WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Spider Foot Thread Security Map

Arul.A*

Chennai 600095

A B S T R A C T

Network security refers to precautions and activities designed to protect the availability and integrity of data exchanged between the network and the digital world. Information security protects digital data from unauthorized access, disclosure, manipulation, alteration or destruction using both hardware and software technologies. According to an analysis by experts working in the field of information security, more than twenty thousand cyber-attacks per month are being made to a medium-sized company. As a result of the analysis carried out, it has been determined that although the level of risk is not high in most of the attacks, it is an intense danger for important data and the severity of these attacks is increased. Systems that provide real-time analysis.

Keywords: Spider foot threat security map, Network security, Cyber security

1. Introduction

Spider Foot Threat Security Map is intelligence automation tool. It integrates with just about every data source available and utilises a range of methods for data analysis, making that data easy to navigate.
It has an embedded web server for providing intuitive web-based interface but can also be used completely via the command-line. It's written in Python 3 and GPL-licensed.

1.1. Objectives

An analysis to carry out in order to determine the level of risk is not high in most of the attacks, The cyber-attack can be intense danger for important data and the it will be increased in terms of severity. Spider foot will provide real-time analysis

1.2. Proposed system

Spider Foot Threat Security Map is a reconnaissance tool that automatically queries over 100 public data sources to gather intelligence on IP addresses, domain names, e-mail addresses, names and more.

1.3. Module description

Phone number extractor: identify phone numbers, and lookup carrier information in Google's lib phone number DB

Account finder: Identify the existence of a given account on various sites

Whois: searching Whois servers for domain names and netblocks identified

BGPView: Obtain network information from BGPView API

* *Arul.A Tel: +916381673320*
E-mail address: aruljaiseeman@gmail.com

DNS Raw: Retrieves raw DNS records such as MX, TXT and others.

1.4. Significance

. Spider foot will integrate with every data source available and utilizes a range of methods for data analysis, making that data easy to navigate.

1.5. Methodology

An embedded web-server for providing the back-end support and intuitive web-based interface but can also be used completely via the command-line which developed under python3 libraries and GPL licensed

1.6. Originality of the project

The new Network security approach needs to designed to protect the availability and integrity of data exchanged between the network and the digital world. Information security protects digital data from unauthorized access, disclosure, manipulation, alteration or destruction using both hardware and software technologies.

1.7. Conclusion

An automated tool and embedded web-server has been designed and developed to provide a user friendly and intuitive web-based interface for Spider Foot Threat Security Mapping.

REFERENCES

Vacas et al., (2018) [30] outlined a method for using threat intelligence data acquired from open-source intelligence feeds to improve the accuracy and capabilities of intrusion detection systems.

Hayes & Cappa (2018) [28] have demonstrated that OSINT may be used to do risk assessments for the company in order to prevent potential cyber-attacks on its critical infrastructure

Herrera-Cubides et al., (2020) [32] conducted a study with an aim to investigate the evolution of production of research and study material in OSINT platform. This analysis looks at two of the material sources of OSINT such as research knowledge distribution databases and repositories pertaining to educational resources