International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

Cross Platform Penetration Testing Suite

Ms. Shyaml Virnodkar, Rahul Gupta, Tejas Bharambe

[1]*Asst Professor, Department of Computer Engineering, K J Somaiya Institute of Engineering and Information Technology, Sion, Mumbai*
[2,3] *Student, Department of Computer Engineering, K J Somaiya Institute of Engineering and Information Technology, Sion, Mumbai*

Abstract *- As the computer literacy is increasing day by day, the threats to the end users is growing rapidly. As the users are increasing there is also a growing need for information security. In order to keep itself and its users safe in the cyberspace, various corporations conduct compliance audits of their systems. A part of the compliance audit is Vulnerability Assessment and Penetration Testing (VAPT). Ethical Hackers test the security of various system components and report it to the management for their further addressable. In order to carry out the tests needed, the Ethical hackers have to use tools to ease their task. These tools run on machines like Desktop or Laptop, which in turn reduces the portability. Cross platform Penetration Testing Suite will facilitate the use of these tools on any mobile device, thus having a testing device in a Ethical hacker's pocket. The suite will have packages of standard penetration testing tools and a UI will be provided to the end user to use it more efficiently. This suite does not require root access of the user's phone.*

Keywords - Penetration Testing; Android; Ethical Hacking tools.

I.INTRODUCTION

The number of users in the cyberspace is increasing at a great pace, and there is still a lot of arena of users needed to be covered. The estimated number of internet users in 2017 was 3.58 billion[1],while the estimated total population of the world is 7.6 billion[2].On the other hand, the global losses from cyber attacks is estimated to be $400 billion each year[3].The ever-increasing numbers of users along with the population growth with the addition of the existing insecure systems, makes the cyberspace vulnerable to use. The corporations providing different services in the cyberspace have to focus on the security of their implemented and to-be implemented infrastructures.

Penetration testing is a type of security testing that is used to test the insecurity of an application. It is conducted to find the security risk which might be present in the system. If a system is not secured, then any attacker can disrupt or take authorized access to that system. Security risk is normally an accidental error that occurs while developing and implementing the software. For example, configuration errors, design errors, and software bugs, etc. Penetration testing is one of potential solutions to support and enhance the security practice. It is a technique used by ethical hackers to simulate attacks and looks for the security weakness, before the real hacker attacks the system. Metasploit, Nessus, Kali, Burpsuite and Cain & Abel are example of famous penetration testing tools.

Even though there are many penetration testing tools on the internet to be used on mobile phone, all the existing tools require root system access and many users do not have their phones rooted as it voids the warranty of the phone and also it is very difficult for the user to install and use those tools. In this paper, we develop a testing kit called Cross platform Penetration testing Suite which compiles selected penetration testing tools necessary to test networks and web application. The main Objective of this tool is to provide very easy access to the tools and increase portability while conducting penetration testing.

The contributions for this work can be described as follows. First, we create a solution for one stop service for performing the penetration testing, which will cover basic tools to start-off the penetration testing. Our tool can scan the host for open ports, conduct xss injection, detect ssl vulnerabilities, generate a payload and lookup the who is directory for information, carry smtp exploitation, conduct a nessus scan. Second, it will eliminate the task of carrying a big device, thus giving an array of tools in a Ethical Hacker's pocket

II. BACKGROUND AND RELATED WORKS

A. Kali Linux

Kali Linux [4] is the operating system for ethical hacking, digital forensics, advanced penetration testing and security auditing. It includes more than 400 penetration testing tools or programs in order to test networks on their organizations' behavior to see vulnerabilities of each device. Penetration testing tools in Kali that can be categorized as followings: Information Gathering, Vulnerability Identification, Penetration Testing, Wireless Attacks, Web Application, Digital Forensics, Sniffing and Spoofing, Password Attacks, and Reverse Engineering. Kali Linux is every popular among security experts who know well what tools and commands they need for each penetration testing case. However, it is not possible to use it on the mobile device.

B. CVE and CPE

CVE or Common Vulnerabilities and Exposures is a dictionary of information security vulnerability names

provided by MITRE. CVE database provides several types of vulnerability names such as vulnerability scanner database, software vendor patches and updates. On the other hand, Common Platform Enumeration (CPE) [5] are used to search the vulnerability on CVE for each platform. CPE is a used for making security measurable in most of technology industry.

C. Metasploit Payload.

Metasploit Pro [6] is an exploitation and vulnerability validation tool that helps divide the penetration testing workflow into smaller and more manageable tasks. With Metasploit Pro, one can leverage the power of the Metasploit Framework and its exploit database through a web based user interface to perform security assessments and vulnerability validation. A payload is the shell code that runs after an exploit successfully compromises a system. The payload enables one to define how to connect to the shell and what one wants to do to the target system after taking control of it. A payload can open a Meterpreter or command shell. Meterpreter is an advanced payload that allows to write DLL files to dynamically create new features as per need.

D. Vulnerability Scanner-Nessus.

The world's most widely used vulnerability Management software, Nessus, is currently used by 23000 organisations [7].Nessus is used for vulnerability assessment, which includes the vulnerability detection, determining their severity to the system and possible solutions to patch those vulnerabilities.

E. Related Works

There are some works that are related to penetration testing using the android device. Kali Net hunter [8] is a kit which provides features for conducting only specific tests like keyboard attacks, wireless attacks, MITM bad usb attacks etc. Also this product works on only one plus one and selective Nexus device, which are costly, thus creating a hurdle to use this product on any generalized android phone. This product also requires root access to system folders thus reducing the number of users. Their product has a user interface for selecting the type of tests ,and redirecting the user to cli(command line interface) for results. Their works are similar to us, but we have some tools that are not in their product and certainly of very much help to the user. To the best of our knowledge, there is no existing penetration testing suite like ours that is specifically designed to give a great interface, works on different mobile platforms of Android, Windows, ios, blackberry etc. and considering delicate needs of the Ethical Hackers.

III. ANALYSIS AND DESIGN

A. System Architecture and Overview

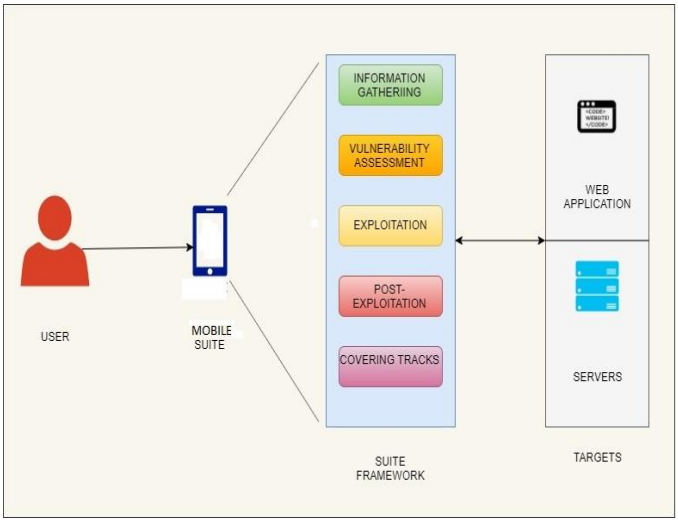


Figure 1.Android Penetration Testing Suite System Architecture

Fig. 1 illustrates the system architecture of Cross Platform Penetration Testing Suite. The Suite interacts with the user through the material User interface that runs on the android operating system. The target, web application and the servers on the network are on the right hand side of the figure. The product framework consists of five stages (1)Information gathering, (2)Vulnerability Assessment, (3)Exploitation (4)Post- Exploitation, (5)Covering Tracks.

Moreover, to perform penetration testing with the target devices, Suite uses wireless interfaces which are WI-FI or Bluetooth to communicate and penetrate the target device.

B. System Structure Chart

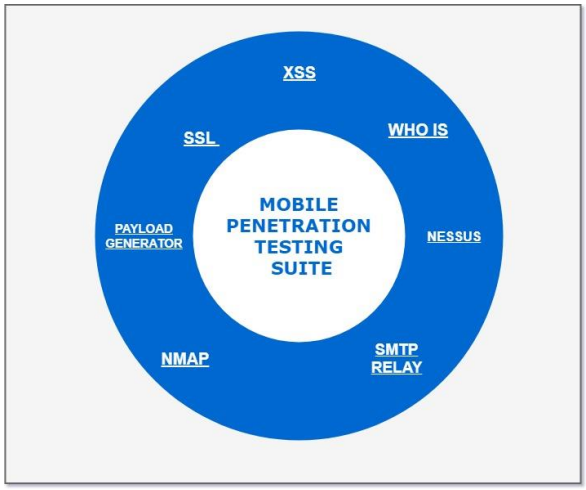


Figure 2.Structure Chart

Fig. 2 shows the Suite Structure Chart.

The detailed description of each module are given below:-

- *Whois*-This is a directory of domains and contain information regarding the owners and name servers of the domain. The tool will search the directory and will return results tailored to the user's need.
- *Nmap*-This tool scan the given host and returns the results as required by the user. Generally this tool is used for port scanning, OS detection by Ethical Hackers. Following options will be available to the user in Nmap.
    - All Scan
    - Ping Scan
    - UDP Scan
    - Intense Scan
    - Os detection
    - Traceroute
    - Quick Scan
- *SMTP open relay*-In big enterprises, mail servers are used for communication. If these mail servers are not configured properly then, an attacker can take advantage of this and fill the mail server with spoofed emails from non-existing or unknown email ids.
- XSS Scan-Cross site scripting has been listed in OWASP top 10 2017[9].It is a flaw that most of the developers are unaware of and thus is a major problem. Our module uses xsssniper [12],an open source tool to detect xss vulnerabilities. It is used on the server side thus reducing testers problem to install this tool.
- SSL vulnerability scanner-Secure socket layer encryption is used when security is a priority while hosting a web application. Our tool detects various ssl vulnerabilities and specifies vulnerabilities like Heart bleed, ticket bleed etc.
- *Payload Generator*-A payload is the shell code that runs after an exploit successfully compromises a system. The payload enables one to define how to connect to the shell and what one wants to do to the target system after taking control of it. The Generator will have options of the type of payload to be generated. This payload can be then used by Ethical Hacker to test the remote system.
- *Vulnerability Scanner*-This tool will scan the host completely and return the vulnerabilities in the system with references, cve numbers, their severity .

IV. IMPLEMENTATION AND SETTINGS

A. Hardware and Software Specifications.

We have implemented the cross platform penetration testing suite using ionic framework. Our suite thus works on all mobile os like android, ios, windows etc. Our suite does not require os version to be latest and our application is light in weight. Our application does not require system access/root access..

As for the hardware specifications it requires an android device which run 6.0 and newer versions. For the suite to run smoothly, it is recommended that the phone have 2gb ram and snapdragon 650 or equivalent processor. However, the phone can run on device with less than 2 gb of ram and lower processors.

TABLE 1.HARDWARE AND SOFTWARE SPECIFICATIONS

Device	Hardware and Software Specifications
Android Phone	• Android v.6.0 or above • 2gb ram or above • Snapdragon 650 or above
Target	• Any Web Application • Multiple server system supported

B. System Implementation.

As mentioned above the application has been implemented using ionic framework and python. The application has UI which lets user interacts with the different tools that have been designed and the actual working of the tools have been implemented in python. We have used flask framework to receive and send data using the REST api. The usage of highly efficient tools like xsssniper ,ssl, nessus is possible due to server side implementation. Pdf report generation, sharing reports ,user notification has been implemented.

Following are the algorithms of the tools included in the suite:-

1. Whois.

1)Take url from the user

2)send data in json

3)Using python whois on server side, we pass the url to whois.

4)Get the result, jsonify and send to the mobile.

5)Display the data.

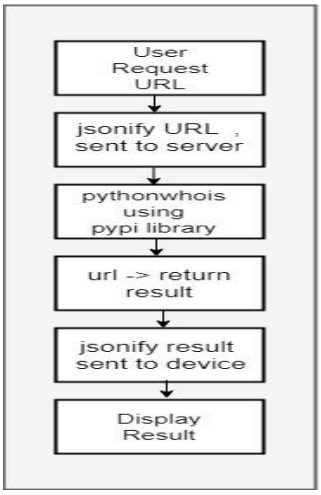


Figure 3.Flow Diagram for whois

2. Nmap

1)Get url as input from user

2)Using socket extract ip address

3)Enter port range 1-1024.

4)Using python-nmap wrapper, determine open ports and send them to the device.

5)Display host ip, state and list of open ports.

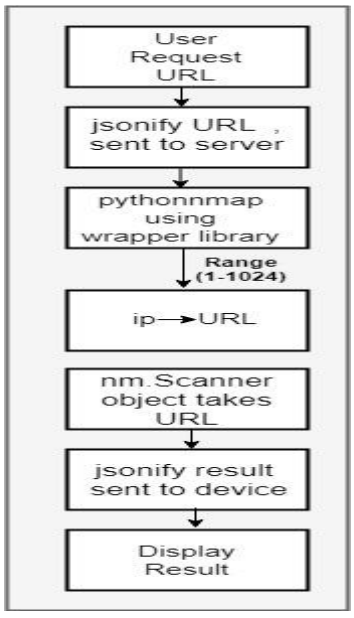


Figure 4.Flow diagram of Nmap

3. Smtp Open Relay Exploitation

1)Take web address or the ip address as the input from the user.

2)Using port scanner in background, check whether port 25 is being used and is it open.

3)If open notify the user that open relay exploitation is possible.

4)Take the sender's email, recipient's email, subject, body of the mail.

5)Create a simple Mail object and pass all the above as parameters to it.

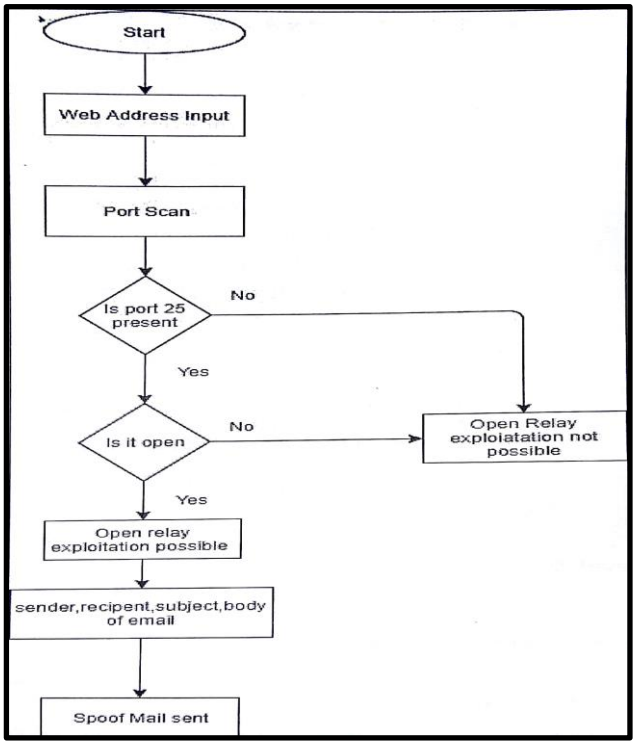


Figure 5. Flowchart of Smtp Open Relay Exploitation

4. Detection of XSS

1)Get url and filename from the user

2)Create a scan engine.

3)In scan engine, import machanize.

- ➔ Create crawler, crawl all web pages
- ➔ Crawl all forms
- ➔ Add pages and forms to target list.
- ➔ Send target list to scanner

4)In scanner import machanize.

- ➔ Check target url with payload.
- ➔ Check tags with payload.
- ➔ Determine stored injection.

5)Collect scanner results.

6)Record them in txt file.

7)Convert txt file into pdf file.

8)Export that pdf file into reports/xss folder.

9)Notify the user

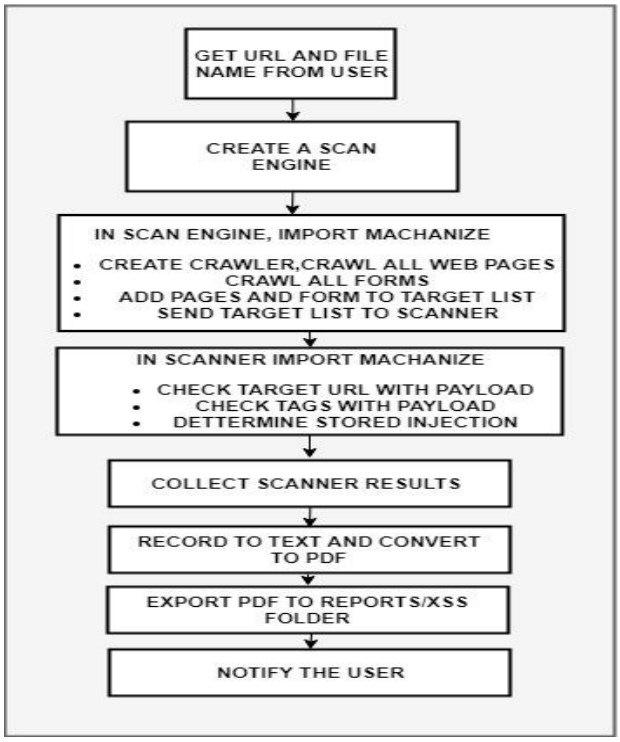


Figure 6.Flow DIagram of Xss Detection

5. Detection of SSL vulnerabilities

1)Collect url and filename from user.

2)Call interface to check ssl vulnerabilities

3)Run testssl shell script

4)Collect results in txt file.

5)Convert the txt file into pdf file.

6)Export the pdf file into reports/ssl folder

7)Notify the user.

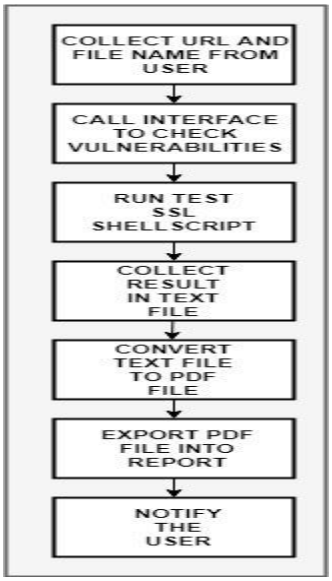


Figure 7.Flow Diagram of SSL Detection

6. Payload Generator.

1)Take the payload type from the user.

2)Display the various options available for the particular type of payload.

3)Set the options for the payload.

4)Load the Metasploit MSFPC program and execute for the payload requirements.

5)Export the payload to the Phone's internal memory.

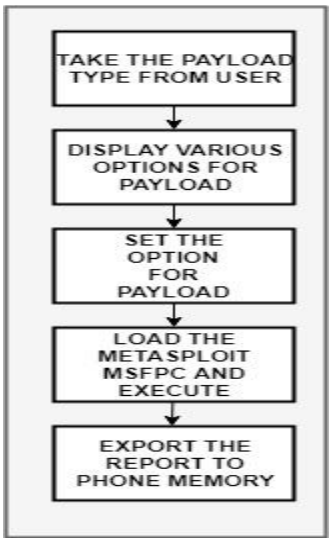


Figure 8.Flow Diagram of Payload Generator

7. Vulnerability Scanner

1)Scan the hosts for its system information and record it.

2)Scan the host for open ports and record it.

3)Search the CVE directory[12] for matching types.

4)For Web application Vulnerabilities, check the table below,

TABLE 2.

Web application Vulnerabilities	
-Remote file inclusion	-Command Injection
-Local file inclusion,	-Blind SQL Injection
-Cross site crossing,	-SQL Injection,
-Cross site scripting,	-LDAP Injection,
-Session management,	-Buffer overflow
-sever side injection	-X-path Injection
-cross site refrence forgery	-HTTP Splitting

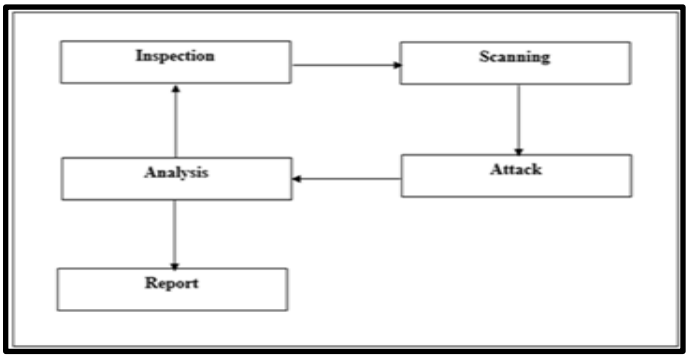


Figure 9.Flow Diagram for Vulnerability Scanner

V. IMPLEMENTATION RESULTS

Figure 10 shows the main menu of the cross platform penetration testing suite which features the all modules.

1. INFORMATION GATHERING

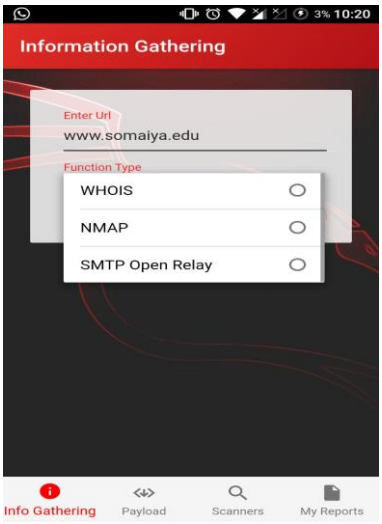


Figure 10.Information Gathering

2. SCANNERS

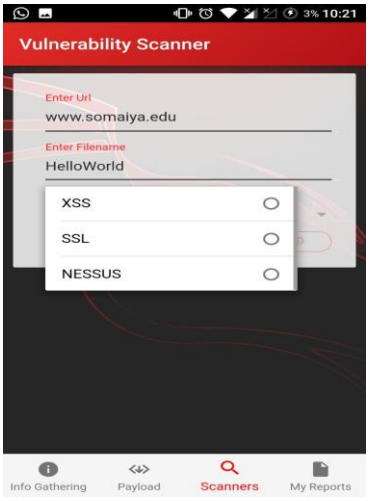


Figure 11.Scanners

3. EXPLOITATION

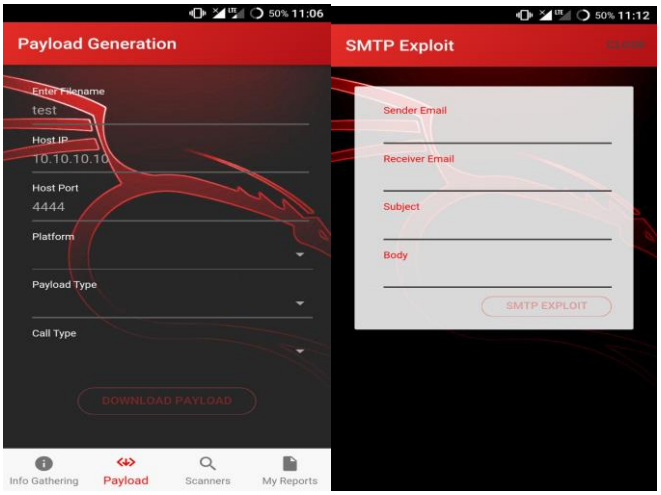


Figure 12.Exploitation

4. REPORTS

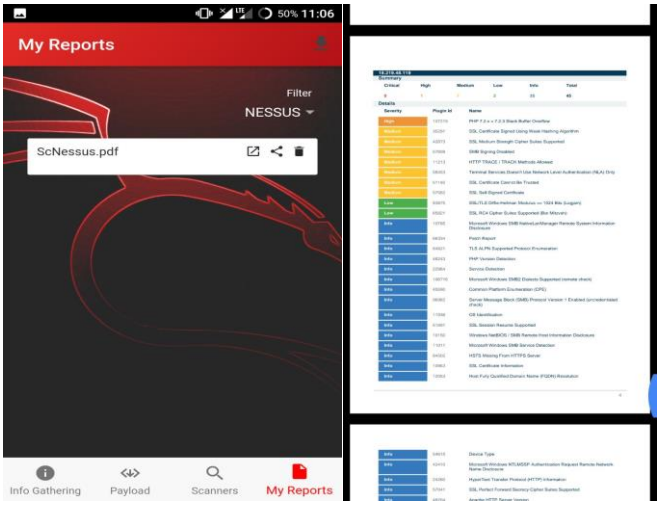
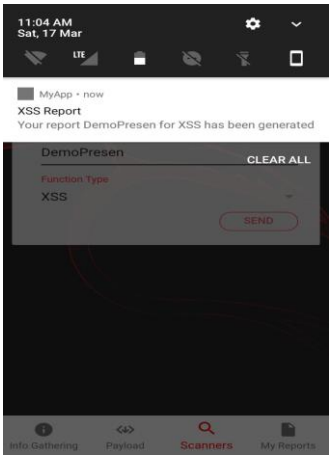


Figure 13.REPORTS

5. NOTIFICATIONS



VI. CONCLUSIONS AND FUTURE WORK

Cross Platform Penetration Testing Suite is built to help Ethical Hackers to determine the possible vulnerabilities and risks in the systems with ease of portability. The system has been developed by combining various technologies like the nmap, Metasploit MSFPC, Nessus, Xss Sniper. We developed the tool with the following recommendations of OWASP top 10 and CVE. There is scope to expand the tool in various other sectors like the Internet of Things (IoT).For future work we would like to add Wireless attack tools and interceptor tool to test web application.

ACKNOWLEDGEMENT

This project is supported and carried out under the guidance of Ms.Shyamal Virnodkar ,Assistant Professor, K J Somaiya Institute of Engineering and Information Technology, Mumbai University.

REFERENCES

[1] Statista, the statistics portal,'Number of internet users worldwide from 2005 to 2017 (in millions)' July 2017 [Online] Available:https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

[2]Wikipedia, 'World population' 31 December 2017 [Online] Available: https://en.wikipedia.org/wiki/World_population

[3] IT proportal, 'The growing demand for Ethical Hackers' 26 November 2015 [Online] Available:https://www.itproportal.com/2015/11/26/the-growing-demand-for-ethical-hackers/

[4]Kali Linux. "Kali Linux Official Documentation" [Online]. Available: http://docs.kali.org/

[5] Common Platform Enumeration [Online]. Available: https://cpe.mitre.org/

[6] Metasploit Basics [Online] Available: https://metasploit.help.rapid7.com/docs/metasploit-basics

[7]Tenable.io, 'Nessus' [Online] Available: https://www.tenable.com/products/nessus/nessus-professional

[8]Kali Net Hunter [Online]. Available: https://www.kali.org/kali-linux-nethunter/

[9] OWASP, 'Top 10 2013-A1-Injection' 19 March 2017 [Online] Available: https://www.owasp.org/index.php/Top_10_2013-A1-Injection
Available: http://ieeexplore.ieee.org/document/7725026/

[10]Common Vulnerabilities Exposure[Online] Available: https://cve.mitre.org/

[11] SciEpub,'A Hybrid Algorithm for Detecting Web Based Applications Vulnerabilities' 2016 [Online] Available: http://pubs.sciepub.com/ajcrr/4/1/3/

[12] XSSSniper is an handy xss discovery tool. Available: https://github.com/gbrindisi/xsssniper