

Exercise DNS Scan with dnsenum

1. Introduction and description

dnsenum is a multithread script to enumerate information on a domain and to discover non-contiguous IP blocks.

In addition, the tool offers added value with:

- * Google Searches
- * Brute-forcing hosts
- * Whois netrange lookups
- * Reverse lookups

Please give a short description of the following points:

1. describe the benefit of the Google option
2. describe the benefit of the brute-force option
3. describe the benefit of whois netrange option
4. describe your lesson learned

2. Answer

1. Also known as **Google scraping** (allinurl: -www site:target.com) this can be helpful to find additional domains to a **reverse dns lookup** or when **zone transfer** is disabled. (It should be in most cases)
2. Benefit lays in finding additional subdomains when your results on standard dns queries doesn't satisfy you. Bruteforcenames from dnsenum tool are based on research, by analysing thousands of domains.

The first four (subdomains-100.txt, subdomains-500.txt, subdomains-1000.txt and subdomains-10000.txt) were created by analysing the most commonly occurring subdomains in approximately 86,000 zone files that were transferred as part of a separate research project. These wordlists are sorted by the popularity of the subdomains (more strictly by the percentage of zones that contained them in the dataset).

3. It calculates C Class domain ranges and perform whois queries on it, but I can't see a real benefit of it yet.

```
hacker@hikali: ~/Desktop/Exercises/Reconnaissance/Exercise 3/dnscan
File Edit View Terminal Tabs Help

Launching Whois Queries:
-----
whois ip result: 62.2.85.0 -> 62.2.85.0/28
whois ip result: 80.74.140.0 -> 80.74.140.0/24
whois ip result: 193.135.215.0 -> 193.135.215.0/29

compass-security.com
-----
193.135.215.0/29
62.2.85.0/28
80.74.140.0/24

Performing reverse lookup on 280 ip addresses:
-----

0 results out of 280 IP addresses.
```

4. The more time you spend in information gathering, the more results you get. The best thing is to combine different tools and techniques, but as we've already learned in previous exercises it can be a very time consuming task.