Implementing DMZ in improving network security of web testing

ABSTRACT

We research about to design and to implement network security system in internal web testing using De-Militarized Zone(DMZ) Method and Microtic Router on server of Organization. Data analysis techniques that possible to use in this by descriptive method. The significances of this method study are a) To avoid the attack of bypassing who intend to access the system or device without permissions and b) To improve network security on web testing services on server of Organization. The data that are obtained by having literature review and observation. Literature review assists the researchers to collect the theory on De-Militarised Zone Method in improving network security. Observation was carried out directly to the field to observe the running system. Based on the results and discussion, it is shown that the application of De-Militarized Zone Method on the microtic can secure by the web testing on server of any organization and can maintain the whole series of online services that are available on the server.

1. INTRODUCTION

Network security system is a method of protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system it is used to protect and to prevent the access by unauthorized users to the network in order to avoid various threats without any obstacles. In addition, security system is also used to monitor and to prevent unauthorized access, misuse of information, modification of contain and even deletion of important data on a server. The threats can be categorized into two types internal and external threats. Internal threat could exist intentionally or unintentionally whereas External threat could be tapping system from others. The threat forms of computer network security become varies by day by day. Therefore, the first thing that we should be kept in mind is that no network of computers that is anti-tapping or no network is completely safe from various threats from people who have bad intention. Because the nature of network is having communication openly and the information can be accessed also by people who intend to misuse them. Therefore, we need security system which is highly needed to secure the data in a computer network openly. The precautions that we have to take to protect the network is the duty of network administrator. As we known, the purpose of making network security is one way to anticipate the bad risk at both physical and non-physical threats, either directly or indirectly because the level of crime in computer security system could be classified from annoying to very dangerous ones. Physical forms of crimes that could lose information are the damage the computer and network communication devices, theft, computer hardware or network devices as well. In another side, non-physical category includes the damage of operation system, the damage of applications, the threat of virus and sniffing in which the crime is done by wiretapping techniques or through monitor to steal the personal data of any person or organization.

2. WHAT IS DE-MILITARIZED ZONE (DMZ) ?

A DMZ Network is a perimeter network which protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic in network by providing buffer between the public internet and private networks of Organization. The aim of a DMZ is to allow an organization to access untrusted networks, such as the internet, while ensuring its private network

or LAN remains secure. Organizations typically store external-facing services, end devices and resources, as well as servers for the Domain Name System (DNS), File Transfer Protocol (FTP), Voice over Internet Protocol (VoIP), mail, proxy, and web servers, in the DMZ. These servers and resources are isolated and given limited access to the LAN to ensure that they can be accessed via the internet but the internal LAN cannot. As we show that DMZ approach makes it more difficult for a hacker to gain unauthorized direct access of an any organization's data and internal servers via the internet.

2.1. WORKING

A DMZ network acts as a barrier between the internet and a company's internal network. A security gateway, such as a firewall, isolates the DMZ by filtering traffic between the DMZ and a LAN. Another security gateway protects the default DMZ server by filtering traffic from external networks. It's advantageously situated between two firewalls, and the DMZ firewall configuration ensures that incoming network packets are examined by a firewall—or other security tools—before reaching the DMZ servers. This means that even if a clever attacker manages to get past the first firewall, they must also gain access to the DMZ's hardened services before they can cause harm to a company. If an attacker is successful in breaching the external firewall and compromising a system in the DMZ, they must then breach an internal firewall to obtain access to sensitive business data. Although a highly competent bad actor may be able to break a secure DMZ, the resources within it should trigger alarms that provide ample warning that a breach is taking place.

3. REQUIREMENT FOR DMZ

The high number of attacks and cybercrimes to web application in private organization or public institutions in several countries is related to the negligence of objects that were attacked and because of the failure to detect vulnerabilities which were zero-day. It is then easy to infiltrated by criminals who always prepare to ruffle the data in the system.

Therefore, the researchers design and implement the De-Militarized Zone and Microtic Router to secure the data of online test result using simulation access through Local Area Network (LAN) or internet. [20] stated that computers for server should be fast CPU, large hard drive, good RAM. Otherwise, the hardware needed to network implementation with DMZ method is:

Computer server and client with the minimum specification:

• Processor Intel Celeron

• Hard Disk Drive 20 GB

• RAM / Memory 1024 MB

• Ethernet Card 100/1000 Mbps

Then, the software needed in designing the network security with De-Militarized Zone method is:

In Computer client

• Operation system Windows 7

• Mozilla Firefox

• Nmap Scanner

In computer Server

• Operation system Linux ubuntu server 16.04

• Web server Apache

In Microtic Device

• Microtic Router OS

• Firewall

4. Network System without DMZ

The security condition of this network resources in the current research object should be improved because the topology still uses system that installs server for local access and internet access in the same network group and connects directly to host server without a firewall. It may allow certain people to attack directly to the resources easily. The simple scheme model used today before using De-Militarized Zone Method can be seen in this Figure 1.

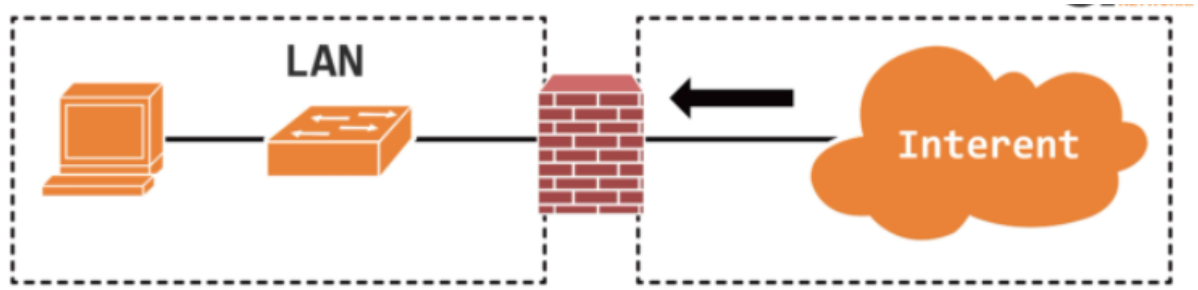


Fig.1: Network Scheme without DMZ

5. Network System With DMZ

In currently designed network security system, it's seeking to establish a firewall zone of De-Militarized Zone (DMZ) in private network by using simulation access through Local Area Network (LAN) or internet. DMZ Firewall is security network boundary which is located between corporate/private LAN network and public network. With that firewall, all traffics are forced to pass through one single concentrated check point where all traffics will be controlled. Giving segmentation to firewall system is useful to protect server in LAN Corporate network from hacker attacks. The designing system of network security with De-Militarized Zone Method is shown in Figure 2.

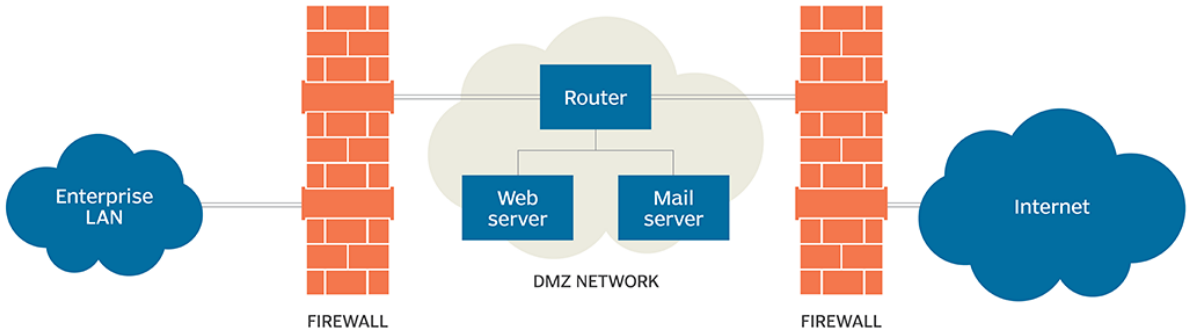


Fig.2 : Network Scheme using DMZ

In this figure the design of new system uses microtic device as DMZ server. Here, DMZ server will be a protector when someone tries to access the resources in server at DMZ zone from public network such as internet. In this user will access the resources which is web server running in an Operating System Open Source, Linux Ubuntu 16.04 as Linux product and other which is widely used by people. In default, system in web server will run at local network area and which is only accessed from port 80 but when accessing from internet, so the local network traffic will be replaced to a public IP address and port 80 will be directed to port 81.

6. THE RESULTS OF ANALYSIS AND APPLICATION OF NEW SYSTEM

In this system , the first step is to installing microtic until the selection of packages because it is needed to make a DMZ Zone for DMZ server for a security system. Therefore, the important thing to do first is installing microtic operation system in a computer server. When the installation of microtic is done, the next is setting the IP in DMZ server that needs minimum 2 interfaces. Here, the first interface is for accessing internet and the second interface is as connector to DMZ zone where the server placed.

The IP addresses are different, between ether 1 and 2. Interface for gateway accessing to internet in DMZ server is 192.168.56.1 and for web server simulation use IP 192.168.0.50 which is put into DMZ server.

List of IP and Interface DMZ Server

No.	Name of Interface	IP Address	Function
1.	ether1	192.168.56.2	Accessing to internet
2.	ether2	192.168.0.1	Accessing to DMZ Zone

Table1.1

It should be observed that microtic supports the firewall in the DMZ system so testing and setting microtic in server are not as complicated as. Therefore, in setting the DMZ parameter in microtic, it needs some commands as shown in Figure 8.:

```
/ip firewall filter
add chain=forward connection-state=established
comment="allow established connections"
add chain=forward connection-state=related
comment="allow related connections"
add chain=forward connection-state=invalid
action=drop comment="drop invalid connections"
```

Fig.8 : Connection setting

Setting up DMZ server is to minimize and maintain only valid connection. It can be proven by showing and releasing information about open port service using NMAP command in server where the port 80 for service http, port 225 for SSH service and port 443 for server which used service as https and others ports are closed. In Figure 9, all are 3 port are open because they have only been allowed by DMZ server to be accessed from outer network or internet. Yet, other ports are closed because they are not allowed by DMZ server as shown in port 22. Furthermore, it is explaining the testing results which inform that scanning tool done cannot detect the host location of server clearly because of it cannot access from outer network or internet because is not directly connected to server of organization but it is protected by DMZ server. Therefore, host that is likely accessed from outside network or internet is host DMZ server.

```
Nmap scan report for siakad.akba.ac.id
([redacted])
Host is up (0.38s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE          VERSION
22/tcp   closed ssh
80/tcp   open   http             Apache httpd
|_http-methods: No Allow or Public header in
OPTIONS response (status code 301)
|_http-title: Did not follow redirect to
https://siakad.akba.ac.id/
255/tcp  open   ssh              (protocol
2.0)
| ssh-hostkey: 1024
c1:8d:fe:41:3c:b7:e0:93:a3:9f:2f:b2:8b:94:0c:0
0 (DSA)
| 2048
f2:df:f5:cf:ba:ef:1a:e3:22:0f:fe:73:d3:a4:c2:1
c (RSA)
|_256
47:a9:7d:94:4d:3b:1f:69:8c:db:89:22:b9:ee:38:6
a (ECDSA)
256/tcp  closed fw1-secureremote
443/tcp  open   ssl/https?
|_http-methods: No Allow or Public header in
OPTIONS
```

Fig.9 : Application result of DMZ

When attack is occurs by attacker, DMZ server automatically will detect that attacks by putting them into database of microtic address list. After microtic detects the existing of DDOS or brute force attacks, IP automatically does reach server because it has been blocked by microtic. The blocking results can be seen in Figure 12.

The testing results are strengthened by the research results of [14] which revealed that applying Militarized Zone will provide better security both for infrastructures of wired and wireless network. It is stated by [10] that DMZ is a major concept in hardware firewall which functions to improve the server security of web testing system especially internal and external network that are closely related to the using of microtic device to control the network.

Fig. 12: Unable accessed Web server

Fig. 12: Unable accessed web server

CONCLUSION

In this proposed work, the aim is to implement De-Militarized Zone that improves the security of any network. Now days, attackers have become more sophisticated and technologically advanced, so everyone needs to implement more security methods in order to avoid any attack. De-Militarized Zone is that kind of security method which separates public ally accessible resources on the basis of their confidentiality forming trusted network and blocking their access inside of any trusted network. Then, the scanning results by using DDOS technique also shows that the server is safe and inaccessible by intruders because DMZ server automatically detect the existence of IP access.

REFERENCES

[1] Science DMZ “https://fasterdata.es.net/science-dmz/”

[2] International Journal of Engineering & Technology “Implementing DMZ in Improving Network Security of Web Testing in STMIK AKBA” https://arxiv.org/ftp/arxiv/papers/1901/1901.04081.pdf

[3] The medical science DMZ: a network design pattern for data-intensive medical science ” https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7651886/”

[4] Fortinet : DMZ “https://www.fortinet.com/resources/cyberglossary/what-is-dmz” S. Prabhakar, “NETWORK SECURITY IN DIGITALIZATION : ATTACKS AND DEFENCE,” Int. J. Res. Comput. Appl. Robot., vol. 5, no. 5, pp. 46–52, 2017.

[5] DMZ improve network : https://www.nstec.com/network-security/how-does-a-dmz-improve-network-security/

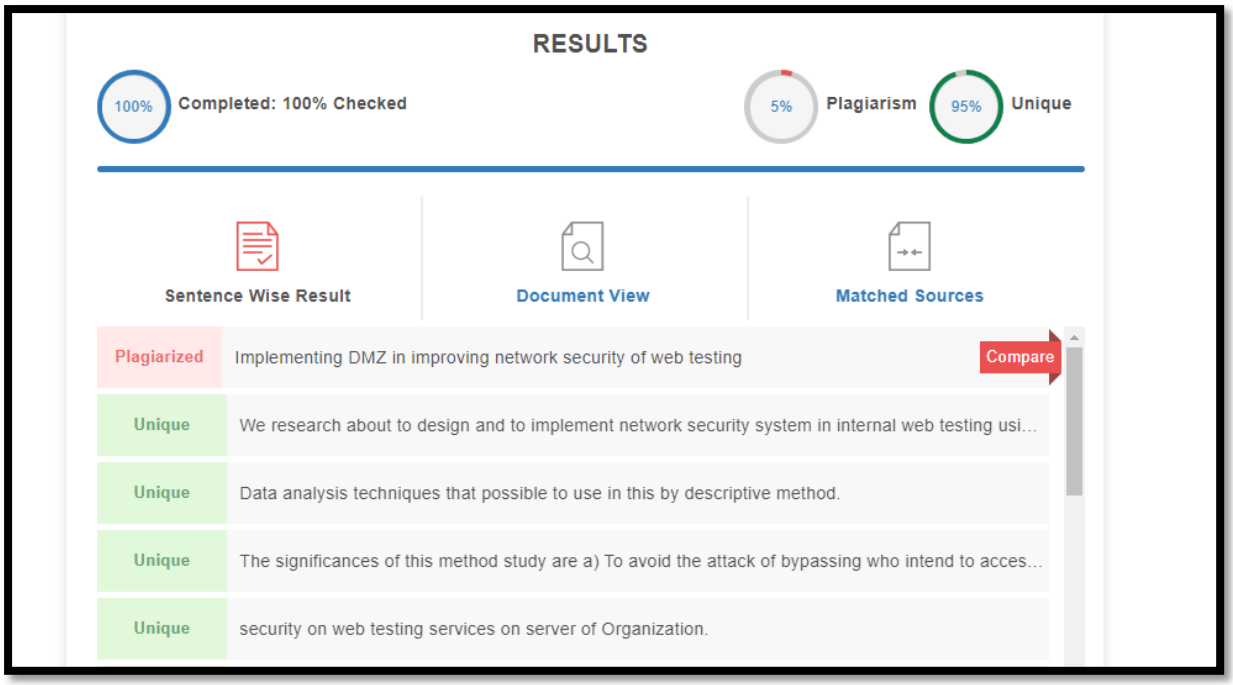
[6] What is used of firewall https://www.ad-net.com.tw/why-firewall-is-used/

[7] definition of DMZ https://www.techtarget.com/searchsecurity/definition/DMZ

[8] Science DMZ Network Architecture. http://fasterdata.es.net/science-dmz/.

[9] Peisert S, Barnett WK, Dart E, et al. The Medical Science DMZ. J Am Med Inform Assoc. 2016;236:1199–1201.

[10] V. Selvi, R. Sankar, and R. Umarani, “The Design and Implementation of On-Line Examination Using Firewall security,” IOSR J. Comput. Eng., vol. 16, no. 6, pp. 20–24, 2014.


RESULTS
100%
Completed: 100% Checked
5%
Plagiarism
95%
Unique
Sentence Wise Result
Document View
Matched Sources
Plagiarized
Implementing DMZ in improving network security of web testing
Compare
Unique
We research about to design and to implement network security system in internal web testing usi...
Unique
Data analysis techniques that possible to use in this by descriptive method.
Unique
The significances of this method study are a) To avoid the attack of bypassing who intend to acces...
Unique
security on web testing services on server of Organization.