Passwords Attack

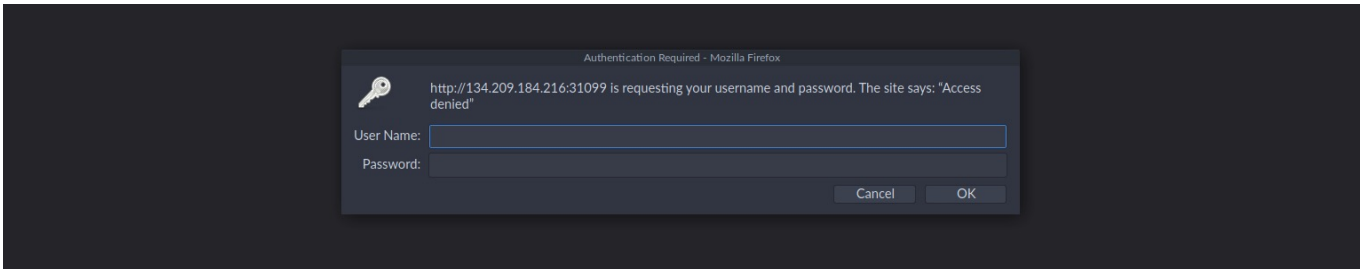
We found an unusual host on the network during our black box penetration test and had a closer look at it. We discovered a web server on it that is running on a non-standard port. Many web servers or individual contents on the web servers are still often used with the Basic HTTP AUTH scheme. Like in our case, we found such a webserver with such a path, which should arouse some curiosity.

The HTTP specification provides two parallel authentication mechanisms:

1. `Basic HTTP AUTH` is used to authenticate the user to the HTTP server.
2. `Proxy Server Authentication` is used to authenticate the user to an intermediate proxy server.

These two mechanisms work very similarly as they use requests, response status codes, and response headers. However, there are differences in the status codes and header names used.

The Basic HTTP Authentication scheme uses user ID and password for authentication. The client sends a request without authentication information with its first request. The server's response contains the `WWW-Authenticate` header field, which requests the client to provide the credentials. This header field also defines details of how the authentication has to take place. The client is asked to submit the authentication information. In its response, the server transmits the so-called realm, a character string that tells the client who is requesting the data. The client uses the Base64 method for encoding the identifier and password. This encoded character string is transmitted to the server in the Authorization header field.



As we don't have any credentials, nor do we have any other ports available, and no services or information about the webserver to be able to use or attack, the only option left is to utilize password brute-forcing.

There are several types of password attacks, such as:

Password Attack Type
`Dictionary attack`

Password Attack Type
`Brute force`
`Traffic interception`
`Man In the Middle`
`Key Logging`
`Social engineering`

We will mainly focus on `Brute Force` and `Dictionary Attacks`. Both of these attacks will find the password by `brute forcing` the service.

Brute Force Attack

A `Brute Force Attack` does not depend on a wordlist of common passwords, but it works by trying all possible character combinations for the length we specified. For example, if we specify the password's length as `4`, it would test all keys from `aaaa` to `zzzz`, literally `brute forcing` all characters to find a working password.

However, even if we only use lowercase English characters, this would have almost half a million permutations - `26x26x26x26 = 456,976` -, which is a huge number, even though we only have a password length of `4`.

Once the password length starts to increase, and we start testing for mixed casings, numbers, and special characters, the time it would take to brute force, these passwords can take millions of years.

All of this shows that relying completely on brute force attacks is not ideal, and this is especially true for brute-forcing attacks that take place over the network, like in `hydra`.
That is why we should consider methods that may increase our odds of guessing the correct password, like `Dictionary Attacks`.

Dictionary Attack

A `Dictionary Attack` tries to guess passwords with the help of lists. The goal is to use a list of known passwords to guess an unknown password. This method is useful whenever it can be assumed that passwords with reasonable character combinations are used.

Luckily, there is a huge number of passwords wordlist, consisting of the most commonly used passwords found in tests and database leaks.

We can check out the SecLists repo for wordlists, as it has a huge variety of wordlists, covering many types of attacks.
We can find password wordlists in our PwnBox in `/opt/useful/SecLists/Passwords/`, and username wordlists in `/opt/useful/SecLists/Usernames/`.

Methods of Brute Force Attacks

There are many methodologies to carry a Login Brute Force attacks:

Attack	Description
Online Brute Force Attack	Attacking a live application over the network, like HTTP, HTTPs, SSH, FTP, and others
Offline Brute Force Attack	Also known as Offline Password Cracking, where you attempt to crack a hash of an encrypted password.
Reverse Brute Force Attack	Also known as username brute-forcing, where you try a single common password with a list of usernames on a certain service.
Hybrid Brute Force Attack	Attacking a user by creating a customized password wordlist, built using known intelligence about the user or the service.