School of Computer Science Engineering and Technology
Bennett University (The Times Group)

Program- BTech-3rd Semester
Course Code- CSET213
Year- 2025
Date- 11/08/2025

Type- Sp. Core-I
Course Name-Linux and Shell Programming
Semester- Odd
Batch- Cyber Security (B01-B14)

Lab Assignment 8

Exp No	Name		CLO Achieved			Marks
		CO1	CO2	CO3	CO4	
1	Linux Commands-Networking Commands	√				2

Objective: To Learn Linux networking commands for network setting, administration, and security.

Outcomes: After successful execution of this lab, the students will be able to do network setting, administer, and check security using commands.

Network Setting Configuration Commands

Command Syntax Purpose Covered in

Command	Syntax	Purpose
ip	ip [options]{object} [subcommand]	Display IP address, subnet mask, and MAC address settings.
ifconfig	ifconfig [options] [interface]	Display current IP address information for each NIC recognized by the system.
iwconfig	iwconfig [options] [interface]	Provide wireless NIC configurations and settings.
nmcli	nmcli [options] [subcommand] [arguments]	View and manage network settings.
ethtool	ethtool [options] {device name}	Manage NIC driver and network configurations.
hostnamectl	hostnamectl [options] [subcommand][arguments]	View system's network hostname.
netcat	netcat [options]	Test connectivity and send data across network connections.
iftop	iftop [options] [-i {interface}]	Display bandwidth usage information.
traceroute	traceroute [options] {destination}	Report the network path between the source and destination computers.
tracepath	tracepath [options] {destination}	Report the network path between the source and destination computers.
resolvectl	resolvectl query {domain-name}	Manually query name resolution services.
dig	dig {domain name}	Test name resolution.
nslookup	nslookup {domain name}	Gather information about and test name resolution.
host	host {domain name}	Gather information about and test name resolution.
whois	whois [options] {domain name}	Display hostname, FQDN, IP address, and other information about a given host.
arp	arp [options]	Discover information about known MAC addresses.

Network Security Configuration Commands

Command	Syntax	Purpose
Iptables	iptables [options][-t table][commands] {chain/rule specification}	Manage packet filtering and stateful firewall functions.
firewall-cmd	firewall-cmd [options]	Configure firewall by querying and modifying zones or services as desired.
Ufw	ufw [options] {action}	Configure iptables.
Ping	ping [options] {destination}	Generate a response request from the sending computer, which should receive a reply from the destination computer.
Traceroute	traceroute [options] {destination}	Display each hop along the network path.
Tracepath	tracepath [options] {destination}	Display each hop along the network path.
Mtr	mtr [options] [hostname]	Test network connection quality
netstat	netstat [options]	Gather information about TCP connections to the system.
Ss	ss [options]	Gather information about TCP connections and display in a simple output.
Tcpdump	tcpdump [options] [-i{interface}] [host {IP address}]	Determine traffic type and content.
Nmap	nmap [options] [target]	Report extremely detailed information about a network.

Security Management Commands

Command	Syntax	Purpose
md5sum	md5sum[options] [file name]	Calculate the hash value of a file with the MD5 hash function.
sha#sum	sha#sum[options][file name]	Calculate the hash value of a file with the SHA hash function.
chcon	chcon{-u|-r|-t}{context value} {file or directory name}	Temporarily change the SELinux context of a resource.
apparmor_ status	apparmor_status	*No additional options or subcommands.* Display the current status of AppArmor profiles.
aa-complain	aa- complain{path to profile}	Place an AppArmor profile in complain mode.
aa-enforce aa-enforce	aa-enforce aa- enforce {path to profile}	Place an AppArmor profile in enforce mode.
aa-disable aa-disable	aa-disable aa-disable {path to profile}	Disable an AppArmor profile, unloading it from the kernel.
aa-unconfined	aa-unconfined	*No additional options or subcommands.* List processes with open network sockets that don't have an AppArmor profile loaded.

Problem1: Find out information about your network and get the following information:

a. Display IP address, subnet mask, and MAC address settings. (odd Number batch)
b. Display current IP address information for each NIC recognized by the system. (even number batch)
c. Display IP Address of www.google.com(odd Number batch)
d. Display MAC address of your machine(even number batch)
e. Display Network statistics (odd Number batch)
f. Calculate hash of a file using SHA (even number batch)
g. Display each hop between your machine and www.google.com (odd Number batch)
h. Display the Kernel IP routing table. (even number batch)

Problem2: Find the name of the service which uses TCP port 2605, as documented in /etc/services, and write the service name to the file /home/student/port-2605.txt. Find all the ports used for TCP services IMAP3 and IMAPS, again as documented in /etc/services, and write those port numbers to the file /home/student/imap-ports.txt. (All Batches)

Submission Instructions:

1. Submission requires the screen shots of all the incurred steps to execute a shell script or a video showing the whole process.
2. All these files are in single zip folder.
3. Use the naming convention: Prog_CourseCode_RollNo_LabNo.docx (Example: BCA3rdSem_CBCA221_ E21BCA002_Lab1.1)
4. Submission is through LMS only