Linux Command Cheat Sheet

- Linux Network Command Cheat Sheet
- Linux Shell Scripting Command Cheat Sheet
- Linux Security Command Cheat Sheet

Part 3

Linux Network Command Cheat Sheet

Using Linux network commands, you can manage and troubleshoot network connections, interfaces, routing tables, and other networking-related functions.

Command	*Description*
arp	You can use this command to display and manipulate the kernel's ARP cache (Address Resolution Protocol).
ifconfig	This command displays and configures network interfaces on the system.
ip	You can use this command to display and manipulate routing, network devices, and tunnels.
netstat	This command is used to display active network connections, routing tables, and network interface statistics.
ss	This command is used to display information about active network connections and sockets.
ping	This command is used to test connectivity to a network device by sending ICMP (Internet Control Message Protocol) packets.
traceroute	This command is used to trace the path of network packets from the source to the destination.
mtr	This command is a network diagnostic tool that combines the functionality of ping and traceroute.
dig	This command is used to query DNS (Domain Name System) servers to resolve domain names into IP addresses.
host	This command is used to perform DNS lookups and display DNS-related information.
nslookup	This command is used to query DNS servers to resolve domain names into IP addresses.
route	This command is used to display and manipulate the IP routing table.
iptables	This command is used to configure the kernel firewall (netfilter) rules for packet filtering, NAT (Network Address Translation), and port forwarding.
nmap	This command is a network exploration and security auditing tool that can scan hosts and services on a network, and detect open ports and vulnerabilities.
tcpdump	Using this command, you can capture and analyze network traffic in real-time or from a packet capture file.
hostname	This command is used to display or set the hostname of the local system.

Linux Shell Scripting Command Cheat Sheet

Shell scripting commands are used to create scripts that automate tasks on Linux systems. The shell script is a program written in a scripting language that runs on the command line or from within another script.

Command	Description
echo	This command is used to print messages or variables to the standard output.
read	This command is used to read input from the user and store it in a variable.
if	This command is used to conditionally execute a block of code based on a specified condition.
else	This command is used to execute a block of code if the previous condition is not true.
elif	This command is used to execute a block of code if the previous condition is not true, but another condition is true.
while	This command is used to repeatedly execute a block of code as long as a specified condition is true.
for	This command is used to iterate over a list of items and execute a block of code for each item in the list.
case	This command is used to execute a block of code based on a specified value or pattern.
function	This command is used to define a reusable block of code that can be called multiple times with different parameters.
exit	This command is used to exit the shell or a script with a specified exit code.
test	This command is used to evaluate expressions or test conditions, such as file existence, equality, or numeric comparison.
expr	This command is used to evaluate mathematical expressions or manipulate strings.
cut	This command is used to extract a specific portion of a line or file based on a specified delimiter or field.
sed	This command is used to manipulate and transform text based on a specified pattern or regular expression.
awk	This command is used to process and manipulate text data using a series of patterns and actions.
grep	This command is used to search for a specific pattern or string in a file or output.
find	This command is used to search for files or directories that match a specified pattern or criteria.
xargs	This command is used to build and execute commands from standard input or arguments.

kill	This command is used to send signals to processes, such as terminating or restarting them.
ps	This command is used to display information about running processes on the system.
[and]	These are shorthand for the "test" command and are used to evaluate conditional expressions.
&& and ||	These are used to chain commands together and execute them conditionally based on the success or failure of the previous command.
$	This symbol is used to reference the value of a variable in the shell.
#	This symbol is used to comment out a line of code in a shell script.
cd	This command is used to change the current working directory.
ls	This command is used to list the contents of a directory.
touch	This command is used to create an empty file or update the modification time of an existing file.
mkdir	This command is used to create a new directory.
rm	This command is used to remove files or directories.
mv	This command is used to move or rename files or directories.
cp	This command is used to copy files or directories.
cat	This command is used to display the contents of a file or concatenate files.
grep	This command is used to search for a pattern in a file or stream.
awk	This command is used to manipulate and analyze text data.
cut	This command is used to extract specific columns or fields from a file or stream.
find	This command is used to search for files or directories that match certain criteria.
chmod	This command is used to change the permissions of a file or directory.
chown	This command is used to change the owner of a file or directory.
tar	This command is used to create or extract compressed archive files.
zip	This command is used to create or extract compressed zip archive files.
curl	This command is used to transfer data from or to a server.
wget	This command is used to download files from the internet.
export	This command is used to set an environment variable.
source	This command is used to execute a script within the current shell.
alias	This command is used to create a shortcut for a command or a set of commands.

Linux Security Command Cheat Sheet

The Linux Security command line interface manages security-related tasks on a Linux system. The commands in this section are used to create and monitor security features, as well as audit security on the system.

Command	Description
passwd	Users can use this command to change their passwords.
chpasswd	This command is used to change the passwords of multiple user accounts at once.
chroot	By using this command, you can create a virtualized system with limited resources.
chmod	It is used to change the permissions of a file or directory.
chown	It is used to change the owner of a file or directory.
su	This command is used to switch to another user account.
sudo	This command is used to execute a command as another user, usually the root user.
ssh	This command is used to establish a secure remote connection to another system.
scp	This command is used to securely copy files between systems.
sftp	This command is used to securely transfer files between systems.
iptables	This command is used to manage firewall rules and configurations.
netstat	This command is used to display active network connections and their status.
tcpdump	This command is used to capture and analyze network traffic.
nmap	This command is used to scan and detect open ports on a system or network.
fail2ban	This command is used to monitor log files and ban IP addresses that show suspicious activity.
lynis	This is a security auditing tool for Linux and Unix-based systems. It performs a system scan and provides a report of security issues, recommendations, and configuration errors.
snort	Snort is a free and open-source network intrusion detection system. It monitors network traffic and alerts administrators when it detects suspicious activity.
gpg	GNU Privacy Guard (GPG) is a free software implementation of the OpenPGP standard. It is used for encrypting and signing files and emails.
openssl	This command-line tool is used for encryption, decryption, and certificate management. It supports a wide range of cryptographic algorithms and protocols.

ufw	Uncomplicated Firewall (UFW) is a user-friendly front-end tool for managing iptable firewall rules. It simplifies the process of configuring firewall rules by providing a set of pre-configured profiles for common services and applications.
firewalld	This command-line tool manages firewall rules on Linux systems. It provides a dynamically managed firewall with support for network zones and services.
selinux	This is a security module that provides mandatory access control for Linux systems. It restricts access to resources based on the security context of processes and files.
chkrootkit	A command used for detecting rootkits and other types of malware on a Linux system.
rkhunter	A command used for detecting rootkits, backdoors, and other types of malware on a Linux system.
auditd	A command used for auditing and monitoring system activity. It records events and activities on the system, allowing you to investigate security incidents.
logwatch	This is a command used for analyzing log files and generating reports. It can be used to detect security breaches and other unusual activity.
tripwire	This command is used for file integrity monitoring. It detects unauthorized changes to critical system files and alerts you to potential security breaches.
apparmor	This is a security framework that provides mandatory access control for Linux applications. It can be used to limit the access of applications to critical system resources.
OpenSCAP	This command is used for system hardening and compliance checking. It provides a framework for assessing and improving the security posture of the system.
AIDE	This is an advanced intrusion detection system that monitors files and directories for changes. It can help detect unauthorized changes to system files, which may be a sign of a security breach.