Linux Utilities - really useful commands!

Clamav

* ClamAV is an open source antivirus engine for detecting trojans, viruses, malware & other malicious threats.
* We’ll be using to remove any malware, and identify and remove infected files (affected by virus)
* installation/setup
  + Sudo apt-get update
  + Sudo apt-get install clamav clamav-daemon
  + sudo systemctl stop clamav-freshclam
    - Stop clamav process
  + sudo freshclam
    - Update virus signitures
* Basic usage
  + Clamscan --infected --remove --recursive /home/rafi/Documents
  + Clamscan --infected --remove --recursive /
    - --infected: print infected files
    - --remove: remove infected files
    - --recursive: scan subdirectories of given folder
* WARNING: clamscan may not work - might say “killed”. If this happens, increase memory
* Clamtk - GUI version
  + Install: sudo apt-get install clamtk
  + Usage: clamtk
  + Scan directory, individual file - scan a directory lol
  + View quarantined files
  + Whitelist directories (don’t scan)

Manual pages

* Documentation manual for commands
* Useful for understanding command arguments
* Default opens in vim
* Usage
  + man clamscan
  + Exit: :q

Gufw

* Very simple Firewall GUI powered by UFW - uncomplicated firewall
* Installation
  + sudo apt-get install gufw
* Usage:
  + gufw
  + Click ‘status’ to turn on firewall
    - You’ll get points j for this lol
  + Rules: allow/deny traffic on ports for certain services

Ranger

* File manager through the term<>inal
* Installation
  + sudo apt install ranger
* Usage
  + Ranger
  + Use arrow keys:
    - =>: enter directory
    - <=: go to parent
    - ^: go up
    - ↓ : go down
    - q: exit

Tiger

* Tiger collection of shell scripts for security audit and host intrusion detection written entirely in shell language. It’s major purpose is to check the system configuration and status. It scans system configuration files, file systems, and user configuration files for possible security problems and reports them.
* Somewhat old (hasn’t been updated from 2018)
* Installation
  + sudo apt install tiger
    - Remember tripwire
* Usage
  + sudo tiger
    - Produces log file with warnings, gives warning path at the end of output
  + sudo tigexp acc015w
  + sudo tiger -E
  + cat <path-to-log-file>
    - Produces log file with warnings, gives warning path at the end of output

Lynis

* Lynis is a security auditing tool and performs a security scan of the system. The primary goal is to test security defenses and provide tips for further reduce security vulnerabilities. It will also scan for general system information, vulnerable software packages, and possible configuration issues.
* Reviews a ton of categories
* Installation
  + Sudo apt install lynis
* Basic Usage
  + lynis audit system
    - GREEN: good
    - Yellow: Not found or just a suggestion
    - RED: possible vul
  + Lynis show details <test-id>
    - Get more information about the suggestions/warnings offered at end of
    - the output

Text Editors

* Gedit
  + Pros: simple interface, use of mouse
  + Cons: Very few features
* Nano
  + Pros: somewhat simple interface, more keyboard commands than gedit
  + Cons: not many commands
  + Go over saving
  + Go over inserting from other file
  + Go over deleting line
  + Go over search for word
* Vim
  + Pros: Large variety of keyboard commands, color-coded
    - https://vim.rtorr.com/
  + Cons: Very difficult at first
  + Go over insertion vs normal modes
  + Normal:
    - Arrw keys
    - w - next word
    - b - prev word
    - { - next blank line
    - } - previous blank line
    - d - delete
      * dd - delete current line
    - v - select text
      * y - copy
      * p - paste
      * d - delete
    - u - undo
    - r + ctrl - redo
    - / - search forward for pattern
    - ? - search backward
    - :wq - save and exit

\*Both Vim and Nano open directly in the terminal