Fierce

Fierce tries to find name servers for the given domain and perform a zone transfer on each one. It also checks for a wildcard DNS record and guesses subdomains using an internal wordlist.

Type fierce -h for help (this works for most things):

fierce -dns google.com

To specify a custom wordlist:

fierce -dns google.com –wordlist /path/to/wordlist/

Wildcard domains

A Wildcard DNS record is a DNS record that will match any request when there is no record available that explicitly matches that request. The Wildcard DNS record is uses an asterisk as the first label: \*.domain.com.

For example:

www.domain.com A 1.1.1.1

vpn.domain.com A 1.1.1.2

test.domain.com A 1.1.1.3

\*.domain.com A 1.1.1.1

Requesting the IP for a domain that is not explicitly defined, such as xw4647.domain.com will return the wildcard response of 1.1.1.1.

Tools like Fierce will first make a request for an unlikely subdomain (e.g sffvfdghdf9w3534.google.com) before guessing common names from a wordlist to determine if wildcard domains are present.