The forensic approach uses snort from SQL injection attacks on the server

Dian kurnia[#1], Hendry[*2], Muhammad Syahputra Novelan[#3]

[#]*Computer System & Science and Technology & Universitas Pembangunan Panca Budi*
Jl. Jend. Gatot Subroto Km 4,5 Sie Sikambing Medan 20122 Sumatera Utara, Indonesia

Abstract *Forensic analysis is an action that must be done by network administrators in knowing the source of attacks that occur on the server. Preventive action needs to be taken if there are many high priority attacks from threats on a server. On This research carried out an attack scenario on a server that was designed and then there was an attack scenario that was carried out in the form of an attack with SQL injection techniques. SQL injection technique which is implemented using classic techniques, namely the union join method. The server has also set a snort as an Intrution Detection System when an attack occurs, the snort function will work in detecting SQL Injection attacks. In the implementation of this study SQL injection attacks with union join method is able to find the database name, table and find the administrator username and password so that the attacker login becomes valid as a website administrator. SQL injection using the join union method with the help of sqlmap software is only able to hack the website if a bug occurs on the website, especially on table relationships created by the website creator.*

Keywords — *Server, Sql Injection, Snort, forensic*

I. INTRODUCTION

Hackers can use SQL injection techniques to find the credentials of other users in the database and impersonate these users, this attack also allows hackers to be able to change and delete databases stored in a system and attackers can take advantage of the syntax and capabilities of SQL, as well as the strength and flexibility to support database operation functions and system onality functions available to the database. SQL injection is not a vulnerability that exclusively affects Web applications, code that receives input from sources that are not trusted and then uses inputs that make up dynamic SQL [1]. The SQL Injection case occurs when an attacker can insert a series of SQL statements into a query by manipulating input data into the application [2].

Based on this definition, it can be said that the SQL Injection attack is very dangerous because the attacker has successfully entered the database system and can manipulate the data that exists in the system database. The process of improper data manipulation by the attacker can cause harm to the owner of the injected website. Data and information leakage is fatal. These data can be misused by irresponsible parties. Data and information security is very important in maintaining the resilience of a website. Based on these descriptions, it is considered necessary to test the security of our website against SQL Injection attacks, as well as to analyst the weaknesses of the existing system, so that further action can be obtained to improve the system[3].

Other researchers suggest that SQL injection is a type of hacking on computer security where an attacker can get access to a database in the system. SQL Injection is also an attack similar to XSS attacks in that the attacker makes use of vector applications and also with Common in XSS attacks. SQL injection is also one of the most powerful weaknesses for business impact, because it can cause the dismantling of all sensitive information stored in a database application, including useful information such as usernames, passwords, names, addresses, telephone numbers, and credit card details.

Web server is a software or software that provides data-based services that are used to receive requests or requests from internet users or commonly called clients in the form of http or https which will then be displayed in the form of web pages. Web server other than as software or software can also be classified in hardware or hardware[4].

Web server as software functions to serve client requests while as hardware, the web server functions as a storage place for all data. Web server and its function is what helps us when searching the internet, Web server can be called to do or will transfer user request files through a communication protocol that has been determined in such a way. The requested webpage consists of text files, videos, images, files and others[5].

Intrusion Detection System (IDS) is a system that can detect suspicious activity in a system or network. The Intrusion Detection System (IDS) also functions as a detector for entering and leaving suspicious activities related to network traffic. In addition, the Intrusion Detection System (IDS) serves as a warning to the system or administrator[6].

Other studies suggest that SQL injection using command attacks makes it very easy for an attacker to bypass the administrator login on a website. This can also be detected using a snort, but for prevention a script repair is needed on the website that is the target of the attacker[7].

In this study, researchers used SQL injection attacks to see the extent of measurement of data

security from a web server simulation that we made on the Ubuntu OS server and Kali Linux. Researchers try to do a SQL injection attack on a server that will be built and will be done by using several hosts in order to maximize testing of attacks on the web server that we build on Ubuntu server, and know the resilience of the server from SQL injection attacks.

II. THEORY

A. Snort

Snort is free and open source software for conducting intrusion detection and prevention systems created by Martin Roesch in 1998. Snort has the ability to conduct real-time traffic analysis and packet recording on an Internet Protocol (IP) network. It carries out protocol analysis, content search, and content matching. This program can also be used to detect probes or attacks, but is not limited to, operating system fingerprinting attempts, common gateway interfaces, buffer overflows, server message block probes, and stealth port scans[8].

Snort is a libpcap and logger-based sniffer package that can be used as an Intrusion Detection System (IDS). This rule is based on logging to match content patterns and detect various attacks, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and more. Snort has real-time alerts that are able to notify warnings sent to syslog, Server Message Block (SMB) WinPopup messages, or separate file alerts [9].

In the use of Snort still based on the command-line can provide enough difficulty for users who are accustomed to the Graphical User Interface (GUI) so that there are some supporting parties who develop such as Acid, Microsoft Windows, and IDS centers with php bases that can be accessed using the web GUI based browser.

There are 4 modes in running Snort as a network security analysis, namely:

1) ***Logger Mode***, This type of mode works in recording all data traversed on the network to be analyzed later.

2) ***Sniffer Mode***, This type of mode works by capturing and viewing data that passes on the network

3) ***Intrusion Detection Mode***, This type makes Snort work as a detection activity against various attacks on the network that follows based on the rules (Rules).

4) ***Inline Mode***, Types that work actively as a security on the network by blocking the attack and responding to attacks using Rules that are combined with Firewalls to allow or not data on the network based on the rules that have been determined.

B. Rules Snort

Rules Snort is a database that contains patterns of attacks in the form of signature types of attacks, Rules Snort must be regularly updated. so that when a new attack pattern occurs, Snort can detect that pattern as an attack. Writing rules Snort has rules that rules must be written in one line (single line) [10].

To read and make rules, understand the parts of the rules consisting of the Rules Header and Rules Options. The Rules Header contains actions, protocols, IP addresses, port numbers, destination hosts. Rules Options contain messages that will be displayed later, can be explained from 1 Rules command as follows :

```
Alert tcp any any -> $HOME_NET
(msg:"ICMP DETECT";)
```

From the Rules above can be seen for the Rules Header marked from the tcp any any Alert -> $ HOME_NET and for the Rules Options the contents of the message in between (msg: "ICMP DETECT";).

C. Data AcQuisition (DAQ)

Data AcQuisition (DAQ) is an additional module for the Input / Output package in Snort that is used to activate the Pervention feature in Snort.

Here are some DAQ modules to support Snort to work with the Prevention feature:

1) ***Packet CAPture (PCAP)***, can make Snort work by default with Sniffer and Intrusion Detection System (IDS).

2) ***AFPACKET***, makes Snort work in inline mode by using 2 interfaces that bridge each other without any additional Firewalls.

3) ***NetFilter Queue (NFQ)***, makes Snort work inline using Queue and netfilter or Firewall.

4) ***IPFW***, makes Snort work in inline mode for Open BSD and FreeBSD using pf and ipfw sockets.

5) ***DUMP***, allows Snort to test inline and normalization mechanisms.

D. Intrusion Detection System (IDS)

Intrusion Detection System (IDS) is software that is used to monitor the network for any unpleasant activities and bridge the normal functioning of the system causing several policy violations. this review of several intrusion detection systems and software that highlights their main classifications, performance evaluations and measurements[6].

Intrusion detection system can be classified into 3 parts, namely:

1) ***Host Intrusion Detection System (HIDS)***, This type is placed on a single device such as a server or workstation, where data is analyzed locally to the machine and collected this data from various sources. HIDS can use anomalous and misuse detection systems.

2) ***Network Intrusion Detection System (NIDS)***, NIDS are deployed at strategic points in infrastructure networks. NIDS can capture and analyze data detecting known attacks by comparing patterns or alerts from a database or detecting illegal activities by scanning traffic for anomalous activity.

NIDS is also referred to as "Packet-sniffer", because it captures packets that pass through communication media.

3) ***Hybrid Intrusion Detection System***, management and alerting of both network-based and host-based intrusion detection devices, and provides a logical complement to NID and HID. central intrusion detection management[11].

In most IDS is a passive system where the task of this IDS is only to detect intrusion when an attack occurs and give a warning to the network admin that an attack is occurring.

E. Types - Types of SQL injection attacks

SQL injection attacks have several types of attacks in several ways, namely:

1) ***Classical SQL Injection***, is the most common way to use the UNION method in combining two queries to display important information from the database. before injecting using UNION, an attacker must understand how the query will be executed to get important information in it. An attacker can enter a malicious character such as single quote tags, double minus and so on to produce an error message, where the error message will be used to exploit the web.

2) ***Blind SQL Injection***, is often referred to as true / false, which is when the injection is successful but does not display an error message to the attacker, but instead returns to the page itself or displays some, all content or does not display any content from the web. this technique requires a long time due to guessing the information contained in the database and the response from the request is true / false. if the url being manipulated produces true values, it will display the content but if the url being manipulated produces false values, it will not process requests from the attacker.

3) ***Double Blind SQL Injection / Time-based***, when the injection of the url fails using blind sql injection technique, it doesn't rule out the possibility that the web has a gap against sql injection. Injection is likely to be successful but can be handled in the database so that when the injection is done successfully, but the results cannot be seen in the application and are not visible to the attacker. Double blind sql injection technique is a combination of blind sql injection / classical sql injection with a time delay. if the url combined with time delay will generate a command in accordance with the requested request, then the web application can be injected using a SQL injection attack.

SQL Injection handling analysis is done by initializing a variable in the programming code or the program code that retrieves data from the database (query), validating dangerous characters such as single quote, double quote, comment, tautology, etc. limits input length that will be entered so that the attacker cannot inject by entering a long input into the login form Overcoming error messages that come out of the database by disappearing or hiding in the program code.

III. RESULT AND DISCUSSION

A. Computer Network Layout

In this study will configure a SQL Injection attack, web server and security system that has the ability to monitor networks, detect (detect) suspicious activity on the network, the Terminal Console will function as a Snort binary output that is processed and stored into a MySQL database.

The SQL injection attack system that will be built can be described with the following topology as shown in Fig. 1 and Fig. 2 :

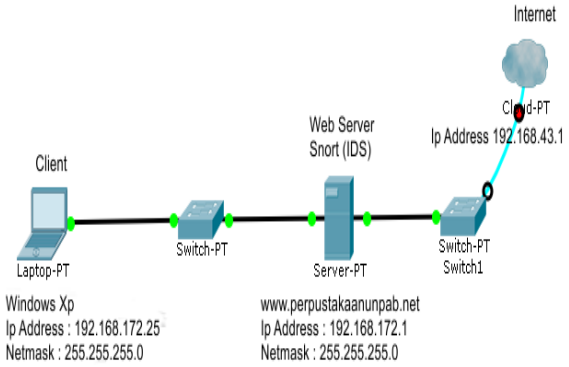


Fig. 1 System Topology Before SQL Injection Attack Occurs

The explanation of the network system topology above is as follows:

1) On the client is a place of testing the configuration results on the web server

2) Switch is a means of connecting connectivity on the network to the web server and the internet

3) The server is a tool for the configuration of the web server and snort (IDS)

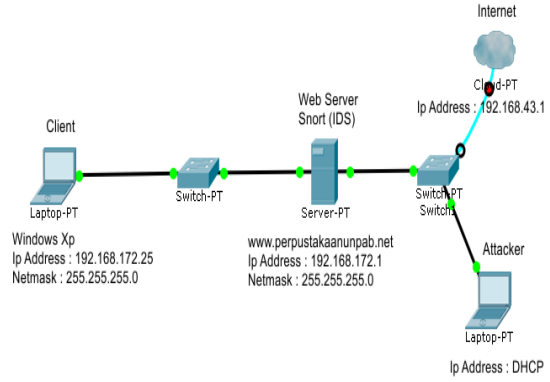


Fig. 2 System Topology After SQL Injection Attack

The explanation of the network system topology above is as follows:

1) On the client is a place of testing the configuration results on the web server

2) Switch is a means of connecting connectivity on the network to the web server and the internet

3) The server is a tool for the configuration of the web server and snort (IDS)

4) Attacker functions with the aim to carry out an attack on the server.

B. Network Management System

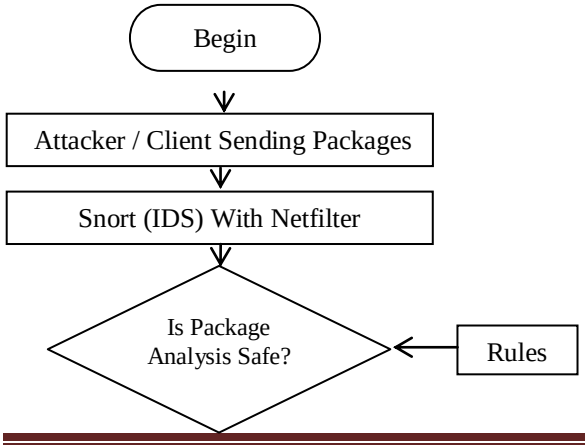
In Figures 1 and 2 above can be explained by IP addressing in the following table:

III. TABLE I
IP ADDRESS CONFIGURATION

No	Hardware/ Software Network	Port Ether net	Alamat IP / IP Address
1	Internet resources	_	Address 192.168.43.1
2	Ubuntu Server	Eth0	Address 192.168.43.141 Netmask 255.255.255.0
	Web Server	Eth1	Address 192.168.172.1 Netmask 255.255.255.0
	Snort (IDS)	Eth0	Address 192.168.43.0/24
3	Attacker	Eth0	*Dynamic Host Configuration Protocol* (DHCP)
4	Client Connected Local Network	Eth1	Address 192.168.172.25 Netmask 255.255.255.0 Gateway 192.168.172.1

In table I. Observation of IP addresses can be determined that the internet source is from a hotspot or uses wifi connected to the server. Then in the ubuntu server, a web server and Snort IDS configuration have been configured, for IP observations the server can do network setup using several commands.

Flowchart SQL Injection, Snort (IDS) and Web Server attack systems can be seen on the following pictures:



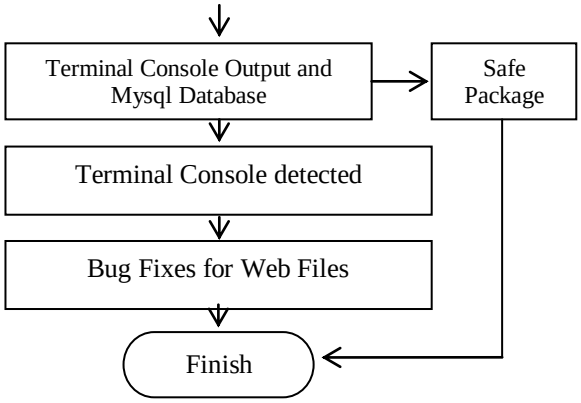


Fig 3. IDS system flowchart to be built

In flowchart Figure 3 shows the IDS system with Netfilter detecting an attack packet sent by the attacker. This attack package is captured and matched with the rules in the local.rules snort. Then if the fingerprint packet matches, the terminal on the console will display a notification that the server is attacked. Notifications are tailored to captured attacks. If the package that snort receives is safe, the notification does not appear. If the attack is identified as SQL injection, then bug analysis is needed on the website and blocking the MAC Address of the attacker.

IV. IMPLEMENTATION

The appearance of the website is usually in the form of hypertext (HTML) or hypermedia which is sent to users via the World Wide Web. To display a web design or content of a website, a web browser or software based on web is needed. The purpose of web design is to create a website that includes a collection of online content including documents and applications residing on a web server. It can also, a website in the form of a collection of text, images, sounds and other content, and can be interactive or static.

At this stage of research analysis the web server is only a place to test the SQL Injection attack website http://www.daftarunpab.net

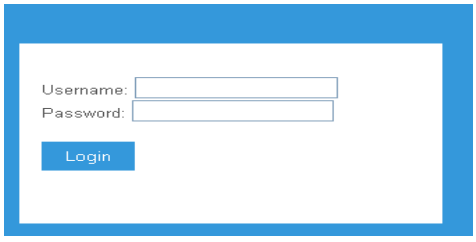


Fig 4. Website views that are the target of attacks

A. Testing SQL Injection Attacks With SQLMAP

This test will carry out attacks using SQL Injection attacks on SQLMAP software namely TCP (Transmission Control Protocol) which works by sending TCP packets by looking for weaknesses or

exploitation on a website and forcing entry into databases server so that it can be able to get databases information and access rights. databases, the attack will make the web server owner will get a loss because the databases information has been known to the attacker.

SQLMAP is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection weaknesses and taking over server databases.

SQL injection is a hacking technique where an attacker can insert SQL commands through a URL to be executed by the database. This bug or vulnerability occurs due to the negligence of a programmer or webmaster in doing web programming such as unfiltered variables in the web.

An attacker by carrying out a SQL injection attack can take over and manipulate a database on a server, following the command in SQLmap to carry out a SQL Injection attack :

```
sqlmap -url http://www.daftarunpab.net
 --dbs --forms
```

```
sqlmap -url http://www.daftarunpab.net --
dbs --forms -D akademik --tables
```

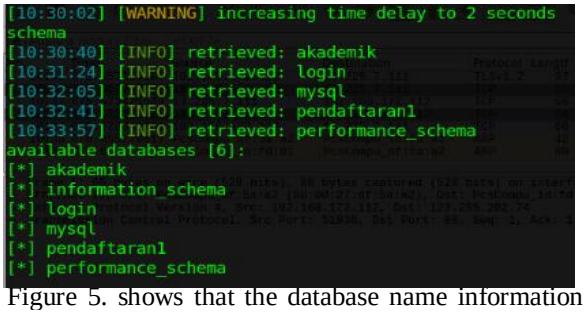


Figure 5. shows that the database name information that we need through exploitation or weaknesses of the website using sqlmap, with weaknesses on the website forms, known the database name used on the target website is “akademik”.

```
sqlmap -url http://www.daftarunpab.net --
dbs --forms -D akademik -T admin --
columns
```

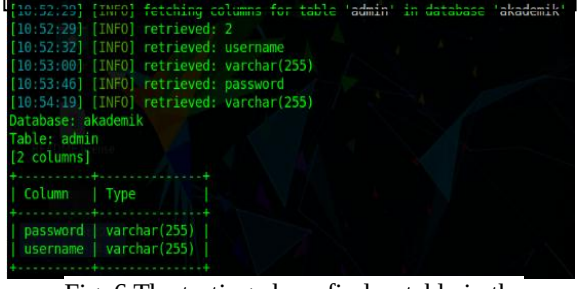


Fig. 6 The testing phase finds a table in the "academic" database

Figure 6 at this test stage, Sql Injection technique with the union join command type can find data in the database in the form of an admin table. This table is also performed sql injection techniques so that known data types from the username and password on the target website. the data type in the username is varchar (255) and the username data type is varchar (255).

```
sqlmap -url http://www.daftarunpab.net --
dbs --forms -D akademik -T admin -C
password,username --dump
```

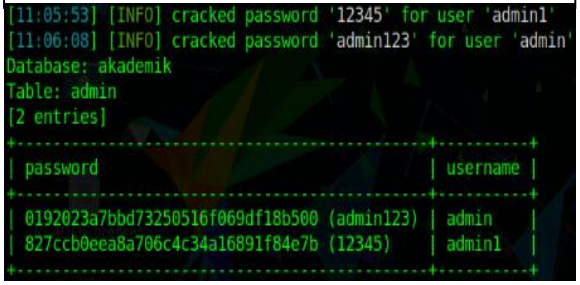


Fig 7. Test by using word.list in describing the md5 encrypted password

Figure 7 in this testing phase, Sql Injection technique can find data from the username and password variables from the "admin" table. It is known that the password variable uses secure hash technique, namely md5 encryption. The encrypted username is then described using the wordlist.txt tool on the Linux operating system. The admin username is "admin123" and the username admin1 is "12345".

B. Forensic Analysis With Snort

Snort has the ability to conduct real-time traffic analysis and packet recording on an Internet Protocol (IP) network. It carries out protocol analysis, content search, and content matching. This program can also be used to detect probes or attacks, but is not limited to, operating system fingerprinting attempts, common gateway interfaces, buffer

overflows, server message block probes, and stealth port scans.

At this stage the snort will function as a detection of excessive incoming and outgoing traffic in the form of an attack on the web server and the snort will be identified by using an alert on the terminal console that the web server has an attack.

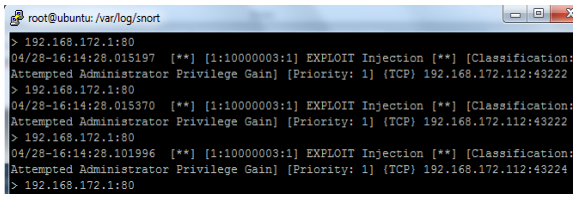


Fig 8. Identify Sql injection attacks with the snort system

Figure 8, snort works and displays the results of identification on the terminal console with a notification in the form of an alert. This alert appears when a snort rule is created that can fingerprint a captured sql injection attack. Snort rules that can be identified are 1000003, in the form of EXPLOIT Injection attacks with the classification of attacks "Attempted Administrator Privillage Gain" in this

case Sql Injection technique entered into the server into an administrator account so that the level of the attack becomes priority 1 or "high". The attack technique also utilizes TCP protocol path with IP Address as the source of the attack namely 192.168.172.112 with port 43222. The attack technique targets Ip Gateway Server which is 192.168.172.1 with port 80. Notifications that appear repeatedly and are identified by snort prove that the attack is still ongoing and prevention must be done immediately. if ignored, the attacker can easily inject into the database and find out the username and password of the targeted website.

V. CONCLUSIONS

The results of the study note that attacks with SQL Injection Techniques are still used by attackers to find out username and password data in a server database. MD5 as an encoding technique can be easily described if the words in the username and password in "word.list" match the data in the username and password in the database of a target server. Snort is able to work and identify scenarios of SQL Injection attacks according to the rules set on the local.rules snort system. Identification of Sql Injection attacks can work well but there is a need for prevention techniques in dealing with Sql injection attacks such as blocking the Mac Address and IP Address of the source of the attack detected by the snort.

ACKNOWLEDGMENT

The research published is actually my work, and there is no duplicate of someone else's work and has never been published in another journal before. for quotations in writing this journal, I cite from other journal publications. I believe this scientific work can be developed by other readers. Thank you to all of you.

REFERENCES

[1] *SQL Injection Attacks and Defense*. .
[2] C. Anley, "*Advanced SQL Injection In SQL Server Applications*," 2002.
[3] D. A. Kindy and A. K. Pathan, "*A Detailed Survey on Various Aspects of SQL Injection in Web Applications : Vulnerabilities , Innovative Attacks , and Remedies*," pp. 1–13, 2012.
[4] S. Mohammad, S. Sajjadi, and B. T. Pour, "*Study of SQL Injection Attacks and Countermeasures*," vol. 2, no. 5, 2013.
[5] A. Muttaqin, S. R. Akbar, and U. Brawijaya, "*Web server embedded system 1,2,3*," vol. 1, no. 1, pp. 50–54, 2014.
[6] D. I. Jaringan and U. Diponegoro, "1) , 2) , 2)," vol. 3, no. 2, pp. 171–178, 2015.
[7] I. Print, "*InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan Analisis Forensik Serangan SQL Injection dan DoS Menggunakan Instrution Detection System Pada Server Berbasis Lokal*," vol. 2, pp. 0–4, 2020.
[8] D. Kurnia, "*Perancangan VLAN pada Jaringan Lokal Web Server LKP Karya Prima Menggunakan Ubuntu Server*," no. x, 1978.
[9] E. K. Dewi and P. Kasih, "*Analisis log snort menggunakan network forensic*," vol. 02, pp. 72–79, 2017.
[10] N. Khamphakdee, N. Benjamas, and S. Saiyod, "*Improving Intrusion Detection System Based on Snort Rules for Network Probe Attacks Detection with Association Rules Technique of Data Mining*," vol. 8, no. 3, pp. 234–250, 2015.
[11] S. Som, S. Sinha, and R. Kataria, "*STUDY ON SQL INJECTION ATTACKS : MODE ,*" vol. 1, no. 8, pp. 23–29, 2016.
[12] Mohammad Dawood Momand, Dr Vikas Thada, Mr. Utpal Shrivastava, " *Intrusion Detection System in IoT Network*", SSRG International Journal of Computer Science and Engineering – Volume 7 Issue 4, 2020