SindhUniv. Res. Jour. (Sci. Ser.) Vol. 53 (03) 275-282 (2021)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

A Novel Algorithm for Fortifying Enterprise Network using Demilitarized Zone

H. TUNIO, M. Y. KOONDHAR[++], Z. A. MAHER, R. SHAH*, M. HYDER, P. K. BUTT

Information Technology Centre, Sindh Agriculture University Tandojam

Received 16th January 2021and Revised 28thJuly2021

Abstract: Network Security is a significant component in the age of Information Technology. Attacks against network infrastructure are regarded as among the serious hazard in modern era. Amongst the most critical elements of communication network is the web server. To deal with the web server threats, pre-emptive measures need to be implemented. DDOS attack prevention has always been a hot topic for researchers in the gigantic field of network security. New techniques have been launched to tackle the threats but with the advance in technology, the hackers also come up with unconventional performances to get ransom for exploiting the organization's data and services. The presented defence methodology deals with the security of public facing servers of an enterprise network by setting up a DMZ (Demilitarized Zone) using a Mikrotik router firewall policy. The main objective of this study is to design a topology with a DMZ secured by a Mikrotik router, to test the network with the eminent scanning tools available i.e. Nmap and Nikto, And to implement the Mikrotik firewall policies prudently for the DMZ so that only trustworthy users get access through the network and the hackers sending huge network traffic to let the services down, get blocked automatically. The network was tested and verified by kali Linux machine and penetration testing was accomplished with Slowloris attack. Finally, the comparison of scanning tools for the DMZ and a non-DMZ area in a network were provided. Whole simulation was done on the GNS3 network emulator to get the results like real environment. And the virtual machines for servers and network devices were created in Virtual Box software. The network was designed in a way to consider the easy implementation in a real scenario i.e. an enterprise business. Considering the security of a network with web servers, from DDOS or other similar attacks, the results of the study were clear that having a DMZ in a network secured by an extra layer of firewall can prevent the loss of data and services. As the consequences, Slowloris attack by the hacker was not successful because of the firewall rules applied on Mikrotik and the web server was still available to the standard users.

Keywords: DDOS, DMZ, Kali Linux, Mikrotik, Nmap, Nikto, Slowloris, Web Server.

1. INTRODUCTION

In today's modern world, cyber culture has turn into a widespread and unavoidable cause of intelligence distributing and other specialized actions involving shopping, business, advertisements, bank transactions, and essential services (Humayun *et al.,* 2020). Now a days the whole world is completely linked via the cyberspace or internet, but still its security and defense continues to be a big question for the industrial communities and research (Khoumsi *et al.*, 2016). With the development of network technology, this technology will gradually expose its shortcomings (Li et al. 2021). This much use of cyber space in today's world has drastically increased the criminal activities and cyber threats. The fundamental reason for this growth is the extreme usage of Web applications in nearly every single area of life (Humayun *et al.,* 2020). The requirement to bring improved guidelines and strengthened security is the invention of the high society, where attackers do their element, and for that in the parallel IT security and information specialists do efforts to upsurge security heights, new skills disembark, and new professions are obtainable (Charpentier, 2013). One benefit that hackers provide us is that they make the jobs available in the field of information technology.

2. LITERATURE REVIEW:

The present application relates generally to a system architecture for securing a data environment (Ratica *et al.,* 2018).The penetration test intended to improve the IT enterprise to detect defenselessness in their approach guarantee their reliability in the web application and maintain advance security procedure (Charpentier, 2013). Securing a network is a big task for IT professionals. This goal becomes more difficult if network is connected to the internet. To accomplish the network security, it is important to understand the network system and design it wisely. Designing a network needs best practiced and skills which include dividing the network into different portions. As Rababah *et al.,* (2018) mentioned, network contains segments. First segment contains the server like HTTP

[++] Corresponding author email: yaqoobkoondhar@gmail.com

* College Education, Government of Sindh, Pakistan

server Email server Domain name server which is said to be as Demilitarized Zone. While the other segment can contain the FTP server and other private machines which is called as internal/private network. Also, they added that, Deployment of firewall will not only increase the network security, but it will also enhance the level of service agreements and will contribute to improved network performance and availability through providing quality of service.

3. DEMILITARIZED ZONE AS NETWORK PERIMETER:

With the technology and science advancement, several currently used network security management tools and technologies are even now on the edge of abolition, sorelated branches should wage consideration to the invention of security management and continually update technical measures of network security (Shi, 2020). An attacker could access a web server, but it would be worse if the attacker could access the database through a web server (Rababah *et al.,* 2018). The solution provided by Iskandar *et al.,* (2018) for this kind of extreme situation can be the deployment of a client riddle model. The client riddle rules goals are to endure from the attacks which are used to diminish the capability of server to process requests in the foundation aspect, i.e. joining by the use of Demilitarized zone technique that is achieved in Mikrotik device (Iskandar, Virma, Ahmar, 2018). According to Dadheech *et al.,* (2018), A separate zone is given by DMZ to organization where all the public fronting servers can be placed like web server and E-mail so they can be preserved in different method from confidential and database servers which are located inside the endangered interior network. In Shrimali, (2017) research paper, the author has formed DMZ also an exterior network, but also no argument is here for interior system sanctuary that is foremost apprehension here.

4. PROPOSED MODEL:

Here the proposed model contains three steps, The design of network having a DMZ with a Mikrotik router, analysis of network weaknesses, and the Implementation of enhanced security. The basic DMZ structure is created first, after identifying the assets and resources that need protection. This research is based on experimental studies of designing a secure DMZ network. After designing the DMZ network topology in GNS3 which is a network simulator, the next objective to be achieved in the research is to analyze and find out the network vulnerabilities by scanning the designed network before implementing the algorithm for Mikrotik firewall built in rules. Once the vulnerabilities are found the last objective of this research to be complete is to implement the Mikrotik router firewall rules in such a way that only allowed ports such as port 80, will remain open to access the web server and all other ports will remain inaccessible from outside the network. Mikrotik router firewall rules will block the unauthorized access to the web server and database server. In the end, a network attack is designed through kali Linux to test and verify the system.

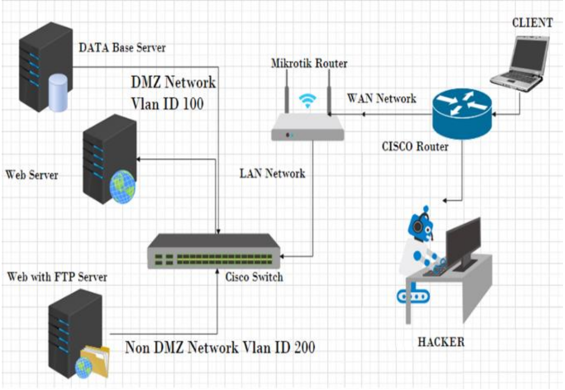


Fig. 1 (DMZ Network Design Using Mikrotik Router)

With support of VirtualBox all the servers are installed on it and virtual machines have been created which are then integrated in GNS3 for preparing prototype for collecting the results. Web server and database server are installed on Linux OS (Ubuntu 20.04) separately. And on the web server two packages are running one is Webmin and second is Virtualmin. For network designcisco switch,is used here for distribution of network through Vlan configuration, and Mikrotik Router for firewall configuration. Cisco router is added for external network connection. Static routing is configured on cisco router. For Hacker side, which is used here for penetration testing, Kali Linux is used to generate the attack to crash down the web services which are running on web server.Whole designed scenario is created on GNS3, which is a network simulator tool and all the given services are integrated in it.

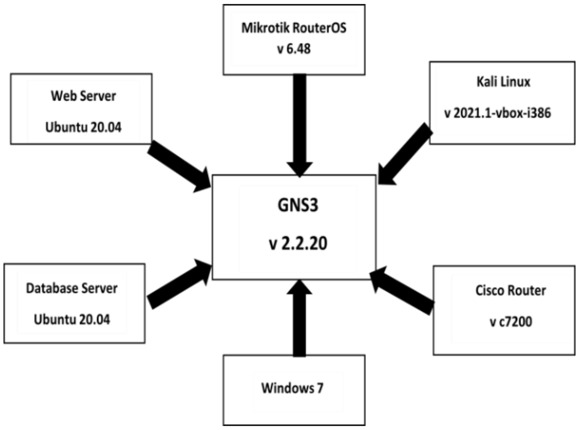


Fig. 2(Prototype designed in GNS3)

Gns3

GNS3 stands for graphical network simulator 3 is a software for network emulator that was first released back in 2008 (Rabiâ, 2018). It is extensively used for experimental purposes research and learning by all over the world (Patel, 2020). It is mainly used for having the actual organization's behavior and emulating it in the designed network scenario. It integrates the real environment devices with each other and provides the simulation for conducting desired results for the research and learning purposes. Kuldeep and S, (2014) mentioned that it provides the results as close as possible to the real networks from the simulated one. In this research, GNS3 version 2.1.9 is used for simulating the network designed in it required OS for GNS3 is Windows 7 (64 bit), with 4GB RAM and at least 1GB of storage.

Virtual Box

VirtualBox is a hypervisor used for creating the virtual machines and having different OS environments to be used simultaneously. Originally it was developed by Innotek, later in 2008, the company was acquired by Sun Microsystems. It supports multiple operating systems like windows, Linux, mac, etc. VirtualBox tool is reliably more lightweight than other hypervisors like VMware WorkStation (Miles & Tashakkori, 2010). In this study, the virtual box is used to create several virtual machines like webserver, database server, kali Linux machine,Mikrotik routerOS and a windows 7 machine. Which will all be integrated in GNS3 for analyzing the system and simulating results.

Webmin And Virtualmin

Webmin is a powerful tool that is used to manage the Linux or Unix servers and all other tools in Linux/Unix, with an ease of providing a Graphical User Interface (Cooper, 2000). All functionalities of webmin are divided into modules, which are nothing but CGI programs that are responsible for managing the services (Cameron, 2000).For Unix and Linux systems, Virtual inis a flexible and more powerful control panel web hosting tool (Lotchi, 2013). This tool is mainly used for managing virtual domains, websites, database servers, mailboxes, and several other applications. In my research, I have used Virtualmin to create a database server which is then integrated with the webserver. And webserver is GUI based by the help of using Webmin in Ubuntu.

Mikrotik RouterOS

Mikrotik RouterOS (operating system) is said to be a developed OS at the commercial side which is especially designed for the implanted devices as an effective network mechanism for example routers, client end devices, wireless APs (access points) and more (Jílek and Žalud, 2012). Mikrotik corporation is the owner of this routerOS. Mikrotik basically provides an inclusive establishment of successful, reliable, and easy to manage Supervision of networks (Barmon, 2020). In this research, the Mikrotik routerOS is used to implement an extra layer of security for the DMZ and internal network by deploying its built-in firewall rules.

Kali Linux

Kali Linux is an operating system that can be installed as a main OS or as a virtual machine in a virtual environment (Marbun *et al.,* 2019). The attacker's side OS being used is kali Linux because of various reasons as it is a secure OS and open source as well also it comes with many preinstalled applications and tools used for hacking such as Slowloris Nmap Zenmap etc. Each of its unit is used to perform security analysis and penetration testing for the network and for web applications. All the utilities are slightly different in performing tasks, but the goal is same (Gunawan *et al.,* 2018). It also has support for programming languages like python and Perl. Perl is built-in and its interpreter is pre-installed in kali Linux. So, Perl scripting used for the Slowloris attack (which is being tested in this research) would be easy to run in kali. Kali Linux OVA file is used here for simulating the penetration testing.

Windows 7

Windows 7 was made public in 2009 on 22 October. Windows 7 is known to be claimed as one of the most secure and protected versions of all its ascendants and descendants (Zhang *et al.*, 2010). Windows 7 is comparatively easy to install and easy to manage, Majority of the desktops, netbooks, and laptops yet use windows 7 as it is easier to perform system recovery on it.It is compatible with most of the software (Gulchehra *et al.*, 2021). In thesis research, I have used windows 7 to only represent the client side by using web browser service.

Cisco Router And Switch

Cisco switches and routers are being used for the purpose of routing and inter-vlan routing (Crichigno*et al.,* 2019). Cisco routers are the most common routers used in networking worldwide. Routers and switches family of cisco uses software called IOS (Rabiâ, 2018). Here, in my work, I have used a cisco router for connecting the internal network with the external network by static routing.

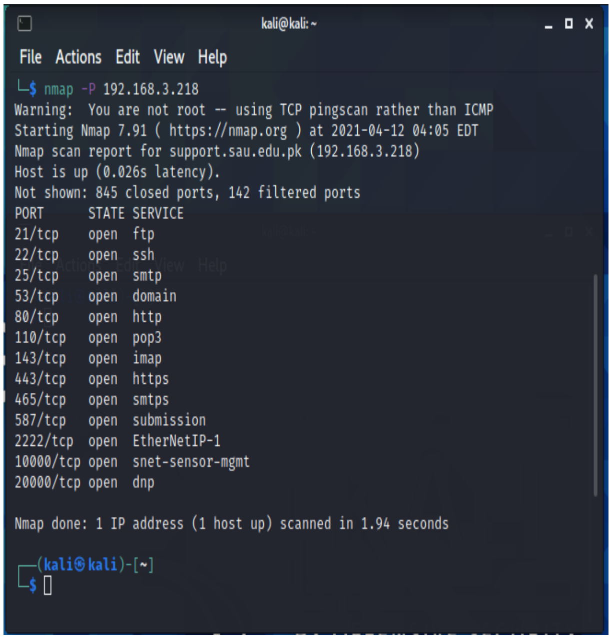
5. <u>MATERIALS AND METHODS:</u>

Designing Network PrototypeHaving DMZ Network Infrastructure

Now for the designing of the network, I have connected all the virtual machines and configured them in gns3 to get the results by simulating whole scenario. DMZ network and server privileges are assigned in Mikrotik router. And the cisco router is used for connectivity with the external network where from a hacker is attempting RUDY or DDoS attack on server because server has the open port 80 for accessing the web browser and this port is open for worldwide users publicly. So that anyone could access website through that port. Not all the users are trustable, by making the path available for public as well as securing it from illegal actions is the purpose of this network topology. Which can be implemented in real world. All simulation is done on GNS3, there are six virtual machines created having different OS and different services are running on it. Firstly, there are three Virtual LANs created in the internal network namely Vlan 100, Vlan 200, Vlan 300. Having IP addresses 192.168.3.0/24, 192.168.4.0/24, and 192.168.5.0/24 respectively. Vlan 100 contains the web server which is having IP address 192.168.3.218/24. And a separate database server which is assigned IP address 192.168.3.216/24 from the given 192.168.3.0/24 network. Vlan 100 is the Demilitarized Zone (DMZ).The server contains IP address 192.168.4.1/24 from the network 192.168.4.0/24. Vlan 200 is a Non-DMZ network. Vlan 300 contains a Client PC which is using the web server from the internal network. It has IP address 192.168.5.1/24 from the 192.168.5.0/24 network. All these vlans are created on a cisco switch. Webserver of DMZ network is connected through ethernet1 port of the switch. Database server is connected through ethernet2 port. Likewise non-DMZ web server is connected through port ethernet3, and Client PC is connected through port ethernet4 of the cisco switch. The switch is than connected to the ethernet0 port of the Mikrotik RouterOS by its port ethernet0.Mikrotik router is installed in virtual machine. It is imported in the GNS3 and configured as core router and the firewall is configured on it, So Mikrotik router is responsible to provide network connectivity as well as security. From the internal network it has IP address 192.168.3.1/24 and from external network or port e1. It has IP address assigned 121.52.154.2/30 which is a public IP address. This network connects the Mikrotik router to the cisco router's port f0/0 by public network 121.52.154.0/30.F0/0 port of cisco router is assigned IP address 121.52.154.1/30. Other port of the cisco router is connected to another public network 111.111.111.0/30. F1/0 port of the router is assigned 111.111.111.1/30 IP address.

For the testing purpose of the network, Kali Linux virtual machine is also installed which will act as the Hacker's machine. This hacker is connected to public network 111.111.111.0/30.Kali Linux is installed to design an attack, Slowloris.pl RUDY attack which was configured in kali Linux because open port of web server is port 80 and attack can be made when attacker has found any open port on server, so through Nmap on kali Linux it is possible to scan open ports on server. Mikrotik RouterOS will be used to secure the Demilitarized zone.Kali Linux is used for penetration testing in this research to test the network security by generating a Slowloris.pl RUDY attack and examining the after effects of that attack on the internal web server and database server.

After designing the network topology with a DMZ in it, next step is to identify the vulnerabilities of the existing system before deploying the firewall rules in the Mikrotik RouterOS. To test the weaknesses of the system, kali Linux is used, and the tool used here for scanning the network and its open ports is Nmap. The result of the scanning is shown below. For frangibility testing, when firewall rules are not implemented yet and to check what impact will be done on Nmap scanning results.



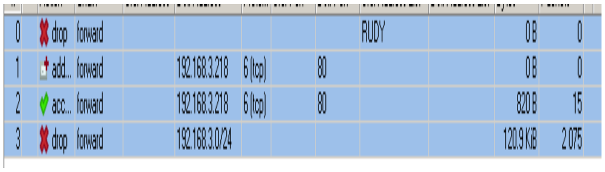
```
└─$ nmap -P 192.168.3.218
Warning:  You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-12 04:05 EDT
Nmap scan report for support.sau.edu.pk (192.168.3.218)
Host is up (0.026s latency).
Not shown: 845 closed ports, 142 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
2222/tcp  open  EtherNetIP-1
10000/tcp open  snet-sensor-mgmt
20000/tcp open  dnp

Nmap done: 1 IP address (1 host up) scanned in 1.94 seconds

┌──(kali㉿kali)-[~]
└─$ ▯
```

Fig. 3 (Result before firewall rules)

In the above figure, results shows that when there is no firewall between a server and hacker, then all by default ports of webserver are in open state. They will be easily detected by the hackers and threats who will scan them by getting access into the network. Attack could be made by any open port that are present in the list of scanned results. Mikrotik firewall rules helps to protect a server from threats and because of firewall a DMZ network was designed.Which will act as the security layer between the internal and external networks. Mikrotik router has GUI based interface which can be accessed through a software called winbox installed on client PC. After installing winbox and connecting the winbox with the Mikrotik router we will configure vlans and firewall rules on the Mikrotik router.



0	✗ drop	forward						RUDY		0 B	0
1	add...	forward		192.168.3.218	6 (tcp)		80			0 B	0
2	✓ acc...	forward		192.168.3.218	6 (tcp)		80			820 B	15
3	✗ drop	forward		192.168.3.0/24						120.9 KiB	2 075

Fig. 4 (Mikrotik firewall rules)

Given rules are based on the efficient and simplified algorithm designed for this research.

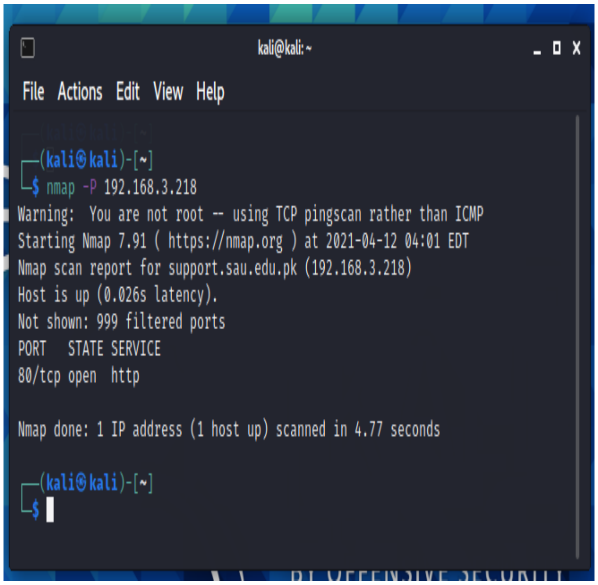
Algorithm

```
Rule 1:
Input:
        Ip_addr = user_Ip;
        Packet_rate = incoming_traffic;
        threshhold_value = 50;
        threshold_time = 0;
        List = RUDY;
        HTTP_Request = 80;
        RUDY = threshold_value>50;
Start
        If (Ip_addr = RUDY & threshold_time = 0++)
        then
Block Ip_addr;
        Block IP address in the List RUDY;
        else (Ip_addr =! RUDY)
        Set threshold_time 0 again;
        GOTO Rule 3;
Rule 2:
        If Ip_addr(packet_rate <= threshold_value)
        then
GOTO Rule 3;
        else
        Ip_addr = RUDY;
        Add IP address in the List RUDY;
Rule 3 & 4:
        If (Ip_addr = HTTP_Request)
        then
Allow Ip_addr;
Allow incoming packets to access web server;
        else
        Drop Ip_addr;
        Discard the incoming packets;
Stop
```

Let's discuss each rule given here. Starting from the bottom, Rule number 4 describes that all other ports except of port 80 are blocked to DMZ network and all the users accessing services other than web browser will not be allowed. Rule number 3 describes that only port 80 on the webserver is open for clients. In rule 1 a list has been created with name 'RUDY' which will contain the IP address of users which are not allowed through rule 4. In rule 2, router will block the users which are present in the list created in rule 1.

6. VERIFICATION AND TESTING AFTERIMPLEMENTING FIREWALL RULES:

For the justification of the presented methodology, I have verified and tested the system through the scanning tools of kali Linux. And by generating an attack from the hacker's side.Kali Linux OS is operated from a hacker's side, which is attempting the attack to stop or crash the web services on port 80. Screenshot attached shows the results for verifying and scanning the open ports of the webserver which is placed in the DMZ network through the NMAP utility which comes built-in in Kali Linux after implementing the firewall rules. After implementation of Mikrotik firewall rules, Nmap utility is used here to test the frangibility of the system one more time and to check whether the open ports other than port 80 are still detectable or not. Figure attached below shows the results of scanning the webserver in DMZ network which has IP address 192.168.3.218.



```
┌──(kali㉿kali)-[~]
└─$ nmap -P 192.168.3.218
Warning:  You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-12 04:01 EDT
Nmap scan report for support.sau.edu.pk (192.168.3.218)
Host is up (0.026s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds

┌──(kali㉿kali)-[~]
└─$ ▌
```

Fig. 5 (Results of Nmap Scanning After Firewall Rules)

It is shown that only port 80 is the open port of web server available and Not Shown:999 filtered ports it means that there is firewall configured between web server and the hacker which is not allowing hacker to scan more open ports on web server. In DMZ environment only the required ports could be allowed to access by clients. For web penetration testing two most common tool are used in kali Linux, first is Nmap and other is Slowloris-master that is a RUDY attack and called DDoS attack.After these all steps, servers configured in DMZ network are ready for penetration testing. Now at this stage of testing the network, kali Linux server again comes in place, and this will perform as hacker side which will generate a RUDY attack that is a type of slow DoS attack.Slowaris.pl tool is configured in kali Linux to perform RUDY attack and then the results will be collected.

Firstly, Starting the Kali Linux virtual machine in the GNS3, when is in running state and connected to the internet or Wi-Fi then the downloaded slowloris.pl master file from the GitHub website that is located on desktop and is needed to run in the terminal by opening the terminal directly through the desktop by right clicking the mouse or keypad of laptop. That's our attack file. The terminal window will be opened and to test the network (web server) with the help of attack that is Slowloris RUDY attack, we need to type the command: **perl slowloris.pl -dns 192.168.3.218 -options**. This command will generate the attack on the web server by sending multiple hundreds of sessions which will ultimately crash the web server and it will not be able to operate and provide any services to anyone. Here, to tackle this problem of crashed services of web server, DMZ network is protected by Mikrotik firewall rules, so open port to reach the web server is only port 80. But Slowloris is that attack which require port 80 to be allowed in web server. So that's why the firewall rules are implemented in a way that will also serve the need to stop the Slowloris attack as well. According to this research all required servers and software are running well and it is ready for testing and collecting the results.

7. RESULTS AND DISCUSSION

From the designed topology, the results that were achieved in GNS3 are that each machine is running and providing the required service.

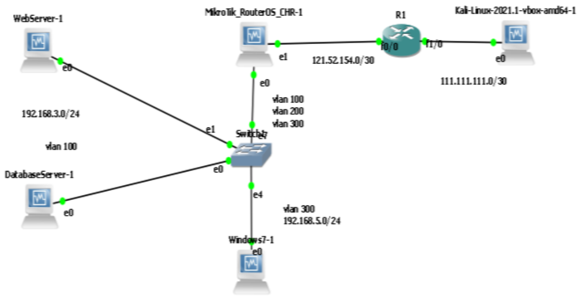


Fig. 6 (Designed Network Topology)

Here, as shown in above figure, the installed machines, like Mikrotik router, Web servers, Database server, a Client PC, Cisco router and a kali Linux machine are installed and are up as the green light indicates. To identify the network frangibility. The Nmap tool were used, and the web server were scanned through Nmap before implementing the Mikrotik firewall rules in it. After the rules were defined, the network is tested by initiating an attack from the kali Linux machine which acts as the hacker side. From the kali Linux, the hacker has started a DDOS Slowloris RUDY attack on the web server which is placed in the DMZ of the network and is publicly accessible. The command for the attack is 'perl slowloris.pl -dns 192.168.3.218 -options'. What this code does is that it sends a huge number of small sessions to the web server which is beyond its limit. As a result, the web server will not be able to handle this manynumbers of sessions and it will be crashed, not providing any services to anyone at all. But after implementing the rules described by the algorithm used, if the web server will get the number of sessions exceeding the limit given in the firewall rules i.e. 50, the Mikrotik router will automatically block the hacker's IP only and the web server will still be able to get accessed by other normal users. As the results are concluded, it shows that having a DMZ infrastructure in a network will eventually provide the better security for the web server as well as the database server. It is important to create or design a DMZ system into your network topology.

8. CONCLUSION

The existing research conclude that a DMZ network secured with Mikrotik router firewall policies can surely provide an extra security layer for the servers placed in it. A web server is a public server which need to be publicly accessible and yet vulnerable to the attacks and threats. A strong mechanism is required to secure it, so here this research is based on algorithm that shows how to secure a demilitarized zone with having servers in it from the external and internal threats. The network designed in this study is having 2 networks, one is internal network, and other is the external network. The internal network is further divided into 3 vlans. Vlan 100, which is the DMZ zone where webserver and a database server is implemented, vlan 200 is a non-DMZ network which is placed for testing purpose and the comparison purpose. Vlan 300 is the client network. The database server is placed on a separate IP location. Web server and database servers are ubuntu Linux virtual machines. Kali Linux machine is placed for generating the attack on the webserver and collecting the results. There are 3 objectives in this research to be achieved. First is to design the DMZ network infrastructure for an enterprise. Second is to test the network before implementation of the Mikrotik router firewall rules and note down results found. Third is to secure the whole network with the Mikrotik router firewall rules. Lastly, whole network is tested and verified by attacking it with the kali Linux host. The Slowloris master Rudy attack, which is a DDOS attack is generated on the web server, which crashes the whole web services if there is no Mikrotik router firewall implemented in between the internal and external network. Hence the study concludes that by implementing a Mikrotik router in a DMZ network, the servers placed in it are secured from all the cyber threats and by placing database server on a separate IP location, the data is also more secured. Mikrotik router blocks the IP of hacker and as consequences, the attack is restricted so the web server is up to provide the required services again.

REFERENCES:

Crichigno, J., E. Bou-Harb, N. Ghani, (2019). A Comprehensive Tutorial on Science DMZ. IEEE Communications Surveys and Tutorials, 21(2), 2041–2078. https://doi.org/10.1109/COMST.2018.2876086

Gulchehra, K., R. Maprat, K. Shoira, A. Nurislom, A. Ugli, (2021). International Journal On Human Computing Studies www.journalsresearchparks.org/index.php/IJHCSe-Comparative characteristics of operating systems of the windows 7th and 10th generations family. www.journalsresearchparks.org/index.php/IJHCS

Gunawan, T. S., M. K., Lim, N. F., Zulkurnain, M. Kartiwi, (2018). On the review and setup of security audit using Kali Linux. In Indonesian Journal of Electrical Engineering and Computer Science Vol. 11, Issue 1, 51–59. Institute of Advanced Engineering and Science. https://doi.org/10.11591/ijeecs.v11.i1.pp51-59

Hailey, J. (2008). Ubuntu: A Literature Review A Paper Prepared for the Tutu Foundation.

Humayun, M., M. Niazi, N Jhanjhi, M Alshayeb. and S. Mahmood, (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, 45(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

Iskandar, A., E. Virma, A. S. Ahmar, (2018). Implementing DMZ in Improving Network Security of Web Testing in STMIK AKBA. In International Journal of Engineering & Technology Vol. 7, Issue 2.

Jílek, T., L. Žalud, (2012). Security of remote management of embedded systems running Mikro Tik RouterOS operating system using proprietary protocols. IFAC Proceedings Volumes (IFAC-Papers Online), 11(PART 1), 169–173. https://doi.org/10.3182/20120523-3-cz-3015.00034

Kajwadkar, S., V. K. Jain, (2018). A Novel Algorithm for DoS and DDoS attack detection in Internet of Things. 2018 Conference on Information and Communication Technology, CICT 2018. https://doi.org/10.1109/INFOCOMTECH.2018.8722397

Khoumsi, A., M. Erradi, W. Krombi, (2018). A formal basis for the design and analysis of firewall security policies. Journal of King Saud University - Computer and Information Sciences, 30(1), 51–66. https://doi.org/10.1016/j.jksuci.2016.11.008

Li, J., J. Huang, L. Tian, J. Wang, (2021, April). New Active Defense Technology under the Background of Power Information Network Security. In Journal of Physics: Conference Series Vol. 1852, No. 2, 022071. IOP Publishing.

Liu, X., Yang, X., & Xia, Y. (2010). NetFence: Preventing Internet Denial of Service from Inside Out. http://arxiv.org/abs/1009.0033

Marbun, P. A., A. Almaarif, A., Budiono, (2020). Website Security Analysis of Department and Integrated Services One Door of XYZ Regency using Kali Linux. 227–233. https://doi.org/10.5220/0009908302270233

Mishra, S., S. K., Sharma, M. A. Alowaidi, (2020). Analysis of security issues of cloud-based web applications. Journal of Ambient Intelligence and Humanized Computing. https://doi.org/10.1007/s12652-020-02370-8

Mursyidah, H., A. Arhami, M. Hidayat, H. T. Anita, &R. dhona. (2019). Analysis and implementation of the Port Knocking method using Firewall-based Mikrotik RouterOS. IOP Conference Series: Materials Science and Engineering, 536(1). https://doi.org/10.1088/1757-899X/536/1/012129

Najafabadi, M. M., T. M. Khoshgoftaar, A. Napolitano, C. Wheelus, (n.d.). RUDY Attack: Detection at the Network Level and Its Important Features. http://www.gartner.com/newsroom/id/2344217

Nanda, S., T.C. Chiueh, (n.d.). A Survey on Virtualization Technologies.

Puchianu, D. C., N. Angelescu, G. Predusca, D. Circiumarescu, E. D Iaconu, (2020,). Comparative study of power consumption on Mikrotik and Fortigate routers. Proceedings of the 12th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2020. https://doi.org/10.1109/ECAI50035.2020.9223210

Rababah, B., Zhou, S., & Bader, M. (2018). Evaluation the Performance of DMZ. International Journal of

Wireless and Microwave Technologies, 8(1), 1–13. https://doi.org/10.5815/ijwmt.2018.01.01

Redya, V., K. S. Chatrapati, V. N. Kamalesh, (2013). Paper on Types of Firewall and Design Principles. In International Journal of Science and Research (Vol. 5). www.ijsr.net

Sabri, S., N. Ismail, A. Hazzim, (2021). Slowloris DoS Attack Based Simulation. IOP Conference Series: Materials Science and Engineering, 1062(1). https://doi.org/10.1088/1757-899X/1062/1/012029

Schagen, N., K. Koning, H., Bos, C. Giuffrida, (2018). Towards automated vulnerability scanning of network servers. Proceedings of the 11th European Workshop on Systems Security, Euro Sec 2018. https://doi.org/10.1145/3193111.3193116

Shi, G. (2020). Application of Computer Information Management Technology in Network Security. Journal of Physics: Conference Series, 1578(1). https://doi.org/10.1088/1742-6596/1578/1/012046

Shin, S., H. Wang, G. Gu, (2015). A first step toward network security virtualization: From concept to prototype. IEEE Transactions on Information Forensics and Security, 10(10), 2236–2249. https://doi.org/10.1109/TIFS.2015.2453936

Tashakkori, R. (2014). Improving believability of simulated characters. https://www.researchgate.net/publication/234828652

Theses, E., D. Theses, M. Papers, M. Patel, (2020). Scholarship at UWindsor Scholarship at UWindsor Demilitarized Zone: An Exceptional Layer of Network Security to Demilitarized Zone: An Exceptional Layer of Network Security to Mitigate DDoS Attack Mitigate DDoS Attack. https://scholar.uwindsor.ca/etd/8306

Wang, A., M. Iyer, R. Dutta, G. N., Rouskas, I. Baldine, (2013). Network virtualization: Technologies, perspectives, and frontiers. In Journal of Lightwave Technology Vol. 31, Issue 4. 523–537. https://doi.org/10.1109/JLT.2012.2213796

Xu, C., P. Li, Y. Luo, (2018). A programmable policy engine to facilitate time-efficient science DMZ management. Future Generation Computer Systems, 89, 515–524.https://doi.org/10.1016/j.future.2018.07.016