Linux Checklist: Knowledge Gaining

Attempt initial login via easy-to-guess passwords; otherwise boot into single-user-mode to change the root password

Phase 1: Information Gathering (Upon Initial Login)		
Purpose	Command	Checked?
Dump history to file	`history > h.txt` `chattr +i h.txt`	
Change passwords Create password changing script for all users	`passwd [username]` See page [pagenumber]	
Set up backdoor account	`usermod -s /bin/bash nobody` `passwd nobody`	

Lock unknown admin users and write up inject
Change shell to rbash
	`passwd -l [username]`
	`usermod -L [username]`
	`usermod -s /bin/rbash [username]`	

Check operating system info	`cat /etc/{issue,issue.net}`
	`uname -a`
	`lsb_release`	

Enumerate users	`cat /etc/sudoers`
	`getent passwd | egrep -v\`
	`'(nologin,false)'`
	`getent group\`
	`{sudo,wheel,admin,root}`	

Check services
 	
Check ports for protocol
	`lsof -Pi`
	`netstat -tulpn`
	`ss -tlp`
	`pstree`
	`grep [portnum] /etc/services`	

Networking Information
 	
Check network connectivity
	`ip a`
	`route`
	`arp -a`
	`cat /etc/resolv.conf`
	`ping -c 2 {8.8.8.8,espn.com}`	

10 second hunt	`{who,w}`
	`lastlog`
	`crontab {-e,-l}`
	`tail /var/log/{auth.log,secure}`	