Ubuntu Hardening Cheat Sheet

Comments are in parenthesis - ()
CLI commands start with a pound sign (in terminal) - #
Replace <text> with your query - "<text>" Examples: "apache"
Any vi command can be replaced with gedit for a gui editor

Task	Command
Updates - Gui	Search (ubuntu logo, top button on left hand pane)for the update manager and open it. While within the Update Manager, Settings -> Updates tab Check important and recommended updates Set automatic updates to Daily Click Close then check and install updates
Users	System Settings -> User Accounts Unlock (Lock on top right of page) Demote users (Click account type) Delete users (minus sign - on user)
Install Packages	# apt-get install vim (Editor) # apt-get install gufw (Ubuntu Firewall) # apt-get install clamav (Antivirus) # apt-get install rkhunter (Searches file system for rootkits and potential vulnerabilities) # apt-get install fail2ban (Manages SSH connections) # apt-get install auditd (audit policies) # apt-get install bum (Boot-up manager)
Disable Guest	#vim /etc/lightdm/lightdm.conf Look for "allow-guest=" and set it to false (Restart afterwards)
Check crontabs	# vi /etc/crontab (anacron is default) # cd /etc/cron.d/ (Check for unknown files) # cd /etc/cron.hourly/ # cd /etc/cron.daily/ # cd /etc/cron.weekly/ # cd /etc/cron.monthly/ # crontab -l

Password Policy	# gedit /etc/login.defs A text editor should open Ctrl-F and change the following: Search: PASS_MAX_DAYS Set: PASS_MAX_DAYS 90 Search: PASS_MIN_DAYS Set: PASS_MIN_DAYS 10 Search: PASS_WARN_AGE Set: PASS_WARN_AGE 7
Check Services	#ps aux (Checks for running services) #ps aux | grep "<service>" (Checks for a service) #losf -Pi (Shows services running and listening) #losf (Shows all services and their files)
Disable unnecessary services	# /etc/init.d/<service> stop # stop <service> # service <service> stop
Find SSH keys	#vim ~/.ssh/authorized_keys #vim /home/[user-name]/.ssh/authorized_keys
Check Log Files	# cd /var/log/ (Logs are stored in /var/log/) # ls (while in /var/log/) A series of log files should be listed. Important log files: auth.log syslog xorg.0.log Viewing Log files from CLI: # cat auth.log | less (| is located on the left hand side of the keyboard)
Check File Permissions	# ls -la (shows all files and permissions) # chmod 700 (Root - RWX Users - None Global - None) # chmod 750 (Root - RWX Users - RX Global - None) # chmod 755 (Root - RWX Users -RX Global - RX) # chmod 764 (Root - RWX Users -RW Global - R)

	R = Read W = Write X = Execute
Files to Check:	#ls -la /etc/shadow (Set Permissions: #chmod 0640) (Defaults: Root - RW User - R Global - none) #ls -la /etc/passwd (Set Permissions: #chmod 0644) (Defaults: Root - RW User - R Global - R) #ls -la /etc/pam.conf (Set Permissions: #chmod 0644) (Defaults: Root - RW User - R Global - R) #ls -la /etc/group (Set Permissions: #chmod 0644) (Defaults: Root - RW User - R Global - R)
rkhunter	Start rkhunter scan #rkhunter -c Log file is located in /var/log/rkhunter #cat /var/log/rkhunter/rkhunter.log | less
bum	To run the boot-up manager type in: #bum A management console should pop up with lightbulbs and checks. Disable (unclick the checkbox) and restart to remove malicious items from startup. (Google each item to see if it's necessary)
Clamav Utilization	Setup the Clam Database #sudo freshclam This should take a while to download and update files Perform a scan # clamscan -r / (Scans the entire filesystem)
Gufw Config	Search -> Firewall Configuration When gufw opens, Click the unlock button (lock) and authenticate Turn firewall on (Explicit and implicit denies can be added here)

auditd config	`#auditctl -e 1  (Enables audits)`