University of Essex | Online

Computing Department

MSc Cyber Security Project

Can Open-Source Anti-Spam Tools Be Repurposed to Provide a Tool to Prevent Spear Phishing and To Inform Users of Attacks?

Mohonee Kalina

Supervisors: Prof. Douglas Millward
Dr Oli Buckley

January 16, 2023

Declaration

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where states otherwise by reference or acknowledgment, the work presented is entirely my own.

Abstract

Phishing attacks are a severe concern for organisations of all sizes. These targeted cyber-attacks are designed to trick individuals into disclosing sensitive information or accessing malicious websites, often by pretending to be a legitimate source, such as a bank or a colleague (EZMarketing, 2021). These attacks can have significant financial repercussions for companies and damage their reputation and brand. As spear phishing attacks become more common and sophisticated, organisations must adopt effective email security measures to protect against these threats (Aslam, 2015). The aim of this paper is to provide insights on how phishing emails work and how they can be detected and blocked with open-source software. This paper will be accompanied with a full email system to demonstrate different scenarios to help consolidate my points. Consequently, users' attention will be caught whenever emails are received, and they can decide whether to trust the source of the mail and whether the mail should be opened or not.

Key words: phishing, open-source, email

Acknowledgements

I would first like to thank my supervisor Prof. Douglas Millward of the Computing department at University of Essex. Prof. Millward was always ready to help whenever I ran into trouble or had a question about my research or writing. He continuously allowed me to write this paper on my own, but he gave me advice when he believed I needed it.

I would also like to thank Dr Oli Buckley of the Computing department at University of Essex as the second reader of this thesis, and I am gratefully indebted to him for his very valuable comments on this thesis.

Finally, I must express my very profound gratitude to my parents, sister and to my friends for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them.

Table of Contents

List of Figures

List of Tables

1 Introduction

In this chapter, the risks of phishing and how the project will be developed will be looked into.

Phishing attacks are often initiated through email and may use various tactics to trick the recipient. For example, the email may come from a legitimate organisation, such as a bank or a government agency (Shearn, 2019). It may include a sense of urgency to pressure the victim into taking immediate action. The email may contain a link that appears to be legitimate but that takes the victim to a fake website designed to capture their login credentials or other sensitive information. In addition to email-based phishing attacks, attackers may also use social media or other online platforms to carry out phishing attacks. For example, an attacker may create a fake social media profile and use it to send friend requests to a large number of people. Once a victim accepts the friend request, the attacker can send the victim a message containing a malicious link or attachment.

Phishing attacks can be highly effective, as they rely on social engineering techniques to manipulate victims into divulging sensitive information (Usharani, 2022). For example, an attacker may send an email that appears to come from a trusted friend or colleague and that asks the victim to click on a link or download an attachment. In many cases, victims may not realize that they have been targeted until it is too late, and their sensitive information has already been compromised.

Recently, many of my co-workers have been warned by our IT Security team, who was carrying out a survey on Cyber-attacks at work. The team sent some mails using other email addresses and many of my colleagues were easily fooled and were caught clicking on links and opening attachments sent to them by unknown and untrusted sources. After some days, the entire staff received emails from the IT Security team stating that many of the co-workers downloaded content from suspicious parties. Despite being in the IT field, many of us are not aware of the dangers associated when opening attachments and clicking on links sent to us. Consequently, sensitive data stored on our machines can be lost or compromised. This incident pushed different teams in office to work on awareness cyber-attacks sessions so as to make sure the staff is well aware of the dangers associated with these attacks and how to deal with them. Regular surveys are sent to staff, and they are reminded of the dangers. This motivated me to do my project around phishing and how users can be educated about these attacks.

Risks of phishing

Phishing attacks pose a significant risk to individuals and organisations because they can result in the loss of sensitive information, financial damage, identity theft, damage to devices, and reputational damage (Hashemi, 2016). If a user falls for a phishing attack and reveals his financial information, an attacker may be able to use it to make unauthorized purchases or steal his money. This can result in significant financial loss, especially if the attacker can access a large amount of money.

Identity theft is another serious risk of phishing attacks. If an attacker obtains a user’s personal information, they may be able to use it to steal his identity and commit crimes in his name. This can have serious consequences, including damage to his reputation and legal problems. Some phishing attacks may try to download malware onto one’s device, which can damage or compromise it (Khandelwal, 2022). This can result in the loss of important files or the inability to use the device until it is repaired. This could include losing confidential data, damaging the company’s reputation, and causing financial losses, consequently losing business and customer trust, which can seriously affect the organisation (Zurier, 2016).

Having considered the dangers of phishing, this project will help in filtering mails and educating users. A Waterfall model approach will be used to address spear phishing threats since the requirements of the system is already set and there will be minimum client intervention. This structured, linear approach involves five key steps: gathering requirements, designing a solution, implementing it, testing it, and maintaining it over time. The different sections which will be covered are:

Section 2: Literature Review where background, examples of phishing, types of phishing and technologies used in phishing will be discussed.

Section 3: Methodology will demonstrate how the tool for the project is developed using open-source anti-spam tool.

Section 4: Critical Review of the system

Section 5: Evaluation & Results, demonstrating how the system implemented is blocking and spam mails and analysing different scenarios of attacks.

Section 6: Conclusion, discussing what worked well and some of the future works.

2 Literature review

In this chapter, current approaches to the education of phishing will be addressed. First, an overview about phishing attack, what is it, why people fall for phishing, forms of phishing threats, and negative impact of security scams will be addressed. Next, countermeasures to reduce phishing threats both user education and filtering approaches will be discussed.

2.1 Background

The first known phishing attack occurred in the mid-1990s when attackers used email to trick AOL (aka America Online) users into giving away their login credentials. These early phishing attacks were relatively simple and easy to detect. They often contained numerous spelling and grammar errors and used noticeable, generic subject lines such as “urgent account update (Kalio, 2022). As the internet and email usage became more widespread in the late 1990s and early 2000s, phishing attacks became more sophisticated and challenging to detect. Attackers began using more personalized, targeted attacks, and they also began using social engineering techniques to manipulate victims into giving away their information.

One of the most famous phishing attacks occurred in 2005 when attackers targeted the financial services firm Morgan Stanley employees. According to Kalio (2022), the attackers sent personalized emails to employees, claiming to be from the company’s human resources department and requesting that the employees update their personal information on a fake website (Kalio, 2022). The employees who fell for the scam ended up giving away their login credentials, allowing the attackers to access the company’s systems and steal sensitive financial data.

Over the years, phishing attacks have become even more sophisticated and difficult to detect (Kalio, 2022). Today, attackers use a variety of tactics to trick victims, including creating fake websites that closely mimic real ones, using complex, hard-to-spot URLs, and even impersonating trusted organisations or individuals. They may also use malware or other malicious software to access a victim's device or steal sensitive information.

Spear phishing is a cyber-attack targeting specific individuals or organisations (Suganya, 2016). Unlike regular phishing attacks, which are indiscriminate and often sent to large numbers of people in the hope of tricking at least a few of them into giving away sensitive information, spear phishing attacks are carefully tailored to the specific victim (Nayab, 2015). This makes them much more difficult to detect and defend.

The term "spear phishing" was coined in 2006 when hackers used this technique to steal sensitive information from the Pentagon (Kalio, 2022). Since then, spear phishing has become a significant problem for businesses and organisations of all sizes. According to the Anti-Phishing Working Group, more than 100,000 reported spear phishing attacks in 2019 alone.

Below are some examples of standard phishing emails:

1. "Your account has been compromised": This type of phishing email may claim that a user's account has been compromised and that he must take immediate action to protect it (Fatima, 2019).
2. "You have received a package": This phishing email may claim that the user has received a package and ask him to click on a link to track it or provide personal information to receive the package.
3. "There is a problem with your account": This type of phishing email may claim a problem with the user's account, such as an overdue bill or a suspicious charge. The email may ask the user to click on a link or provide personal information to resolve the issue.
4. "You have won a prize": This type of phishing email may claim that you have won a prize, such as a gift card or a trip, and ask you to click on a link or provide personal information to claim your prize.

5. “You have a new message”: This phishing email may claim that a user has a new message or notification and ask him to click on a link to view it (Hebert, 2022). The link may take the user to a malicious website or ask him to provide personal information.
6. “Your account will be closed”: This type of phishing email may claim that your account will be closed unless you take immediate action, such as clicking on a link or providing personal information.

It is essential to be cautious when receiving any of these emails and to verify the message’s authenticity before responding. When receiving an email that seems suspicious, it is always a good idea to contact the organisation or individual directly using a phone number or email address you know to be legitimate.

2.1.1 Types of phishing

Several types of phishing include clone phishing, spear phishing, and web spoofing. Clone phishing is an attack in which the attacker creates a duplicate of a legitimate website or email to trick the victim into entering their personal information on the fake site (Nayab, 2015). The attacker typically sends a link to the fake site in an email, purporting to be from a legitimate organisation. When the victim clicks on the link, they are redirected to the affected area, which looks identical to the legitimate site. The victim may then enter their login credentials or other sensitive information, which the attacker can use to gain access to their accounts.

Whaling

One type of phishing attack is called “whaling,” which targets high-level executives or individuals with significant authority or access within an organisation.

In a whaling attack, the attacker will often use a combination of tactics to convince the target to give away sensitive information or take a specific action, such as clicking on a link or opening an attachment. These tactics may include impersonating a trusted individual or organisation, creating a sense of urgency or importance, or using official-looking documents or graphics to create a sense of legitimacy (Nayab, 2015). One standard method of whaling is known as “CEO fraud,” in which the attacker impersonates the CEO or another high-ranking executive and sends an email to an employee requesting sensitive information or directing them to take some action. The email may appear to be from a legitimate email address and may contain seemingly legitimate content, such as company logos or language that seems to be authentic.

Another tactic that attackers may use in a whaling attack is “spear phishing,” in which the attacker targets a specific individual or group with a personalized attack (Nayab, 2015). It may involve gathering information about the target’s interests or professional background to create a more convincing attack.

To protect against whaling attacks, it is essential for individuals to be vigilant and to carefully verify the authenticity of any requests for sensitive information or actions. It may involve checking with a trusted colleague or supervisor before taking action or providing any information (Suganya, 2016). It is also vital for organisations to have robust security protocols in place, such as email authentication measures and employee training programs, to help prevent these types of attacks.

In addition to the risk of financial loss or identity theft, a prosperous whaling attack can also have significant consequences for an organisation (Suganya, 2016). It can compromise the confidentiality of sensitive information, disrupt business operations, and damage the organisation’s reputation. Therefore, it is crucial for individuals and organisations to be aware of the risks and to take steps to protect themselves from these types of attacks.

Vishing

Vishing and phishing are forms of cybercrime that involve using fake emails or websites to trick people into divulging sensitive information or installing malware (Suganya, 2016). Vishing, also known as voice phishing, is a type of social engineering attack that uses voice calls or voice messages to manipulate individuals into giving away sensitive information, such as passwords, credit card numbers, or personal identification numbers (PINs) (Webe, 2018). Vishing attacks often involve automated phone systems that mimic the voice and branding of legitimate organisations, such as banks or tech support. The attacker may also use pretexting or create a fake identity or story to gain the victim’s trust.

Both vishing and phishing attacks can be challenging to detect, as they often use sophisticated tactics to mimic legitimate communication (Webe, 2018). It is essential for individuals to be cautious when giving out sensitive information and to verify the authenticity of emails and websites before entering personal information or clicking on links.

To protect against vishing and phishing attacks, individuals can take the following precautions:

- Be suspicious of unsolicited phone calls or messages, even if they appear to be from a legitimate organisation (Webe, 2018). Do not give out personal information or account numbers in response to these calls or messages.
- Do not click on links in emails or texts from unfamiliar sources. According to Webe (2018), if you are unsure whether an email or text is legitimate, contact the organisation directly using a phone number or website that you know is legitimate.
- Enable two-factor authentication on your accounts, which requires an additional verification step when logging in. Webe states that this can help protect against attackers who may have obtained your password through a phishing attack.
- Use a password manager to create and store strong, unique passwords for each account.
- Keep your operating system, web browser, and antivirus software up to date with the latest patches and updates (Webe, 2018). These updates often include fixes for vulnerabilities that can be exploited in phishing and vishing attacks.

HTTPS phishing

HTTPS phishing, also known as SSL phishing or HTTPS spoofing, is a type of cyber-attack that uses fake websites that appear legitimate to trick individuals into entering sensitive information or installing malware (Nayab, 2015). These fake websites are designed to mimic legitimate websites and use the HTTPS protocol to encrypt the data transmitted between the website and the user’s device. It can make it difficult for users to differentiate between legitimate and fake websites, as HTTPS often implies that the website is secure.

There are several methods attackers may use to conduct HTTPS phishing attacks:

- Using a fake SSL certificate: Attackers may use a fake SSL certificate to create a fake website that appears legitimate. SSL certificates encrypt data transmitted between a website and a user's device and are typically issued by trusted certificate authorities (CAs) (Nayab, 2015). However, attackers can create fake SSL certificates and use them to create fake websites that appear to be legitimate.
- Obtaining a valid SSL certificate: In some cases, attackers may obtain a valid SSL certificate for a fake website through phishing attacks or other means (Nayab, 2015). It can make it difficult for users to distinguish between legitimate and fake websites, as a valid SSL certificate implies that the website is secure.
- Hijacking legitimate websites: Attackers may also use HTTPS phishing to hijack legitimate websites by replacing the website's content with a fake version (Nayab, 2015). This type of attack can be complicated to detect, as the website's URL and SSL certificate remain unchanged.

To protect against HTTPS phishing attacks, individuals can take the following precautions:

- Be cautious when entering sensitive information on websites. Verify the website's authenticity before entering personal information or making a purchase.
- Look for the padlock icon in the address bar, indicating that the website uses HTTPS. Note that the presence of HTTPS does not guarantee that a website is legitimate.
- Install browser extensions, such as HTTPS Everywhere that automatically connect to websites using HTTPS when available.
- Use a password manager to create and store strong, unique passwords for each account.
- Keep your operating system, web browser, and antivirus software up to date with the latest patches and updates (Nayab, 2015). These updates often include fixes for vulnerabilities that can be exploited in HTTPS phishing attacks.

It is essential to remain vigilant and cautious when using the internet, as HTTPS phishing attacks and other cyber-attacks can be challenging to detect. Following best practices and taking precautions can help protect yourself against these attacks.

Pop-up phishing

Pop-up phishing, also known as browser-based phishing, is a type of cyber-attack that uses fake pop-up windows or advertisements to trick individuals into divulging sensitive information or installing malware (Nayab, 2015). These fake pop-ups are often designed to mimic legitimate websites. They may appear as notifications, alerts, or warnings, creating a sense of urgency that prompts the user to take action.

Pop-up phishing attacks often occur when a user visits a compromised website or clicks on a malicious link (Suganya, 2016). The attacker may use a variety of tactics to trick the user into interacting with the fake pop-up, such as claiming that the user's device has been infected with malware or that the user needs to update their software (Nayab, 2015). The user may be prompted to enter sensitive information, such as login credentials or credit card numbers, or download a file containing malware.

To protect against pop-up phishing attacks, individuals can take the following precautions:

- Be cautious when interacting with pop-ups or ads, even if they appear to be from a legitimate source. Do not enter personal information or click on links in response to these prompts.
- Use a reputable pop-up blocker to prevent pop-ups from appearing in your browser.
- Keep operating system, web browser, and antivirus software up to date with the latest patches and updates. These updates often include fixes for vulnerabilities that can be exploited in pop-up phishing attacks.
- Do not download files from unfamiliar websites or sources.
- Enable two-factor authentication on your accounts, which requires an additional verification step when logging in. This can help protect against attackers who may have obtained the user's password through a phishing attack.

It is essential to be vigilant when using the internet and to be cautious when interacting with pop-ups or ads.

SMS phishing

SMS phishing, also known as “smishing,” is a type of online scam that involves sending a text message (SMS) that appears to be from a legitimate source but is controlled by a cybercriminal (Suganya, 2016). An SMS phishing attack aims to trick the recipient into providing sensitive information, such as passwords, credit card numbers, or personal identification numbers (PINs).

SMS phishing attacks can occur in a variety of ways. For example, an attacker may send a text message claiming to be from a bank or government agency and ask the recipient to click on a link or provide personal information (Nayab, 2015). The link or website may look legitimate, but it is controlled by the attacker and is used to steal the victim’s statement.

Another common tactic in SMS phishing attacks is to send a message claiming to be from a famous company or service, such as a ride-sharing app or a streaming service and ask the recipient to update their account information (Suganya, 2016). The message may contain a link that takes the victim to a fake website that looks like the real thing but is controlled by the attacker.

SMS phishing attacks can be challenging to detect, as the messages often look and feel like legitimate texts from trusted sources (Suganya, 2016). However, there are some tell-tale signs that you can look for to protect yourself from these scams. These include:

1. Unsolicited text message: SMS phishing attacks often come in the form of an unsolicited text message from an unknown sender (Suganya, 2016). Be cautious before responding if you receive a letter from someone you don’t know.

2. Urgent or threatening language: SMS phishing attacks may use critical or threatening language to get you to act quickly (Suganya, 2016). For example, an attacker might say that your account will be closed if you don’t respond immediately.

3. Request for personal information: An SMS phishing attack may ask you to provide personal information, such as passwords, credit card numbers, or social security numbers (Suganya, 2016). Be cautious about giving this information in response to an unsolicited message.

4. Incorrect branding or logos: An SMS phishing attack may use symbols or branding that appears to be from a legitimate source (Suganya, 2016). Upon closer inspection, you may notice that the logo is slightly off or the branding doesn’t match the organisation.

5. Suspicious link: If you receive a text message that includes a link, be cautious about clicking on it. If you hover the mouse over the link, you should see the URL it will take you to (Suganya, 2016). If the URL looks suspicious or doesn't match the organisation the message is supposedly from, it is likely a phishing attack.

Spear phishing

Spear phishing is designed to trick a specific individual or group into giving away sensitive information (Suganya, 2016). In spear phishing attacks, the attacker typically uses personal information about the victim, such as their name, job title, or location, to create a sense of familiarity and trust. The attacker may also use social engineering techniques to persuade the victim to divulge sensitive information or click on a malicious link.

Web Spoofing

Web spoofing, also known as URL spoofing or domain spoofing, is a phishing attack involving creating a fake website that looks similar to a legitimate website (Suganya, 2016). The attacker typically uses a slightly altered version of the legitimate website's URL or a similar-looking domain name to trick the victim into thinking they are visiting the legitimate site. When the victim visits the fake site, they may be prompted to enter sensitive information, such as login credentials or financial information, which the attacker can use to gain access to their accounts.

These attacks can be highly effective for several reasons:

1. They often use social engineering techniques to manipulate people into taking the desired action. This can include using urgency or fear to persuade people to act quickly or using the appearance of authority or trustworthiness to convince people to disclose sensitive information.
2. They often use spoofed or fake websites and emails to create a sense of authenticity. These can be designed to look like they are from a legitimate source, such as a bank or government agency, and can be difficult for people to distinguish from the real thing.
3. They often target people who are busy or distracted, as they may be more likely to overlook warning signs or to make mistakes when responding to a phishing attack.

4. They often use generic or personalized messages to increase their chances of success (Suganya, 2016). Generic messages can be sent to large numbers of people at once, while personalized messages can be tailored to specific individuals or groups and may be more convincing.
5. They often use current events or hot topics to gain people's attention and make their messages more relevant. This can include using the COVID-19 pandemic or natural disasters to solicit donations or obtain sensitive information.
6. They often use a sense of urgency or a time-limited offer to persuade people to act quickly without fully thinking through the consequences.
7. They often use a sense of fear or a threat of consequences to persuade people to take the desired action (Suganya, 2016). For example, they might claim that an account will be closed unless certain information is provided or that legal action will be accepted unless a payment is made.

Overall, phishing attacks are effective because they rely on manipulating human emotions and psychology rather than technical vulnerabilities. By understanding these tactics and being aware of the signs of a phishing attack, individuals can better protect themselves and their organisations from them.

2.1.2 Technologies used in Phishing

Several technologies are commonly used in phishing attacks. These include:

1. ***Email:*** Email is a standard method for delivering phishing attacks, as it allows attackers to send large numbers of fraudulent messages to potential victims. These emails may contain links to fake websites or malware attachments.
2. ***Websites:*** Attackers may create fake websites that mimic real ones to trick victims into entering sensitive information (Suganya, 2016). These websites may be designed to look like login pages for popular websites or may be used to collect personal data under the guise of a survey or other legitimate-seeming form.
3. ***Social engineering:*** Phishing attacks often rely on social engineering techniques, which involve manipulating victims into divulging sensitive information or taking

specific action (Suganya, 2016). This may include creating a sense of urgency or fear in the victim or convincing the victim that the attacker is a trusted authority figure.

4. ***Malware:*** Attackers may use malware, or malicious software, in phishing attacks to gain access to a victim's device or steal sensitive information from the device (Suganya, 2016). This may involve installing a keylogger on the victim's machine, which records every keystroke made on the device, or installing a malware program that can capture login credentials or other sensitive information.

Here's an example of how a phishing attack might work:

1. The attacker creates a fake website that looks like a login page for a popular online service, such as a bank or social media platform.
2. The attacker sends an email to many potential victims, claiming to be from the online service and asking the victims to update their login information on the fake website.
3. Some victims fall for the scam and enter their login credentials on the fake website.
4. The attacker captures the login credentials and uses them to access the victims' accounts.
5. The attacker may then use the victims' accounts to steal sensitive information or to send phishing emails to the victims' contacts.

2.1.3 Preventing phishing

Phishing can be prevented in various ways, which includes complex methods as well. But, the two most common simple ways are:

Filtering:

1. Implementing email filtering: Email filtering involves setting up rules that automatically flag or block emails that meet specific criteria, such as having suspicious links or attachments (Rahman, 2016). This can help prevent phishing emails from reaching the user's inbox.

2. Implementing website filtering involves setting up rules that block access to certain websites based on their content or reputation (Rahman, 2016). This can help prevent users from accidentally visiting phishing websites.

User education:

1. ***Providing training:*** Training users on recognizing and avoiding phishing attacks can help them become more vigilant in spotting and preventing such threats (Al-Sarawi, 2016). This can involve explaining the common tactics that phishers use, showing examples of phishing emails and websites, and teaching users how to verify the legitimacy of links and attachments before clicking on them.
2. ***Displaying warnings:*** Displaying warnings when users click on suspicious links or visit suspicious websites can help alert them to the potential danger and encourage them to proceed cautiously (Rahman, 2016). This can be implemented through browser extensions or other security software.
3. ***Promoting safe browsing habits:*** Encouraging users to adopt safe browsing habits, such as not clicking on links in emails from unknown sources, not entering sensitive information on suspicious websites, and keeping their security software up to date, can also help prevent phishing attacks.

2.1.4 Mitigations against phishing

There are several methods that organisations and individuals can use to mitigate the risk of phishing attacks. Some of these include:

1. ***Filtering:*** One way to reduce the risk of phishing attacks is to use filtering tools that can identify and block fraudulent emails before they reach the user's inbox (Rahman, 2016). These tools may use various techniques, such as analyzing the content of the email, checking the sender's reputation, or examining the links and attachments in the email.
2. ***Employee education:*** Educating employees about the dangers of phishing attacks and how to recognize them can effectively reduce the risk of successful attacks (Suganya, 2016). This may involve training on the types of phishing attacks that are most common and

teaching employees how to verify the authenticity of emails and websites before providing sensitive information.

3. ***Two-factor authentication:*** Implementing two-factor authentication (2FA) can help to prevent attackers from accessing an account even if they manage to obtain a victim's login credentials (Suganya, 2016). With 2FA, the user must provide an additional form of authentication, such as a code sent to their phone, to log in (Rahman, 2016).
4. ***Domain Name System Blocklists (DNSBLs):*** DNSBLs are lists of IP addresses or domain names that are known to be associated with spam or other malicious activity (Suganya, 2016). Some email servers and filtering tools use DNSBLs to identify and block fraudulent emails.
5. ***Antivirus software:*** Antivirus software can help protect against phishing attacks by identifying and blocking malicious software that may be used in an attack. It is essential to keep the software up to date to ensure it can detect the latest threats (Rahman, 2016).

Implementing these and other security measures is essential to protect against phishing attacks effectively. Regularly reviewing and updating these measures is also necessary to stay ahead of evolving threats.

2.2 Critique of current mitigation

While the mitigation approaches listed above can be effective at reducing the risk of phishing attacks, they need to be more fool proof and can be bypassed by sophisticated attackers (James, 2019). There are several reasons why people are looking for more secure ways to protect against phishing attacks:

1. ***Evolving threats:*** Phishing attacks constantly evolve, and attackers continually find new ways to bypass existing security measures (James, 2019). This means that organisations and individuals must be constantly vigilant and regularly review and update their security measures to stay ahead of emerging threats.

2. ***Human error:*** One of the biggest challenges in protecting against phishing attacks is that they often rely on human error. Even with training and awareness programs, it is difficult to prevent all employees from falling victim to a phishing attack at some point.
3. ***Limited effectiveness:*** Some current mitigation approaches, such as email filtering and DNSBLs, can effectively block known threats, but they may need help identifying and securing new or unknown threats (James, 2019). This means that attackers may bypass these measures and deliver their attacks successfully.
4. ***Complexity:*** Implementing and maintaining adequate security measures can be complex and time-consuming, especially for organisations with large numbers of employees or devices to protect. This can make it challenging to keep up with the latest threats and ensure that all employees follow proper security protocols.

In summary, while current mitigation approaches can help reduce the risk of phishing attacks, they could be more fool proof and need more secure, effective protection methods.

2.3 Can phishing be mitigated using filtering only or is user education important?

Anti –phishing researchers have developed different methods to help internet users recognize and avoid phishing attacks. Much of their work focused on developing techniques to warn users about phishing websites. However, less effort has been concentrated on training users and educate them how to identify such threats.

Dos:

- Security browsers and software should be kept updated all the time.

- Links should be hovered over to be able to distinguish obvious fakes

- E-mails should be inspected for obvious red flags so as not to click on some link that has been sent in an e-mail to visit the website.

Don’ts:

- Blindly trust unknown senders and click on links sent by them.

- Send suspicious e-mails to friends and family.

- Download material that is identified by browser or software of security to be malicious.

- Provide information like credit card or social security card numbers, or home address to sites which may be suspicious (Mary & Molly, 2015).

A study used a game to train users so that they can identify phishing scams. Training materials were provided to the users. The results of the study reveal that the games turned out to be an auspicious way of training users to detect phishing threats (Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong & Nunge, 2007). Users should be trained so that they do not blindly follow links to websites, particularly, where they are used to provide their credentials. It is unrealistic to believe that all users will recognize and comprehend the risks posed by phishing and conduct their browsing accordingly. There will always be some users who will assume that some deceptive websites are legitimate. Therefore, it is important that academics and professionals find ways to decrease phishing attacks (Kirda & Kruegel, 2006).

An alternative way to identify phishing scams is the filtering of the email content. In recent years, spam filters based on email content have been widely discussed (A. Bratko, 2016). Filtering is the automatic division of messages into legal email and phishing email. The phishing email filter is responsible for classifying new mails. It can examine messages to categorise them either separately (for example, just looking for specific distinct words in emails in the case of keyword filtering), or through a learning-based filter that examines a collection of labelled training data (pre-collected messages) P. Resnick,2008). The header(s) and body are the two components of an email message. A systematic set of fields, including From, To, Subject, and others, make up email headers. In an email, header lines that indicate specific routing information, such as the sender, receiver, and date, are always placed before the body of the message.

According to a test performed, Microsoft used data from honeypots and the feedback of more than 300000 Hotmail users to train its SmartScreen phishing filter (S. Myers, 2007). The filter evaluates more than 100000 attributes of an email and uses a learning algorithm based on Bayesian statistics. A team of experts constantly tunes the filter and adapts it to the latest spamming and phishing techniques. Consequently, using a combination of both user education and filtering can help decrease phishing attacks.

2.4 A critical review of the sources

The sources listed are a mix of articles and blog posts on phishing and how to protect against it. These sources provide information on the dangers of phishing, how to recognize and avoid phishing attacks, and best practices for preventing phishing in organisations. Some sources also offer tips and recommendations for combating phishing, such as implementing email filtering and training users on recognizing and avoiding phishing attacks.

EZMarketing's (2021) article "Why phishing is more dangerous than ever, and how to protect yourself" discusses the increasing prevalence and sophistication of phishing attacks and provides tips for protecting against them, such as being cautious with links and attachments, using anti-phishing tools, and educating employees about phishing.

Hebert et al.'s (2022) article "How to recognize and avoid phishing scams" from Consumer Advice provides an overview of phishing and how it works, as well as tips for recognizing and avoiding phishing attacks, such as being cautious with links and attachments, not sharing personal information, and looking out for unusual requests or language.

Packetlabs's article "Prevent phishing in your organisation: 4 steps" discusses the importance of protecting against phishing attacks and provides four steps for preventing phishing in organisations, including implementing email filtering, training employees, and regularly updating security software.

Theme Marketplace's article "Preventing phishing attacks - 8 best practices" provides an overview of phishing and how it works, as well as eight best practices for preventing phishing attacks, such as educating employees, implementing email filtering, and using two-factor authentication.

Sanford's (2021) article "Preventing phishing: 7 tips for stopping phishing attacks" from ConnectWise discusses the dangers of phishing and provides seven tips for preventing phishing attacks, including educating employees, using anti-phishing tools, and being cautious with links and attachments.

Shearn's (2022) article "Dangers of phishing" from CIO Solutions discusses the risks of phishing. It provides tips for protecting against it, such as being cautious with links and attachments, using anti-phishing tools, and educating employees.

Security Magazine's article "4 recommendations to combat phishing" provides an overview of phishing and four recommendations for combating it, including implementing email filtering, training employees, and regularly updating security software.

Villadiego's (2017) article "Council post: The dangers of phishing" from Forbes discusses the risks of phishing and provides tips for protecting against it, such as being cautious with links and attachments, using anti-phishing tools, and educating employees.

Zurier's (2016) article "5 tips for combating phishing" from Dark Reading provides an overview of phishing and five tips for combating it, including educating employees, implementing email filtering, and using two-factor authentication.

As a result, the credibility and reliability of the sources were evaluated. The accuracy and of the information obtained from online sources was verified before being used. Some factors which were taken into consideration when evaluating the quality of the online sources included the credentials and expertise of the author, the reputation and credibility of the publication or website, and the presence of evidence and citations to support the information provided.

The blogs gathered information from various sources, including research studies, news articles, government reports, and personal experiences.

In these blogs and articles, they tested phishing techniques by creating simulated phishing attacks and measuring how well users can recognize and avoid them. They also pushed prevention measures through phishing simulation campaigns, training, and security awareness assessments.

3 Methodology

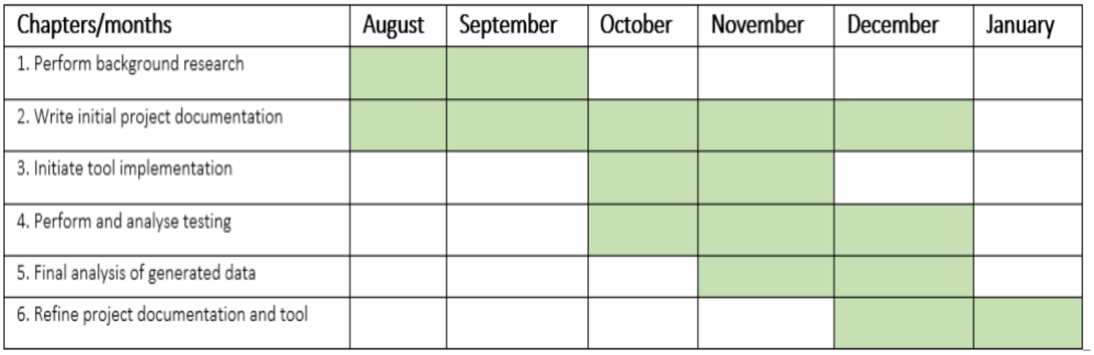
This chapter will demonstrate how the tool for the project is developed using qualitative study.

In terms of methodology, a project using the waterfall software development cycle to address spear phishing would involve the following steps:

1. ***Identify the problem and the stakeholders:*** This involves understanding the nature of spear phishing attacks and the potential impact on individuals and organisations. The stakeholders, in this case, would include individuals who may be targeted by these attacks, as well as organisations that may be affected by them.

2. ***Define the scope and objectives of the project:*** The project's content should be defined in terms of the expected goals and outcomes. For example, the project may develop a tool to help individuals and organisations protect themselves against spear phishing attacks.

3. ***Develop a detailed plan:*** The next step is to develop a detailed plan that outlines the specific tasks, resources, and timelines required to achieve the project's objectives. This plan should include detailed descriptions of the technical requirements and the particular steps that will be taken to develop and test the tool as per *figure 3.1*.



Chapters/months	August	September	October	November	December	January
1. Perform background research	🟩	🟩				
2. Write initial project documentation	🟩	🟩	🟩	🟩	🟩	
3. Initiate tool implementation			🟩	🟩		
4. Perform and analyse testing			🟩	🟩	🟩	
5. Final analysis of generated data				🟩	🟩	
6. Refine project documentation and tool					🟩	🟩

Figure 3.1 - Gantt chart of proposed system

4. ***Implement the plan:*** The implementation phase involves carrying out the tasks and activities outlined in the project plan. This will include designing and developing

the tool using open-source anti-spam tool and conducting user testing, and also making necessary revisions.

5. ***Test and evaluate the tool:*** Once it has been developed, it should be thoroughly tested and assessed to ensure that it meets the project's objectives and performs as intended. This may involve conducting simulated pear phishing attacks and measuring the tool's effectiveness in detecting and preventing these attacks.

6. ***Deploy and maintain the tool:*** Once it has been tested and evaluated, it can be deployed and made available to individuals and organisations who want to use it to protect themselves against spear phishing attacks. This may involve ongoing maintenance and updates to the tool to ensure its continued effectiveness.

While spear phishing can be a highly effective means of carrying out cyber-attacks, it raises significant ethical concerns.

The Waterfall model is a linear software development process that follows a sequential and rigid approach to software development. It is characterized by a series of distinct phases, each of which must be completed before the next step can begin. The stages in the Waterfall model include requirements gathering and analysis, design, implementation, testing, deployment, and maintenance.

3.1 Qualitative study

I recently conducted a qualitative study of the project. The study aimed to identify the successes and challenges experienced during the project and to understand the experiences and perspectives of the individuals involved.

To gather data for the study, literature review was carried out. Related topics around phishing attack was consulted. During the analysis phase of the study, the data collected was carefully reviewed. Patterns and themes were looked upon and waterfall model was used.

The idea behind the waterfall process constitutes the following. (i) A linear and sequential path may exist between the consecutive phases, (ii) The standards may be maintained at places, where the outputs or deliverables could be generated or (iii) Few techniques, which aim to achieve the necessary output, may be suggested (Joachim Schramm, 2014). The waterfall model has many benefits.

One such benefit is that it could legibly recognise the number of related phases through which a process in software development should traverse.

There is a chance that these phases will appear in many process models since they might have different layouts and slight variations in their scope and impact. The phases also include the following:

(1) Defining the requirements for describing the system's final appearance

(2) Analysing the requirements for categorizing it into functionality groups and non-functionality groups (such as the features)

(3) Creating an architectural design for the system and its corresponding elements

(4) Programming and executing the system

(5) Confirming the performance of the system and its associated elements

(6) Putting the system to work in a real-world environment

(Luca Cernuzzi, 2005)

Using the Waterfall model or any other software development approach is inappropriate or ethical to address spear phishing on other people (Gupta, 2015). Spear phishing is a type of cyber-attack involving targeted, personalized emails or other forms of communication to trick individuals into divulging sensitive information or clicking on malicious links.

Instead of using the Waterfall model or any other software development approach to address spear phishing on other people, it is crucial to focus on prevention and education (Hassan, 2014). This can involve implementing technical measures, such as spam filters and email encryption, and educating employees and others about recognizing and avoiding spear phishing attacks. It is also essential to have policies and procedures in place to report and respond to suspected spear phishing attacks.

Overall, using the waterfall software development cycle to address pear phishing involves a systematic and structured approach to identifying and addressing the problem. By following this methodology, it is possible to develop a tool to help individuals and organisations protect themselves against these attacks.

3.2 Reasons to do this mitigation system

I plan to use a waterfall model to develop a solution to spear phishing attacks. In the analysis phase, I will gather information about the problem I am trying to solve, including the types of spear phishing attacks that are most common and the vulnerabilities that these attacks exploit. Using my solution, I will also gather information about the users' needs and requirements.

In the design phase, I will use the information gathered in the analysis phase to design my solution. This will involve creating a detailed plan or blueprint for the answer, including its features and functionality. According to my design plan, I will begin building the solution in the implementation phase. This will involve writing code, testing the resolution, and debugging any issues.

I will test the solution in the testing phase to ensure it works correctly and meets the users' needs. This will involve performing various types of testing, such as unit testing, integration testing, and acceptance testing. In the deployment phase, I will deploy the solution in a production environment and make it available to users. This will involve installing the solution on servers, configuring it for the production environment, and performing necessary maintenance or updates (James, 2019). In the maintenance phase, I will monitor the solution and make any critical updates or changes to ensure that it continues to function correctly and meet the users' needs.

SpamAssassin, an open-source mail filter will be used. It uses text analysis to identify spam. The filter uses a giant rule base to examine an incoming mail (John, Koutsias, 2000). Failure to comply with a certain rule will result in the mail having points assigned to it. If the mail amasses more than 5.0 points, then it is classified as spam. SpamAssassin analyses both the header of the mail and its body. The filter takes advantage of blacklists (Harald Baayen, 2002). SpamAssassin is an open-source tool. These tools can be easily accessed and are often more customisable. Since, the source code is available, users can modify the tool to suit their specific needs or add new features to improve its performance as mentioned by Richard M. Stallman. Additionally, the open-source community often provides support and updates for these tools, making them a good choice for those who want to stay up to date with the latest developments in spam detection technology.

3.3 Tool setup

To build and set up a mail server system like the one I described, below steps was followed:

1. ***Create and configure the Virtual machine.*** This involves setting up the virtual machine environment, installing the necessary operating systems, and configuring the network settings for each Virtual machine.
2. ***Install and configure the software for each Virtual machine.*** This includes, installing and configuring the Social Engineer Toolkit (SET) Framework on Virtual machine 1, installing and configuring Postfix and SpamAssassin on Virtual machine 2, and installing and configuring Thunderbird on Virtual machine 3.
3. ***Configure the mail server system.*** This involves correctly setting up the necessary accounts and email addresses and configuring the DNS records to route email messages to and from the mail server.
4. ***Test and debug the system.*** Once the system is set up, it is essential to test and debug it to ensure that it functions correctly and that all components work together as expected.

In my design, three virtual machines are setup, using a tool such as VMware. VM1 acts as the attacker, VM2 acts as the Mail Transfer agent (MTA) and the spam filter, and VM3 acts as the email client. This is a standard configuration for a mail server, but there are many other ways to set up a mail server, depending on your specific needs. *Figure 3.2* illustrates a model of my tool.

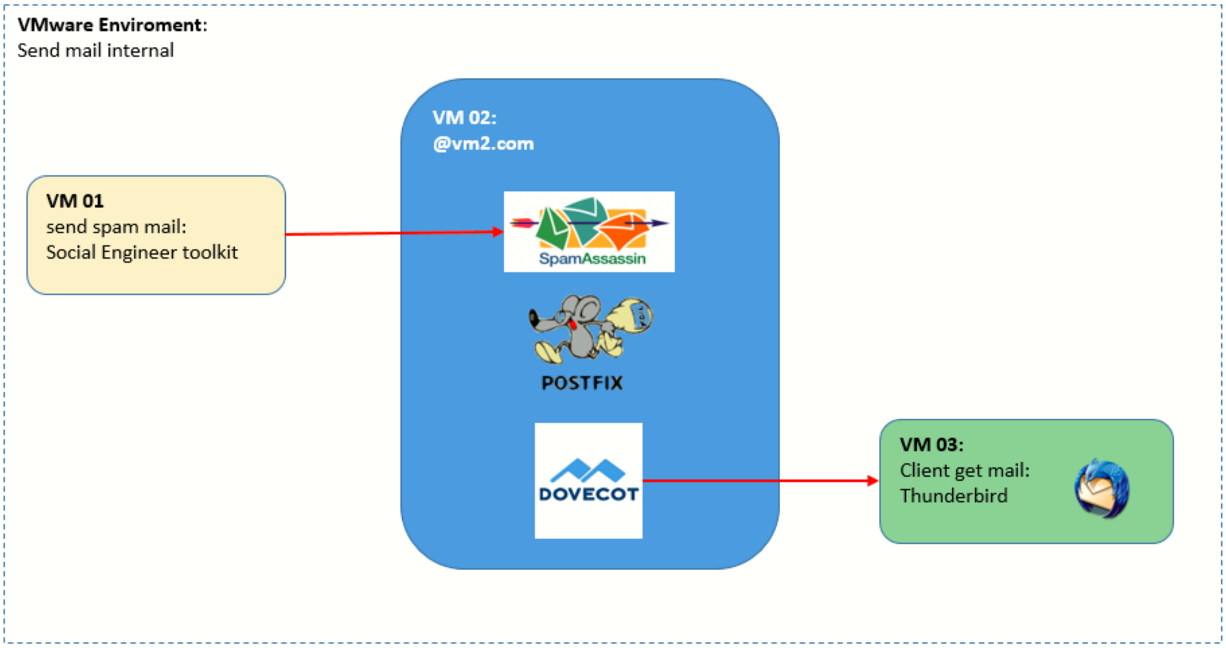
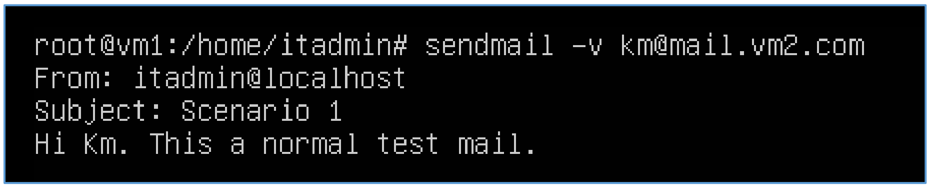


Figure 3.2 - Model of Sending Mail and Assessing Spam Mail

3.3.1 Configuring the three Virtual Machines (VMs)

Virtual Machine 1 (VM1) is used to send both non-spam and spam emails. Non-spam emails are sent using the sendmail command lines, while spam emails are sent using the open-source Social Engineer Toolkit (SET), as part of testing and experimentation.

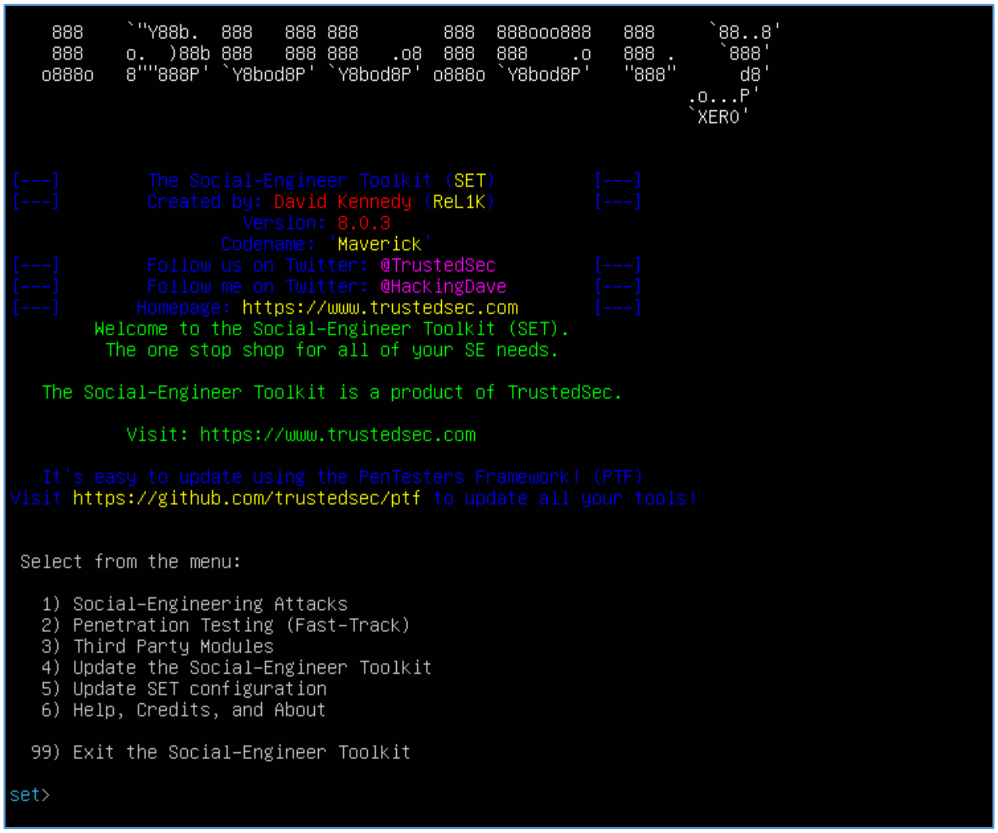
Figure 3.3 illustrates VM1 sending a **non-spam email** using the *sendmail* command lines.



```
root@vm1:/home/itadmin# sendmail -v km@mail.vm2.com
From: itadmin@localhost
Subject: Scenario 1
Hi Km. This a normal test mail.
```

Figure 3.3 - Non-spam mail sent from VM1

Figure 3.4 illustrates VM1 sending a **spam email** through the *Social Engineer Toolkit (SET)*.

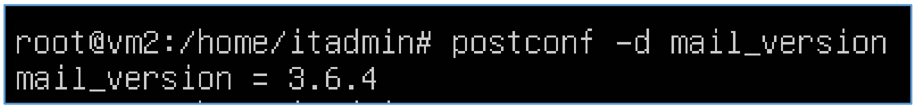


```
    888     `"Y88b.  888    888 888         888  888ooo888   888      `88..8'
    888     o.  )88b 888    888 888    .o8  888  888    .o   888 .     `888'
   o888o    8""888P'  `Y8bod8P'  `Y8bod8P' o888o `Y8bod8P'   "888"      d8'
                                                                    .o...P'
                                                                    `XERO'


[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

Figure 3.4 - Spam mail sent from VM1

Virtual Machine 2 (VM2) is used as the Mail Transfer Agent (MTA). The mail transfer agent is responsible for routing and delivering email messages between servers and clients. The VM consists of the mail-sending services Postfix and Dovecot. Furthermore, this VM contains the SpamAssassin service which helps to protect against spam and phishing emails by keeping track of the spam scores, when activated.

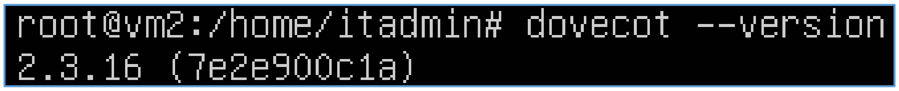
Figure 3.5 shows the **Postfix service version** installed on VM2.



```
root@vm2:/home/itadmin# postconf -d mail_version
mail_version = 3.6.4
```

Figure 3.5 - Postfix version on VM2

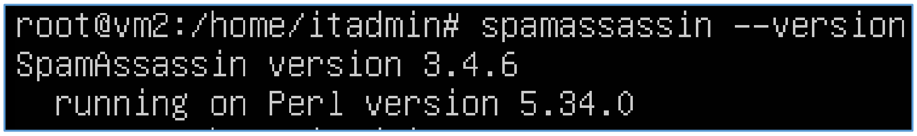
Figure 3.6 shows the **Dovecot service version** installed on VM2.



```
root@vm2:/home/itadmin# dovecot --version
2.3.16 (7e2e900c1a)
```

Figure 3.6 - Dovecot version on VM2

Figure 3.7 shows the **SpamAssassin service version** installed on VM2.



```
root@vm2:/home/itadmin# spamassassin --version
SpamAssassin version 3.4.6
  running on Perl version 5.34.0
```

Figure 3.7 - SpamAssassin version on VM2

Virtual Machine 3 (VM3) is used as the Email Client Mail and consists of the Thunderbird mail application as shown in *Figure 3.8*. The email client is software that allows users to send and receive emails. In this case, Thunderbird receives emails sent from VM1 and determines whether the email is spam or not.

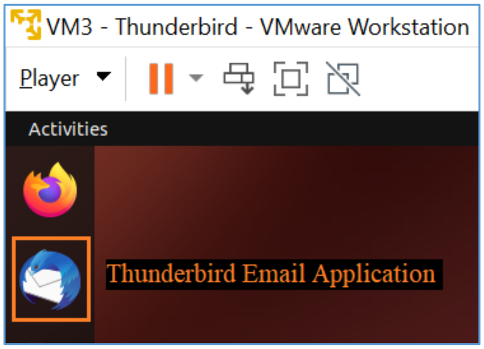

VM3 - Thunderbird - VMware Workstation
Player
Activities
Thunderbird Email Application

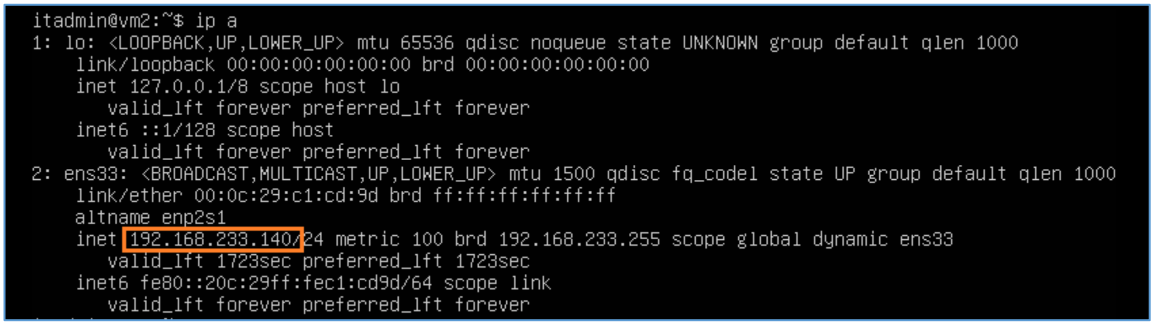
Figure 3.8 - Thunderbird installed on VM3

3.3.2 Connecting the three Virtual Machines (VMs)

An IP address is used to allow communication among the three virtual machines. Since VM2 serves as the Mail Transfer Agent, all communications must go through it. Thus, the latter's IP address is used in both VM1 and VM3.

To connect the three virtual machines (VMs), the following procedures must be followed.

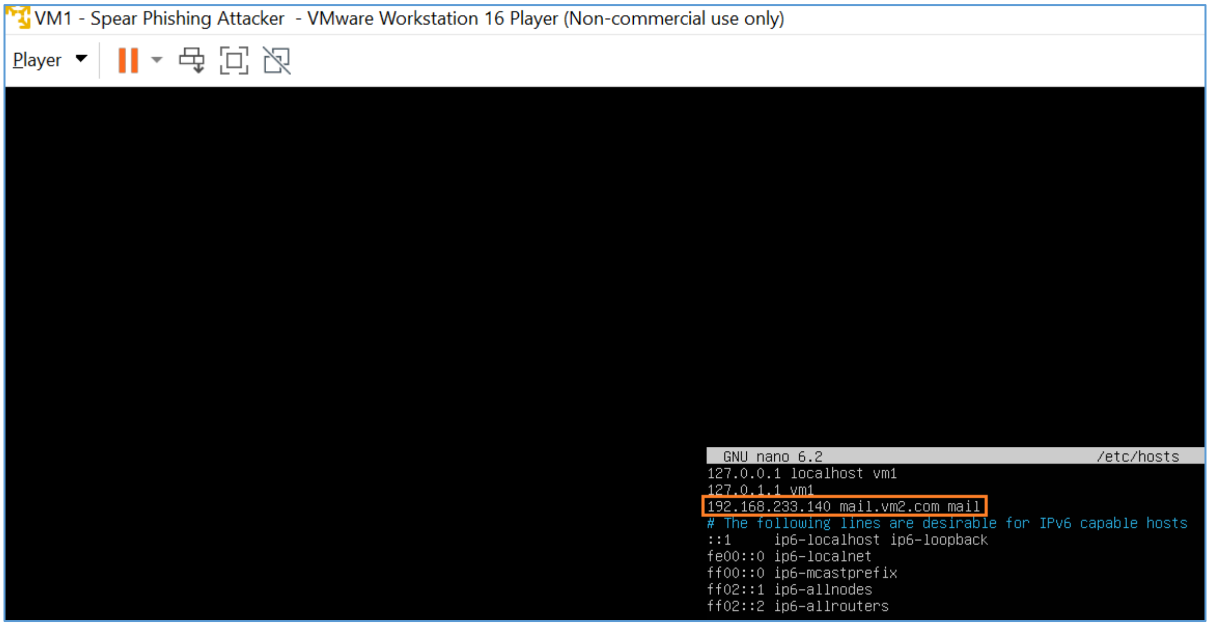
1. The IP Address (ens33) of VM2 is verified using the command line **# ip a,** as shown in *Figure 3.9*.



```
itadmin@vm2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c1:cd:9d brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.233.140/24 metric 100 brd 192.168.233.255 scope global dynamic ens33
       valid_lft 1723sec preferred_lft 1723sec
    inet6 fe80::20c:29ff:fec1:cd9d/64 scope link
       valid_lft forever preferred_lft forever
```

Figure 3.9 - Verifying the IP Address of VM2

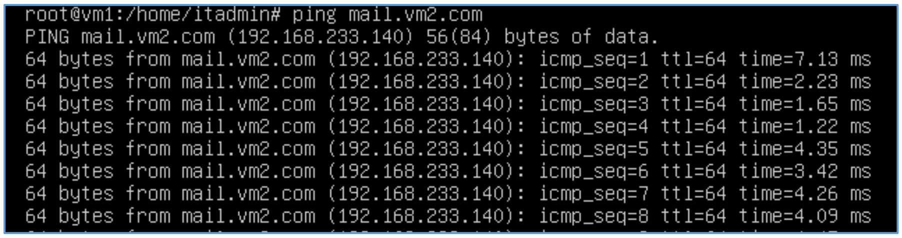
2. The IP address of VM2 is added to the configuration file hosts in VM1 as shown in *Figure 3.10*.


VM1 - Spear Phishing Attacker - VMware Workstation 16 Player (Non-commercial use only)
Player

```
  GNU nano 6.2                                              /etc/hosts
127.0.0.1 localhost vm1
127.0.1.1 vm1
192.168.233.140 mail.vm2.com mail
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Figure 3.10 - Placing VM2's IP Address in host configuration file

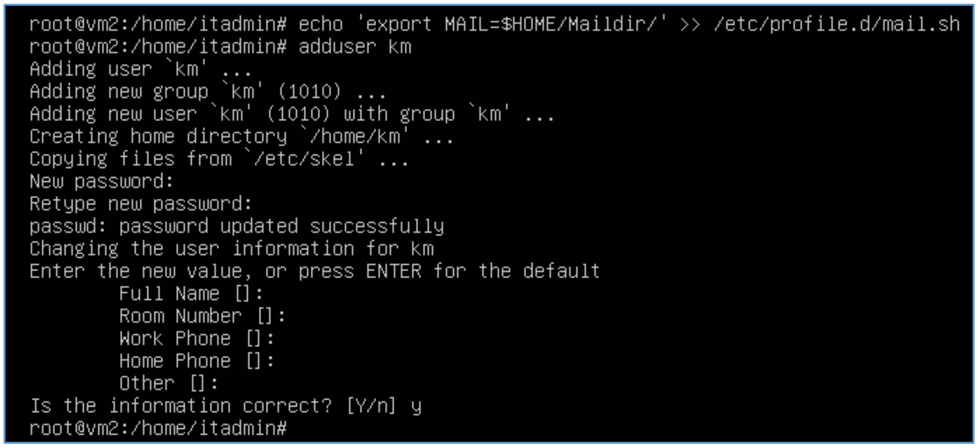
3. It is crucial to verify that the aforementioned modification has enabled VM1 and VM2 to communicate. As shown in *Figure 3.11*, this is accomplished with the command line **# ping mail.vm2.com**.



```
root@vm1:/home/itadmin# ping mail.vm2.com
PING mail.vm2.com (192.168.233.140) 56(84) bytes of data.
64 bytes from mail.vm2.com (192.168.233.140): icmp_seq=1 ttl=64 time=7.13 ms
64 bytes from mail.vm2.com (192.168.233.140): icmp_seq=2 ttl=64 time=2.23 ms
64 bytes from mail.vm2.com (192.168.233.140): icmp_seq=3 ttl=64 time=1.65 ms
64 bytes from mail.vm2.com (192.168.233.140): icmp_seq=4 ttl=64 time=1.22 ms
64 bytes from mail.vm2.com (192.168.233.140): icmp_seq=5 ttl=64 time=4.35 ms
64 bytes from mail.vm2.com (192.168.233.140): icmp_seq=6 ttl=64 time=3.42 ms
64 bytes from mail.vm2.com (192.168.233.140): icmp_seq=7 ttl=64 time=4.26 ms
64 bytes from mail.vm2.com (192.168.233.140): icmp_seq=8 ttl=64 time=4.09 ms
```

Figure 3.11 - Successful connection between VM1 & VM2

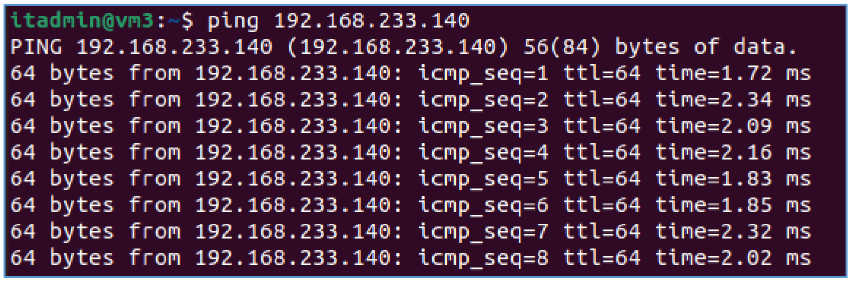
4. A new user is created in VM2 using the **# adduser** command line as shown in *Figure 3.12*.



```
root@vm2:/home/itadmin# echo 'export MAIL=$HOME/Maildir/' >> /etc/profile.d/mail.sh
root@vm2:/home/itadmin# adduser km
Adding user `km' ...
Adding new group `km' (1010) ...
Adding new user `km' (1010) with group `km' ...
Creating home directory `/home/km' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for km
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root@vm2:/home/itadmin#
```

Figure 3.12 - Adding user 'km' in VM2

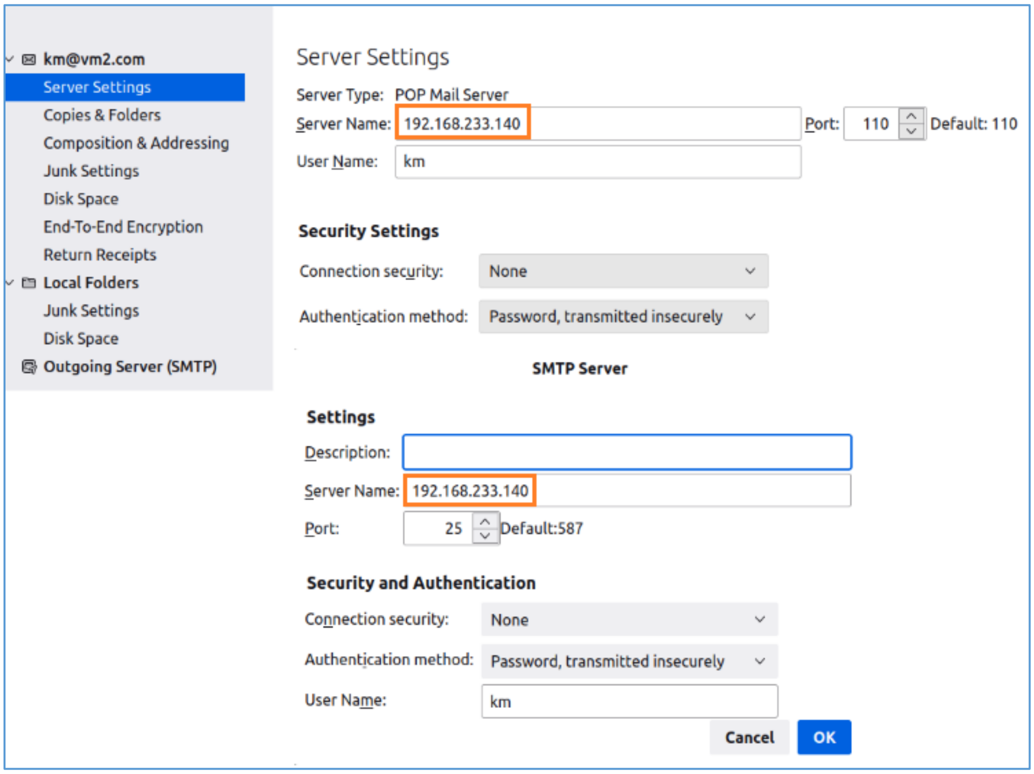
5. Again, it is crucial to check whether VM3 can communicate with VM2 before creating the user account in Thunderbird. This is accomplished with the command line **# ping 192.168.233.140** (VM2's IP address), as shown in *Figure 3.13*.



```
itadmin@vm3:~$ ping 192.168.233.140
PING 192.168.233.140 (192.168.233.140) 56(84) bytes of data.
64 bytes from 192.168.233.140: icmp_seq=1 ttl=64 time=1.72 ms
64 bytes from 192.168.233.140: icmp_seq=2 ttl=64 time=2.34 ms
64 bytes from 192.168.233.140: icmp_seq=3 ttl=64 time=2.09 ms
64 bytes from 192.168.233.140: icmp_seq=4 ttl=64 time=2.16 ms
64 bytes from 192.168.233.140: icmp_seq=5 ttl=64 time=1.83 ms
64 bytes from 192.168.233.140: icmp_seq=6 ttl=64 time=1.85 ms
64 bytes from 192.168.233.140: icmp_seq=7 ttl=64 time=2.32 ms
64 bytes from 192.168.233.140: icmp_seq=8 ttl=64 time=2.02 ms
```

Figure 3.13 - Successful connection between VM3 & VM2

6. After connecting VM2 and VM3, the user account is created in Thunderbird by using the IP address of VM2, as shown in *Figure 3.14*.



Server Settings

Server Type: POP Mail Server

Server Name: 192.168.233.140 Port: 110 Default: 110

User Name: km

Security Settings

Connection security: None

Authentication method: Password, transmitted insecurely

SMTP Server

Settings

Description:

Server Name: 192.168.233.140

Port: 25 Default:587

Security and Authentication

Connection security: None

Authentication method: Password, transmitted insecurely

User Name: km

Figure 3.14 - User Account creation in Thunderbird

7. The user account is successfully created with the Inbox and Trash as shown in *Figure 3.15*.

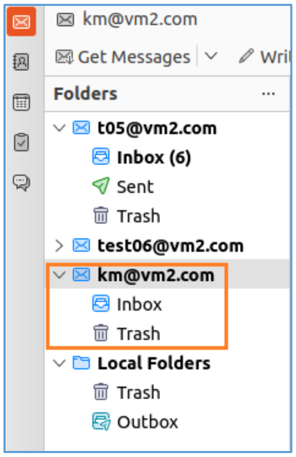


Figure 3.15 - Successful creation of user account in Thunderbird

4 Critical Review

In this chapter, we look at how a mail server works. A mail server is a computer or a group of computers responsible for sending, receiving, and storing electronic messages, also known as email. A mail server typically consists of two components: a mail transfer agent (MTA) and a mail delivery agent (MDA).

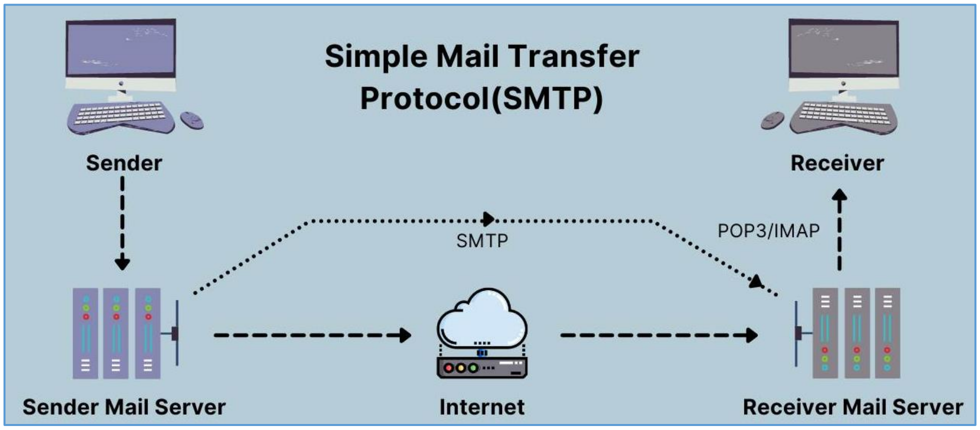


Figure 4.1 - How does mail work? (Singh 2022)

As it can be seen from *figure 4.1* (Singh 2022), the mail transfer agent (MTA) is responsible for transporting messages between mail servers. This is typically done using the Simple Mail

Transfer Protocol (SMTP), a standard for sending and receiving email messages over the internet. The mail delivery agent is responsible for delivering messages to the appropriate mailbox on the mail server. This is typically done using the Post Office Protocol (POP3) or the Internet Message Access Protocol (IMAP), both standard protocols for accessing email on a mail server.

The tool helps prevent spear phishing attacks by implementing strict authentication protocols to ensure that only authorized users can access the server and send email messages. This can help prevent attackers from impersonating legitimate users and sending spear-phishing messages to others.

Another way it can help prevent spear phishing is by using spam filters and other types of malware protection. These filters can scan incoming and outgoing email messages for signs of phishing attempts, such as links to suspicious websites or attachments that contain malware. If a message is flagged as potentially malicious, the server can either block it or quarantine it until an administrator can further investigate it.

5 Evaluation and Results

In this chapter, we test and examine the results of my project to combat phishing using a waterfall model. The system was tested on phishing and non-phishing emails dataset and evaluated following several scenarios. This project aimed to develop a tool to accurately identify phishing emails to protect individuals and organisations from these cyber-attacks. The results of our evaluation are discussed in the following sections.

5.1 System testing

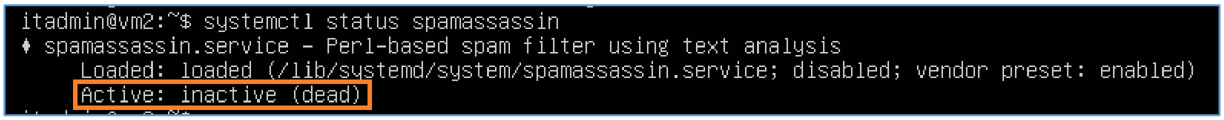
As mentioned above, once the system is set up, it is essential to test and debug it in order to ensure that it functions correctly as expected. Therefore, six scenarios are considered to demonstrate how the system respond to non-spear phishing (non-spam) and spear phishing (spam) attacks.

5.1.1 Scenario 1

Sending a non-spam mail from VM1 through the Mail Transfer Agent in VM2 and showing the received mail in Thunderbird (VM3).

In this scenario, both the SpamAssassin service and Thunderbird's junk filter are deactivated.

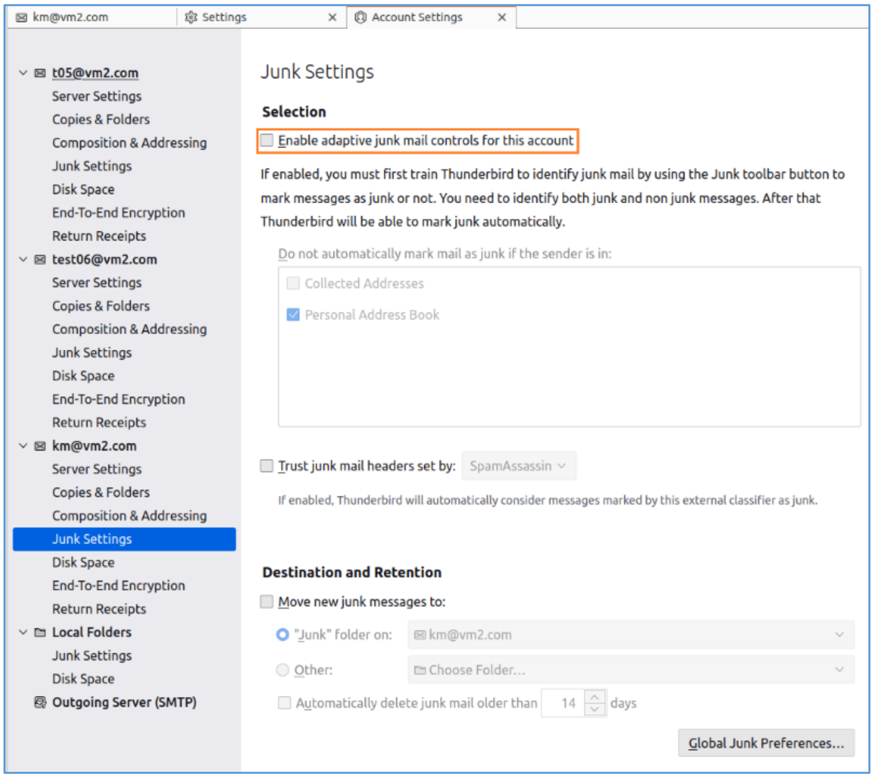
- SpamAssassin service is inactive as shown in *Figure 5.1*.



```
itadmin@vm2:~$ systemctl status spamassassin
● spamassassin.service - Perl-based spam filter using text analysis
     Loaded: loaded (/lib/systemd/system/spamassassin.service; disabled; vendor preset: enabled)
     Active: inactive (dead)
```

Figure 5.1 - Scenario 1: SpamAssassin service is deactivated

- Junk mail setting is inactive as shown in *Figure 5.2*.



Junk Settings

Selection

□ Enable adaptive junk mail controls for this account

If enabled, you must first train Thunderbird to identify junk mail by using the Junk toolbar button to mark messages as junk or not. You need to identify both junk and non junk messages. After that Thunderbird will be able to mark junk automatically.

Do not automatically mark mail as junk if the sender is in:

□ Collected Addresses

☑ Personal Address Book

□ Trust junk mail headers set by: SpamAssassin

If enabled, Thunderbird will automatically consider messages marked by this external classifier as junk.

Destination and Retention

□ Move new junk messages to:

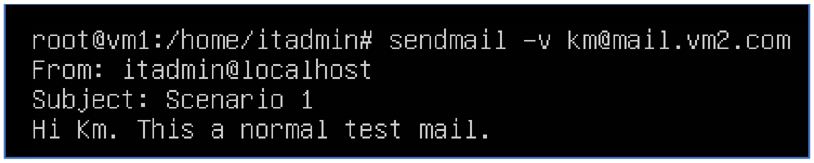
● "Junk" folder on: km@vm2.com

○ Other: Choose Folder...

□ Automatically delete junk mail older than 14 days

Figure 5.2 - Scenario 1: Thunderbird's junk setting is deactivated

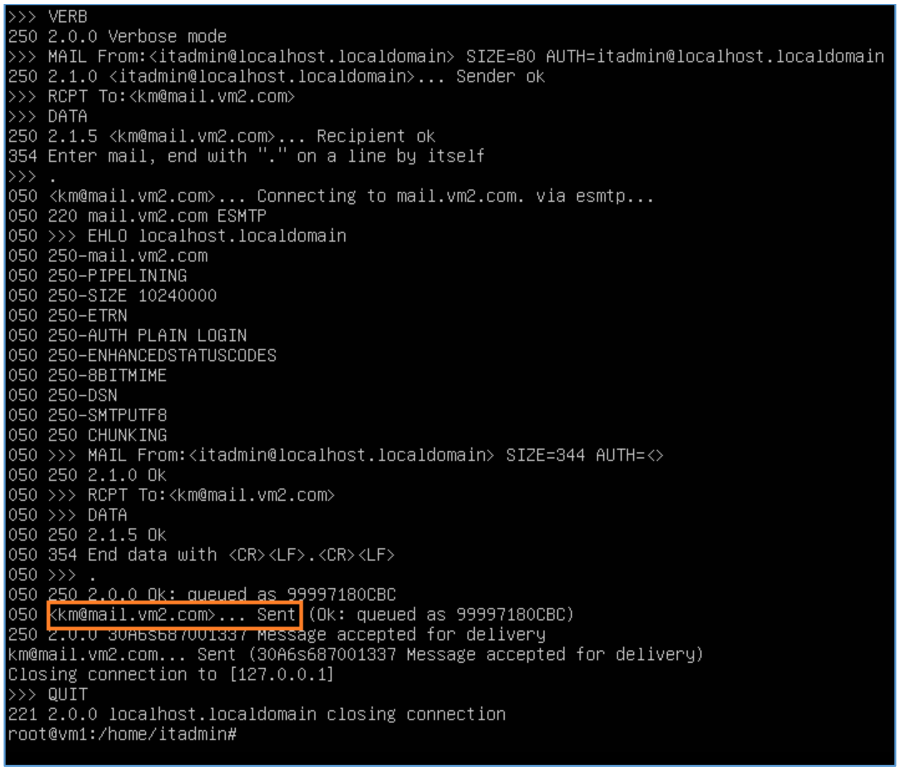
- Sending a non-spam mail to user mail address km@mail.vm2.com, from VM1 as shown in *Figure 5.3*.



```
root@vm1:/home/itadmin# sendmail -v km@mail.vm2.com
From: itadmin@localhost
Subject: Scenario 1
Hi Km. This a normal test mail.
```

Figure 5.3 - Scenario 1: Non-spam mail being sent from VM1

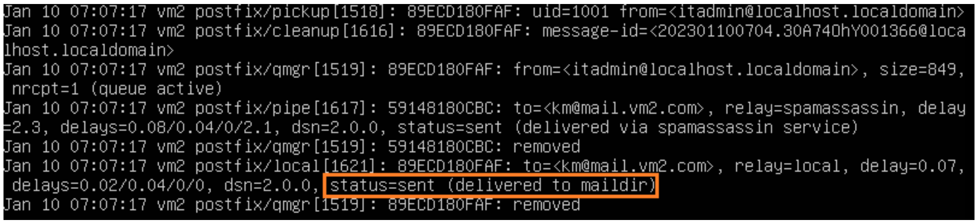
- Mail is successfully sent from VM1 as shown in *Figure 5.4*.



```
>>> VERB
250 2.0.0 Verbose mode
>>> MAIL From:<itadmin@localhost.localdomain> SIZE=80 AUTH=itadmin@localhost.localdomain
250 2.1.0 <itadmin@localhost.localdomain>... Sender ok
>>> RCPT To:<km@mail.vm2.com>
>>> DATA
250 2.1.5 <km@mail.vm2.com>... Recipient ok
354 Enter mail, end with "." on a line by itself
>>> .
050 <km@mail.vm2.com>... Connecting to mail.vm2.com. via esmtp...
050 220 mail.vm2.com ESMTP
050 >>> EHLO localhost.localdomain
050 250-mail.vm2.com
050 250-PIPELINING
050 250-SIZE 10240000
050 250-ETRN
050 250-AUTH PLAIN LOGIN
050 250-ENHANCEDSTATUSCODES
050 250-8BITMIME
050 250-DSN
050 250-SMTPUTF8
050 250 CHUNKING
050 >>> MAIL From:<itadmin@localhost.localdomain> SIZE=344 AUTH=<>
050 250 2.1.0 Ok
050 >>> RCPT To:<km@mail.vm2.com>
050 >>> DATA
050 250 2.1.5 Ok
050 354 End data with <CR><LF>.<CR><LF>
050 >>> .
050 250 2.0.0 Ok: queued as 99997180CBC
050 <km@mail.vm2.com>... Sent (Ok: queued as 99997180CBC)
250 2.0.0 30A6s687001337 Message accepted for delivery
km@mail.vm2.com... Sent (30A6s687001337 Message accepted for delivery)
Closing connection to [127.0.0.1]
>>> QUIT
221 2.0.0 localhost.localdomain closing connection
root@vm1:/home/itadmin#
```

Figure 5.4 - Scenario 1: Mail successfully sent

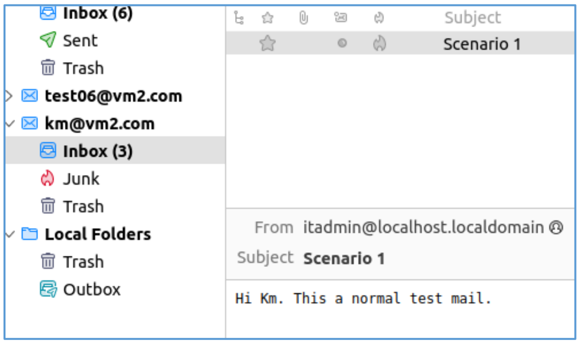
- The mail log from VM2 showing that the mail is successfully delivered to the mail directory as shown in *Figure 5.5*.



```
Jan 10 07:07:17 vm2 postfix/pickup[1518]: 89ECD180FAF: uid=1001 from=<itadmin@localhost.localdomain>
Jan 10 07:07:17 vm2 postfix/cleanup[1616]: 89ECD180FAF: message-id=<202301100704.30A740hY001366@loca
lhost.localdomain>
Jan 10 07:07:17 vm2 postfix/qmgr[1519]: 89ECD180FAF: from=<itadmin@localhost.localdomain>, size=849,
 nrcpt=1 (queue active)
Jan 10 07:07:17 vm2 postfix/pipe[1617]: 59148180CBC: to=<km@mail.vm2.com>, relay=spamassassin, delay
=2.3, delays=0.08/0.04/0/2.1, dsn=2.0.0, status=sent (delivered via spamassassin service)
Jan 10 07:07:17 vm2 postfix/qmgr[1519]: 59148180CBC: removed
Jan 10 07:07:17 vm2 postfix/local[1621]: 89ECD180FAF: to=<km@mail.vm2.com>, relay=local, delay=0.07,
 delays=0.02/0.04/0/0, dsn=2.0.0, status=sent (delivered to maildir)
Jan 10 07:07:17 vm2 postfix/qmgr[1519]: 89ECD180FAF: removed
```

Figure 5.5 - Scenario 1: Successful mail delivery message from message log

- The mail is successfully received in Thunderbird in VM3 as shown in *Figure 5.6*.

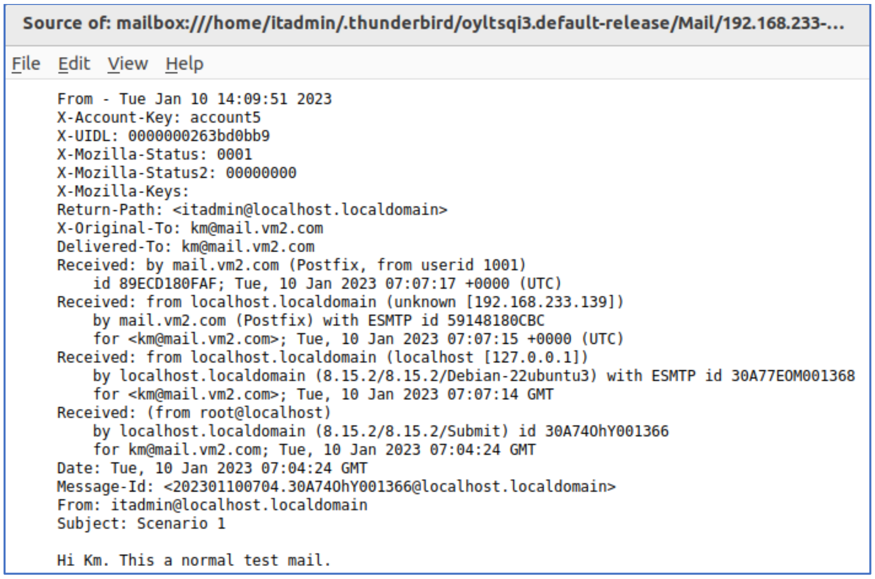


From itadmin@localhost.localdomain
Subject **Scenario 1**

```
Hi Km. This a normal test mail.
```

Figure 5.6 - Scenario 1: Thunderbird successfully receives message

- The view source of the mail as shown in *Figure 5.7*, concludes that the mail did not pass through the SpamAssassin service since it was initially set as inactive. Thus, there is no spam status from SpamAssassin service.


Source of: mailbox:///home/itadmin/.thunderbird/oyltsqi3.default-release/Mail/192.168.233-...
File
Edit
View
Help

```
From - Tue Jan 10 14:09:51 2023
X-Account-Key: account5
X-UIDL: 0000000263bd0bb9
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: <itadmin@localhost.localdomain>
X-Original-To: km@mail.vm2.com
Delivered-To: km@mail.vm2.com
Received: by mail.vm2.com (Postfix, from userid 1001)
    id 89ECD180FAF; Tue, 10 Jan 2023 07:07:17 +0000 (UTC)
Received: from localhost.localdomain (unknown [192.168.233.139])
    by mail.vm2.com (Postfix) with ESMTP id 59148180CBC
    for <km@mail.vm2.com>; Tue, 10 Jan 2023 07:07:15 +0000 (UTC)
Received: from localhost.localdomain (localhost [127.0.0.1])
    by localhost.localdomain (8.15.2/8.15.2/Debian-22ubuntu3) with ESMTP id 30A77E0M001368
    for <km@mail.vm2.com>; Tue, 10 Jan 2023 07:07:14 GMT
Received: (from root@localhost)
    by localhost.localdomain (8.15.2/8.15.2/Submit) id 30A740hY001366
    for km@mail.vm2.com; Tue, 10 Jan 2023 07:04:24 GMT
Date: Tue, 10 Jan 2023 07:04:24 GMT
Message-Id: <202301100704.30A740hY001366@localhost.localdomain>
From: itadmin@localhost.localdomain
Subject: Scenario 1

Hi Km. This a normal test mail.
```

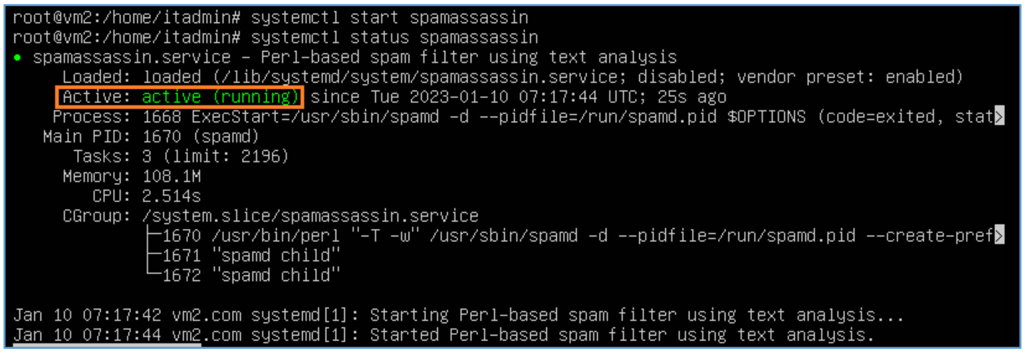
Figure 5.7 – Scenario 1: Mail view source

5.1.2 Scenario 2

Sending a non- spam mail from VM1 through the Mail Transfer Agent in VM2 and showing the received mail in Thunderbird (VM3).

In this scenario, the SpamAssassin service is activated while Thunderbird's junk filter is deactivated.

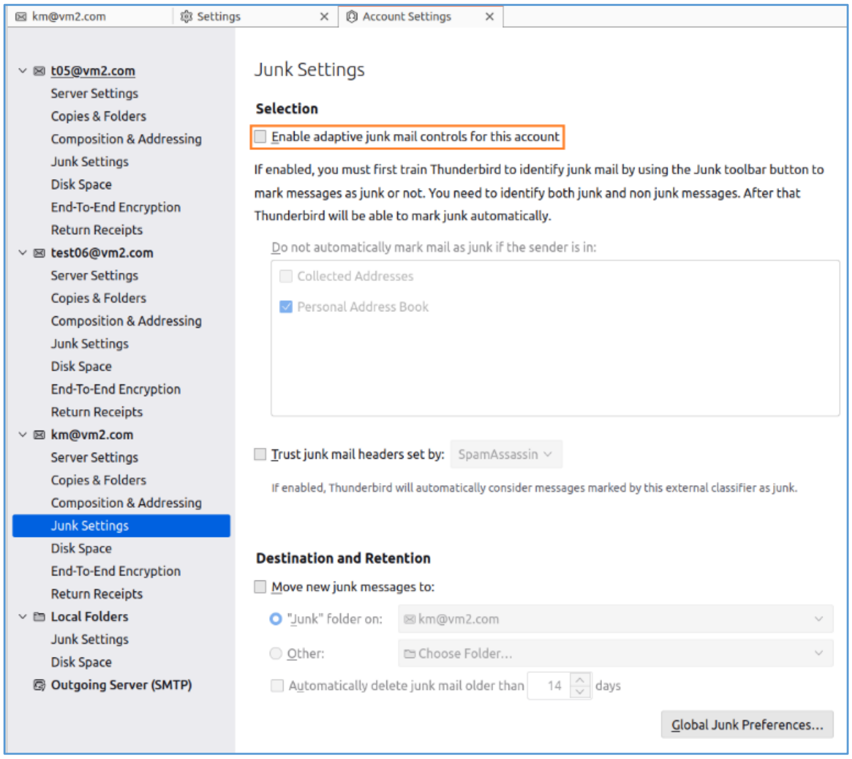
- SpamAssassin service is active as shown in *Figure 5.8.*



```
root@vm2:/home/itadmin# systemctl start spamassassin
root@vm2:/home/itadmin# systemctl status spamassassin
● spamassassin.service - Perl-based spam filter using text analysis
     Loaded: loaded (/lib/systemd/system/spamassassin.service; disabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-01-10 07:17:44 UTC; 25s ago
    Process: 1668 ExecStart=/usr/sbin/spamd -d --pidfile=/run/spamd.pid $OPTIONS (code=exited, stat>
   Main PID: 1670 (spamd)
      Tasks: 3 (limit: 2196)
     Memory: 108.1M
        CPU: 2.514s
     CGroup: /system.slice/spamassassin.service
             ├─1670 /usr/bin/perl "-T -w" /usr/sbin/spamd -d --pidfile=/run/spamd.pid --create-pref>
             ├─1671 "spamd child"
             └─1672 "spamd child"

Jan 10 07:17:42 vm2.com systemd[1]: Starting Perl-based spam filter using text analysis...
Jan 10 07:17:44 vm2.com systemd[1]: Started Perl-based spam filter using text analysis.
```

Figure 5.8 - Scenario 2: SpamAssassin service is activated

- Junk mail setting is inactive as shown in *Figure 5.9.*



- t05@vm2.com
  - Server Settings
  - Copies & Folders
  - Composition & Addressing
  - Junk Settings
  - Disk Space
  - End-To-End Encryption
  - Return Receipts
- test06@vm2.com
  - Server Settings
  - Copies & Folders
  - Composition & Addressing
  - Junk Settings
  - Disk Space
  - End-To-End Encryption
  - Return Receipts
- km@vm2.com
  - Server Settings
  - Copies & Folders
  - Composition & Addressing
  - Junk Settings
  - Disk Space
  - End-To-End Encryption
  - Return Receipts
- Local Folders
  - Junk Settings
  - Disk Space
- Outgoing Server (SMTP)

Junk Settings

Selection

□ Enable adaptive junk mail controls for this account

If enabled, you must first train Thunderbird to identify junk mail by using the Junk toolbar button to mark messages as junk or not. You need to identify both junk and non junk messages. After that Thunderbird will be able to mark junk automatically.

Do not automatically mark mail as junk if the sender is in:

□ Collected Addresses

☑ Personal Address Book

□ Trust junk mail headers set by: SpamAssassin

If enabled, Thunderbird will automatically consider messages marked by this external classifier as junk.

Destination and Retention

□ Move new junk messages to:

● "Junk" folder on: km@vm2.com

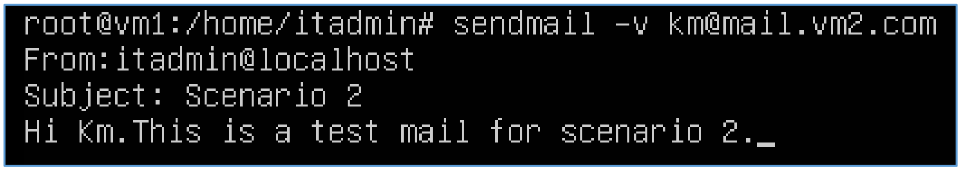
○ Other: Choose Folder...

□ Automatically delete junk mail older than 14 days

Global Junk Preferences...

Figure 5.9 - Scenario 2: Thunderbird's junk setting is deactivated

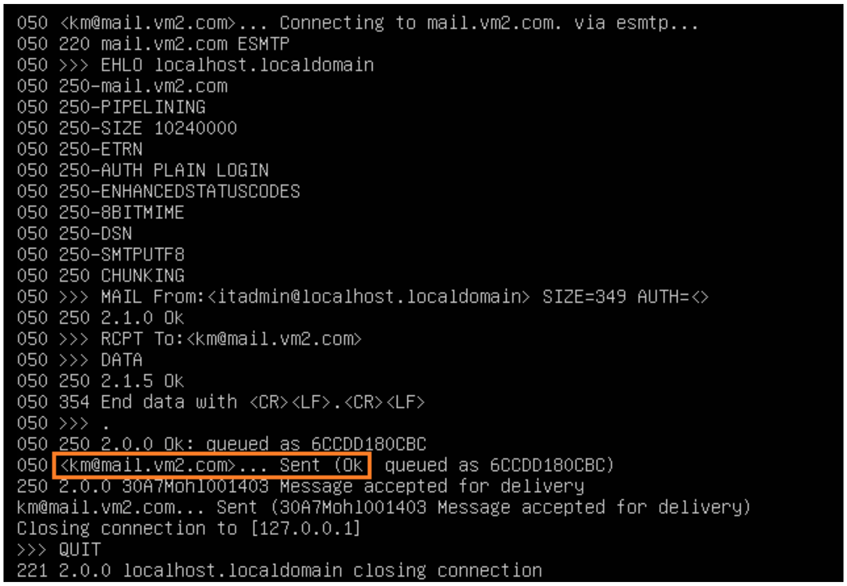
- Sending a non-spam mail to user mail address km@mail.vm2.com, from VM1 as shown in *Figure 5.10*.



```
root@vm1:/home/itadmin# sendmail -v km@mail.vm2.com
From:itadmin@localhost
Subject: Scenario 2
Hi Km.This is a test mail for scenario 2._
```

Figure 5.10 - Scenario 2: Non-spam mail being sent from VM1

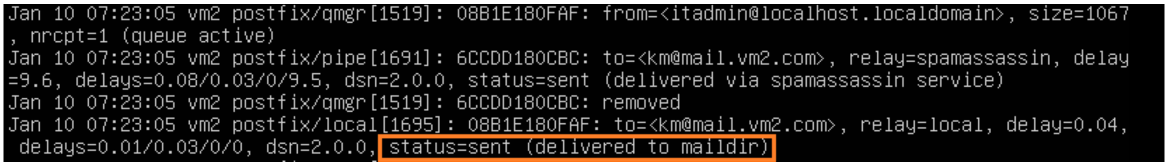
- Mail is successfully sent from VM1 as shown in *Figure 5.11*.



```
050 <km@mail.vm2.com>... Connecting to mail.vm2.com. via esmtp...
050 220 mail.vm2.com ESMTP
050 >>> EHLO localhost.localdomain
050 250-mail.vm2.com
050 250-PIPELINING
050 250-SIZE 10240000
050 250-ETRN
050 250-AUTH PLAIN LOGIN
050 250-ENHANCEDSTATUSCODES
050 250-8BITMIME
050 250-DSN
050 250-SMTPUTF8
050 250 CHUNKING
050 >>> MAIL From:<itadmin@localhost.localdomain> SIZE=349 AUTH=<>
050 250 2.1.0 Ok
050 >>> RCPT To:<km@mail.vm2.com>
050 >>> DATA
050 250 2.1.5 Ok
050 354 End data with <CR><LF>.<CR><LF>
050 >>> .
050 250 2.0.0 Ok: queued as 6CCDD180CBC
050 <km@mail.vm2.com>... Sent (Ok: queued as 6CCDD180CBC)
250 2.0.0 30A7Moh1001403 Message accepted for delivery
km@mail.vm2.com... Sent (30A7Moh1001403 Message accepted for delivery)
Closing connection to [127.0.0.1]
>>> QUIT
221 2.0.0 localhost.localdomain closing connection
```

Figure 5.11 - Scenario 2: Mail successfully sent

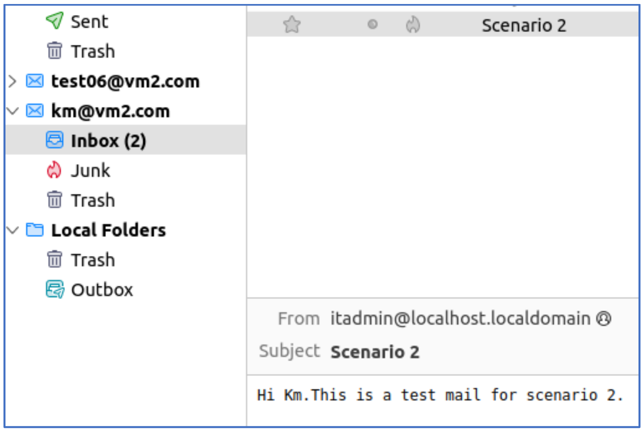
➢ The mail log from VM2 showing that the mail is successfully delivered to the mail directory as shown in *Figure 5.12*.



```
Jan 10 07:23:05 vm2 postfix/qmgr[1519]: 08B1E180FAF: from=<itadmin@localhost.localdomain>, size=1067
, nrcpt=1 (queue active)
Jan 10 07:23:05 vm2 postfix/pipe[1691]: 6CCDD180CBC: to=<km@mail.vm2.com>, relay=spamassassin, delay
=9.6, delays=0.08/0.03/0/9.5, dsn=2.0.0, status=sent (delivered via spamassassin service)
Jan 10 07:23:05 vm2 postfix/qmgr[1519]: 6CCDD180CBC: removed
Jan 10 07:23:05 vm2 postfix/local[1695]: 08B1E180FAF: to=<km@mail.vm2.com>, relay=local, delay=0.04,
 delays=0.01/0.03/0/0, dsn=2.0.0, status=sent (delivered to maildir)
```

Figure 5.12 – Scenario 2: Successful mail delivery message from message log

➢ The mail is successfully received in Thunderbird in VM3 as shown in *Figure 5.13*.



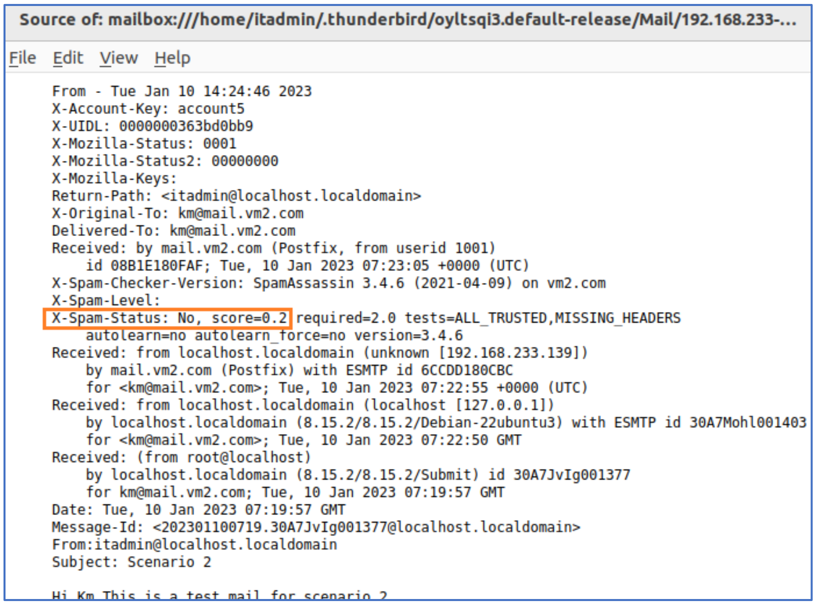
From itadmin@localhost.localdomain

Subject **Scenario 2**

```
Hi Km.This is a test mail for scenario 2.
```

Figure 5.13 - Scenario 2: Thunderbird successfully receives mail

- The view source of the mail as shown in *Figure 5.14*, concludes that the mail passed through the SpamAssassin service. Also, by having a Spam-Status: *No* with a score 0.2, the mail has been identified as a **non-spam** mail by SpamAssassin.



Source of: mailbox:///home/itadmin/.thunderbird/oyltsqi3.default-release/Mail/192.168.233-...

```
From - Tue Jan 10 14:24:46 2023
X-Account-Key: account5
X-UIDL: 0000000363bd0bb9
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: <itadmin@localhost.localdomain>
X-Original-To: km@mail.vm2.com
Delivered-To: km@mail.vm2.com
Received: by mail.vm2.com (Postfix, from userid 1001)
    id 08B1E180FAF; Tue, 10 Jan 2023 07:23:05 +0000 (UTC)
X-Spam-Checker-Version: SpamAssassin 3.4.6 (2021-04-09) on vm2.com
X-Spam-Level:
X-Spam-Status: No, score=0.2 required=2.0 tests=ALL_TRUSTED,MISSING_HEADERS
    autolearn=no autolearn_force=no version=3.4.6
Received: from localhost.localdomain (unknown [192.168.233.139])
    by mail.vm2.com (Postfix) with ESMTP id 6CCDD180CBC
    for <km@mail.vm2.com>; Tue, 10 Jan 2023 07:22:55 +0000 (UTC)
Received: from localhost.localdomain (localhost [127.0.0.1])
    by localhost.localdomain (8.15.2/8.15.2/Debian-22ubuntu3) with ESMTP id 30A7Mohl001403
    for <km@mail.vm2.com>; Tue, 10 Jan 2023 07:22:50 GMT
Received: (from root@localhost)
    by localhost.localdomain (8.15.2/8.15.2/Submit) id 30A7JvIg001377
    for km@mail.vm2.com; Tue, 10 Jan 2023 07:19:57 GMT
Date: Tue, 10 Jan 2023 07:19:57 GMT
Message-Id: <202301100719.30A7JvIg001377@localhost.localdomain>
From:itadmin@localhost.localdomain
Subject: Scenario 2

Hi Km This is a test mail for scenario 2
```

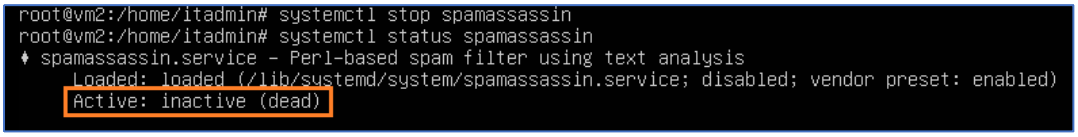
Figure 5.14 - Scenario 2: Mail view source

5.1.3 Scenario 3

Sending a spam mail from VM1 through the Mail Transfer Agent in VM2 and showing the received mail in Thunderbird (VM3).

In this scenario, both the SpamAssassin service and Thunderbird's junk filter are deactivated.

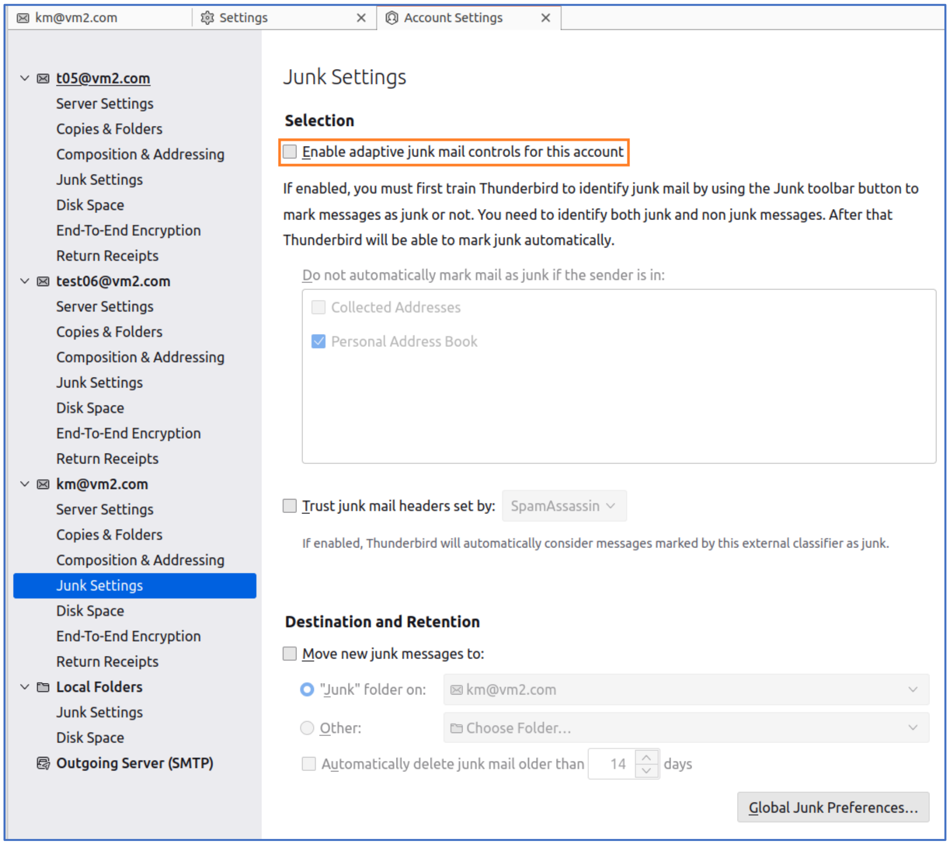
- SpamAssassin service is inactive as shown in *Figure 5.15*.



```
root@vm2:/home/itadmin# systemctl stop spamassassin
root@vm2:/home/itadmin# systemctl status spamassassin
♦ spamassassin.service - Perl-based spam filter using text analysis
     Loaded: loaded (/lib/systemd/system/spamassassin.service; disabled; vendor preset: enabled)
     Active: inactive (dead)
```

Figure 5.15 - Scenario 3: SpamAssassin service is deactivated

- Junk mail setting is inactive as shown in *Figure 5.16*.



Junk Settings

Selection

☐ Enable adaptive junk mail controls for this account

If enabled, you must first train Thunderbird to identify junk mail by using the Junk toolbar button to mark messages as junk or not. You need to identify both junk and non junk messages. After that Thunderbird will be able to mark junk automatically.

Do not automatically mark mail as junk if the sender is in:

☐ Collected Addresses

☑ Personal Address Book

☐ Trust junk mail headers set by: SpamAssassin

If enabled, Thunderbird will automatically consider messages marked by this external classifier as junk.

Destination and Retention

☐ Move new junk messages to:

● "Junk" folder on: km@vm2.com

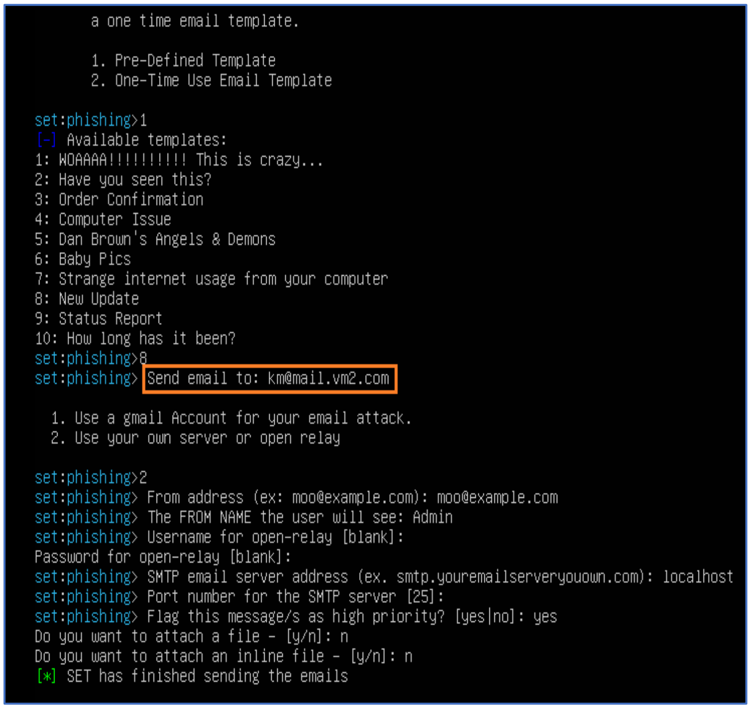
○ Other: Choose Folder…

☐ Automatically delete junk mail older than 14 days

Global Junk Preferences…

Figure 5.16 - Scenario 3: Thunderbird's junk setting is deactivated

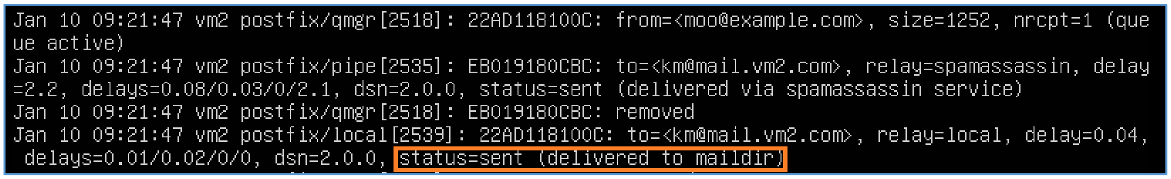
- Sending a spam mail through the Social Engineer Toolkit (SET) to user mail address km@mail.vm2.com, from VM1 as shown in *Figure 5.17*.



```
       a one time email template.

       1. Pre-Defined Template
       2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: WOAAAA!!!!!!!!!! This is crazy...
2: Have you seen this?
3: Order Confirmation
4: Computer Issue
5: Dan Brown's Angels & Demons
6: Baby Pics
7: Strange internet usage from your computer
8: New Update
9: Status Report
10: How long has it been?
set:phishing>8
set:phishing> Send email to: km@mail.vm2.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com): moo@example.com
set:phishing> The FROM NAME the user will see: Admin
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com): localhost
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]: yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
[*] SET has finished sending the emails
```

Figure 5.17 - Scenario 3: Spam mail sent from SET

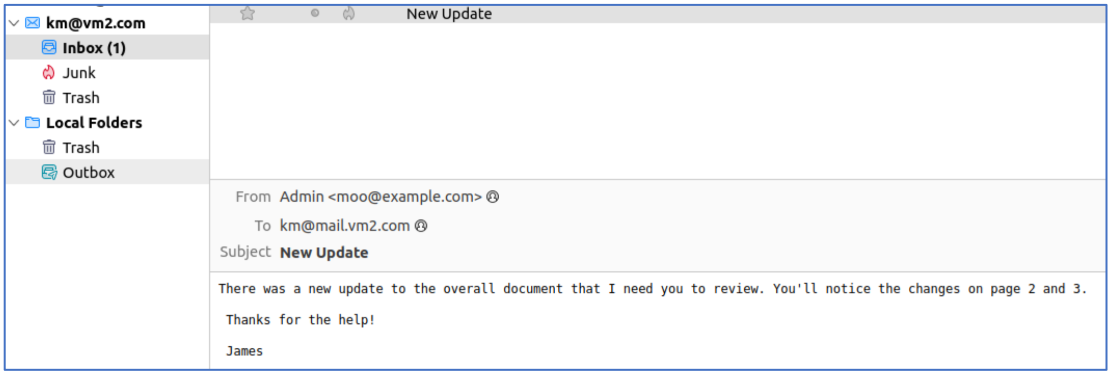
- The mail log from VM2 showing that the mail is successfully delivered to the mail directory as shown in *Figure 5.18*.



```
Jan 10 09:21:47 vm2 postfix/qmgr[2518]: 22AD118100C: from=<moo@example.com>, size=1252, nrcpt=1 (que
ue active)
Jan 10 09:21:47 vm2 postfix/pipe[2535]: EB019180CBC: to=<km@mail.vm2.com>, relay=spamassassin, delay
=2.2, delays=0.08/0.03/0/2.1, dsn=2.0.0, status=sent (delivered via spamassassin service)
Jan 10 09:21:47 vm2 postfix/qmgr[2518]: EB019180CBC: removed
Jan 10 09:21:47 vm2 postfix/local[2539]: 22AD118100C: to=<km@mail.vm2.com>, relay=local, delay=0.04,
 delays=0.01/0.02/0/0, dsn=2.0.0, status=sent (delivered to maildir)
```

Figure 5.18 - Scenario 3: Successful mail delivery message from message log

- The mail is successfully received in Thunderbird in VM3 as shown in *Figure 5.19*.

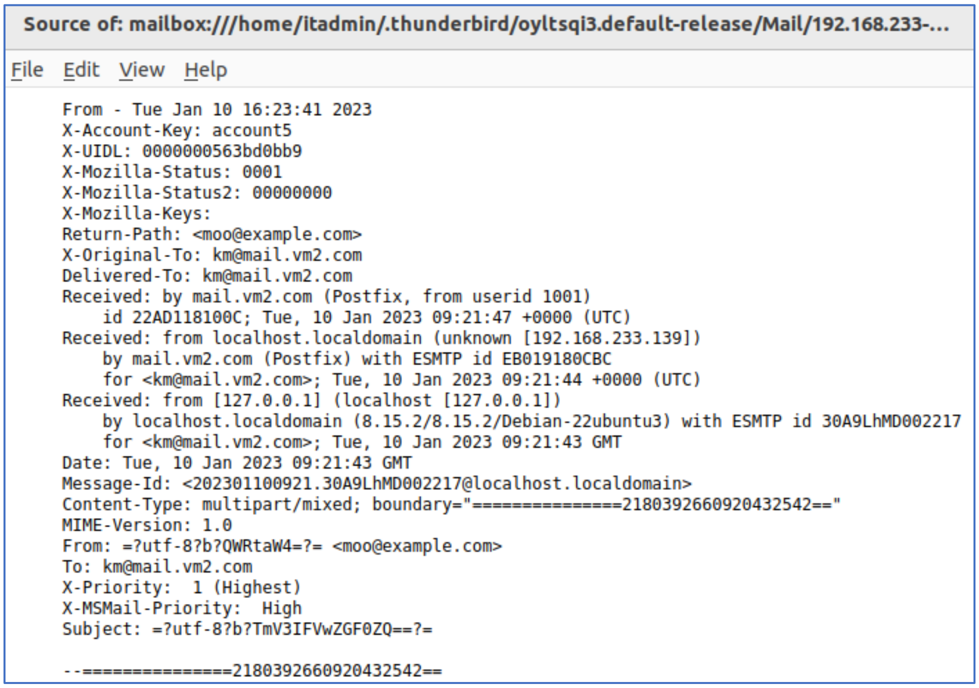


From Admin <moo@example.com>
To km@mail.vm2.com
Subject **New Update**

```
There was a new update to the overall document that I need you to review. You'll notice the changes on page 2 and 3.

 Thanks for the help!

 James
```

Figure 5.19 - Scenario 3: Thunderbird successfully receives mail

- The view source of the mail as shown in *Figure 5.20*, concludes that the mail did not pass through the SpamAssassin service since it was initially set as inactive. Thus, there is no spam status from SpamAssassin service. Also, since the junk setting is deactivated in Thunderbird, the mail is not marked as junk.


Source of: mailbox:///home/itadmin/.thunderbird/oyltsqi3.default-release/Mail/192.168.233-...
File
Edit
View
Help

```
From - Tue Jan 10 16:23:41 2023
X-Account-Key: account5
X-UIDL: 0000000563bd0bb9
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: <moo@example.com>
X-Original-To: km@mail.vm2.com
Delivered-To: km@mail.vm2.com
Received: by mail.vm2.com (Postfix, from userid 1001)
    id 22AD118100C; Tue, 10 Jan 2023 09:21:47 +0000 (UTC)
Received: from localhost.localdomain (unknown [192.168.233.139])
    by mail.vm2.com (Postfix) with ESMTP id EB019180CBC
    for <km@mail.vm2.com>; Tue, 10 Jan 2023 09:21:44 +0000 (UTC)
Received: from [127.0.0.1] (localhost [127.0.0.1])
    by localhost.localdomain (8.15.2/8.15.2/Debian-22ubuntu3) with ESMTP id 30A9LhMD002217
    for <km@mail.vm2.com>; Tue, 10 Jan 2023 09:21:43 GMT
Date: Tue, 10 Jan 2023 09:21:43 GMT
Message-Id: <202301100921.30A9LhMD002217@localhost.localdomain>
Content-Type: multipart/mixed; boundary="===============2180392660920432542=="
MIME-Version: 1.0
From: =?utf-8?b?QWRtaW4=?= <moo@example.com>
To: km@mail.vm2.com
X-Priority:  1 (Highest)
X-MSMail-Priority:  High
Subject: =?utf-8?b?TmV3IFVwZGF0ZQ==?=

--===============2180392660920432542==
```

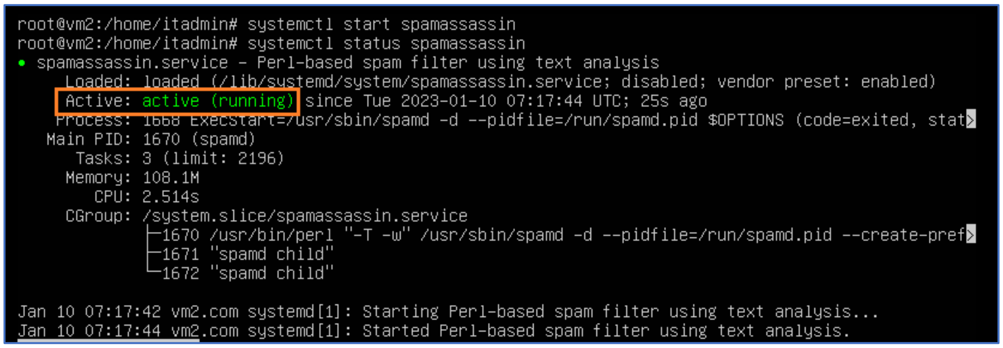
Figure 5.20 - Scenario 3: Mail view source

5.1.4 Scenario 4

Sending a spam mail from VM1 through the Mail Transfer Agent in VM2 and showing the received mail in Thunderbird (VM3).

In this scenario, the SpamAssassin service is activated while Thunderbird's junk filter is deactivated.

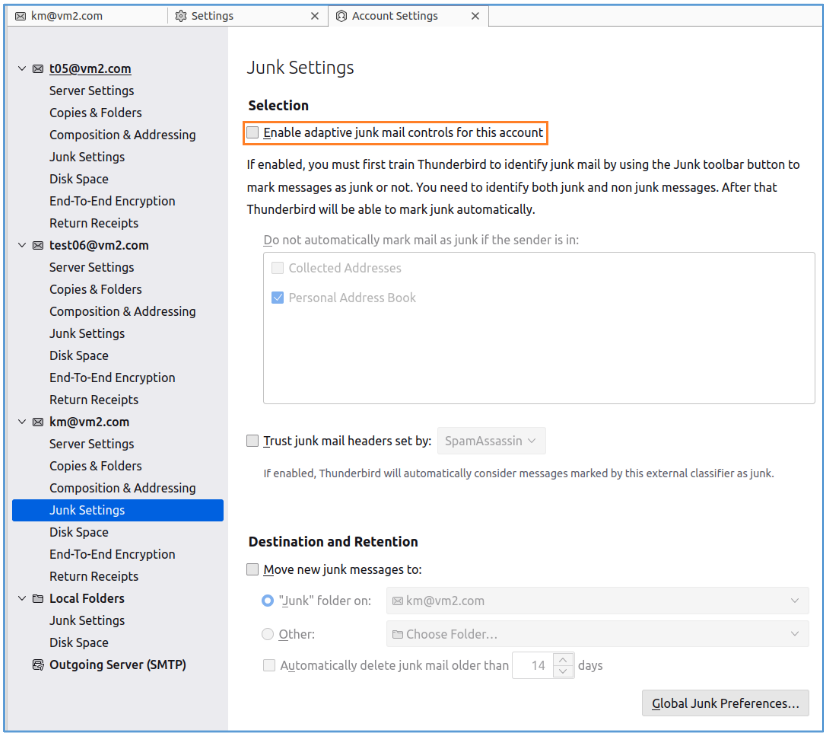
- SpamAssassin service is active as shown in *Figure 5.21*.



```
root@vm2:/home/itadmin# systemctl start spamassassin
root@vm2:/home/itadmin# systemctl status spamassassin
● spamassassin.service - Perl-based spam filter using text analysis
     Loaded: loaded (/lib/systemd/system/spamassassin.service; disabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-01-10 07:17:44 UTC; 25s ago
    Process: 1668 ExecStart=/usr/sbin/spamd -d --pidfile=/run/spamd.pid $OPTIONS (code=exited, stat>
   Main PID: 1670 (spamd)
      Tasks: 3 (limit: 2196)
     Memory: 108.1M
        CPU: 2.514s
     CGroup: /system.slice/spamassassin.service
             ├─1670 /usr/bin/perl "-T -w" /usr/sbin/spamd -d --pidfile=/run/spamd.pid --create-pref>
             ├─1671 "spamd child"
             └─1672 "spamd child"

Jan 10 07:17:42 vm2.com systemd[1]: Starting Perl-based spam filter using text analysis...
Jan 10 07:17:44 vm2.com systemd[1]: Started Perl-based spam filter using text analysis.
```

Figure 5.21 - Scenario 4: SpamAssassin service is activated

- Junk mail setting is inactive as shown in *Figure 5.22*.



Junk Settings

Selection

□ Enable adaptive junk mail controls for this account

If enabled, you must first train Thunderbird to identify junk mail by using the Junk toolbar button to mark messages as junk or not. You need to identify both junk and non junk messages. After that Thunderbird will be able to mark junk automatically.

Do not automatically mark mail as junk if the sender is in:

□ Collected Addresses

☑ Personal Address Book

□ Trust junk mail headers set by: SpamAssassin

If enabled, Thunderbird will automatically consider messages marked by this external classifier as junk.

Destination and Retention

□ Move new junk messages to:

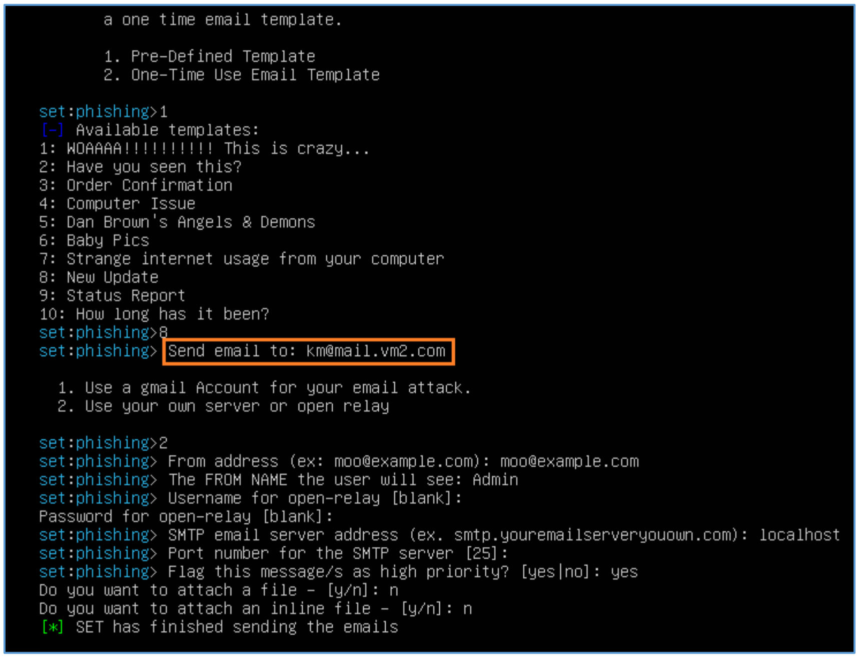
● "Junk" folder on: km@vm2.com

○ Other: Choose Folder…

□ Automatically delete junk mail older than 14 days

Figure 5.22 - Scenario 4: Thunderbird's junk setting is deactivated

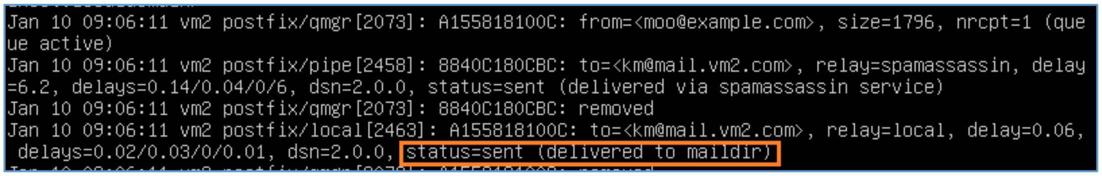
- Sending a spam mail through the Social Engineer Toolkit (SET) to user mail address km@mail.vm2.com, from VM1 as shown in *Figure 5.23*.



```
       a one time email template.

       1. Pre-Defined Template
       2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: WOAAAA!!!!!!!!!! This is crazy...
2: Have you seen this?
3: Order Confirmation
4: Computer Issue
5: Dan Brown's Angels & Demons
6: Baby Pics
7: Strange internet usage from your computer
8: New Update
9: Status Report
10: How long has it been?
set:phishing>8
set:phishing> Send email to: km@mail.vm2.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com): moo@example.com
set:phishing> The FROM NAME the user will see: Admin
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com): localhost
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]: yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
[*] SET has finished sending the emails
```

Figure 5.23 - Scenario 4: Spam mail sent from SET

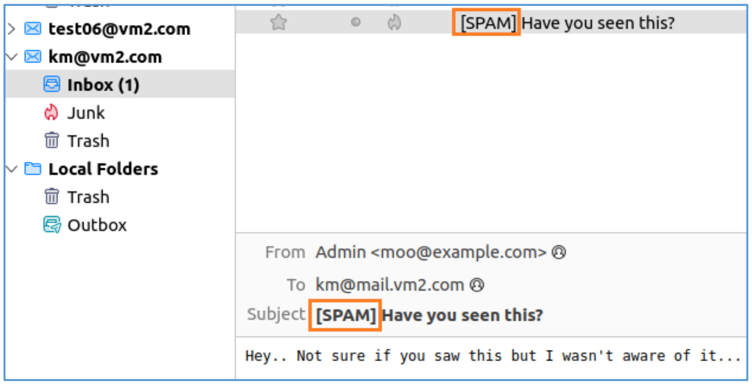
- ➢ The mail log from VM2 showing that the mail is successfully delivered to the mail directory as shown in *Figure 5.24*.



```
Jan 10 09:06:11 vm2 postfix/qmgr[2073]: A155818100C: from=<moo@example.com>, size=1796, nrcpt=1 (que
ue active)
Jan 10 09:06:11 vm2 postfix/pipe[2458]: 8840C180CBC: to=<km@mail.vm2.com>, relay=spamassassin, delay
=6.2, delays=0.14/0.04/0/6, dsn=2.0.0, status=sent (delivered via spamassassin service)
Jan 10 09:06:11 vm2 postfix/qmgr[2073]: 8840C180CBC: removed
Jan 10 09:06:11 vm2 postfix/local[2463]: A155818100C: to=<km@mail.vm2.com>, relay=local, delay=0.06,
 delays=0.02/0.03/0/0.01, dsn=2.0.0, status=sent (delivered to maildir)
```

Figure 5.24 - Scenario 4: Successful mail delivery message from message log

- ➢ The mail is successfully received in Thunderbird in VM3. Since the SpamAssassin service is activated, the mail is marked as [SPAM] as shown in *Figure 5.25*.



From Admin <moo@example.com>

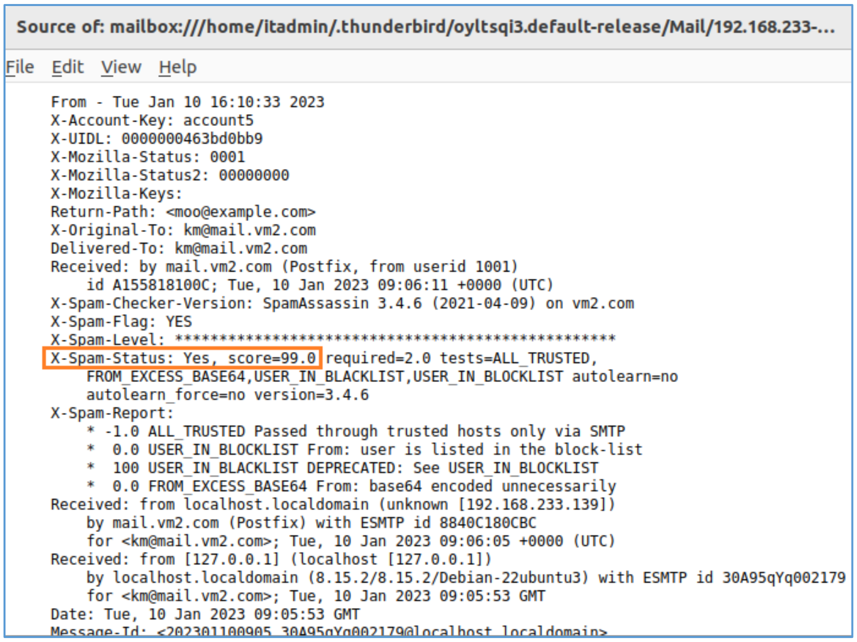
To km@mail.vm2.com

Subject [SPAM] Have you seen this?

Hey.. Not sure if you saw this but I wasn't aware of it...

Figure 5.25 - Scenario 4: Thunderbird successfully receives mail

- The view source of the mail as shown in *Figure 5.26*, concludes that the mail passed through the SpamAssassin service. Also, by having a Spam-Status: *Yes* with a score *99.0*, the mail has been identified as a **spam** mail by the SpamAssassin service.


Source of: mailbox:///home/itadmin/.thunderbird/oyltsqi3.default-release/Mail/192.168.233-...
File Edit View Help

```
From - Tue Jan 10 16:10:33 2023
X-Account-Key: account5
X-UIDL: 0000000463bd0bb9
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: <moo@example.com>
X-Original-To: km@mail.vm2.com
Delivered-To: km@mail.vm2.com
Received: by mail.vm2.com (Postfix, from userid 1001)
    id A155818100C; Tue, 10 Jan 2023 09:06:11 +0000 (UTC)
X-Spam-Checker-Version: SpamAssassin 3.4.6 (2021-04-09) on vm2.com
X-Spam-Flag: YES
X-Spam-Level: **************************************************
X-Spam-Status: Yes, score=99.0 required=2.0 tests=ALL_TRUSTED,
    FROM_EXCESS_BASE64,USER_IN_BLACKLIST,USER_IN_BLOCKLIST autolearn=no
    autolearn_force=no version=3.4.6
X-Spam-Report:
    * -1.0 ALL_TRUSTED Passed through trusted hosts only via SMTP
    *  0.0 USER_IN_BLOCKLIST From: user is listed in the block-list
    *  100 USER_IN_BLACKLIST DEPRECATED: See USER_IN_BLOCKLIST
    *  0.0 FROM_EXCESS_BASE64 From: base64 encoded unnecessarily
Received: from localhost.localdomain (unknown [192.168.233.139])
    by mail.vm2.com (Postfix) with ESMTP id 8840C180CBC
    for <km@mail.vm2.com>; Tue, 10 Jan 2023 09:06:05 +0000 (UTC)
Received: from [127.0.0.1] (localhost [127.0.0.1])
    by localhost.localdomain (8.15.2/8.15.2/Debian-22ubuntu3) with ESMTP id 30A95qYq002179
    for <km@mail.vm2.com>; Tue, 10 Jan 2023 09:05:53 GMT
Date: Tue, 10 Jan 2023 09:05:53 GMT
Message-Id: <202301100905.30A95qYq002179@localhost.localdomain>
```

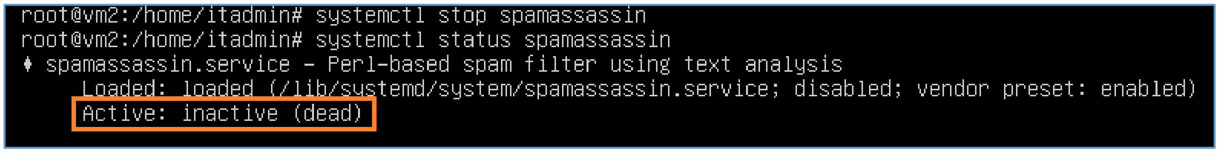
Figure 5.26 - Scenario 4: Mail view source

5.1.5 Scenario 5

Sending a spam mail from VM1 through the Mail Transfer Agent in VM2 and showing the received mail in Thunderbird (VM3).

In this scenario, the SpamAssassin service is deactivated while Thunderbird's junk filter is activated.

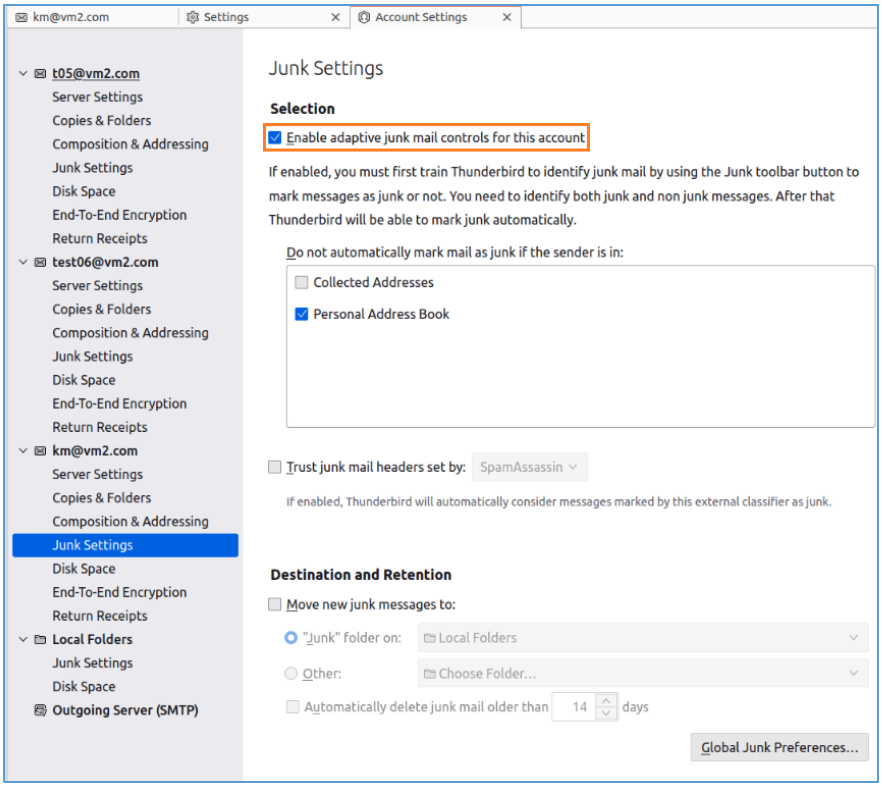
➢ SpamAssassin service is inactive as shown in *Figure 5.27*.



```
root@vm2:/home/itadmin# systemctl stop spamassassin
root@vm2:/home/itadmin# systemctl status spamassassin
● spamassassin.service - Perl-based spam filter using text analysis
     Loaded: loaded (/lib/systemd/system/spamassassin.service; disabled; vendor preset: enabled)
     Active: inactive (dead)
```

Figure 5.27 - Scenario 5: SpamAssassin service is deactivated

➢ Junk mail setting is active as shown in *Figure 5.28*.



Junk Settings

Selection

☑ Enable adaptive junk mail controls for this account

If enabled, you must first train Thunderbird to identify junk mail by using the Junk toolbar button to mark messages as junk or not. You need to identify both junk and non junk messages. After that Thunderbird will be able to mark junk automatically.

Do not automatically mark mail as junk if the sender is in:

☐ Collected Addresses

☑ Personal Address Book

☐ Trust junk mail headers set by: SpamAssassin

If enabled, Thunderbird will automatically consider messages marked by this external classifier as junk.

Destination and Retention

☐ Move new junk messages to:

● "Junk" folder on: Local Folders

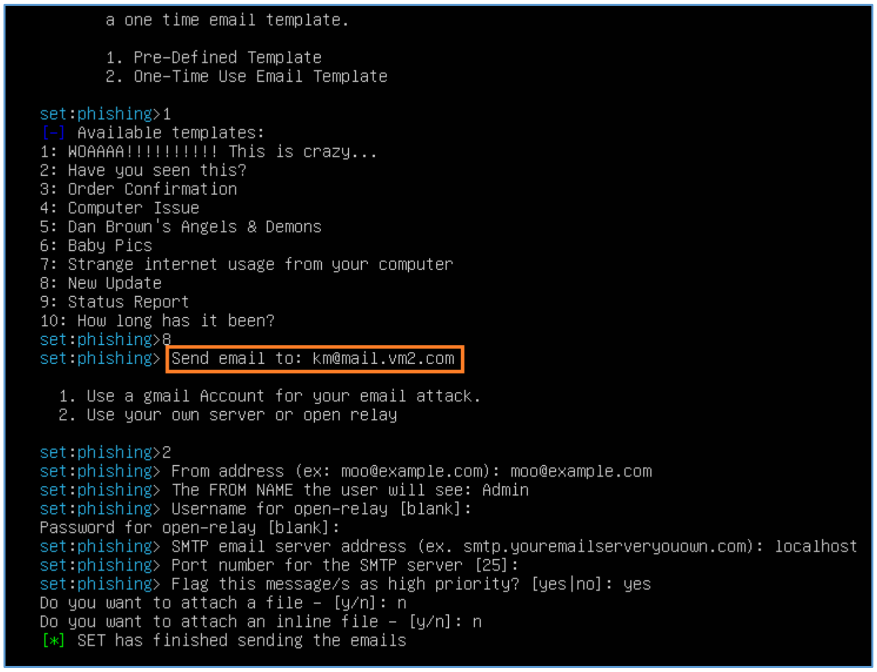
○ Other: Choose Folder...

☐ Automatically delete junk mail older than 14 days

Global Junk Preferences...

Figure 5.28 - Scenario 5: Thunderbird's junk setting is deactivated

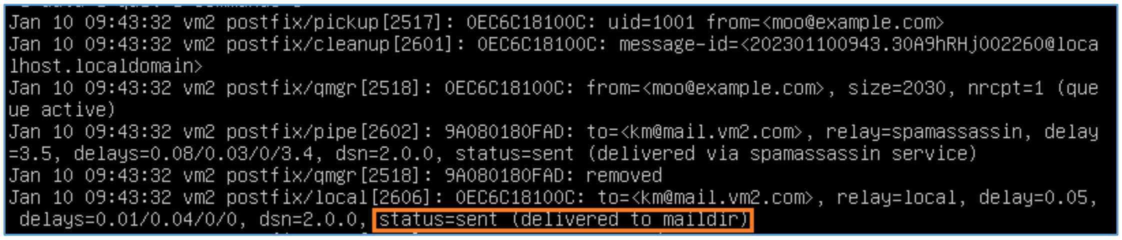
➢ Sending a spam mail through the Social Engineer Toolkit (SET) to user mail address km@mail.vm2.com, from VM1 as shown in *Figure 5.29*.



```
        a one time email template.

        1. Pre-Defined Template
        2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: WOAAAA!!!!!!!!!! This is crazy...
2: Have you seen this?
3: Order Confirmation
4: Computer Issue
5: Dan Brown's Angels & Demons
6: Baby Pics
7: Strange internet usage from your computer
8: New Update
9: Status Report
10: How long has it been?
set:phishing>8
set:phishing> Send email to: km@mail.vm2.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com): moo@example.com
set:phishing> The FROM NAME the user will see: Admin
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com): localhost
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]: yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
[*] SET has finished sending the emails
```

Figure 5.29 - Scenario 5: Spam mail sent from SET

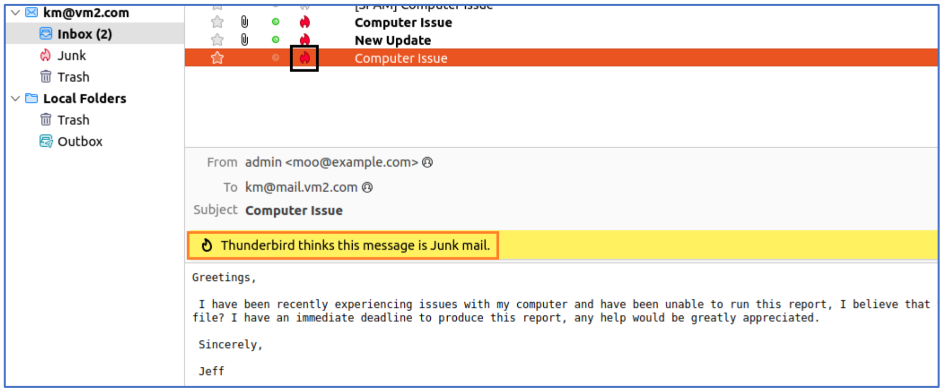
- ➢ The mail log from VM2 showing that the mail is successfully delivered to the mail directory as shown in *Figure 5.30*.



```
Jan 10 09:43:32 vm2 postfix/pickup[2517]: 0EC6C18100C: uid=1001 from=<moo@example.com>
Jan 10 09:43:32 vm2 postfix/cleanup[2601]: 0EC6C18100C: message-id=<20230110094 3.30A9hRHj002260@loca
lhost.localdomain>
Jan 10 09:43:32 vm2 postfix/qmgr[2518]: 0EC6C18100C: from=<moo@example.com>, size=2030, nrcpt=1 (que
ue active)
Jan 10 09:43:32 vm2 postfix/pipe[2602]: 9A080180FAD: to=<km@mail.vm2.com>, relay=spamassassin, delay
=3.5, delays=0.08/0.03/0/3.4, dsn=2.0.0, status=sent (delivered via spamassassin service)
Jan 10 09:43:32 vm2 postfix/qmgr[2518]: 9A080180FAD: removed
Jan 10 09:43:32 vm2 postfix/local[2606]: 0EC6C18100C: to=<km@mail.vm2.com>, relay=local, delay=0.05,
 delays=0.01/0.04/0/0, dsn=2.0.0, status=sent (delivered to maildir)
```

Figure 5.30 - Scenario 5: Successful delivery message from message log

- ➢ The mail is successfully received in Thunderbird in VM3. Since Thunderbird's junk filter is activated, the mail is also marked as junk. But since SpamAssassin service is deactivated, the mail is not marked as [SPAM], as shown in *Figure 5.31*.



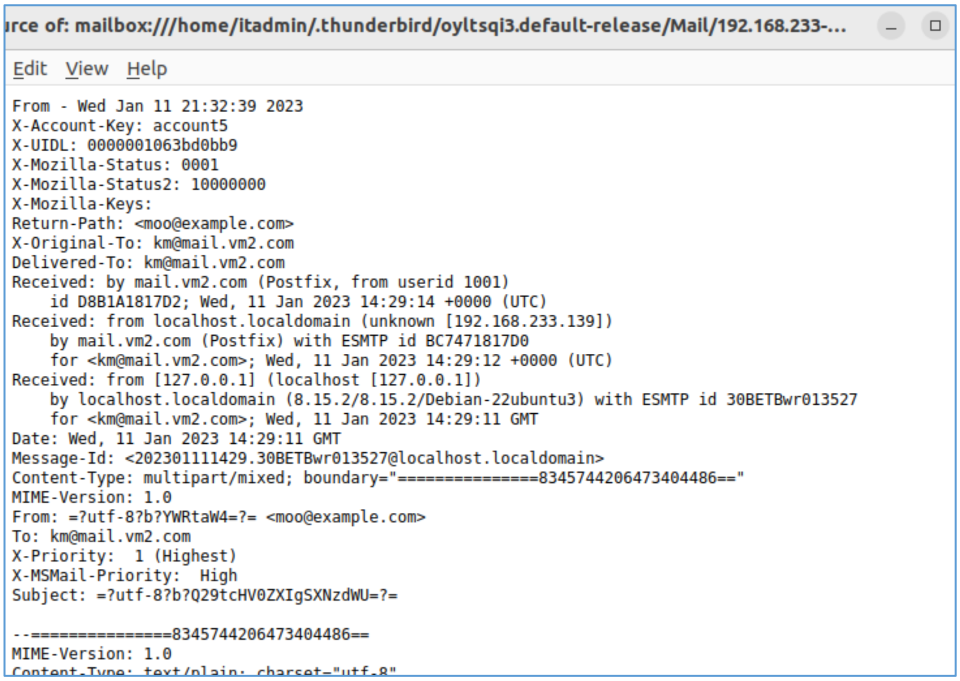
From admin <moo@example.com>
To km@mail.vm2.com
Subject **Computer Issue**

Thunderbird thinks this message is Junk mail.

```
Greetings,

 I have been recently experiencing issues with my computer and have been unable to run this report, I believe that
file? I have an immediate deadline to produce this report, any help would be greatly appreciated.

 Sincerely,

 Jeff
```

Figure 5.31 - Scenario 5: Thunderbird successfully receives mail

- The view source of the mail as shown in *Figure 5.32*, concludes that the mail did not pass through the SpamAssassin service, so there is no spam status from SpamAssassin. However, mail is marked as junk in Thunderbird. But, there is no indication of spam or junk mail in the source code.


ırce of: mailbox:///home/itadmin/.thunderbird/oyltsqi3.default-release/Mail/192.168.233-...
Edit View Help

```
From - Wed Jan 11 21:32:39 2023
X-Account-Key: account5
X-UIDL: 0000001063bd0bb9
X-Mozilla-Status: 0001
X-Mozilla-Status2: 10000000
X-Mozilla-Keys:
Return-Path: <moo@example.com>
X-Original-To: km@mail.vm2.com
Delivered-To: km@mail.vm2.com
Received: by mail.vm2.com (Postfix, from userid 1001)
    id D8B1A1817D2; Wed, 11 Jan 2023 14:29:14 +0000 (UTC)
Received: from localhost.localdomain (unknown [192.168.233.139])
    by mail.vm2.com (Postfix) with ESMTP id BC7471817D0
    for <km@mail.vm2.com>; Wed, 11 Jan 2023 14:29:12 +0000 (UTC)
Received: from [127.0.0.1] (localhost [127.0.0.1])
    by localhost.localdomain (8.15.2/8.15.2/Debian-22ubuntu3) with ESMTP id 30BETBwr013527
    for <km@mail.vm2.com>; Wed, 11 Jan 2023 14:29:11 GMT
Date: Wed, 11 Jan 2023 14:29:11 GMT
Message-Id: <202301111429.30BETBwr013527@localhost.localdomain>
Content-Type: multipart/mixed; boundary="===============8345744206473404486=="
MIME-Version: 1.0
From: =?utf-8?b?YWRtaW4=?= <moo@example.com>
To: km@mail.vm2.com
X-Priority:  1 (Highest)
X-MSMail-Priority:  High
Subject: =?utf-8?b?Q29tcHV0ZXIgSXNzdWU=?=

--===============8345744206473404486==
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
```

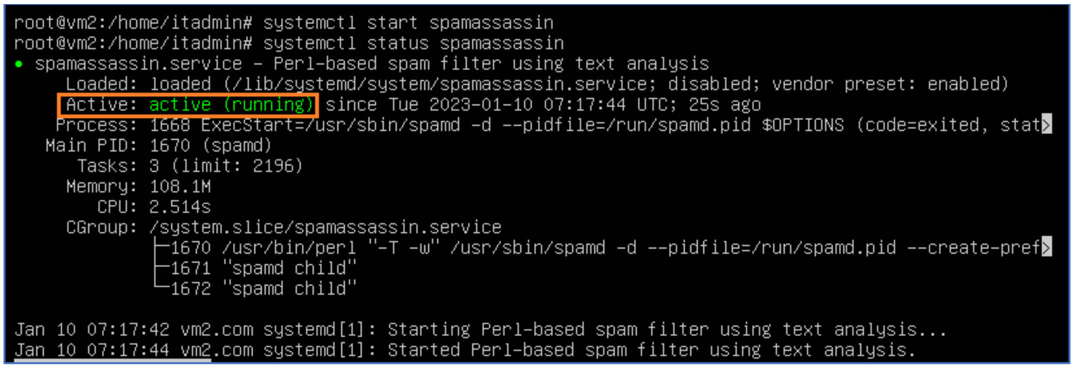
Figure 5.32 - Scenario 5: Mail view source

5.1.6 Scenario 6

Sending a spam mail from VM1 through the Mail Transfer Agent in VM2 and showing the received mail in Thunderbird (VM3).

In this scenario, both the SpamAssassin service and Thunderbird's junk filter are activated.

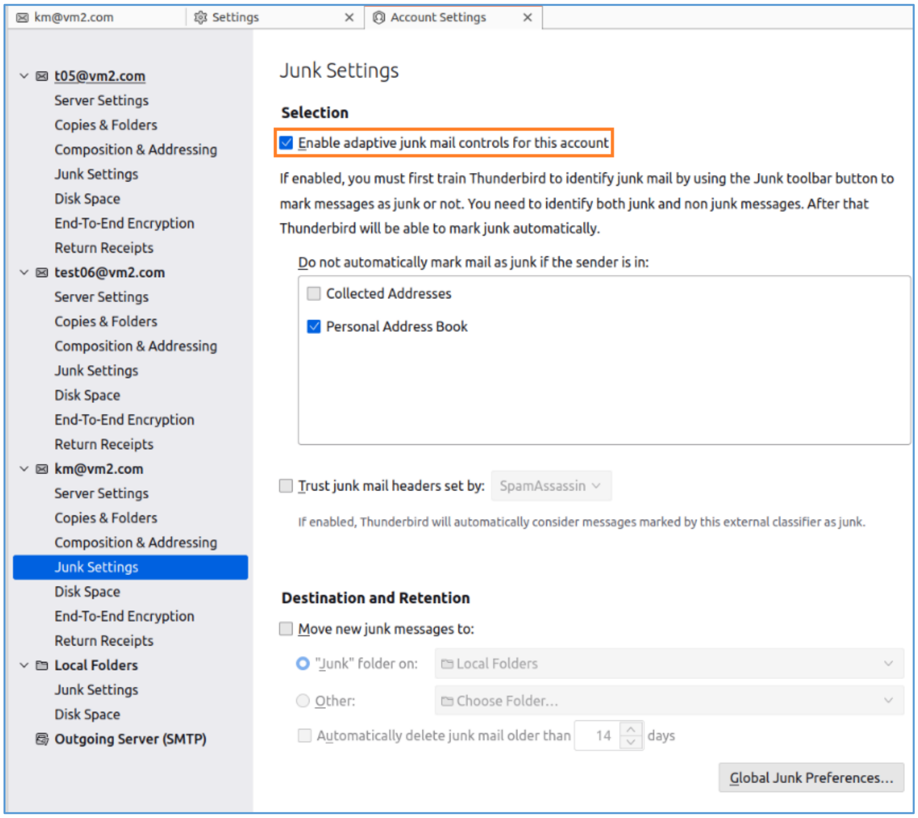
- SpamAssassin service is active as shown in *Figure 5.33*.



```
root@vm2:/home/itadmin# systemctl start spamassassin
root@vm2:/home/itadmin# systemctl status spamassassin
● spamassassin.service - Perl-based spam filter using text analysis
     Loaded: loaded (/lib/systemd/system/spamassassin.service; disabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-01-10 07:17:44 UTC; 25s ago
    Process: 1668 ExecStart=/usr/sbin/spamd -d --pidfile=/run/spamd.pid $OPTIONS (code=exited, stat>
   Main PID: 1670 (spamd)
      Tasks: 3 (limit: 2196)
     Memory: 108.1M
        CPU: 2.514s
     CGroup: /system.slice/spamassassin.service
             ├─1670 /usr/bin/perl "-T -w" /usr/sbin/spamd -d --pidfile=/run/spamd.pid --create-pref>
             ├─1671 "spamd child"
             └─1672 "spamd child"

Jan 10 07:17:42 vm2.com systemd[1]: Starting Perl-based spam filter using text analysis...
Jan 10 07:17:44 vm2.com systemd[1]: Started Perl-based spam filter using text analysis.
```

Figure 5.33 - Scenario 6: SpamAssassin service is activated

- Junk mail setting is active as shown in *Figure 5.34*.



Junk Settings

Selection

☑ Enable adaptive junk mail controls for this account

If enabled, you must first train Thunderbird to identify junk mail by using the Junk toolbar button to mark messages as junk or not. You need to identify both junk and non junk messages. After that Thunderbird will be able to mark junk automatically.

Do not automatically mark mail as junk if the sender is in:

☐ Collected Addresses

☑ Personal Address Book

☐ Trust junk mail headers set by: SpamAssassin

If enabled, Thunderbird will automatically consider messages marked by this external classifier as junk.

Destination and Retention

☐ Move new junk messages to:

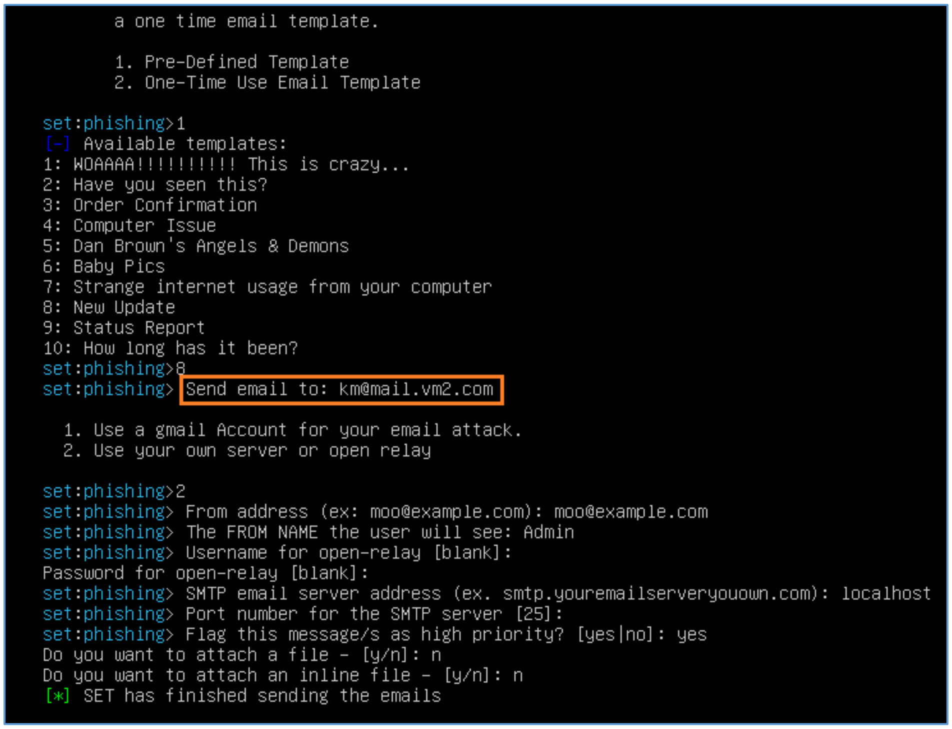
● "Junk" folder on: Local Folders

○ Other: Choose Folder...

☐ Automatically delete junk mail older than 14 days

Figure 5.34 - Scenario 6: Thunderbird's junk setting is activated

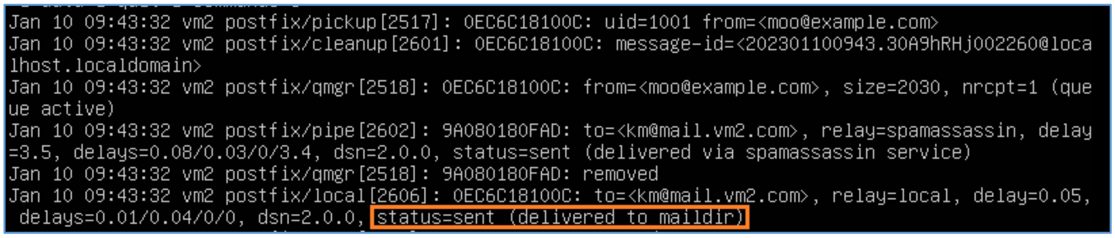
- Sending a spam mail through the Social Engineer Toolkit (SET) to user mail address km@mail.vm2.com, from VM1 as shown in *Figure 5.35*.



```
        a one time email template.

        1. Pre-Defined Template
        2. One-Time Use Email Template

   set:phishing>1
   [-] Available templates:
   1: WOAAAA!!!!!!!!!! This is crazy...
   2: Have you seen this?
   3: Order Confirmation
   4: Computer Issue
   5: Dan Brown's Angels & Demons
   6: Baby Pics
   7: Strange internet usage from your computer
   8: New Update
   9: Status Report
   10: How long has it been?
   set:phishing>8
   set:phishing> Send email to: km@mail.vm2.com

     1. Use a gmail Account for your email attack.
     2. Use your own server or open relay

   set:phishing>2
   set:phishing> From address (ex: moo@example.com): moo@example.com
   set:phishing> The FROM NAME the user will see: Admin
   set:phishing> Username for open-relay [blank]:
   Password for open-relay [blank]:
   set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com): localhost
   set:phishing> Port number for the SMTP server [25]:
   set:phishing> Flag this message/s as high priority? [yes|no]: yes
   Do you want to attach a file - [y/n]: n
   Do you want to attach an inline file - [y/n]: n
   [*] SET has finished sending the emails
```

Figure 5.35 - Scenario 6: Spam mail sent from SET

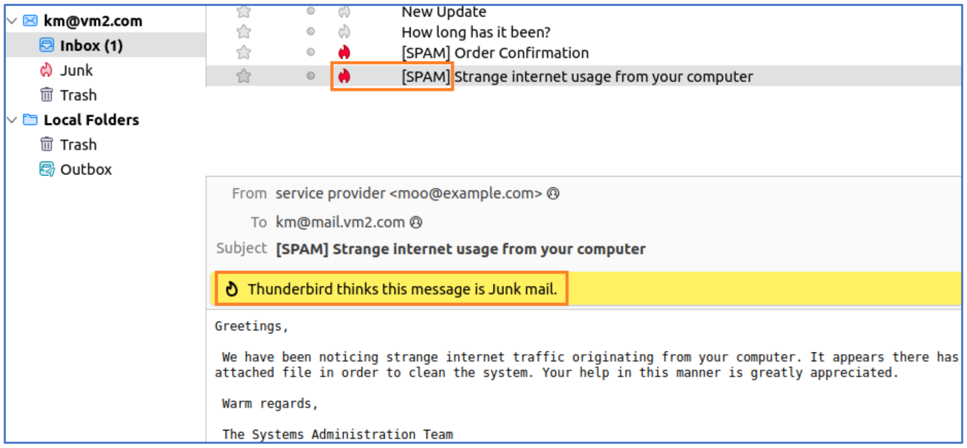
- The mail log from VM2 showing that the mail is successfully delivered to the mail directory as shown in *Figure 5.36*.



```
Jan 10 09:43:32 vm2 postfix/pickup[2517]: 0EC6C18100C: uid=1001 from=<moo@example.com>
Jan 10 09:43:32 vm2 postfix/cleanup[2601]: 0EC6C18100C: message-id=<202301100943.30A9hRHj002260@loca
lhost.localdomain>
Jan 10 09:43:32 vm2 postfix/qmgr[2518]: 0EC6C18100C: from=<moo@example.com>, size=2030, nrcpt=1 (que
ue active)
Jan 10 09:43:32 vm2 postfix/pipe[2602]: 9A080180FAD: to=<km@mail.vm2.com>, relay=spamassassin, delay
=3.5, delays=0.08/0.03/0/3.4, dsn=2.0.0, status=sent (delivered via spamassassin service)
Jan 10 09:43:32 vm2 postfix/qmgr[2518]: 9A080180FAD: removed
Jan 10 09:43:32 vm2 postfix/local[2606]: 0EC6C18100C: to=<km@mail.vm2.com>, relay=local, delay=0.05,
 delays=0.01/0.04/0/0, dsn=2.0.0, status=sent (delivered to maildir)
```

Figure 5.36 – Scenario 6: Successful mail delivery message from mail log

- The mail is successfully received in Thunderbird in VM3. Since the SpamAssassin service is activated, the mail is marked as [SPAM] and since Thunderbird's junk filter is activated, the mail is also marked as junk, as shown in *Figure 5.37*.



km@vm2.com
Inbox (1)
Junk
Trash
Local Folders
Trash
Outbox

New Update
How long has it been?
[SPAM] Order Confirmation
[SPAM] Strange internet usage from your computer

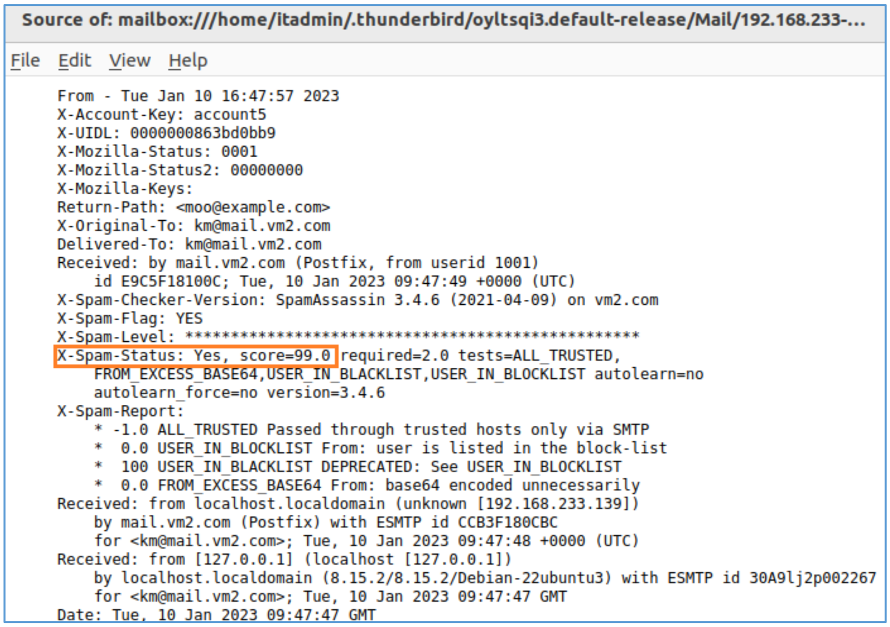
From service provider <moo@example.com>
To km@mail.vm2.com
Subject **[SPAM] Strange internet usage from your computer**

Thunderbird thinks this message is Junk mail.

```
Greetings,

 We have been noticing strange internet traffic originating from your computer. It appears there has
attached file in order to clean the system. Your help in this manner is greatly appreciated.

 Warm regards,

 The Systems Administration Team
```

Figure 5.37 - Scenario 6: Thunderbird successfully receives mail

- The view source of the mail as shown in *Figure 5.38*, concludes that the mail passed through the SpamAssassin service. By having a Spam-Status: *Yes* with a score 99.0, the mail has been identified as a **spam** mail by the SpamAssassin service. Also, the mail is marked as junk in Thunderbird.



Source of: mailbox:///home/itadmin/.thunderbird/oyltsqi3.default-release/Mail/192.168.233-...

```
From - Tue Jan 10 16:47:57 2023
X-Account-Key: account5
X-UIDL: 0000000863bd0bb9
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: <moo@example.com>
X-Original-To: km@mail.vm2.com
Delivered-To: km@mail.vm2.com
Received: by mail.vm2.com (Postfix, from userid 1001)
    id E9C5F18100C; Tue, 10 Jan 2023 09:47:49 +0000 (UTC)
X-Spam-Checker-Version: SpamAssassin 3.4.6 (2021-04-09) on vm2.com
X-Spam-Flag: YES
X-Spam-Level: **************************************************
X-Spam-Status: Yes, score=99.0 required=2.0 tests=ALL_TRUSTED,
    FROM_EXCESS_BASE64,USER_IN_BLACKLIST,USER_IN_BLOCKLIST autolearn=no
    autolearn_force=no version=3.4.6
X-Spam-Report:
    * -1.0 ALL_TRUSTED Passed through trusted hosts only via SMTP
    *  0.0 USER_IN_BLOCKLIST From: user is listed in the block-list
    *  100 USER_IN_BLACKLIST DEPRECATED: See USER_IN_BLOCKLIST
    *  0.0 FROM_EXCESS_BASE64 From: base64 encoded unnecessarily
Received: from localhost.localdomain (unknown [192.168.233.139])
    by mail.vm2.com (Postfix) with ESMTP id CCB3F180CBC
    for <km@mail.vm2.com>; Tue, 10 Jan 2023 09:47:48 +0000 (UTC)
Received: from [127.0.0.1] (localhost [127.0.0.1])
    by localhost.localdomain (8.15.2/8.15.2/Debian-22ubuntu3) with ESMTP id 30A9lj2p002267
    for <km@mail.vm2.com>; Tue, 10 Jan 2023 09:47:47 GMT
Date: Tue, 10 Jan 2023 09:47:47 GMT
```

Figure 5.38 - Scenario 6: Mail view source

Finally, to evaluate and compare the outcomes of my designed tool, a summary of the above-described scenarios, is presented in *Table 1*.

Scenario	Description	Remark
1	Sending a **non-spam** mail from VM1 through the Mail Transfer Agent inVM2 and showing the received mail in Thunderbird (VM3). SpamAssassin service - desactivated Thunderbird's junk filter - deactivated	**No spam status** from SpamAssasin service in the source code.
2	Sending a **non-spam** mail from VM1 through the Mail Transfer Agent inVM2 and showing the received mail in Thunderbird (VM3). SpamAssassin service - activated Thunderbird's junk filter - deactivated	**Spam-Status: No** Score: 0.2 Mail identified as a **non-spam** mail by SpamAssassin.
3	Sending a **spam** mail from VM1 through the Mail Transfer Agent in VM2 and showing the received mail in Thunderbird (VM3). SpamAssassin service - desactivated Thunderbird's junk filter - deactivated	**No spam status** from SpamAssassin service. Mail is **not marked as junk**.
4	Sending a **spam** mail from VM1 through the Mail Transfer Agent in VM2 and showing the received mail in Thunderbird (VM3). SpamAssassin service - activated Thunderbird's junk filter - deactivated	**Spam-Status: Yes** Score: 99.0 Mail identified as a **spam** mail by SpamAssassin.
5	Sending a spam mail from VM1 through the Mail Transfer Agent in VM2 and showing the received mail in Thunderbird (VM3). SpamAssassin service - deactivated Thunderbird's junk filter - activated	**No spam status** from SpamAssassin service. Mail **marked as junk** in Thunderbird. No indication of spam or junk mail in the source code.
6	Sending a spam mail from VM1 through the Mail Transfer Agent in VM2 and showing the received mail in Thunderbird (VM3). SpamAssassin service - activated Thunderbird's junk filter - activated	**Spam-Status: Yes** Score: 99.0 Mail identified as a **spam mail** by SpamAssassin and marked as **junk** in Thunderbird.

Table 5.1 - Summary of the six tested scenarios

With reference to the table, the conclusion that can be derived from the six testing scenarios is that activating both the SpamAssassin service and the Thunderbird's junk filter is more effective and the best strategy to alert users to spam mail. A genuine spam email will thereafter be flagged as [SPAM] by the SpamAssassin service and as junk by the Thunderbird mail service. As a result, the user will be reminded not to read spam email and will be protected from spear phishing attacks.

5.2 How is my system better than existing systems?

- Scalability: My system can handle increasing user and email messages without performance degradation.
- Reliability: My system can operate consistently and can be reused on another machine to detect the spam.
- Security: The measures in place to protect the system and email messages from unauthorized access or tampering.
- Usability: The system's ease and functionality for users and administrators.
- Cost: The financial costs associated with implementing and maintaining the system, including hardware and software expenses, labour costs, and other overhead.

My mail server system protects against phishing attacks by using the following:

- Spam filters: The use of spam filters, such as SpamAssassin , can help identify and block phishing emails based on specific characteristics or patterns.
- Email authentication: Implementing email authentication protocols, such as SPF, DKIM, and DMARC, can help verify the authenticity of email messages and prevent fraudulent statements from being delivered to users.
- User education: Providing users with training and resources on recognizing and avoiding phishing attacks can help reduce the risk of successful attacks.
- Policies and procedures: Implementing policies and procedures for handling suspicious emails, such as a process for reporting potential phishing attacks, can help mitigate the impact of successful attacks.

To determine whether the mail server system is better or worse than existing systems, it would be helpful to consider these and other factors in the context of the specific goals and requirements. It may also be beneficial to compare the system to other mail server systems in terms of particular features and capabilities, such as the type and number of supported protocols, the level of customisation and configuration options, and the level of integration with other systems and applications.

It is also worth noting that the "best" mail server system for a given organisation to use may vary depending on the specific needs and goals of that organisation. For example, a highly scalable and reliable system may be a top priority for a large enterprise with thousands of users. In contrast, a lower cost and simple user interface system may be more critical for small businesses with limited resources.

Ultimately, the decision of which mail server system is "best" will depend on the specific needs and goals of the organisation, as well as the resources available to implement and maintain the system. Careful research and planning can help ensure that the chosen method is well-suited to the organisation's needs and provides the desired performance and functionality.

One primary ethical concern with spear phishing is the deception involved. To carry out a successful spear phishing attack, the attacker must create a compelling and believable message or communication that appears to come from a trusted source. This often involves manipulating the appearance of the message or creating fake websites or documents that look legitimate. This deception can have severe consequences for the victims of spear phishing, who may suffer financial losses, identity theft, or other harm resulting from falling for the attack.

Another ethical concern with spear phishing is the potential for harm to the victim's organisation or community. By tricking an individual within an organisation into divulging sensitive information, an attacker can gain access to sensitive business data or systems. This harm may extend beyond the immediate victim to affect other individuals or organisations, such as customers or partners.

In addition to the direct harm caused by spear phishing, this type of attack raises broader ethical concerns about the proliferation of cyber-attacks and their impact on society. Cyber-attacks can undermine trust in online communication and commerce, and the increasing prevalence of spear phishing and other types of cyber-attacks can erode people's confidence in the security of the online world.

Given these ethical concerns, individuals and organisations must protect themselves against spear phishing attacks. This can include educating employees about the risks of spear phishing and how to identify and avoid these attacks, implementing technical measures such as email filtering and two-factor authentication, and being cautious about the information shared online. It is also essential for society to address the root causes of cyber-attacks, such as the lack of cybersecurity regulation and the availability of tools and resources for carrying out these types of attacks.

Consequently, this is why the project was developed and tested on virtual machine using open-source tools so as not to harm other users.

6 Conclusion & Future Works

This chapter of this research displays and discusses the research findings. Hence, recommendations are provided relying on these findings. Also, this chapter concludes the study by giving suggestions for future works to the subject area and focusing on the limitations were faced during conducting the study.

6.1 What worked in the project?

As the project manager for the effort to address spear phishing threats using the Waterfall model, I found that several key elements of this approach contributed to its success.

First and foremost, the emphasis on gathering requirements and defining the project scope at the outset proved extremely valuable. By carefully assessing the organisation's needs and goals, we could tailor the solution we developed to meet these requirements. This helped to ensure that the answer was effective and addressed the specific challenges and threats faced by the organisation.

In addition, the focus on testing and quality assurance was crucial in ensuring that our solution was effective. By conducting simulated spear phishing attacks and gathering feedback from employees, we were able to identify any weaknesses or areas for improvement and make adjustments as needed. This helped ensure that the solution could effectively protect against spear phishing threats and that employees were aware of and understood the new procedures and policies.

Finally, the maintenance and ongoing support provided as part of the Waterfall model helped to ensure that the solution remained effective over time. By providing ongoing training and updates to the technical measures in place, we were able to stay ahead of new threats and continue to protect against spear phishing attacks.

Overall, the Waterfall model proved to be a successful approach for addressing spear phishing threats. Its emphasis on gathering requirements, testing and quality assurance, and ongoing support were critical factors in its success.

6.2 My contributions to the project

As the project manager for this effort to address spear phishing threats using the Waterfall model, my contributions included:

1. Leading the project team and overseeing the overall process of gathering requirements, designing a solution, implementing it, testing it, and maintaining it over time.
2. Working with the organisation to understand their specific needs and goals and using this information to develop a solution that meets these requirements.
3. Coordinating the development of training materials and policies to educate employees on recognizing and avoiding spear phishing attacks and implementing technical measures such as email filters and authentication protocols.
4. Conducting simulated spear phishing attacks and gathering feedback from employees to ensure that the solution was adequate and that employees understood and followed the new procedures and policies.

5. Providing ongoing support and maintenance to ensure the solution's effectiveness, including training and updating the technical measures.

Overall, my contributions as the project manager were focused on leading the team and coordinating the efforts to address spear phishing threats using the Waterfall model, with a focus on gathering requirements, designing a solution, implementing it, testing it, and maintaining it over time.

6.3 Future Developments

There are several potential areas for future development regarding spear phishing threats using the Waterfall model.

One area that could be considered is the use of artificial intelligence and machine learning technologies to enhance the effectiveness of email security measures. For example, machine learning algorithms could analyse email patterns and identify potentially malicious emails in real-time, allowing organisations to block these threats before they can reach employees.

Another potential area for development is the use of multi-factor authentication (MFA) to increase the security of email accounts and protect against spear phishing attacks. MFA requires additional forms of authentication, such as a code sent to a mobile phone and a password to access an account. This can make it much more difficult for attackers to gain unauthorized access to sensitive information.

Finally, there may be opportunities to develop new training materials and policies to educate employees on recognizing and avoiding spear phishing attacks. This could involve incorporating interactive elements, such as simulations or quizzes, to help employees better understand and remember the critical principles for staying safe online.

Overall, there are many potential areas for future development regarding spear phishing threats using the Waterfall model. By leveraging new technologies and approaches, organisations can continue to evolve their strategies and stay ahead of new threats.

Some strategies and technologies can be used to protect against phishing attacks, including spam filters, email authentication protocols, user education, and policies and procedures for handling suspicious emails. Implementing a combination of these measures can help reduce the risk of successful phishing attacks and mitigate their impact.

However, it is important to note that no single solution is foolproof, and phishing attacks are constantly evolving and becoming more sophisticated. As such, it is crucial to stay up-to-date with the latest threats and best practices and regularly review and update your phishing protection measures.

In addition to technical measures, there are also non-technical strategies that can be effective in preventing phishing attacks. For example, creating a culture of security awareness within an organisation can help encourage employees to be more vigilant and less likely to fall for phishing scams.

Protecting against phishing attacks requires a multi-faceted approach that combines technical and non-technical measures (Mohtashimi, 2016). By taking a proactive and comprehensive approach to phishing protection, organisations and individuals can better defend against these attacks and reduce the risk of harm.

To protect against spear phishing attacks, it is essential to implement a combination of technical and non-technical measures. This can include spam filters, email authentication protocols, user education, and policies and procedures for handling suspicious emails. In addition, organisations can implement security awareness training programs to help educate employees about the signs of spear phishing attacks and how to identify and avoid them.

It is also important to regularly review and update your spear phishing protection measures, as spear phishing attacks are constantly evolving and becoming more sophisticated. By taking a proactive and comprehensive approach to spear phishing protection, organisations and individuals can better defend against these attacks and reduce the risk of harm.

User education is vital to protect against phishing attacks and cyber-attacks (Byarswright, 2022). By educating users about the risks and tactics of phishing attacks, organisations can help employees and other individuals to become more aware of the signs of phishing and more capable of identifying and avoiding these types of attacks.

There are several key topics that organisations can cover when educating users about phishing attacks:

- What is phishing: It is essential to explain to users what phishing is and how it works. This can include examples of common phishing attacks, such as email and website phishing, and the tactics that attackers use to trick individuals into revealing sensitive information or taking the desired action.
- How to identify phishing attacks: Users should be taught to recognize the signs of phishing attacks, such as suspicious email addresses, unusual requests for personal information, and links that go to unexpected or unfamiliar websites. It can also be helpful to provide users with resources, such as lists of standard phishing email subject lines, to help them identify phishing emails.
- What to do if you receive a phishing email: Users should be instructed on what to do if they receive a phishing email. This can include deleting the email, reporting it to the appropriate authorities, and not clicking on any links or attachments.
- How to protect against phishing attacks: Users should be taught about the various measures they can take to protect themselves against phishing attacks, such as keeping their software and security protocols up to date, using strong passwords, and being cautious when providing personal information online.

In addition to covering these topics, it can be helpful to use interactive and engaging methods for delivering user education, such as online training modules, simulations, and quizzes. This can help to ensure that users retain the information and are more likely to apply it in real-world situations.

Overall, user education is an essential component of any phishing protection strategy. By educating users about the risks and tactics of phishing attacks, organisations can help to reduce the risk of successful attacks and mitigate their impact.

- Check the sender’s email address: Phishers often use fake or forged email addresses that mimic those of legitimate organisations or individuals. Check the sender’s email address carefully and ensure that it is legitimate before interacting with the email or message.
- Be cautious when providing personal information: Be especially wary of requests for personal information, such as your name, address, or login credentials.

Legitimate organisations will typically not ask for this information via email or other unsecured channels.

- Use spam filters and email authentication protocols: Implementing spam filters and email authentication protocols, such as SPF, DKIM, and DMARC, can help to identify and block phishing emails before they reach your inbox.
- Keep your software and security protocols up to date: Keeping your software and security protocols up to date can help to protect against phishing attacks and other types of cyber-attacks.

Following these and other best practices can significantly reduce your risk of falling victim to phishing and cyber-attacks.

If you suspect you have been the target of a spear phishing attack, taking immediate action is essential to protect yourself and minimize the attack's potential impact. Here are some steps you can take:

1. Do not click on any links or open attachments in the suspicious email or message.
2. Forward the email or message to your organisation's IT or security team or a trusted third party, such as your email provider's security team.
3. Change any passwords or log in credentials that may have been compromised due to the attack. Be sure to use strong, unique passwords and enable two-factor authentication if possible.
4. Monitor your accounts and financial statements for any unauthorized activity.
5. If you provided any sensitive information, such as login credentials or financial information, report the incident to the relevant authorities and take steps to protect yourself, such as freezing your credit or changing your account numbers.
6. Review your security practices and consider implementing additional measures to protect against future attacks, such as email authentication protocols and providing user education on identifying and avoiding phishing attacks.

By taking these steps and remaining vigilant, you can help to mitigate the impact of a spear phishing attack and protect yourself against future attacks.

1. Technology solutions: Governments can also invest in technology solutions that can help detect and prevent phishing attacks. This might include software that can identify and block phishing emails or systems that monitor suspicious activity on websites and alert authorities.
2. Victims' assistance: Governments can provide support and resources to individuals and organisations victimized by phishing attacks. This might include financial aid to cover losses, counselling services to help cope with the emotional impact of the attack, and guidance on how to take steps to protect against future attacks.

Overall, governments need to take a multi-faceted approach to combat phishing. This might include education and awareness, law enforcement, regulation and standards, international cooperation, technology solutions, and assistance to victims. By working together and leveraging various strategies, governments can help protect their citizens and organisations from the harmful effects of phishing.

6.4 General measures to discourage phishing

There are several measures that individuals and organisations can take to discourage phishing and protect themselves from these types of attacks. Some of the most effective measures include:

1. ***Educating users:*** One of the most effective ways to discourage phishing is to inform users about the threat (Staff, 2022). This can be done through regular training and awareness programs and simulated phishing attacks that help users learn to identify and report phishing attempts.
2. ***Implementing technical controls:*** Technical controls, such as spam filters and email gateways, can help to identify and block phishing emails before they reach users. These tools can be configured to flag emails containing suspicious links or attachments or from known phishing domains.

3. ***Enforcing solid passwords and enabling two-factor authentication:*** Strong passwords and two-factor authentication (2FA) can make it more difficult for attackers to access sensitive accounts. Users should be encouraged to use unique, complex passwords for each account, and 2FA should be enabled whenever possible.
4. ***Regularly updating software and systems (Kalio, 2022):*** Keeping software and procedures updated with the latest patches and updates is critical for security. These updates often include fixes for known vulnerabilities that attackers could exploit.
5. ***Monitoring for suspicious activity:*** Regularly monitoring for suspicious activity, such as unusual login attempts or access to sensitive data, can help to identify and respond to potential phishing attacks.
6. ***Using caution when interacting with unknown entities:*** Users should be cautious when interacting with unknown entities, whether by email, phone, or in person. They should verify the legitimacy of any request for sensitive information before complying and be aware of common phishing tactics, such as requests to update account information or to click on a link to verify their login credentials.
7. ***Implementing a secure communication channel:*** For sensitive communications, organisations should consider using a secure communication channel, such as a virtual private network (VPN) or a secure messaging app, to protect against potential interception or tampering.
8. ***Establishing a response plan:*** A clear and well-defined response plan can help organisations quickly and effectively respond to phishing attacks and minimize the potential impact. This should include procedures for identifying and reporting phishing attempts and steps for recovering from a successful attack.

By taking these and other measures to discourage phishing, individuals and organisations can significantly reduce their risk of falling victim to these attacks and protect themselves from the potential harm they can cause.

6.5 Contributions

In my contribution to addressing spear phishing attacks, I have developed a system that aims to provide a more secure and effective method for protecting against these types of attacks. One of the critical features of my design is its ability to analyse incoming emails and identify those likely to be spear phishing attacks. This is achieved through advanced machine learning algorithms trained on a large dataset of known phishing emails. These algorithms can analyse various aspects of the email, such as the content, sender, and links, to determine the likelihood that it is a spear phishing attack.

Another essential feature of my system is its ability to alert users to the presence of a spear phishing attack and provide guidance on how to respond. This may involve displaying a warning message to the user, highlighting potentially suspicious elements of the email, or giving information on verifying the email's authenticity before taking action. In addition, my system includes several security measures to help protect against spear phishing attacks. These may consist of two-factor authentication, which requires an additional form of authentication to log in, and strong, unique passwords for all accounts.

My system aims to provide a comprehensive approach to protecting against spear phishing attacks by combining advanced email analysis, user education, and security measures. Using my method, organisations and individuals can significantly reduce their risk of falling victim to these attacks and protect their sensitive information and assets.

7 List of references

A. Bratko, G. V. Cormack, B. Filipic, T. R. Lynam, and B. Zupan. Spam filtering using statistical data compression models. Journal of Machine Learning Research, 6:2673–2698, 2006.

Ali, S. U., Rahman, M. S., & Al-Sarawi, S. F. (2016). Preventing phishing attacks: A review of existing approaches. International Journal of Advanced Computer Science and Applications, 7(7), 53-61.

Byarswright (2022) *Cyber claims Phishing scam prevention and identification*, *Byars Wright*. Available at: https://www.byarswright.com/phishing-scam-prevention/ (Accessed: December 21, 2022).

EZMarketing (2021) *Why phishing is more dangerous than ever, and how to protect yourself*, *EZComputer Solutions*. EZComputer Solutions. Available at: https://www.ezcomputersolutions.com/blog/why-phishing-is-dangerous/ (Accessed: December 21, 2022).

Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Security*, *27*(6), 581–612. https://doi.org/10.3233/jcs-181253

Gupta, R. and Kumar Shukla, P. (2015) "Performance analysis of anti-phishing tools and study of Classification Data Mining Algorithms for a novel Anti-phishing system," *International Journal of Computer Network and Information Security*, 7(12), pp. 70–77. Available at: https://doi.org/10.5815/ijcnis.2015.12.08

Harald Baayen, Hans van Halteren, Anneke Neijt, and Fiona Tweedie. 2002. An experiment in authorship attribution. In Journ´ees internationales d'Analyse statistique des Donn`ees Textuelles.

Hashemi, M., Mohtashimi, S., & Zare, Z. (2016). A survey of anti-phishing techniques. International Journal of Computer Science and Information Security, 14(3), 1-8.

Hassan, M. A., Al-Shawabka, A., & Al-Nemrat, A. (2014). A review of anti-phishing techniques. International Journal of Advanced Computer Science and Applications, 5(6), 61-68.

Hebert, A. *et al.* (2022) *How to recognize and avoid phishing scams*, *Consumer Advice*. Available at: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (Accessed: December 21, 2022.

Ian Androutsopoulos, John Koutsias, V. Chandrinos, George Paliouras, and C. Spyropoulos. 2000. An evaluation of naive bayesian anti-spam filtering. In Workshop on Machine Learning in the New Information Age.

James, L. (2019). Crossing the phishing line. *Phishing Exposed*, 137–214. https://doi.org/10.1016/b978-159749030-6/50009-x KnowBe4 (no date) *Phishing techniques*, *Phishing*. Available at: https://www.phishing.org/phishing-techniques (Accessed: December 21, 2022).

Joachim Schramm, Patrick Dohrmann, Andreas Rausch, Thomas Ternité, "Process Model Engineering Lifecycle: Holistic Concept Proposal and Sy tematic Literature Review", in proceedings of 40th Euromicro Conference on Software Engineering and Advanced Applications, 2014

Kalio, S. (2022) "Phishing attack: Raising awareness and protection techniques." Available at: https://doi.org/10.31234/osf.io/uxeth

Khandelwal, S. and Das, R. (2022) "Image processing-based phishing detection techniques," *Phishing Detection Using Content-Based Image Classification*, pp. 7–16. Available at: https://doi.org/10.1201/9781003217381-2.

Khandelwal, S., & Das, R. (2022). Phishing and Cybersecurity. *Phishing Detection Using Content-Based Image Classification*, 1–6. https://doi.org/10.1201/9781003217381-1

Kirda, E., & Kruegel, C. (2005, July). Protecting users against phishing attacks with antiphish. In 29th Annual International Computer Software and Applications Conference (COMPSAC'05) (Vol. 1, pp. 517-524). IEEE.

Luca Cernuzzi, Massimo Cossentino, Franco Zambonelli, "Process models for agent-based development", Engineering Applications of Artificial Intelligence, vol. 18, pp. 205–222, 2005

Mary Salvaggio, Molly Graizzaro, “97% Of People Globally Unable to Correctly Identify Phishing Emails, 2015”, Article, http://newsroom.mcafee.com/press-release/97-people-globally-unablecorrectly-identify-phishing-emails

Microsoft’s Anti-Phishing Technologies and Tactics. (n.d.). *Phishing and Countermeasures*, 551–562. https://doi.org/10.1002/9780470086100.ch15

Mohd, M., Shahzad, S., & Qasim, U. (2015). Phishing attacks: An overview and classification. International Journal of Computer Applications, 107(6), 1-6.

Nayab, M., Aslam, M., & Adeel, M. (2015). A survey on phishing attacks and countermeasures. International Journal of Advanced Computer Science and Applications, 6(8), 38-44.

S. Myers. Introduction to phishing. In M. Jakobsson and S. Myers, editors, Phishing and Countermeasures, pages 1–29. Wiley, 2007.

Sanford, D. (2022) *Preventing phishing: 7 tips for stopping phishing attacks*, *ConnectWise*.

Shearn, J. (2021) *Dangers of phishing*, *CIO Solutions*. Available at: https://www.ciosolutions.com/dangers-of-phishing/ (Accessed: December 21, 2022).

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, July). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In Proceedings of the 3rd symposium on Usable privacy and security (pp. 88-99). ACM.

Singh, G. (2022) How does email work? A dummies guide, Medium. Building Mailmodo. Available at: https://medium.com/building-mailmodo/how-does-email-work-a-dummies-guide-bd1ef894797e (Accessed: January 16, 2023).

Sonowal, G. (2021). Characteristics of phishing websites. *Phishing and Communication Channels*, 97–113. https://doi.org/10.1007/978-1-4842-7744-7_5

Sonowal, G. (2022). Phishing and Communication Channels. https://doi.org/10.1007/978-1-4842-7744-7

Staff, S. (2022) *4 recommendations to combat phishing*, *Security Magazine RSS*. Security Magazine. Available at: https://www.securitymagazine.com/articles/98585-4-recommendations-to-combat-phishing (Accessed: December 21, 2022).

Suganya, V. (2016) “A review on phishing attacks and various anti phishing techniques,” *International Journal of Computer Applications*, 139(1), pp. 20–23. Available at: https://doi.org/10.5120/ijca2016909084.

Team, G.L.S. (2022) *Phishing 201: Advanced phishing techniques*, *Global Learning Systems*. Available at: https://globallearningsystems.com/advanced-phishing-techniques/ (Accessed: December 20, 2022).

Usharani, B. (2022) “Machine learning and deep learning techniques for phishing threats and challenges,” *Cyber-Physical Systems*, pp. 123–146. Available at: https://doi.org/10.1002/9781119836636.ch6.

Villadiego, R. (2017) *Council post: The dangers of phishing*, *Forbes*. Forbes Magazine. Available at: https://www.forbes.com/sites/forbestechcouncil/2017/09/14/the-dangers-of-phishing/ (Accessed: December 21, 2022).

Weber, L. (2018) *Easy online security: Phishing -- viruses -- cyberfraud -- Lifelock -- equifax -- ransomware*. Lincolnwood, IL: Publications International, Ltd.

Zurier, S. (2016) *5 tips for combating phishing*, *Dark Reading*. Available at: https://www.darkreading.com/operations/5-tips-for-combating-phishing (Accessed: December 21, 2022).