**Passive Recon**

**Google**

Basically, crawls every webpage on the planet, can be really specific for searches

* Cat Site:godaddy.com
  + Will look for cats specifically on godaddy.com
* **Site:godaddy.com filetype:pdf**
  + Will show all pdf files on godaddy.com
  + Can use ‘-‘ to filter out results too

Google Hacking Database on exploit-DB

* Can use certain searches to see if there’s admin login pages without even touching the site

Wayback machine

* Can see past history on the internet
* Archives

**Shodan**

Grabs banners and HTTP headers for us without making the request ourself, which still makes it passive

Internet device scanner

* Hostname:facebook.com port:80
  + Will then show all the websites with the hostname: facebook that have port 80 open
* Net:72.21.192.0/19
  + Running a scan on the whole network range
  + Can filter out what sites are using Apache Tomcat etc.
* WordPress
  + Will scan all devices connected to the internet that have WordPress interacting through a network

**WhoIs**

* Shows who’s behind a server or IP
* Like the gov website for companies and their owners
* Name servers
* Domain status
* Can also be done through the cmd line

**NetCraft**

* Provides a unique aspect to searching
* Keeps track of sites
  + What the ip was, if its changed
  + What the web server was running, Apache etc.
* Sites end up in this data base once it’s been indexed by google

**Job Postings**

* Companies will often disclose their architecture here
* Or the OS that they’re using
* They will specify these as they will need to hire someoneN with these specialties