International Journal of Electronics and Communications System
Volume 2, Issue 2, 65-73.
ISSN: 2798-2610
http://ejournal.radenintan.ac.id/index.php/IJECS/index
DOI: *10.24042/ijecs.v2i2.13543*

Application of Domain Keys Identified Mail, Sender Policy Framework, Anti-Spam, and Anti-Virus: The Analysis on Mail Servers

Khairan Marzuki*
Universitas Bumigora Mataram, INDONESIA

Naufal Hanif
Universitas Bumigora Mataram, INDONESIA

I Putu Hariyadi
Universitas Bumigora Mataram, INDONESIA

Article Info

Article history:
Received: August 18, 2022
Revised: November 18, 2022
Accepted: December 30, 2022

Keywords:

Amavisd-Antivirus;
ClamAV;
DKIM;
Server;
SpamAssassin;
SPF.

Abstract

Viruses spread through email are often sent by irresponsible parties that aim to infect email users' servers. This background encouraged the author to analyze the application of DKIM, SPF, anti-spam, and anti-virus to avoid spam, viruses, and spoofing activities. The goal is for the server to prevent spam, spoofing, and viruses to ensure the security and convenience of email users and prevent the impact of losses caused by them. The design and analysis of DKIM, SPF, anti-spam, and anti-virus applications use the NDLC methodology. The process includes designing spam, spoofing, and virus filtering systems and performing installation and configuration simulations. The next stage is implementation, during which the previously developed system is tested on the spam filtering system, spoofing, and viruses. The last stage is the monitoring stage, where supervision is conducted on the approach to determine its success level. This study concludes that applying the DKIM protocol can prevent spoofing through private and public key-matching methods for authentication. Meanwhile, the application of the SPF protocol can prevent spoofing by authorizing the IP address of the sending server. Additionally, SpamAssassin, ClamAV and Amavisd-New can prevent spam and viruses from entering by checking email headers, bodies, and attachments.

To cite this article: K. Marzuki, N. Hanif, and I. P. Hariyadi, "Application of Domain Keys Identified Mail, Sender Policy Framework, Anti-Spam, and Anti-Virus: The Analysis on Mail Servers," *Int. J. Electron. Commun. Syst.,* vol. 2, no. 2, pp. 65-73, 2022

INTRODUCTION

Technology development is currently very rapid, so that technology can facilitate human work in almost all fields. Electronic mail is one of the technological advances in communication and can replace the function of letters. One of the most widely used internet services is e-mail. E-mail is electronic mail based on text files, but with the development of technology, e-mail is more attractive to users[1]–[3]. Cost and time efficiency are the reasons that make many people switch from mail to e-mail[4]. It can send text and audio files, videos, photos and other extension files.

Efficiency of e-mail was also accompanied by many threats[5], [6]. A serious threats accompany the convenience of e-mail by using e-mail as a medium for committing crimes in cyberspace because e-mail is the main means of transporting spam, viruses and malware on the network[7]. A severe threat accompanies the convenience of email by using e-mail as a medium for committing crimes in cyberspace because e-mail is the primary means of transporting spam, viruses and malware on the network [8]–[10]. Spam is unwanted email, spam e-mail is sent to a recipient, and the message is useless to the recipient[11]–[13]. Spam is sent on the network to increase resource consumption, such as network traffic[14], [15]. Only some spam emails enter the spam folder that has been provided[16].

On the other hand, non-spam e-mails sometimes end up in the spam folder, so important e-mails are sometimes not read by e-mail recipients. E-mail is one source of

• **Corresponding author:**
Khairan Marzuki, Universitas Bumigora Mataram, INDONESIA. ✉ khairan.marzuki@universitasbumigora.ac.id

cybercrime activity[6]. One example of a threat from a crime that uses e-mail is e-mail spoofing[5] E-mail spoofing is considered dangerous because it falsifies the data in the email header[17] on behalf of a legitimate person or organization—spoofing e-mail attack with various contents of the message to deceive the victim[3], [18], [19]. E-mail spam, spoofing and viruses are highly, unwanted by users and e-mail service providers, so it is necessary to implement a system to prevent spam e-mail, copying and viruses[20]–[22]. It is hoped that procedures for avoiding spam emails, spoofing and viruses can reduce the impact of losses caused by them [23], [24].

Numerous research trends exist about The Analysis on Mail Servers disaster mapping using bibliometric analysis, including the MAIL SERVER from the perspective of Domain Keys Identified Mail. Firewall security on the Operating System and Mail Transfer Agent Security used. The Mail Transfer Agent used is Zimbra Mail Server [25]. Nurlina and Irmayana investigated emails with the yahoo.com domain and provided a spam folder that utilizes an anti-spam program called Spam-Assassin. This anti-spam program is integrated into the mail server software used [26]. Furthermore, other researchers use Microsoft Exchange, qmail, Exim, and Sendmail as more common among mail server programs. Based on the tests that have been carried out, if you enter the appropriate username and password, you can enter mail and you can send messages or receive messages from the server to the client and the system is able to send or reply to emails from one account to another[27].

However, there are relatively few studies published in credible publications that explore the DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) in authenticating and authorizing e-mail client. There is yet to be be free from spoofing actions of the term "AntiSpam and AntiVirus". AntiSpam and AntiVirus are needed to protect the email server from spam emails and viruses. The method applied by AntiSpam and AntiVirus is by checking the header, body, and email attachments [28].

By offering thorough information on the benefits of implementing DKIM, SPF, AntiSpam, and AntiVirus, this study seeks to cover research gaps, contribute to the research field, and serve as a platform for primary prevention research. This research is also to save mail server resources by blocking electronic mail that is considered spam. To improve the quality of electronic mail security, users can avoid spoofing activities and viruses and malware inserted via electronic mail.

METHOD

Analysis Stage

In this stage, the authors collect data using literature studies. The authors read scientific articles, books, and journals to obtain information about spam emails, email spoofing, and viruses. Furthermore, the data that has been collected is then analyzed. This stage consists of two parts: data collection and analysis.

Data Collecting

The author used the literature study method at the data collection stage by studying several scientific journals discussing email spam, spam, spoofing, and viruses. Besides that, the author also uses e-books concerning email spam, viruses, and spoofing. After reading several scientific journals, information was obtained about several scientific journals related to spam emails, viruses, and email spoofing.

Data Analysis

Based on the data collection results, it can obtain the analysis results. There has been no trial of ClamAV as an anti-virus on the mail server[29]. The results of this analysis encourage the author to research the study of the application of DomainKeys identified mail (DKIM), sender policy framework (SPF), Anti-spam, and AntiVirus on Mail Servers.

Design Stage

This stage consists of 4 (four) parts, namely the design of the spam, virus, and spoofing email filtering system, the trial network design, the IP addressing plan, the email account design, and hardware and software requirements.

Virus dan Spoofing

The design of the spam, virus, and spoofing email filtering system used is shown in Figure 1.

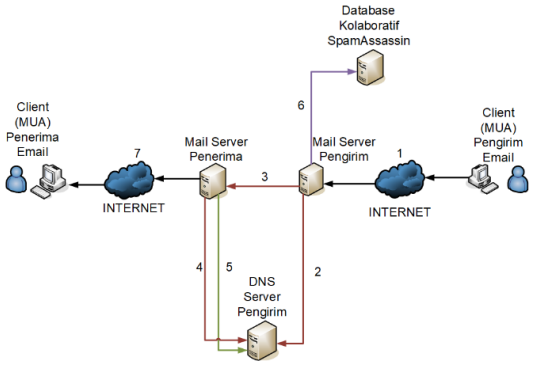

Figure 1. Spam, Spoofing, and Virus Email Filtering System Design

Based on Figure 1, the design of the spam, virus, and email spoofing email filtering system can be explained. Step 1, the user sends an email using a web-based Mail User Agent (Roundcube). The user accesses Roundcube utilizing a browser. Step 2, the sending mail server forwards the email to the mail server. Recipient by adding a private key to the email header. Step 3, the sending mail server publishes the public key on its DNS server. Step 4, the receiving mail server takes the public key on the sending email's DNS server to match the private key in the email header. The email will be considered spam if the private key does not match the public key. If the private key reaches the public key, then the process will continue in step 5. Step 5, the receiving mail server matches the IP address of the sending mail server with the sender ID framework on the SPF record located at the sending DNS server.

If the SPF record is on the sending DNS server m and does not authorize the email server's IP address that sends the email, then the email will be blocked or marked as spam[30]. If the email server administrator has confirmed the sender's email address, then the process will continue on the 6th process. In the Step 6, the recipient's mail server will check the SpamAssassin collaborative database, and the spam email filtering process uses SpamAssassin and ClamAV as anti-spam and anti-virus emails with Amavisd-New as a liaison between the SMTP server and SpamAssassin and ClamAV.

Note: the red line represents the DKIM process (numbers 2, 3, and 4), the green line represents the SPF process (number 5), and the purple line represents the SpamAssassin process (number 6).

Test Network Design

The test network design used is as shown in Figure 2. This design is implemented using a rented VPS from a VPS service provider, and the VPS has installed the CentOS Linux operating system release 7.3.1611. The VPS service provider, 103.112.162.164, gives the VPS that has been rented one public IP address. We will install the CentOS Web Panel, DNS server configuration, and Mail server configuration on the VPS. The client computer has installed the Windows 10 operating system and the Google Chrome browser application to access the web-based Mail User Agent (Roundcube).

IP Addressing Design

IP addressing is necessary because it is an identity-addressing interface. The following is the IP address on each interface to communicate between connected devices, and IP addressing can be seen in the Table 1.

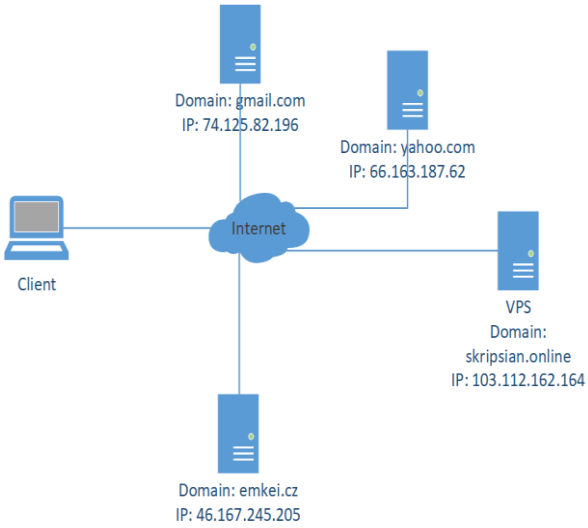

Figure 2. Trial Topology Design Drawing

Table1. IP Addressing

No	Device	IP Address	Network	Interface
1	DNS Server, HTTP Server, SMTP Server, POP3/IMAP Server (VPS)	103.112.162.228/25	103.112.162.128	Eth 0
2	*Client*	DHCP	DHCP	-

Email Account Design

The following are the needs for an email account to support what will be done in building or preparing for implementation, as shown in Table 2.

Hardware and Software Requirements

Here are the hardware and software requirements to support what will be done in building or preparing for implementation.

1. Hardware Requirements

One VPS unit with specifications is shown in table 3. One laptop unit with specifications is shown in the following table 4. Intel Core i3- One laptop unit with specifications as shown in table 4 below. One unit of Intel Core i3 of the laptop with specifications as shown in Table 4.

2. Software Requirements

The software needed is Linux CentOS release 7.3.1611 as a VPS operating system. CentOS Web Panel as a tool to facilitate server configuration, Dovecot as Mail Delivery Agent, Postfix as Mail Transfer Agent, Roundcube as a Mail User Agent, Apache as the web server, Bind9 as the DNS server, Microsoft Windows 10 as the client operating system, and Google Chrome as browser client to access Roundcube.

Table 2. Email Account Requirements

No	Alamat *Email*	*Domain*
1	naufalhanif1477.nh@gmail.com	gmail.com
2	naufalhanif74@yahoo.com	yahoo.com
3	hendarto@skripsian.online	skripsian.online
4	hendarto@ridho.org	ridho.org
5	yunita@skripsian.online	skripsian.online
6	naufalhanif@skripsian.online	skripsian.online

Table 3. VPS Specification

Component	Specification
CPU	*Virtual CPU* a7769a6388d5 1 *Core* (2400 MHz)
RAM	1 GB
Hard Drive	25 GB

Table 4. Client Specification

Instrument	Specification
CPU	7100U, 2.4GHz
RAM	4 GB
Hard Drive	1TB

Simulation Stage (Prototyping)

This stage consists of 2 parts, they are installation and configuration on the VPS and conducting trials using various scenarios. The first trial was carried out by sending spoofing emails through Emkei's Mailer on behalf of one of the users in the riparian. Online domain and then sending the spoofing emails to the Gmail mail server after applying DKIM and SPF to the writings.online mail server. The second trial was conducted to test the performance of AntiSpam on the reports. Online mail server by sending spam emails via Gmail and then sending the spam emails to a user in the Simulation (Prototyping) Stage of the writing.online mail server. The third trial was conducted to test the anti-virus performance on the scripts. Online mail server by sending an email containing a virus via Gmail to one of the users on the writings.online mail server after the application of ClamAV. The third trial compared the email headers sent by one of the users on the reports—online mail server to Gmail after implementing DKIM, SPF, AntiSpam, and AntiVirus.

Installation And Configuration

The installation and configuration of DKIM, SPF, AntiSpam, and AntiVirus is carried out on a VPS that filters incoming spam emails and viruses and prevents email spoofing in the name of a thesis. The Windows 10 operating system and browser have been installed on the client's computer. Google Chrome to access the Mail User Agent Roundcube, the client must be connected to the internet network to access the Mail User Agent provided by the scripts.

Trials

This trial phase consists of 2 parts: configuration verification and testing using various scenarios. Configuration verification is done to verify the DNS server and Mail server functions by performing nslookup. So that it can verify the DNS server function, send emails between users on the built mail server, and send emails from the built server to other email servers to verify the functionality. Mail servers. The test scenarios consist of several procedures, such as testing before the application of spam, virus, and spoofing email filtering and testing after implementing spam, virus, and spoofing email filtering.

Implementation Stage

The implementation stage is the part of implementing the system that has been designed. The system that has been designed can be operated and used optimally according to needs. In addition to the implementation phase, testing of the new system will be carried out, and the new system's shortcomings will be seen for further system development. In this phase, the author will build a mail server. Then on the mail server DKIM, SPF, AntiSpam, and AntiVirus will be applied to filter, authorize, and authenticate email. The author will analyze the mail server before and after DKIM, SPF, AntiSpam, and AntiVirus.

Monitoring Stage

After implementation, the monitoring stage is essential in designing the network design. The purpose of the monitoring stage is to ensure the computer network is running according to the objectives in the analysis stage. In this phase, the author will monitor spam activities in the writings. Online mail server by using the scripts.online mailing server and monitor spoofing activities on Yahoo! Mail, Gmail, and thesis online.

RESULTS AND DISCUSSION

Installation and Configuration Results

Based on the data collection results, it can obtain the analysis results. The first scientific journal discusses email spoofing investigations using the DFRWS method by manually checking email headers. The second scientific journal discusses email spoofing investigations using the header analysis method to find header email spoofing patterns and then create an algorithm to classify email spoofing and legitimate email. The third scientific journal discusses the application of the naive Bayes algorithm on the client side, which will increase the accuracy of spam email detection by 99.98%. The fourth scientific journal discusses filtering important words in email using the Pos Tagger method for learning about the Naive Bayes classification. The fifth scientific journal discusses creating a Mail User Agent application that can filter spam with the Naive Bayes method. Handling email spoofing has not implemented authentication and authorization methods to add information to the email header.

The installation and configuration phase consists of installing the CentOS Web Panel and configuring the Mail server. The server used in this study is a Virtual Private Server that has been rented from a VPS service provider. The VPS IP address provided by the VPS service provider is 103.112.162.228 with the Linux operating system CentOS release 7.3.1611. The VPS has been installed on SSH Server so that the VPS can be accessed via other devices [31] via the internet network, as shown in Figure 3.

CentOS Web Panel Installation Results

CentOS Web Panel makes installing and configuring the server easier because the server installation process will be done automatically. The server configuration process can be done quickly through the web-based CentOS Web Panel configuration page. The installation stage of the CentOS Web Panel contains three commands. The command to enter the src directory, which aims to be the location for storing the CWP installer file with the #cd /usr/local/src command, the command to download the latest version of the CWP installer file with the #wget http:// command. centos-webpanel.com/cwp-latest, the authority to install the downloaded installer file with the command #sh cwp-latest. The results of the CWP installation as shown in figure 4.

Mail Server Configuration Results

To check the mail server function, it is necessary to create an email account on the mail server by entering the Email menu and then selecting the Add Email Account sub-menu, as shown in Figure 5. The DKIM, SPF, AntiSpam, and AntiVirus installation process is carried out on the Email menu, then enters the MailServer Manager sub-menu. Checks the AntiSpam/AntiVirus check box, Install DKIM & SPF, and rDNS Check to install Spam-Assassin, ClamAV, Amavis, DKIM, and SPF, as shown in figure 6. DKIM configuration is done on the Email menu and then entered in the DKIM Manager sub-menu, as shown in Figure 7.

```
[root@ns1 ~]# rpm --query centos-release
centos-release-7-3.1611.el7.centos.x86_64
```

Figure 3. Linux CentOS release 7.3.1611

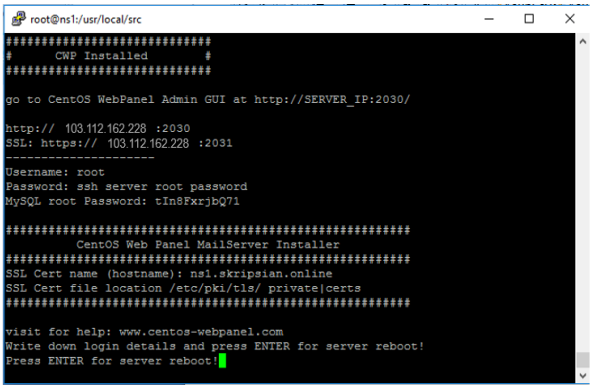

Figure 4. CWP Installation Results

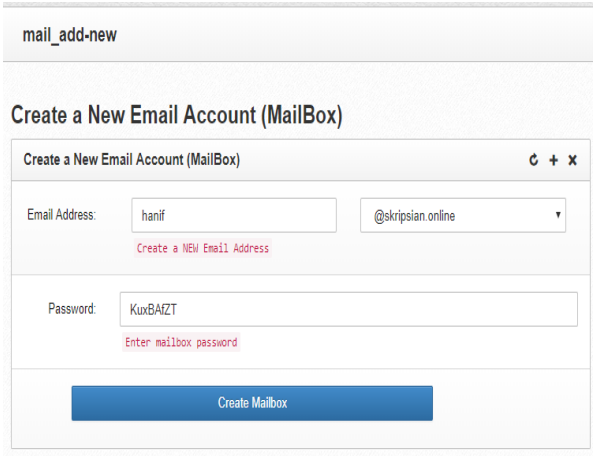

Figure 5. Creating an Email Account

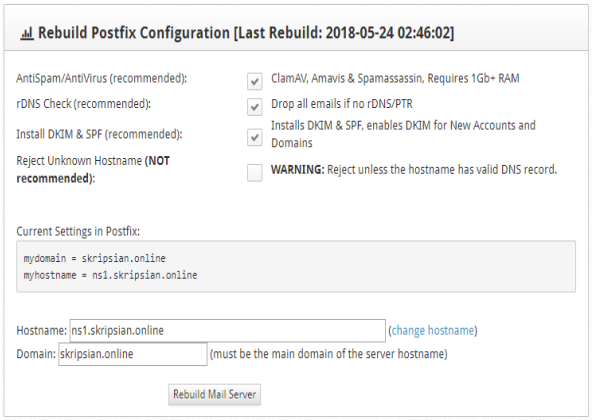

Figure 6. Installing DKIM, SPF, AntiSpam, and AntiVirus

Figure 7. Adding DKIM Records to the Zone File

SPF configuration is done on the Email menu and then entered in the SPF Manager sub-menu, as shown in Figure 8. In the thesis file.online.db, you will see an additional two lines at the bottom, as shown in Figure 9. On line 1 thesis.online. INTXT "v=spf1 mx a ip4: 103.112.162.228/32 a: ns1. thesis. online -all" is an SPF record, v=spf1 means the SPF version used is the SPF version, a: ns1.skripsi.

Online means only allowing sending emails with hostname ns1. thesis.online, ip4: 103. 112. 162. 228/32, which means that it only allows sending emails from servers with IP address 103.112.162.228 -all means rejecting all emails that do not comply with these rules. In line 2 are DKIM records, where parameter v=DKIM1 means the DKIM version used is DKIM version 1, parameter k=rsa implies the type of cryptography used is RSA, and parameter p is the public key used. order ns1. thesis. Online, to be a trusted host, you must add the hostname on line 2 in the TrustedHosts file at the bottom with the command #nano /etc/opendkim/TrustedHosts, as shown in the following Figure 10.

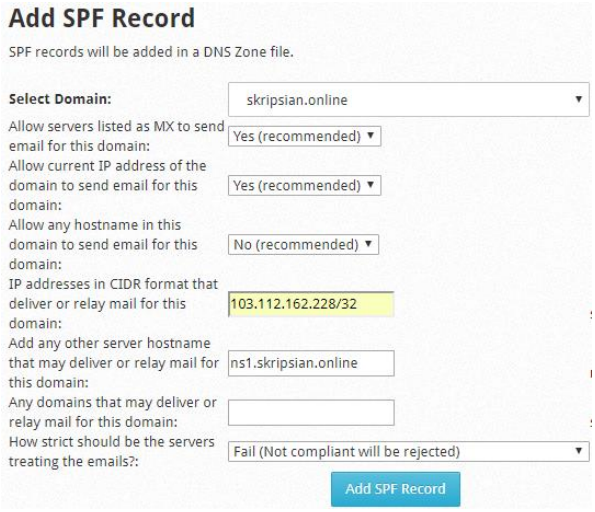

Figure 8. Adding an SPF Record to the Zone File

Figure 9. DKIM and SPF Record

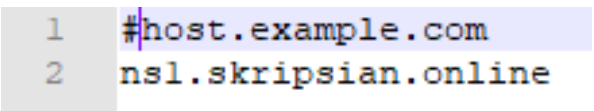

Figure 10. TrustedHosts File Configuration

In the main.cf file, several parameters are added, such as smtpd_milters = inet:127.0.0.1:8891, non_smtpd_milters = $smtpd_milters, milter_default_action = accept, and milter_protocol = 2 which are found in lines 1 to 4 which function to filter email, as shown in figure 11.

Test Results

The tests carried out after filtering, authentication, and email authorization were applied were the trial of sending email spoofing, testing sending spam emails, testing emails containing viruses, and testing email header checking.

Test Sending Spoofing Emails

The trial process of spoofing emails on the email server will be different after the SPF and DKIM protocols are applied to the mail server because the SPF and DKIM protocols will authenticate and authorize every email from the writings. Online mail server. The process occurs after applying the SPF, and DKIM protocols send a spoofing email using Emkei's Fake Mailer. It opens the www.emkei.cz site using a browser, and then on the www.emkei.cz site, the attacker writes the sender's email address. Namely, hendarto@skripsian.online, and the email recipient's address is naufalhanif1477.nh@gmail.com. When the spoofing email passes through the Emkei's Fake Mailer mail server, the spoofing email does not get a private key, only found on the writings. The online mail server looks like Figure 12.

```
1  smtpd_milters = inet:127.0.0.1:8891
2  non_smtpd_milters = $smtpd_milters
3  milter_default_action = accept
4  milter_protocol = 2
```

Figure 11. Main.cf File Configuration

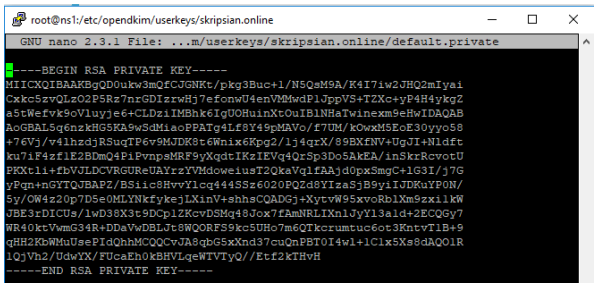

Figure 12. The Private Key on skripsian.online

When the spoofing email enters the Gmail mail server, the email will be considered spam because the email does not have a private key on the scripts.online mail server that matches the public key placed on the scripts.online DNS server, so the message does not have digital signatures in email headers (DKIM processes), which looks like Figure 13 and Figure 14.

The Gmail mail server will check the SIDF (Sender ID Framework) on the DNS server records of writings.online, because the IP address of Emkei's Fake Mailer is 46,167,245,205. The spoofing email is considered spam because the SPF record on the DNS server of writings.online only allows sending email from an authorized address. Namely IP address 103.112.162.228, which is the mail server address of writings.online, and the value of the Received-SPF parameter in the email header is a fail so that the email will be marked as spam email by the Gmail server.

Gmail blocks the spoofing email (SPF process) looks, like the following Figure 15 and Figure 16. Emkei's Fake Mailer mail system receives error code 550-5.7.1 from the Gmail server. Then, Emkei's Fake Mailer mail system sends an error notification[32] to the real user's email address so that the real email user can know that his email has been used by irresponsible people, as seen in figure 17.

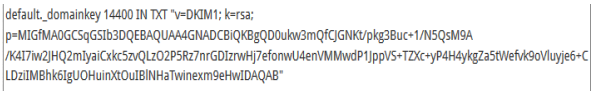

Figure 13. Public key on the DNS Server writings.online

Figure 14. Email Header Snippet

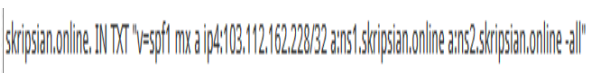

Figure 15. Record image on thesis.online

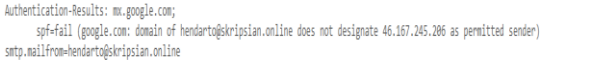

Figure 16. Received-SPF Parameters in Email Header

Test Sending Virus

The test to send an email that contains a virus is done by sending an email with the contents X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-TANDARD-ANTIVIRUS-TEST-FILE!$H+H* which is standard EICAR to perform an anti-virus test on the mail server, emails containing viruses are sent from the Gmail Mail email service to the writings.online email service, as shown in Figure 18.

After the email containing the virus is sent to one of the email users on the scripts.online mail server, the email will be blocked by Amavisd-New because the email has been detected as containing a virus by ClamAV, an anti-virus mail server scripts.online. The way to check that the email has been blocked is to open the mail server log[33] with the command #cat /var/log/maillog, as shown in Figure 19.

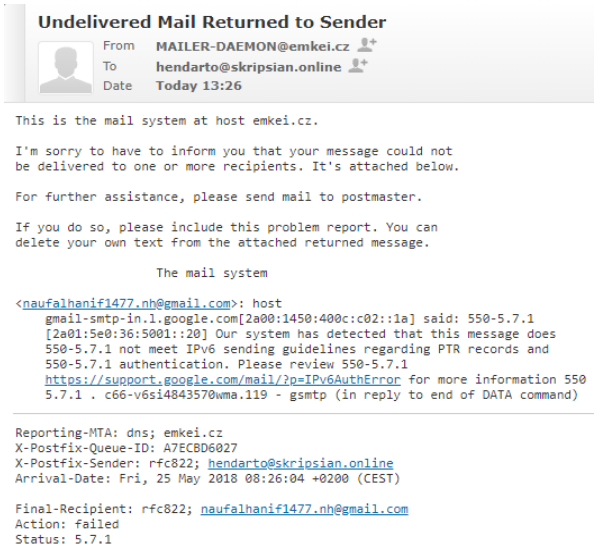

Figure 17. Email from Gmail Indicated as a Spam

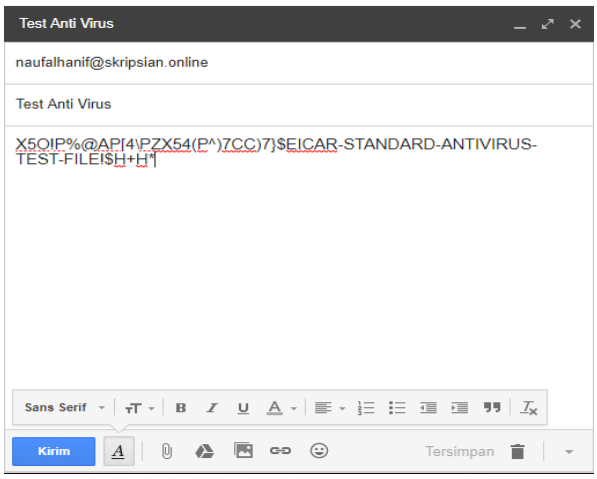

Figure 18. EICAR Test from Gmail

Checking Header Email

This test was carried out by sending an email using one of the email users on the thesis.online email service to one of the email users on the Gmail email service, then check the email header and compare the email headers before and after DKIM and SPF implementation. , anti-spam and anti-virus, the email headers after applying DKIM, SPF, anti-spam, and anti-virus look like Figure 20.

Figure 19. Email from Gmail is Blocked

Figure 20. Snippets of Email Headers in Gmail

Figure 20 shows the difference in email headers after applying DKIM, SPF, and anti-virus. Namely, there are additional X-Virus-Scanned and DKIM-Signature parameters.

CONCLUSION

Based on the results of the experiments that have been carried out, the following conclusions can be obtained: 1) Application of the DomainKeys Identified Mail protocol can prevent email spoofing by authenticating it using the private key and public key (Asymmetric keys) matching method; 2) The application of the Sender Policy Framework protocol can prevent email spoofing by authorizing it using the sending server IP address matching method; 3) The application of SpamAssassin, ClamAV, and Amavisd-New can prevent spam and virus emails from entering by checking the header, body, and email attachments.

SUGGESTION

The suggestions for further development of this research are as follows: 1) Develop an

email spoofing authentication and authorization system by adding the DMARC protocol; 2) Develop an anti-spam system using the SpamAssassin collaborative database, namely Pyzor, Razor2, and DCC and use the blacklist and whitelist features of SpamAssassin to maximize SpamAssassin performance; 3) Develop an anti-spam system by adding other tools such as Barracuda Central, Spamhaus, SpamCop, SORBS, and others.

REFERENCES

[1] S. R. Barley, D. E. Meyerson, and S. Grodal, "E-mail as a source and symbol of stress," *Organ. Sci.*, vol. 22, no. 4, pp. 887–906, 2011, doi: 10.1287/orsc.1100.0573.

[2] L. Stebbins, "Email Is Evolving--Are You ?," no. March, 2016.

[3] F. A. Mir and M. T. Banday, "Control of spam: A comparative approach with special reference to India," *Inf. Commun. Technol. Law*, vol. 19, no. 1, pp. 27–59, 2010, doi: 10.1080/13600831003589350.

[4] S. H. Fisher and R. Herrick, "Old versus new:The comparative efficiency of mail and internet surveys of state legislators," *State Polit. Policy Q.*, vol. 13, no. 2, pp. 147–163, 2013, doi: 10.1177/1532440012456540.

[5] M. Tariq Banday, "Effectiveness and Limitations of E-Mail Security Protocols," *Int. J. Distrib. Parallel Syst.*, vol. 2, no. 3, pp. 38–49, 2011, doi: 10.5121/ijdps.2011.2304.

[6] A. S. Babrahem, E. T. Alharbi, A. M. Alshiky, S. S. Alqurashi, and J. Kar, "Study of the Security Enhancements in Various E-Mail Systems," *J. Inf. Secur.*, vol. 06, no. 01, pp. 1–11, 2015, doi: 10.4236/jis.2015.61001.

[7] S. G. Waghmare and S. A. Pathak, "G LOBAL J OURNAL OF E NGINEERING S CIENCE AND R ESEARCHES," vol. 90, no. C, pp. 90–94, doi: 10.5281/zenodo.1485323.

[8] Y. P. Hoiriyah, Bambang Sugiantoro, "INVESTIGASI FORENSIK PADA E-MAIL SPOOFING MENGGUNAKAN METODE HEADER ANALYSIS," *J. Ilm. DASI*, vol. 17, no. 4, pp. 20–25, 2016.

[9] K. Marzuki and A. Apriani, "Evaluasi Penerapan Teknologi Informasi E-Learning Pada Kampus Swasta Menggunakan Cobit 4.1," *J. Bumigora Inf. Technol.*, vol. 1, no. 2, pp. 161–166, 2019.

[10] S. Hameed, T. Kloht, and X. Fu, "Identity based email sender authentication for spam mitigation," in *8th International Conference on Digital Information Management, ICDIM 2013*, 2013, pp. 14–19. doi: 10.1109/ICDIM.2013.6694015.

[11] H. M. Hamad and W. A. Abudalal, "The Two secured Factors of Authentication," vol. 24, no. 1, pp. 1–13, 2016.

[12] H. P. Shitole and S. Y. Divekar, "Secure Email Software using e-SMTP," *Int. Res. J. Eng. Technol.*, pp. 3967–3971, 2019, [Online]. Available: www.irjet.net

[13] S. Hameed, X. Fu, P. Hui, and N. Sastry, "LENS: Leveraging social networking and trust to prevent spam transmission," *Proc. - Int. Conf. Netw. Protoc. ICNP*, pp. 13–18, 2011, doi: 10.1109/ICNP.2011.6089044.

[14] M. Alazab and R. G. Broadhurst, "Cyber-Physical Security," *Cyber-Physical Secur.*, no. January, 2017, doi: 10.1007/978-3-319-32824-9.

[15] A. G. Gani, "Cybercrime (Kejahatan Berbasis Komputer)," *J. Sist. Inf. Univ. Suryadarma*, vol. 5, no. 1, pp. 16–29, 2014, doi: 10.35968/jsi.v5i1.18.

[16] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A survey of phishing email filtering techniques," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2070–2090, 2013, doi: 10.1109/SURV.2013.030713.00020.

[17] A. Zadgaonkar, S. Kashyap, and M. Chandra Patel, "Developing a Model to Detect E-mail Address Spoofing using Biometrics Technique," *Int. J. Sci. Mod. Eng.*, no. 1, pp. 2319–6386, 2013, [Online]. Available: http://www.commtouch.com/Site/News

[18] A. C. Kigerl, "An empirical assessment of the CAN SPAM Act," *ProQuest Diss. Theses*, p. 112, 2010, [Online]. Available: https://login.pallas2.tcl.sc.edu/login?url=https://search.proquest.com/docview/610183396?accountid=13965%0Ahttp://resolver.ebscohost.com/openurl?c

tx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQuest+Dissertations+%26+Theses+Global&rft_va

[19] M. T. Banday, F. A. Mir, J. A. Qadri, and N. A. Shah, "Analyzing Internet e-mail date-spoofing," *Digit. Investig.*, vol. 7, no. 3–4, pp. 145–153, 2011, doi: 10.1016/j.diin.2010.11.001.

[20] R. Oppliger, "Certified mail: The next challenge for secure messaging," *Communications of the ACM*, vol. 47, no. 8, pp. 75–79, 2004. doi: 10.1145/1012037.1012039.

[21] O. L. Barakat, D. Koll, and X. Fu, "Gavel: A fast and easy-to-use plain data representation for software-defined networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 16, no. 2, pp. 606–617, 2019, doi: 10.1109/TNSM.2019.2903440.

[22] D. Mooloo, "An SSL-Based Client-Oriented Anti-Spoofing Email Application," pp. 1–5.

[23] M. A. Hama Saeed, "Malware in Computer Systems: Problems and Solutions," *IJID (International J. Informatics Dev.*, vol. 9, no. 1, p. 1, 2020, doi: 10.14421/ijid.2020.09101.

[24] L. Cailleux, A. Bouabdallah, and J. M. Bonnin, "A confident email system based on a new correspondence model," *Int. Conf. Adv. Commun. Technol. ICACT*, pp. 489–492, 2014, doi: 10.1109/ICACT.2014.6779010.

[25] H. Mukhtar, Daniel Adi Putra Sitorus, and Yulia Fatma, "Analisa Dan Implementasi Security Mail Server," *J. Fasilkom*, vol. 10, no. 1, pp. 25–32, 2020, doi: 10.37859/jf.v10i1.1906.

[26] N. Nurlina and I. Irmayana, "Studi Banding Spam-Assassin Mail Server Dengan dan Tanpa Filter di Sisi Mail Client," *Creat. Inf. Technol. J.*, vol. 1, no. 2, p. 77, 2015, doi: 10.24076/citec.2014v1i2.12.

[27] A. P. Sari, I. Kanedi, and H. Aspriyono, "Designing Mail Server Using Exchange Server At SMPN 17 Bengkulu City Perancangan Mail Server Dengan Menggunakan Exchange Server Di SMPN 17 Kota Bengkulu," vol. 1, no. 2, pp. 131–138, 2022.

[28] I. P. Hariyadi and K. Marzuki, "Implementation Of Configuration Management Virtual Private Server Using Ansible," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 19, no. 2, pp. 347–357, 2020, doi: 10.30812/matrik.v19i2.724.

[29] R. Chaganti and Y. Marotu, "A study on Clamwin Antivirus software and its Performance Evaluation," no. April 2018, pp. 0–6, 2021, doi: 10.13140/RG.2.2.10842.26562.

[30] Proofpoint, *August 2016*, no. August. 2016. doi: 10.1162/leon_r_01372.

[31] L. E. Wurdiana Shinta, "Plagiarism Checker X Originality Report," *J. Edudikara*, vol. 2, no. 2, pp. 3–5, 2021.

[32] P. Verma, A. Goyal, and Y. Gigras, "Email phishing: text classification using natural language processing," *Comput. Sci. Inf. Technol.*, vol. 1, no. 1, pp. 1–12, 2020, doi: 10.11591/csit.v1i1.p1-12.

[33] G. N. Concepts, *Network security 3*. 2011. doi: 10.1016/B978-1-59749-594-3.00003-X.