International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 945-949 www.ijaem.net ISSN: 2395-5252

Enhanced Security Model for Email Server

Himanshu Sharma

DEPARTMENT OF INFORMATION TECHNOLOGY, MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY, DELHI

Submitted: 01-06-2022 Revised: 10-06-2022 Accepted: 15-06-2022

The article is based on the security-related problems that are any how affecting the Mail Server

And its solutions that have been developed throughout the last years in order to give a remarkable, ultimate and a safer mailing for the expanding internet community of present days.

In today’s world internet is the key to connecting the world in an easy and fast way and almost every single person accesses the internet in their day-to-day life as the internet grows internet-based attack increases.

The development of technologies that is growing rapidly make information sent quickly from one place to another in a very easy way.

The existence of email is very important because it can make people easier to send and collect reports in a few seconds therefore it is necessary to make email server secure.

Domain Name Server (DNS) configuration is also needed for installing Zimbra Mail Server.

When most people use the Internet, they use domain names to specify the website that they want to visit. However, computers use IP addresses to identify different systems connected to the Internet and route traffic through the Internet. The Domain Name System (DNS) is the protocol that makes the Internet usable by allowing the use of domain names.

DNS is widely trusted by organizations, and DNS traffic is typically allowed to pass freely through network firewalls. However, it is commonly attacked and abused by cybercriminals. As a result, the security of DNS is a critical component of network security therefore we need a well protecteddns server so that we can prioritize the security of email server.

I. INTRODUCTION

An email server, or simply mail server, is an application or computer in a network whose sole purpose is to act as a virtual post office. The server stores incoming mail for distribution to local users and sends out outgoing messages. This uses a client-server application model to send and receive messages using Simple Mail Transfer Protocol (SMTP).

An email server may also be known as a mail or message transer agent.

A secure email server is one of the highly critical assets in any organization. A compromised or unsecured email server can have a negative impact on the reputation of the business and may result in legal and financial issues.

Maintaining an on-premise or in a private cloud secure email server is never an easy task. There are many different important points to consider if you are aiming for a secure email server. IT Engineers or administrators in an organization are responsible for running a secure email server, on behalf of the organization. Engineers who work for MSPs are responsible for maintaining a secure email server on behalf of their customers.

STRUCTURE OF PAPER

The paper is organized as follows: In Section 1, the introduction of the paper is provided along with the structure, important terms, objectives and overall description. In Section 2 we have information about the platform and tools we have used. In Section 3 we have the complete information on how to secure the email server. Section 4 tells us about the future scope and concludes the paper with acknowledgement and references.

OBJECTIVES

Securing mail server -Information to be better protected from malicious actors:

1. Encryption: When securing your mail server, make sure you are using secure connections. Encrypt POP3 and IMAP authentication and use SSL and TLS.
2. Mail relay configuration: Avoid being an open relay for spammers by specifying which domains/IP addresses your mail server will relay mail for.
3. Connections and default settings: To avoid DoS attacks, limit the number of connection and authentication errors that your systems will accept. Remove unneeded server functionality by disabling any unnecessary

default settings. Have a dedicated mail server and move other services like FTP to other servers. Keep total, simultaneous, and maximum connections to your SMTP server limited.

4. Access Control: To protect your server from unauthorized access, implement authentication and access control. For example, SMTP authentication requires users to supply a username and password to be able to send mail from the server. Make sure access to your servers is on a need-to-have basis and is shared with as few people as possible.
5. Abuse prevention: Check DNS-based blacklists (DNSBLs) and reject email from any domains or IPs listed on them. Check Spam URI Real-time Blocklists (SURBL), and reject any messages containing invalid or malicious links. Also, maintain a local blacklist and block any IP addresses that specifically target you. Employ outbound filtering and use CAPTCHA/reCAPTCHA with your web forms.

II. RELATED WORKS

A. Linux-

From smartphones to cars, supercomputers and home appliances, home desktops to enterprise servers, the Linux operating system are everywhere.

Just like Windows, iOS, and Mac OS, Linux is an operating system. In fact, one of the most popular platforms on the planet, Android, is powered by the Linux operating system. An operating system is a software that manages all of the hardware resources associated with your desktop or laptop. To put it simply, the operating system manages the communication between your software and your hardware. Without the operating system (OS), the software would not function.

The Linux operating system comprises several different pieces:

1. Bootloader
2. Kernel
3. Init System
4. Daemons
5. Graphical server
6. Desktop Environment
7. Applications

a. Why uses Linux? - Linux has evolved into one of the most reliable computer ecosystems on the planet.

Linux server is free and easy to install and the cost of operating linux machines is very low incomparison to other o.s-based machines.

B. Mail Server Mail Server is a server which its job is to send and receive emails through the internet. A Mail Server can receive emails from clients and send them to another Mail Servers and other clients. In order for a server to function as a Mail Server, Mail Server software is needed which enables System Administrators to create and manage email accounts on the server. There are 3 protocols in Mail Server, Simple Mail Transfer Protocol (SMTP), Post Office Protocol V3 (POP3), and Internet Message Access Protocol (IMAP). The SMTP protocol is responsible for sending emails and handling messages that sent. The POP3 and IMAP protocols are responsible for receiving messages and processing incoming messages.Messages that have been sent by the sender will be collected and stored into one file in mail server database. The grouping is based on the purpose of the email. In an email that is sent, there has been information about the destination of the recipient of the email and the origin of the sender, as well as information like the date and time of sending the email. When the recipient reads the e-mail from the sender, it means that the e-mail recipient has accessed the mail server and reads messages or files stored in the mail server database that are displayed through the application and browser by that user. There are some Mail Server Softwares that can be installed in a server like Zimbra Mail Server, Postfix, and SquirrelMail. There are some advantages a company could get when a company have a Mail Server such as more bandwidth efficient, faster and more efficient, easy to configure, and security can be guaranteed.

C. Domain Name System (DNS) DNS is a system that stores, manages, and processes data information from domains or hostnames and related records. DNS is responsible in translating domains to IP addresses. If the user wants to access google.com, then DNS will look for an IP address from google.com so that the computer can connect with Google. There are some advantages when using DNS like users no longer have to remember the IP Address of a computer, the host name of a computer does not change so that user can Implementation of Zimbra Mail Server 2 remember more easily, and ssers only use one domain name to explore both on the internet and intranet.There are a few types of DNS such as A record which maps hostname to 32-bit IP address (IPv4), AAAA record which maps hostname to 128-bit IP address (IPv6), MX Record which maps domain to mail exchange server, CNAME Record which creates an alias from a domain, and NS Record which mapping domains into one list of DNS servers.

Besides DNS types, there are also DNS Manager such as DNS resolver which makes DNS requests from an application program, Recursive DNS server which searches through DNS based on the request of the resolver, then gives an answer to the resolver, and Authoritative DNS server which responds after recursive searching. The response can be an answer to another DNS server. DNS resolver searches the host address on the HOSTS file. If the host address that was searched for has been found and given, the process is complete. The DNS resolver searches for cache data that has been made by the resolver to store the results of previous requests. If there is, then stored in the cache data and the results are given and completed. DNS resolver searches the first DNS server address specified by the user. DNS server is assigned to find the domain name in the cache. If the domain name searched by the DNS server is not found, then the search is done by looking at the database file (zones) that the server has. If it is still not found, the search is done by contacting another DNS server that is still associated with the server in question. If it has been found then stored in the cache then the results are given to the client (via a web browser).

III. EMAIL SECURITY

Securing Inbound Email Traffic

Encrypting a mail server and encrypting email traffic are actually two different things. A secure email server requires encryption during transfer, encryption of email, and encryption of saved emails.

<u>End User Side Encryption</u>

PGP/MIME and S/MIME are two options for encrypting emails end-to-end. These two options use certificate-based encryption for emails from the moment they are originating from the end user device until they are received on the recipient’s end user device..

S/MIME uses a public key or asymmetric cryptography as well as digital certificates for emails. Certificates help authenticate the email sender.

<u>Authentication Credentials Encryption</u>

All of the leading email server software providers should uses CRAM-MD5, DIGEST-MD5, and GSSAPI for email credentials encryption.

SMTP Submission Authentication is required to properly identify the sender and to ensure that your email server does not become an open relay abused by 3rd parties.

For email in-transit encryption, TLS is the de facto standard. It can and should be used to secure traffic for webmail, IMAP, and any other client access protocols.

<u>SMTP Services</u>

Simple Mail Transfer Protocol (or SMTP) is the protocol of choice used by most email clients to submit messages to an email server as well as emails servers sending / relaying messages from one server to another on their way to their designated user.

Here are the most commonly occurring security issues when transmitting emails:

1. Unauthorized access to your emails and data leakage
2. Spam and Phishing
3. Malware
4. DoS attacks

SSL (Secure Sockets Layer) is a cryptographic protocol developed by Netscape in 1995 designed to provide enhanced security over network communications and it is the predecessor of TLS (Transport Layer Security). Since all SSL versions currently have a lot of known and exploitable vulnerabilities is no longer recommended for production use. Securing transmission with TLS is the current de facto standard: recommended TLS versions are 1.1, 1.2 and, the latest and most secure, 1.3.

SSL/TLS encrypts the messages between the email client and the email server as well as between email servers. If the encrypted SMTP communication is recorded by a malicious third party, that party will only see what seems to be random characters that replace the email content which means your contacts and message data is still protected and unreadable.

<u>DNSBL and URIBL</u>

Domain Name System Blacklist (DNSBL) or Real-time Blackhole List (RBL) is in essence a service that provides a black list of known domains and IP addresses that have a reputation of being a source of spam. Typically mail server software can be configured to check one or more of these listings.

A DNSBL is more of a software mechanism, rather than a specific list. There are many in existence, which use a wide array of criteria that might get an address listed or unlisted: listing the addresses of machines being used to send spam, internet service providers (ISPs) are known to host spammers, etc.

1. The Spamhaus DBL is a service that blacklists domains found in spam messages and listed as having a poor reputation.
2. The URIBL service is a list of domains detected as sending spam email

DNSBL servers are blacklisted as spammers, and when you define a server as one, emails from such servers are automatically dropped.

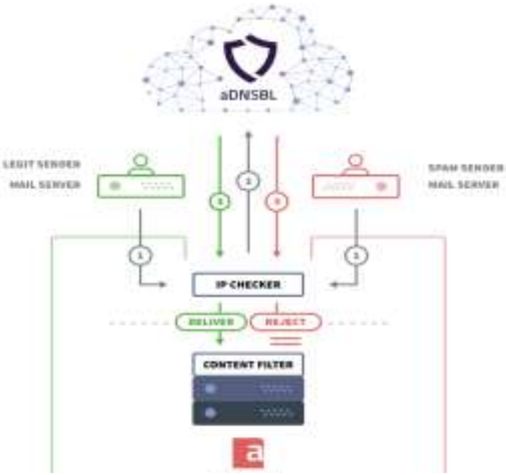

Figure. (1)The DNSBL

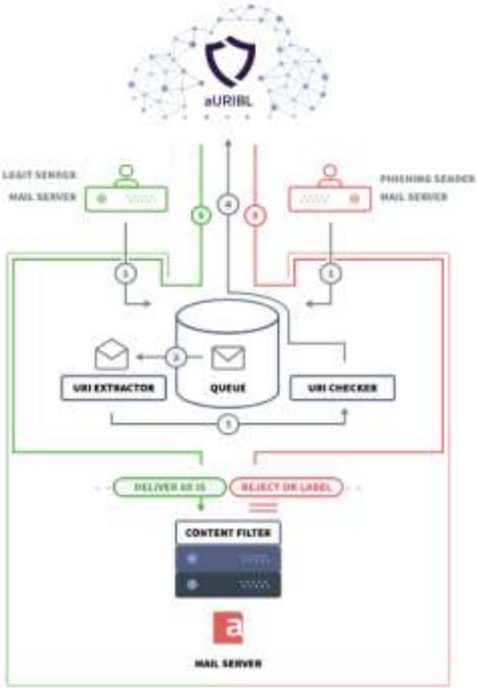

Figure. (2) The URIBL

Content Filtering

Content filters allow you to scan and inspect incoming / outgoing messages and take corresponding actions based on the results automatically. Services such as these mainly scan the content of the email message and decide whether the content matches spam filters and blocks the message from reaching the inbox. Scans also look at image metadata and headers as well as the message text content.

Securing Outbound Email Traffic

Send and Receive Restrictions

Limits can be applied to the messages that are sent by the users you host on your email server. You can control the maximum size that a message can have in its entirety or the size of a message's individual parts or even both of these things. For example, you can control the maximum size of the message header or it's attachments, or set a limit for the maximum number of recipients that a user can add to an outgoing message.

Outbound Spam Protection

Having control over what goes out of your email servers is as important as knowing what comes in. So having a policy to scan the outgoing messages as well as the incoming messages is important because it can stop someone from sending spam messages and as such attracting unwanted repercussions on you.

Securing Mailbox Access

Webmail Two Factor Authentication (2FA)

Making sure your user accounts are secure even though you are probably using SSL/TLS, is important because sometimes user passwords are not the strongest

SSL/TLS Listeners

It is very important that your listeners are configured correctly with good SSL versions and cypher suites

IMAP Encryption and Authentication Recommended Settings

Using an encrypted connection with StartTLS enabled is the best way to ensure that your and your clients data is protected and can't be read by a malicious third party.

Protecting From Brute Force Attacks

A brute-force attack is a type of cyber-attack where a malicious third party tries different passwords and passphrases using an automated script until they find the right combination to gain access to an account or service. It may have been around for a long time, however it is still very popular because of how effective it is against weak passwords, which is why Two Factor

Authentication is an important feature to have on user accounts.

Firewall

One of the critical and truly mandatory network-level security controls is the firewall. A Firewall should have advanced persistent threat analysis features, as they are capable of detecting zero-day security attacks. It is a best practice to run intrusion detection systems (IDS) as well. An email security gateway is required to screen inbound / outbound email traffic.

Firewall filtering rules can be used to deny / allow specific email traffic. This is useful to stop the server from becoming a relay and sending mass spam emails. Packet filtering rules help stop DDoS and DoS attacks.

IV. FUTURE SCOPE AND CONCLUSION

A secure email server essentially has both network and server level security controls. It is a standard practice to configure and maintain your own email server. However, some organizations choose to buy off-the-shelf email server software solutions. If you consider this option, security should be your highest consideration.

There is no completely secure system anywhere in the world. However, some email software solutions provide comprehensive packages covering security at all layers, including network and server levels.

A highly secure email server solution should have:

1. firewall rules
2. secure email gateway
3. server-level controls including encryption, anti-spam / anti-phishing / antivirus, as well as a monitoring, analysis service.

Future Scope

SMTP has a long and illustrious past. It's one of the "killer applications" that led to the explosive growth of the internet. From love letters to stock transactions to family photos, countless users send an endless variety of messages to each other every day. Email in its current form is going to be around for a long time, but will likely undergo a series of incremental updates. For example, client authentication (which didn't exist when the SMTP RFC was written) has almost completely replaced open relaying, and some mail servers now use SSL certificates to verify another server's identity.

ACKNOWLEDGMENT

Foremost, I would like to express my sincere gratitude to My mentor Er. Vibhor Sharma for the continuous support during the project and research paper, for their patience, motivation, enthusiasm, and immense knowledge. Their guidance helped in all the time of research and writing of this paper. I could not have imagined having a better advisor and mentor for my research-based project.

REFERNCES

[1]. A. Gulbrandsen, P. Vixie, A DNS RR for specifying the location of services (DNS SRV), October 1996

[2]. Garrels, M., 2008. Introduction to Linux: A Hands on Guide. s.l.:s.n

[3]. Christensson, P., 2013. Mail Server Definition. [Online]. Available at: https://techterms.com/definition/mail_server

[4]. Prasetiawan, H., 2016. Perancangan Mail Server Zimbra MenggunakanTeknologiVirtualisasiStudiKasus: SMK Pancakarya Kota Tangerang. Jurnal TAM (Technology Acceptance Model), pp. 38-45.

[5]. Hughes, L (1998). Internet E-mail: Protocols, Standards and Implementation. Artech House Publishers. ISBN 978-0-89006-939-4.

[6]. Rhoton, J (1999). Programmer's Guide to Internet Mail: SMTP, POP, IMAP, and LDAP. Elsevier. ISBN 978-1-55558-212-8.

[7]. WWW.ZIMBRA.COM

[8]. Hunt, C (2003). sendmail Cookbook. O'Reilly Media. ISBN 978-0-596-00471-2.