Introduction to Brute Forcing

A Brute Force attack is a method of attempting to guess passwords or keys by automated probing. An example of a brute-force attack is password cracking. Passwords are usually not stored in clear text on the systems but as hash values.

Here is a small list of files that can contain hashed passwords:

`Windows`	`Linux`
unattend.xml	shadow
sysprep.inf	shadow.bak
SAM	password

Since the password cannot be calculated backward from the hash value, the brute force method determines the hash values belonging to the randomly selected passwords until a hash value matches the stored hash value. In this case, the password is found. This method is also called offline brute-forcing. This module will focus on online brute-forcing and explicitly deal with the websites' login forms.

On most websites, there is always a login area for administrators, authors, and users somewhere. Furthermore, usernames are often recognizable on the web pages, and complex passwords are rarely used because they are difficult to remember. Therefore it is worth using the online brute forcing method after a proper enumeration if we could not identify any initial foothold.

There are many tools and methods to utilize for login brute-forcing, like:

- `Ncrack`
- `wfuzz`
- `medusa`
- `patator`
- `hydra`
- and others.

In this module, we will be mainly using `hydra`, as it is one of the most common and reliable tools available.

The following topics will be discussed:

- Brute forcing basic HTTP auth

- Brute force for default passwords
- Brute forcing login forms
- Brute force usernames
- Creating personalized username and password wordlists based on our target
- Brute forcing service logins, such as FTP and SSH