

THC Hydra

Dictionary attack on flask web app protected via http 0auth Authenticaiton protocol

Ammar Khan

# Introduction to Hydra

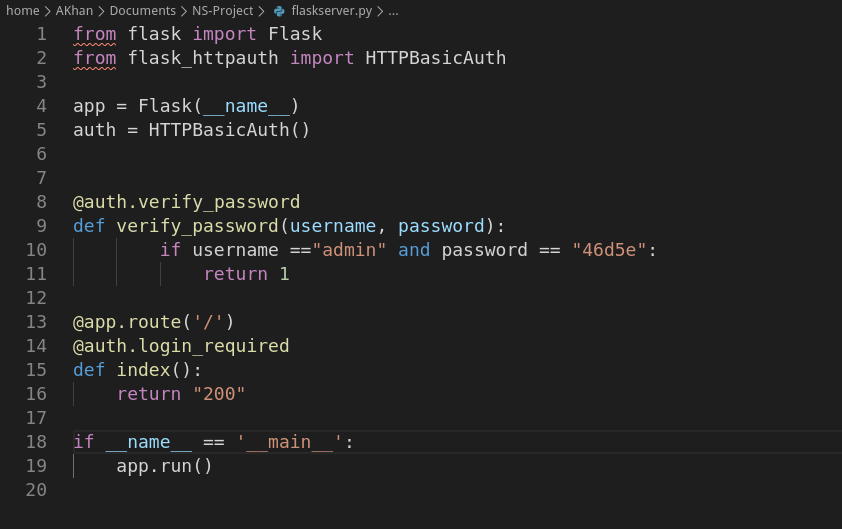
Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

# Problem Statement

All of the PTCL provided modems/routers are protected via HTTP BASIC Authentication protocol. All of them comes with a 5-character password with a mixture of lowercase alphabets and numbers. All of them have the same username as ‘admin’. This project reviews the strength of protocol and the combination of password strings.

# Methodology and Testing Environment

We have deployed a dummy Flask application server that is protected with HTTP Basic Auth protocol and the username is fixed to ‘admin’ and the password string is fixed as ‘46d5e’ , which is a string of length 5 with a mixture of lowercase alphabets and numbers between 0-9. Python code is as follow:



**Method: Dictionary attack with 10M passwords.txt file**

hydra -f -l admin -P passwords.txt -s 5000 -f 127.0.0.1 http-get /

-P: this argument accepts a text file which contains passwords

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

# Test Setup

**CPU:** Intel Xeon E-2276G @4.90 GHz

**RAM:** 64 GB DDR4

**Network:** loopback

**OS:** Fedora 31 with kernel headers 5.6.18-200.fc31.x86\_64

**Penetration Tool:** Hydra v9.0 (c) 2019

**Target**: Flask version 1.1.2

# Results

Attack was started on 2020-06-24 22:06:57 and it completed on 2020-06-24 22:09:05, which is roughly 3 minutes. But, it depends on luck, I-e the password is luckily in the dictionary file. Dictionary files are generated based on leaked passwords on the internet

