Website development –

Hosting –

* Types of hosting
* Companies providing hosting services
* Host your own website
* Multiple domains on a single host

Rev proxy –

1. Caching
2. Load balancer
3. Security
4. Bandwidth reduce – zip/unzipping

**Web server**

Piece of software that serves web content

* Listens on one port or multiple (if so configured)
* http:80, https:443
* One computer can have multiple web servers running on different ports.

**Routing**

Deciding which resource to return

* Static routing – route to a file
* Dynamic routing – route to a web application

Client - Web server – Application server

API - contract defining interface

Secure raspberry pi –

1. Change rpi password for pi - sudo raspi-config
2. Enable ssh – Interfacing options -> SSH -> Enable
3. Create new account for yourself
   1. sudo adduser xyz
   2. sudo gpasswd -a xyz adm
   3. sudo gpasswd -a xyz sudo
4. check if you can ssh in as xyz –
   1. ssh xyz@ip\_address
   2. sudo whoami – check if sudo works
5. Lock pi account as some software relies on pi account so don’t delete it.
   1. sudo passwd -l pi
6. sudo visudo
   1. xyz ALL=(ALL) NOPASSWD:ALL
7. *sudo apt update -y && sudo apt upgrade -y*
   1. Can set up for auto upgrades
8. *systemctl --type=service –state=active*
9. *netstat -an*
10. *sudo apt install ufw -y*
11. *sudo ufw allow 22/tcp comment “SSH”*
12. *sudo ufw allow 8080/tcp “Experimental web server”*
13. *sudo ufw enable*
14. *sudo ufw status*
15. *sudoedit /etc/ssh/sshd\_config*
    1. *AllowUsers xyz,abc*
16. *Ban users with multiple unsecure ssh attempts-*
    1. *sudo apt install fail2ban*
    2. *sudoedit /etc/fail2ban/jail.local*
       1. *[DEFAULT]*
       2. *bantime = 1h*
       3. *banaction = ufw*
       4. *[sshd]*
       5. *enabled=true*
    3. *sudo systemctl enable –now fail2ban*
    4. *sudo sytemctl restart sshd*