Web Server Security Analysis from DDoS Attack using Information Systems Security Assessment Framework Method

Randi Indraguna
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
An information system is a system that provides information for management in making decisions and also for carrying out the operations of an organization or individual, such as in the use of website-based information systems for local governments, with an information system, it is important to protect against cybercrime, especially DDoS Attacks. Reporting from the company Kaspersky DDoS Protection DDoS attacks grew on average in Q1 2020, DDoS attacks lasted 25% longer than in Q1 2019. Therefore, it is important to secure the webserver of a system, so that the system can be protected from various forms of cybercrime. especially DDoS Attacks.The stages of data collection in this study include the literature study and interviews, while the research stage includes information gathering, network mapping, vulnerability testing, and analysis of reports used on the research object of an information system web server.The results of the study proved that the Information Systems Security Assessment Framework (ISSAF) method can be used to analyze the vulnerability of a web server from an information system, in the form of some data regarding server information, network mapping, the level of vulnerability of a server in this study is level 1: low, and does not have The anti-clickjacking X-Frame-Options and The X – XSS – Protection and in the next stage, the highest attack packet data penetration test is 1220689 and the lowest attack packet data is 28240 which is normal, and then the data is analyzed.

Keywords
Web Server, DDoS Attack, System Information,Penetration Testing (ISSAF).

1. INTRODUCTION
Security is one of the important factors that must be considered in building a website. This is a challenge for website developers because there is no definite guarantee of the definition of safe itself. no system is completely safe, is not a mere statement, but has been felt in reality. [1].Especially in the security of a web server, in the sense that the webserver is a service provider for the browser so that the browser can display data or pages requested by internet service users. [2]. The security of a vulnerable system will be easily attacked by hackers so that they can take over a system and make it possible to manipulate or steal the data taken. Hacker is someone who has the ability to programming and computer networks. [3]. Especially in the form of DDoS Attack attacks, in general, DDoS Attacks experienced an increase in Q1 2020, compared to what happened in 2019 the spike in DDoS Attack attacks had decreased by 90 percent compared to the previous year which had reached 100 percent and then in 2020 experienced two times compared to 2019, which was 180 percent.

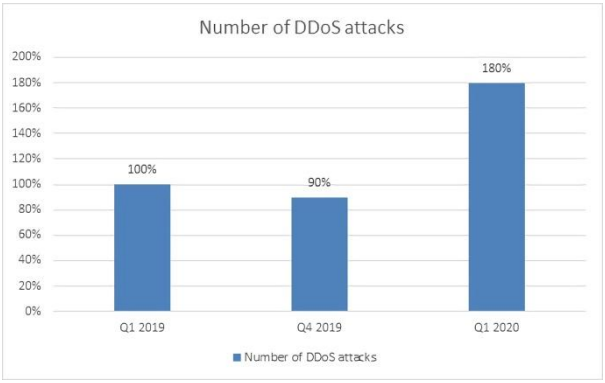

Figure 1. 2020 DDoS Attack Upgrade

Figure 1, Kaspersky company has analyzed the form into a graph so that it can be seen the difference in the increase in attacks every year against DDoS Attacks.
To secure the webserver from hacker attacks, it is better for web server owners to do a self-test on their own server. Through this self-test, web server owners will find out where the vulnerability of the existing system is. One of these self-test methods is penetration.[4]. Information Systems Security Assessment Framework (ISSAF) is an optimal penetration testing process stage that aims to provide direction to auditors to conduct complete and correct tests, and to avoid errors in performing random attack tests. [5].

1.1 Study Literature
1.1.1 Previous Study
Previously, some studies discussed the analysis of web server security in various systems such as those based on websites and other applications and using several testing methods such as the OWASP and ISSAF methods. In a study conducted by Guntoro, Costaner, and Musfawati (2020) with the title "Security Analysis of the Web Server Open Journal System (OJS) Using the Issaf and Owasp Method (Case Study of OJS at LancangKuning University)". The researcher discusses the vulnerability of the webserver on the LancangKuning University Open Journal System system, there are two methods used by researchers, namely the Open Web Application Security Project (OWASP) method and the Information Systems Security Assessment Framework (ISSAF) method. webserver from SQL Injection and Site Scripting attacks. The results of this study are to find vulnerabilities in the Open Journal System (OJS) webserver,

After checking the Open Journal System (OJS) webserver, the results obtained are that the site is classified as safe.[4].

Furthermore, there is also research conducted by Lisa HandasariYanti, Iqbal, Banta Cut (2019) with the title "Analysis of Web Server Security from Remote Os Command Injection Attacks on Government Agencies of Banda Aceh City". The researcher discusses testing the security of the Banda Aceh City government agency web server, the method used is purposive sampling using the Owasp Zap tool version 2.7.0, the purpose of this study is to test the security of the Banda Aceh City government agency web server using the Remote OS Command technique. Injections. The results of this study are to get an analysis of the intensity of attacks on the system of each Banda Aceh City government agency so that each agency gets different analysis results. study of literature.[2].

Research conducted by Yunanri W, Imam Riadi, Anton Yudhana (2016) with the title "Analysis of Web Server Security Using the Penetration Testing Method (PENTEST)". Researchers about the benefits, strategies, and methodologies in penetration testing, the method used are the method of penetration testing (pentest) or finding weaknesses in an application or website that is used on a web server, the purpose of this research is to determine and find out the kinds of attacks that may be done on the system and the consequences that occur because of the weaknesses contained in the system. The result of this research is to produce procedures or work steps in conducting penetration testing.[3].

In addition, research conducted by Mohammad Muhsin and Adi Fajaryanto (2015) with the title "Application of Web Server Security Testing Using the OWASP Version 4 Method (Case Study of Online Exam Web Server)". The researcher discusses the security of the webserver on the web-based online exam system at the University of Muhammadiyah Ponorogo, the method used is the Open Web Application Security Project (OWASP), the purpose of this study is to determine the vulnerability of the online exam application from the Faculty of Engineering, University of Muhammadiyah Ponorogo and want to know test results and analysis results of the methods used. The results of this study are that there are authentication, authorization, and session management that have not been implemented properly, so there need to be improvements from the system developer.[6].

Another study was conducted by Raden TeduhDirgahayu, YudiPrayudi, and Adi Fajaryanto (2015) with the title "Implementation of the ISSAF and OWASP Method Version 4 for Web Server Vulnerability Testing". The researcher discusses the webserver vulnerability in the IKIP PGRI Madiun system, the method used is the Open Web Application Security Project (OWASP) method and the Information Systems Security Assessment Framework (ISSAF) method. PGRI Madiun IKIP system. The results of this study are the Information Systems Security Assessment Framework (ISSAF) method that the system can still be penetrated while with the Open Web Application Security Project (OWASP) method there is authentication, authorization, and session management that has not been implemented properly.[7].

1.1.2 Information System Concept

Systems and information have each understanding that can be understood, the system is defined as a collection or set of elements, components, or variables that are organized, interact with each other, depend on each other, and are integrated according to Mujahidin and Putra. [8]. This system describes a real event as a real object, such as places, objects, and people who exist and occur. [9].A system has certain characteristics or properties, which characterize that it can be said to be a system according to sutabri, some explanations about the characteristics or properties of a system, among others :

1. Components
   The system can be said to be a set of elements or a set of sets that interact with each other to achieve the goals of a particular process. If these components cannot work together, it will cause defects in the system.[10].
2. Bondary
   Restricting other systems or with their external environment. This system boundary allows a system to be viewed as a single unit. Boundaries can also be said to be the scope of a system or subsystem.[10].
3. Environments
   The environment is a characteristic that is outside the system that can make the system beneficial or detrimental to the system.[11].
4. Interface
   The system interface in question is a means that allows each subsystem to be interconnected so that sources of information can be viewed in an orderly manner on the system.[12].
5. Input
   The input in question is everything that enters the system for processing. Input can change something that is physically visible or not on the system. The input can also be an energy signal when processing the system. [10].
6. Processing
   The processed energy signal will be classified into useful outputs. This output is useful for other subsystem inputs. A system can have a processor or the system itself as a processor. [13].
7. Output
   System output is the result of the system processing. Output can also be in the form of system components in the form of various forms of output produced, as well as the form of output produced by processing components.[10].
8. Goal
   A system must have the desired goal. If a system does not have a target, then the operation of the system is useless.[14].

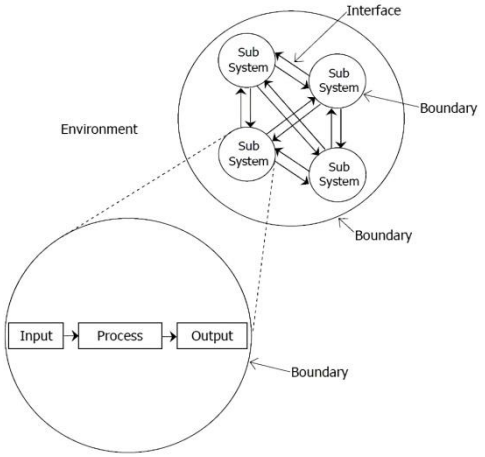

Figure 2. System Characteristics

Figure 2, describes the components of the system that are related to each other. Meanwhile, information is data that has been processed into a form that has meaning for the recipient and has real value for current or future decisions.[15].According to Jogiyanto, the quality of information is influenced by several factors, namely:

1. Accuracy
   Information is said to be accurate if there are no errors or things that make the information damaged. The information must be accurate because the data obtained are based on data collection methods in the field at the time of research.[16].
2. Timeliness
   The information provided must be timely so that the information provided is easily accepted by the community itself because the information is useful in decision making. [16].
3. Relevancy
   Information is said to be relevant if the information is useful for its users or users. [16].The accuracy of information is marked by the information presented is not misleading, misleading in the sense that it is free from errors and can explain what is meant. [17].

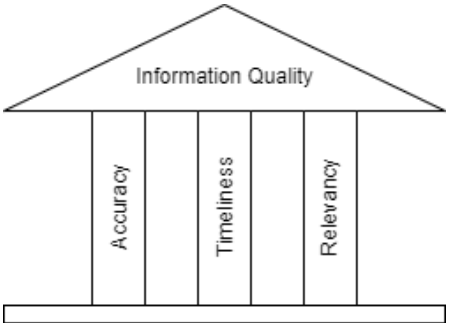

Figure 3. Information Quality

Figure 3, explains that accuracy, timeliness, and relevance are the supporting parts of the quality of information. So it can be concluded that the information system is a collection of data in a useful unit that is conveyed properly and correctly so that the recipient can receive the information properly and correctly. [18].Information quality is often used as a criterion for assessing the performance function of an information system.[19].Information quality is very important in increasing user confidence in receiving information.

1.1.3 Information System Security Concept

Computer systems have four very important security parameters, namely:

1. Physical Security
   Physical security is the main thing that is very important in protecting the system, which includes buildings, infrastructure, and other supports against threats related to the physical environment.
2. System Security
   System security includes how to further protection is carried out by users, such as users who can enter the system, and who have the right to access the system.
3. Application Security
   Application security includes how secure the application is, whether there are security holes or security vulnerabilities in the application and whether the application can be attacked or compromised by outside parties.
4. Data Security
   Data security includes how secure the data is stored, and whether the data can be accessed or retrieved by outsiders who are not responsible or not who have access to the data.

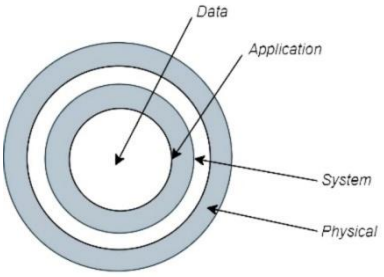

Figure 4. Information System Security Parameters

Figure 4, illustrates the importance of the components of the information system security parameters that are applied.Modification of data or theft of data resulting in loss of ownership of information systems. These components include Confidentiality, Integrity, and Availability according to Solomon and Chapple in 2009. These three components of information systems are the basis of any well-designed information system security program. The three components include:

1. Confidentiality
   The term Confidentiality generally means confidentiality according to Cole in 2005. [20].ensure that the information can be accessed by these people only guarantee the confidentiality of the data received, sent, or stored.[21].
2. Integrity
   The term Integrity in general can be interpreted as wholeness. [20]. ensure that the information is intact, accurate, and has not been modified by unauthorized parties. [22].
3. Availability
   The term Availability can be interpreted as availability according to Cole in 2005. [20]. Availability ensures timely authorization of users of the system and uninterrupted access to information from systems in a network.

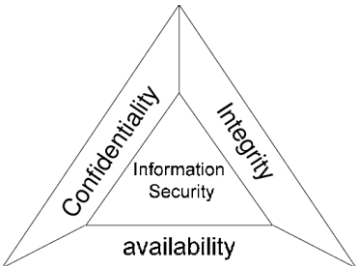

Figure 5. *The CIA Triad*

Figure 5, The three components are also known as the "CIA Triad" which is then described as a triangle as a form of information security.

1.1.4 Types of Security Threats

Security threats can occur because of the weakness of a system, therefore it is necessary to know the types of security threats in a system. The threats to computer systems are categorized into four according to Simamarta, namely:

1. Interruption, is a threat or attack that has an impact on the availability of data in a computer system that contains information that has been tampered with or deleted so that if needed it cannot be accessed again or there is no more

information displayed on the previous system because already exposed to the threat of an interrupt-type attack. [23].

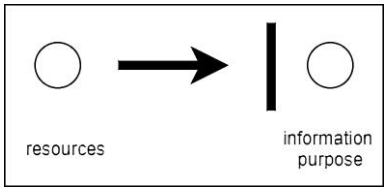

Figure6. Interruption

Figure 6, explains the type of interruption attack, where there are 2 parties involved, namely the source of information and the destination of information, related to the theory of interruption that has been described previously.

2. Interception, is a threat or attack in the form of confidentiality, so that confidential information can be known by third parties or irresponsible parties so that information is intercepted. Just as information on a computer system is intercepted by unauthorized or unauthorized persons.[23]. If a third party succeeds in obtaining access rights to read data or information from a computer system, data theft will occur on the system, so that the system experiences data loss.

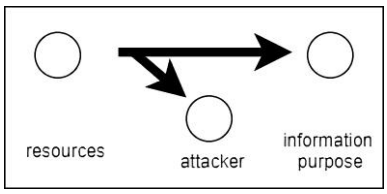

Figure7. Interception

Figure 7, explains how the type of interception attack, where there are 3 parties involved, namely the source of information, the attacker, and the destination of the information, is related to the intercept theory that has been described previously.

3. Modification, is a threat or attack in the form of integrity, which results in the authenticity of the information being manipulated by a party who is not responsible for the purpose of the information. Like a person who is not entitled to information which then intercepts information traffic and then changes the direction and destination according to the wishes of the person or attacker.[23].

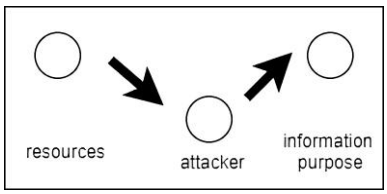

Figure8. Modification

Figure 8, explains how the type of modification attack, in which there are 3 parties involved, namely the source of information, the attacker, and the destination of the information, is related to the modification theory that has been described previously.

4. Fabrication, is a threat or attack in the form of integrity. Like people who are not entitled to information who then falsify the information with the aim that the individual who gets the data comes from the individual desired by the recipient of the data.[23].

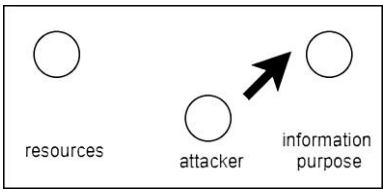

Figure9. Fabrication

Figure 9, explains how the type of fabrication attack is, where there are 3 parties involved, namely the source of information, the attacker, and the destination of the information, related to the fabrication theory that has been described previously.

1.1.5 Web Server

The web server is a service provider for the browser so that the browser can display data or pages requested by internet service users. [2].In general, the webserver has an important role in managing and being a liaison between the browser and the server when you want to process web pages that contain documents, videos, photos, or various other forms of files.

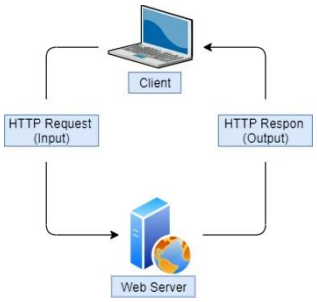

Figure10.How Web Servers Work

Figure 10, For the way it works, the client/user makes a request through the browser to the server (HTTP Request), then the server receives the request/request and processes it into a web page (HTTP Response) which will be returned to the client/user.

1.1.6 DDoS Attack

Distributed Denial of Services (DDOS) is one type of attack that exploits the web. This attack causes the server to be down and the system error. [24]. By increasing the traffic of a server so high that the server cannot handle access requests from users.

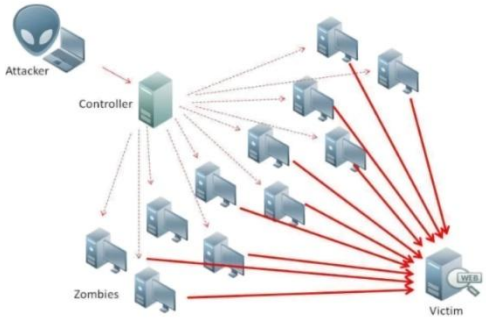

Figure11.DDoS Attack Scheme

Figure 11, shows an attacker carrying out an attack on a server, using a large number of computer bots.

1.1.7 Penetration Testing

Penetration Testing is a strategy used to test for deficiencies or vulnerabilities in networks, computer systems, or web applications. The three components of vulnerability assessment testing are based on the scope and type of audit. The three components are as follows:

1. Black Box Testing
   In this methodology, the analyst does not know the objectives to be attempted. The analyzer only finds all the framework vulnerabilities that depend on experience and skills. [4].Researchers simulate as an attacker, to audit security.
2. White Box Testing
   In this methodology, the analyzer is provided with all the total data, for example, network design, framework setup, and the analyzer plays an internal review of the security framework. Analysts re-enact this activity, eg risk representation is available within the bounds of objectives and strategies. This test requires top-down skills to improve results.[4].
3. Gray Box Testing
   This methodology combines two methodologies, namely Black Box Testing with White Box Testing. In this methodology, an analyst must know about testing an organization or framework.[4].

2. METHODOLOGY

2.1 Research Scenario

This research scheme starts from the analyst not knowing the purpose to be tried. The analyzer only finds all the vulnerabilities of the framework that depend on skills by using a checking system, so the researcher simulates himself as an attacker, to audit security in performing the simulation.

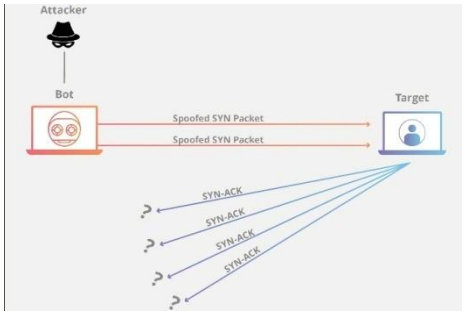

Figure12.SYN Flooding Attack

Figure 12, This attack uses an application that sends an attack to exploit the TCP protocol by sending an SYN with a spoof on a large number of IP addresses, every incoming connection will be responded to by the server waiting for the connection process to run, even though it never happens. This will result in every process that enters the server which results in an overload.

2.2 Research Stages

Information Systems Security Assessment Framework (ISSAF) is a series of activities carried out to identify and exploit security vulnerabilities in a network, system, and application. In its application, ISSAF is a penetration test method that has a clear structure. [25].an be understood, so that researchers in conducting research will be guided by the stages in the ISSAF framework.

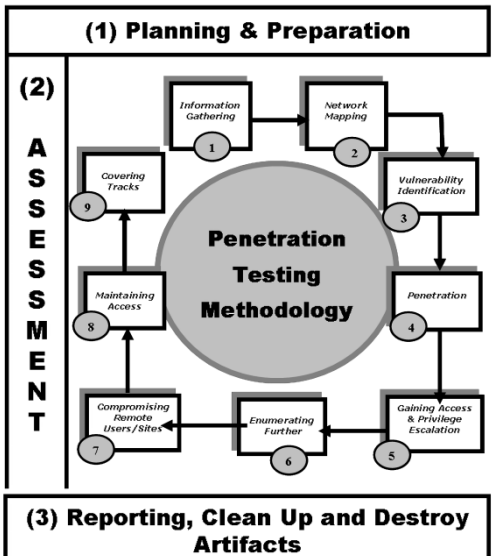

Figure13. ISSAFMethodology

Figure 13, the ISSAF method shows the stages in analyzing web server vulnerabilities in information systems, which can be described in 5 stages, namely:

1. Information Gathering
   searching for information on a web server from an information system, it can be used to collect sufficient information about the existing system in the object of research.
2. Network Mapping
   visualize the network connectivity used on the webserver object on the information system website.
3. Vulnerability Testing
   aims to determine the level of the weakness of a system, and information about the shortcomings of the system.
4. Penetration Testing
   stages of simulating attacks on a web server of an information system.
5. Analysis and Reports
   At this stage the analyst makes a brief report related to the simulation carried out on the object of research.

2.2.1 Information Gathering

On the Windows operating system using one of the whois tools can be accessed in a browser with the link https://whois.domaintools.com/.

Figure14.Whois Scan

Figure 14, the results of a scan carried out to obtain information about the web server such as the date of update and expiration, and the manager. After that, scan the SSL Scan on the https://www.ssllabs.com/ site.

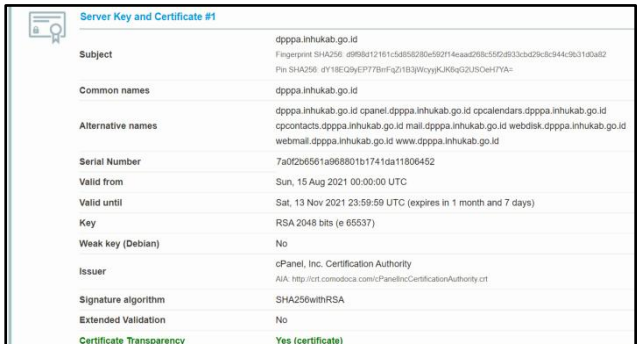

Figure15. SSL Scan

Figure 15, the results of a scan carried out to obtain information about the certificate status of the webserver.

2.2.2 Network Mapping

At this stage using the Zenmap tool on the Windows operating system by entering the IP Address of the site. then wait for the scanning process from the IP Address.

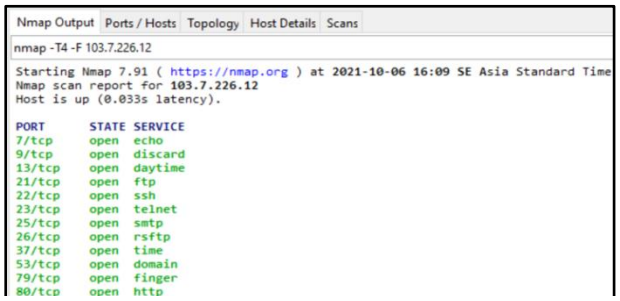

Figure16.Zenmap Scan

Figure 16, results of a scan carried out containinformation on several ports that are available and have an open status.

2.2.3 Vulnerability

This stage uses the acunetix web vulnerability tools found on the Windows operating system by entering the IP address of the site.

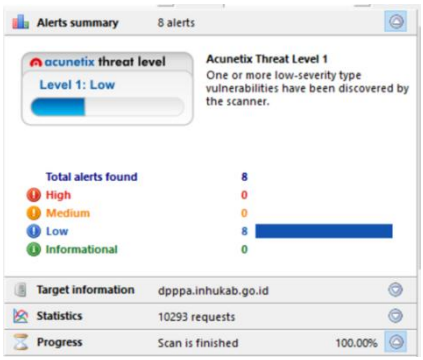

Figure17.AcunetixVulnerability Scan

Figure 17, the results of a scan that was carried out got a low score at level 1 which has several warnings. Next on the Linux terminal by typing the command to perform a vulnerability scan.

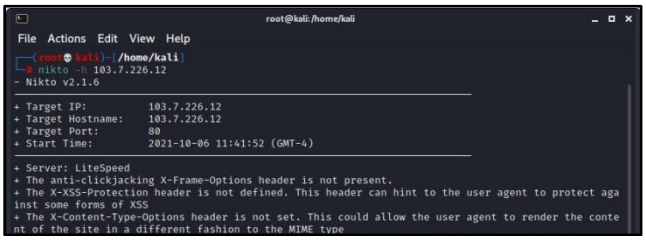

Figure18.Linux Vulnerability Scan

Figure 18, the result of a scan done on the site does not have The anti-clickjacking X-Frame-Option and The X-XSS-Protection.

2.2.4 Penetration Testing

In doing this simulation using one of the tools LOIC (Low Orbit Ion Cannon) as an application to perform attack simulations by sending attack packets.

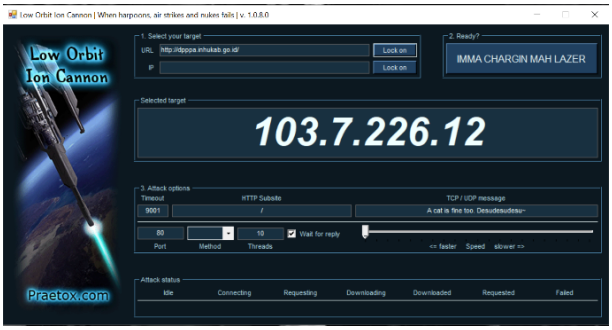

Figure19. Low Orbit Ion Cannon (LOIC)

This tool has several features in carrying out the simulation process, such as the IP Address input box, Method, and others. In addition, this simulation process requires several devices to perform testing so as to obtain some data that supports web server vulnerability analysis, as for the device requirements in Table 1 :

Table1.Device Requirements

Device Name	User	Specification		
MSI Modern 14	1	OS	:	Windows
		Model	:	Modern Series
		RAM	:	8 GB
		Version	:	Modern 14
Vivo v15	2	OS	:	Android
		Model	:	Vivo 1819
		RAM	:	6 GB
		Version	:	10

Table 1, simulation process is carried out using 2 devices that have installed LOIC (Low Orbit Ion Cannon) tools, after installing the tools for testing on the information system website and then making some settings or setting the attack process on these tools.

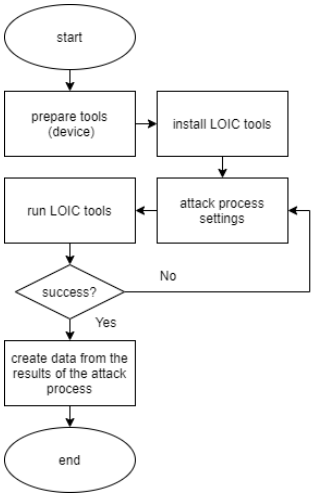

Figure20.Simulation Flowchart

Figure 20, describes the process that occurs from the beginning of the attack simulation, setting tools, and making analyses and reports from the data obtained. The object of the research is a web server from one of the local government information systems. The data obtained from user 1 testing on July 29, 2021, using the LOIC (Low Orbit Ion Cannon).

Table2.Dataset (User 1)

Device	Thread	Requested	Status
User 1	100	314670	normal
User 1	200	317074	normal
User 1	300	264145	normal
User 1	400	288405	normal
User 1	500	273318	normal
User 1	600	621582	normal
User 1	700	497109	normal
User 1	800	400481	normal
User 1	900	770239	normal
User 1	1000	1220689	normal

Table 2, using User 1 as a test device in conducting be simulations and carried out 10 experiments with a thread range of 100 to 1000. And getting normal status on 10 users 1 test data with the highest requested data amounting to 1220689. Next, simulation of web vulnerability testing the information system server was carried out with LOIC (Low Orbit Ion Cannon) tools from user 2 test data on August 1, 2021, and August 2, 2021 on Table 3.

Table3. Dataset (User 2)

Device	Thread	Requested	Status
User 2	100	41176	DDoS
User 2	200	41441	DDoS
User 2	300	42311	DDoS
User 2	400	41128	DDoS
User 2	500	42443	DDoS
User 2	600	29334	normal
User 2	700	28636	normal
User 2	800	28240	normal
User 2	900	28829	normal
User 2	1000	28338	normal

Table 3, using User 2 as a test device in conducting simulations, and carried out 10 experiments with a thread range of 100 to 1000. On August 1, 2021, the results were obtained with the highest requested DDoS and requested the status of 42443, while on August 2 2021 got results with normal status with the highest requested amounting to 29334. After receiving several attack packages from the DDoS Attack simulation that was carried out, there was an impact on the information system.

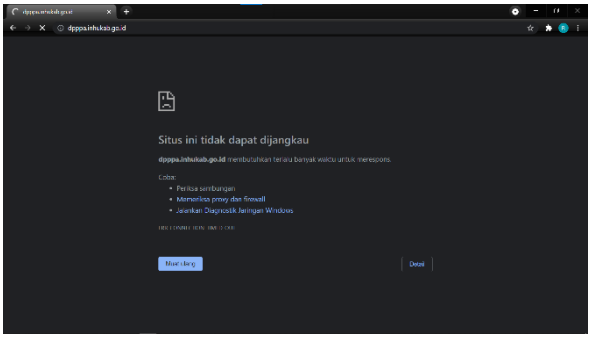

Figure21.Impact of DDoS Attack Simulation

Figure 21, resulted in the site being down / inaccessible at all and the impact of the attack lasted for several minutes.

2.2.5 Analysis and Reports

After analyzing the vulnerability of the information system web server, a summary will be made to simplify and see the overall vulnerability of the webserver through the Information Systems Security Assessment Framework (ISSAF) method.

Table4.Summary

Stage	Number of Main Information	Description of Main Information
Information Gathering	4	Web server created on July 4, 2011.
		Web server last updated on August 20, 2021.
		Web server expiration on July 6, 2022.
		Web server has a transparency certificate.
Network Mapping	2	Main protocol, port 80 on http protocol is open.
		Main protocol, port 443 on https protocol is open.
Vulnerability	3	Webserver has a low level of vulnerability and has 8 warnings.
		website does not have X - Frame-Optionsanti-clickjacking which works to detect which browsers are allowed to render website pages in frames or iframes and can also guarantee that website content is not embedded into other websites.
		In addition, the website also does not have The X – XSS – Protection which functions to configure the configuration of the cross-site-scripting

		protection filter that is already in the browser.
PENTEST (ISSAF)	3	in penetration testing experiments using device user 1 on threads 100 to 1000 with 10 attempts of sending DDoSAttack, the result is getting all normal status on the website.
		in penetration testing using device users 2 on 100 to 1000 threads with 10 attempts of sending DDoSAttack, the result got 5 tries in DDoS state and 5 tries after that in normal state on website.
		Web server is classified as safe, it is analyzed that the web server service can handle DDoS attacks well after simulating DDoS attacks.

Table 4, produces a brief description of the simulation process that has been carried out and has been analyzed based on the process that occurred over several days.

3. CONCLUSION

Information systems web server vulnerabilities can be identified using the Information Systems Security Assessment Framework methodology or method. By going through several stages of research, namely Information Gathering, Network Mapping, Vulnerability, Penetration Testing so that analysis can be carried out which is then used as a final report or summary. Vulnerability testing and analysis, the webserver of the information system website has a low level of vulnerability with 8 warnings of vulnerability information. The information system website also does not have The anti-clickjacking X-Frame-Options which functions to detect a browser is allowed to render website pages in frames or iframes and can also guarantee that the website content is not embedded into other websites other than that, the website also does not have The X – XSS – Protection which functions to configure the cross-site-scripting protection filter configuration that is already in the browser.

4. REFERENCES

[1] M. Dahlan, A. Latubessy, M. Nurkamid, "Analysis of Web Server Security Against Possible SQL Injection Attacks" Proceedings of Snatif.pp. 251–258, 2015.

[2] L. H. Yanti and B. Cut, "Analysis of Web Server Security from Remote Os Command Injection Attacks on Government Agencies of Banda Aceh City," J. Ris. and Inov. Educator., vol. 1, no. 2, pp. 92–98, 2019.

[3] Yunanri, I. Riadi, and A. Yudhana, "Analysis of Webserver Security Using Penetration Testing Method (PENTEST)," Annu. res. Semin., vol. 2, no. 1, pp. 300–304, 2016.

[4] G. Guntoro, L. Costener, and M. Musfawati, "Security Analysis of the Web Server Open Journal System (Ojs) Using the Issaf and Owasp Method (Case Study of OJS at Lancang Kuning University)," JIPI (Journal of Scientific Research and Inform Learning. , vol. 5, no. 1, p. 45, 2020, doi:10.29100/jipi.v5i1.1565.

[5] G. Ary, S. Sanjaya, G. Made, A. Sasmita, D. Made, and S. Arsa, "Evaluating the Security of Institution X's Website through Penetration Testing Using the ISSAF Framework," vol. 8, no. 2, pp. 113–124, 2020.

[6] A. F. Mohmmad Muhsin, "Application of Web Server Security Testing Using the OWASP Method version 4 (Online Exam Web Server Case Study)," vol. 151, no. 1, pp. 10–17, 2015.

[7] T. Dirgahayu, Y. Prayudi, and A. Fajaryanto, "Application of ISSAF and OWASP Method version 4 for Web Server Vulnerability Testing," J. Ilm. NERO, vol. 1, no. 3, pp. 190–197, 2015, [Online]. Available:http://nero.trunojoyo.ac.id/index.php/nero/article/download/29/27.

[8] A. Herliana and P. M. Rasyid, "Information System Monitoring Software Development in Phase," J. Inform., no. 1, pp. 41–50, 2016.

[9] M. L. Harumy, T.H.F., Julham Sitorus, "Attendance Information System at Pt . Cospar Sentosa Jaya Using Java Programming Language," J. Tek. Informatics, vol. 5, no. 1, pp. 63–70, 2018.

[10] O. Fajarianto, M. Iqbal, and J. T. Cahya, "Decision Support System for Recruitment Selection Using the Weighted Product Method," J. Sisfotek Glob., vol. 7, no. 1, pp. 49–55, 2017.

[11] P. E. S. and L. S. Sudjiman, "COMPUTER BASED MANAGEMENT INFORMATION SYSTEM Paul Eduard Sudjiman and Lorina Siregar Sudjiman, "COMPUTER BASED MANAGEMENT INFORMATION SYSTEM," J. TeIKA, vol. 8, pp. 55–67, 2018.

[12] M. D. Irawan and L. Hasni, "Employee Payroll System at Lkp Grace Education Center," JurTI (Journal of Teknol. INFORMASI), vol. 1, no. 2, pp. 125–136, 2018, doi:10.31227/osf.io/bupme.

[13] A. Setiawan and AI Purnamasari, "Development of Smart Homes With ESP32 Microcontrollers and MC-38 Door Magnetic Switch Sensors Based on Internet of Things (IoT) To Improve Early Detection of Residential Security," J. RESTI (System Engineering and Information Technology), vol. 3, no. 3, pp. 451–457, 2019, doi:10.29207/resti.v3i3.1238.

[14] AA Permana, "Design of a Savings and Loan Information System for Teachers and Employees Cooperatives at SMP Negeri 45 Jakarta," JIKA (Jurnal Inform., vol. 1, no. 2, pp. 79–87, 2017, doi: 10.31000/jika.v1i2. 1400.

[15] I. K. Rachmawati, Y. Handoko, F. Nuryanti, M. Wulan, and S. Hidayatullah, "The influence of convenience, customer trust and information quality on online purchasing decisions," Semin. Nas. Sis. inf. 2019, vol. 3, no. September, pp. 1617–1625, 2019.

[16] O. A. Ruslinda Agustina, Rara Gustina, "Accounting at Pt Indomarco Prismatama Branch," vol. 14, no. 1, 2021.

[17] S. Romla and A. Ratnawati, "E-Commerce Purchase Decisions Through Ease of Use, Quality of Information and Quality of Web Service Interaction," J. Ekon. and Business, vol. 19, no. 1, p. 59, 2018, doi:10.30659/ekobis.19.1.59-70.

[18] H. M. Jumasa, "Design and Build a Mobile-Based

Digital Library (Case Study: University of Muhammadiyah Purworejo)," INTEK J. Inform. and Technol. Inf., vol. 2, no. 1, pp. 32–38, 2019, doi:10.37729/intek.v2i1.87.

[19] Y. Krisdiantoro, I. Subekti, and Y. W. Prihatiningtias, "The Effect of System Quality and Information Quality on Net Benefits with Intensity of Use as a Mediation Variable," J. Akunt. Actual, vol. 5, no. 2, pp. 149–167, 2018, doi:10.17977/um004v5i22018p149.

[20] A. Nur, "Analysis and Testing of Library Information System Vulnerabilities," J. Mandiri, vol. 3, no. 1, pp. 99–115, 2019.

[21] H.Maulana.J.S., Bestin.S.S, Renaldi.J.A, and T. F.P.F, "Iso 17799 Policies on Organizations as Management of Information Security Systems," Angew. Chemie Int. Ed. 6(11), 951–952., vols. 3, no. 2, pp. 67–74, 1967.

[22] M. Ridwan, Z. Arifin, and Y. Yulianto, "Design of E-Voting Using Web-Based Rivest Shamir Adleman (RSA) Algorithm Security (Case Study: Election of Chairperson of Bem Fmipa)," Inform. Mulawarman J. Ilm. Computing Science., vol. 11, no. 2, p. 22, 2016, doi:10.30872/jim.v11i2.210.

[23] M. Aritonang, "Designing Security Applications to Restrict Access Rights," vol. 2, no. 1, pp. 108–111, 2016.

[24] N. Sugianti, Y. Galuh, S. Fatia, and K. F. H. Holle, "Detection of HTTP-Based Distributed Denia of Services (DDOS) Attacks Using the Fuzzy Sugeno Method," JISKA (Jurnal Inform. Sunan Kalijaga), vol. 4, no. 3, p. 18, 2020, doi:10.14421/jiska.2020.43-03.

[25] R. H. Hutagalung, L. E. Nugroho, and R. Hidayat, "Analysis of Penetration Tests Using ISSAF," Hacking Digits. Forensics Expo., pp. 32–40, 2017.