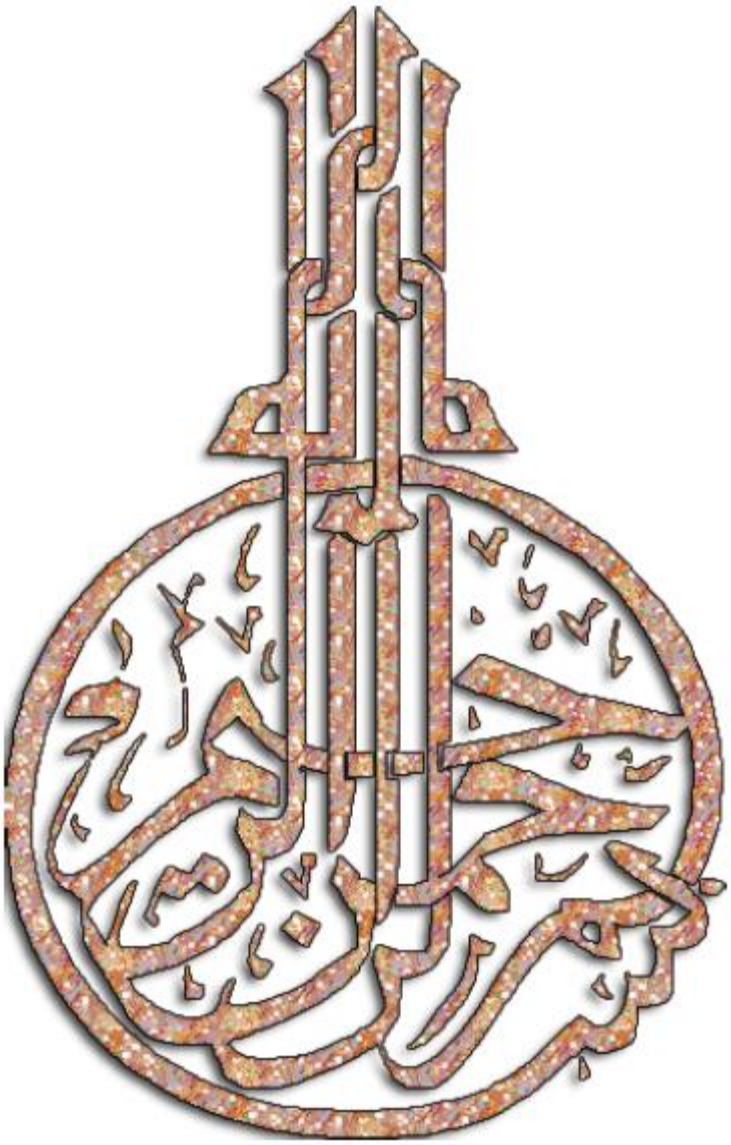
تحليل أمن وأداء الشبكات لتطبق أفضل معمارية لأمن الشبكات

ماجد محمد رحيل العنـزي

بحث مقدم لنيل درجة الماجستير في العلوم
(الهندسة الكهربائية وهندسة الحاسبات / هندسة الحاسبات)

كلية الهندسة
جامعة الملك عبد العزيز - جدة

ربيع الأول ١٤٤٠هـ - نوفمبر ٢٠١٨م



تحليل أمن وأداء الشبكات لتطبق أفضل معمارية لأمن الشبكات

ماجد محمد رحيل العنـزي

بحث مقدم لنيل درجة الماجستير في العلوم (الهندسة الكهربائية وهندسة الحاسبات / هندسة الحاسبات)

إشراف

د. نايف ضيف الله هلال العتيبي

كلية الهندسة
جامعة الملك عبد العزيز
جدة – المملكة العربية السعودية
ربيع الأول ١٤٤٠هـ - نوفمبر ٢٠١٨م

تحليل أمن وأداء الشبكات لتطبق أفضل معمارية لأمن الشبكات

ماجد محمد رحيل العنـزي

المستخلص

يعتبر معيار الحماية ضد الهجمات والمخاطر من أهم الاعتبارات التي تراعى اليوم في شبكات الحاسب، وبصفة عامة تعتمد حماية الشبكة ضد الهجمات والمخاطر على ثلاث ركائز رئيسية وهي: تصميم الشبكة، التجهيزات المناسبة، العنصر البشري المؤهل وعند اختلال أي من هذه الركائز الثلاث ينهار مفهوم الشبكة الآمنة. حيث تهدف الهجمات الرقمية ضد الشبكات إلى تعطيل الخدمات التي تقدمها الشبكة للعملاء وذلك عن طريق تدمير البيانات أو تعطيل عمل الأجهزة الشبكية وعادة ما تكون هذه البيانات والأجهزة الشبكية المهمة داخل مراكز البيانات والتي تعتبر أهم أجزاء شبكات الخادم-العميل. ومن أجل تصميم مركز بيانات آمن، ينبغي إجراء تحليل للمخاطر بهدف العثور على المخاطر التي تنطوي عليها الهجمات المحتملة لتحديد السياسات الأمنية لمركز البيانات. في هذا العمل قمنا باقتراح تصميم شبكي يوفر مستوى أمني عالي لمراكز البيانات مع الحفاظ على أداء الشبكة وذلك بتطبيقنا لمفهوم المنطقة المنزوعة السلاح (DMZ) والشبكات المحلية الافتراضية (VLANs) ثم تقييم التحسن باستخدام تقنية تحليل المخاطر.

وقد قمنا بتصميم ثلاثة شبكات بواسطة GNS3 وتم تصميم التصميم الرئيسي لجميع الشبكات من أربعة خوادم (خادم الويب، خادم البريد الإلكتروني ، تطبيقات الويب ، التحكم في النطاق) وأجهزة الشبكة الأخرى على أساس كل تصميم , تم تصميم الخوادم والمستخدمين

والمتسللين من الأجهزة الظاهرية في VMware Workstation. كل جهاز متصل بـ GNS3 ويتم اختبار الاختراق باستخدام Kali Linux. ثم يتم محاولة استغلال الثغرات من خلال بروتوكولات HTTP وFTP و SMB.

تصميم الشبكة الأولى أقل أمانًا للأسباب التالية: لا تحتوي الشبكة على أي جدار حماية لتأمين حركة المرور. يعتمد الأمر فقط على قائمة الوصول غير الآمنة الخاصة بالموجه بشكل فعال نظرًا لأنها شديدة التعرض لهجمات انتحال (IP) كذلك التصميم غير آمن لأن جميع الخوادم موجودة على نفس الشبكة عند وجود خادم عام متصل بالإنترنت. يكمن الخطر في السماح للأشخاص الغير مصرح لهم بالوصول إلى أي جهاز متصل في نفس الشبكة، وبالتالي يمكن لهم الوصول إلى خوادم أخرى تعتبر خادمًا محليًا.

تصميم الشبكة الثاني هو متوسط الأمان لأنه يحتوي على جدار حماية يقوم بتصفية حركة المرور ويمنع أي حركة مرور غير مرغوب فيها وأنشطة ضارة تحدث في الشبكة.

تصميم الشبكة الثالث يعتبر هذا التصميم مؤمنًا بشكل مسبق، وله جداران واحد هو جدار حماية متعدد الطبقات والآخر جدار الحماية NGFW، ويتم عزل الخوادم العامة في منطقة مختلفة وشبكة فرعية تسمى منطقة DMZ لأن الخوادم يمكن الوصول إليها من خارج الإنترنت وعزلها في منطقة منفصلة يقلل من المخاطر.

وقمنا بفحص المنافذ. لنحصل على قائمة من المنافذ، والتي يمكن استخدامها لمواصلة استهداف خادم الويب. ثم أنشأنا هجومًا مستهدفًا الانظمة الثلاثة السابقة، وقمنا بفحص الهدف باستخدام OWASP-ZAP للعثور على أي ثغرة في الموقع، ووجدنا نقطتين رئيسيتين هما

(CWE-22) و SQL (CWE-89)

وحاولنا استغلال الثغرة، ثم وصلنا إلى موقع الإنترانت من خلال الثغرة الأمنية. بعد التأكد من أن الثغرة traversal Path قابلة للاستغلال، استخدمنا Metasploit للحصول على وصول غير مصرح به إلى الويب.

لقد لاحظنا في تصميم الشبكات الثلاث:

في التصميم الأول: هو اقل امانا، يستطيع المخترق الوصول إلى اي جهاز في الشبكة إذا كان لديه إمكانية الوصول إلى الخادم العام.

التصميم الثاني: هو متوسط الأمان لأنه يحتوي على جدار حماية يقوم بتصفية حركة المرور ويمنع أي حركة مرور غير مرغوب فيها وأنشطة ضارة تحدث في الشبكة.

في التصميم الثالث: يتميز التصميم بجدار الحماية NGFW والذي يمكن أن يمنع هجمات التطبيقات والشبكات ويحتوي أيضًا على الكثير من الميزات مثل تصفية عناوين URL ومكافحة الفيروسات وIPS وما إلى ذلك.

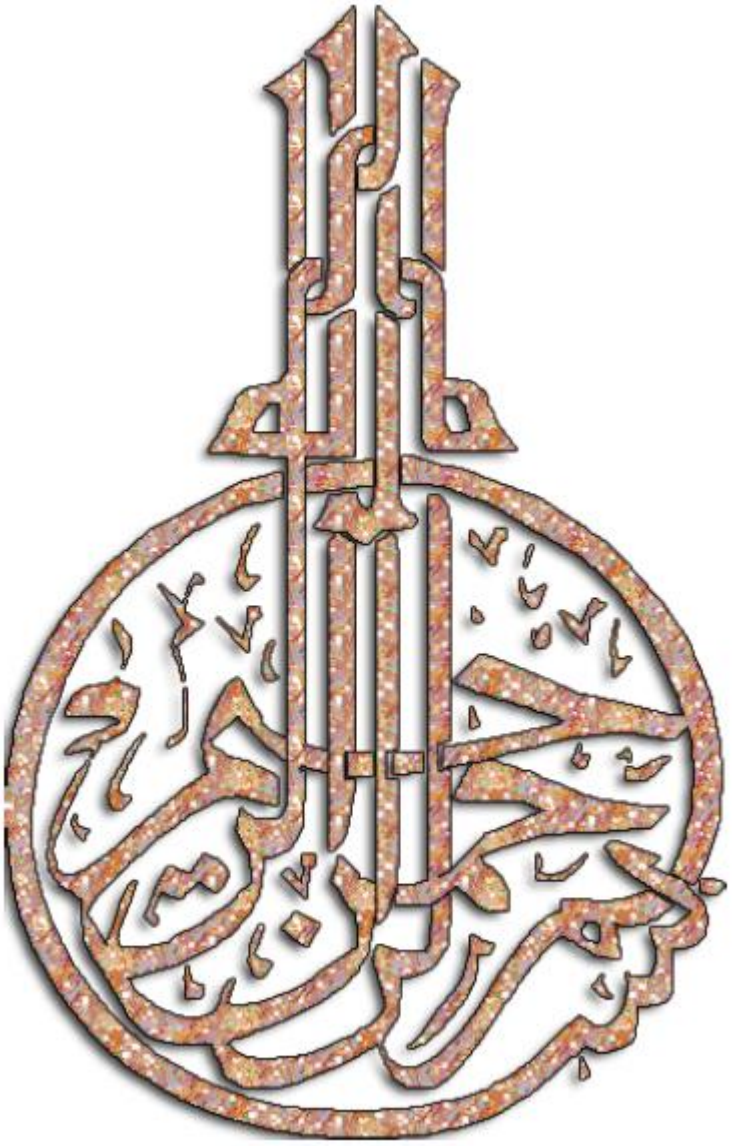
بعد استخراج النتائج توصلنا الى مجموعة من التوصيات وهي يجب عزل جميع الخوادم العامة المتصلة بالإنترنت ووضعها في منطقة DMZ. يجب تكوين جدار الحماية للسماح فقط بالمرور من الإنترنت إلى منطقة DMZ، وإيقاف كل حركة المرور المرسلة إلى الشبكة المحلية, يجب تكوين جدار الحماية للسماح لمستخدمي LAN بالوصول إلى الإنترنت من خلال HTTP و https, يجب وضع جميع مستخدمي الشبكة في شبكات VLAN , يجب أن تكون جميع مواقع الويب وتطبيق الويب آمنًا ويجب إصلاح جميع الثغرات الأمنية التي تم اكتشافها قبل نشر التطبيق. أخيرًا، يجب تأمين خادم الويب من خلال جدار حماية تطبيق الويب لمنع جميع هجمات التطبيقات (حقن SQL، XSS، CSRF وغيرها)

Analyzing security and performance of networks applying different network security architecture best practices

Majed Mohammed Rahil Al - Anezi

A thesis submitted for the requirements of the Degree of Master of Science in
[Electrical and Computer Engineering \ Computer Engineering]

Faculty of Engineering
King AbdulAziz University- Jeddah
RABI' I , 1440 H – November, 2018G



Analyzing security and performance of networks applying different network security architecture best practices

By

Majed Mohammed Rahil Al - Anezi

A thesis submitted for the requirements of the Degree of Master of Science in
[Electrical and Computer Engineering \ Computer Engineering]

Supervised By
DR. NAIF DEAFALLA HILAL ALOTAIBI

FACULTY OF ENGINEERING
KING ABDULAZIZ UNIVERSITY
JEDDAH- SAUDI ARABIA
RABIʾ Ⅰ, 1440 H – November, 2018G

Analyzing security and performance of networks applying different network security architecture best practices

Majed Mohammed Rahil Al - Anezi

Abstract

Today, network security is one of the most prominent issues to be considered in networks. In general, network security depends on three main factors: network design, appropriate equipment, trained personnel. The attacks against network are designed to disrupt network services by either destroying data or disrupting network devices. These data and important equipment are usually contained in what is known as data centres, which are the most important parts of client-server networks. For secure data centre design, risk analysis should be conducted to find the risks involved in potential attacks to determine the security policies of the data centre. In this work, we will propose a network design that provides a higher security level for the data centre not affecting the network performance using a Demilitarized zone concept (DMZ) and virtual LANs (VLANs) then evaluate the improvement by using risk analysis technique.

Through our research, we designed three safety ratings in networks. The network is designed by GNS3 and the main design of all networks is designed from 4 servers (web server, email server, web application, the domain controller) and other network devices based on each design

Servers, users, and hackers are designed for virtual machines in VMware Workstation. Each device is connected to GNS3 and the penetration is tested using Kali Linux on a virtual machine. The penetration is then tested through the HTTP, FTP, and SMB protocols.

The first design is less secure for the following reasons: network does not contain any firewall to secure and filter traffic. It only depends on the unsafe router access list effectively because it is highly vulnerable to IP spoofing attacks. The design is not secure because all servers are on the same network even if there is a public server connected to the Internet. The risk lies in allowing the hacker access to any public server and thus hacker can access other servers that are considered a domestic server.

The second design is an average security because it contains a firewall that filters traffic and prevents any unwanted traffic and malicious activities occurring in the network.

The third This design is considered advance secured design, it has two firewall one is multilayer firewall (stateful) and other is Next

Generation firewall NGFW, and the public servers are isolated in different zone and subnet which is called DMZ zone because the servers are accessible from outside which internet and reduce and mitigate the risks, we isolated it.

We attempted to conduct a port scan. This provided us with a listing of listening ports, which could be used to further target the web server.

We set up a targeted attack against this system, and we scanned the target using OWASP-ZAP to find any gap in the website, so we got, two major weaknesses are Path Traversal (CWE-22), And SQL (CWE-89). We tried to exploit the gap in the path, then we got to the intranet site through the vulnerability. After we make sure that Path traversal vulnerability is exploitable, we used an exploit code in Metasploit to get unauthorized access to the web server.

We have noticed the design of the three networks:

In the first design, Hacker can reach all the machine in the network if he got access to the public server and he can be used the compromised machine to each other, so the Design is not secure.

The second design: it is an average security because it contains a firewall that filters traffic and prevents any unwanted traffic and malicious activities occurring in the network.

In third design: The design has next-generation firewall NGFW which can prevent application and network attacks and has a lot of features such as URL filtering, antivirus, IPS, etc.

By extraction the result we have come up with a set of recommendations. All public servers connected to the Internet must be isolated and placed in a DMZ zone. The firewall must be configured to allow only traffic from the Internet to the DMZ zone, and to stop all traffic sent to the LAN. The firewall must be configured to allow LAN users to access the Internet through HTTP and https. All network users must be placed in VLANs. All websites and the web application must be secure and all security vulnerabilities detected before the application is deployed must be fixed. Finally, the web server must be secured by the web application firewall to prevent all application attacks (SQL injection, XSS, CSRF…etc)