**Useful Links, File Locations and Commands**

**Disabling root login, securing (possible disabling of) SSH, sudoer file security and change password for root:**

SSH server may need to be installed via: *sudo apt-get install ssh*

Go to /*etc/ssh/sshd\_config*

* sudo vi /etc/ssh/sshd\_config (use Esc, then :wq to write and quit the editor)
* Disable root login: *PermitRootLogin* ***no***
* Change root’s password: *sudo passwd root*

**Killing users and processes:**

Use *who -u* to get a list of who’s on the box.

*killall -u [user] (Useful for ordinary malicious users)*

*kill -HUP [pid]* (Useful for a malicious hijacking root)

<https://phoenixnap.com/kb/how-to-kill-a-process-in-linux>

best way to kill a user:

who -u (get the process id of the user)

sudo kill -HUP [pid]

**Find and delete malicious users and groups:**

*userdel -rf [user]* (Deletes a user and their home directory material)

Search the */etc/passwd* and */etc/group*

**Download and run an antivirus (clamav):**

Run the following commands: (You need to install epel (Extra Packages for Enterprise Linux)

*apt install -y clamav*

*apt install -y clamd*

Scan the entire system by running clamav on the root like so (BE SURE TO OUTPUT THE RESULT TO A TEXT FILE WITH A FILE WITH EITHER THE ALLIGATOR MOUTHS OR --log=FILE):

*sudo clamscan -r --log=[where you want the output] /* (Also, be warned you my get a database error, be sure to run *sudo freshclam* if that happens)

<https://www.clamav.net/documents/installing-clamav>(Installation)

<https://www.clamav.net/documents/scanning> (Scanning guide)

**Disable and uninstall unnecessary services:**

*sudo systemctl* (Lists all services)

*sudo systemctl [enable, disable, stop, start, restart] [service]*

(Start and stop, self-explanatory, enable and disable toggle if the service will start automatically on reboot, and restart simply restarts a running service.)

**Monitoring logs + Wireshark + nmap:**

Useful directory locations:

*/var/log/*

*auth.log* (Logins)

*messages* (Critical errors)

*httpd* (Server logs)

/apt/history.log(apt package logs)

Use *tail -f --lines=[amount of lines you want at a time]* to monitor logs in real time.

sudo nmap --script vuln localhost

**Update Packages (yum):**

*sudo apt update*

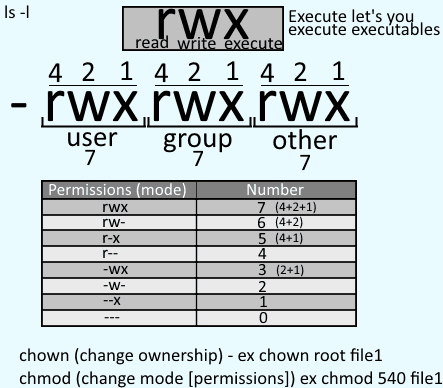
*sudo apt list* (Show all installed packages)

**Locking down critical files:**

*sudo lsattr [filename]* to list file attributes

*sudo chattr +i [filename]* to make a file immutable.

*sudo chmod [XXX] [filename]* to change the permissions of a file



**Installing a personal firewall (UFW = firewall of choice) (Potentially optional):**

*sudo apt -y install ufw*

*sudo ufw enable (or disable)* [Toggle the firewall]

*sudo ufw status numbered(*or *sudo ufw status verbose)* [List the rules of the firewall]

We should then, as a default, deny incoming traffic and allow outgoing.

*sudo ufw default deny incoming*

*sudo ufw default allow outgoing*

Then we can just allow whatever services we need.

*sudo ufw allow ssh (or 22)*

*sudo ufw allow http (or 80)*

*sudo ufw allow from 192.168.0.23 to any ports 22 (Allows SSH connections from that IP)*

*sudo ufw delete (rule no)* [Delete a particular rule]

**Secure your box for specific services:**

This up to you. If you got ecommerce, work on learning to secure apache and WordPress. If you have Windows, learn AD security and so on and so forth.

**Check for 777 files in home directory:**

**Stronger Password Policies / Aging:**

*sudo apt-get -y install libpam-pwquality cracklib-runtime*

Edit */etc/pam.d/common-password*

Change:

password requisite pam\_pwquality.so retry=3

to:

password requisite pam\_pwquality.so retry=3 minlen=8 maxrepeat=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 reject\_username enforce\_for\_root

minlen = minimum length | lcredit = lowercases require | dcredit = numbers required | ocredit = special credits required | reject\_username = Reject password if contains the username or the username in reverse | enforce\_for\_root = Makes root even abide by the rule

**Login.defs config:**

*FAILLOG\_ENAB=yes*

*CREATE\_HOME=yes*

**Install an IDS (Intrusion Detection System):**

**Backup the system (again):**

^^^ See the first ‘Backup the system’ part. ^^^