



CyberSaint
SECURITY



Network Security Assessment Using Internal Network Penetration Testing Methodology

Author: Sunny thakur

Date-10/14/2024

Abstract— The rapid advancement of information technology presents a critical challenge for computer network security and the sensitive information they protect. However, awareness of the importance of securing these networks remains alarmingly low. According to a survey by Symantec, only 13% of the 3,300 companies surveyed globally prioritized security system upgrades within the next year. This lack of attention to security measures creates exploitable gaps that malicious actors can leverage to compromise system stability. With the growing frequency and sophistication of cyber-attacks each year, there is an undeniable need for continuous enhancement of security measures. To address this, periodic assessments through **penetration testing** are essential in identifying vulnerabilities within networks and systems, thereby reinforcing security protocols and reducing the risk of data breaches or loss. This research applies **internal network penetration testing** across five attack vectors, revealing security risks ranging from 20% to 80% in the systems analyzed. The findings underscore that each system harbors vulnerabilities that could be exploited if not properly secured.

Keywords— Penetration testing, network security, vulnerability.

I. INTRODUCTION

The evolution of information technology plays a pivotal role in modern society. As technology continues to rapidly transform, ensuring the security of information has become a critical concern (Mason, 1986). Due to the high value of information, access is often restricted to individuals with specific authority. When sensitive information falls into unauthorized hands, it can lead to significant damage to the rightful owner. For example, within organizations, confidential data such as product designs,

proprietary algorithms, and internal processes are typically reserved for authorized personnel. This underscores the necessity for robust information security systems that align with established standards.

The growing complexity of information technology presents new challenges for the security of both computer networks and information systems. According to a survey by Symantec, only 13% of the 3,300 companies worldwide surveyed prioritized upgrading their security systems within the year (Symantec State of Security Survey, 2011). This lack of awareness leaves organizations vulnerable, with

security gaps that attackers can exploit to compromise system integrity.

. Cyber-attacks have led to numerous instances of data theft, affecting both public and private sectors. For example, nearly 21.5 million individuals had their personal data stolen from government offices. Additionally, a series of attacks on global financial institutions since late 2013 resulted in the theft of approximately \$1 trillion USD. More than 100 banks across 30 countries were targeted by attackers who installed spyware on bank employees' computers, secretly monitoring their activities and facilitating unauthorized money transfers. According to breachlevelindex.com, over 3 billion data records were lost or stolen between 2013 and June 2015, affecting a wide range of sectors, including retail, government, education, and finance.

II. LITERATURE REVIEW

A. Network Security

Network security is essential to monitor and control network access, preventing unauthorized users from exploiting network resources. The responsibility for maintaining network security lies with the network administrator. There are five key principles in network security:

- **Confidentiality:** Information must only be accessible to those with the appropriate authorization.
- **Integrity:** Only authorized individuals are allowed to modify information, ensuring its accuracy and consistency.
- **Availability:** Information must be accessible to authorized users whenever required.
- **Authentication:** The identity of the sender must be verified to ensure that the source of the information is legitimate and not falsified.
- **Nonrepudiation:** Both the sender and the recipient of information cannot deny having sent or received the message, ensuring accountability.

B. Penetration Testing

Penetration testing is a technique employed to assess the security posture of a system or network by simulating an attack. According to the **OWASP methodology**, web application security testing

specifically targets the security aspects of web applications, where the process actively analyzes the application to identify vulnerabilities, technical flaws, and weaknesses. Once security issues are discovered, the findings are reported to the system owner, along with a detailed assessment of potential impacts and technical recommendations for remediation.

Penetration testing is a proven method for addressing security vulnerabilities in various environments, including applications, networks, and operating systems. The primary goal is to identify vulnerabilities and attempt to exploit them, focusing on weaknesses that have been identified or left unaddressed in prior security evaluations.

There are **three main types** of penetration testing:

1. **Black-Box Testing:** Conducted without prior knowledge of the systems or networks used by the organization. The tester approaches the target as an external attacker with no insider information.
2. **White-Box Testing:** Performed with full knowledge of the organization's infrastructure, allowing for a more comprehensive evaluation of the internal system components.
3. **Grey-Box Testing:** A hybrid approach that combines elements of both black-box and white-box testing, offering a balanced assessment based on partial knowledge of the system.



Fig. 1. Types of Penetration Testing

III. METHODOLOGY

This research adopts the **internal network penetration testing** method to assess security

vulnerabilities. The steps followed in this research are illustrated in the diagram below:

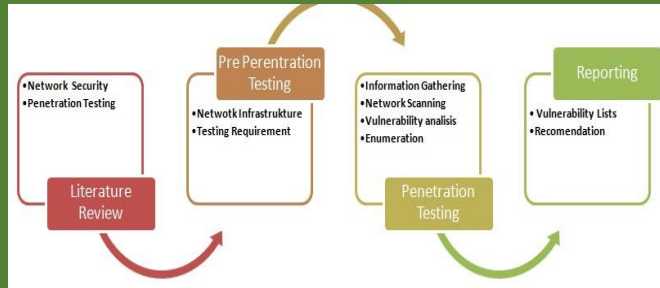


Fig. 2 Methodology

- **Literature Review:** This step involves a thorough review of relevant literature, including books, articles, and research papers, to gain a deep understanding of network security and penetration testing techniques.
- **Pre-Penetration Testing:** Before starting the test, an analysis of the network security is conducted to identify the key components that need to be evaluated during the assessment.
- **Penetration Testing:** In this phase, the actual penetration tests are carried out, targeting the identified security vulnerabilities. Various exploitation techniques are used to assess the system's defenses and identify gaps in security.
- **Reporting:** After completing the penetration test, a comprehensive report is prepared. This report details the vulnerabilities found, the risks associated with them, and provides actionable recommendations to improve the system's security posture.

IV. PENETRATION TESTING

A. SCOPE OF PROJECT

Scope of testing on servers on the internal network there are 5 servers in one network. IP network of internal network is X.X.X.0/24. The following is the list of IP servers that will be tested.

TABLE I
LIST OF IP SERVER

IP ADDRESS	
S1	X.X.X.68
S2	X.X.X.77
S3	X.X.X.103
S4	X.X.X.123
S5	X.X.X.152

The above IP address is taken based on scanning the host through the internal network using the white box method. Each of these IP represents each existing server. only 5 machines are taken as examples of testing.

Some of the things tested in the server penetration testing on the internal network are as follows.

TABLE III
VULNERABLE INFORMATION

ID Vulnerable	Information
V1	Vulnerable web application
V2	Vulnerable of Plugin
V3	Default Username and Password
V4	DOS
V5	Cross Site Scripting

The ID is used to provide an identity for the security holes that are found later in the system. Its important applied to evaluate system or server based on internal network.

b. Information Gathering

This information is obtained using Zenmap tools with banner grabbing methods to get all information about the machines.

TABLE IIIII
INFORMATION S1 MACHINE

IP Address	X.X.X.68
Operating System	Linux 3.10
Device Type	Web Server
Hostname	XXX
Active Port	Services
21	FTP (ProFTPD or KftPD)
22, 2222	SSH (OpenSSH 7.4 (protocol 2.0))
25, 587	SMTP (Postfix smtpd)
80, 10000	HTTP (Apache httpd 2.4.6 (PHP 5.4.16))
110, 995	Pop3 (Dovecot pop3d)
143, 993	IMAP (Dovecot imapd)
443	HTTPS (Apache/2.4.6)
53	Domain (ISC BIND 9.9.4)

TABLE IVV
INFORMATION S2 MACHINE

IP Address	X.X.X.77
------------	----------

Operating System	Linux 3.10
Hostname	Sistem Informasi Presensi
Device Type	Server
Active Port	Services
222	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2
53	ISC BIND 9.9.5-3 (Ubuntu Linux)
80	Apache httpd 2.4.7 ((Ubuntu))
3306	MySQL 5.5.38-0ubuntu0.14.04.1

TABLE V
INFORMATION S3 MACHINE

IP Address	X.X.X.103
Operating System	3com Embedded
Device Type	Switch
Hostname	Baseline Switch
Active Port	Services
80	GoAhead WebServer (LinkSys SLM2024 or SRW2008 - SRW2016 switch http config)
443	ssl/http GoAhead WebServer (Linksys SRW2024 switch http config)

TABLE VI
INFORMATION S4 MACHINE

IP Address	X.X.X.123
Operating System	Hp Laser Jet
Device Type	Printer
Hostname	HP LaserJet M3027 MFP Series
Active Port	Services
21	HP FTP Print Server 3.0
23	HP Jetdirect Telnet
80,280, 631	HP-ChaiSOE 1.0

TABLE VII INFORMATION S5
MACHINE

IP Address	X.X.X.152
Operating System	Windows Xp (x32)
Device Type	Host
Hostname	Splash.php
Active Port	Services
80	Apache httpd 2.4.3 ((Win32) OpenSSL/1.0.1c PHP/5.4.7)
443	Apache httpd 2.4.3 ((Win32) OpenSSL/1.0.1c PHP/5.4.7)
49152	Portable SDK for UPnP devices 1.4.7 (Windows 6.2.9200 2; UPnP 1.0)

c. Penetration Testing 1. Penetration Testing on S1 Machine

After getting information about the target, proceed with the vulnerability analysis method, which analyzes the the weaknesses of the system that can be exploited during the attack session. based on the information above, web applications use WordPress with version 4.24. then the examiner will enter the WordPress Login Page for enumeration to get information about the username and password.

```

root@DESKTOP-MA4840T: ~
File Edit View Search Terminal Help

[+] Enumerating usernames ...
[+] Identified the following 1 user/s:
+-----+
| Id | Login | Name |
+-----+
| 1 | admin | admin - TEKNOLOGI |
+-----+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Fri Sep 14 22:47:36 2018
[+] Requests Done: 391
[+] Memory used: 65.52 MB
[+] Elapsed time: 00:00:54
root@DESKTOP-MA4840T: ~#

```

Fig. 3 Enumeration Username Using Wpscan

In this case, the username is obtained, but the password cannot be indicated because the combination of characters in the password is difficult to hack. The test continued by finding the weaknesses of the web server using the Owasp Zap tool.

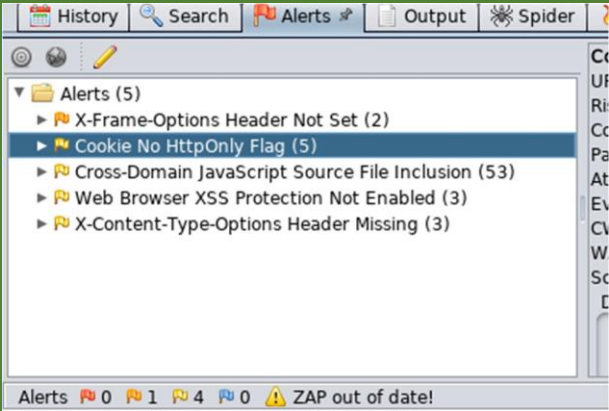


Fig. 4 Finding Vulnerable Using OWASP Zap Tools

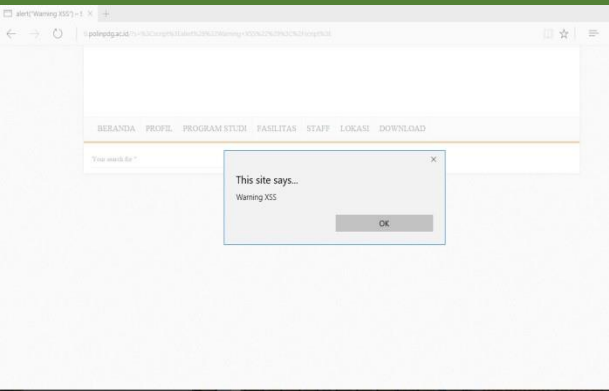


Fig. 5 XSS Attack on TI Web Server later using the Cross Site Scripting attack type.

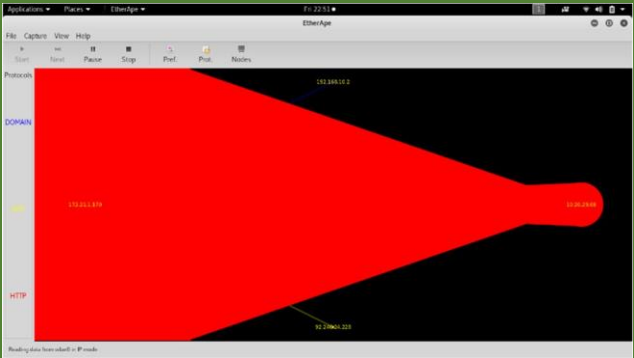


Fig. 7 Network Traffic Monitoring Using Etherape Tools

After perform DOS attack, the database connection on the web cannot be accessed for a while. weakness in the web scripting section that can be exploited

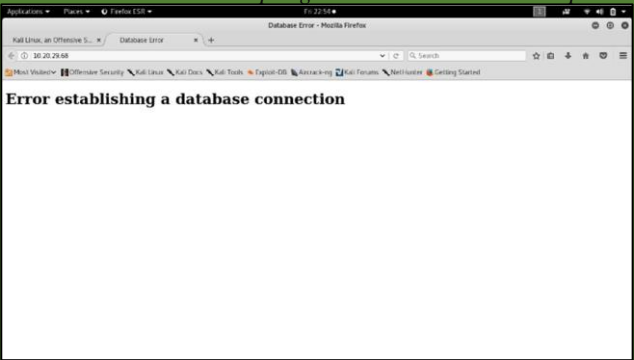


Fig. 8 Error Database Connection

TABLE VIII
RECOMMENDATION S1 MACHINE

The next test is DOS attack. Based on information that the machine use XMLRPC Protocol in the application, the testers can attack through the protocol to overload and flood the server by sending a lot of requests in a small time. The attack was carried out using metasploit tools with wordpress xmlrpc dos module and make lot request to server.

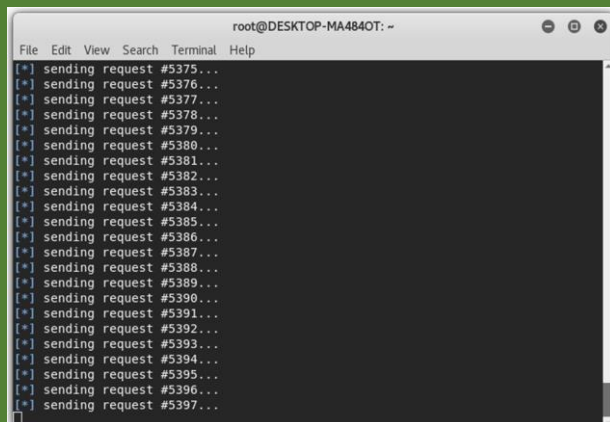


Fig. 6 DOS Attacking using Metasploit Tools

After the attack was carried out a lot of network traffic was drawn on the following etherape tools.

	ErrorDocument 403 http://127.0.0.1/ </ Files> Allow IP 192.168.1.10/24 to approve the IP administrator which is exemplified in the IP above to configure
V6	<ul style="list-style-type: none"> Hazard characters must be filtered from the web application input Filters must be applied to ASCII and HEX values Update IDS (Intrusion Detection System) which functions as the first signal provider if an intruder tries to break into a computer security system

2. Penetration Testing on S2 Machine

There are several weaknesses of security that can be exploited. The testing scenario on this server is to get data from the web application. These data can be used by person who are not responsible for the application. This can trigger integrity weaknesses and confidentiality data. Testers try to sign in using default authentication for the login page.

ID of Vulnerable Detect	Recommendation
V1	<ul style="list-style-type: none"> Wordpress updates with the latest version to minimize the discovery of security holes The xmlrpc protocol should be hidden from information obtained using wpscan tools There are 2 ways to detect the occurrence of XML-RPC attacks on wordpress, namely the appearance of the message "error Connecting to Database" when the website is accessed, which indicates that the database is dead. In addition there are a lot of "POST /xmlrpc.php HTTP / 1.0" entries on the web server log
V2	change the default username in the wordpres login page
V5	<ul style="list-style-type: none"> blocking of the IP from the sender who sends a large number of requests at the same time Block access to the xmlrpc.php file. In this way the XML-RPC attack will fail before reaching its target of wordpress. The trick is to edit the .htaccess file and add the following lines: <Files xmlrpc.php> Order Deny, Allow Deny from all Allow from 192.168.1.10/24 Satisfy all

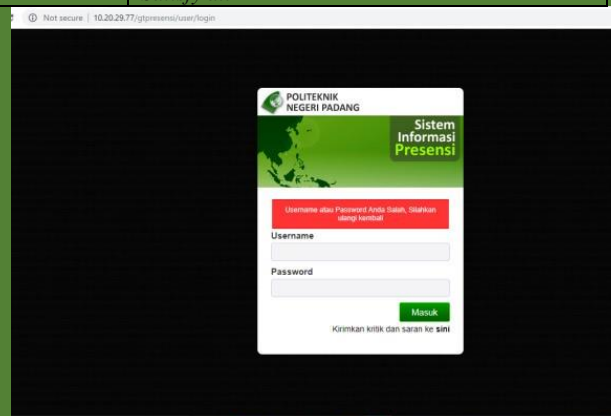


Fig. 9 Wrong Default Username and Password

The server contains weaknesses in XSS, the testers try to insert some characters to disguise authentication, so the login process can be forwarded in.

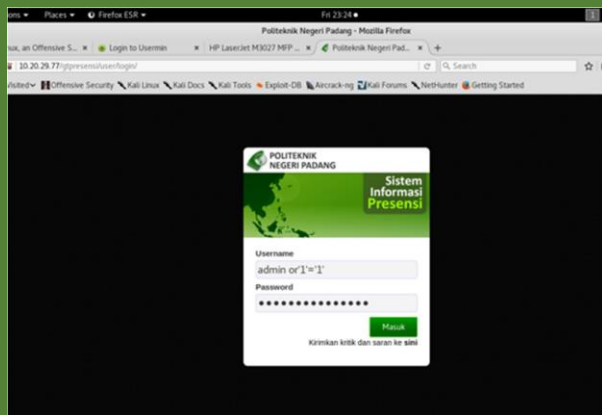


Fig.10 Inject Query to Login Page

Then the tester will try to retrieve data from the application based on the URL directory of the unprotected server. Access to the directory will be shown by the following picture.

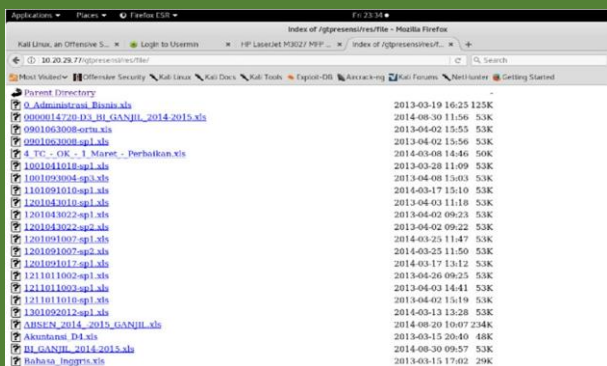


Fig. 11 Data from Directory Server

TABLE IX
EVALUATION AND RECOMMENDATION ON S2 MACHINE

ID of Vulnerable Detect	Recommendation
V1	URL directory to access confidential data that is not protected. This causes data exploitation, therefore give authentication to access the URL directory in the system
V6	The server it can be injected using the XSS method to disguise the username and password so that it can escape session authentication

3. Penetration Testing on S3 Machine

For the S3 machine perform privilege escalation to login page using default username and password to entering the system.

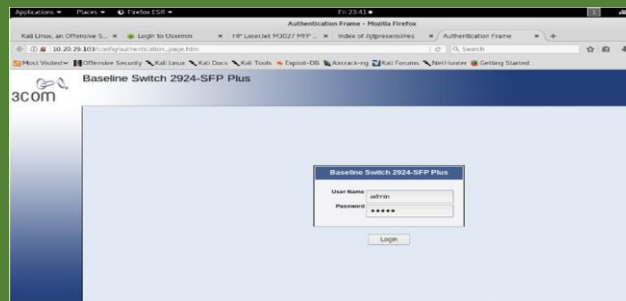


Figure 12. Testing Default Password on Baseline Switch Server

The tester successfully entered the system. This is a security gap that needs to be fixed, because if unauthorized user can enter the system, the settings can be damaged. Consequently the infrastructure and services on the network do not run optimally.

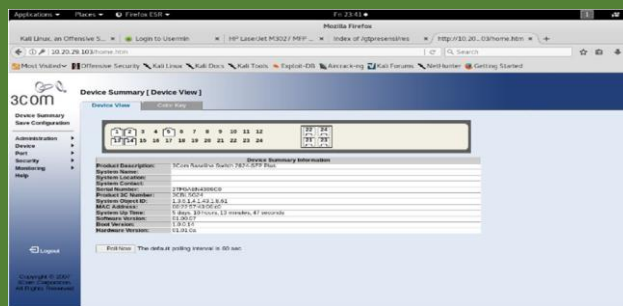


Fig.13 Successfully entered the system

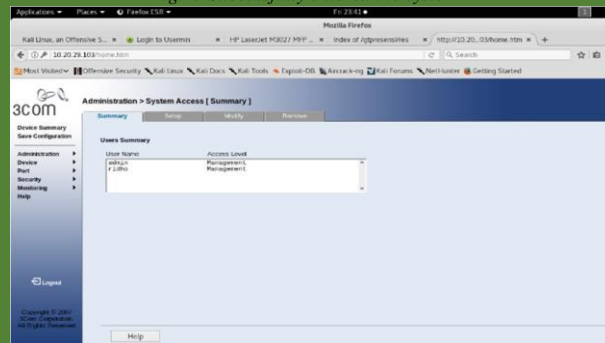


Fig. 14 Create New User in System

Testers can add users as administration to configure the system.

TABLE X
EVALUATION AND RECOMMENDATION FOR S3 MACHINE

ID of Vulnerable Detect	Recommendation
V3	Change the username with a combination of unusual characters making it difficult to numerate
V4	Change the password with a combination of unusual characters making it difficult to crack and using encryption method to secure authentication

4. Penetration Testing on S4 Machine

After the examiner visits the IP through the browser, the system page does not have protection. So that can be accessed

by anyone without protection. This is very dangerous for the system, because unauthorized user can configure and take over the system.

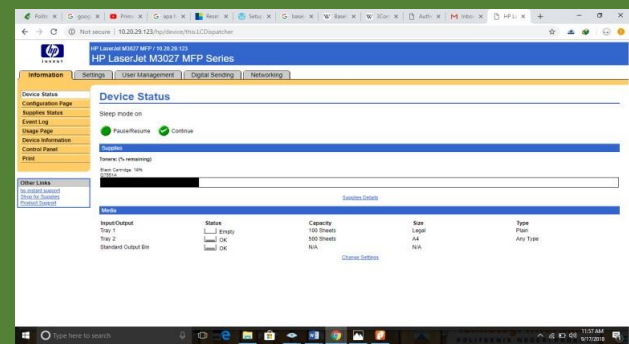


Fig. 15 Enter a System without protection

TABLE XI

EVALUATION AND RECOMMENDATION FOR S4 MACHINE

ID of Vulnerable Detect	Recommendation
V1	There is no protection from the application so that it can be accessed by anyone. therefore add protection to the system such

From the results of testing the level of security on the network, each device has a vulnerability level of 20% -80%. 60% of devices that have been tested can be attacked using XSS attacks and 60% use the default username and password for the login process to the system

TABLE XII

SUMMARY OF FINDING

Machines	DOS	Cross Site Scripting (XSS)	Metasploit	Plugin Attack	Default Username and Password
S1	<div></div>	<div></div>	<div></div>	<div></div>	
S2		<div></div>			
S3		<div></div>			<div></div>
S4					<div></div>
S5					<div></div>

V. CONCLUSIONS

	as authentication with a combination of characters that are difficult to get by hackers

From the results of penetration testing it can be concluded that almost every device has a weakness and can be attacked.. For this reason several recommendations are given so that device security can be improved.

REFERENCES

[1]

Gupta, A., Kavita, & Kirandeep, K. (2013). Vulnerability assessment and penetration testing. *International Journal of Engineering Trends and Technology*, 4(3), 328.

[2]

Felderer, M., Büchler, M., Johns, M., Brucker, A. D., Breu, R., & Pretschner, A. (2016). Chapter one-security testing: A survey. *Advances in Computers*, 101, 1–51.

[3]

Hamisi, N.Y., Mvungi, N.H., Mfinanga, D.A. and Mwinyiwiwa, B.M.M., “Intrusion detection by penetration test in an organization network”, *ICAST 2009*.

[4]

Kaur, M. S., & Singh, M. S. (2016). Penetration testing management. *International Journal of Advanced Research in Computer and Communication Engineering*, 5(3), 171–177.

[5]

Kli’ma, T. (2016). PETA: Methodology of information systems security penetration testing. *Acta Informatica Pragensia*, 5(2), 98–117.

[6]

Mattadi, E., & Kumar, K. V. (2015). Evaluation of penetration testing and vulnerability assessments. *International Journal of Electronics Communication and Computer Engineering*, 6(5), 144–148.

[7]

Pritchett Willie L, S. D. (2013). *Kali Linux Cookbook*. Birmingham,UK: Packt Publishing Ltd.

[8]

Endraca, A, King, B., Nodalo, G., Maria, M. S., & Sabas, I.(2013). *Web Application Firewall (WAF)*. *International Journal of eEducation, e-Business, e-Management and e-Learning*

[9]

Pritchett Willie L, S. D. (2013). *Kali Linux Cookbook*. Birmingham,UK: Packt Publishing Ltd.

[10]

Muniz Jospeh, L. A. (2013). *Web Penetration Testing with Linux*.

Birmingham, UK: Packt Publishing Ltd.

[11]

A.K. Kyaw, F. Sioquim, and J. Joseph, “Dictionary attack on Wordpress: Security and forensic analysis,” in *2015 2nd International Conference on Information Security and Cyber Forensics, InfoSec 2015*, 2016, p. 158–164.

[12]

S.P. Ganesh and G. Anandhi, “Database Security: A Study on Threats And Attacks”, *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 4(6), pp. 512-513, 2015.