Circuit: Jurnal Ilmiah Pendidikan Teknik Elektro
Volume 8 No. 1 September 2023 - February 2024
ISSN: 2549-3698; E-ISSN: 2549-3701
DOI: 10.22373/crc.v8i1.20808

Analysis Server Security Assessment of Staffing Management Information System Using the NIST SP 800-115 Method at UIN Ar-Raniry Banda Aceh

Irfan Murti Raazi[a], Malahayati[a], Basrul[b], Rezqi Malia[c], Mulkan Fadhli[a]
[a]Universitas Islam Negeri Ar-Raniry Banda Aceh
[b]Institut Agama Islam Negeri Lhokseumawe
[c]Universitas Teuku Umar

E-mail: irfanmurtiraazi@gmail.com

Submitted: 24-11-2023 Accepted:13-01-2024 Published:01-02-2024

Abstract

Ar-Raniry State Islamic University management information system has been implemented based on technology. It becomes vulnerable to attacks brought on by weaknesses (vulnerabilities). The degree to which institutions are able to improve their access to authority inside the system is gauged by this research. To evaluate the server's dependability based on confidentiality, integrity, and availability, penetration testing is necessary. The NIST SP 800-115 approach, which comprises of four testing stages—planning, discovery, attack, and reporting—is used to conduct the server security assessment. The findings demonstrate the Security Management Information System contains nine vulnerabilities in various ways with varying improvements. Two of these vulnerabilities are classified as high threat: DNS Server Spoofed Request Amplification DDoS by blocking access from the public network or rejecting the query; and Interception Attack by enhancing the SSL/TLS protocol through a stunnel. The remaining seven vulnerabilities are classified as medium threat. However, Ar-Raniry's campus server vulnerability level is categorized as medium threat.

Keywords*: Penetration Testing*, NIST SP 800-115, *Server Security*

Abstrak

Universitas Islam Negeri Ar-Raniry Banda Aceh telah memanfaatkan Sistem Informasi Manajemen Kepegawaian berbasis teknologi. Hal ini rawan terjadinya serangan yang disebabkan oleh kerentanan (*vulnerability*). Penelitian ini menjadi tolak ukur sejauhmana institusi mampu melakukan perbaikan terhadap dalam memperoleh akses kewenangan dalam system. Perlu dilakukan penetration testing untuk menilai kelayakan server berdasarkan aspek; *confidentiality, integrity,* dan *availability*. Penilaian keamanan server dilakukan dengan metode NIST SP 800-115 yang terdiri dari 4 tahapan pengujian; *planning, discovery, attack,* dan *reporting.* Hasil dari penelitian ini menunjukkan bahwa Sistem informasi Manajemen Kepegawaian memiliki 9 kerentanan yang dapat dieksploitasi dengan cara perbaikan yang berbeda-beda dengan rincian 2 kerentanan yang berada dalam *threat level high* yaitu: *DNS Server Spoofed Request Amplification DDoS* dengan membatasi akses dari jaringan publik/kofigurasi ulang menolak *query* tersebut, dan *Interception Attack* dengan perbaikan protokol SSL/TLS mengunakan stunnel, serta tujuh kerentanan dalam *threat level medium.* Dapat disimpulkan, tingkat keparahan kerentanan server UIN Ar-Raniry berada pada *threat level medium*.

Kata kunci: *Uji Penetrasi, NIST SP 800-115, Keamanan Server*

Introduction

In the era of increasingly advanced and widely developing technology as it is today, the intensity of using computer technology is an inseparable part of human life [1]. Therefore, the ability and curiosity of humans in using digital technology is also increasing. However, in line with the development of information technology, there are also various types of cybercrime, relating to network security system issues, and information as an asset in implementing network security reliability. Information is the most important part of an institution/organization information system. This begins with the reliability of network security to maintain the validity and integrity of data and ensure the availability of services for users [2]. In order to stop reckless parties from consistently using threat and attack tactics to accomplish their objectives.

There are various facets of information security that need to be recognized and safeguarded. Information security features include availability, integrity, and secrecy [3]. System security is therefore a primary concern for any institution or business in order to prevent several forms of attack methods and information theft, including server system hacking. Based on information from the news portal British Broadcasting Corporation (BBC) stated that cybercrime in 2020 has occurred cyberattacks that attacked the University of California, San Francisco on June 1, 2020. Anonymous hackers who carried out ransomware cyberattacks on university servers and found data from the Faculty of Medicine regarding Covid-19 research. The hackers asked for a ransom of US $ 3 million to provide a decryption key, because the hackers succeeded in encrypting seven servers owned by the university so that the university negotiated a breakdown of US $ 1.14 million [4].

This instance demonstrates how crucial data sets are gathered on institutional or corporate servers, making them vulnerable to attacks and unauthorized access by third parties. Therefore, it is necessary to protect information by applying a structured approach to avoid the risks that may arise. Because cybercrime can happen anywhere and at any time, especially at colleges where the security system is disregarded and the level of security is deemed secure, a system security analysis was chosen. In this instance, preventing server system hacking will be achieved by patching the system's vulnerabilities. But prior to patching a vulnerability, an evaluation of the server's current security is necessary.

Based on the description above, researchers took the initiative to conduct server security assessment research on the Staffing Management Information System on the Ar-Raniry State Islamic University server in order to determine the level of vulnerability to university server security and help minimize crime. As for one of the activities carried out by scanning the target vulnerability and conducting penetration testing using the National Institute of Standards and Technology (NIST SP 800-115) method with a case study at Ar-Raniry State Islamic University as the target in conducting an analysis of server security assessments. Open ports and services that are operating on them are used for this test.

The NIST SP 800-115 method was selected as a step in the security assessment process of a server because it offers suggestions for vulnerabilities and contains tools and procedures that are simple to understand and apply in the security testing process. The assessment in this method uses the Common Vulnerability Scoring System (CVSS) which is easy for users to understand even if they are not experienced in the field of penetration testing.

Method

The research methodology employed in this study is literature study, which is the examination of research objects in the form of literary works, including theses, books, journals, websites, and papers that serve as primary sources. However, system penetration testing is done using a qualitative descriptive method for this reason. NIST SP 800-115 black box testing was used to conduct this test on the Staffing Management Information System. NIST SP 800-115 is a guide published in 2008 by the National Institute of Standards and Technology (NIST) which was established in 1901 and is now part of the United States Department of Commerce. NIST has issued several series of publications, one of which is NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, a method issued specifically to assist organizations in determining how effective an entity is to be assessed in meeting security objectives and providing recommendations in dealing with security issues [5].

In order to determine the constraints in the scope of the test techniques and targets, the institution or organization conducting penetration testing of a system must obtain authorization from the owner of the object. One of the techniques used is black box testing. Black box testing is a testing activity carried out to find out the external workings of a system [6]. It was important to gather information using search engines and other tools in order to assess and identify the sort of exploitation because the test simply looked at the interface and functionality, and the tester was only given the test target's IP address. The research data was taken from the results of testing on utilities and tools when carrying out testing activities for Staffing Management Information Systems. The results obtained have different conditions and impacts.

The purpose of this test is to identify system vulnerabilities and offer suggestions for mitigating those shortcomings. Furthermore, NIST SP 800-115 offers a penetration testing methodology that will be applied in this investigation. It begins with planning, then divides discovery into two parts: information collection and vulnerability scanning. Next comes attack, reporting test results, and suggestions for improvement. The picture of the research flow can be seen in Figure 1.

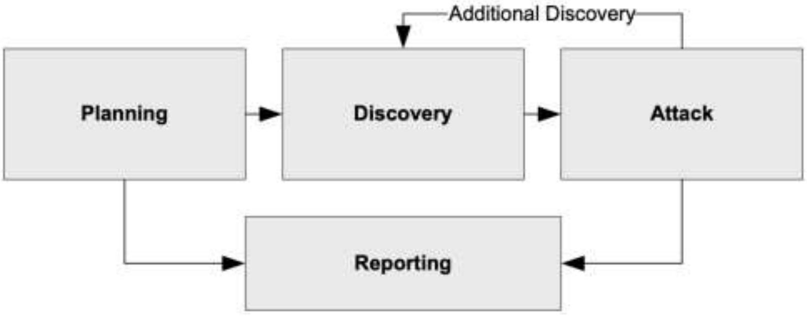


Figure 1. Research Flow

a. Planning

At this point, planning is done by figuring out the purpose, scope, and aim of the testing. In this instance, the university server hosts the Staffing Management Information System, which is the test's target. In order to give researchers information specific to the information system domain, this test employs the black box testing technique.

b. Discovery

At this stage using utilities and tools to gather information about the system. To determine the condition of information system, packets are sent using ping, if the packet is received, it is known that the host is active and can be connected. Next, utilize who is to obtain domain details and personal data about the domain registrant. Additionally, SSLScan offers a color-coded list of flaws and vulnerabilities that may be used to view services on Secure Sockets Layer (SSL)/Transport Layer Security (TLS) servers. Information gathering uses several tools to find vulnerabilities in information systems. NMAP is used for exploration in identifying the port of a host with open, filtered, and closed status. If the port is open and without authentication one way for hackers to access the system. Wireshark is used to analyze packets passing through data traffic. When doing a vulnerability scan to find weaknesses on the test target, Nessus is utilized. Because it can go back to the first stage in order to plan for new findings made throughout the testing process, the discovery stage provides flexibility.

c. Attack

At this stage it is part of the NIST SP 800-115 method for testing the information system contained on the Ar-Raniry State Islamic University server to carry out attacks that have been collected at the discovery stage. This stage's goal is to demonstrate how serious a threat a vulnerability hole poses to the system in the event that it is exploited.

d. Reporting

Data pertaining to the test's summary results will be shown at this last stage. At this point, reports are being created utilizing tables to compile the findings from each procedure so that conclusions can be made.

Result and Discussion

The results and discussion in this study include a discussion of the results of the black box testing technique using the NIST SP 800-115 method. The stages used are planning, discovery, attack, and reporting.

a. Planning

This stage is to determine the planning and preparation for penetration testing in accordance with the NIST SP 800-115 method. This includes:

1. Approval of case testing with the black box testing technique in carrying out penetration testing;
2. The test target is a server that contains the Staffing Management Information System.
3. Tests were carried out on the Kali Linux operating system using the tools ping, wireshark, nmap, sslscan, nessus and metasploit framework in the initial

planning. However, you can adjust other tools according to the research needs of obtaining vulnerabilities.

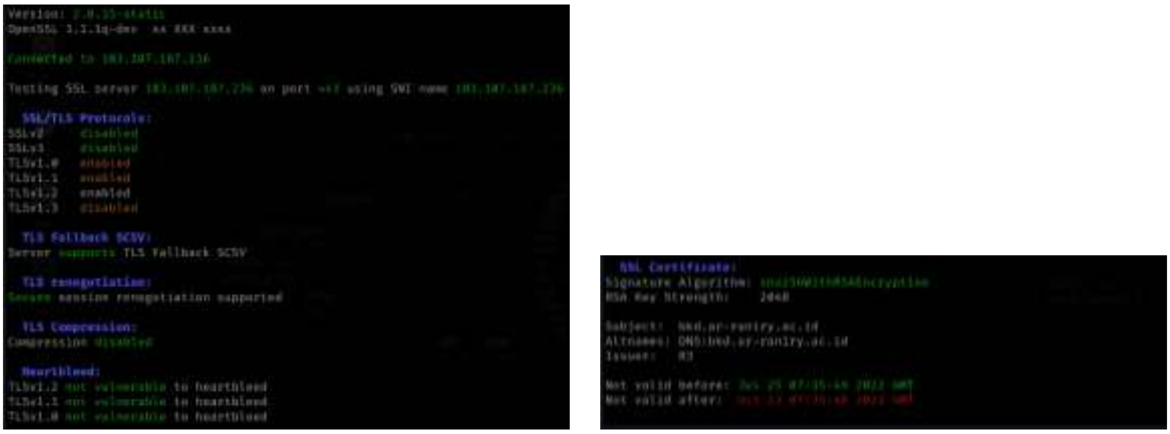
4. The data provided to researchers is only in the form of a Domain Name System (DNS).
5. Submission of report results to Information and Communication Technology (ICT) Center staff.

b. Discovery

Following the completion of the planning stage in accordance with the established protocols, the discovery stage can begin. In this instance, data collection and vulnerability screening on the information system under test will take place during the Discovery step. Tools are therefore needed to gather data regarding the test target for the black box testing technique. Information gathering is gathering information about targets to be tested using ping, whois, and SSLScan tools to find out public information. Information is collected by using tools in the form of hostnames, domain databases, locations, and the security protocols used.

Packet Internet Network Groper (PING) is a command that is used to view a host that is active on the internet network. This is indicated by the status of the packet sent by the client to the server and gets the response sent back, so it can be stated that the host is active [7]. The ping test is carried out 3 times to find out whether the ping test at different times has changed the IP address. From the test results there is no change in the ping period of 2 hours, you will still get the IP address 103.xx.xx 236. Furthermore, whois is used to find information related to the Domain Names System (DNS) of the target IP address. Whois is a database containing user information that has registered in an internet source such as local Indonesian domain names .id, co.id or international domain names such as .com, .net and .org. The information presented is easy to understand, namely domain names, IP addresses and other information [8]. In this case, the use of the whois tool is carried out second after using the ping tool to find the IP address first, from the test results obtained in the form of domain registrant personal data such as the name luthfi; Contact: +62-651-53769; Email: luthfi@ar-raniry.ac.id; and block IP Address: 103.xx.xx.0 – 103.xx.xx.255.

The next process will perform an SSL/TLS security protocol scan on the web server. This scan uses the SSLScan tool to detect security protocols communicating over the internet. SSLScan is a command-line tool that performs security assessments by querying the services received by SSL/TLS servers with the aim of providing a color-coded list of vulnerabilities [9]. It is as shown in Figure 2 that TLSv1.3 status is disabled. SSL and its successor TLS is a protocol for securing communications on the internet. In this case, the web server has implemented Hypertext Transfer Protocol Secure (HTTPS) but is still using protocol versions 1.0 and 1.1. In order to secure data on the internet, it is necessary to replace it with the most recent version by disabling TLSv1.0 and TLSv1.1 and activating the newer TLSv1.3, as shown by the orange hue that is detected. Next, it was discovered that a DNS server needed to purchase or renew a new SSL certificate due to its expiration.



```
Version: 2.0.15-static
OpenSSL 1.1.1q-dev  xx XXX xxxx

Connected to 103.107.187.236

Testing SSL server 103.107.187.236 on port 443 using SNI name 103.107.187.236

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   disabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed
```

```
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  bkd.ar-raniry.ac.id
Altnames: DNS:bkd.ar-raniry.ac.id
Issuer:   R3

Not valid before: Jul 25 07:35:46 2022 GMT
Not valid after:  Oct 23 07:35:45 2022 GMT
```

Figure 2. SSLScan Results

Vulnerability scanning performs vulnerability scanning on test targets to see whether the target has vulnerabilities or not and how severe the vulnerabilities the target has. Vulnerability search starts from port scanning with NMAP, Nessus, and Wireshark tools. In the early stages, port scanning is carried out on the test target using Network Mapping (NMAP) to find out whether there are open ports on the test target. NMAP is an open source tool for exploring and auditing network security in identifying the port of a host [10]. The initial port scanning was carried out on Transmission Control Protocol (TCP) ports where ports other than HTTP and HTTPS were found, therefore it is necessary to do a scan to find out the correct state of the open port. This is done by a User Datagram Protocol (UDP) scan that can determine the state of the port. Thus, all NMAP scan results managed to find several open ports in the test targets which are summarized in Table 1.

Table 1. Ports Scanning Results

No	Port	Protocol	Service
1	22	TCP	SSH
2	80	TCP	HTTP
3	443	TCP	HTTPS
4	2000	TCP	Cisco-SCCP
5	5060	TCP	SIP
6	8008	TCP	HTTP
7	53	UDP	Domain

The next process is scanning the vulnerability of the test target using nessus. Nessus is one of the tools used to evaluate the network and services of a system. This tool has several functions that can be used, namely vulnerability scanning, configuration editing, and others [11]. In this case, the Nessus tool will analyze the protocols available on the network and then carry out tests to find security holes in a system. Testing is carried out automatically to obtain vulnerabilities by scanning 12 times against the target IP address 103.xx.xx.236. Thus, the network and response will determine how long testing takes. The vulnerabilities are detailed in the findings of the Nessus scan, as seen in Figure 3.

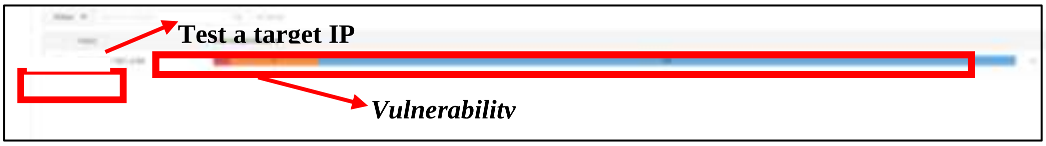


Figure 3. Vulnerability Scanning Nessus

A vulnerability has been identified based on the findings of Nessus's scanning, and each threat level's color description is indicated on the vulnerability icon. High threat levels are indicated by red, medium by orange, and none by blue. In order to make data processing easier, the vulnerability information is gathered and processed in a table. Based on threat level, the vulnerability data from scan findings is displayed in Table 2.

Table 2. Nessus Vulnerability Results

No	Vulnerability	Threat Level	Analysis
1	DNS Server Spoofed Request Amplification DDoS	High	This vulnerability will respond to requests from remote DNS Servers by utilizing amplification to carry out Distributed Denial of Service (DDoS) attacks.
2	TLS Version 1.0 Protocol Detection	Medium	Detected still using the old version of the TLS protocol (1.0) in encrypting data traffic
3	TLS Version 1.1 Protocol Detection	Medium	Detected still using the old version of the TLS protocol (1.1) in encrypting data traffic.
4	SSL Certificate Cannot Be Trusted	Medium	This vulnerability was obtained due to the remote host's SSL certificate chain not being trusted from DNS acd.ar-raniry.ac.id.
5	SSL Certificate Expiry	Medium	Vulnerability of remote host's SSL certificate has expired from DNS acd.ar-raniry.ac.id.
6	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure	Medium	A vulnerability that allows obtaining sensitive information from remote SSL/TLS hosts contained in TLS 1.0 on servers. It is vulnerable to Browser Exploit Against SSL/TLS (BEAST).
7	Nginx < 1.17.7 Information Disclosure	Medium	The web server that is used now is the old version, namely 1.14.2. It is vulnerable to easy disclosure of information.
8	DNS Server Recursive Query Cache Poisoning Weakness	Medium	The vulnerability allowed recursive query name servers so that third parties could query Name Servers (NS) using spoofed addresses into the DNS.

Next, execute network packet sniffing using the Wireshark utility. An application called Wireshark is used to examine data packets found in network traffic [12]. In this experiment, the tester will perform sniffing to obtain important information from monitoring and analyzing packets passing on the network. In this case, the level of security can also be seen from the communication process between the client and the web server on the network. The following shows the HTTP protocol data packet containing POST info.

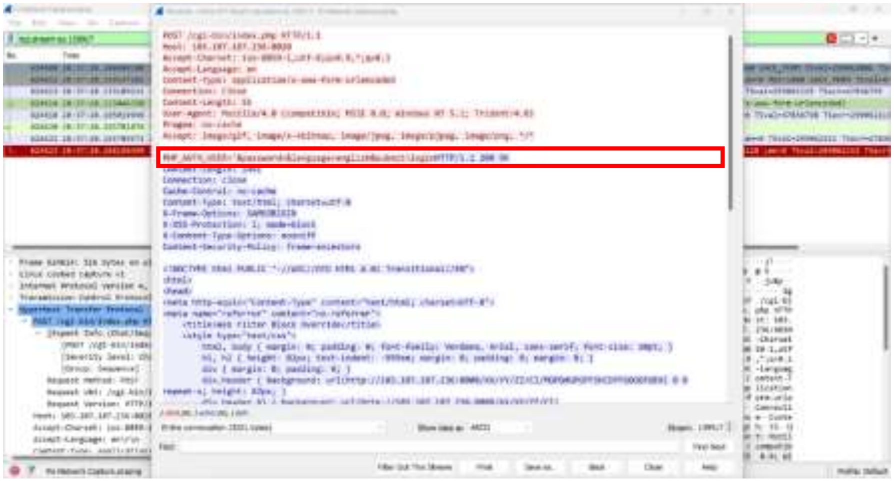


Figure 4. POST Data Package Results

Figure 4 shows the details of the HTTP protocol data packet with the red text part of the request while the blue text is part of the response. The POST data package gets key information PHP_AUTH_USER = & password = & language = english&submit=login dari form url encoded.

c. Attack

This stage is the core stage in this research which is contained in the NIST SP 800-115 method to carry out penetration testing of the findings obtained from the discovery stage. The vulnerabilities that were tested as follows:

1. Brute Force Attack

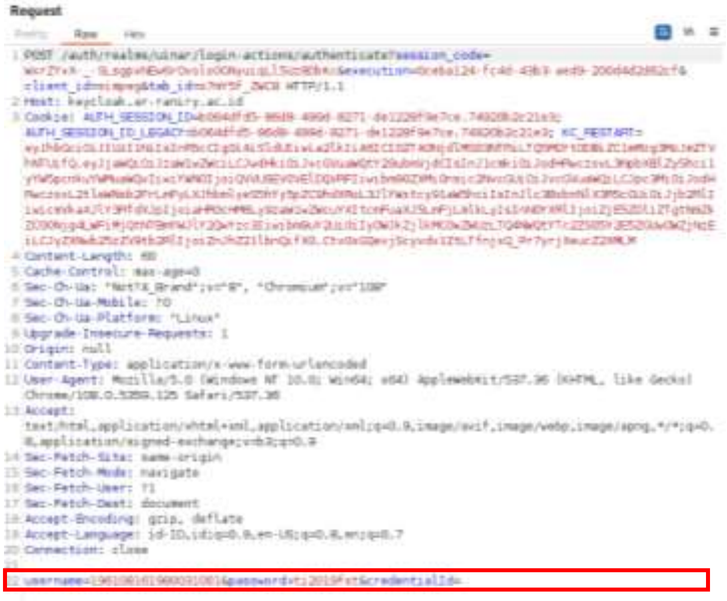
   From NMAP port scanning, there is an SSH service running on port 22 so that it will brute force login to the server via the SSH service which makes it possible to carry out attacks and obtain more accurate information on the target system. This attack uses the hydra tool to look up the username and password on the SSH server. The search results show 0 valid passwords found, which means you don't get valid results. Thus, testing the brute force login on SSH is not vulnerable.

2. DNS Server Request Amplification

   The DNS amplification exploit is part of a Distributed Denial of Service (DDoS) attack on a DNS server by turning small queries into larger payloads to bring the server down. This test uses the Metasploit Framework as a DNS amplification attack. The results of DNS amplification can be seen by sending requests with a data packet length of 64 bytes to the test target, then the server responds with a data packet length of 8.75x Amplification, which is 534 bytes.

3. Interception Attack

   From the results of Wireshark sniffing and the use of the old version of the SSL/TLS communication security protocol, it is suspected that there is an information leak in the encoded url form which has obtained a key and no sensitive information is found, also known as Cleartext Logins Permitted. In this case, testing was carried out using the BurpSuite tool as an intercept experiment. Interception is a threat to confidentiality obtained illegally to access information from a computer system [13]. The attack is carried out to find out if there is communication that is not properly encrypted by SSL/TLS, causing information leakage problems.



```
POST /auth/realms/uinar/login-actions/authenticate?session_code=
[illegible]&execution=[illegible]&
client_id=simpeg&tab_id=[illegible] HTTP/1.1
Host: keycloak.ar-raniry.ac.id
Cookie: AUTH_SESSION_ID=[illegible];
AUTH_SESSION_ID_LEGACY=[illegible]; KC_RESTART=
[illegible]
Content-Length: [illegible]
Cache-Control: max-age=0
Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

username=[illegible]&password=[illegible]&credentialId=
```

Figure 5. Interception Attack

In Figure 5 it can be seen that the exploitation results occur in the login request process into the system which shows sensitive information in the form of usernames and passwords when the login request process is not encrypted. Thus, it is very easy for an attacker to explore when he gets information in the form of a username and password.

4. Denial of Service SynFlood

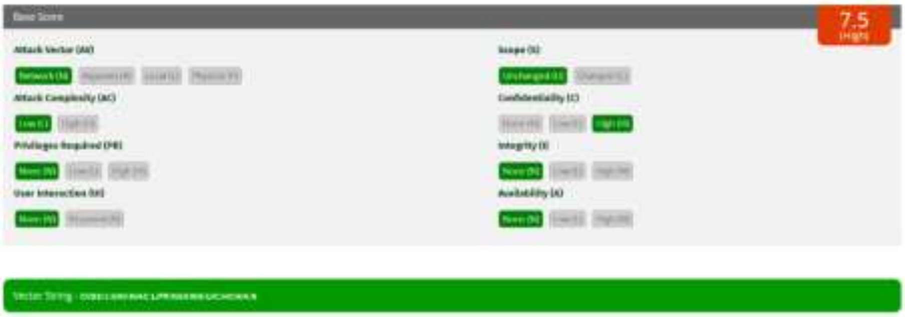
   Denial of Service (DoS) exploit by implementing SynFlood DoS exploit. SynFlood DoS is an attack on a network that will be flooded with a lot of fake traffic on the server which causes the system to down and not operate properly [14]. This test uses the metasploit framework and wireshark tools to analyze network traffic details during the SynFlood DoS exploitation process. Thus, the DoS effect can be known to be almost impossible to access by users with continuously sent traffic that keeps the system busy. Exploitation that occurs in TCP by sending SYN packets and spoof IP addresses so that incoming connections are responded to by the server, but the connection never runs.

5. Common Vulnerability Scoring System (CVSS)

   Tests that have been performed on the target 103.xx.xx.236 will be represented using the Common Vulnerability Scoring System (CVSS). CVSS is an activity to describe the characteristics and severity of a system's vulnerabilities in covering the main technical characteristics of software, hardware, and firmware. Vulnerability characteristics are obtained by a numerical score that reflects the severity of vulnerability [15]. CVSS falls under the Forum of Incident Response and Security Teams (FIRST) with the aim of responding more effectively to security incidents. Based on the vulnerability rating, the CVSS score can be seen in Table 3.

Table 3. CVSS Score

No	Threat Level	CVSS Score
1	None	0.0
2	Low	0.1 – 3.9
3	Medium	4.0 – 6.9
4	High	7.0 - 8.9
5	Critical	9.0 – 10.0



Base Score 7.5 (High)

Attack Vector (AV)
[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)
[✓ Low (L)] High (H)

Privileges Required (PR)
[✓ None (N)] Low (L) High (H)

User Interaction (UI)
[✓ None (N)] Required (R)

Scope (S)
[✓ Unchanged (U)] Changed (C)

Confidentiality (C)
None (N) Low (L) [✓ High (H)]

Integrity (I)
[✓ None (N)] Low (L) High (H)

Availability (A)
[✓ None (N)] Low (L) High (H)

Vector String - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Figure 6. Results of Interception Attack Analysis via CVSS

In the Interception attack analysis results through the Common Vulnerability Scoring System (CVSS) which obtains a high threat level with a base score of 7.5. In this case, because the Attack Vector shows techniques in exploiting vulnerabilities, in the vulnerability assessment it will be seen how far the attacker's ability to enter the system indicates Network (N) can easily attack systems through the network, but it will be different if the metrics value indicates Adjacent (A) with a base score of 6.5 which is included in the threat level medium, likewise if the metrics value indicates Local (L) with a base score of 6.2 which is included in the threat level medium and the metrics value Physical (P) obtains a base score of 4.6 which means a threat level is medium.

Attack Complexity (AC), which shows Low (L), which lacks particular attack circumstances when the attack gains easy access to the system, is another criterion that influences the degree of susceptibility. Accordingly, the lower the required complexity, the higher the vulnerability base score. Additionally, the Privileges Required (PR) measure the amount of privilege or access value that an attacker must possess in order to successfully exploit the vulnerabilities in the system. In the User Interaction component of the user requirements assessment if it indicates the metrics value None (N) which means it can be exploited without requiring other user interaction, this if it indicates the metrics value Required (R) is included in a stronger security level because the attacker or other users are related to vulnerable component. Thus, the level of vulnerability will be higher when there is no other user interaction. Next, the impact of changes in vulnerabilities will be affected by the Scope (S) parameter. If the metrics value is Unchanged (U), then changes in vulnerable components have no effect on security coverage; on the other hand, if the metrics value is Changed (C), then the level of vulnerability is very vulnerable to changes made by attackers.

The impact of exploitation of vulnerable components can occur in the form of confidentiality, integrity, and availability which greatly affect the level of vulnerability because it indicates a metrics value of None (N), which means that attacks carried out by attackers do not affect the impact of information security aspects so that it indicates that it does not have a vulnerable component, but if indicates a metrics value Low (L) with a base score of 5.3 which is included in the threat level medium and a metrics value High (H) obtains a base score of 7.5 which means a threat level is high.

d. Reporting

The final stage of this study analyzes the results of the identified vulnerabilities. In addition to analyzing the results, it also provides recommendations on how to overcome the weaknesses found. However, to make it easier to see all the findings of vulnerabilities resulting from failures in confidentiality, integrity and availability, can be seen in the Table 4, Table 5, dan Table 6.

Table 4. Confidentiality Failure Test Results

No	Vulnerability	Recommendation	Base Score	Threat Level
1	Interception Attack	Fixed traffic encryption with SSL/TLS using stunnel.	7.5	High
2	SSL Certificate Cannot Be Trusted	Update SSL certificate.	6.5	Medium
3	TLS Version 1.0 Protocol Detection	Disable TLS 1.0 by enabling TLS 1.2 and 1.3.	6.5	Medium
4	TLS Version 1.1 Protocol Detection	Disable TLS 1.1 by enabling TLS 1.2 and 1.3	6.5	Medium
5	Nginx < 1.17.7 Information Disclosure	Updated nginx server to version 1.17.7	5.3	Medium
6	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure	The SSL/TLS server configuration only uses TLS 1.2 and 1.3	5.3	Medium
	Average Vulnerability Score		6.3	Medium

Table 5. Integrity Failure Test Result

No	Vulnerability	Recommendation	Base Score	Threat Level
1	DNS Server Recursive Query Cache Poisoning Weakness	Limit recursive queries to hosts using name servers by grouping internal addresses.	5.3	Medium
2	SSL Certificate Expiry	Update SSL certificate.	5.3	Medium
	Average Vulnerability Score		5.3	Medium

Table 6. Availability Failure Test Results

No	Vulnerability	Recommendation	Base Score	Threat Level
1	DNS Server Spoofed Request Amplification DDoS	Restrict DNS server access from public networks or reconfigure to deny the query.	7.5	High

The Staffing Management Information System at Ar-Raniry State Islamic University has a vulnerability severity level of 6.4, which is categorized as a medium threat level. This figure is derived from the average base score of the results of vulnerability testing caused by failures in confidentiality, integrity, and availability.

Conclusion

Based on the results of the server security assessment of the staffing management information system using the NIST SP 800-115 method, this study produced 9 exploitable vulnerabilities with details of 2 vulnerabilities in high threat level and 7 vulnerabilities in medium threat level. As a result, the information system is categorized as a medium threat category with a vulnerability severity rating of 6.4. By incorporating the threat hunting life cycle technique, future research can undertake proactive security investigations. Related institutions can then conduct the security evaluation process, guided by the publication of NIST 800-44 on public web server security.

References

[1] T. Astriani, A. Budiyono, A. Widjajarto, J. S. Informasi, F. Rekayasa, and I. Universitas, “Analisa Kerentanan Pada Vulnerable Docker Menggunakan Scanner Openvas Dan Docker Scan Dengan Acuan Standar NIST 800-115,” *J. Tek. Inform. dan Sist. Inf.*, vol. 8, no. 4, pp. 2041–2050, 2021.

[2] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, “Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF,” *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 8, no. 2, p. 113, 2020, doi: 10.24843/jim.2020.v08.i02.p05.

[3] T. Rochmadi and I. Y. Pasa, “Menggunakan Indeks Keamanan Informasi Di Bkd Xyz Measurement of Risk and Evaluation of Information Security Using the Information Security Index in Bkd Xyz Based on Iso 27001 / Sni,” vol. 4, no. 1, pp. 38–43, 2021.

[4] Tidy J, “How hackers extorted $1.14m from University of California, San Francisco,” 2020. https://www.bbc.com/news/technology-53214783 (accessed Aug. 25, 2022).

[5] N. J. Van den Hout, “Standardised Penetration Testing Examining the Usefulness of Current Penetration Testing Methodologies,” no. August, p. 70, 2019.

[6] M. F. Setiawan, R. R. Saedudin, and ..., “Penutupan Celah Keamanan Menggunakan Metode Hardening Studi Kasus: Cloudfri Closing Security Vocations Using The Hardening Method Case Study: Cloudfri,” *e-Proceeding Eng.*, vol. 9, no. 2, pp. 656–663, 2022, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/17635%0Ahttps://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/17635/17379

[7] Ratna Patria, “Memahami Apa Itu Ping dan Fungsinya Saat Jaringan Internet Lambat - DomaiNesia,” Jun. 15, 2022. https://www.domainesia.com/berita/ping-adalah/ (accessed Dec. 25, 2022).

[8] M. Z. Hussain, M. Z. Hasan, M. Taimoor, and A. Chughtai, “Penetration Testing In System Administration,” *Int. J. Sci. Technol. Res.*, vol. 6, no. 6, pp. 275–278, 2017.

[9] Sslscan, “sslscan Kali Linux Tools,” Aug. 05, 2022. https://www.kali.org/tools/sslscan/ (accessed Feb. 07, 2023).

[10] M. S. S. Wardaya, “Penetration Testing terhadap Website Asosiasi Pekerja Profesional Informasi Sekolah Indonesia (APISI),” 2019. [Online]. Available: http://repository.uinjkt.ac.id/dspace/handle/123456789/48282

[11] T. Tan and B. Soewito, “Menggunakan Framework Nist Cybersecurity Di Universitas Zxc,” vol. 6, no. 2, pp. 411–422, 2022, doi: 10.52362/jisamar.v6i2.781.

[12] Z. M. Luthfansa and U. D. Rosiani, “Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet,” *J. Inf. Eng. Educ.*

Technol., vol. 5, no. 1, pp. 34–39, 2021, doi: 10.26740/jieet.v5n1.p34-39.

[13] A. H. Karbasi and S. Shahpasand, “A post-quantum end-to-end encryption over smart contract-based blockchain for defeating man-in-the-middle and interception attacks,” *Peer-to-Peer Netw. Appl.*, vol. 13, no. 5, pp. 1423–1441, 2020, doi: 10.1007/s12083-020-00901-w.

[14] P. Goldschmidt and J. Kučera, “Defense Against SYN Flood DoS Attacks Using Network-based Mitigation Techniques,” in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2021, pp. 772–777.

[15] FIRST, “Common Vulnerability Scoring System,” pp. 1–24, 2019, [Online]. Available: https://www.first.org/cvss/