Technical Answers for Real-World Problems

Review 0

Kushal (18BCE0557)
Siddhartha Varma (18BCE0865)
Akshit Kumar (18BCE0522)

Project Domain - Information Security

Project title - Fast Recon Framework (ReconChimp)

Objective - To create a framework that can do the necessary reconnaissance needed for ethical hacking, in an efficient and faster way to generate on the point results with lesser computation power.

Problem statement

Ethical Hacking is a very important part of modern InfoSec infrastructure. It is necessary to have due to its ability to recognise and identify security weaknesses before someone with malicious intent can exploit them. Ethical hackings first and one of the most important steps is reconnaissance, in which the hacker gathers important URLs and fuzz them with the intention of expanding the attack surface. The problem is that Reconnaissance is a very resource intensive and time consuming process. Modern advancement in technology has ensured more affordable and more powerful computers than ever, but these resources are still not enough to provide Reconnaissance at an affordable level to an average programmer, so we need a way in which we can do the necessary enumerations without sacrificing the quality of our work.

Abstract

An automated reconnaissance framework meant for fast enumeration of an organization. It will have customizable scan engines, which can be used to enumerate the subdomains, endpoints, or gather information. The beauty of ReconChimp is that it will gather everything in one place with a great speed and will be less resource intensive. This framework will be more focused on passive reconnaissance techniques such as google dorking, js file enum, censys and wayback url results to speed up the complete process of reconnaissance rather than active reconnaissance techniques like dir brute forcing etc. It's a smart recon framework which is made with speed and on the point results in mind. It will have a pipeline of reconnaissance, which will be highly customizable. Additionally, it'll also be offered as a service which can be consumed as an API.

References -

[1] Performing Reconnaissance - Multiple Authors
(https://www.sciencedirect.com/topics/computer-science/performing-reconnaissance)

[2] Ethical Hacking: need for Cyber-Security
(https://ieeexplore.ieee.org/abstract/document/8391982/)

[3] Performing Evaluation of Cyber-Sec Tools
(https://www.inderscienceonline.com/doi/abs/10.1504/IJIPSI.2016.078589)

[4] Testing for Security Weakness of Web Applications using Ethical Hacking
(https://ieeexplore.ieee.org/abstract/document/9143018/)