Resource Module 9 - TOOLS

TOOLS

RECON:

(Kali) theHarvester - searches for emails/email patterns
(Kali) sublist3r - searches for sub domains (Ex. "*.tesla.com")
(Web) Hunter.io - searches for emails/email patterns
(Web) crt.sh - searches for subdomains

(Kali) OWASP AMASS - searches ->(See below)

```
**DNS** Basic enumeration, Brute forcing (optional), Reverse DNS sweeping,
Subdomain name alterations/permutations, Zone transfers (optional)

**Scraping** Ask, Baidu, Bing, DNSDumpster, DNSTable, Dogpile, Exalead,
Google, HackerOne, IPv4Info, Netcraft, Riddler, SiteDossier, ViewDNS, Yahoo

**Certificates** Active pulls (optional), Censys, CertSpotter, Crtsh,
Entrust, GoogleCT

**APIs** AlienVault, BinaryEdge, BufferOver, CIRCL, CommonCrawl, DNSDB,
GitHub, HackerTarget, IPToASN, Mnemonic, NetworksDB, PassiveTotal, Pastebin,
RADb, Robtex, SecurityTrails, ShadowServer, Shodan, Spyse (CertDB &
FindSubdomains), Sublist3rAPI, TeamCymru, ThreatCrowd, Twitter, Umbrella,
URLScan, VirusTotal, WhoisXML
Web Archives: ArchiveIt, ArchiveToday, Arquivo, LoCArchive, OpenUKArchive,
UKGovArchive, Wayback
```

WEBSITE TECH

(Web) BuiltWith.com (Most information)
(Web) wappalyzer (Simplest)
(Kali) whatweb

(Kali)BurpSuite