Directory Busting and VHOST Enumeration

@mmar

AIM

Dir Busting

- Find Directories and pages of a website

VHOST ENUMERATION

- Find subdomains of a website

GoBuster is an open-source directory and files brute-forcing tool written in the Go programming language. It is used for discovering hidden files and directories on a web server by generating a list of possible directories and file names and then trying to access them.

FFUF is another tool that is becoming popular due to its fast speed and flexibility it provides

Wordlists

- Wordlists are lists of words or phrases that are used in the directory and VHOST brute-forcing to generate possible directory and VHOST names. These wordlists typically contain common words and phrases that are used in file and directory naming conventions, as well as common VHOST names and subdomains.
- We will be using Seclists for our lecture which can be installed by the following command in Kali Linux or Parrot OS

```
Sudo apt install seclists
```

DIR BUSTING

Dir Busting

Gobuster

```
gobuster dir -u http://10.10.10.10 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

FFUF

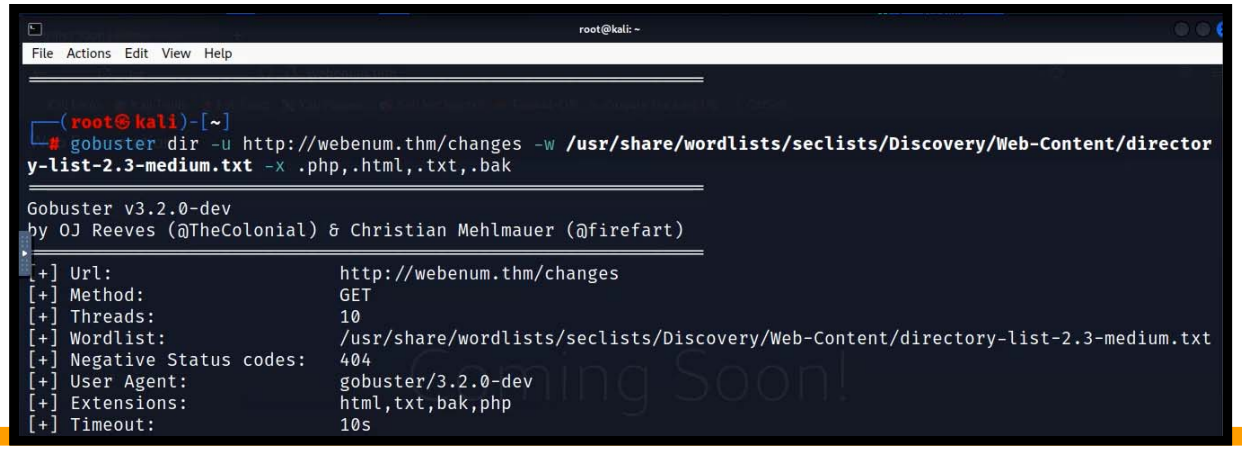
```
ffuf -u http://10.10.10.10/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

Finding Files

- We can specify the extensions for searching files for that extension in the directory

Gobuster

```
gobuster dir -u http://10.10.10.10 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .html,.css,.js
```



Finding Files

- FFUF can also be used to brute force the files

FFUF

```
ffuf -u http://10.10.10.10/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt –e .html,.css,.js,.conf
```

VHOST ENUMERATION

VHOST Enumeration

- VHOST enumeration is the process of identifying virtual hosts (VHOSTs) on a web server. A virtual host is a method of hosting multiple domain names on a single web server. Each domain name is associated with a unique IP address or port number, and the web server uses this information to route incoming requests to the appropriate website.
- VHOST enumeration is often used as part of the reconnaissance phase of a web application penetration test or vulnerability assessment. Attackers can use VHOST enumeration to identify all the virtual hosts hosted on a web server, and then focus their efforts on those hosts that may be vulnerable to attacks.

VHOST Enumeration

Gobuster

```
gobuster vhost -u http://example.com -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt --append-domain
```

FFUF

```
ffuf -u http://example.com -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -H "HOST:FUZZ.example.com"
```

DEMO

THANKS