

Vulnerability Research and Mapping of Campus Network

Justinus Andjarwirawan, Agustinus Noertjahyana, and Devi C. Angi
Informatics Department, Petra Christian University, Surabaya, Indonesia
Email: {justin, agust} @petra.ac.id, m26411163@john.petra.ac.id

Abstract—Vulnerability of computer systems in campus-wide network has been an issue for years, since networks were open to allow anonymous access. It will take many studies of computer security to protect. A vulnerability research and mapping of a network is a step to address the issue, as well as minimizing security breach in the future. Evaluation of a network security can be done by many tools available and also guidelines based on CEH (Certified Ethical Hacker) module and Acunetix for web specific security. These test tools were deployed several times on every target, scanning open ports and sending test scripts to find vulnerabilities. With CEH and Acunetix guidelines, the evaluation shows many common security weaknesses such as Cross-Site Scripting, SQL injection and DDoS vulnerabilities and therefore this evaluation leads to security recommendations based on the weaknesses and security holes found.

Index Terms—vulnerability, penetration testing, vulnerability scanning, certified ethical hacker, acunetix

I. INTRODUCTION

Network security evaluation is done inside Petra Christian University, Surabaya, Indonesia, as the target. The chosen test object has a very common university network configuration. Common configuration also delivers common attacks such as computer virus, trojan, backdoors, spams, as well as cross-site scripting and SQL injection.

Universities today still manage their own web servers, mail servers and databases. The focus of monitoring intrusions is on these servers, besides the routers and firewalls.

In order to reduce the losses caused by hackers or intruders, the first step that must be developed is the observation and evaluation of the servers' security measures.

The Internet has become a critical resource because it can present the desired information easily, quickly, and inexpensively. In its development, the web has expanded its functions. In the era before the presentation of the information is static, after the development of a web-based application technology presentation of information becomes more dynamic nature. When the information held is relatively small, the information search process can be run relatively easy, but when the amount of

information has become outnumbered, then the search process and the appearance of such information into a web page will also be an obstacle, and the application must be able to respond to this.

This technology brings a significant change in the system development process in the Internet network service providers. This technology enables service providers to deliver more innovative services. But behind all the advantages that this technology has a problem in terms of security.

In addition, with the development of WWW and the Internet, causing the movement of information systems to use as a standard. Many systems are not connected to the Internet but still use the web-based apps as the basis for its information systems that are installed and connected to the Intranet network. To that end, the security of web-based information systems and Internet technologies rely on the security of the web system.

Web server security is usually a matter of system administration. By installing a web server in the system, then open up access to outsiders. If the server is connected to the Internet and a web server is set up for the public, it must be careful because opening the access door to the rest of the world.

Often neglected security issues and the importance of system security applications only realized after a disaster. Without a good security system applications, no matter how great the technology it will greatly endanger the institution or organization itself.

Vulnerability is a weakness that threatens the value of integrity, confidentiality, and availability of an asset. Penetration testing or better known as pentest is one method that can be used to evaluate a computer network. In addition, mapping of the vulnerability also needs to be done. Most reports of the penetration test are used to define protections against possible future attack.

A. Problem Statements

Monitoring campus-wide computer network and servers. The first step to evaluate this wide network is collecting all information about the existing network and active servers in the area.

Expected solutions to secure a campus-wide network are based on the evaluation. Mapping is given after a full scan of the entire network. A report of the whole scanning, penetration test and test tools results is given at the end of the test. CEH (Certified Ethical Hacker) by EC-Council will be the guideline to analyze and

implement a security policy, as suggested (K. Graves, 2010) [1].

Acunetix is a software as a tool to analyze vulnerabilities of web sites and web based applications. Cross-site Scripting (XSS) and SQL injection are the top security vulnerabilities found.

B. Methodology

Surveys of the existing Local Area Networks (LANs), servers, infrastructure are done both by interviews and own scanning. Accessing to the campus network is available through wireless network, wired network, and also the Internet.

Filter and limitation of the network access through a router or firewall are easily detected by doing a port scanning with nmap tool. A firewall test must be done both ways, from inside the campus network to the Internet and from the Internet to the demilitarized zone (DMZ) of campus network.

II. THEORIES

A. Network Security

There is no network that is capable of anti tapping nor computer network that is completely secure. The nature of a computer network is for communication. Each communication can fall into the hands of others and can be misused. Security systems help secure the network without blocking the user and puts anticipation when the network successfully penetrated. In addition, it is important to make sure that the users in the network have sufficient knowledge about the safety and that they accept and understand how the security plans are made.

There are two main elements of forming a secure network, they are:

1) Firewall, both physical and virtual, which is placed between the device and network services used and the people who may misbehave.

2) The security plan, which will be implemented together with the users to keep the system from penetration from outside.

In addition to those described above, network security can be aimed for information system owners that can keep their information system from compromised by others, which in turn can damage the system.

The type of intruder may include:

The Curious: this type of intruder is basically interested in finding the type of system and data owned by a person or company.

The Malicious: type of intruder is trying to ruin someone else's system or modify a webpage.

The High-Profile Intruder: this type is trying to use someone else's system to gain popularity and fame.

The Competition: this type of intruder is interested in what data you have in the system of organization or others.

Computer security is one important aspect of an information system. Meanwhile, a network itself can also be secured from attacks. In terms of the types of existing network security, they are: Confidentiality, Integrity,

Availability, Non-repudiation, Authentication and Accountability.

B. Hacking

Hacking is a common term that is usually negative, but in the definition itself hacking is a way of someone who manipulates things to perform better or useful for another purpose. A negative person doing a bad hacking is known as a cracker, or those who do cracking a system.

A computer hacker term may mean either bad or good depending on the purpose of hacking. A hacker may damage confidential information, steal confidential information, and also modify them.

But a hacker may do good things for good purposes, that they were called white hat hackers. Its purpose is for an assessment [2] of an organization's network. Also a good hacker term is used for the certification such as CEH. A hacker will do his job ethically to identify attacks which may come from inside and outside of organization. Any possible break in, modifying, stolen information, bypasses found are to be reported.

Hacker term is commonly classified as:

1) White hat hackers, they are the people who browse through or break the security system for malicious purpose. These objectives revolve around the security system testing to find a big gap in the network. Such hacker usually follow a legitimate manner and work in the area of cyber law.

2) Black hat hackers, they are generally subvert the security of computer without authorization with the help of a variety of viruses and other hacking tools. These type of hackers use the technology for fraud vandalism, credit card, or identity theft.

3) Grey hat hackers, they are part mid-way between black hat and white hat hackers.

Understanding and becoming one type of these hackers will strengthen its own organization's strength [3], [4], as one will understand deeply how attacks work.

C. Penetration Test

The purpose of penetration testing is to find vulnerabilities of a system. There are two types of testing, they are: external testing and internal testing.

External testing is to test all available information and access that is available to public or without any kind of authentication.

Internal testing is to recognize the number of network access points internally.

The analysis done in this research to the objective campus is by using the external testing.

The three methods of penetration testing are: Passive, Active and Aggressive. Passive test will test inside web applications, logins and configurations. Active test will do input manipulations, possess access rights and test all known vulnerabilities. Aggressive test will do the vulnerability exploits, reverse engineer a software or system, putting a backdoor, steal codes and manipulate finance related information.

The campus object test is done with the passive type of penetration test.

The penetration phases are: discovery, enumeration, vulnerability mapping, exploitation, as also found in many campus wide penetration tests [5]-[7], and finally report generation.

D. Web Vulnerability Scanner

Vulnerability scanner is a computer program designed to search and map system for weaknesses in applications, computer or network. The increasing use of the internet makes more and more websites are popping up. But it is unfortunate Internet crime continues to increase as the emergence of diverse articles that discuss the issue of hacking.

Vulnerability research is one way to hone and follow the developments in the world of hacking activities. Vulnerability research is the process of finding and looking for weaknesses that allows a system to be hacked.

Website security may be the most overlooked aspects at this time. Though securing the company should be a top priority in any organization. Hackers seek to concentrate their efforts on web-based applications (such as shopping carts, forms, login page). Web applications are accessible 24 hours a day, 7 days a week and serve to control valuable data since web applications have direct access, such as customer databases. Web applications are often created but less testing so it is more likely to have vulnerabilities and less attention. Acunetix Web Vulnerability Scanner (www.acunetix.com) automatically checks web applications against SQL Injection, XSS and other web vulnerabilities.

Tool Acunetix Web Vulnerability Scanner 9.5 is used in this research and can also display the level of the scanning results.

III. ANALYSIS

The purpose of this research is to find weaknesses, that are the vulnerabilities of the network and systems, then also to deliver solutions to secure those vulnerabilities.

The tools used for the test are penetration tools softwares that are suggested by CEH.

The first tool is for footprinting, using Angry IP Scanner (angryip.org), and then scanning with Acunetix, and finally enumeration with Softperfect Network Scanner. Some tools that are suggested by CEH are paid commercial applications. The rest are open source applications.

According to CEH, 90% of the time a hacker spends their time is to collect information. The rest are to take over the target.

Footprinting which is the first thing to do as a hacker is to define the target by doing port scanning to all available IP addresses of the target network, to find available services and active hosts.

Footprinting the campus network finds information:

- Target IP addresses
- Live services: web (http & https), ftp, ssh
- Host names
- Application version (e.g. web server version)

The Acunetix tool delivers a report that counts the numbers of vulnerabilities and the level of the security

vulnerability, from low, medium, to high; as in Microsoft [8]. Table I shows major vulnerabilities found in the testing.

TABLE I. VULNERABILITY SUMMARY

Description				
No.	Attacks	Vulnerability	Total alerts	Level
1	Cross Site Scripting (XSS)	Cross site scripting (verified)	12	High
		jQuery cross site scripting	8	High
2	SQL Injection	Blind SQL Injection	7	High
3	CSRF (Cross Site Request Forgery) protection	HTML form without CSRF protection	18	Medium

A. Footprinting

Footprinting is a process to uncover and gather as much information as possible about the target network. The purpose of doing footprinting, among others, collecting information about the target network, the target information systems, and information about an organization.

In this technique, the tools used are Angry IP Address.

B. Scanning Fingerprinting and Enumeration

Scanning fingerprinting is one of the procedures to identify the host, port, and services in a network. Additionally, fingerprinting scanning marks the beginning of a hacker attack (pre-attack). Through this fingerprinting scanning, hackers will find a variety of possibilities that could be used to take over a victim's computer.

Scanning can be categorized in three types, they are:

1) Port scanning: Port can be like an open door. So, in real life, one must pass through a door first then enter a room separately. Thus, a system is impossible to provide public services such as web servers, ftp servers, and mail servers without passing through or open a port. To make a search of ports it can be done in 2 ways, including manually (with the help of telnet) or by using a tool.

2) Network scanning: Network scanning is one step which does to host or active computers in a network. The more active computers that can be known, it will be easier for hackers to attack. This is because the hacker only requires one entrance while as a target or victim, must keep some doors, tens or even hundreds of doors.

3) Vulnerability scanning: Vulnerability scanning is aimed at finding the weakness of a system. By knowing vulnerability or weaknesses in a system, only a small step to enter the victim's computer. But if any weaknesses tried one by one, it will require a long time, then the vulnerability scanner tool can help accelerate the search for weaknesses.

Fingerprinting itself has two types, they are:

Active fingerprinting, it is when a tester has direct contact to the system. This tester or hacker will send packets to targets and find the responses.

Passive fingerprinting, it is when a tester is gathering packets of information without a direct contact on the target.

Enumeration is a term with similar process that is excavation to obtain usernames, machine names, resources, shares, and services of a system. This kind of information can be obtained through SNMP (Simple Network Management Protocol). The tool used is SoftPerfect Network Scanner (www.softperfect.com). This test will succeed only if the target runs an SNMP agent and without authentication. SNMP is commonly available to public access but only inside an organization to monitor network usage, but it is possible to add additional information.

In this research, this is the kind of vulnerability scanning type that will be used to evaluate the security of the network server.

IV. TESTING

First step is footprinting that will use Angry IP Scanner tool which this tool can display the details of a range of IP addresses. As a system administrator, this tool is very helpful in saving time monitoring the network. When there are common hacking tools from laptop or workstation connected to the network, it can immediately know that there is a possible attack.

Second step is fingerprinting with Acunetix Web Vulnerability Scanner 9.5 scanning to a subnet of an IP network. It helps to find vulnerable IP addresses or hostnames. This tool also provides level of vulnerabilities.











Third step is enumeration with SoftPerfect. Open ports are detected. Open ports does not mean a security hole, but they are open services that must present for operations. List of open ports is a list of test targets, which is used for the next test.



















Overall, the test targets are those to IP addresses and hostnames found by pretest tools above. Any non-detectable hosts or servers are not tested. They may be closed systems or proprietary systems that are not running on top of TCP/IP or not IP based application systems.

Each targeted test is reported separately, generated by the test tools and examined. The levels of vulnerabilities found or possible holes, weaknesses; are labeled and given the information of which service that are affected.

One example of a report is shown in Table II:

TABLE II. TEST RESULT

No.	Level	Report
1	High	 Web Alerts (162)  PHP Hash Collision denial of service vulnerability (1)
2	Medium	 Apache httpd remote denial of service (1)  Apache httpOnly cookie disclosure (1)  Directory listing (12)  Error message on page (30)  HTML form without CSRF protection (2)  PHP hangs on parsing particular strings as floating point number (1)  Source code disclosure (2)  Webalizer script (1)

3	Low	 Apache 2.x version older than 2.2.10 (1)  Apache mod_negotiation filename bruteforcing (1)  Documentation file (5)  Login page password-guessing attack (1)  MySQL username disclosure (6)  Possible sensitive directories (2)  Session Cookie without HttpOnly flag set (1)  Session Cookie without Secure flag set (1)  TRACE method is enabled (1)
4	Informational	 Broken links (10)  Email address found (27)  Error page web server version disclosure (1)  GHD: Possible PHP configuration file (config.php) (1)  GHD: SQL error message (6)  Password type input with auto-complete enabled (1)  Possible internal IP address disclosure (14)  Possible server path disclosure (Unix) (20)  Possible username or password disclosure (12)

Denial of Service vulnerability is noted as a high and medium level threats. Most Denial of Service [9] vulnerabilities found on running Apache servers with PHP modules which are not configured correctly, such as:

- Directory and files exposure
- Unprotected form fills which can lead to system freeze, cross site scripting and SQL injection as well
- Web script exposure (javascript)
- Back end script exposure

In low level threat findings, there is an opening for brute force on login page. Web server should have limitation by limiting the attempts of users login or else brute force will occur endlessly. Latest versions of applications, web servers and their modules are recommended in this low level finding.

Additionally, there is an informational findings to recommend:

- Remove broken links as it will expose server information such as directories and web server features.
- SQL error message and backend such as PHP error message should be hidden to cover its file location in the system and also the file names of the scripts.

At the network level, it is suggested to deploy an Intrusion Detection System to anticipate any intrusion attempt, as suggested (Bhuyan, 2013) with network anomaly detection [10].

When an intrusion occurs, the first priority is to stop the source and identify the origin [11]

V. CONCLUSION

Port scannings were not completely tested on all available ports, which may miss a few known services that changed their default ports.

Many web sites and web applications are found to be vulnerable to Distributed Denial of Service (DDoS).

Old versions of web servers are also spotted. Many web applications are found to have using old versions and deprecated functions which could cause a Cross-Site Scripting and SQL injection attacks. These are the most

vulnerabilities found commonly in other organizations [12].

The suggestions are to always keep an up to date versions of operating systems and applications. Also to do periodic tests. It is also suggested to classify port penetration attempts and in percentage values and weights, therefore administrators will have priorities to anticipate future attacks based on the most probable attempts.

Recommendations by the tools used in the tests are exposing as little information as possible about the system itself, and also limit and filter any key in information from the users to prevent brute force and DDoS attacks.

ACKNOWLEDGMENT

The author wish to thank the ICCCV committees for accepting this paper, and also Agustinus Noertjahyana and Devi C. Angi for supporting the research.

REFERENCES

- [1] K. Graves, *CEH Certified Ethical Hacker Study Guide*, Sybex, 2010.
- [2] P. C. Behera, C. Dash, and S. Mohapatra, "Ethical hacking: A security assessment tool to uncover loopholes and vulnerabilities in network and to ensure protection to the system," *International Journal of Innovations & Advancement in Computer Science*, vol. 4, pp. 54-61, May 2015.
- [3] J. Conrad, "Seeking help: The important role of ethical hackers," *Network Security*, vol. 2012, no. 8, pp. 5-8, Aug. 2012.
- [4] T. Caldwell, "Ethical hackers: Putting on the white hat," *Network Security*, vol. 2011, no. 7, pp. 10-13, Jul. 2011.
- [5] Y.-P. Lai and P.-L. Hsia, "Using the vulnerability information of computer systems to improve the network security," *Computer Communications*, vol. 30, no. 9, pp. 2032-2047, Jun. 2007.

- [6] N. H. Mvungi, D. A. Mfinanga, and B. M. M. Mwinyiwiwa, "Intrusion detection by penetration test in an organization network," in *Proc. 2009 2nd International Conference on Adaptive Science & Technology*, Accra, Jan. 2009, pp. 226-231.
- [7] Z. Sahri, M. E. S. A. Aziz, K. I. Zolkefley, R. Sadjirin, and M. I. M. Raus, "Implementing IT security penetration testing in higher education institute," *Australian Journal of Basic and Applied Sciences*, vol. 8, no. 21, pp. 67-72, 2014.
- [8] A. Sedigh, K. Radhakrishnana, C. E-A Campbella, and D. Singh, "Trust evaluation of the current security measures against key network attacks," *MAGNT Research Report*, vol. 2, no. 2, pp. 1-9, 2014.
- [9] A. G. Ostapenko, S. S. Kulikov, N. N. Tolstykh, Y. G. Pasternak, and L. G. Popova, "Denial of service in components of information telecommunication system through the example of network storm attacks," *World Applied Sciences Journal*, vol. 25, no. 3, pp. 404-409, 2013.
- [10] M. H. Bhuyan, "Network anomaly detection: Methods, systems and tools," *Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 303-336, Jun. 2013.
- [11] L. M. Chen, M. C. Chen, W.-J. Liao, and Y. S. Sun, "A scalable network forensics mechanism for stealthy self-propagating attacks," *Computer Communications*, vol. 36, no. 13, pp. 1471-1484, Jul. 2013.
- [12] R.-R. Xi, X.-C. Yun, S.-Y. Jin, and Y.-Z. Zhang, "Research survey of network security situation awareness," *Journal of Computer Applications*, vol. 32, no. 1, pp. 1-4, 2012.



Justinus Andjarwirawan is a lecturer in the Informatics Engineering department of Petra Christian University. It is based in Surabaya city, Indonesia. He was born in Central Java, Indonesia in 1972. He has a bachelor degree of Electrical Engineering from Petra Christian University, Indonesia, and a master degree in Computer Science from Asian Institute of Technology, Thailand. His current interest and teaching subjects are Open Source Programming, Mobile Programming, and Web Programming. His research interests are in subjects of computer networking, user experience, user interface, human-computer interaction, web technology, and mobile applications.