DeMilitarized Zone: Network Architecture for Information Security

Sourabh Shrimali
M.Tech (Network Management & Information Security)
School of Computer Science & IT
Devi Ahilya Vishwavidyalaya, Indore, India

ABSTRACT

Information Security refers to the protection of any network and its underlying data. It prevents a network from an unauthorized access, misuse, modification, and deletion of any data inside the network. It targets various security threats and stops them from entering or spreading into the network. It consists of multiple layers of defense in the network; this is known as Defence in Depth Principle. In this each layer has its own policies and protocols to implement; its main aim is to give access to authorized users while blocking malicious users that are carrying threats.

DeMilitarized Zone is the kind of Network Security that based on the Principle of Defence in Depth. It is also represent as "DMZ".

Keywords

Network Security, Information Security, Defence in depth Principle, DeMilitarized Zone, Perimeter Network, Confidential Data and Cyber Breach.

1. INTRODUCTION

In general DeMilitarized Zone "DMZ" is an area between two or more countries restricting each other from any kind of military activity. Thus, in networking, DeMilitarized Zone is a physical or virtual network or sub-network which separates internal network usually LAN & WAN from untrusted external network, i.e. Internet. By doing so, it provides an additional layer of security to any network as hackers are unable to access internal services directly using internet. Because of this, DMZ is also known as "Perimeter Network".

DMZ is an example of Defence-in-Depth principle; it states that "the only way for a system to be more secure is to consider every aspect of security". [1]

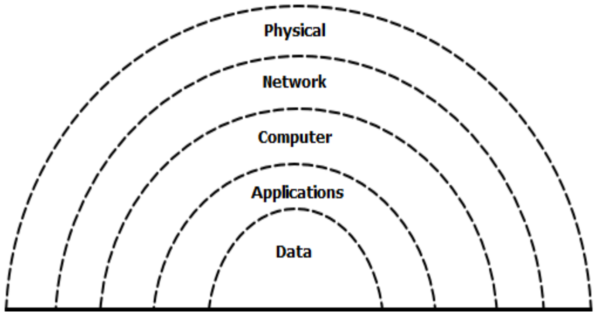


Figure 1: Representing layered security model of Defence in Depth Principle

In this proposed work of network architecture of DMZ to achieve more security; try to configure network by separating external network, demilitarized zone and internal network by putting them on same or different subnets. Using different subnets is more secure because network traffic can't be transmitting to different subnets without being routed. This will bring more security to the system.

Thus, by having different types of firewalls with different set of rules on each side of DMZ causes more security to the network because it will be difficult for any intruder to attack a network having different set of protocols. Since DMZ works on the design of separation, i.e. separation of the Internet and the trusted network on the basis of more confidential data separated from less confidential, by using this design any attacker can be forbid to get into the whole system.

2. OBJECTIVES

Based on the confidentiality of any information; configure the DeMilitarized Zone network with the help of Network Simulator like GNS-3. Performance evaluation of proposed work: catch the data packet that routes inside the network and analyze that whether it can penetrate DeMilitarized Zone or not; if not than the network architecture is strong enough for providing security to any confidential information. And thus objective is fulfilled.

3. LITERATURE SURVEY

Many studies are available in the area of network security. They all are describing the importance of securing any network from unauthorized access like Hacking. Since current Security Measures likes Encryption, Intrusion Detection & Prevention, Patch Management, System Monitoring and Vulnerability Assessment are not sufficient to protect any network from Cyber Breach, so a new way of securing a network was developed which is known as DeMilitarized Zone "DMZ".

Currently, in information security protection of data is done through confidentiality, availability and integrity by configuring firewalls, routers and/or switches. The problem is resources like web servers are publicly accessible and if they are placed inside the trusted network than attacker gets inside the whole trusted system when attacking it. [2]

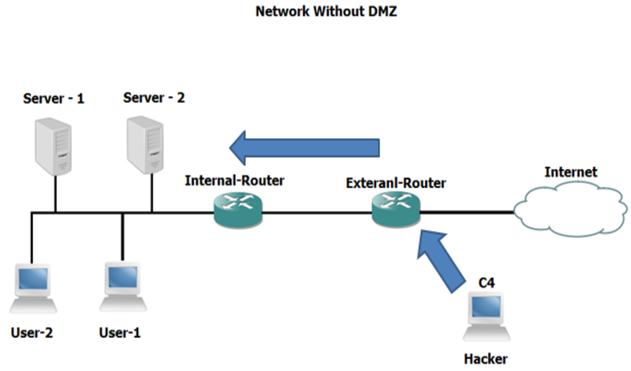


Figure 2: Representing vulnerable network, i.e. Network without DMZ

So, the solution to this problem is to create a separate network, i.e. DeMilitarized Zone which provides enough security without affecting the accessibility of the data. Thus, DMZ is a network which secures the trusted network by keeping non trusted users out. By doing so, if attacker gets success in obtaining an access inside the trusted network they still don't have access to DMZ network. [3]

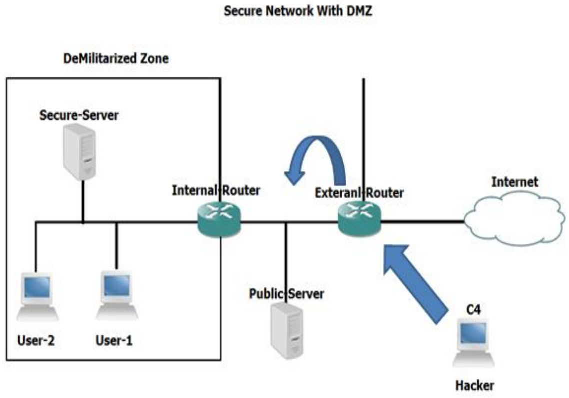


Figure 3: Representing much secure network, i.e. Network with DMZ

In DMZ separation is important, so that an attacker can't get access to all the systems inside the network. In 2014, Information from at least 500 million Yahoo accounts was stolen, Which includes names, email addresses, telephone numbers, dates of birth, etc. In 2015, Kaspersky Lab revealed that it was attacked Duqu 2.0 a type of Malware, variant of Stuxnet. In August 2016, Oracle was attacked by Russian cyber crime groups, and many more.

4. PROPOSED RESEARCH METHODOLOGY

The main aim of the proposed work is to implement a DeMilitarized Zone "DMZ" that it will be useful in the private networks such as any Organization or any company. An experimental configuration is required to study & analyses DeMilitarized Zone consisting of Network Simulators and other required tools. This project includes Network Simulators such as Graphical Network Simulator-3 and Wireshark for packet capturing & sniffing purpose respectively.

4.1 System Configuration

Tool: GNS – 3, Wireshark
Technology: Network Simulation
Operating System: Windows 8.1
Hardware specification: i3 processor, 4GB RAM and 1TB HDD

4.2 Configuration Details

Graphical Network Simulator (GNS - 3) – It is a network simulator that allows us to create virtual complex networks and can perform their emulations. GNS-3 allows emulation by using Cisco Internetwork Operating Systems (Cisco IOS); it allows us to run a Cisco IOS in a virtual environment. GNS-3 is a graphical front end to a product called Dynagen. Dynamips is the core program that allows IOS emulation. [4]

Wireshark - Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross-platform, uses to capture packets; it runs on Linux, MacOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. Wireshark lets the user put network interface controllers that support promiscuous mode into that mode, so they can see all traffic visible on that interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic. [5]

Here the network is created by using GNS-3 which consists of CISCO 3745 Routers and Servers. Also routing protocols are required for communication thus configured EIGRP routing protocol. In this GNS -3 was used because it gives better real time network simulations. Configuration commands for creating DMZ are given below.

```
R4>enable
R4# configuration terminal
R4(config)# interface f0/0
R4(config-if)# ip address 192.168.6.102    255.255.255.0
R4(config-if)# no shut
R4(config-if)#do write
R4(config-if)#exit
```

```
R4>enable
R4# configuration terminal
R4(config)# router eigrp 100
R4(config-router)#network 192.168.6.100
R4(config- router)# no autosummary
R4(config-if)#do write
R4(config-if)#exit
```

After doing all the basic configurations a network was created as shown in figure 4. This network was separated into two sub-networks, i.e. "Public Server" and "Confidential Server" from untrusted external network "Internet" on this basis of confidentiality of information. Now to secure data/information according to proposed work implement "DeMilitarized Zone" at "Confidential Server", i.e. "R4" so that if any attacker breaches into the network they are only able to get access to "Public Server". But they can't breach "DMZ". Thus, the data is safe behind this additional layer of security.

```
R4>enable
R4# configuration terminal
R4(config)# access-list ?
R4(config)# access-list 1 ?
R4(config)# access-list 1 permit 192.168.5.100    0.0.0.255
R4(config)# access-list 1 permit 192.168.6.100    0.0.0.255
R4(config)# interface f0/0
R4(config-if)# ip ?
R4(config-if)# ip access-group 1 in
R4(config-if)# do write
R4(config-if)#exit
```

Note: Here configuration of R4 was mentioned only, because implementation of DMZ was done at this network as inside of it Confidential Server was kept. While the configuration for all the other routers and servers are remain same as that of R4.

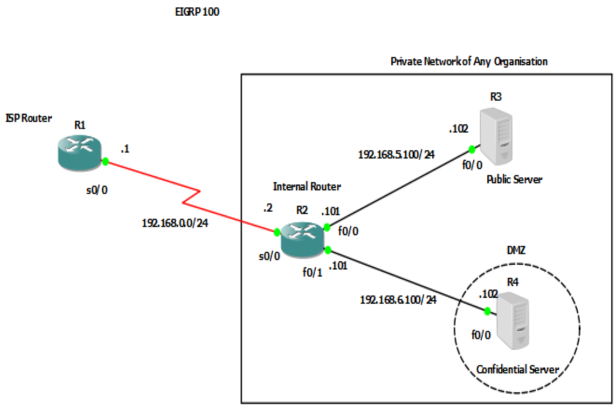
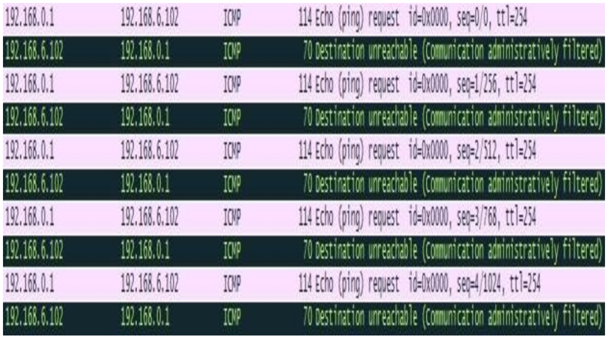


Figure 4: Representing DeMilitarized Zone: Network Architecture for Information Security

This whole concept can be easily understood as confidential and important things were kept inside Bank's Locker and less confidential things at Home. Now, even having sufficient security measures at home if any burglar breaches into it they can't stole confidential things as they are safe inside the Bank's Locker.

4.3 RESULT ANALYSIS

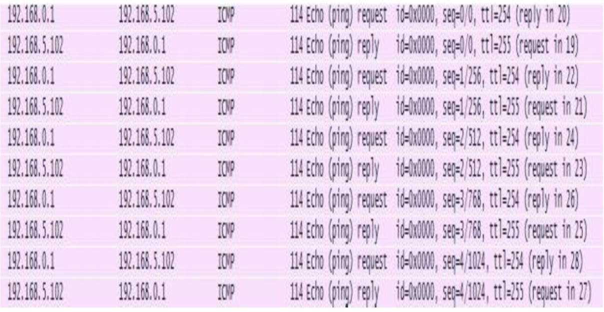
After implementation, ping the network and the result are given below. Since "DMZ" is configured at "Confidential Server", i.e. "R4" whose IP is "192.168.6.102". Initially ping this router & try to capture network traffic coming towards it from untrusted network which is "Internet" whose IP is "192.168.0.1" using "Wireshark" tool and analyses the data packet. If there is "No Reply" from confidential server for each ping "Request" coming from Internet than it means data is secure behind "DeMilitarized Zone".



```
192.168.0.1     192.168.6.102   ICMP   114 Echo (ping) request  id=0x0000, seq=0/0, ttl=254
192.168.6.102   192.168.0.1     ICMP    70 Destination unreachable (Communication administratively filtered)
192.168.0.1     192.168.6.102   ICMP   114 Echo (ping) request  id=0x0000, seq=1/256, ttl=254
192.168.6.102   192.168.0.1     ICMP    70 Destination unreachable (Communication administratively filtered)
192.168.0.1     192.168.6.102   ICMP   114 Echo (ping) request  id=0x0000, seq=2/512, ttl=254
192.168.6.102   192.168.0.1     ICMP    70 Destination unreachable (Communication administratively filtered)
192.168.0.1     192.168.6.102   ICMP   114 Echo (ping) request  id=0x0000, seq=3/768, ttl=254
192.168.6.102   192.168.0.1     ICMP    70 Destination unreachable (Communication administratively filtered)
192.168.0.1     192.168.6.102   ICMP   114 Echo (ping) request  id=0x0000, seq=4/1024, ttl=254
192.168.6.102   192.168.0.1     ICMP    70 Destination unreachable (Communication administratively filtered)
```

Figure 5: No Reply from Confidential Server (DMZ) to the ping request from Internet (Untrusted Network)

But Internet whose IP is "192.168.0.1" should be able to ping "Public Server" whose IP is "192.168.5.102". So ping it and if there is each "Reply" from "Public Server" for every "Ping Request" from "Internet" than it means they both can communicate with each other easily, thus the network that created was configured correctly. And thus, the goal to implement DeMilitarized Zone: Network Architecture for Information Security "DMZ" was achieved successfully.



```
192.168.0.1     192.168.5.102   ICMP   114 Echo (ping) request  id=0x0000, seq=0/0, ttl=254 (reply in 20)
192.168.5.102   192.168.0.1     ICMP   114 Echo (ping) reply    id=0x0000, seq=0/0, ttl=255 (request in 19)
192.168.0.1     192.168.5.102   ICMP   114 Echo (ping) request  id=0x0000, seq=1/256, ttl=254 (reply in 22)
192.168.5.102   192.168.0.1     ICMP   114 Echo (ping) reply    id=0x0000, seq=1/256, ttl=255 (request in 21)
192.168.0.1     192.168.5.102   ICMP   114 Echo (ping) request  id=0x0000, seq=2/512, ttl=254 (reply in 24)
192.168.5.102   192.168.0.1     ICMP   114 Echo (ping) reply    id=0x0000, seq=2/512, ttl=255 (request in 23)
192.168.0.1     192.168.5.102   ICMP   114 Echo (ping) request  id=0x0000, seq=3/768, ttl=254 (reply in 26)
192.168.5.102   192.168.0.1     ICMP   114 Echo (ping) reply    id=0x0000, seq=3/768, ttl=255 (request in 25)
192.168.0.1     192.168.5.102   ICMP   114 Echo (ping) request  id=0x0000, seq=4/1024, ttl=254 (reply in 28)
192.168.5.102   192.168.0.1     ICMP   114 Echo (ping) reply    id=0x0000, seq=4/1024, ttl=255 (request in 27)
```

Figure 6: Reply from Public Server to the ping request from Internet (Untrusted Network)

5. CONCLUSIONS

In this proposed work, the aim is to implement DeMilitarized 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. DeMilitarized Zone is that kind of security method which separates publically accessible resources on the basis of their confidentiality from untrusted network and blocking their access inside of any trusted network. This project uses Graphical Network Simulator (GNS – 3), Wireshark and other penetration & testing tools for experimentation and result analysis respectively.

Catch the data packet that routes inside of the proposed network and analyses that whether it can penetrate DeMilitarized Zone or not; if not than the network architecture is configured correctly and it is strong enough to provide security to any confidential information stored inside that network. The degree of design of the DeMilitarized Zone will determine how secure any network is.

The next challenge for us is to implement "DMZ" in wireless network environment which is Wireless DeMilitarized Zone "WDMZ".

Typically, physical security is the way to ensure that no unauthorized person could gain access to the corporate network and providing harm to them. But now days everyone is using wireless network architecture i.e. "WLAN" and it is continuously growing in enterprise networks, thus making it the new security issue. Initially, IEEE 802.11 proposed Wired Equivalent Privacy "WEP" for wireless security but soon it became an inadequate mechanism, then IEEE 802.11 gave WI-FI Protected Access "WPA" and "WPA-2".

But all these are still not enough to protect any wireless network from eavesdropping, low-level authentication, unauthorized access or any other kind of attack. So it becomes very necessary to implement Wireless DeMilitarized Zone "WDMZ" on wireless network architecture for information security.

Thus, DeMilitarized Zone will provide better security on both wired and wireless network infrastructures.

6. REFERENCES

[1] DMZ (Computing), available at https://www.wikipedia.org/DMZ_(Computing)

[2] Network DeMilitarized Zone – Jack Webb, available at http://www.infosecwriters.com/Papers/jwebb_network_demilitarized_zone.pdf

[3] DeMilitarized Zone (DMZ) – Secure your server network, available at http://omni-bridge.com/blog/2015/09/demilitarized-zone-dmz-secure-your-server-network

[4] Graphical Network Simulator, available at https://www.csd.com/material/GNS3-0.5-tutorial.pdf

[5] Wireshark: Getting Started, available at http://www.staff.ustc.edu.cn/~bhua/Kurose_Labs/Wireshark_INTRO_July_22_2007.pdf

[6] Network Security, available at https://www.cisco.com/products/security/network-security.html

[7] Designing a DMZ – SANS Institute, available at https://www.sans.org/readingroom/whitepapers/firewalls/designing-dmz-950