Linux Checklist: First Line of Defense

Set up initial firewall [iptables, ipfilter, ipfw, PF] allowing traffic on specific ports

Phase 2: Initial Defense		
Purpose	Command	Checked?
Make firewalls persistent Edit /etc/rc.local	`iptables-save > iptables.rules` `iptables-restore < /path/to/iptables.rules`	

Backup important directories and database	`sudo mkdir /data`
	`tar -czf /data/back.tar.gz \ {/home/etc,/var/www/html/}`
	`mysqldump -u root -p --all-databases > \ dump.sql`	

Hash backups	`find /data/back.tar.gz -type f -exec md5sum {} >> backup.tar.gz.md5 \;`	
Install tools	`apt-get install fail2ban nmap iptstate tshark clamav rkhunter sophos`	
Alias commands and log on usage in .bashrc	`alias gcc='echo `date`" gcc" >> /var/log/alias.log && exit'` `source .bashrc`	

Check for backdoors in
/etc/rc.local
/etc/init.d/
/etc/rc3.d/
And dot files
	`cat /etc/rc.local`
	`ls /etc/init.d/`
	`ls /etc/rc3.d/`
	`cat /home/{.bashrc, .login, .profile}`	

Check /etc/sudoers
and
/etc/ssh/sshd_config for vulnerable options
	`NOPASSWD`
	
	`PermitRootLogin no`
	`AuthorizedKeysFile /strange_location`	

Get default list of SUID files	`find / -user root -perm 4000`	

Service Lockdown		
Purpose	Command	Checked?

Set mySQL bind to localhost	`mysqld --help --verbose`
	
	`//This will get the configuration file location`
	
	`//Make sure the following option is 127.0.0.1 not 0.0.0.0`
	
	`[mysqld] bind-address = 127.0.0.1`	

Find web application configuration file		
Change web and database passwords		
Change web admin passwords in SQL		