1. Executive Summary

This report provides a comprehensive overview of the penetration test conducted on the systems within the 192.168.56.0 network. The primary goal of the testing was to identify vulnerabilities within the network and propose solutions to mitigate these risks. The scope of the testing included all virtual machines on the network, namely the Axigen Mail Server, Kali Linux (pentest machine) machine, and the Metasploitable Linux machine.

Through various penetration tools including Nmap, Netcat, wget, Nessus, and enum4linux scans, several vulnerabilities were identified across the tested systems. The Axigen Mail Server exhibited vulnerabilities such as SSH integrity checks bypass, whereas the Metasploitable server showcased critical issues like share mounting remotely and cryptographic material predictability. Kali Linux, on the other hand, demonstrated higher security levels with minimal vulnerabilities.

Based on the findings, several recommendations are proposed to enhance the network's security. These include implementing regular updates to patch vulnerabilities, shutting down unnecessary ports to minimize exposure, deploying robust antivirus software, and enforcing strong password policies. Furthermore, configurations should be double-checked to rectify misconfigurations, especially within the Metasploitable server.

Securing the 192.168.56.0/24 network necessitates immediate attention to address the vulnerabilities present, particularly in the highly vulnerable Metasploitable server. While the Axigen Mail Server and Kali Linux machine are relatively secure, proactive measures are recommended to fortify the overall network security and mitigate potential risks.

1. Introduction

The following report presents the results of a penetration test aimed at identifying vulnerabilities within the computing systems encompassed by the 192.168.56.0 network.

The overarching goal of this penetration testing endeavor is twofold: first, to reveal any vulnerabilities present within the network systems, and second, to propose solutions that will remediate these identified vulnerabilities. By thoroughly scanning each system using a variety of testing methodologies, ranging from Nmap and Netcat scans to Nessus vulnerability assessments and enum4linux reconnaissance, I aim to provide a comprehensive overview of the network's security landscape.

Throughout the testing process, the focus remains on understanding the specific vulnerabilities inherent to each system and identifying actionable recommendations to increase their security. By learning of potential risks and offering solutions, this report endeavors to empower stakeholders with the knowledge and insights necessary to fortify the network against cyber threats and mitigate or prevent potential security breaches.

1. Scope

I am targeting all virtual machines on the 192.168.56.0/24 network. This includes:  
192.168.56.101: Axigen Mail Server  
192.168.56.102: Kali Linux (pentest machine)  
192.168.56.103: Metasploitable

I will be performing an Nmap scan, a Netcat scan, a Nessus scan, and an Enum4linux scan.

4. Details

* + 4.1 Nmap Scan

Nmap is a tool used to scan a network and discover more information about it. An attacker would use nmap or a tool like it to see what hosts are in a network and what ports they have open.

-n was used to make the scan ignore the fact that a DNS server was not present. -Pn was used to skip the host discovery process, as I knew all the IP addresses in the network.

* + - 4.1.2 AxiGen

The following ports were found to be open on the AxiGen Mail Server: SSH (22/tcp), SMTP (25/tcp), HTTP (80/tcp), POP3 (110/tcp), IMAP (143/tcp), HTTPS (443/tcp), SMTP Submission (587/tcp), IMAPS (993/tcp), POP3S (995/tcp), and a Custom Port (9000/tcp).

* + - 4.1.3 Kali Linux

The Kali Linux machine where I performed these tests refused the nmap connection.

* + - 4.1.4 Metasploitable

The following ports were found to be open on the Metasploitable Linux machine: Telnet (23/tcp), SMTP (25/tcp), DNS (53/tcp), HTTP (80/tcp), Ill (Ill/tcp), NetBIOS (139/tcp), Microsoft-DS (445/tcp), Rexec (512/tcp), Login (513/tcp), Shell (514/tcp), RMI Registry (1099/tcp), Subversion (1524/tcp), NFS (2049/tcp), FTP (2121/tcp), MySQL (3306/tcp), PostgreSQL (5432/tcp), VNC (5900/tcp), X11 (6000/tcp), IRC (6667/tcp), AJP (8009/tcp), and Tomcat (8180/tcp)

Top of Form

* + 4.2. netcat Scan

Netcat is a versatile tool used for reading from and writing to network connections. It can be used both as a network diagnostic tool and to transfer data across networks. It can scan ports, transfer files, perform network administration tasks remotely and debug networks. Here, I have used the ‘HEAD’ and ‘OPTIONS’ HTTP methods. ‘HEAD’ is used to retrieve the headers of a given resource which can extract important metadata about the resource without loading the entire page. ‘OPTIONS’ is used to check what kind of things you can do with the resource.

* + - 4.2.2 Axigen

The Axigen Mail Server returned the resource’s name and its URL when prompted with the HEAD method.

When prompted with the OPTIONS method, the Axigen Mail Server returned a 401 HTTP response, which means that access to the resource is restricted and requires authentication. It also tells the scanner what server software is being used, which is Axigen Webmail. It reveals the date and time zone of the server, and it lists that the HTTP options that are allowed for interacting with the resource are OPTIONS, GET, PROPFIND, PUT, DELETE, REPORT and MOVE. It also reveals that basic HTTP authentication is required to access the resource.

* + - 4.2.3 Kali Linux

The Kali Linux machine refused the connection for both the HEAD and OPTIONS methods.

* + - 4.2.4 Metasploitable

The Metasploitable Linux machine revealed the machine’s time zone, the exact operating system that it used, which version of PHP that it used (and the fact that it used PHP at all), and the fact that the returned resource was HTML, giving away that it has some kind of web page.

The Metasploitable Linux machine revealed the date, and unlike the Axigen Mail Server which returned a 401 response, it returned a ‘200 OK’ response. This means that it okayed the connection and did not ask for authentication. It reveals the server’s time zone and details that the server is running Apache version 2.2.8 on Ubuntu, with DAV support enabled. It also revealed the length of the content that was returned, and outlines the exact PHP script that the server runs on. A wealth of information about the network has been revealed through Netcat.

* + 4.3 wget Scan

wget is a utility penetration testers use to download files from web servers. The command –no-check-certificate was used when I ran my scans so that I didn’t receive an error, as none of these web servers have certificates and normally wget does not allow you to retrieve files from web servers without one.

* + - 4.3.2 AxiGen

The Axigen mail server returned the code of the webpage that you would see if you went to a website that it was hosted on. This revealed many things, like how the site itself is structured, where images are stored, the source of the images and what programming languages the website uses. For example, through this scan I was able to find that the webpage of the Axigen mail server uses js, or Javascript.

* + - 4.3.3 Kali Linux

The Kali Linux machine refused the request.

* + - 4.3.4 Metasploitable

The Metasploitable Linux machine also returned the code of the webpage that you would see if you went to a website that it was hosted on. Normally, since this machine is not a web server and does not contain any parts that are meant to be facing the internet, only the person who was actually sat the machine would be able to see its main page. But in this case, since I knew the IP address, I was able to reveal the HTML of the screen you first see when you first run Metasploitable, which reveals essentially everything about what the machine itself is used for, as anyone can look up ‘Metasploitable’ and see what they can do with it. But most pointedly, the Metasploitable initial page reveals the default username and password meaning you could remotely get the credentials to log into the machine and do as you please with it.

* + 4.4 Nessus Scan

Nessus is a popular vulnerability assessment tool used to find vulnerabilities and misconfigurations in networks. It has many features tailored to specific vulnerabilities as well. It gives advanced information on every vulnerability that it finds and provides a solution. It also sorts them into categories based on how severe they are, with the highest being ‘Critical’ and the lowest being ‘Info’.

First, I scanned the entire 192.168.56.0 network with Nessus’ Host Discovery feature. It was able to find all three hosts on the network.

Then, I ran a basic Network scan. The Network scan scans the network itself for vulnerabilities.

Finally, I ran a Web App Test scan. The Web App Test scan scans web-facing applications on the machine for vulnerabilities rather than the network.

* + - 4.4.2 AxiGen

When I scanned the AxiGen mail server with Nessus’ Basic Network Scan, it returned 16 ‘High’ vulnerabilities, one ‘Low’ vulnerability and 104 ‘Info’ vulnerabilities.

When I scanned the AxiGen mail server with Nessus’ Web App Test scan, the the AxiGen Mail Server had 20 Info vulnerabilities.

On that scan, I found the following vulnerability to be of note:  
  
SSH integrity checks can be bypassed such that some packets are omitted, resulting in a connection where some security features are downgraded or disabled. This is known as a ‘Terrapin Attack”. (CVE-2023-488795)

* + - 4.4.3 Kali Linux

When I scanned the Kali Linux machine with Nessus’ Basic Network Scan, it returned one high vulnerability, one medium vulnerability, one low vulnerability, and 59 ‘Info’ vulnerabilities.

The Kali Linux machine only had one Info vulnerability when scanned with the Web App Test Scan.

* + - 4.4.4 Metasploitable

When I scanned the Metasploitable Linux machine with Nessus’ Basic Network Scan, it returned ten ‘Critical’ vulnerabilities, six High vulnerabilities, 24 Medium vulnerabilities, 8 Low vulnerabilities, and 126 Info vulnerabilities.  
  
On the Metasploitable machine’s Network scan, I found the following vulnerabilities to be of note:  
Someone scanning the network could mount shares remotely, allowing them to add files to the machine freely. (CVE-1999-0170) (Critical)

A bug in the random number generator of the system has made all of the cryptographic material generated on the machine guessable, so long as you have the private part of the remote key. (CVE-2008-0166) (Critical)  
  
The machine is configured to use medium-strength ciphers, which are very easy to circumvent if you are on the same physical network. (CVE-2016-2183) (High)  
  
On the Metasploitable machine’s Web Apps scan, I found the following vulnerability to be of note:

The Apache Tomcat service could be exploited to read web application files from the machine. If the machine itself allowed file uploads, an attacker could upload malicious JavaServer pages (JSP) code within various types of file types and initiate privilege escalation, allowing them to execute code remotely. (CVE-2020-1745)

* + 4.5 enum4linux Scan

Enum4linux is a tool used for enumerating information from systems, meaning that it is used for reconnaissance and finding out information about a system. It can gather information such as user accounts, share names, group memberships, policies, and more.

I used enum4linux to scan all three machines in the 192.168.56.0/24 network.

* + - 4.5.2 AxiGen

Enum4linux revealed minimal information about the AxiGen server, only giving some possible generic passwords.

* + - 4.5.3 Kali Linux

Enum4linux revealed minimal information about the Kali Linux server, only giving some possible generic passwords.

* + - 4.5.4 Metasploitable

Upon using enum4linux on the Metasploitable web server, several more things were revealed. Usernames belonging to user accounts, group information, shares, the password policy and the operating system information were all exposed.

1. Summary

All in all, the Kali Linux system is the most secure and needs minimal patches or configuration changes. The Axigen server has a few errors that can be solved relatively easily, but the Metasploitable server is insecure to a shocking degree, to the point where it cannot be safely run on a system that is important due to how easy it would be to hack. Important information such as password requirements can be found with ease with the rudimentary penetration testing tools that I have used in my pentest. There are also various misconfigurations and unpatched bugs, lending to the Metasploitable machine being the most vulnerable in the network by far.

1. Recommendations

I have the following recommendations for the network:

1. Regular updates – Many vulnerabilities that are found are results of bugs that have been or are going to be fixed by the vulnerable asset’s owner. Implement a strict update schedule that brings everything in on the machine up to date. Many of the vulnerabilities that I have found on this network can be easily solved with regular updates.

2. Shut down unnecessary ports – If a machine is not using a port, it should not be open. Open ports are like open doors in a building, if they are not serving a use they should be closed, and if they are serving a use they should be monitored with a firewall. An unnecessarily open port could reveal information about the system and allow a remote attacker to read sensitive information on the network. Also, open ports can give away what the machine’s purpose is and other information about the network, which is critical information for a potential attacker.

3. Implement a firewall – A software or hardware-based firewall would monitor traffic on the ports and take actions or record logs if something that should not be happening, happens. Configure a firewall properly such that the necessary ports cannot be exploited and are only being used for their intended functions. A properly configured firewall should block tools like enum4linux from finding out much of anything about a network from a scan.

4. Implement antivirus – A robust antivirus will protect the machines from the many viruses and malware that can be found on the internet. Many modern antivirus tools employ signature-based detection technology, so it is especially important to keep them updated as well.

5. Implement strong password policies – A weak password policy will invalidate all other security measures you take. With weak passwords, an attacker could remotely authenticate to your machine or a service within it and pose as a user that they are not, or even worse, as an administrator, allowing them to wreak havoc or steal data as they please. CISA recommends passwords be at least 16 characters long, be of mixed case letters, numbers and symbols, and be used only once.

6. Double-check configurations – This is mostly a fix regarding the Metasploitable system. Various systems are misconfigured such that they are less secure than they could be. One of these such systems is NFS; the settings for it on the Metasploitable server allow a scanning attacker to remotely mount a share, which allows them to freely add files to the machine. Go into the system’s NFS settings and correct this.

1. Conclusion

To secure the 192.168.56.0/24 network, it is imperative that the Metasploitable server be addressed first as it is currently much too vulnerable to be deployed and faced out towards the internet. The other two machines on the network, the AxiGen Mail Server and the Linux machine are relatively well secured, but they must also be addressed to create a maximally secure network. Be sure to update all systems regularly, close unnecessary ports, implement a firewall, an antivirus, and strong password policies, and check configurations on all machines.

Annex A – References

*CVE*, cve.mitre.org/. Accessed 6 May 2024.

Annex B – Acronyms

**Telnet: A way to remotely access another computer or server.**

**SMTP: Used for sending emails over the internet.**

**DNS: Converts domain names into IP addresses so computers can communicate.**

**HTTP: The foundation of data communication on the World Wide Web.**

**Ill: Likely a typo or an unspecified service.**

**NetBIOS: Used in Windows environments for sharing resources like files and printers.**

**Microsoft-DS: Helps manage resources in a Windows domain.**

**Rexec: Allows a user to execute commands on a remote system.**

**Login: Provides remote login services.**

**Shell: A command-line interface for interacting with a computer's operating system.**

**RMI Registry: Facilitates communication between different Java Virtual Machines.**

**Subversion: Tracks changes in files and coordinates work among multiple users.**

**NFS: Allows access to files over a network.**

**FTP: Transfers files between computers on a network.**

**MySQL: A popular relational database management system.**

**PostgreSQL: An object-relational database management system.**

**VNC: Allows remote desktop access to another computer.**

**X11: A network protocol for graphical user interfaces.**

**IRC: Internet Relay Chat for real-time text messaging.**

**AJP: Facilitates communication between web servers and servlet containers.**

**Tomcat: A web server and servlet container used for hosting Java web applications.**

**SSH: Securely access a remote computer or server.**

**POP3: Retrieves emails from a mail server.**

**IMAP: Accesses and manages emails stored on a mail server.**

**HTTPS: Secure version of HTTP used for secure web browsing.**

**SMTP Submission: Protocol for submitting emails to a mail server.**

**IMAPS: Secure version of IMAP.**

**POP3S: Secure version of POP3.**

**Custom Port: A port number that's been customized for a specific use.**

Annex C – Detailed Results from Tools

A screenshot of a computer

Description automatically generated

A computer code with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated  
A screenshot of a computer

Description automatically generated

A computer screen with white and orange text

Description automatically generated

A computer screen with white text

Description automatically generated

A screenshot of a computer screen

Description automatically generated



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A blue rectangular object with a black stripe

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated  
  
A screenshot of a computer

Description automatically generated

A computer screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated  
  
A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated