Recon

Google dorking -
https://www.exploit-db.com/google-hacking-database/

Scope Discovery -
https://viewdns.info/reversewhois/
https://crt.sh/?q=facebook.com&output=json

subdomian discovery-
https://github.com/infosec-au/altdns/

screen shot tools -
https://github.com/FortyNorthSecurity/EyeWitness/
https://github.com/dxa4481/Snapper/

Spidering tools -
https://www.zaproxy.org/

Github recon -
https://github.com/michenriksen/gitrob/
https://github.com/trufflesecurity/truffleHog/
https://buckets.grayhatwarfare.com/

s3 buckets discovery -
https://github.com/nahamsec/lazys3/
https://github.com/eth0izzle/bucket-stream/

Check leaked creds -
https://github.com/streaak/keyhacks/

Pastebin -
https://github.com/kevthehermit/PasteHunter/

Waybackmachine -
https://github.com/tomnomnom/waybackurls/

Tech-stack fingerprinting -
https://www.wappalyzer.com/
https://builtwith.com/
https://stackshare.io/
https://retirejs.github.io/retire.js/

OSINT -
slideshare