Linux Command Cheat Sheet

Package Management		
sudo apt-get update	Refresh available updates	
sudo apt-get upgrade	Upgrade all packages	
sudo apt remove	Remove a package	
Sudo apt-get dist-upgrade	Upgrade Ubuntu version	
sudo apt-get install package	Install package with name package	
sudo apt-remove package	Remove package with name package	
sudo apt purge <package></package>	Purge package and configuration files.	
System I	nformation	
date	Show the current date and time	
whoami	Show current username	
User In	formation	
Id	Displays user & groups of current users	
sudo adduser username	To add a new user	
sudo useradd -m username	To add a new user with home directory	
sudo passwd username	Change password of user	
sudo usermod -aG sudo username	To add a new user with administrative privileges	
sudo addgroup groupname	To add a new group	
sudo addgroup developers	To add a group named "developers"	
sudo usermod -aG developers	To add a user named "username" to	
username	the "developers" group	
sudo userdel -r username	To delete user, home directory and mail spool	
Se	curity	
w	Display who is online	
change -I <users></users>	Get user password expiration date	
sudo passwd -l <user></user>	Lock a user account	
sudo passwd -u <user></user>	Unlock a user account	
passwd	Change user password	
Fail2Ban Security Tool		
sudo apt install fail2ban	Automatically detect and ban abusive IP addresses	
sudo fail2ban-client status	Show banned IP addresses	
sudo fail2ban-client status <jail></jail>	Show banned IP addresses	
Backup Application		
sudo apt install deja-dup	Deja Dup is a backup tool with secure encrypts and compress data.	

File Search		
II	List files with permissions and dates	
Locate <filename></filename>	Quick file search	
grep patern file	Search for pattern in file	
grep -r patern directory	Search recursively for pattern in	
	directory	
locate name	Find files and directories in name	
find /home/john -name 'prefix*/	Find files in /home/john that start with	
	"prefix"	
File Cor	mmands	
Is	List files and directories	
ls /path/to/directory	List files and directories in a specific	
	directory	
ls -l	Display detailed information about files	
ls -a	Display all files including hidden files	
ls -lr	Reverse the order of the sort	
ls –color	Colorize the output for better	
	readability	
ls >> output.txt	Export list to file called output.txt	
ls -l >> directory_listing.txt	Export the long format listing of	
	current directory to a file named	
	'directory_listing.txt'	
cp source_file destination	Copy files or directories	
mv source destination	Move (rename) files or directories	
rm file	Remove (delete) files or directories	
touch filename	Create an empty file	
nano filename	Use nano or vim as text editors to	
vim filename	create or edit files	
cat filename	Display content of a file	
Directory Commands and Navigation		
cd directory_path	Change directory	
cd	To go up one level of the directory tree	
cd	Go to the \$HOME directory	
cd /etc	Change to the /etc directory	
mkdir directory_name	Create a new directory Remove an	
	empty directory	
rmdir directory_name	Remove an empty directory	
pwd	Display the current directory	

Linux Command Cheat Sheet

networkctl status hostname hostname Get the IP address of all interfaces hostname Display all IP addresses of the host ip address show Check IP Address ip -a Display all network interfaces and IP address show ip -a Display all network interfaces and IP address ip route show Display the routing table ping google.com (ping 8.8.8.8) Check Network Connectivity ping host ip route show Check the routing table ip route get <ip> Which route will be used to reach host traceroute google.com Trace the route to a destination and identify potential issues whois domain Display bns information for domain dig domain Display DNS information for domain host domain Networking Troubleshooting sudo systemctl restart networking sudo systemctl restart networkd Restart Networking (newer version) sudo systemctl restart networkd Restart Networking (newer version) Flush DNS cache sudo dhclient sudo dhclient sudo dhclient sudo systemctl restart NetworkManager Fierwall sudo apt install ufw Install UFW (Uncomplicated Firewall) sudo ufw enable Turn on the firewall sudo ufw disable Turn off the firewall sudo ufw status Current status and rules sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 43 Allow 443 for HTTPS sudo ufw default allow Allow 41 connections by default propositions by default</ip>	Networking		
hostname -I ip address show Check IP Address ip -a Display all network interfaces and IP address ip route show Display the routing table ping google.com (ping 8.8.8.8) Check Network Connectivity ping host Send ICMP echo request to host ip route show Check the routing table proute get <ip>Which route will be used to reach host traceroute google.com Trace the route to a destination and identify potential issues whois domain Display Whois information for domain dig domain Display DNS IP address for domain Networking Troubleshooting sudo systemctl restart networking sudo systemctl restart networking sudo systemctl restart networkd Restart Networking (newer version) Flush DNS cache sudo dhclient -r sudo dhclient -r sudo systemctl restart NetworkManager Firewall sudo apt install ufw Install UFW (Uncomplicated Firewall) sudo ufw enable Turn on the firewall sudo ufw disable Turn off the firewall sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default</ip>	networkctl status	Get the IP address of all interfaces	
ip address show ip -a Display all network interfaces and IP address ip route show Display the routing table Display for equest to host Display the routing table Display her outing table Display echo request to host Display echo request to host Display echo request to host Display enter out to a destination and identify potential issues Display whois information for domain Display whois information for domain Display DNS IP address for domain Disp	hostname	Get the IP address of all interfaces	
ip -a Display all network interfaces and IP address ip route show Display the routing table ping google.com (ping 8.8.8.8) Check Network Connectivity ping host Send ICMP echo request to host ip route show Check the routing table ip route get <ip>Which route will be used to reach host traceroute google.com Trace the route to a destination and identify potential issues whois domain Display bnos information for domain host domain Display DNS IP address for domain DNS IP address for d</ip>	hostname -l	Display all IP addresses of the host	
ip route show ping google.com (ping 8.8.8.8) Display the routing table ping google.com (ping 8.8.8.8) Check Network Connectivity ping host Send ICMP echo request to host ip route show Check the routing table ip route get <ip>Which route will be used to reach host traceroute google.com Trace the route to a destination and identify potential issues Whois domain Display whois information for domain Display DNS information for domain Display DNS IP address for domain Networking Troubleshooting sudo systemctl restart networking Restart Networking (newer version) sudo systemctl restart networkd Restart Networking (newer version) Flush DNS cache sudo dhclient - sudo systemctl restart NetworkManager Request new IP lease sudo dhclient Sudo apt install ufw Install UFW (Uncomplicated Firewall) sudo ufw enable Turn on the firewall sudo ufw disable Turn on the firewall sudo ufw reset Reset the firewall rules to their default sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 443 Allow 443 for HTTPS Allow all connections by default</ip>	ip address show	Check IP Address	
ping google.com (ping 8.8.8.8) ping host ip route show Check the routing table ip route get <ip> Which route will be used to reach host traceroute google.com mtr google.com whois domain dig domain bisplay by bis information for domain bost domain Networking Troubleshooting sudo systemctl restart networking sudo systemctl restart networkd sudo systemd-resolveflush-caches sudo dhclient -r sudo dhclient -r sudo dystemctl restart NetworkManager Firewall sudo apt install ufw sudo ufw enable sudo ufw reset sudo ufw status sudo ufw allow 22 sudo ufw allow 243 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default</ip>	ip -a		
ping host ip route show Check the routing table ip route get <ip> Which route will be used to reach host traceroute google.com Trace the route to a destination and identify potential issues whois domain Display whois information for domain dig domain Display DNS information for domain Display DNS IP address for domain Networking Troubleshooting sudo systemctl restart networking sudo systemctl restart networkd Restart Networking (newer version) sudo systemd-resolveflush-caches sudo dhclient -r sudo dhclient sudo systemctl restart NetworkManager Firewall sudo apt install ufw Sudo ufw enable Sudo ufw disable Sudo ufw reset Sudo ufw status Sudo ufw allow 22 Allow 22 for SSH Sudo ufw default allow Allow 443 for HTTPS Sudo ufw default allow Allow all connections by default</ip>	ip route show	Display the routing table	
ip route show ip route get <ip> ip route get <ip> Which route will be used to reach host traceroute google.com Trace the route to a destination and identify potential issues whois domain Display whois information for domain dig domain Display DNS information for domain host domain Display DNS IP address for domain Networking Troubleshooting sudo systemctl restart networking sudo systemctl restart networkd Restart Networking (newer version) sudo systemd-resolveflush-caches sudo dhclient -r sudo dhclient -r sudo systemctl restart NetworkManager Release current IP lease sudo systemctl restart NetworkManager Restarts network manager Firewall sudo apt install ufw Install UFW (Uncomplicated Firewall) sudo ufw enable Turn on the firewall sudo ufw disable Turn off the firewall sudo ufw reset Reset the firewall rules to their default sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default</ip></ip>	ping google.com (ping 8.8.8.8)	Check Network Connectivity	
ip route get <ip>Which route will be used to reach host traceroute google.com</ip>	ping host	Send ICMP echo request to host	
traceroute google.com mtr google.com whois domain dig domain host domain Networking Troubleshooting sudo systemctl restart networkd sudo dhclient -r sudo dhclient -r sudo apt install ufw sudo apt install ufw sudo ufw enable sudo ufw reset sudo ufw reset sudo ufw status sudo ufw allow 22 sudo ufw allow 243 sudo ufw default allow Trace the route to a destination and identify potential issues Irace the route to a destination and identify potential issues Irace the route to a destination and identify potential issues Identify potential issues Identify potential issues Insplay NNS information for domain Display DNS information for domain Display DNS IP address for domain Networking Troubleshooting Restart Networking Restart Networking (newer version) Flush DNS cache Release current IP lease Request new IP lease Restarts network manager Firewall sudo apt install ufw Install UFW (Uncomplicated Firewall) Sudo ufw enable Turn on the firewall Sudo ufw disable Turn off the firewall Sudo ufw status Current status and rules Sudo ufw allow 22 Allow 22 for SSH Allow 43 for HTTP Sudo ufw default allow Allow all connections by default	ip route show	Check the routing table	
mtr google.com identify potential issues whois domain Display whois information for domain dig domain Display DNS information for domain host domain Display DNS IP address for domain Networking Troubleshooting sudo systemctl restart networking Restart Networking (newer version) sudo systemctl restart networkd Restart Networking (newer version) sudo systemd-resolveflush-caches sudo dhclient -r Release current IP lease sudo dhclient Request new IP lease sudo systemctl restart NetworkManager Restarts network manager Firewall sudo apt install ufw Install UFW (Uncomplicated Firewall) sudo ufw enable Turn on the firewall sudo ufw disable Turn off the firewall rules to their default sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 80 Allow 80 for HTTP sudo ufw default allow Allow all connections by default	ip route get <ip></ip>	Which route will be used to reach host	
whois domain dig domain host domain Display DNS information for domain Display DNS IP address for domain Display DNS IP address for domain Networking Troubleshooting sudo systemctl restart networking sudo systemctl restart networkd Restart Networking (newer version) sudo systemd-resolveflush-caches sudo dhclient -r Release current IP lease sudo dhclient Request new IP lease sudo systemctl restart NetworkManager Restarts network manager Firewall sudo apt install ufw Install UFW (Uncomplicated Firewall) sudo ufw enable Turn on the firewall sudo ufw disable Turn off the firewall rules to their default sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 80 Allow 80 for HTTP sudo ufw default allow Allow all connections by default	traceroute google.com	Trace the route to a destination and	
dig domain host domain Display DNS IP address for domain Networking Troubleshooting sudo systemctl restart networking sudo systemctl restart networkd sudo systemd-resolveflush-caches sudo dhclient -r sudo dhclient sudo systemctl restart NetworkManager Firewall sudo apt install ufw sudo ufw enable sudo ufw disable sudo ufw reset sudo ufw status sudo ufw allow 22 sudo ufw allow 80 Allow 80 for HTTPS sudo ufw default allow Networking (newer version) Restart Networking Restart Networking Restart Networking Restart Networking Restart Networking Install UFW (Uncomplicated Firewall) Turn on the firewall Sudo ufw enable Sudo ufw disable Turn off the firewall Sudo ufw status Allow 22 for SSH Allow 443 for HTTPS Sudo ufw default allow Allow all connections by default	mtr google.com	identify potential issues	
Networking Troubleshooting sudo systemctl restart networking sudo systemctl restart networkd sudo systemctl restart networkd Restart Networking (newer version) sudo systemd-resolveflush-caches sudo dhclient -r Release current IP lease sudo dhclient Request new IP lease sudo systemctl restart NetworkManager Restarts network manager Firewall sudo apt install ufw Install UFW (Uncomplicated Firewall) sudo ufw enable Turn on the firewall sudo ufw disable Turn off the firewall rules to their default sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default	whois domain	Display whois information for domain	
Networking Troubleshooting sudo systemctl restart networking sudo systemctl restart networkd sudo systemctl restart networkd sudo systemd-resolveflush-caches sudo dhclient -r sudo dhclient sudo systemctl restart NetworkManager Request new IP lease sudo systemctl restart NetworkManager Restarts network manager Firewall sudo apt install ufw Install UFW (Uncomplicated Firewall) sudo ufw enable Turn on the firewall sudo ufw disable Turn off the firewall sudo ufw reset Reset the firewall rules to their default sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 80 Allow 80 for HTTP sudo ufw default allow Allow all connections by default	dig domain	Display DNS information for domain	
sudo systemctl restart networking sudo systemctl restart networkd Restart Networking (newer version) sudo systemd-resolveflush-caches sudo dhclient -r Release current IP lease sudo dhclient Request new IP lease sudo systemctl restart NetworkManager Restarts network manager Firewall sudo apt install ufw Install UFW (Uncomplicated Firewall) sudo ufw enable Turn on the firewall sudo ufw disable Sudo ufw reset Reset the firewall rules to their default sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 80 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default	host domain	Display DNS IP address for domain	
sudo systemctl restart networkd sudo systemd-resolveflush-caches sudo dhclient -r sudo dhclient sudo systemctl restart NetworkManager sudo systemctl restart NetworkManager Firewall sudo apt install ufw sudo ufw enable sudo ufw disable sudo ufw reset sudo ufw status sudo ufw status sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 443 sudo ufw default allow Restart Network manager Restarts network manager Firewall Install UFW (Uncomplicated Firewall) Turn on the firewall Turn off the firewall sudo ufw status Sudo ufw reset Reset the firewall rules to their default sudo ufw allow 22 Allow 22 for SSH Allow 443 for HTTPS sudo ufw default allow Allow all connections by default	Networking Tr	oubleshooting	
sudo systemd-resolveflush-caches sudo dhclient -r sudo dhclient sudo dhclient sudo systemctl restart NetworkManager Firewall sudo apt install ufw sudo ufw enable sudo ufw disable sudo ufw disable sudo ufw reset sudo ufw status sudo ufw status sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Flush DNS cache Release current IP lease Request new IP lease Restarts network manager Turn on the firewall Turn on the firewall Turn off the firewall Sudo ufw disable Sudo ufw reset Reset the firewall rules to their default Sudo ufw allow 42 Allow 443 for HTTPS Sudo ufw default allow Allow all connections by default	sudo systemctl restart networking	Restart Networking	
sudo dhclient -r sudo systemctl restart NetworkManager Firewall sudo apt install ufw sudo ufw enable sudo ufw disable sudo ufw reset sudo ufw status sudo ufw status Sudo ufw allow 80 sudo ufw allow 443 sudo ufw default allow Release current IP lease Request new IP lease Restarts network manager Firewall Install UFW (Uncomplicated Firewall) Turn on the firewall Turn off the firewall Sudo ufw disable Turn off the firewall rules to their default Sudo ufw status Sudo ufw status Sudo ufw allow 22 Allow 22 for SSH Allow 443 for HTTPS Sudo ufw default allow Allow all connections by default	sudo systemctl restart networkd	Restart Networking (newer version)	
sudo dhclient sudo systemctl restart NetworkManager Firewall sudo apt install ufw sudo ufw enable sudo ufw disable sudo ufw reset sudo ufw reset sudo ufw status sudo ufw status sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Request new IP lease Restarts network manager Install UFW (Uncomplicated Firewall) Turn on the firewall Turn off the firewall Current firewall rules to their default Sudo ufw status Sudo ufw allow 22 Allow 22 for SSH Allow 443 for HTTPS Allow 443 for HTTPS Sudo ufw default allow Allow all connections by default	sudo systemd-resolveflush-caches	Flush DNS cache	
sudo systemctl restart NetworkManager Firewall sudo apt install ufw sudo ufw enable sudo ufw disable sudo ufw reset sudo ufw status sudo ufw status sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default		Release current IP lease	
Firewall sudo apt install ufw Install UFW (Uncomplicated Firewall) sudo ufw enable Turn on the firewall sudo ufw disable Turn off the firewall sudo ufw reset Reset the firewall rules to their default sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 80 Allow 80 for HTTP sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default	sudo dhclient	Request new IP lease	
sudo apt install ufw sudo ufw enable sudo ufw disable sudo ufw reset sudo ufw reset sudo ufw status sudo ufw allow 22 sudo ufw allow 80 sudo ufw allow 443 sudo ufw allow 443 sudo ufw disable Allow allow allow 443 sudo ufw allow 443 sudo ufw allow 443 sudo ufw default allow Allow allow allow allow 443 Allow allo		_	
sudo ufw enable sudo ufw disable Turn off the firewall sudo ufw reset Reset the firewall rules to their default sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 80 Allow 80 for HTTP sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default			
sudo ufw disable sudo ufw reset Reset the firewall rules to their default sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 80 Allow 80 for HTTP sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default			
sudo ufw reset sudo ufw status Current status and rules sudo ufw allow 22 Allow 22 for SSH sudo ufw allow 80 Allow 80 for HTTP sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default	sudo ufw enable		
sudo ufw status Sudo ufw allow 22 Allow 22 for SSH Sudo ufw allow 80 Allow 80 for HTTP Sudo ufw allow 443 Allow 443 for HTTPS Sudo ufw default allow Allow all connections by default	sudo ufw disable		
sudo ufw allow 22 sudo ufw allow 80 Allow 80 for HTTP sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default	sudo ufw reset	Reset the firewall rules to their default	
sudo ufw allow 80 Allow 80 for HTTP sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default	sudo ufw status	Current status and rules	
sudo ufw allow 443 Allow 443 for HTTPS sudo ufw default allow Allow all connections by default	sudo ufw allow 22	Allow 22 for SSH	
sudo ufw default allow Allow all connections by default	sudo ufw allow 80	Allow 80 for HTTP	
,	sudo ufw allow 443	Allow 443 for HTTPS	
sudo ufw default deny	sudo ufw default allow	·	
Sudo diw default defly Drop all connections by default	sudo ufw default deny	Drop all connections by default	
sudo ufw allow port Allow traffic on port	sudo ufw allow port	Allow traffic on port	
sudo ufw deny port Block port	sudo ufw deny port	Block port	
sudo ufw allow <app_name> To allow application profiles</app_name>	sudo ufw allow <app_name></app_name>	To allow application profiles	

Testing Latency, Download, and Upload Speeds		
sudo apt install speedtest-cli	Internet speed test software	
speedtest-cli	Run the speed test	
How to Chang	ge DNS Servers	
sudo nano /etc/resolv.conf	Change DNS Servers	
nameserver 8.8.8.8	Add the following lines to replace the	
nameserver 8.8.4.4	IP address with your preferred DNS	
	servers. Save and Exit.	
	Application	
sudo apt-get install clamtk	ClamTK is a GUI anti-virus app	
sudo apt install clamav-dameon	Install ClamAV's daemon (clamd)	
sudo freshclam	Update ClamAV's Virus Definitions	
sudo systemctl start clamav-daemon	Autostart the ClamAV Daemon (clamd)	
sudo systemctl enable clamav-daemon	Scan files, directories, or entire PC.	
clamscan -r /path/to/scan	Recursively scan all files in directory	
SSH L	ogins	
ssh host	Connect to host as your local username	
ssh user@host	Connect to host as user	
ssh -p port user@host	Connect to host using port	
ssh-keygen	Create a new SSH key pair	
File Permissions		
chmod	Connect to host as your local username	
chmod permissions filename	Changing permissions	
chmod u+rw file	Grant read and write permissions to	
	the owner	
chmod g-x file	Remove executive permission from the	
	Group	
chmod a=rx file	Set read & execute permissions for all	
Gnome Extension Shells & Customizing Themes		
sudo apt-get install gnome-tweaks	Install Gnome Tweaks	
Extension Manager	In Store, install extension manager	
Dash to Panel	Horizontal Dock	
Blur My Shell	Frosted blur effect	
User Themes	Change appearance of gnome shell	
www.gnome-look.org www.pling.com	Linux desktop themes and more	
Install VM Tool on Ubuntu Virtual Machine in VMware		
sudo apt-get install open-vm-tools-	Only applies to installation of VM Tool.	
desktop -y		