Web Penetrator – Web App Penetration Testing Tool

Raj Saundatikar*[1], Lakshmi J.V.N*[2]

[1,2]*Department of MCA, Jain University, Bangalore, Karnataka, India.*

[1]*rajsaundatikar@gmail.com*

Abstract—*Everyday new web applications are being developed and used extensively, it is important for developers and testers to improve application security. Penetration testing is a technique that helps developers and testers to ensure that security levels of the web application are at the acceptable level. It is mandatory to perform pen testing regularly to avoid potential risks. Penetration testing is not only restricted to web apps but it can also be performed on IoT devices, networks, computer systems, mobile applications, etc. The goal of this tool is not to cause damage, but instead to identify attack surfaces, vulnerabilities, and other security weaknesses from the perspective of an attacker.*

Keywords– *Penetration testing, Shodan, Traceroute, IP Lookup, whois, ICMP*

I. INTRODUCTION

These days, web applications are used world-wide by users for their personal needs but what make web applications a lot more important are the business intentions to use the web. The wide usage of Web applications and services poses new security challenges on developers, testers, hundreds of new vulnerabilities are being discovered annually, and dozens of new patches are being released monthly. So, sensitive data manipulated for these applications must be protected against the attackers who are trying to find vulnerabilities in this kind of applications, these vulnerabilities come from many sources starting from poor written code.

Web Penetrator can collect useful information about target web applications, such as ping, traceroute, DNS Lookup, Reverse DNS Lookup, Host Records (Subdomain), Shared DNS Servers, Zone Transfer, Whois Lookup, GeoIP Lookup, etc.. Based on this information an ethical hacker gets important knowledge of the target system. Information such as open ports, services running on those ports, and any vulnerable applications they have installed. Moreover, web penetrator can perform some miscellaneous tasks like generating defaced pages, random passwords and message digests.

II. NEED FOR THE STUDY

- Identify unknown vulnerabilities
- Test publicly exposed components, including routers, firewalls and DNS
- Determine vulnerable route for an attack
- Look for loopholes that could cause data theft

III. DESCRIPTION OF THE RESEARCH WORK

A. Problem Statement

Most of the penetration testing software in the market are paid and the size of the software is also big. This project is going to solve the previously mentioned problem by making the tool free, open source, fast and lightweight.

B. Methodology

Web application pen testing is a process that utilizes various techniques on your applications to recognize any existing security risks. Web application developers often accidently overlook security as they focus on code development, visual design, and app management, which is completely understandable. These are all significant components of a good website or mobile app. Web application penetration testing effectively fills the security gap and guarantees all of your web applications are as secure as they can be.

C. Motivation

The purpose of web app penetration testing tool is to explore your business from the perspective of an attacker and mostly to discover and understand the various weak points that can be present in your environment and how to protect your business from them.

D. Scope

The goal of this tool is not to cause damage, but instead to identify attack surfaces, vulnerabilities, and other security weaknesses from the perspective of an attacker.

E. Requirements

Hardware: 2GB RAM, 1GB Storage Space
Software: Windows OS / Linux OS, Python

IV. MODULE-WISE DESCRIPTION

Web Penetrator is a python tool developed for the purpose of information gathering from the target system, which is helpful to find vulnerabilities in the system. It consists of modules such as whois lookup, traceroute, DNS Lookup, Reverse DNS Lookup, GeoIP Lookup, Port Scan, IP Lookup, http header check and Extract Link.

A. Whois lookup

With whois lookup you can easily and quickly find the ISP, hosting provider and contact details for a domain or IP address. There are many uses for whois which can be utilised by cybercriminals and defenders in information security. It is also beneficial for tracking down attackers while defending or finding targets to attack when on the offensive. whois lookup can reveal organisational information, IP ranges to scan and the email addresses of technical staff. This information can be found in the information gathering phase of an assessment or planned attack.

B. Traceroute

It is a network test term used to test number of hops that communication will follow across an IP network. As we all know, the name of the tool used to perform tracing usually uses Traceroute on Linux-based systems and Tracert on Windows operating systems. There are also other variants on these such as tcptraceroute. All tools have similar functions, but have different tracking functions or methods. It is a very good way to see the route of your network connection is taking as it traverses the globe. However, the common reason is its use by computer and network professionals to diagnose problems in a network path. Traceroute can pin point routers that has high response times, indicating network congestion or other problems.

C. DNS Lookup

This domain has multiple related records. You can query the DNS server to find the IP address of the main domain, mail server, DNS server, and other elements (such as SPFrecords). Various tools provide this feature, a common one being nslookup which is available on many operating systems including most Linux distributions and Microsoft Windows. Another tool available on Linux-based systems is the Dig tool. Usually, this is an advanced tool that contains many features not found in nslookup.

D. Reverse DNS Lookup

A reverse DNS record is simply an entry that converts an IP address back to a host name. Most users are familiar with forward lookup, also known as an A record that searches an IP address from a host name so that an Internet service is able to be accessed. When an attacker or penetration tester evaluates an organization, they will commonly try to map the footprint of the organization in order to find the all the weak points to attack. By gathering records of possible IP addresses, host names and IP network blocks that are related to the targeted organization an attack surface is able to developed. In addition to resolving a single IP address, this reverse DNS tool also allows you to resolve a range of IP addresses or search for all reverse DNS addresses that contain domain names.

E. GeoIP Lookup

IP Geolocation attempts to find the location of an IP address in the real world. IP addresses have been assigned to organizations, and they are constantly changing associations. It may be difficult to determine exactly where the IP address is in the world. The database of this information is for public use.

F. Port Scan

Port scanning method is used to determine open ports and services available on a network host. It is sometimes used by security professionals to audit computers for vulnerabilities, it is also used by hackers to target victims. It can be used to send requests to connect to the targeted computers and monitor ports which appear to be opened, or those that respond to the request.

G. Reverse IP Lookup

This method known as Reverse IP Lookup is a way to identify hostnames that have DNS records associated with an IP address. The Web server can be configured to provide services for multiple virtual hosts through a single IP address. This is a common method in shared hosting environments. It is also common in many organizations and can be good way to extend the attack surface when going after a web server. For example, if your main target website appears to be secure, you can access the underlying operating system by attacking a less secure website on the same server. Bypass the security controls of the target website.

H. Extract Link

The purpose of this tool is to provide a fast and easy way to extract links from a web page. Domains and resources

and listing links that a page links to can tell you a lot about the page. There are various reasons for using such tool from web page testing, web page development to security assessments and internet research.

I. HTTP header check

Information can be collected in a check of the HTTP Headers from a web server. Server side software can be diagnosed often down to the exact version running. Web application technologies, cookie strings and other data can be gathered from the HTTP Header. This gathered information can be used when troubleshooting or when planning an attack against the web server.

J. Ping

Ping is used to decide the connectivity and latency of internet connected hosts. Ping is a network troubleshooting tool that shows the response time between two internet addresses. By default ping tools are installed in most operating systems. It does not matter if you are using any OS such as Solaris, Windows, FreeBSD or Ubuntu Linux; ping is ubiquitous. Ping uses specific type of packet known as ICMP, commonly known as ICMP request and ICMP reply.

V. FUTURE SCOPE

In the future we can add more features like

Zone transfer: Zone transfer will attempt to get all DNS records for a target domain.

Find Shared DNS Servers: Find hosts sharing DNS servers.

TCP Scan: To determine the status of an Internet facing service or firewall.

Banner Grabbing: To discover network services by querying the service port.

VI. CONCLUSION

This tool is suitable for cyber security enthusiasts because it makes the requirements in extracting, gathering and analysing information efficient. If a website is hacked then the attacker can steal confidential data and can affect web application availability. Thus securing web applications is crucial. Web application penetration testing effectively fills the security gap and guarantees all of your web applications are as secure as they can be.

VII. REFERENCES

[1] https://ieeexplore.ieee.org/abstract/document/9036175

[2] https://ieeexplore.ieee.org/document/8378035

[3] https://www.redteamsecure.com/approach/web-application-penetration-testing-methodology

[4] https://www.researchgate.net/publication/269978805_WAPTT_-_web_application_penetration_testing_tool

[5] https://www.researchgate.net/publication/328358747_Study_on_Penetration_Testing_of_Modern_Web_Application_Vulnerabilities