- ## 1. Information Gathering

  - **whois**: whois target.com
  - **nslookup**: nslookup target.com
  - **dig**: dig target.com
  - **host**:
    - Nameservers: host -t ns target.com
    - Mail servers: host -t mx target.com
  - **sublist3r**: sublist3r -d target.com
  - **amass**: amass enum -d target.com
  - **assetfinder**: assetfinder --subs-only target.com
  - **findomain**: findomain -t target.com
  - **massdns**: massdns -r resolvers.txt -t A -o S -w results.txt subdomains.txt
  - **httprobe**: httprobe < subdomains> live_subdomains.txt
  - **nmap**:
    - Scan hosts: nmap -iL live_hosts.txt -oA nmap_scan
    - Web servers: whatweb -i live_hosts.txt
  - **aquatone**: aquatone-discover -d target.com
  - **gau**: gau target.com | tee gau_urls.txt
  - **hakrawler**: hakrawler -url target.com -depth 2 -plain | tee hakrawler_output.txt
  - **github-search**: github-search target.com
  - **gitrob**: gitrob -repo target.com
  - **fierce**: fierce --domain target.com
  - **dirsearch**: dirsearch -u target.com -e *
  - **ffuf**: ffuf -w wordlist.txt -u https://target.com/FUZZ
  - **gowitness**: gowitness file -f live_hosts.txt -P screenshots/
  - **nuclei**: nuclei -l live_hosts.txt -t templates/
  - **metagoofil**: metagoofil -d target.com -t doc,pdf,xls,docx,xlsx,ppt,pptx -l 100
  - **theHarvester**: theHarvester -d target.com -l 500 -b all
  - **dnsenum**: dnsenum target.com
  - **dnsrecon**: dnsrecon -d target.com
  - **shodan**: shodan search hostname:target.com
  - **censys**: censys search target.com
  - **spiderfoot**: spiderfoot -s target.com -o spiderfoot_report.html

2. Subdomain Enumeration

- **subfinder**: subfinder -d target.com -o subfinder_results.txt
- **waymore**: waymore -d target.com -o waymore_results.txt
- **subjack**: subjack -w subdomains.txt -t 20 -o subjack_results.txt

3. Vulnerability Scanning

- **xsstrike**: xsstrike -u https://target.com
- **gf**:
    - XSS: gf xss | tee xss_payloads.txt
    - SQLi: gf sqli | tee sqli_payloads.txt
    - LFI: gf lfi | tee lfi_payloads.txt
    - SSRF: gf ssrf | tee ssrf_payloads.txt
    - IDOR: gf idor | tee idor_payloads.txt
    - SSTI: gf ssti | tee ssti_payloads.txt
- **git-secrets**: git-secrets --scan
- **ffuf**: ffuf -w wordlist.txt -u https://target.com/FUZZ

4. Miscellaneous Tools

- **arjun**: arjun -u https://target.com -oT arjun_output.txt
- **unfurl**: unfurl -u https://target.com -o unfurl_results.txt
- **dalfox**: dalfox file live_hosts.txt
- **gospider**: gospider -S live_hosts.txt -o gospider_output/
- **meg**: meg -d 1000 -v /path/to/live_subdomains.txt
- **wfuzz**: wfuzz -w wordlist.txt -u https://target.com/FUZZ
- **wafw00f**: wafw00f target.com
- **wpscanner**: wpscan --url target.com
- **cloud_enum**: cloud_enum -k target.com -l cloud_enum_output.txt
- **gobuster**: gobuster dns -d target.com -t 50 -w wordlist.txt
- **masscan**: masscan -iL live_hosts.txt -p0-65535 -oX masscan_results.xml
- **paramspider**: paramspider --domain target.com --output paramspider_output.txt

5. Network and DNS Tools

- **dnswalk**: dnswalk target.com
- **dnsx**: dnsx -l subdomains.txt -resp-only -o dnsx_results.txt
- **dnsgen**: dnsgen -f resolvers.txt -t A -o S -w dnsgen_results.txt
- **dnsvalidator**: dnsvalidator -t 100 -f resolvers.txt -o validated_resolvers.txt
- **httx**: httx -silent -l live_subdomains.txt -mc 200 -title -tech-detect -o httx_results.t