Generating & Detecting Phishing Emails Using Kali Linux And Their Protecting Measures

Ganesh Kadam[1], Arun Hattarge[2]
[1,2]Assistant Professor, Dept of Computer Engineering
[1, 2] G H Raisoni Institute of Engineering & Technology, Pune, Maharashtra

Abstract- *Today phishing email is one of the common and dangerous way of hacking. In this paper we investigate how phishing emails are generated using spoofing techniques in kali Linux and smtp server. Next, we study some clues to detect phishing emails and penetration testing. Phishing emails are generally used to send infected attachments. This paper mainly focus on to overcome these phishing email issues to secure email communication.*

Keywords- Phishing, spoofing, kali Linux, payload, smtp server

I. INTRODUCTION

Electronic mail (email or e-mail) is a method of exchanging messages between people using electronic devices. Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously, they need to connect, typically to a mail server or a webmail interface to send or receive messages or download it. Every day millions of emails communicated over the world so, emails are the most favorite way to transmit messages from one another. Emails are specially targeted by hackers to send infected files, images, and pdfs to create backdoors. Generally in phishing emails, hackers create fake emails using spoofing techniques, smtp servers and kali Linux then it send to target the victim.[1] Identifying fishing emails is very complicated task to newbie. Phishing emails are look like as identical as original emails but there are several ways to detect phishing emails by observing itspatterns, emails body, address and other details.
This paper will describe details procedure about how to create fake phishing mails using spoofing in kali Linux and identifies several ways to detect it by observing its patterns.

II. WHAT IS PHISHING?

Phishing is the cybercrime in which a target are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive date such as personally identifiable information , banking and credit card details, and passwords.

The information is then used to access important accounts and can result in identify theft and financial loss.

Email Spoofing

Email spoofing [1] is the fabrication of an email header in the hopes of duping the recipient into thinking the email originated form someone or somewhere other than the intended source. Because core email protocols do not have a built-in method of authentication, it is commonplace for span and phishing emails to use said spoofing to trick the recipient into trusting the origin of the message.

The ultimate goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation. Although the spoofed messages are usually just a nuisance requiring little action besides removal, the more malicious varieties can causes significant problems, and sometimes pose a real security threat.

As an example, a spoofed email may purport to be from a well-known retail business, asking the recipient to provide personal information like a password or credit card number. The fake email might even ask the recipient to click on a link offering a limited time deal, which is actually just a link to download and install malware on the recipient’s device.

III. KALI LINUX INTORDUCTION

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are used in various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.

Kali is having more than 600 penetration testing tools which is used to study penetration testing on various devises and systems.

Here in kali Linux sendemail program is used to generate fake mail by using terminal commands. Smtp server account will generate api key which is used to send fake mail to victim. We create fake mail as like as original so, victim might think that is generated from original source.

IV. PROCESS OF CREATING FAKE MAIL IN KALI LINUX

Requirements: Kali Linux, any smtp server account (here we used sendgrid as smtp server)

Steps:

1. Open Kali Linux operating system.
2. Open browser and log in to sendgridsmtp server account and copy server, port and api/password key.
2. Open Terminal and enter following command using proper credentials to generate fake email.

```
root@kali :sendemail -t (destination address ) –f (from eg. foo@bar.com ) –s (server:port) –xu (smtp server username ) –xp (smtp password/apikey) –u (subject) –m (message)
```

When victim opens email then he/she will see mail coming from smtp server with hiding original credentials. If required attacker or hacker should include malicious link, infected images, files etc. to hack or create backdoor on victims system.

V. HOW TO DETECT PHISHING EMAIL

There are several ways available to detect phishing emails and its infected contents. Here will discuss these ways.

Good Antivirus Program: A good antivirus program always stop phishing emails reaching your inbox. It will also safeguard you from any cybercriminal attacks. Again it's not enough to just install antivirus software's because Hackers are so expert now to bypass security and access your system by passing vulnerability. Today cyber criminals have plenty of tricks to deceive you.

So, if you are not installing antivirus program and you still want to detect phishing mails then following are the methods which explains it.

1. Email send from public domain:

No legitimate organization will contact you from an address that ends '@gmail.com'. Not even Google. With the exception of independent workers, every organization likes banks, finance companies etc. will have its own email domain and company accounts. For example, legitimate emails from Google will read '@google.com'.

If the domain name (the bit after the @ symbol) matches the apparent sender of the email, the message is probably legitimate. The best way to check an organizations domain name is to type the company's name into a search engine.

Carefully looking at emails address also gives you some clues regarding phishing mail. Your inbox displays a name, like 'Bank Statement', and the subject line. When you open the email, you already know what is the message is from and jump straight into the content. When hacker create fake email addresses, then have the choice to select the display name, which doesn't have to relate to the email address at all. But hackers rarely depend on their victim's ignorance alone. The fake email addresses will use the spoofed organization's name in the local part of the address.

Suppose you receive email from any xyz bank or financial organization and the sender address is 'paymoney@notice-access-123.com'.

A Genuine email from bank would have the organization's name in the domain name, indicating that it had come from xyz bank. So that xyz bank isn't in the domain name is proof that this is a scam.

2. Misspelled domain name:

There are another clue hidden in domain names that provide a strong indication of phishing scams. The problem is that anyone can buy a domain name from registrar. And although every domain name must be unique, there are plenty of ways to create addresses that are indistinguishable from the one that's being spoofed.

Example, the hacker bought the domain 'xyzrnedia.com' (that's is r-n-m-e-d-i-a, rather than m-e-d-i-a) and this will detect by observing email domain name.

3. Poorly written email:

You can often tell if an email is scam if it contains poor spelling and grammar. Many people will tell you that such errors are part of a 'filtering system' in which cyber criminals target only the most gullible people.

The theory is that, if someone ignores clues about the way the message is written, they're less likely to pick up clues during the scammer's endgame.However, this really only applies to outlandish schemes like the oft-mocked Nigerian prince scam, which you really do have to be incredibly naive to fall victim to.That, and scams like it, are manually operated: once someone takes to the bait, the scammer has to reply. As such, it benefits the crooks to make sure the pool of respondents contains only those who might believe the rest of the con.But this doesn’t apply to phishing.

Automated attacks

With phishing, scammers don’t need to monitor inboxes and send tailored responses. They simply dump thousands of crafted messages on unsuspecting people.Remember, many of them are from non-English-speaking countries and from backgrounds where they will have limited access or opportunity to learn the language.

With this in mind, it becomes a lot easier to spot the difference between a typo made by a legitimate sender and a scam.

When crafting phishing messages, scammers will often use a spellchecker or translation machine, which will give them all the right words but not necessarily in the right context. Maximum time no individual word is spelled incorrectly, but the message is full of grammatical errors that a native speaker wouldn’t make. By using above method we can detect its fake email generated from attacker.

4. It includes suspicious attachments or links:

Phishing emails come in many forms, but the one thing they all have in common is that they contain a payload. This will either be an infected attachment that you’re asked to download or a link to a bogus website that requests login and other sensitive information.

What is an infected attachment?

An infected attachment is a seemingly benign document that contains malware.It doesn’t matter whether the recipient expects to receive an invoice from this person or not, because in most cases they won’t be sure what the message pertains to until they open the attachment.When they open the attachment, they’ll see that the invoice isn’t intended for them, but it will be too late. The document unleashes malware on the victim’s computer, which could perform any number of nefarious activities.

We advise that you never open an attachment unless you are fully confident that the message is from a legitimate party. Even then, you should look out for anything suspicious in the attachment.

For example, if you receive a pop-up warning about the file’s legitimacy or the application asks you to adjust your settings, then don’t proceed.

Contact the sender through an alternative means of communication and ask them to verify that it’s legitimate.

Suspicious links:

You can spot a suspicious link if the destination address doesn’t match the context of the rest of the email.

For example, if you receive an email from Netflix, you would expect the link to direct you towards an address that begins ‘netflix.com’.

Unfortunately, many legitimate and scam emails hide the destination address in a button, so it’s not immediately obvious where the link goes to.Unfortunately, the rest of the message is pretty convincing, and you might click the link without giving it a second thought.To ensure you don’t fall for schemes like this, you must train yourself to check where links go before opening them.Thankfully, this is straightforward: on a computer, hover your mouse over the link and the destination address appears in a small bar along the bottom of the browser.On a mobile device, hold down on the link and a pop-up will appear containing the link.

5. The message creates a sense of urgency:

Scammers know that most of us procrastinate. We receive an email giving us important news, and we decide we’ll deal with it later.But the longer you think about something, the more likely you are to notice things that don’t seem right.Maybe you realize that the organization doesn’t contact you by that email address, or you speak to a colleague and learn that they didn’t send you a document.

Even if you don’t get that ‘a-ha’ moment, coming back to the message with a fresh set of eyes might help reveal its true nature.That’s why so many scams request that you act now or else it will be too late. This has been evident in every example we’ve used so far.

VI. CONCUSION

Phishing email attacks are an ongoing threat to society and are becoming increasingly sophisticated.

Successful Phishing attacks can cause financial loss for victims and put their personal information at risk. In this way this paper explains how important it is for individuals to recognize signs of phishing.Spam filters will never be fully effective, so it’s up to each of us to read the context of messages and look for anything suspicious.It is therefore crucial that you educate people to understand and analyze the way phishing works and what to do if they receive a malicious email.

REFERENCES

[1] Sunil Kumar, Dilip Agarwal, "Hacking Attacks, Methods, Techniques And Their Protection Measures", in International Journal for Science and Advance Research in Technology , vol. 4, no. 4, pp. 2253- 2257, April 2018.

[2] ShivamKharje, RupalSonawane, "ANDROID BACKDOORS", in International Journal of Advances in Electronics and Computer Science , vol. 4, no. 2, pp. 52-55, Feb 2017.

[3] Pawan Kesharwani1, SudhanshuShekhar Pandey, Vishal Dixit, Lokendra Kumar Tiwari, “A study on Penetration Testing Using Metasploit Framework”, International Research Journal of Engineering and Technology, vol. 5, no. 12, pp 193-200, Dec 2018.