International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Vulnerability Assessment and Penetration Testing using Webkill

Deepesh Seth[1], Ms. N. Priya[2]

[1]Master of Computer Application, [2]Assistant Professor,
[1,2]Department of MCA, Jain Deemed-to-be University, Bangalore, Karnataka, India

ABSTRACT

Data is more defenseless than any time in recent memory and each mechanical development raises new security danger that requires new security arrangements. web kill tool is directed to assess the security of an IT framework by securely uncovering its weaknesses. The performance of an application is measured based on the number of false negatives and false positives. Testing technique that is highly automated, which covers several boundary cases by means of invalid data as the application input to make sure that exploitable vulnerabilities are absent.

Keywords: *Information Gathering, Exploit Vulnerabilities, analysis victim sip address*

How to cite this paper: Deepesh Seth | Ms. N. Priya "Vulnerability Assessment and Penetration Testing using Webkill" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.357-360, URL: www.ijtsrd.com/papers/ijtsrd37919.pdf

IJTSRD37919

INTRODUCTION

The subject that is chosen is Web Kill Tool which is a kind of a Testing some vulnerable websites and ip address where you can get the information about the victims systems or can be an vulnerable system of an organization. Because it's an penetration testing tools which you can scan some vulnerability url's to gather information and exploit some vulnerability of an victims system. In penetration-testing tools is to automate certain tasks, improve testing efficiency and discover issues that might be difficult to find using manual analysis techniques alone. The topic that is selected is The Web kill is an type of an information gathering tool. In this tool have several different tool which can get the information through victims Ip address or any website where you get different information from the different tool and it also analyse the victims details like in this project where have many tool like trace route, also called trace path or tracert, is a network tool used to determine the path packets take from one IP address to another. And another one is Who is it is an internet service used to lookup the information about the domain name etc. This type of tools I have used to make that project to gather information.

In this project i am using python programming in the projects tools and also run in kali linux, you can also do that project in windows but i am run this tools in kali linux. I am doing this project because when a hacker can do hack to any victims first steps is to gather information about the victims than attack to the victims system where you can get many personal information about the victims

Description of Research work

Problem Statement:

The problem statement of this project would be to make or create a successful through python programming where the tools made for testing the vulnerability of websites and some vulnerable system to exploits their vulnerability and analyze them.

Proposed System:

This project is going to solve the above mentioned problem by making the tool free, open source, fast and lightweight. The proposed system aims at overcoming the disadvantages of the system in existence by providing a better solution in terms of gathering data. In this project maximum data gathered at once will be 20MB it could be any file, larger files cannot be gathered.

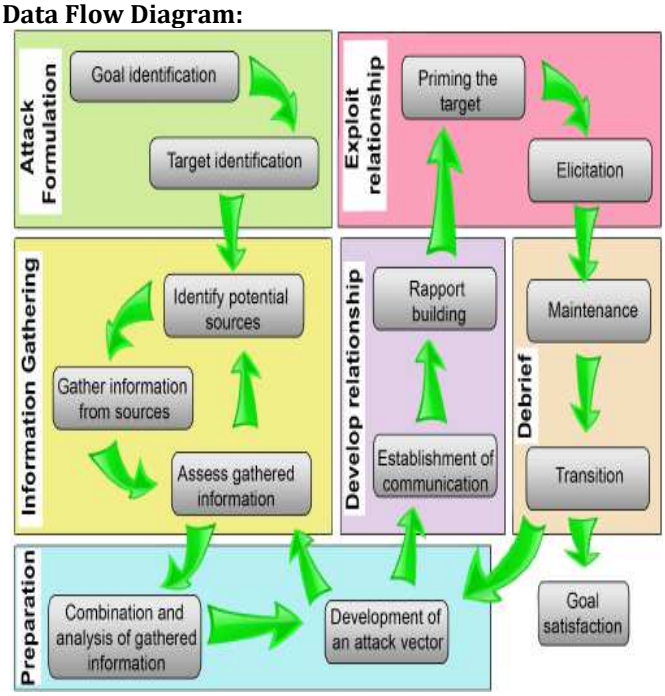
Motivation:

The motivation of this project is to make an effective open source Web kill Penetesting tool.

Scope:

The objective and scope of Mini Project Web Kill Tool it's an Penetesting Tool which can scan the ip address to get gather information. In this there are many different testing tools which are also scan the url to get the information in the different data which the help of some mini tools. We can also check some vulnerable website to get some organization data or an some personal information through scan some random vulnerable ip address.

Data Flow Diagram:



Tool Description:

Information Gathering

Information gathering is an art that every penetration-tester (pen-tester) and hacker should master for a better experience in penetration testing. It is a method used by analysts to determine the needs of customers and users. Techniques that provide safety, utility, usability, learn ability, etc. for collaborators result in their collaboration, commitment, and honesty. Various tools and techniques are available, including public sources such as Who is, nslookup that can help hackers to gather user information. This step is very important because while performing attacks on any target information (such as his pet name, best friend's name, his age, or phone number to perform password guessing attacks(brute force) or other kinds of attacks) is required.

Information Gathering Techniques

As a ethical hackers it utilize a major assortment of tools and techniques to get this valuable data about their objectives, just as areas and information assortment programming they'll be utilizing towards the data gathering objective.

Let's look at the top methods used to gather information about any target.

Social engineering: This remembers for individual visit, telephone discussions and email satirizing assaults. What every one of these techniques share for all intents and purpose is the brain research of human shortcoming, expected to get greatest information about the objective.

Search engines: Web crawlers can be utilized to bring data about anything, and this incorporates organizations, people, benefits, and even genuine hacks, as found in our past article about Google Hacking.

Social networks: Facebook, Twitter, LinkedIn and other informal organizations are incredible wellsprings of data to manufacture a profile, particularly while focusing on people.

Domain names: These are enlisted by associations, governments, public and private organizations, and individuals. Accordingly, they're an extraordinary beginning stage when you need to research somebody. Individual data, related areas, tasks, administrations and advancements can be found by examining space name data.

Internet servers: legitimate DNS workers are an extraordinary wellspring of data, as they frequently incorporate each and every surface guide uncovered toward the Internet—which implies an immediate connect to related administrations, for example, HTTP, email, and so forth. In our past article about detached DNS, we investigated the significance of DNS workers, and particularly aloof DNS-recon administrations, for example, the ones we offer here at Security Trails.

Every one of these procedures are truly helpful when joined with big business security apparatuses. Continue perusing to find how to boost your data gathering results by utilizing some truly cool infosec utilities.

Ordinary infiltration testing apparatuses can be arranged into a few structures dependent on the kind of testing they perform. The various classifications are as per the following:

Host-Based Tools: Host-based testing instruments generally run a chain of tests on the nearby working framework to find its specialized shortcomings and qualities. They can confirm other normal design botches just as exclusions in the OS.

Network-Based Tools: Network-based testing apparatuses are intended to check the security setup of an OS from far off areas over an organization. These testing apparatuses may evaluate the fix condition of the product for network administration, look into any undesirable organization administrations and powerless organization benefits that are empowered, etc.

Application Testing Proxies: This apparatus permits the security analyzer to focus more on the graphical UI side while testing a Web administration or Web application.

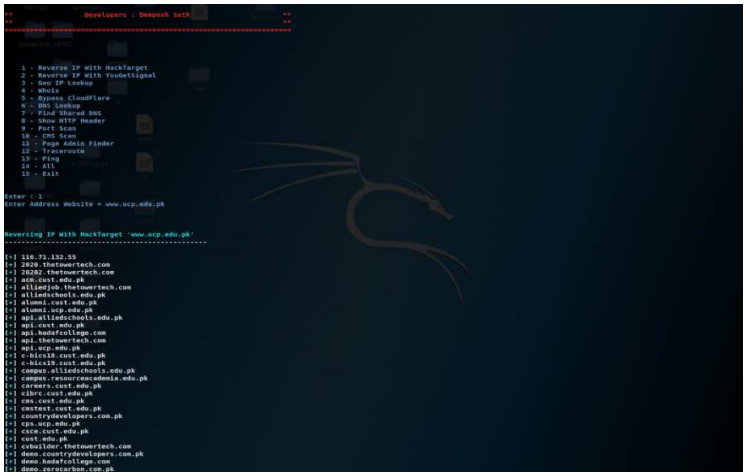
Application Scanning Tools: This apparatus is the most recent section in the class of infiltration testing instruments. These apparatuses help to perform entrance testing sweeps of programming applications utilized for general purposes.

Infiltration testing apparatuses give a speedy and straightforward approach to recognize explicit security weaknesses. They are amazingly natural, and can even be worked by beginner clients.

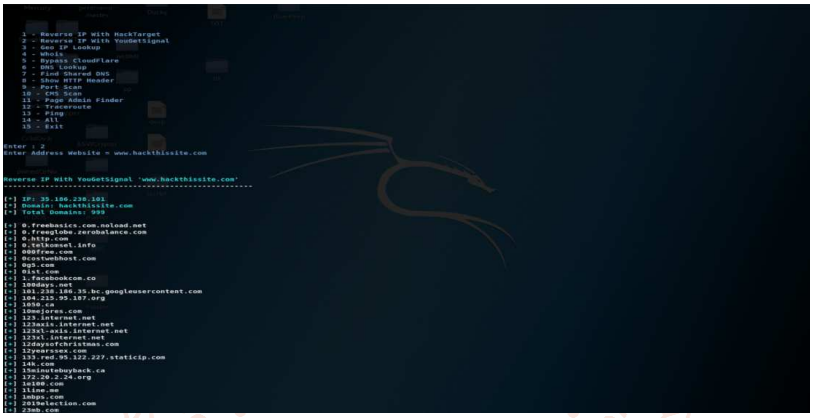
Penestesting Tools:

1. Reverse IP Address with Hack Target:

Reverse IP Lookup is a unimaginably amazing asset with some high-esteem business applications. Recover a rundown of all spaces utilizing a similar IP address as you, and having similar assets Track down malignant conduct of phishing or defrauding sites that live on a similar hosts.



2. **Reverse IP Address with You Get Signal:** The You Get Signal is a features that gives an opposite IP query highlight. In layman's terms, the site will attempt to get the IP address for each hostname entered and afterward it will do a converse IP query on it, so it will find different hostnames that are related with that specific IP. An exemplary circumstance is the point at which the site is facilitated on a mutual worker. On the off chance that we had the errand of entering a site, at that point we could do a converse query for the site hostname on You Get Signal and afterward endeavor to break into different destinations (if in scope). At that point we could heighten advantages to get into the objective site facilitated on a similar worker.

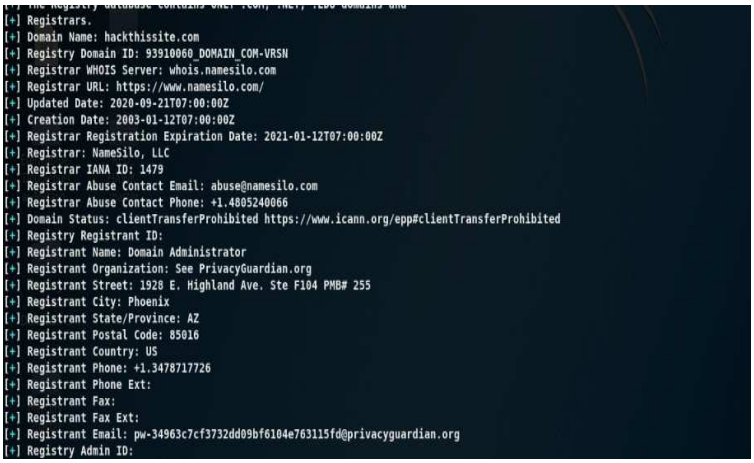


3. **Geo IP Lookup:** IP Geolocation involves attempting to discover the location of an IP address in the real world. IP addresses are assigned to an organization, and as these are ever-changing associations, it can be difficult to determine exactly where in the world an IP address is located. Different services provide databases of this information for public use. Maxmind is one of the most well known. Its service is used for many things including fraud prevention. As an example, a merchant can use the IP location of a customer to cross-reference with Credit Card data to reduce credit card fraud.

4. **Whois Lookup:**

Whois is a service that provides basic information about a registered domain, such as domain owner contact information, domain availability status and the company with which the domain is registered (also called the Registrar).

A. Owner of website.
B. Email id used to register domain.
C. Domain registrar.
D. Domain name server information.
E. Related websites



5. Port Scan:

Port Scanning is the name for the technique used to identify open ports and services available on a network host. It can be used to send requests to connect to the targeted computers, and then keep track of the ports which appear to be opened, or those that respond to the request.

Future Scope

This tool is python based and, this might be worked upon in the future. More features related to penetesting tool will be added in the future. There are various future scopes for the tool, firstly that is a testing were you can collect the information of an vulnerable ipadress, secondly analysis the data and implement.

Conclusion

Information gathering is only one of the underlying advances taken during most infosec examinations, and there are numerous approaches to do it, with various strategies and apparatuses. While leading exploration on any objective, you'll be shocked at how much information you get about the host or space name you are examining.

References

[1] *Anderson, Ross J. (2008). Security engineering: a guide to building dependable distributed systems (2nd ed.). Indianapolis, IN: Wiley. p. 1040. ISBN 978-0-470-06852-6.* Chapter 2, page 17

[2] **^** *"Social Engineering Defined". Security through Education. Retrieved 3 October 2018.*

[3] **^** Lim, Joo S., et al. "Exploring the Relationship between Organizational Culture and Information Security Culture." Australian Information Security Management Conference.

[4] **^** Anderson, D., Reimers, K. and Barretto, C. (March 2014). Post-Secondary Education Network Security: Results of Addressing the End-User Challenge. publication date 11 March 2014 publication description INTED2014 (International Technology, Education, and Development Conference)

[5] ^Jump up to: *[a] [b] [c] Schlienger, Thomas; Teufel, Stephanie (2003). "Information security culture-from analysis to change". South African Computer Journal.* ***31****: 46–52.*

[6] **^** Jaco, K: "CSEPS Course Workbook" (2004), unit 3, Jaco Security Publishing.