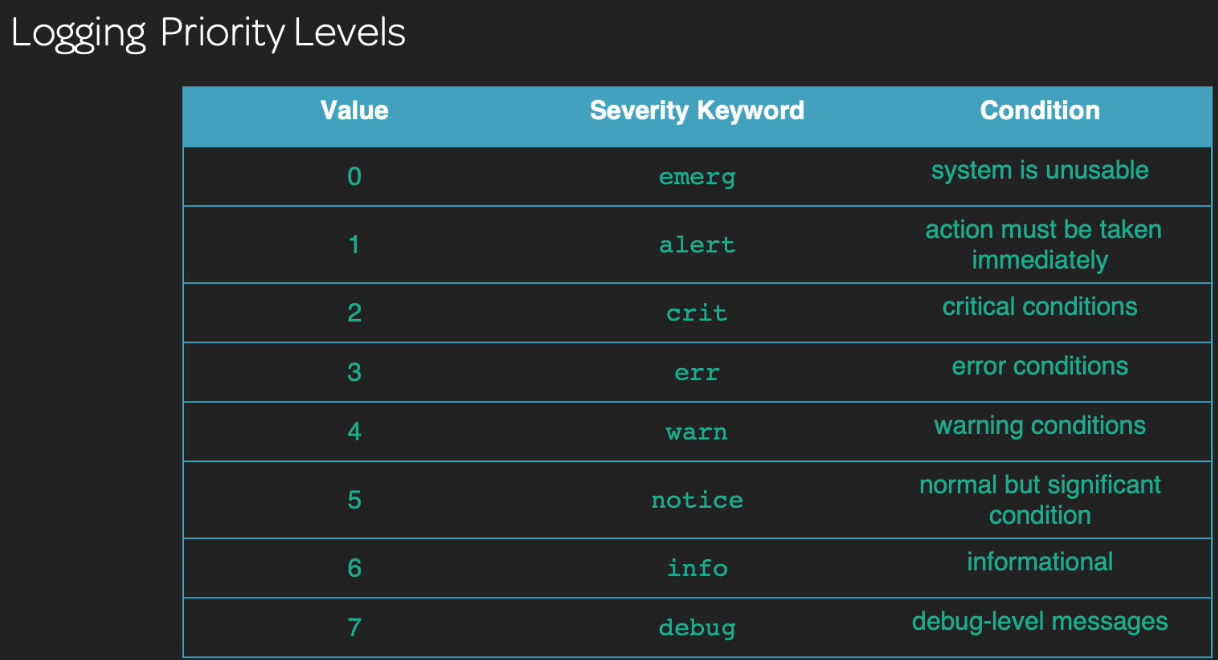
/var/log/dmesg : linux kernel boot messages

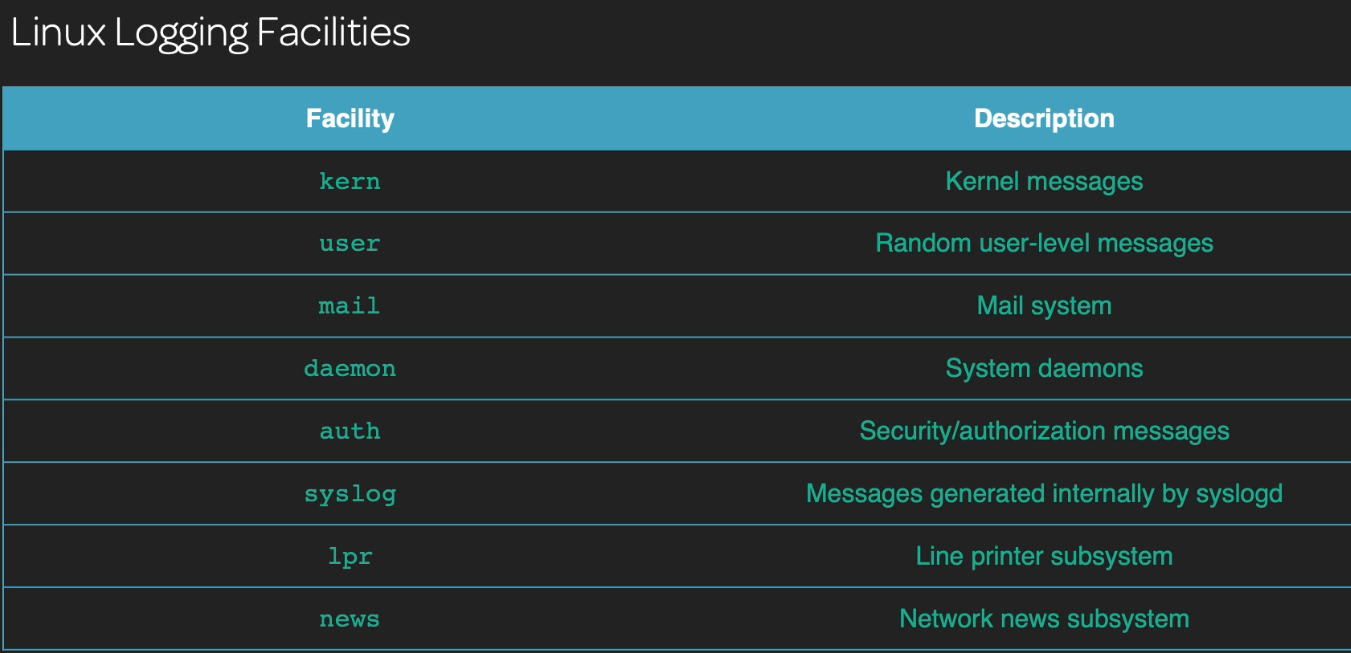
/var/log/messages: standard system log messages

/var/log/secure : security log messages, containing information on login attempts

/var/log/maillog : local email log messages (from and to this server)

On systems that are not using sysyemd, these logs are managed by rsyslog





Dmesg: A utiliy that allows an administrator to view the /var/log/dmesg file in a text pager.

Logger : command that can be used to send information to the /var/log/messages log file.

**Rsyslog**

/etc/rsyslog.conf : this is the main configuration file for the rsyslog logging daemon.

/etc/logrotate.conf : this is the main configuration file for the lograte daemon that is responsible for managing the storage and rotation of old log files.

/etc/logotate.d/ : Extra logrotate configurations for other daemons can be placed here.

Logrotate : the logrotate command will rotate logs based on the specified configuration file.

**Indroduction to the systemd journal:**

What the journal collects:

\* kernel log messages

\* system log messages, the same as what syslog would collect

\* system services that send output to standard output and standard error

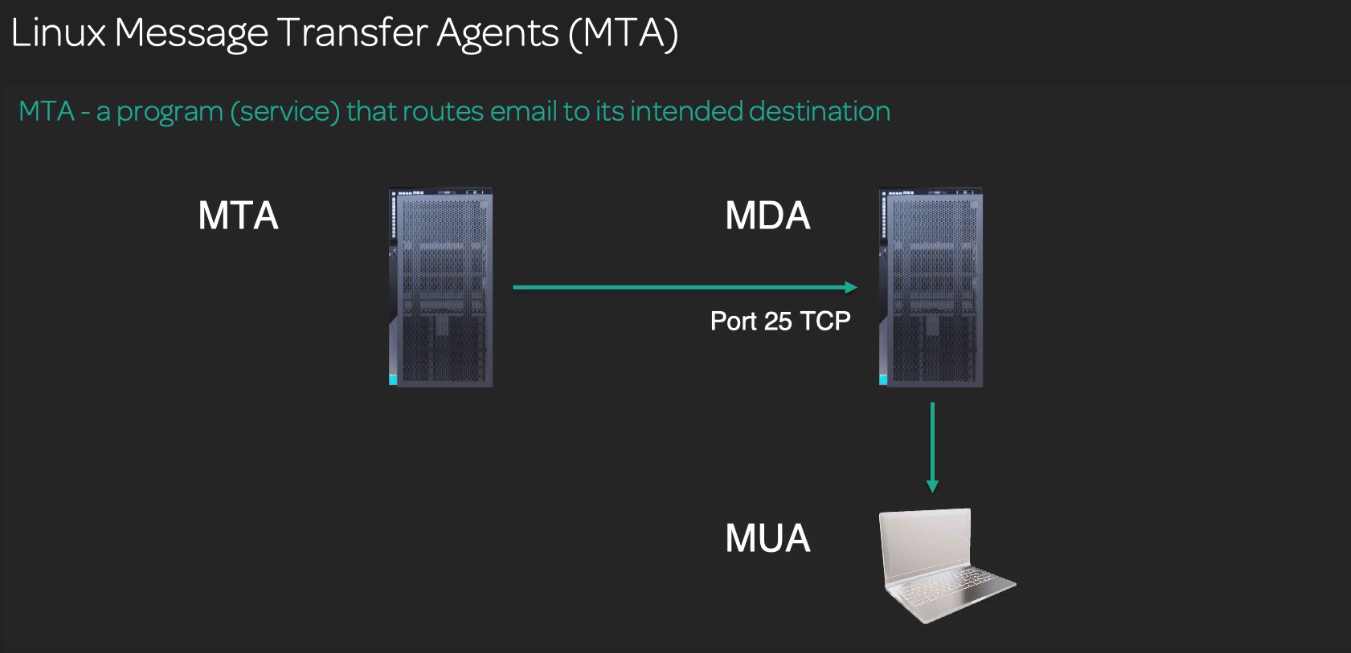
\* Audit records for SELinux messages.

The default location for the journal is /run/log/

**Chapter 12**

## 108.3 Mail Transfer Agent (MTA) Basics

Basics of a message transfer agent:



Sendmail : one of the oldest MTA systems around was default on many linux distributions, notoriously difficult to configure

Postfix : modern MTA found on many linux distributions, simpler to configure, greate security

Exim : used to be the default MTA for debian based distributions, has a good security record, easier to configure than sendmail

Sendmail Emulation layer: system administrators can use ‘sendmail’ style commands on other MTA’s (postfix,exim , etc) as if they were managing a sendmail installation

Email forwarding and Aliases :

/etc/aliases : this is a plain-text file that can be modified to to set up forwarding addresses for users on a system

Newaliases : After a modification to the /etc/aliases file is performed the newaliases command will then regenerate the /etc/aliases.db file that the MTA uses for maill delivery.

Mail: the mail command can be used to send an mail to a user from the command line or to view the email of a user on the system.

Mailq : the mailq command is used to view the mail that resides in the email queue , waiting to be sent to its destination.

~/.forward : A local configuration file that can be set up within a user’s home diretory to forward email destined for itfself to sent to another user and/or an external email address.

**Chapter 13**

## 108.4 Manage Printers and Printing

The common unix printing system (CUPS)

http://localhost:631 : this is the default URL for the locally intall CUPS server. It will require a root login to add or remove printers here.

/etc/cups : Directory that contains the configuration files for the cups print sever daemon and printer settings. It is preferable to use the web interface to manage the configuration files located in this directory.

The line print Daemon :

Ipstat : Displays the status of CUPS server and configured printers and queues.

Ipadmin : administrator’s tool to add, modify, and delete printers.

Ipinfo: this command displays available printer devices and drivers that can be used

Ipc: olde command that can be used to view information about installed printers. The status command will show the status of all installed printers.

Lpr: this command sends a print job to the default printer. To specify a different printer use the –P switch followed by the printer name

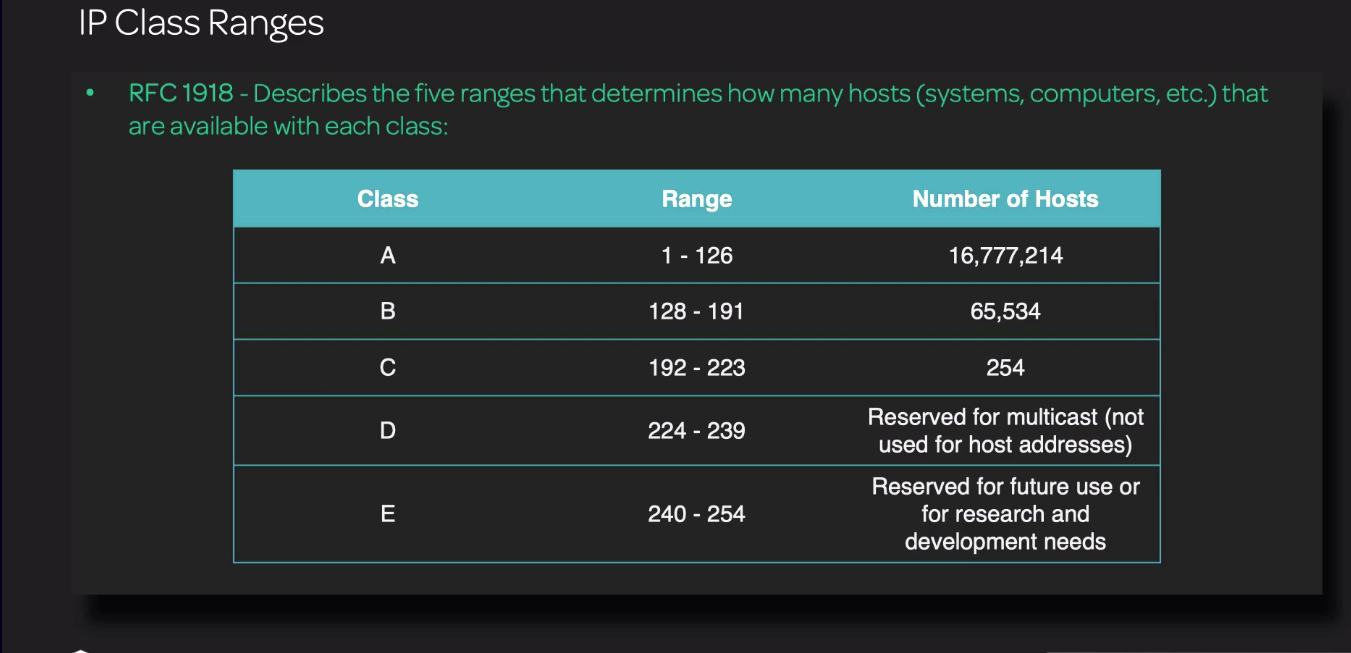
Lpq: this command displays the cups printer queue. Use the –a option to view all print queues.

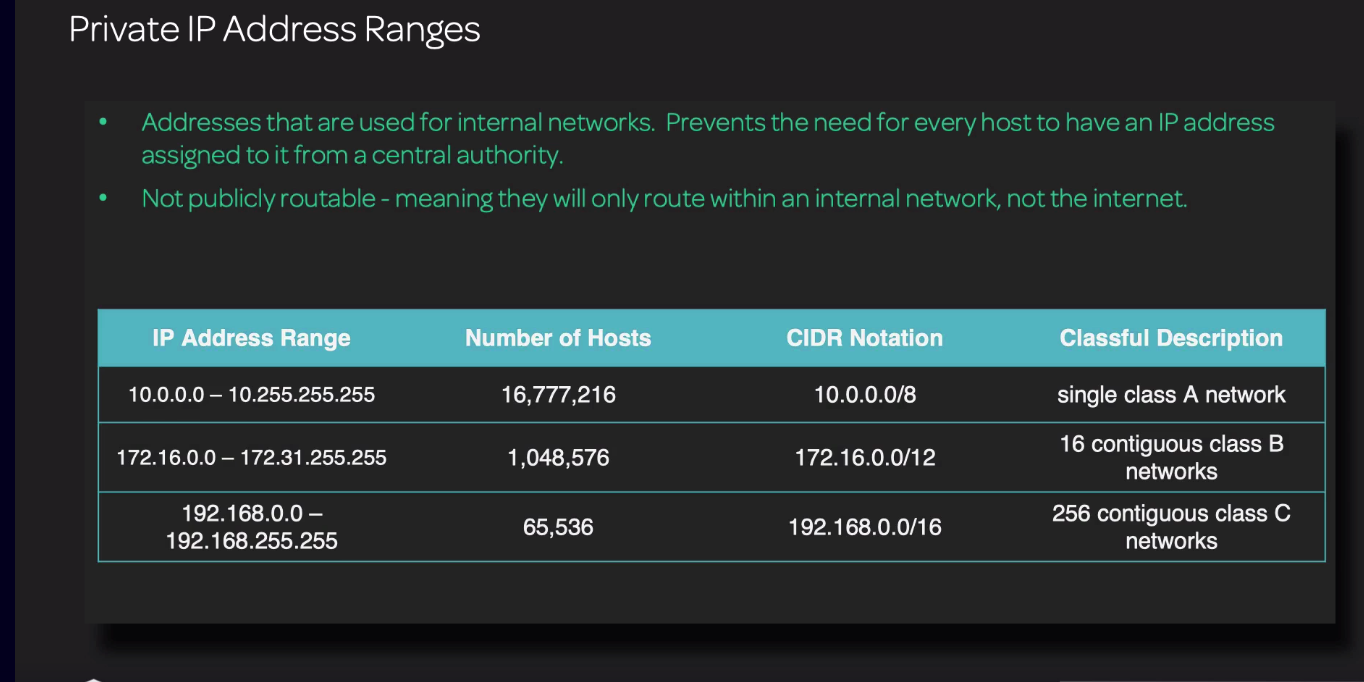
Lprm: this command will remove a print job from the print queue. A job ID must be specified. To remove all jobs from the queue just pass a ‘-’ to the command.

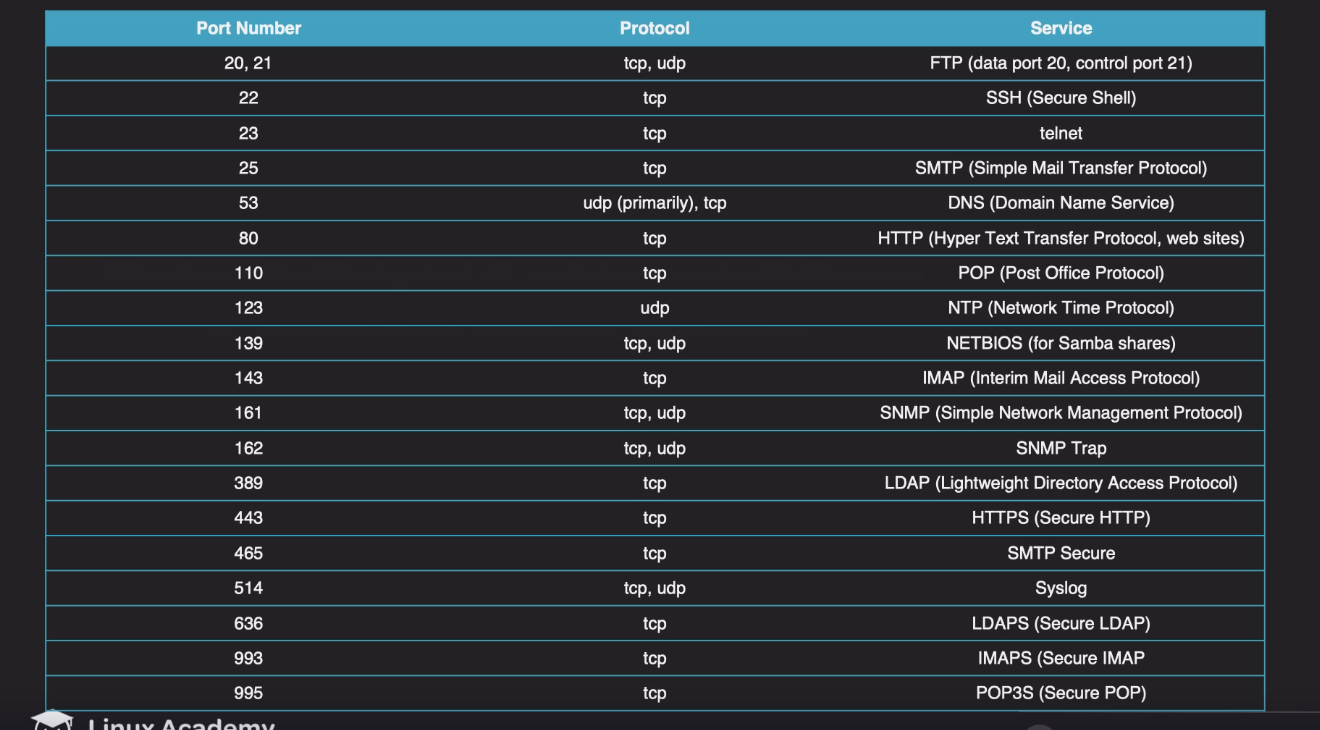
Chapter 14

## 109.1 Fundamentals of Internet Protocols

Notworkint fundamentals:







**Chapter 15**

## 109.2 Persistent Network Configuration

NetworkManger:

Nmcli: the networkManager command line interface. This is the command line utility used for configuring network devices and their connection settings.

Nmcli dev : this is short ‘device’ which is the physical hardware that we use to connect to a network.

Nmcli con : this is short of connection which contains the network configuration settings assigned to a particular device. We assign out IP address And DNS settings to a connection

Ip : this command can modify IP address settings route setting and show interface statistics. This is from the iproute2 project.

Ip addr show : displays IP address information  
 ip route show : displays the routing table

Ip –s addr : show statistics on configured interfaces

Hostnamectl : command that is used to persistently configure the computer’s host name.

Legacy networking tools:

Ifconfig: the previous standard networking utility for linux. This command has been deprecated in favor of the ip command

Ifdown: this command is used to bring down a specific network interface

Ifup: this command is used to bring up a specific network interface.

Route: this utility will display the routing table and add and delete routes. It has been deprecated in Favor of the ip route command

**Chapter 16**

109.3 Basic Network Troubleshooting

Testing connectivity

Ping : this command is used to test a system’s ability to communicate with another network device by sending LCMP packets across the network.

Ping6 : provides the same functionality as ping by but defaults to IPv6 packerts instead.

Traceroute : Displays a listing of the ‘hops’ a packet will traverse to get to a destination. Used to verify network routing and to look for breaks in network communicaton.

Ttraceroute6: this is the IPv6 equivalent of the traceroute command.

Tracepath: a modern relacement for the traceroue command, but utilizes UDP packets instead of ICMP.

Tracepath6: the IPv6 equivalent of the traceroute command

Netstat: this command is used to display network connections and their state on a system. Can also be used to view the routing table. Part of the ‘net-tools’ package since it is deprecated.

Ss : modern eqnivalent of the netstat command. This command does not show the routing table.

**Chapter 17**

## 109.4 Configure Client-Side DNS

/etc/hosts : a text file that will contain the localhost entry mapped to the loopback addresses( both IPv4 and IPv6). This file can also be used to map other hostname to IP addresses.

/etc/hostname : systems will use this file for a computer;s hostname. The hostnamectl file will write a system’s new hostname to this file.

/etc/reslov.conf : this file contaons the IP address od DNS name servers that the host will use for name resolution.

/etc/nsswitch.conf : among other tasks, this file is used to determine the order in which name resolution occurs.

Host : this command is used to reslove domain names to IP addresses.

Dig: this command is used to query DNS servers for particular types of DNS records.

Gerent: this command directly queries the /etc/nsswitch.conf file and its corresponding database locations for information.

**Chapter 18**

110.1 Perform Security Administration Tasks

Determine the current security state of a system

Who : list out the currently logged in users on a system.

w : this command will also list the currently logged in users, but can also show what processes they are currently running.

Last : this command shows a listing of users who were logged into the system(but are now logged out ). to find out what users had failed login attempts, use :

last –f /var/log/btmp

Lsof : this command can be used to determine what files are currentl opened on the system. Also, network ports are considered files in linux, so opend network ports can be found with this command as well.

Find : this find command can be used to locate all files that have the SUID or SGID bit set on them:

Find / -pren –u+s

Ulimit: this command can be used to set limits on the amount of resources in a system that a user can utilize.

Chage : change the user’s password expiration information.

Passwd: this command sets a user’s password.

/etc/sudoers : the default configuration file for configuring users and/or groups that are granted elevated privileges. Use the visudo command to edit this file.

Sudo : the sudo command allows a user to run a command as root, or as another user. This command is typically applied to a user pr group to allow elevated privileges.

Su : the substitute user command. Provide a dash(-) to assume a login shell of the specified user. If no user is specified, the root user is assumed.

Checking local network security:

Lsof this command can be used to determine what files are currently opened on the system. Also network ports are considered files in linux, so opened network ports can be found with this command as well, use the following to find out what network ports are open:

lsof -I

Fuser: this command can be used to list all PID’s that are assidned to a particular file or network port that is in use.

Netstat, ss: use the following switches to view active connections(TUNA):

-t = TCP connections

-u = UDP connections

-n = show IP addresses instead of hostmanes

-a = show listening and non- listening socketsl

Nmap : the network map command is used to scan a host for open ports and services.

**Chapter 19**

110.2 Set Up Host Security

Securing local logins:

/etc/nologin : this file can be used to display a message on the console when someone attempts to log in with an account that is using the /sbin/nologin shell.

Securing network services:

Xinetd: the “super-daemon”. The xinetd daemon controls access to variois network services.

TCP Wrappers: this functionality utilizes a hosts.allow and/or a hosts.deny file to determine acess to network services.

Systemd.socket : A systemd socket unit file is used in place of xinetd on modern linux distributions. This type of unit will allow for on-demand activation of network services. TCP Wrappers can be used in conjuction with systemd socket units.

**Chapter 20**

110.3 Securing Data with Encryption

GPG(GNU privacy Guard):

Gpg: this command is used to generate, list, import, export and revoke gpg keys.

gpg –gen-key : starts the process to generate a new gpg public key.

gpg --export: used to export a public gpg key.

gpg –import: used to import another user’s public key into your keyring

Gpg –list –keys : list the gpg keys on your keyring

Gpg –e file\_name: Encrypt a file with your default gpg public key.

Gpg file\_name : Decrypt a file from a user

~/.gnupg: hidden directory within each user’s home folder that contains the gpg keyring and configuration files for GPG keys.

SSH(secure shell):

Ssh : the secure shell command. This allows us to make secure, encrypted connections to remote systems.

Ssh-copy-id : this command will copy our public ssh key to another system, anf set up the proper permissions for the authorized\_keys file on the remote host.

Ssh-agent : this command acts as a wrapper around an enviroment so that it can handle authentication for key files that use passphrases.

Ssh-add : this command adds the passphrase to the ssh-agent.