## **Basic HTTP Authentication**

Web applications often employ authentication mechanisms to protect sensitive data and functionalities. Basic HTTP Authentication, or simply Basic Auth, is a rudimentary yet common method for securing resources on the web. Though easy to implement, its inherent security vulnerabilities make it a frequent target for brute-force attacks.

In essence, Basic Auth is a challenge-response protocol where a web server demands user credentials before granting access to protected resources. The process begins when a user attempts to access a restricted area. The server responds with a 481 Unauthorized status and a WWW-Authenticate header prompting the user's browser to present a login dialog.

Once the user provides their username and password, the browser concatenates them into a single string, separated by a colon. This string is then encoded using Base64 and included in the Authorization header of subsequent requests, following the format Basic <encoded\_credentials>. The server decodes the credentials, verifies them against its database, and grants or denies access accordingly.

For example, the headers for Basic Auth in a HTTP GET request would look like:

Code: http

GET /protected\_resource HTTP/1.1

Host: www.example.com

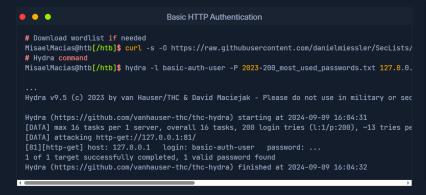
Authorization: Basic YWxpY2U6c2VjcmV0MTIz

## **Exploiting Basic Auth with Hydra**

To follow along, start the target system via the question section at the bottom of the page.

We will use the http-get hydra service to brute force the basic authentication target.

In this scenario, the spawned target instance employs Basic HTTP Authentication. We already know the username is basic-auth-user. Since we know the username, we can simplify the Hydra command and focus solely on brute-forcing the password. Here's the command we'll use:



Let's break down the command:

- -l basic-auth-user: This specifies that the username for the login attempt is 'basic-auth-user'.
- -P 2023-200\_most\_used\_passwords.txt: This indicates that Hydra should use the password list contained in the file '2023-200\_most\_used\_passwords.txt' for its brute-force attack.
- 127.0.0.1: This is the target IP address, in this case, the local machine (local host).
- http-get /: This tells Hydra that the target service is an HTTP server and the attack should be performed using HTTP GET requests to the root path ('/').
- -s 81: This overrides the default port for the HTTP service and sets it to 81.

Cheat Sheet

? Go to Questions

Table of Contents

Introduction

Introduction

Password Security Fundamentals

Dictionary Attacks

Hybrid Attacks

Hydra

Hydra

Basic HTTP Authentication

Clogin Forms

**Brute Force Attacks** 

Brute Force Attacks

Medusa

Medusa

Web Services

Custom Wordlists

Custom Wordlists

Skills Assessment

Skills Assessment Part 1

Skills Assessment Part 2

My Workstation

OFFLINE

● Start Instance

○ / 1 spawns left

