**BRUTE-FORCE ATTACK ON HTTP 0AUTH AUTHENTICATION Via THC-HYDRA**

**THC Hydra:**

Hydra is a parallelized network logon cracker. Hydra works by using different approaches of generating possible passwords, such as wordlist attacks, brute-force attacks and others. Hydra is commonly used by penetration testers together with a program named crunch, which is used to generate wordlists. Hydra is then used to test the attacks using the wordlists that crunch created.

**Background:**

Most the routers/modems provided by ISPs are protected by HTTP basic authentication and contains 5 or 6-digit strings randomly generated by companies using RE comprising of lowercase alphabets and numbers. It is not a secure way as these combinations can be breached very easily using brute-force method.

**Attack to be performed:**

We are going to use brute-force attack to a flask-based webserver to crack Auth0 authentication protocol using THC-Hydra. Parallel cracker will generate passwords sequentially using RE specified in the command. For the sake of testing we are going to use the same RE for password, but we are going to reduce password length to reduce number of attempts which will reduce time taken to exhaust possible combinations for password.

**Method: Brute-**

**Force**

hydra -l admin -x 2:2:1 -s 5000 -f 127.0.0.1 http-get /

-l: represents the username field. Could be a fixed string or a text file.

-x: represents the password field. Could be a regular expression to generate combinations or a text file.

-s: source port on which to attack launch followed by source address.

-f: If the security is breached, it stops the attack without checking next combinations.

http-get: method to make the call to source.

/: route on which to perform attack on.