IJSEA

by Agustinus Noertjahyana

Submission date: 29-Mar-2023 07:54PM (UTC+0700)
Submission ID: 2049931728
File name: IJSEA04041003.pdf (226.26K)
Word count: 4111
Character count: 21561

International Journal of Science and Engineering Applications
Volume 4 Issue 4, 2015, ISSN-2319-7560 (Online)

Information Management System and Website Server Penetration Testing Case Study University

Agustinus Noertjahyana
Informatics Engineering
Petra Christian University
Surabaya, Indonesia

Richard Pangalila
Informatics Engineering
Petra Christian University
Surabaya, Indonesia

Justinus Andjarwirawan
Informatics Engineering
Petra Christian University
Surabaya, Indonesia

Abstract: A developing organization need information technology in its operational activity. However what is often considered is how to ensure that data saved in server is safe from unauthorized parties. Therefore, this thesis reviews how a person who is appointed as a security analyst do penetration testing in a system with variety tools given and how the report can be understood from by people from managers to programmers. Besides giving the how-to knowledge, this thesis also reviews how secure is the organization under review in keeping their data safe from other parties who are not supposed to get access to important operational activity data.

Keywords: Safety, Data, Evaluation, Penetration Testing, Security

1. INTRODUCTION

An organization who runs a system using IT-based always use computer in its operational activity. With development of IT, a need of storage medium or even data center is needed which called servers. However with such development, security is an aspect to be aware of by anyone who uses centralized system, because hacking, manipulation or even loss of data might happen if done by hacker who have bad deed to take sensitive data from an organization [1].

To reduce loss caused by hacker, the first step needed is to evaluate server securities. It's to reduce the risk of misconduct of available resources in an organization [2].

Most people within organization might get confused when requested to do a server security evaluation. This is because lack of knowledge in server evaluation. The method to evaluate an object security by penetrating it is called Penetration Testing or known as Pen testing [3].

Development in Petra Christian University is getting bigger and there's a lot of need in information system to run its operational activity. PCU has a lot of servers in each building such as P Building, T Building and RP Building. With network availability in each area of building throughout wireless and wired network, there's a need to pay attention it's relevancy between hacker and server within the network. Computer Center in RP Building held the main server which provides the basic system of students' academic activity.

Moreover things that also needed to be aware of is the student and staffs behavior because the one who conduct hacking is human themselves, sometimes a bad human behavior might bring bad effect directly or indirectly. Because of those problems, the most needed help is reducing and anticipate attacks from hackers which is monitoring servers in RP Building while doing penetration testing.

2. BASIC THEORY

2.1 Computer Security

The main goal of computer security is to protect information within it. Computer security is based on some aspects which listed on Ethical Hacking and Countermeasures module [3], such as:

Privacy, an object that is private which only limited few person who has access to it.

Confidentiality, data given to other party and being kept to select person.

Integrity, information not allowed to be changed unless by information owner.

Authentication, user verification through login window using user credentials and password, if matched it will be accepted and *vice versa*.

Availability, data availability when needed.

There are some steps to secure computer which explained in Ethical Hacking and Countermeasures module [3], such as:

Assets, assets protection is an important aspect and the first step from computer security implementation.

Risk analysis, identification to risk that might happen, such as a potential event to cause harm to systems.

Network security, all devices connected to network need to be assessed its security.

Tools, tools used on PC have an important role in security because the tools need to be secure.

Priority, whole PC protection.

2.2 Certified Ethical Hacking

Certified Ethical Hacker is a professional certification provided by International Council of E-Commerce Consultants (EC-Council).

Ethic hacker usually hired by organization who trusted them to do penetration testing o network or computer system with common method used by hacker to find and fix security vulnerabilities. If hacking done without organization authorization, it will be counted as cybercrime, but whereas authorized or requested it will be a legal action.

Certified hacker have certification in findings security vulnerabilities and system flaw using knowledge and tools like a real hacker.

Citing from EC-Council website, the certification code for CEH is 312-50 and it's in version 8 as of 2013. EC-Council also offers other certification which called Certified Network Defends Architect or known as CNDA. This certification is designed for America government agency and only available on certain agency with different names but have the same content, this certification code is 312-99.

2.3 Penetration Testing

Citing from CEH module, penetration testing is a method to evaluate computer system security or network by simulating attack from a dangerous source and a part of security audit [3]. This attack simulation is done like black hat hacker, cracker and others. The goal is to decide and know what kind of possible attack to be done to system and what risk might happen because of system vulnerability.

When doing penetration testing, intensive analysis is needed in each flaw caused by system weakness. Later on after the whole analysis is done, it will be documented and given to the owner along with solutions and effects caused by existing security vulnerability.

3. PEN TESTING METHODOLOGY

3.1 Penetration Testing Technique

There are a lot of things to be tested in penetration testing, it's because to give more picture to identify more threats such as communication failure, e-commerce, or even loss of private information. Moreover when facing public infrastructure such as e-mail gateway, remote access, DNS, password, FTP, IIS and site server, everything need to be tested from hardware through software.

There are some supporting factors like goals, limitation and procedure adaptation needed to maximize penetration testing. In spite of that there are some consideration between cost and the level op people doing the test. Finally there's also need of clear documentation and explanation of risk potential and findings results from analysis results and tests to client.

Citing from Licensed Penetration Tester module, there are some common techniques used in penetration testing, such as:

1. Passive Research : used to find all common information used in an organization
2. Open Source Monitoring : how open an organization to keep information integrity and private
3. Network Mapping and OS Fingerprinting : used to get network configuration being tested
4. Spoofing : system disguise testing in a computer registered to system, tested on both external and internal side
5. Network sniffing : running data capture in a network
6. Trojan Attacks : malware sent in a network in form of e-mail attachment or sent through a chat room
7. Brute-Force Attack : common technique to open password and able to overload a system or even denying access to whole requests
8. Vulnerability Scanning : overall checking on infrastructure target area of organization network
9. Scenario Analysis : final testing consists with testing and more accurate vulnerability security risk scoring in real-world case

3.2 Penetration Testing Scope

When doing penetration testing, there will be limitation to cover the need of clear analysis, such as how destructive the test will be. Based on the effect of testing, penetration testing divided into two types, they are destructive and non-destructive tests. Both of these tests will map all vulnerabilities and verify any findings with exploits available but the nondestructive type won't go as far doing Denial of Service and Buffer Overflow like the destructive test will do to prevent disruption on system.

3.3 Penetration Testing Types

As explained in LPT module there are two teams in penetration testing, red team and blue team [3]. Blue team is the one who test with the acknowledgement of IT staff, usually it comes with lower cost and the need of main activity to think about how a sudden attack being launched. In contrary, the red team does the testing without the knowledge of IT staff but with the managers of the company's consent. The goal of red team is to detect network and system's flaw with security check from the attacker's perspective to infrastructure.

Apart from teaming, there are kinds of penetration testing such as black-box, white-box or grey-box. They are differentiated by how they do the penetration test. Black-box pen test uses external method which the tester given only the information of the organization without any blueprint or organization schema, they will do penetration testing like a real hacker and cost more time and money. Unlike black-box pen test, white-box pen test uses internal method which the tester given all of the information of the blueprint or organization schema while the test will be conducted like a real staff inside the organization and also the target of tests already decided beforehand. This kind of testing method might be conducted with or without any announcement to the internal IT staff. The last kind is grey-box, where the tester will do the test from inside the organization while analyzing each applications vulnerabilities. This test will need a complete knowledge and also test from black-box kind to get a whole picture of vulnerabilities.

3.4 Research Flowchart

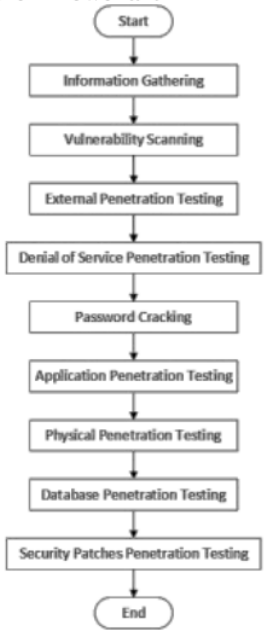

Figure 1. Research Flowchart

The flowchart on Figure 1 is based on LPT module and it will be implemented on this research. For the first step of research is to gather information regarding to physical server location, network type, and devices being used and other information related to PCU servers. After collecting all data, there will be a vulnerability scan. The next step will be external penetration testing to find out what information can be gathered and related to PCU servers from the sites. After collecting enough data, there will be a DoS pentest to find out how the servers managed to stay available under attack. Password cracking is needed to be done to find out weak passwords on systems [4].

Tests will be continued with application to evaluate PHP version, framework and additional services used on servers. Besides running softwares, physical access need to be tested such as how the servers being positioned, cabling arrangements, and other things related to physical access. Next step is to conduct database penetration testing such as MySQL, PostgreSQL, and its kind. The last step is to find out the security patch is applied or not in the system.
Later on after completing the whole tests, there will be a report based on LPT flowchart module as a standard that being used by analyst.
Based on the Penetration Testing module, this research will run under grey-box method to since some of the network schema already known and given from the foundation and also this test will be known as a blue team since it came from internal side of the foundation. To minimize service disruption this test will be on the non-destructive side.

4. APPLICATION IMPLEMENTATION

4.1 WHOIS

Citing from Internet Corporation for Assigned Names and Numbers (ICANN) website, WHOIS is a query and respond protocol that commonly used to query database regarding registered user or internet resources such as domain name, IP address block, or automated system, and also used for other information. This protocol save and send database content in a format readable by human [5].

4.2 NSLookup

Based on UNIX manual book inside the operating system, NSLookup is a command-line tool for network administration which available on all operating system to grab information about Domain Name System record [6]. Citing from Computer Hope said that during the development of BIND 9, Internet System Consortium wanted to deprecate NSLookup in favor of host and dig which provide higher level of industry acceptance, but later it was reversed during the launch of BIND 9.3 and finally there is a full support of NSLookup function
NSLookup means Name Server Lookup, it didn't use DNS library to do query so the result might differ from other function dig.
NSLookup is operatable in interactive mode and non interactive mode. When the mode is interactive, it can be used as an argument like common applications. If operated on non interactive mode, information is searched based on argument which was set beforehand as destined.

4.3 NetCraft

Netcraft is an Internet Service Provider in England. Netcraft was paid to provide services like: internet security service, application testing, source code review and automated penetration testing. Netcraft also provide data and analysis from any internet aspect.

4.4 ID Serve

Based on GRC.com, the founder's site, ID Serve is a freeware developed by Steve Gibson and useful to investigate essential security [7]. The main function is to do general check of a webserver. This program can give information regarding operating system used in server and other additional functions also included such as cookie and reverse DNS. Gibson Research Corp. developed many softwares useful for users. Usually the tools developed including:

- Finding vulnerabilities in server
- Firewall filter configuration
- HTTP and non HTTP server identification
- Reverse DNS Lookup using DNS to find out IP address

ID Serve is useful to create a security test to webserver. ID Serve functioned to give out information in readable form for users, the application also shows a port status is closed or hidden. The other function of ID Serve is to track a domain name from an IP address which shown in users' computer firewall log and ensure the owner for the security of their commercial sites.

4.5 HTTPRecon

Based on the project owner Marc Ruef's site, HTTPRecon defined as a site fingerprinting tool, this project runs on HTTP fingerprinting research area. The goal is to find out HTTP implementation in a complete way and also help in identifying vulnerability potential. The approach method used is automated from many sources to simplify and increase efficiency in enumeration website. Other method like banner-grabbing, code enumeration status and analysis used on header is also being used in this program.

4.6 OpenVAS

Based on OpenVas.org site, OpenVAS (Open Vulnerability Assessment System) is a framework contains some services and tools to offer security vulnerability findings and giving solutions [8]. This program is available for free under GPL license and the newest version is 8.0. This research will run the virtual operating system version provided by OpenVAS on Virtual Machine Oracle VirtualBox.

4.7 Acunetix

Based on Acunetix.com, Acunetix Web Vulnerability Scanner is an automated security test application which checks security vulnerability like SQL Injection, cross site scripting and exploitable vulnerability. This program focused on variety of exploits and vulnerabilities which make this program better than other vulnerability scanners [9].

5. APPLICATION TESTING

5.1 Information Gathering

5.1.1 WHOIS

With site such as DomainTools, information regarding the history of a domain is listed and viewed in WhoIs format, where information like domain creation date, owner of domain and simple information such as server system being used, location and IP address included in it. The result shown that www.xxxxx.ac.id and its subdomain listed under the name Mr. Justinus Andjarwirawan.

5.1.2 NSLookup

Domain www.xxxxx.ac.id is listed in PANDI domain registrar and have the IP address 203.189.120.xxx, along with Mail Exchanger from Google and the Nameserver located on local server owned by Petra with name Peter and Jacob and a backup DNS on ZoneEdit. There's a TXT type DNS which list domain verification so when e-mail sent from xxxxx.ac.id domain it won't be blacklisted. Other subdomain dewey.xxxxx.ac.id alongside bakp.xxxxx.ac.id only show canonical name or other alias as digilib.xxxxx.ac.id for Dewey and cpanely.xxxxx.ac.id for BAKP. While sim.xxxxx.ac.id site shows result 203.189.120.xxx as its IP address.

5.2 Webserver Footprinting

5.2.1 NetCraft

Www.xxxxx.ac.id site appeared for the first time on May 1996. This site is owned by Petra Christian University and there are few times hosting change from PT. Telkom Indonesia then developed by PCU foundation alongside the change there's also IP address change from 203.130.237.183 to 203.189.120.xxx and lastly to 203.189.120.xxx.

Sim.xxxxx.ac.id site first appeared on August 2011 with IP 203.189.120.xxx. No historical change of server for this site but there's a reboot activity shown 40 days ago during the test.
Dewey.xxxxx.ac.id site first appeared on November 2001, this site is an online library catalogue. This site is also under the foundation and there are changes to hosting for 3 times with IP address firstly shown as 202.43.253.210 to 203.189.120.xxx and lastly 203.189.120.xxx.
The last site, bakp.xxxxx.ac.id first appeared on June 2012, no historical changes on server or reboot activity shown because this site is not yet listed on NetCraft database before. Currently the IP address shown is 203.189.120.xxx.

5.2.2 ID Serve

From test result www.xxxxx.ac.id identified running an Apache based server with version 2.2.21 in UNIX operating system with OpenSSL module version 0.9.8. Sim.xxxxx.ac.id shown running under Debian with PHP version 5.2.6.1, the next site is Bakp.xxxxx.ac.id running under Apache version 2.2.27 with OpenSSL version 0.9.8. Lastly dewey.xxxxx.ac.id running a Debian OS with Apache version 2.2.16.

5.2.3 HTTPRecon

Differ from ID Serve result, www.xxxxx.ac.id shown using HTTP Apache webserver version 1.3.33, while dewey.xxxxx.ac.id and sim.xxxxx.ac.id both are running Apache 2.0.55. Lastly bakp.xxxxx.ac.id identified running Apache version 2.0.52.

5.3 Vulnerability Scanning

5.3.1 OpenVAS

From test result in Figure 2, Dewey.xxxxx.ac.id has 4 high, 3 medium, 2 low, and 28 log vulnerabilities. While Www.xxxxx.ac.id has 7 high, 19 medium, 2 low, and 97 log vulnerabilities. Bakp.xxxxx.ac.id has 8 high, 19 medium, 2 low, 96 log vulnerabilities. The last one is Sim.xxxxx.ac.id has the most vulnerabilities with numbers 19 high, 16 medium, 2 low, and 29 log vulnerabilities.

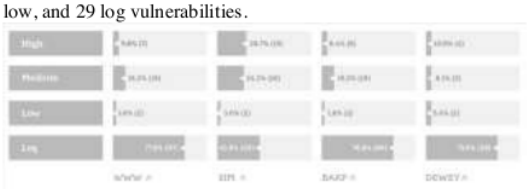

Figure 2. Vulnerabilities Numbers Graph Based On OpenVAS Scan Results

Figure 3. Vulnerabilities Summary Table Based On Open VAS Scan Results

Based on vulnerabilities summary which have been summarized on Figure 3, even Sim.xxxxx.ac.id has a lot of vulnerabilities number but those number mostly showing the same issue faced by this site, which means most issues such as OpenSSL and Apache can just be updated to the latest version to fix the issue shown. While Www.xxxxx.ac.id and Bakp.xxxxx.ac.id both have variety vulnerability which increased possibilities to be attacked from those vulnerabilities.

5.3.2 Acunetix

Vulnerability scan result from www.xxxxx.ac.id shows 476 warnings with 0 high, 166 medium, 17 low and 293 informational level warnings. While Bakp.xxxxx.ac.id shows 565 warnings with 67 high, 223 medium, 15 low, and 260 informational warnings. Less warning produced from Dewey.xxxxx.ac.id site with total of 93 warnings consist of 31 high, 18 medium, 19 low, and 25 informational warnings. The last site Sim.xxxxx.ac.id shows the lowest of all with 5 high, 32 medium, 10 low, and 40 informational warnings with total of 87 warnings. Details of diagram can be shown in Figure 4.

Figure 4. Vulnerabilities Numbers Graph Based On Acunetix WVS Scan Results

Figure 5. Vulnerabilities Summary Table Based On Acunetix WVS Scan Results

Based on scan summary results on Figure 5, each sites have identical vulnerabilities which means the sites can be attacked mostly using the same method such as DoS. To prevent those vulnerabilities summarized above, the server need to be reconfigured properly.

5.4 Analysis

5.4.1 Open VAS and Acunetix Web Vulnerability Scanner Scan Comparison

Both tools shows different scan results which tells how they check from different aspects. Open VAS focuses on external access to system which made this app inferior from Acunetix WVS when doing sites scan. The way Acunetix displays vulnerabilities scan result into a report needs to be praised because the program can limit how far the information should go when given to clients or programmers. However both software accuracy can't be assured since some of the method still rely on banner grabbing method.
These tools shows how a system is vulnerable but some still need to be proven through source code scan or configuration checkup to ensure these vulnerabilities are exists on system. And because of the limited access to system and its contents, this research can't go through detailed scan.

5.4.2 ID Serve and HTTPRecon Scan Comparison

HTTPRecon and ID Serve sometimes shows different result and there's a need to define which tools is better. Based on the testing method, ID Serve used only single method which is identifying server through its banner to identify the server whereas HTTPRecon uses fingerprinting method to compare server response with database to identify which is the most relevant version of server being used.

Banner-grabbing method is commonly used to identify servers, but nowadays to harden servers people reconfigure the banner identity to prevent further possibility of being attacked due to its' identity.

5.4.3 Problems Occurred During Penetration Testing

There are some factors which become limitation such as resource availability and time to test a site is too long (ie. Using Acunetix default scan profile might take weeks to finish a complex site) and might cause Denial of Service or the ISP might filter and block the connection between the tester and target sites because of the many requests given to sites tested.

Other problem mentioned is how PCU site not secured on some forms that tested which caused email spamming to lecturers and staffs on PCU while testing. This problem is caused because no captcha code exist on both resignation and deferral admission form. However after this event, programmers of PCU fixed this issue.

And to prevent further things happened, other testing needed such as password brute-forcing, DoS test and any testing was stopped.

5.4.4 Overall Security Test Results

System security for administration sites which tested in this research is categorized as not good, because there's no regular maintenance to system. From Acunetix security scan result, Sim.xxxxx.ac.id still has the best security amongst other site tested but there are need of some security patches to minimize vulnerabilities on system. Other sites that affected by SQL Injection and Cross Site Scripting need to be fixed soon because of mostly common attack that might be launched. Even though there are no access through system logs, it is suggested that every other sites not tested in this research need to be evaluated thoroughly especially in the migration process of Single Sign On method that being implemented on most campus academic system. Denial of Service might also happen if servers not reconfigured properly.

Other than the vulnerability mentioned above, there is a possibility to have site information being leaked due to file listing not being restricted on sites servers.

6. REFERENCES

[1] Hariwibowo, Dody. 2011. Keamanan Komputer | Pengantar Teknologi Informasi. 02 06. Accessed 10 21, 2014. http://dhoddycreater.wordpress.com/makalah-pti/keamanan-komputer.

[2] Barnatt, Christopher. 2012. ExplainingComputer.com: Computer Security. 09 13. Accessed 10 20, 2014. http://explainingcomputer.com/security.html.

[3] EC-Council. 2012. Certified Ethical Hacker v8 : Module 20 Penetration Testing. Amerika: EC-Council.

[4] EC-Council. 2012. Certified Ethical Hacker v8 : Module 12 Hacking Webservers. Amerika: EC-Council.

[5] Internet Corporation for Assigned Names and Numbers. n.d. WHOIS Primer | ICANN WHOIS. http://whois.icann.org/en/primer.

[6] Computer Hope. n.d. Linux and Unix nslookup command help and examples. http://www.computerhope.com/unix/unslooku.htm.

[7] Gibson, Steve. 2003. GRC | ID Serve - Internet Server Identification Utility. Oct 06. https://www.grc.com/id/idserve.htm.

[8] OpenVAS. 2015. OpenVAS - About OpenVAS Software. http://www.openvas.org/software.html.

[9] Acunetix. 2015. Web Application Security with Acunetix Web Vulnerability Scanner. https://www.acunetix.com/vulnerability-scanner/.

IJSEA

ORIGINALITY REPORT

6%	6%	3%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.coursehero.com Internet Source	3%
2	Submitted to Michigan Technological University Student Paper	2%
3	www.smoketechnologies.in Internet Source	1%
4	ijece.iaescore.com Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		