Documents

Export Date: 26 Aug 2020

Search: TITLE-ABS-KEY(Experimental Assessment of Freeware Penetratio...

1) Azaharimohdyusof, M., Samadshibghatullah, A.
Experimental assessment of freeware penetration testing tools against network environment
(2019) International Journal of Advanced Science and Technology, 28 (1), pp. 339-350.

1) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85080143352&partnerID=40&md5=0522958bba3b7f30b3e65b142f2f502
Document Type: Article
Publication Stage: Final
Source: Scopus

Search: TITLE-ABS-KEY(Experimental Assessment of Freeware Penetration Testing Tools against Network Environment)

International Journal of Advanced Science and Technology
Vol. 28, No. 1, (2019), pp. 339-350

Experimental Assessment of Freeware Penetration Testing Tools against Network Environment

[1]Mohd AzahariMohdYusof, [2]Abdul SamadShibghatullah
[1]*Faculty of Computing & Technological Science, Kolej University Poly-Tech MARA Kuala Lumpur, Malaysia*
[2]*Faculty of Information and Communication Technology UniversitiTeknikal Malaysia Melaka, Malaysia*

Abstract

Nowadays, penetration testing tools are very essential assessment tools that can be used by network administrator in an organization to find out any vulnerabilities and security threats in a network system or web application. The penetration testing tools can be obtained in the market by making a selection in terms of performance, reliability, compatibility and stability. This paper is prepared to make the selection and evaluation against the best three penetration testing tools have been selected in terms of performance. There are eight measurement parameters are used to evaluate its performance includes how many vulnerabilities can be detected, speed of scanning activities, report of vulnerabilities, signature method, user facilities, up-to-date database, integrated technology and intelligent tool. The evaluation has been conducted and the results show Acunetix is the best tool compared to the other two tools that have been evaluated.

Keywords*: Penetration testing tools, vulnerabilities, threat and performance.*

1. INTRODUCTION

Nowadays, most organizations use penetration testing tool to check and evaluate the security level of the network or web application (Lovepreet et al., (2015). It can also serve as vulnerability testing because it can assess the security model of the network as a whole. Apart from that, it will help organizations to understand for better defense against its network infrastructure.

Penetration testing tool has several strengths, such as to know the security vulnerabilities in network systems, help network users to avoid many network downtime, maintain the reliability of the user and take care of security insurance requirements (Ramesh & Gupta, 2015). The strength of the penetration testing tool has proved that it is a powerful tool.

We know that the threat assessment is a critical step in the organization's information security lifecycle. The step must be organized using a penetration testing tool to evaluate organization’s information security and to observe how the organization defends against an attack to ensure the network always operates in a good condition. Moreover, penetration testing tools offer many benefits in the network security development. As a network administrator, they have faced some challenges to manage and maintain the security level of an organization’s network environment especially the network performance and internet access from suspicious activity. That’s why a penetration testing tools is needed by an organization to establish a baseline assessment of security. It involves gathering information of the organization such as security infrastructure and then using this information to identify known or potential security vulnerabilities.

Thus, solutions to problems is to select and evaluate the best three penetration testing

ISSN: 2005-4238 IJAST

tools that have been selected in terms of performance. The three penetration testing tool will be installed and implemented on a host or network to identify whether it is able to deal with various threats to network systems and web applications.

2. AN OVERVIEW OF PENETRATION TESTING TOOLS

According to Bacudio et al. (2011), penetration testing tool is a method used to check the network environment of an organization, which is composed of hardware, software and user. Typically, network administrators use penetration testing tool to help them find security vulnerabilities before any hackers try to exploit their organization's network environment. Moreover, there are several advantages that have been identified with the use penetration testing tool (Secforce Ltd., 2015). It includes manage risk properly, increase business continuity, minimize client-side attacks, protect clients, partners and third parties, comply with regulation or security certification, evaluate security investment and protect public relationships and brand issues.

Penetration testing tool can reveal vulnerabilities in the target system and the risk of vulnerabilities, whether it's high/medium/low risk level. The reported risk classification will make it easier for network administrators to take appropriate action with the purpose of improvement in the target system. Not only that, penetration testing tool can minimize the exploitation activities so that the organization can protect clients, partners and third parties.

There are three types of penetration testing tool based on Course Technology Cengage Learning (2011) and they are black-box testing, white-box testing and gray-box testing. Black-box testing is also called zero-knowledge testing because the tester does not require information that there is vulnerability on the target system. White-box testing is known as a complete-knowledge testing because the tester should check the security situation that exists on the target system, such as the types of attacks that can occur on the target system and detailed information about the organization's network environment. Tester also need the network topology information and asset inventory for full security audit. Gray-box penetration testing is an approach that is often used by the tester to test the vulnerability so that they can exploit the vulnerabilities found. Tester uses this type of penetration testing tool because the tester has a limited knowledge of the internal information towards the network or web application.

Usually, there are four important steps to be followed to perform penetration testing tool. The first step, we need to list the vulnerabilities or potential problems that would cause a breach of security to the system. The second step, list the vulnerabilities based on priority, which is based on the critical case. The third step, test penetration testing tool that will be used to determine whether it can access network, server or website application that is not allowed to be hacked. The fourth step, if the unauthorized access is possible, the system has to be corrected and all the steps that have been declared to be run until the vulnerability is fixed.

3. PENETRATION TESTING TOOLS

There are many penetration testing tools available in the market today to secure the network or web applications. Penetration testing tool can be categorized into two functions and they are scanners and attackers. The following are the best ten penetration testing tool based on Software Testing Help (2015).

Metasploit: Metasploit is the most popular penetration testing tool that can be used by the tester (Santokhi, 2013). It is based on the exploit concept that uses a specific code to check some important information for the target system. Typically, it is used on a server, network or web application and it consists of the command-line and GUI. It can work for multiple operating systems, such as Linux, Apple and Microsoft.

Wireshark: Wireshark is a network protocol analyzer and has a number of advantages to get information, such as network protocols, packet information, decryption and many more (Lamping et al., 2014). There are some kind of operating system that can be used to implement Wireshark, such as Windows, Linux, OS X, Solaris, FreeBSD and NetBSD. It's easy to be owned by anyone because it is provided in
the form of a free version.

W3af: W3af is stand for Web Application Attack and Audit Framework, where it is a command-line interface (Riancho, 2016). It is easily available for free download and can be implemented in Linux, Apple and Microsoft. There are some features on W3af, such as fast HTTP requests, integration of web and proxy servers into the code and injecting payloads into various kinds of HTTP requests.

Core Impact: Core Impact is used by the tester to check the mobile device, network, password identification and cracking (Core Security Corporation, 2016). It consists of two forms of interface and they are a command-line and GUI. It can be implemented on a Microsoft operating system. Core Impact has several advantages, such as multi-vector testing capabilities across network/web/mobile and test more common vulnerability exploits. It can also be used to evaluate the security posture using the same techniques employed by today's cyber-criminals.

BackTrack: BackTrack is the best penetration testing tool, which it can only be implemented on a Linux operating system (Selvan, 2012). BacTrack is used to discover vulnerabilities of a website, such as SQL injection and file inclusion. The major tools of BackTrack includes information gathering, vulnerability assessment, exploitation tools, privilege escalation, maintaining access, reverse engineering, RFID tools, stress testing, forensics, reporting tools, services and miscellaneous.

Netsparker: Netsparker is a commercial product known as a web application scanner. It can identify vulnerabilities and very popular used to exploit SQL injection and local file induction (Urban, 2015). There are two types of interfaces provided by the vendor, command-line and GUI and can only be implemented on a Microsoft operating system.

Nessus: The main purpose of using Nessus tool is to detect potential vulnerabilities on the tested systems. This tool is installed and implemented on Windows platform. According to Tenable Network Security Inc. (2012), the Nessus tool can be implemented by using Professional Feed or Home Feed plug-ins. By default, Nessus running on port 8834 and can be accessed using any web browser. Basically, there are four navigation tabs at the top of Nessus interface and they are Results, Scans, Policies and Users, where it has own function.

John The Ripper: A free and fast password cracker that is used to detect weak Unix password (Software Testing Help, 2015).

Acunetix: Acunetix is a web vulnerability scanner that is used to identify web servers by using a specific IP address or range of IP address (Acunetix Ltd., 2016). It can explore and display any information of the entire website structure during its working. The common security issues can be audited using Acunetix because it can detects file inclusion automatically. It contains a port scanner and network alerts that is used to scan a port of the web servers.

Nmap: Nmap or Network Mapper, which it is free open source tool that is available under the General Public License (GNU) as published by the Free Software Foundation (Software Testing Help, 2015). Most of the tester using Nmap to help them find the

characteristics of the target system. The characteristics required by the tester, such as hosts, services, operating systems, packet filters or firewalls.

4. RESEARCH METHODOLOGY

There are four phases in conducting this research as outlined in Figure 1.

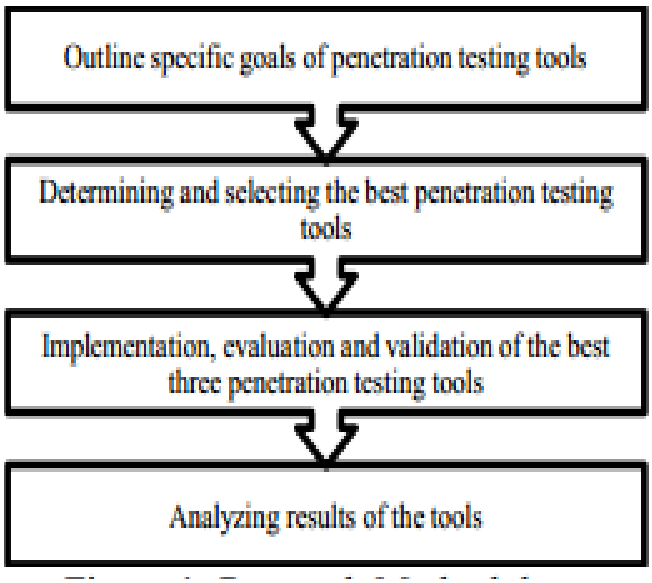

Figure 1: Research Methodology

Outline specific goals of penetration testing tools: The first phase is outline specific goals of penetration testing tools. A specific goal is something that we want to achieve. It is used to know what we want and then we can go for it in a constructive and productive way. It is very essential step and it need to specify before a research to be conducted. The specific goals of using penetration testing tools in this research are to find out and detect vulnerabilities of a network or web application, where the penetration testing tool is an open source tool.

Determining and selecting the best penetration testing tools: The second phase is determining and selecting the best penetration testing tools. This phase is very important because there are many penetration testing tools are available in the market today. This phase is performed by listing the best ten penetration testing tool based on Software Testing Help (2015). Next, three out of ten penetration testing tools will be selected, which they have vulnerability detection and open source tool as stated in the first phase. Based on the analysis shown in Table 1, it shows BackTrack, Nessus and Acunetix are considered as the best three penetration testing tools for the evaluation.

Table 1: The Best Ten Penetration Testing Tools

Tool	Description		
	Vulnerability Detection?	Open Source?	Commercial Product?
Metasploit	√	X	√
Wireshark	X	√	X
W3af	X	√	X
Core Impact	X	X	√
BackTrack	√	√	X
Netsparker	√	X	
Nessues	√	√	X
John The Ripper	X	√	X

Acunetix	√	√	X
Nmap	X	√	X

Implementation, evaluation and validation of the best three penetration testing tools: The third phase is implementation, evaluation and validation of the best three penetration testing tools have been selected and they are BackTrack, Nessus and Acunetix as shown in Figure 2. The main purpose of the implementation is to test and validate the BackTrack, Nessus and Acunetix in order to gain the right results based on eight measurement parameters as follows:

1.How many vulnerabilities can be detected
2. Speed of scanning activities
3. Report of vulnerabilities
4. Signature method
5. User facilities
6. Up-to-date database
7. Integrated technology
8. Intelligent tool

BackTrackNessusAcunetixRouterNetwork System / Web Application1. Install BackTrack, Nessus and Acunetix.2. Implement BackTrack, Nessus and Acunetix.3. Determine the potential vulnerabilities.4. Evaluate and validate BackTrack, Nessus and Acunetix.

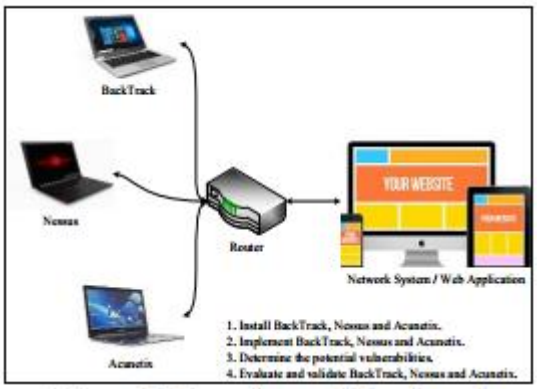

Figure 2: Experimental Design of Evaluation and Validation

Analyzing results of the tools: The fourth phase is analyzing results of the tools. Results are the main objective of this research to be formed in a statement that explains or interprets the data. The result will be exposed after the implementation and evaluation task of BackTrack, Nessus and Acunetix.

5. RESULTS AND DISCUSSION

This section discusses the evaluation results of BackTrack, Nessus and Acunetix in terms of performance. The result is based on the outcome of implementation of BackTrack, Nessus and Acunetix as described below:

How Many Vulnerabilities Can Be Detected: The total number of vulnerabilities can be detected by BackTrack, Nessus and Acunetix are measured based on two categories of measurement and they are total of detection and level of vulnerabilities as shown in Figure 3 with measurement scale as follows:

1 – 2 : no powerful
3 – 4 : less powerful
5 – 6 : powerful

7 – 8 : more powerful
9 – 10 : completely powerful

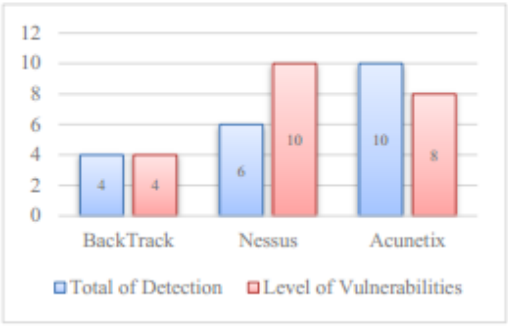

Figure 3: Results of Vulnerabilities Detection

BackTrack has detected 7 vulnerabilities on the target website with two types of vulnerabilities and they are cross-site scripting (XSS) and cross-site request forgery (CSRF). Nessus has detected 53 vulnerabilities on the target scan and has a level of vulnerabilities as shown in Figure 4.

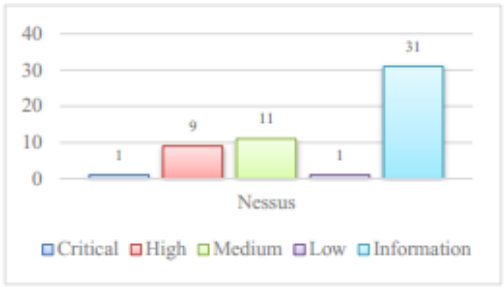

Figure 4: Level of Vulnerabilities on Nessus

Acunetix has detected 89 vulnerabilities on the target website and has a level of vulnerabilities as shown in Figure 5.

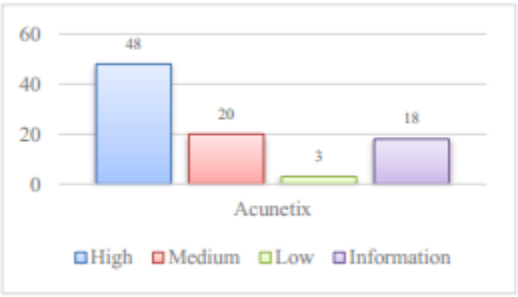

Figure 5: Level of Vulnerabilities on Acunetix

Speed of Scanning Activities : The speed of scanning activities of BackTrack, Nessus and Acunetix are measured based on two categories of measurement and they are time taken and detection travel as shown in Figure 6 with measurement scale as follows:

1 – 2 : very slow
3 – 4 : slow
5 – 6 : fast
7 – 8 : faster
9 – 10 : completely faster

Figure 6: Results of Scanning Activities

BackTrack takes 11 minutes 42 seconds to scan 7 vulnerabilities found on the target website. Nessus takes 20 minutes 14 seconds to discover 53 vulnerabilities found on the target scan. Acunetix has detected 89 vulnerabilities within 16 minutes 13 seconds on the target website.

Report of vulnerabilities: The report of vulnerabilities have been produced by BackTrack, Nessus and Acunetix are measured based on four categories of measurement and they are accuracy, concisely, clearly and well structured as shown in Figure 7 with measurement scale as follows:
1 – 2 : not satisfied
3 – 4 : barely satisfied
5 – 6 : satisfied
7 – 8 : mostly satisfied
9 – 10 : completely satisfied

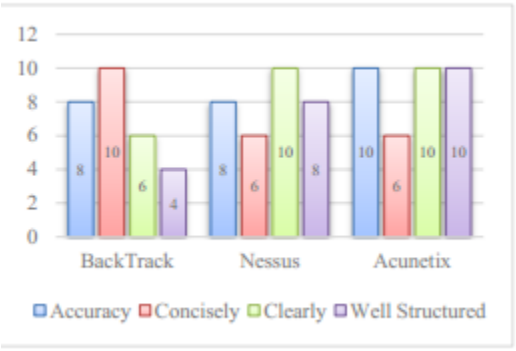

Figure 7: Results of Vulnerabilities Report

Signature Method: The signature method has produced on BackTrack, Nessus and Acunetix are measured based on two categories of measurement and they are signature type and signature capability as shown in Figure 8 with measurement scale as follows:
1 – 2 : not sophisticated
3 – 4 : barely sophisticated
5 – 6 : sophisticated
7 – 8 : more sophisticated
9 – 10 : completely sophisticated

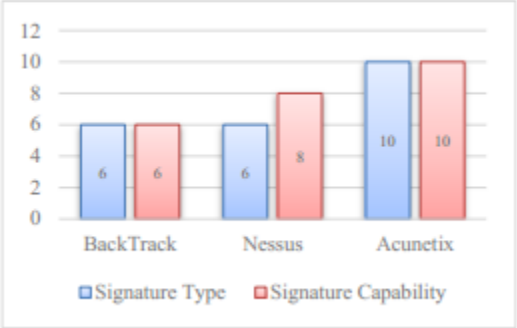

Figure 8: Results of Signature Method

User Facilities: The user facilities have provided on BackTrack, Nessus and Acunetix are measured based on seven categories of measurement and they are simple installation and well documented, easy to update, well-designed GUI, efficient, the tool should be easy to remove, easy to troubleshoot a problem and easy to make interconnectivity between applications or hardware as shown in Table 2 with measurement scale as follows:

1 – 2 : not easy and efficient
3 – 4 : barely easy and efficient
5 – 6 : easy and efficient
7 – 8 : more easy and efficient
9 – 10 : completely easy and efficient

Table 2: Results of User Facilities

Tool	Measurement Parameters	Measurement Scale
BackTrack	Simple installation and well documented	10
	Easy to update	6
	Well-designed GUI	6
	Efficient	6
	The tool should be easy to remove	10
	Easy to trouble shoot a problem	2
	Easy to make interconnectivity between application or hardware	10
Nessus	Simple installation and well documented	6
	Easy to update	8
	Well-designed GUI	10
	Efficient	8
	The tool should be easy to remove	10
	Easy to trouble shoot a problem	2
	Easy to make interconnectivity between application or hardware	10
Acuneti	Simple installation and	10

x	well documented	
	Easy to update	8
	Well-designed GUI	10
	Efficient	10
	The tool should be easy to remove	10
	Easy to trouble shoot a problem	2
	Easy to make interconnectivity between application or hardware	10

Up-to-date Database: Up-to-date database has provided on BackTrack, Nessus and Acunetix are measured based on two categories of measurement and they are updated database and database capability as shown in Figure 9 with measurement scale as follows:

1 – 2 : not updated
3 – 4 : less updated
5 – 6 : updated
7 – 8 : often updated
9 – 10 : completely updated

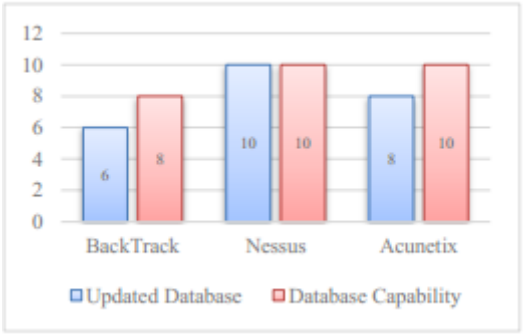

Figure 9: Results of Up-to-Date Database

Integrated technology: The technology has produced on BackTrack, Nessus and Acunetix are measured based on three categories of measurement and they are detection scope, detection capability and key functionality as shown in Figure 10 with measurement scale as follows:

1 – 2 : not good
3 – 4 : barely good
5 – 6 : good
7 – 8 : mostly good
9 – 10 : completely good

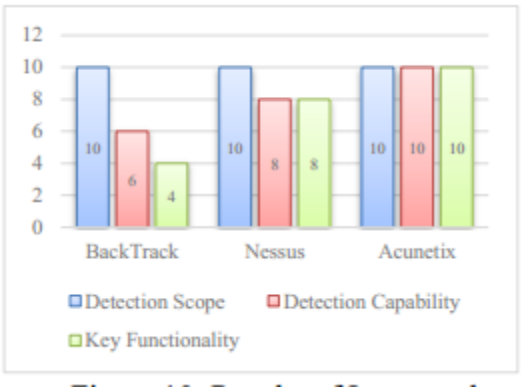

Figure 10: Results of Integrated Technology

Intelligent Tool :BackTrack, Nessus and Acunetix can be an intelligent agent to performs the scanning activity when it running on a host or network. It is measured based on three categories of measurement and they are scanning method, detection method and report generation as shown in Figure 11 with measurement scale as follows:

1 – 2 : not intelligent
3 – 4 : barely intelligent
5 – 6 : intelligent
7 – 8 : mostly intelligent
9 – 10 : completely intelligent

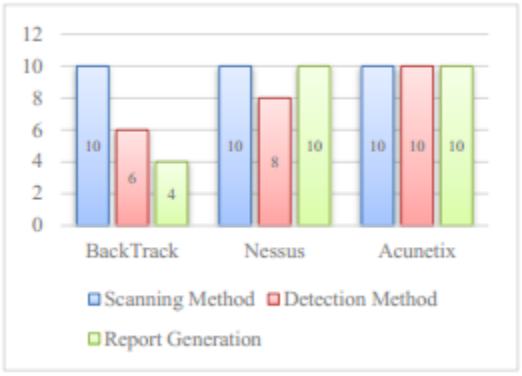

Figure 11: Results of Intelligent Tool

The results as analyzed as shown in Table 3, it proved the best penetration testing tool is Acunetix. It can be used to secure a network or web application against possible vulnerabilities before intruders perform their attacks. Moreover, the Acunetix has a useful technology namely AcuSensor technology and can be an intelligent agent to identify more vulnerabilities compared to Nessus and BackTrack.

Table 3: Comparison of Obtained Results

Tool	Measurement Parameters	Results	Overall Results
BackTrack	How many vulnerabilities can be detected	40%	60.8 %
	Speed of scanning activities	50%	

	Report of vulnerabilities	70%	
	Signature method	60%	
	User facilities	63%	
	Up-to-date database	70%	
	Integrated technology	66.6 %	
	Intelligent tool	66.6 %	
Nessus	How many vulnerabilities can be detected	80%	
	Speed of scanning activities	80%	
	Report of vulnerabilities	80%	
	Signature method	70%	84.2 %
	User facilities	77.2 %	
	Up-to-date database	100 %	
	Integrated technology	93.3 %	
	Intelligent tool	93.3 %	
Acunetix	How many vulnerabilities can be detected	90%	
	Speed of scanning activities	100 %	
	Report of vulnerabilities	90%	
	Signature method	100 %	94.5 %
	User facilities	85.8 %	
	Up-to-date database	90%	
	Integrated technology	99.9 %	
	Intelligent tool	99.9%	

6. CONCLUSION AND FUTURE WORK

Vulnerability assessment is a critical task to identify weaknesses in a network or web application. Any potential vulnerability found in the network or web application to allow any hackers to perform their attack. Penetration testing tools can be used to secure the network or web application by detecting any potential vulnerability before the attacks are performed by hackers. The research was completed by implementing the best three penetration testing tools namely BackTrack, Nessus and Acunetix. There are two suggestions regarding to future work of the research. The first suggestion is expanding the evaluation scope of penetration testing tools in terms of reliability, compatibility and stability. The second suggestion is expanding the specific goals of penetration testing tools, which is assess vulnerabilities using the real-world exploits like hacking schemes.

ACKNOWLEDGEMENT

First of all, we would like to thank to Allah Almighty, who made us capable to complete this research. Last but not least, we would like to sincerely express our gratitude to our colleagues, such as providing useful information and knowledge related to our research.

REFERENCES

[1] Acunetix Ltd.2016, January 5. *Audit your website security with Acunetix Web Vulnerability Scanner.* Retrieved June 29, 2016, from http://www.acunetix.com/

[2] Bacudio, A. G., Yuan, X., Chu, B.-T. B., & Jones, M. (2011). An Overview of Penetration Testing. *International Journal of Network Security & Its Applications (IJNSA), 3*(6), 19-38.

[3] Core Security Corporation. 2016. *Core Impact.* USA: Core Security Corporation.

[4] Course Technology Cengage Learning. 2011. *Penetration Testing: Procedures and Methodologies.*USA: EC-Council.

[5] Lamping, U., Sharpe, R., &Warnicke, E. 2014. *Wireshark User's Guide.* Australia: General Public License.

[6] Lovepreet, Kaur, P., Singh, E. G., &Khurana, S. 2015. A Descriptive Study of various Penetration Testing Tools and Techniques. *International Journal of Computer and Communication System Engineering (IJCCSE), 2*(3), 420-424.

[7] Ramesh, & Gupta, G. 2015. Securing Networks Using Network Penetration Testing. *International Journal for Multi Disciplinary Engineering and Business Management (IJMDEBM), 3*(1), 1-3.

[8] Riancho, A. 2016. *w3af - Web Application Attack and Audit Framework Documentation.* Argentina: Offensive Security.

[9] Santokhi, M. 2013, August 28. *Metasploit - Exploit Learning Tree.* Retrieved June 29, 2016, from https://www.exploit-db.com

[10] Secforce Ltd. 2015, June 1. *Penetration Testing - Be one step ahead in Security* . Retrieved June 27, 2016, from www.secforce.com

[11] Selvan, S. 2012, July 26. *Wireshark Released Version 1.8.1 and 1.6.9 to Close Critical Vulnerability.* Retrieved June 29, 2016, from http://www.ehackingnews.com

[12] Software Testing Help. 2015, January 5. *Software Testing Help*. (Powerful Penetration Testing Tools For Every Penetration Tester) Retrieved June 28, 2016, from http://www.softwaretestinghelp.com/

[13] Tenable Network Security Inc. 2012. *Nessus 5.0 - Installation and Configuration Guide.* Columbia: Tenable Network Security Inc.

[14] Urban, B. 2015, January 20. *Netsparker*. Retrieved June 29, 2016, from https://www.netsparker.com/