House Snake

By Shaun Kämmerling

Typical Day at the Office

Aim

To introduce the world to House Snake.

Introduction

House Snake is a HTTP Basic Authentication Brute Forcing tool that I made as my Sensepost Academy research project. I named it house snake because it was programmed using python, and much like its namesake, it isn't very threatening.

Introduction cont

Scope

- HTTP Basic Authentication
- The Beginning
- The Middle
- The End
- Usage
- Conclusion

HTTP Basic Authentication

HTTP Basic Authentication

HTTP Basic Authentication is the simplest technique for enforcing access control to web resources. It does not make use of cookies, session identifiers or login pages. Instead it makes use of standard fields in the HTTP header.

The username and password are combined in to a string “username:password”. The resulting string is then base64 encoded and inserted into the request header. If the username and password are valid, the response code from the website will be 200 OK. Otherwise the response code is 401 UNAUTHORIZED.

HTTP Basic Authentication

Basic authentication does not provide any confidentiality protection for the credentials. Therefore HTTPS is generally used in conjunction with Basic Authentication to provide a measure of security.

Example **Authentication: Basic dXNlcm5hbWU6cGFzc3dvcmQ=**

HTTP Basic Authentication cont

The Beginning

The Beginning

Before starting the process of building House Snake I had to research a few things:

- What is HTTP Basic Auth
- How to test House Snake
- How to Host a website locally
- How to interact with my website using Python

The Middle

The Middle

With the initial research out the way I began the task of building House Snake. I started by first learning how to make my tool interact with my website. I made use of a single URL, one username and one password.

After getting that to work I stepped it up by writing a few more functions that will enable my script to make use of lists for the different parameters.

For House Snake to target multiple targets I had to host multiple targets. After some research I was able to host 5 unique websites on my host machine.

I incorporated the *argparse* module to enable the user to customize the usage with command line arguments.

The End

(Not the end of the presentation)

The End

The research project instructions included some requirements that House Snake had to conform to. The list of targets must be a CSV file, and the tool must be able to output the results to a JSON file.

I spent a while working with the needed modules before I was able to fulfill these requirements. Once the basic coding was complete I spent some time incorporating a few quality of life modules.

Usage

Usage

House Snake is a Linux command line tool. It has been programmed in python 3 but makes use of some python 2 modules. To avoid unnecessary errors it should be run using python 2.

It takes a target URL, a username and password and attempts to access a website. It also accepts lists of urls, usernames or passwords. Any valid username and password pairs will be output to the terminal. Using the verbose will also display the failed attempts.

When the output flag is used, the output will be saved to a json file in the current directory.

The different options can be displayed with the help flag.

Usage cont

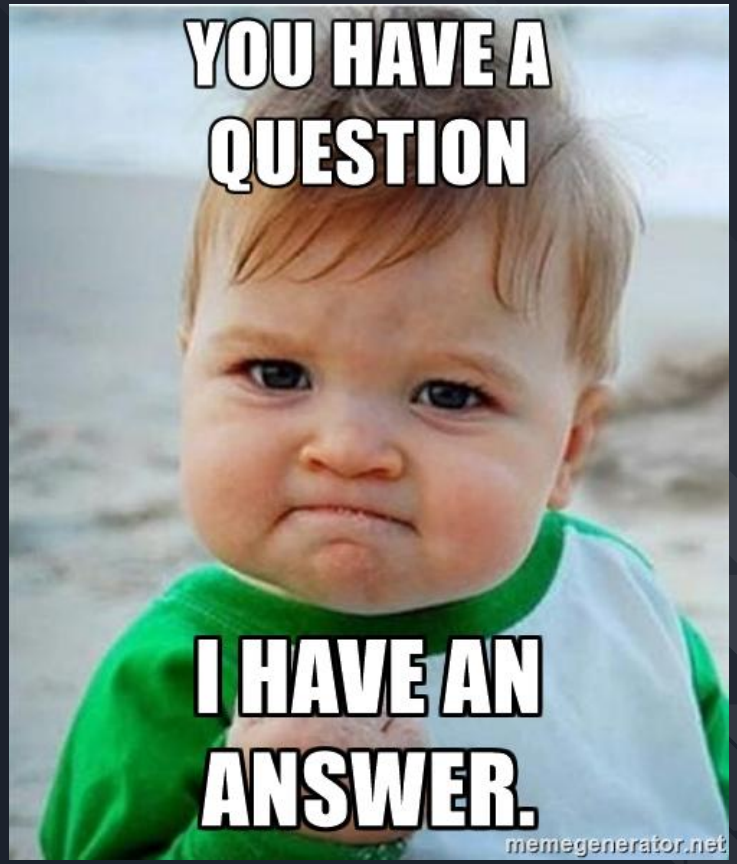
[INSERT DEMO]

Conclusion

Conclusion

Working on this project has been a great learning experience. Even though it was frustrating at times, I did enjoy it. I liked working on a problem and finally finding a solution to it. House Snake is not very pretty or very useful, but it works as intended, and it is mine.

Questions?




END OF PRESENTATION
THANK YOU FOR YOUR ATTENTION
memegenerator.net