- Ping and DNS
- https://www.whois.com/whois
- (Note social eng aspect of linked, google searches, Facebook and financial data, wayback machine)
- Google hacking (https://pentest-tools.com/information-gathering/google-hacking this entire website is a goldmine of information!!)
- Active reconnaissance vs passive reconnaissance
- Nmap
- Footprinting
- recon-ng (a kali linux tool): https://tools.kali.org/information-gathering/recon-ng
- Demos:
- We could try setting up a website rn and asking people to do passive + active reconnaissance and present all the info gathered at the end maybe?
- Links:
- https://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-passive-reconnaissance-potential-target-0146938/
- https://null-byte.wonderhowto.com/how-to/five-phases-hacking-0167990/

mention dig
britishairways.com
http://www.palash.in/
http://famillemyriam.org
sans.org
glassdoor.com

robots.txt

Purpose:
- Narrow down to specific targets and techniques
- Avoid broad scans
- Identify brands/versions to target vulnerabilities
    - OS
    - Patch Level

Passive vs Active
Passive:
- First/Most basic step
- Indistinguishable from ordinary public traffic
- Google search
- Browsing company web pages

Active:

- Want to know what kind of servers they're running before doing this
- Network scanning
- Social engineering
- Spear phishing
- Ping sweep: Super noisy/obvious

Whois
A Whois query is a database search, to a Whois server on TCP port 43, and it is used to resolve contact information about domain names, ip address blocks, and Autonomous System numbers.
uclaacm.com has WhoIsGuard
WISDOMJOBS.COM

Netcraft
Hosting history -> OS
We can see under the heading "Hosting History" the netblock owner, IP address(es), operating system, web server, and when the server was last changed. All of this can be useful to the hacker, including the date last changed. This date generally represents the date the system was last rebooted or updated.
In the case above, we can see it was last updated Sept. 28, 2007. This would imply that any security OS patches that have been supplied in the interim have NOT been applied to this system. As a hacker, this is juicy information as it tells us that any vulnerabilities to this system that have been found since Sept. 28, 2007 are still available on this system as no vulnerability patches have been applied.
britishairways.com
palash.in

Google Hacking
Using keywords with Google searches is a great way to find web pages that website owners may not want you to see!
site: website.com -site:www.website.com
inurl:/admin/login.asp & intext:password
inurl:login.php & intitle:Admin Login
inurl:login.aspx & intitle:Admin Login
inurl:login & intitle:Admin Login
intext:admin & inurl:gov -github & filetype:sql

Recon-ng
https://hackertarget.com/recon-ng-tutorial/
glassdoor.com

recon-ng

help
show modules
keys list
keys add facebook_api <number>
use recon/domains-vulnerabilities/xssposed
show info
set source glassdoor.com
run

wayback machine

Ping
https://www.whois.com/whois
(Note social eng aspect of linked, google searches, Facebook and financial data, wayback machine)
Google hacking (https://pentest-tools.com/information-gathering/google-hacking this entire website is a goldmine of information!!)
Active reconnaissance vs passive reconnaissance
Nmap
Footprinting
recon-ng (a kali linux tool): https://tools.kali.org/information-gathering/recon-ng

Demos:
We could try setting up a website rn and asking people to do passive + active reconnaissance and present all the info gathered at the end maybe?

- Reconnaissance and Footprinting
- Client-Server Model
    - Nmap
    - Port Scanning
    - Websites that document vulnerabilities
    - Burp Suite