

```
root@zsean0:~/Tools# amass enum -brute -active -d yahoo.com -o amass-output.txt
Querying VirusTotal for yahoo.com subdomains
Querying Spyse for yahoo.com subdomains
Querying Sublist3rAPI for yahoo.com subdomains
Querying ThreatCrowd for yahoo.com subdomains
Querying ViewDNS for yahoo.com subdomains
Querying URLScan for yahoo.com subdomains
Querying Yahoo for yahoo.com subdomains
Querying Crtsh for yahoo.com subdomains
Querying SiteDossier for yahoo.com subdomains
Querying Riddler for yahoo.com subdomains
Querying Robtex for yahoo.com subdomains
Querying Netcraft for yahoo.com subdomains
Querying HackerTarget for yahoo.com subdomains
Querying Entrust for yahoo.com subdomains
Querying Exalead for yahoo.com subdomains
Querying IPv4Info for yahoo.com subdomains
Querying Pastebin for yahoo.com subdomains
Querying Google for yahoo.com subdomains
Querying Dogpile for yahoo.com subdomains
```

Let's continue hacking! Step Two: Expanding our attack surface

Tools at the ready, it's time to see what's out there!

This is the part where I start to run my subdomain scanning tools listed above to see what's out there. Since personally I enjoy playing with features in front of me to begin with I specifically look for domains with functionality, so whilst the tools are running I will start dorking. Some common keywords I dork for when hunting for domains with functionality:

login, register, upload, contact, feedback, join, signup, profile, user, comment, api, developer, affiliate, careers, upload, mobile, upgrade, passwordreset.