VOL 2 (2018) NO 4 - 2

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

# Network Security Assessment Using Internal Network Penetration Testing Methodology

Deni Satria#, Alde Alanda#, Aldo Erianda#, Deddy Prayama#

#Information Technology Department, Politeknik Negeri Padang, Indonesia
E-mail: deni@pnp.ac.id

*Abstract*— **The development of information technology is a new challenge for computer network security systems and the information contained in it, the level of awareness of the importance of network security systems is still very low. according to a survey conducted by Symantec, the desire to renew an existing security system within a year within a company has the result that only 13% of respondents consider changes to the security system to be important from a total of 3,300 companies worldwide as respondents. This lack of awareness results in the emergence of security holes that can be used by crackers to enter and disrupt the stability of the system. Every year cyber-attacks increase significantly, so that every year there is a need to improve the security of the existing system. Based on that, a method is needed to periodically assess system and network security by using penetrarion testing methods to obtain any vulnerabilities that exist on the network and on a system so as to increase security and minimize theft or loss of important data. Testing is carried out by using internal network penetration testing method which tests using 5 types of attacks. From the results of the tests, each system has a security risk of 20-80%. From the results of these tests it can be concluded that each system has a security vulnerability that can be attacked.**

*Keywords*— **Penetration testing, network security, vulnerability.**

## I. INTRODUCTION

The development of information technology has an important role in people's lives. With the development of technology that is always undergoing change, making information security an important factor (Mason, 1986). Once the importance of the value of information often causes the information to be accessed only by certain people who have authority. So that the fall of information into the hands of unauthorized parties can cause harm to the information owner. For example, a lot of important information in a company is only allowed to be known by certain people in the company, such as information about products that are under development, algorithms and techniques used to produce these products. For this reason, the security of the information system used must be guaranteed and in accordance with existing standards.

The development of information technology is a new challenge for computer network security and information systems, according to a survey conducted by Symantec, the level of awareness of the desire to renew an existing security system within a year within a company gets results that only 13% of respondents consider change the security system is important from a total of 3,300 companies worldwide as respondents (Symantec State of Security Survey, 2011). This lack of awareness results in the emergence of security holes that can be used by crackers to enter and disrupt the stability of the system.

Cyber attacks have caused various personal data thefts. In government offices there have been nearly 21.5 million people who have experienced theft of data from office computers. In addition to government offices, attacks also occur in banks in the world. Cyber attacks have started since the end of 2013 and have stolen about 1 trillion US Dollars. More than 100 banks in the world from 30 countries affected by cyber attacks. The hacker installs spyware into a computer that is used by bank employees and observes the workings of bank employees and secretly transfers to bank accounts that are used for theft of money. According to brearchieveindex.com from 2013 to June 2015 there have been more than 3 billion lost and stolen data involving all types of people such as retail, government, education, financial and others.

## II. LITERATURE REVIEW

### A. Network Security

Network security is very important to monitor network access and prevent unauthorized use of network resources. Network security tasks are controlled by the network

administrator. Security aspects defined by five points, namely Confidentiality, require that information can only be accessed by those who have authority. Integrity, requires that information can only be changed by those who have the authority, availability, requires that information be available to parties who have the authority when needed, authentication, requires that the sender of an information be identified correctly and there is a guarantee that the identity obtained is not false. Nonrepudiation, requires that both senders and recipients of information cannot deny sending and receiving messages.

### *B. Penetration Testing*

Penetration Testing is a method used to evaluate the security of a system or computer network by performing an attack simulation. In the OWASP methodology Web Application Security Testing focuses only on the security of web applications, where the process involves actively analyzing web applications, to find weaknesses, technical defects, and weaknesses. Security issues that have been discovered will be given to the system owner, which is included with a report that contains information about the estimated impacts that arise as well as technical solutions to these problems.

Penetration testing has proven effective in helping to deal with security issues on the network. Penetration testing techniques are not only aimed at applications, but can also be applied to networks, and operating systems, where the main purpose is to find and then try to exploit vulnerabilities that are known or detected in previous evaluations contained in certain technologies

There are 3 types of penetration testing, namely:

1. Black-Box
   Penetration testing without knowing what systems or networks are used by an organization
2. White-Box
   Penetration testing by knowing the infrastructure information that is in an organization
3. Grey-Box
   It is a penetration test that combines blax-box with white box

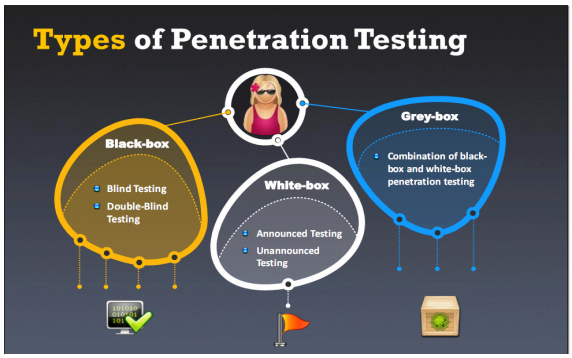


Fig. 1. Types of Penetration Testing

## III. METHODOLOGY

This research uses internal network penetration testing method. The steps that will be carried out in this research can be seen in the picture below

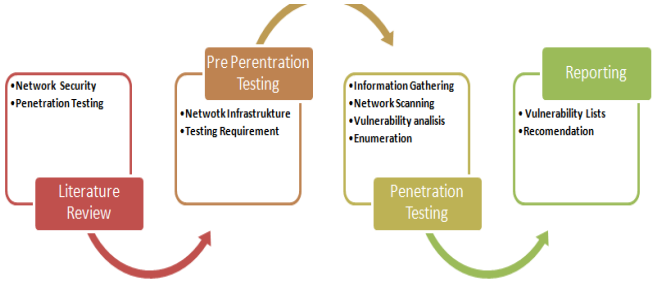


Fig. 2 Methodology

a. Literature Review by reading and understanding the literature in the form of books, sites, and scientific works related to network security and penetration testing
b. In the pre penetration testing stage, network security analysis is performed and then what components are needed to be assessed in the network.
c. Penetration Testing, at this stage assessment is carried out by using various tests on security loopholes contained in the system and exploiting the current system.
d. Reporting, after completing the assessment of the security of the system, then make a report based on the results of the assessment and provide recommendations on the security risks found in the system.

## 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 KnfTPD) |
| 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 Tesing*

*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.

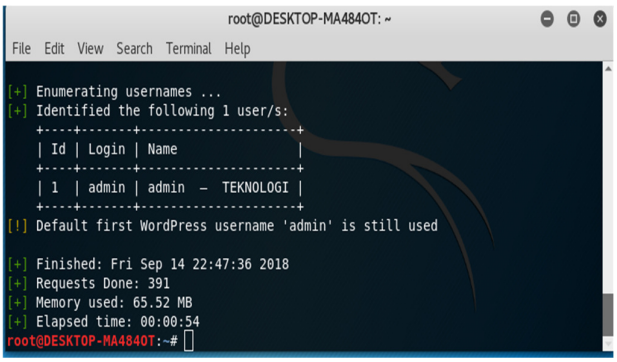


Fig. 3 Enumeration Username Using Wpscan

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.

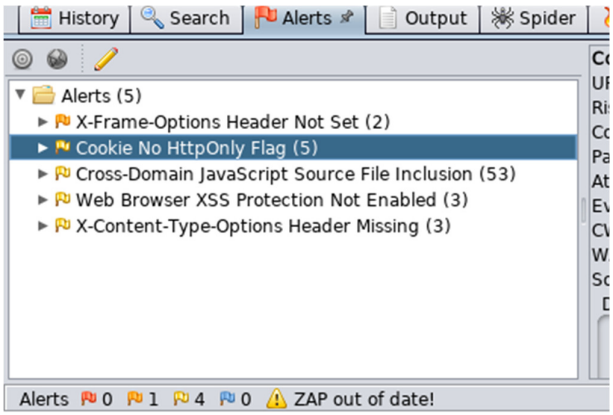


Fig. 4 Finding Vulnerable Using OWASP Zap Tools

Based on the picture above, found 5 things that become a weakness in the web scripting section that can be exploited later using the Cross Site Scripting attack type.

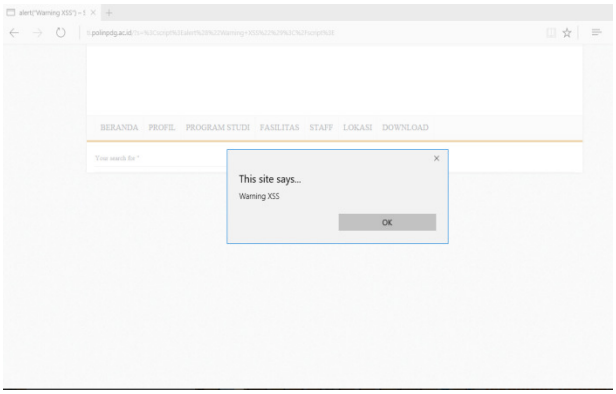


Fig. 5 XSS Attack on TI Web Server

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.

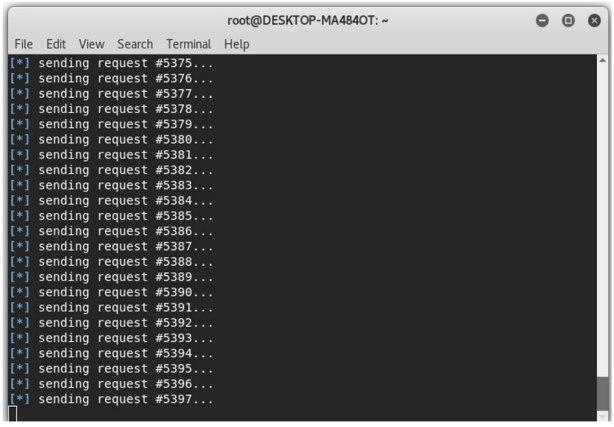


Fig. 6 DOS Attacking using Metasploit Tools

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

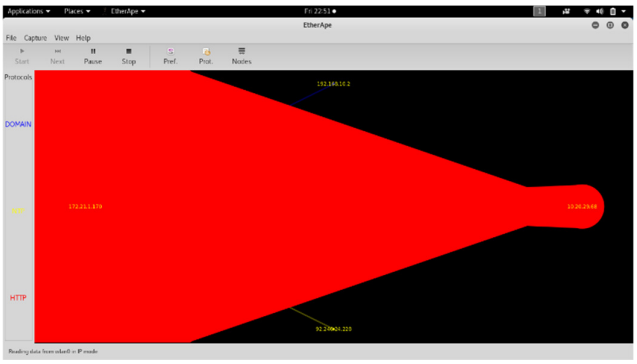


Fig. 7 Network Traffic Monitoring Using Etherape Tools

After perform DOS attack, the database connection on server becomes down. consequently the web cannot be accessed for a while.

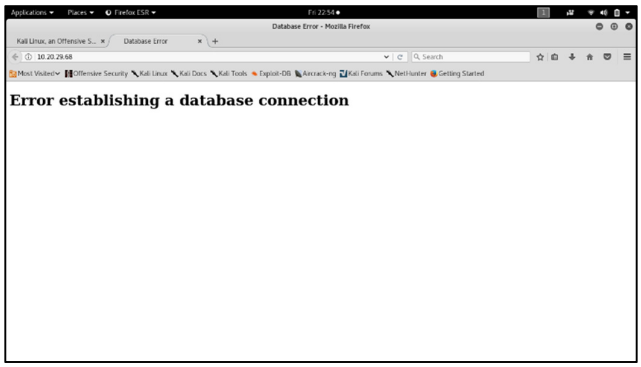


Fig. 8 Error Database Connection

TABLE VIII
RECOMMENDATION S1 MACHINE

| ID of Vulnerable Detect | Recommendation |
|---|---|
| V1 | • Wordpress updates with the latest version to minimize the discovery of security holes<br>• The xmlrpc protocol should be hidden from information obtained using wpscan tools<br>• 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 | • blocking of the IP from the sender who sends a large number of requests at the same time<br>• 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:<br><Files xmlrpc.php><br>Order Deny, Allow<br>Deny from all<br>Allow from 192.168.1.10/24<br>Satisfy all |

| | |
|---|---|
| | ErrorDocument 403 http://127.0.0.1/<br></ Files><br>Allow IP 192.168.1.10/24 to approve the IP administrator which is exemplified in the IP above to configure |
| V6 | • Hazard characters must be filtered from the web application input<br>• Filters must be applied to ASCII and HEX values<br>• 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.

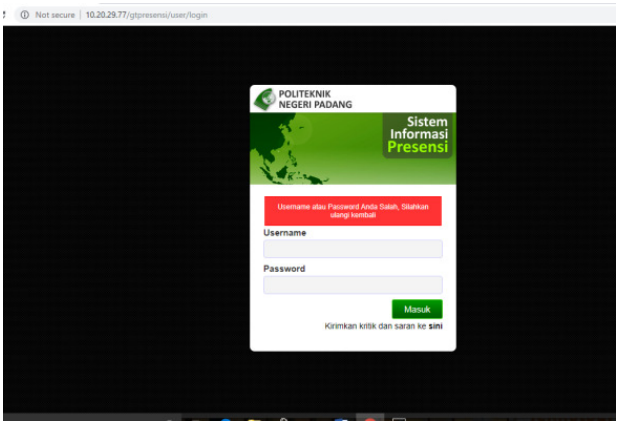


Fig. 9 Wrong Default Username and Password

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

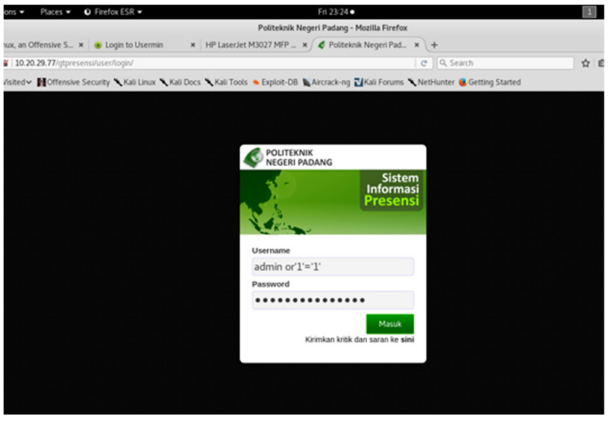


Fig.10 Inject Query to Login Page

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.

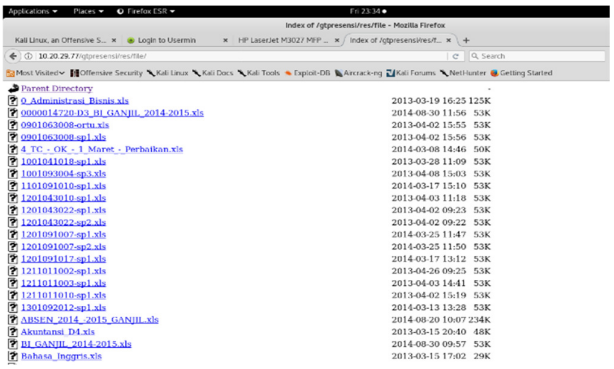


Fig. 11 Data from Directory Server

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.

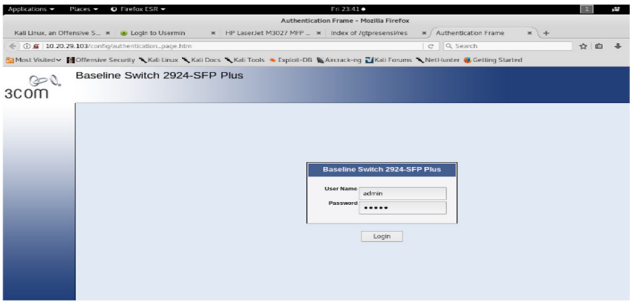


Figure 12. Testing Default Password on Baseline Switch Server

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.

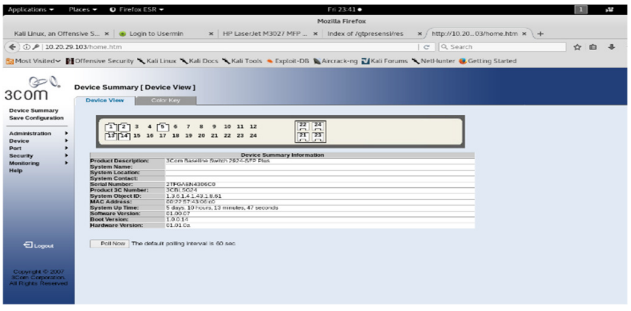


Fig.13 Successfully entered the system

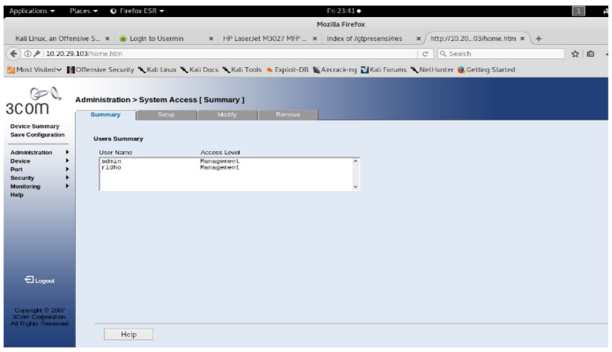


Fig. 14 Create New User in System

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.

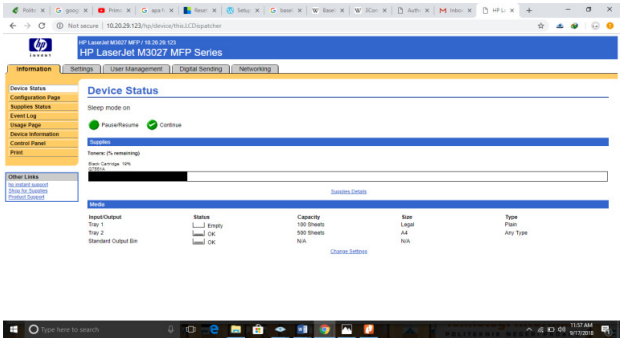


Fig. 15 Enter a System without protection

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

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 | ✓ | ✓ | ✓ | ✓ | |
| S2 | | ✓ | | | |
| S3 | | ✓ | | | ✓ |
| S4 | | | | | ✓ |
| S5 | | | | | ✓ |

## V. CONCLUSIONS

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] Klı´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 eEduciation, 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.