Subdomain Bruteforcing

`Subdomain Brute-Force Enumeration` is a powerful active subdomain discovery technique that leverages pre-defined lists of potential subdomain names. This approach systematically tests these names against the target domain to identify valid subdomains. By using carefully crafted wordlists, you can significantly increase the efficiency and effectiveness of your subdomain discovery efforts.

The process breaks down into four steps:

1. `Wordlist Selection`: The process begins with selecting a wordlist containing potential subdomain names. These wordlists can be:
   - `General-Purpose`: Containing a broad range of common subdomain names (e.g., `dev`, `staging`, `blog`, `mail`, `admin`, `test`). This approach is useful when you don't know the target's naming conventions.
   - `Targeted`: Focused on specific industries, technologies, or naming patterns relevant to the target. This approach is more efficient and reduces the chances of false positives.
   - `Custom`: You can create your own wordlist based on specific keywords, patterns, or intelligence gathered from other sources.
2. `Iteration and Querying`: A script or tool iterates through the wordlist, appending each word or phrase to the main domain (e.g., `example.com`) to create potential subdomain names (e.g., `dev.example.com`, `staging.example.com`).
3. `DNS Lookup`: A DNS query is performed for each potential subdomain to check if it resolves to an IP address. This is typically done using the A or AAAA record type.
4. `Filtering and Validation`: If a subdomain resolves successfully, it's added to a list of valid subdomains. Further validation steps might be taken to confirm the subdomain's existence and functionality (e.g., by attempting to access it through a web browser).

There are several tools available that excel at brute-force enumeration:

Tool	Description
dnsenum	Comprehensive DNS enumeration tool that supports dictionary and brute-force attacks for discovering subdomains.
fierce	User-friendly tool for recursive subdomain discovery, featuring wildcard detection and an easy-to-use interface.
dnsrecon	Versatile tool that combines multiple DNS reconnaissance techniques and offers customisable output formats.
amass	Actively maintained tool focused on subdomain discovery, known for its integration with other tools and extensive data sources.
assetfinder	Simple yet effective tool for finding subdomains using various techniques, ideal for quick and lightweight scans.
puredns	Powerful and flexible DNS brute-forcing tool, capable of resolving and filtering results effectively.

DNSEnum

`dnsenum` is a versatile and widely-used command-line tool written in Perl. It is a comprehensive toolkit for DNS reconnaissance, providing various functionalities to gather information about a target domain's DNS infrastructure and potential subdomains. The tool offers several key functions:

- `DNS Record Enumeration`: `dnsenum` can retrieve various DNS records, including A, AAAA, NS, MX, and TXT records, providing a comprehensive overview of the target's DNS configuration.
- `Zone Transfer Attempts`: The tool automatically attempts zone transfers from discovered name servers. While most servers are configured to prevent unauthorised zone transfers, a successful attempt can reveal a treasure trove of DNS information.
- `Subdomain Brute-Forcing`: `dnsenum` supports brute-force enumeration of subdomains using a wordlist. This involves systematically testing potential subdomain names against the target domain to identify valid ones.
- `Google Scraping`: The tool can scrape Google search results to find additional subdomains that might not be listed in DNS records directly.
- `Reverse Lookup`: `dnsenum` can perform reverse DNS lookups to identify domains associated with a given IP address, potentially revealing other websites hosted on the same server.
- `WHOIS Lookups`: The tool can also perform WHOIS queries to gather information about domain ownership and registration details.

Let's see `dnsenum` in action by demonstrating how to enumerate subdomains for our target, `inlanefreight.com`. In this demonstration, we'll use the `subdomains-top1million-5000.txt` wordlist from SecLists, which contains the top 5000 most common subdomains.

Code: bash

```
dnsenum --enum inlanefreight.com -f /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -r
```

In this command:

- `dnsenum --enum inlanefreight.com`: We specify the target domain we want to enumerate, along with a shortcut for some tuning options `--enum`.
- `-f /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt`: We indicate the path to the SecLists wordlist we'll use for brute-forcing. Adjust the path if your SecLists installation is different.
- `-r`: This option enables recursive subdomain brute-forcing, meaning that if `dnsenum` finds a subdomain, it will then try to enumerate subdomains of that subdomain.

Subdomain Bruteforcing

```
MisaelMacias@htb[/htb]$ dnsenum --enum inlanefreight.com -f  /usr/share/seclists/Discovery/DNS/subdomains-top1million-
```

```
dnscmd version 1.2.0

-----   inlanefreight.com   -----


Host's addresses:
-----------------

inlanefreight.com.                      300      IN    A        134.209.24.248

[...]

Brute forcing with /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt:
-------------------------------------------------------------------------------

www.inlanefreight.com.                  300      IN    A        134.209.24.248
support.inlanefreight.com.              300      IN    A        134.209.24.248
[...]


done.
```

Connect to Pwnbox
Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 139ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet

+1 Using the known subdomains for inlanefreight.com (www, ns1, ns2, ns3, blog, support, customer), find any missing subdomains by brute-forcing possible domain names. Provide your answer with the complete subdomain, e.g., www.inlanefreight.com.

Submit your answer here...

+10 Streak pts Submit

Previous Next