Security in Virtual DMZ Designs

XXXXX Unitec Institute of Technology, New Zealand, XXXXX, Thames Coromandel District Council, New Zealand, and XXXXX, Brno University of Technology, Czech Republic

e-mail:XXXXXX

Abstract — **Virtualization as a technology has existed for almost three decades now. By emulating physical resources, virtualization enables to utilize the full capacity of their hardware resources. Traditional physical DMZs (*demilitarized zones*) can be virtualized in three different ways. In this paper the level of security of these three virtualized DMZs was compared to the level of security of traditional physical DMZs. The DMZs considered, represented a typical part of a network of an organization. A test bed was set up Using VMware ESXi 4.1 hypervisor to determine which DMZ design was the most secure. A quantitative research methodology approach was used to collect data with the help of a range of vulnerability assessment tools. Based on the research, conclusion was drawn that all security elements, like firewalls and the inspection algorithms in the firewall, determine the level of security of a virtual DMZ and not its being physical or virtual.**

Keywords: **Virtualization, emulation, security, firewall, Demilitarized Zone**

I. INTRODUCTION

The aim of this paper is to determine which virtual DMZ design, is the most secure to implement while still retaining the information security of the network. Accordingly, the primary research question, "Is it secure to implement DMZ in a virtual network infrastructure?" was investigated to answer by carrying out this research. Other secondary questions to be considered to facilitate the primary research question were: 1) How can virtualized DMZs be implemented? 2) Which is the most secure type of virtual DMZ? 3) Which DMZ design is appropriate for a specific business requirement? 4) What impact will virtual DMZs have on information security in contrast to traditional DMZs? 5) What is to be avoided while deploying VMs in a DMZ?

The paper "DMZ Virtualization with VMware infrastructure" [1], suggests three deployment strategies and firewall implementations, to establish virtual DMZs. Understanding which deployment strategy is best suited is essential for effective virtualization. It is also believed that cloud computing will be an integral part of computing in future, the investigation of how secure our cloud is, is yet another area that motivates this research, with a view to explore whether virtualization is really secure for cloud computing. Since virtualization is one of the underlying technologies that formulate our cloud's data centres [2], cloud users need to know how secure virtualization is. In order to answer the above questions, vulnerability assessment was conducted in a virtualized environment. Results of vulnerability assessment were used to justify the stability of the environment and would suggest what security policies are to be employed to secure virtual infrastructure with DMZs and be a part of both the private and public cloud.

The organisation of this paper is as follows: next Section 2 covers state of the art, related works and contribution this paper makes, Section 3 covers the proposed research methodology used for the current study, and Section 4 covers the data anaysis. Section 5 covers the discussion and conclusion followed by the references.

II. STATE OF THE ART

Virtualization introduces a new layer of implementation to our traditional computer networks [3]. Considering the implementation of this new layer virtualization introduces new security issues in the network. One of the benefits of virtualization is its ability to easily scale up server environments. Although a benefit, it is also a great concern for security administrators. The scalability factor in large network deployments can lead to inconsistency in monitoring the server environment [4]. VMM (Virtual Machine Monitors) gives administrators the flexibility for deploying new virtual machines in their server environment and they are no longer bound to acquiring physical resources. Over a period of time this has an impact on the security mechanisms within the network, as the work load on administrators also increases and may lead to inconsistency in security mechanisms as well [3].

In a traditional network the physical machines are connected to the network via a particular port on the switch that can be monitored. In a virtual environment this is not the case; large virtual machine deployment can be attached to one physical port on the network. These virtual machines, if communicating with each other, do not need to pass traffic onto the physical port; they can communicate with each other, as they are part of one single virtual switch. In other words, inter-VM traffic is opaque to the physical network, because they lie within the hypervisor layer [5]. Furthermore, virtual machines can easily bypass IP filtering on firewalls [6]. When a VM migrates from one host to another it might change its security zone if the physical NIC of the host to which the VM should be migrated is placed outside the firewall security zone [7]. All these issues among others leads to design problems in virtual environments and adds to the complexity of the network. When virtual environments are not designed carefully, detectable loop holes can be left in the entire network. Cleeff, Pietersand & Wieringa (2009) in their paper "Security implications Of Virtualization: A literature Study" [8] mention that there is a limit to knowing what physical network resources should be, and what should not be virtualized.

Virtual infrastructures can be designed in numerous ways. Paper [1] suggested that virtualization can design our traditional DMZ in three different ways as discussed below.

A. Design 1 - Partially Collapsed DMZ with physical trust zones

Physical servers are separated by physical firewalls. This design is considered to be least complex. The DMZ is divided

into different security trust zones with physical firewalls between each physical server cluster. The virtual machines that are part of the external trust zone are kept on the same server and are separated from the internal trust zone with the help of a physical firewall. Similarly, the virtual machines that are part of the internal trust zone are kept separated with the help of a physical firewall on the same physical server.

B. Design 2 - Partially Collapsed DMZ with virtual separation of trust zones

The trust zones are separated with the help of physical firewalls. However, the design is different from Design 1 in terms of deploying virtual machines. In this design, both, external and internal trust zone virtual machines are kept on the same host. VMware'sESXi server's inbuilt virtual switches are used to enforce separation of trust zones within the design. Each virtual switch has dedicated NICs that are separated from the other NICs on the same physical server, with the help of physical firewalls. Virtual machines that are part of the external trust zone are connected to the external zone's virtual switch. This virtual switch is connected to the dedicated NIC for the external zone on the physical host. Similar configurationsare also done for the internal trust zone. Any communication between external and internal trust zone VMs has to pass through physical firewalls.

C. Design 3 - Fully Collapsed DMZ

A fully collapsed DMZ is the most complex design in terms of designing virtual DMZ trust zones using VMware. In this design, all virtual machines are deployed on the same physical host. Along with the virtual machines, the firewalls are also deployed on the same physical host. This means the firewalls are virtual firewall appliances within VMware'sESXi server. In this design, one NIC of the physical host is dedicated to the internet traffic and the second NIC is dedicated to the production LAN traffic. The external and internal DMZ trust zones do not haveNICs associated with them. They are separated with the help of dedicated virtual switches and virtual firewalls that filter the traffic passing between the two trust zones and the rest of the network

D. Design 4–Traditional Physical DMZ

In a traditional DMZ, the network infrastructure consists of physical servers and physical firewalls. Typically, in a traditional DMZ design the web/FTPserver and the DNS server are separated from the database server with the help of a hardware firewall appliance (physical firewall). The external trust zone servers are connected to a dedicated physical switch and the physical servers, as part of the internal trust zone, are connected to a separated dedicated physical switch.

Consolidating all physical DMZ resources into virtual ones, introduces the risk of managing security trust zones, as VMs are flexible in their placement, with features like live migration and high availability. MacDonald and Young [9] stated that it is possible to collapse all the physical servers into virtual servers, in their research paper "*Server Virtualization can Break DMZ Security*".

IDSs and IPSs have been used as tools to secure data traffic in virtual environments by equipment distributors having designed software-based appliances that can be integrated into the hypervisor like an API application [10]. These appliances provide firewall, IDS and IPS features that are smart enough to understand the underlying virtualization layer, unlike traditional firewalls. In a paper published in 2009 by TrendMicro [11], it was suggested that these appliances can still maintain the integrity of security zones even after the VM is migrated from one host to another. This appliance is called a "coordinated VM watchdog", as it monitors the VM behaviour in the hypervisor.

When designing security zones in virtual infrastructure, MacDonald & Young [9] suggested that each security zone should be completely separated from one another. A dedicated NIC should be used to host one security zone on a physical machine. In situations where limited NICs are available, VLANs can be used to separate security zones with VLAN tagging. However, a dedicated physical NIC is the best option.

III. PROPOSED RESEARCH METHODOLOGY

As part of quantitative research methodology selected, experiments were conducted to perform various tests. The experiments were repeated multiple times. Thus, each treatment was applied to many experimental units instead of just one. By doing so, the statistical accuracy of the experiments was increased significantly. The next section explains the use of vulnerability assessment to conduct experiments with replication.

A. Vulnerability Assessment for Data Collection

This assessment was conducted in a way that would determine the most secure virtual DMZ design deployment. To accomplish this, different virtual DMZ designs, were tested in terms of network vulnerability. The vulnerability assessment and penetration testing methodology approach suggested by Alisherov & Sattarova [12] was modified to collect and analyse data for this research.

Since the authors of the research were the only persons involved in the setup of the experimental test bed and performing various vulnerability assessment tests, white-box penetration testing techniques were used. The scope of the research was limited to vulnerability assessment phase within white-box penetration testing.

B. Methodical Approach to Vulnerability Assessment

The vulnerability assessment experiments, conducted approached the vulnerability assessment process in a sequential way. The following steps describe this iterative methodological approach.

Step 1 – First a particular virtual DMZ design was determined for conducting the experiment.

Step 2 – The place (node) for conducting the experiment was determined. In this case, it was placed outside the designed network, which replicated an internet user.

Step 3–The IP address of the published website was gathered by pinging the website name.

Step 4–A network scan was performed on the subnet to see any other live hosts on the subnet.

Step 5–Network vulnerability assessment tools were used to scan for vulnerabilities on the detected hosts. This test was performed five times to scan for vulnerabilities on each host. This would rule out any inconsistency while collecting data as suggested in principle of replication [13].

Step 6– The collected data was recorded in a benchmark matrix and compared to the expected values of a live host.

Step 7– Return to step 1 for conducting vulnerability assessment on the next design. Continue this process for all the virtual DMZ designs.

IV. VIRTUAL DMZ – EXPERIMENTAL TEST BED

The experimental setup for the research covers the core network design and the technologies that were used to design the experimental setup along with their configuration settings. The core design remained unchanged during the whole research. The variables within this logical network design were the different virtual DMZ designs as discussed.

Five vulnerability assessment tools used to identify which virtual DMZ design was the most secure one were Nmap, Tenable Nessus Vulnerability Scanner, GFI LAN Guard, Shadow security Scanner and X-Scan. These tools were selected based on their exploit database as some of them use exploits based on OVAL (open vulnerability assessment language).

V. DATA ANALYSIS

The following sections discuss the data analysis for each of the individual DMZ designs.

The figures describe each vulnerability parameter and the level of accuracy of detection by vulnerability assessment tools, i.e. the success rate of identifying correct information as a percentage. This means, more the vulnerabilities were detected, the higher the percentage of vulnerability for this parameter and more likely the parameter is to be exploited by malicious users. Sections below discuss these evaluation charts in brief.

A. Design 1 - Partially Collapsed DMZ with physical trust zones

In Figure 1, the percentage of vulnerability for a partially collapsed DMZ, where the trust zones are separated with the help of traditional hardware firewalls, is depicted along the Y-axis. The overall vulnerability for each individual vulnerability parameter was calculated using the data from all vulnerability assessment tools for each virtual DMZ design.

In Figure 1 we can see that the open ports parameter is the biggest security risk within Design 1. The calculated percentage of vulnerability of all tools was as high as 88% for the open ports parameter.

The percentage of vulnerability detected for the route, services and OS fingerprint parameter was analysed and calculated to be 74%, 70% and 69%, respectively. Although these are not as high as the open ports parameter, taken together they can still provide sufficient information to launch an attack.

The percentage of vulnerability for the MAC address parameter was calculated to be 29%, since none of the tools could provide sufficient information regarding the MAC address.

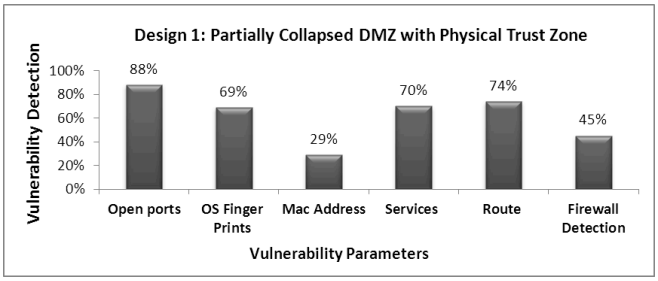

Figure 1: Vulnerability detection of each individual vulnerability parameter in a partially collapsed DMZ with physical trust zone

B. Design 2 - Partially Collapsed DMZ with virtual separation of trust zones

In **Error! Reference source not found.** we can clearly see that the open ports parameter with 85% vulnerability is the easiest parameter to exploit when wanting to hack a server. The OS fingerprint parameter was the second most vulnerable; with 75% as the level of vulnerability and the third highest vulnerable parameter was the services parameter with 70% vulnerability.

The level of vulnerability detection for the route parameter was 15%, as compared to 74% in Design 1. However, the vulnerability detection of firewalls in Design 2 was 50%, which is an increase of 5% compared to Design 1.The scan tools were again accurate in 29% of cases in extracting information of the MAC address.

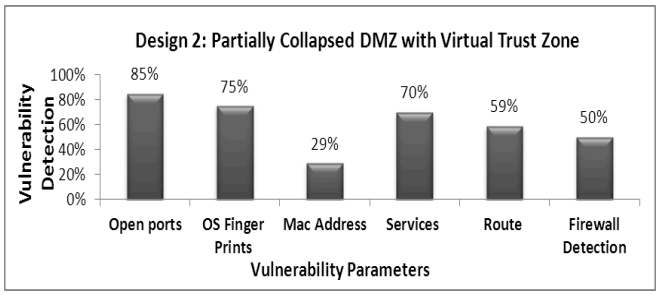

Figure 2: Vulnerability detection of each individual vulnerability parameter in a partially collapsed DMS with virtual trust zone

C. Design 3 - Fully Collapsed DMZ

In a fully collapsed DMZ design, scanning tools extracted information about open ports with an accuracy of 85% (Figure.1). Again, like in all the other DMZ designs, this was the most vulnerable parameter. MAC address information produced by the tools had an accuracy of 29%. The scan tools produced an accuracy level of 75% for the OS fingerprint parameter. This was followed by the services and routes parameter with a vulnerability detection of 69% and 62%, respectively.

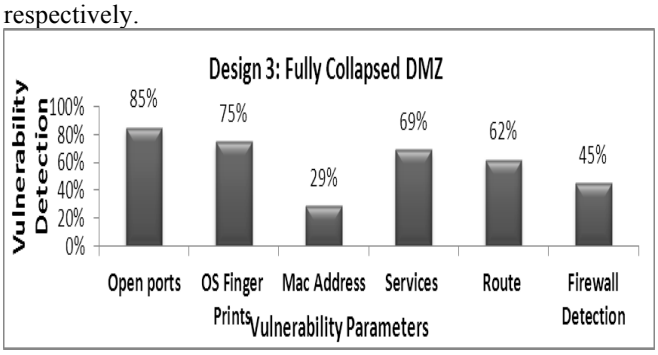

Figure.1- Vulnerability detection of each individual vulnerability parameter in a fully collapsed DMZ

D. Design 4 – Traditional Physical DMZ

As we move to the traditional DMZ design, we can see that the vulnerability detection for open ports was as high as 93% (see Figure 4). Second most accurately detected parameter was the OS fingerprint with a vulnerability detection of 74%. The services parameter was the third most accurate detected parameter with an accuracy of 70%. The scan tools produced unchanged information with an accuracy of 29% in detecting the MAC address, just like in all other DMZ designs. The

scanning tools produced accurate results for the route parameter in 60% of cases and in 45% for the firewall detection parameter.

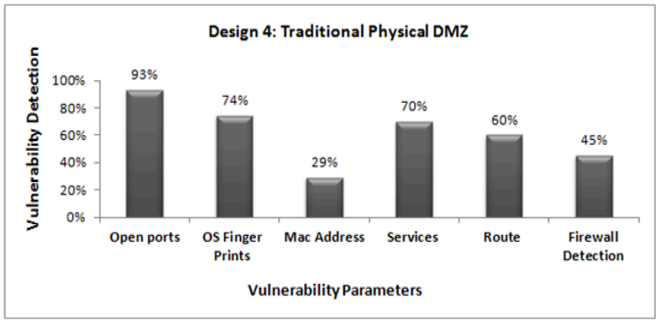

Figure.2- Vulnerability detection of each individual vulnerability parameter within a traditional physical DMZ

VI. Discussion and Conclusion

The aim of this research was to determine which virtual DMZ design would be the most robust to use. From the results of experiments conducted, the findings describe factors that could affect the choice of a particular DMZ design. The risk factor was determined by aggregating the percentage of vulnerability detection discussed in Section 5 for each DMZ design and comparing it with remaining three designs. The aggregated percentage risk factors for the 4 designs were 62.5% for Design 1, 61.3% for Design 2, 60.8% for Design 3, and 61.8% for Design 4. The percentages have been rounded off to the nearest integer value. Based on the data analysis conducted in the previous section, there is only a maximum difference of 1.7% in the vulnerability risk factor between Design 1(most) and Design 3(least). However, the designs could be inferred to vary only about 1% over all four DMZ designs as depicted in Figure 5.

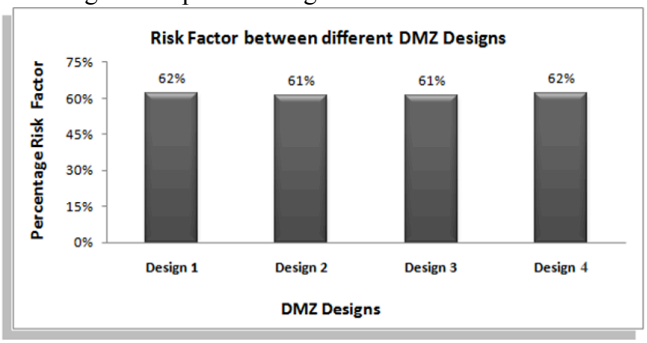

Figure 5- Overall Vulnerability Risk Factor across different DMZ designs

The overall risk factor for Design 1 and 4 was calculated to be 62%, as compared to 61% for Design 2 and Design 3. While Design 1 is the partially collapsed DMZ with physical trust zone, Design 2 is the partially collapsed DMZ with virtual separation of trust zones, Design 3 is the fully collapsed DMZ and Design 4 represents the traditional DMZ.

Based on the results depicted by the experiments conducted in this research, generally all three virtual DMZ designs were equally secure. The difference lies in the implementation of each DMZ design. This includes the way security policies are implemented and the choice of firewall vendors that is reflected in the quality of their filtering mechanisms.

As shown in Figure 6.1 the risk factor of all three DMZ designs is almost equivalent to the risk factor of traditional DMZs. This implies that virtual DMZs are as robust or as weak as traditional DMZs. The implementation of a DMZ design depends greatly on how much money an organization is willing to invest in designing and implementing a virtual solution. The initial cost for implementing a fully virtualized solution can be more expensive since virtualization as a technology is not cheap. Once implemented, organisations can save huge costs, as the overhead management of a virtual infrastructure is less than physical infrastructure based DMZ. Virtualized DMZ requires less hardware resources, therefore in terms of electrical consumption, it is a cost efficient solution.

In this research, the following things could not be considered due to the limited scope of the project and could be further extended by:

- Comparing VMware ESXi's implementation and administration of virtual DMZs with other bare-metal virtualization solutions like Citrix' XenServer, Microsoft Hyper-V; etc.
- Evaluating the security issues introduced by other virtualization solutions to an existing network, as compared to VMware ESXi virtual solution. Compare performance vectors of other virtualization to VMware's ESXi.
- Conduct similar vulnerability assessment tests by placing the web server in a public cloud, i.e. in different datacentres where they provide VPS (virtual private servers).

References

[1] VMware. (2008). DMZ virtualization with VMware Infrastructure. Retrieved fromhttp://www.vmware.com/files/pdf/dmz_virtualization_vmware_infra_wp.pdf

[2] Armbrust M., Fox a., Griffith R., Joseph A., Katz R., konwinski A., Lee G., Patterson D., Rabkin A., Stoica i., Zaharia M. (2010) A View of Cloud Computing. Retrived from http://cacm.acm.org/magazines/2010/4/81493-a-view-of-cloud-computing/fulltext.

[3] Bleikertz, S. (2010). Automated security analysis of infrastructure clouds. Master's Paper, Technical University of Denmark/Norwegian University of Science and Technology, Denmark/Norway.

[4] Hietala, J.D. (2009). Top virtualization security mistakes and how to avoid them- A SANS whitepaper. Retrieved fromhttp://www.sans.org/reading_room/analysts_program/McAfee_Catbird_Virtualization_Jul09.pdf

[5] Sparks, W.J., James, D.G. (2008). Server Virtualization Products and Information Security. Retrieved fromhttp://www.infosecwriters.com/text_resources/pdf/DJames_Virtualization.pdf

[6] Apani. (2009). Securing Physical and Virtual IT Assets Without Hardware Firewalls or VLANs- A New Approach: An Identity-Aware Network Inside the Perimeter. Retrieved from http://www.arrowecs.co.uk/dns_CMS/uploaded. Files/DNS/Security_Solutions/Apani/Apani-Securing-Physical-and-Virtual-Assets-Without-Hardware-Firewalls-or-VLANs%5B1%5D.pdf.

[7] Xianqin, C., Han, W., Sumei, W., Xiang, L. (2009). Seamless virtual machine live migration on network security enhanced hypervisor. DOI: 10.1109/ICBNMT.2009.5347800

[8] Cleeff, A. and Pieters, W. and Wieringa, R.J. (2009) *Security Implications of Virtualization: A Literature Study*. In: 2009 IEEE International Conference on Computational Science and Engineering (CSE09), volume 3, 29 Aug - 31 Aug, Vancouver, BC, Canada. pp. 353-358. IEEE Computer Society. ISBN 978-0-7695-3823-5.

[9] MacDonald, N., Young, G. (2007). Server Virtualization can Break DMZ Security. Gartner Research (ID: G00147785).

[10] Young, G., MacDonald, N., Pescatore, J. (2007). Limited Choices Are Available for Network Firewalls in Virtualized Servers.Retrieved from http://www.reflexsystems.com/Content/News/20071220-GartnerVirtualSecurityReport.pdf

[11] Trend Micro. (2009). Meeting the Challenges of Virtualization Security- A Trend Micro WhitePaper. Retrieved from http://trendedge.trendmicro.com/pr/tm/te/document/wp02_virtsec_090812us.pdf

[12] Alisherov, F.A., Sattarova, F.Y.(2009). Methodology for Penetration Testing. *International Journal of Grid and Distributed Computing*.**2** (2): 43-50.
[13] Kothari, C.R. (2004). Research Methodology - Methods and Techniques.New Age International Publishers, New Delhi..