**Intro to Live Operating Systems**

A live OS can be booted from an external disc, CD, DVD, USB or card

Connect the stick or disk into the machine and confirm within the BIOS that the machine can boot the OS before the internal hard drive

* The live OS will then be booted instead of the native OS
* Can also be booted in a VM

Useful for security

* Tails
* Knoppix
* Puppy Linux
* JonDo/Tor-Secure-Live-DVD
* Tiny Core Linux

Download ISO from online, then burn the disc image on to a disk which will create a bootable disk

To create a bootable USB or SD, software will be needed

* Rufus / Pen Drive Linux / Tails
* Download software
* Select SIO
* Put in USB and it does it for you

Creating the right settings in the BIOS

Access the BIOS using the function keys

Tab to ‘BOOT’

* Move the method of booting to the highest priority
* E.g., move ‘Removable Devices’ or ‘CD-ROM / DVD’ to the top, above ‘Hard Disk Image’
  + This will cause device to boot the removable device before the Hard Drive

Booting in a VM

Select the ISO as a disk in the virtual CD drive

* Create template for the live OS
* For non-persistence, select do not create virtual disk image
* For persistence, select do create virtual disk image
* Go into settings of the new VM
* Storage: select the drive you want to mount it from e.g., CD drive or USB drive
* Choose your VDI which is your ISO file
* Tick the box for ‘Live CD/DVD’
  + This means that the virtual disk will not be removed when the guest system ejects it
* Tails is now bootable

Persistent

* Changes are retained
* You can make changes within the operating system e.g., download files onto the OS which will be retained the next time you boot it up
* Disadvantage is if an attacker has physical or remote access to the device could take control of the OS which would persist too
* Can often be upgraded without having to download the whole ISO again

Non-persistence

* No changes are saved
* No evidence retained after OS is shut done
* Any hacker cannot persist after the OS is shut down as everything is lost
* You can force non-persistence to a USB at the hardware level as well by using a write-lock USB or SD

Suggested USB

* SanDisk 64GB Ultra Fit USB 3.0 Flash Drive – 130mb/s
* Hardware encryption USB 3.0
  + Aegis Secure Key 3.0 – has pin on drive to unlock / decrypt
* Always remember your plausible deniability encryption