Security and Fstab

Security

- Strong Passwords
- 8 or more characters
- Use * ! # ( ) along with numbers and upper/lower case letters
- Keepass(X) great program to safely store passwords

Encryption

- Can encrypt home directory during the installation
- Use eCryptfs and install it using “sudo apt install ecryptfs-utils
- Mount the partition to be encrpyted “sudo mount -t ecryptfs /srv /srv”
- Follow the prompts and remember your passphrase
- Copy some files over “sudo cp -r /etc/default /srv”
- Umount it “sudo umount /srv”
- Look at a file “cat /srv/default/cron” and the data will be encrypted.
- Remount it to continue to encrypt files stored in that partition.

Automatically Mounting Encrypted Partitions
There are a couple of ways to automatically mount an ecryptfs encrypted filesystem at boot. This example will use a /root/.ecryptfsrc file containing mount options, along with a passphrase file residing on a USB key.
First, create /root/.ecryptfsrc containing:

```
key=passphrase:passphrase_passwd_file=/mnt/usb/passwd_file.txt
ecryptfs_sig=5826dd62cf81c615
ecryptfs_cipher=aes
ecryptfs_key_bytes=16
ecryptfs_passthrough=n
ecryptfs_enable_filename_crypto=n
```

Adjust the ecryptfs_sig to the signature in /root/.ecryptfs/sig-cache.txt.
Next, create the /mnt/usb/passwd_file.txt passphrase file:

```
passphrase_passwd=[secrets]
```

Now add the necessary lines to /etc/fstab:

```
/dev/sdb1
/mnt/usb  ext3     ro 0 0
/srv /srv ecryptfs defaults 0 0
```

Make sure the USB drive is mounted before the encrypted partition.
Finally, reboot and the /srv should be mounted using eCryptfs.

UFW/iptables Firewall

- UFW (uncomplicated firewall)
- Installed by default but disabled
- Uses rules to allow/block firewall features
- Check status “sudo ufw status”
- Enable “sudo ufw enable”
- Should create rules before enabling the firewall
- “sudo ufw allow 22” (Opens tcp and udp port 22 for ssh access) “sudo ufw allow ssh”
- “sudo ufw allow 22/tcp” (only allow 22 tcp traffic)
- “sudo ufw reject out ssh” (block outbound ssh on port 22)
- “sudo ufw delete reject ssh” (delete reject ssh rule)
- “sudo ufw deny proto tcp from 12.34.56.78 to any port 22” (reject ssh from ip 12.34.56.78)
- “sudo ufw reset” (reset the firewall to defaults)
- “sudo ufw app list” (shows applications rules for ufw)
- “sudo ufw app info Name” (shows rules for the named application)
- “sudo ufw allow Name” (allow traffic to and from application)
- “sudo ufw looging on” (logging is off by default)
- `“sudo ufw default deny incoming”`
- `“sudo ufw default allow outgoing”`

Antivirus Programs

- Clamav and Clamav-daemon
- Clamtk GUI
- clamscan -r -i Downloads/

FSTAB

- Purpose: to mount internal drives for use
- Making Changes:
- cat /etc/fstab (view file)
- sudo fdisk -l (list the drives. Also df -h)
- sudo mount -a (mount all the drives)
- Remember that the mount point must already exist, otherwise the entry will not mount on the filesystem. To create a new mount point, use root privileges to create the mount point. Here is the generalization and an example:

- `sudo mkdir /path/to/mountpoint`
- `sudo mkdir /media/disk2`

- **`Be careful with this file as it can quite easily cause your system not to boot.`**