E-mail Spoofer

Project Work
Submitted in partial fulfillment of the
Requirement for the award of degree of

Bachelor of Technology
In
Computer Science & Engineering

Submitted By
Ashwani Kumar Singh
(1613101200)

Under the supervision of
Mr. S Ponmaniraj Sir

GALGOTIAS
UNIVERSITY

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY
GREATER NOIDA - 201306

SCHOOL OF COMPUTING AND SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that this project report "Email Spoofer" is the bonafide work of "Ashwani Kumar Singh" who carried out the project work under my supervision.

SIGNATURE	SIGNATURE
Dr Munish Sabharwal	Mr. S Ponmaniraj
HEAD OF THE DEPARTMENT	SUPERVISOR
Professor & Dean	Asst. Professor
School of Computing Science & Engineering (SCSE)	

TITLE

Email - Spoofer

Email Spoofing version 1.1

(Fully Undetectable Email Spoofer)

TABLE OF CONTENT

ABSTRACT

Email spoofing is referred to as malicious activity in which the origin details have been altered so as to make it appear to originate from a different source. This mechanism is mostly being applied in the defence department of any nation's government.
SMTP server and SPF record is used to forge the real sender's email at the attacker's side to make the mail look more real and authentic. Email spoofing has become an integral part of any investigation agency and intelligence as this is the most widely used tool to capture or to trap the suspects by doing social engineering through this tool.

INTRODUCTION

1. Overall description

Email spoofing is referred to as malicious activity in which the origin details have been altered so as to make it appear to originate from a different source. Sending fake emails is usually used to convince the receiver so that he stays unaware of the real sender. Email spoofing may be effectively used to launch phishing attacks on the receivers. The attacker may also use the attack with some amplification and in addition use mass mailer to spam mail users. Infections may be propagated by the means of spoofed emails to attack victims. There are a variety of attackers who do email spoofing. The list starts from people trying to just have fun by sending spoofed messages to users. Other serious attacks are done by wrongdoers to make damages to the systems.

Causes of email spoofing include compromised account information from where emails are sent. Sometimes user browsers are infected so as to use them to send spoofed emails. Email service providers' versatility may be attacked by misusing the SMTP protocol.

Implementation of security relies on usage of physical medium like smart cards. The end users may also implement verification for the originators of email to prevent them from falling into the attacks of spoofed emails. Digital signatures and certificates are also recommended to ensure that the emails are genuine.

Email spoofing attacks may be launched by some mischievous users just to do poking into other user accounts to simply have fun. For the sake of mischief usually friends send spoofed emails to their friends to make fun. This category is though not considered to be criminal, but the attacker should avoid doing such activities because faking identity is in itself a wrongdoing which should not be done. Such practices are not widely discouraged. However, spoofing anyone other than yourself is illegal in some jurisdictions [2]. Email spoofing attacks may be launched with simply having an email account and any email client like Outlook. The technique to spoof the identity of the sender is to change the display name for the sender and send emails from the client. Such attacks are launched within an organization to surprise the receivers. Both the above stated categories are treated as innocent since they are not intended to cause damage to the victim. More kinds of severe

attacks are possible when the attackers have much more malicious intent. In such cases the attackers may cause some serious damages to the victim.

The most famous and frequently used attack that is done by the means of email spoofing is phishing attack. The attackers in this case are usually interested in the information regarding the particular user.

An example of a phishing email, disguised as an official email from a (fictional) bank. The sender is attempting to trick the recipient into revealing confidential information by "confirming" it at the phisher's website. Note the misspelling of the words received and discrepancy. Such mistakes are common in most phishing emails. Also note that although the URL of the bank's webpage appears to be legitimate, it actually links to the phisher's webpage

The users of email accounts are also susceptible to being misused by attackers. If an attacker gets to somehow obtain the credentials of a user of email, then he may use it to propagate mass emails to produce spam attacks on other users. The email user may not even make out that his account is compromised and being used for bad purposes. Hackers may also infect browsers with malware to compromise their security and misuse them to send spoofed emails. It is easy to spoof because the protocol that is used called SMTP lacks authentication. If the site server is configured to allow SMTP connections then the attackers may exploit this and issue commands to send some emails that may appear to originate from choice of the attacker. This email address may be either of two – a correct email address or any address that is of the choice of the attacker that is correctly formatted. There are email service providers that may be vulnerable to attacks of forged or spoofed emails. If in case there are a lot of bounced emails , one should be alert and analyse the logs to make proper remedial measures. However, if your email address is being spoofed, you may experience large numbers of messages appearing in your inbox that have bounced back because the original spam message was undeliverable to the intended recipients. These messages are referred to as "backscatter."

The motivation of making this project is from a research paper : “Email Spoofing” by Kunal Pandove. The motive is to develop a fully undetectable email spoofing tool which will help intelligence and investigation agencies in capturing suspects.

2. Purpose

Email spoofing is a popular tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate or familiar source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation
The main purpose is to spoof email tools to facilitate an offensive service for getting the suspects into trap by sending spoofed emails from their incharge or head's email address.

3. Motivation & Scope

Intelligence industries like NIA, IB, etc want a wide variety of tools and services which can be used by them to track their suspects and get their information for the security of the Nation. Indian defence knows how to get their enemies down physically but this time it is a war which is bloodless and by using computers and devices so there should be that type of weapons too at indian defence side. So, they are developing it on their own as well as asking for help from commercial people too. In this scenario, Our tool fits into it and can be deployed in indian defence as well as the intelligence department.

This methodology can be explored more in future and applied to other areas in the IT industries and other nation's security teams like the CIA, etc.

Proposed System

While doing requirement analysis, we found the following listed requirements:

- A domain with SPF capability
- Another domain to host website
- Google Cloud Server
- VM Instance
- SMTP server

This model of our tool which has been developed using php version 5 which also includes CSS and html. In the model, it is inclusive of Google cloud server's machine_of_configuration: Debian9, Apache server & database of Mysql with SMTP server installed on it and also there is a domain with SPF record and DNS records.

An SMTP server which is used as a private server which is mostly being used by industries to send emails in bulk is being used by our tool for sending the mails. On our domain's dns record, added a new record which is of that private SMTP server which allows that SMTP server to send mails on behalf of our domain and that SMTP is matched with google vm machine to send mails.

Implementation

Email spoofing is referred to as malicious activity in which the origin details have been altered so as to make it appear to originate from a different source. Sending fake emails is usually used to convince the receiver so that he stays unaware of the real sender. Email spoofing may be effectively used to launch phishing attacks on the receivers. The attacker may also use the attack with some amplification and in addition use mass mailer to spam mail users. Infections may be propagated by the means of spoofed emails to attack victims. There are a variety of attackers who do email spoofing. The list starts from people trying to just have fun by sending spoofed messages to users. Other serious attacks are done by wrongdoers to make damages to the systems.

Causes of email spoofing include compromised account information from where emails are sent. Sometimes user browsers are infected so as to use them to send spoofed emails. Email service providers' versatility may be attacked by misusing the SMTP protocol.

Implementation of security relies on usage of physical medium like smart cards. The end users may also implement verification for the originators of email to prevent them from falling into the attacks of spoofed emails. Digital signatures and certificates are also recommended to ensure that the emails are genuine.

Email spoofing attacks may be launched by some mischievous users just to do poking into other user accounts to simply have fun. Out of sake of mischief usually friends send spoofed emails to their friends to make fun. This category is though not considered to be criminal, but the attacker should avoid doing such activities because faking identity is in itself a wrongdoing which should not be done. Such practices are not widely discouraged. However, spoofing anyone other than yourself is illegal in some jurisdictions [2]. Email spoofing attacks may be launched with simply having an email account and any email client like Outlook. The technique to spoof the identity of the sender is to change the display name for the sender

and send emails from the client. Such attacks are launched within an organization to surprise the receivers. Both the above stated categories are treated as innocent since they are not intended to cause damage to the victim. More kinds of severe attacks are possible when the attackers have much more malicious intent. In such cases the attackers may cause some serious damages to the victim.

The most famous and frequently used attack that is done by the means of email spoofing is phishing attack. The attackers in this case are usually interested in the information regarding the particular user.

An example of a phishing email, disguised as an official email from a (fictional) bank. The sender is attempting to trick the recipient into revealing confidential information by "confirming" it at the phisher's website. Note the misspelling of the words received and discrepancy. Such mistakes are common in most phishing emails. Also note that although the URL of the bank's webpage appears to be legitimate, it actually links to the phisher's webpage

The users of email accounts are also susceptible to being misused by attackers. If an attacker gets to somehow obtain the credentials of a user of email, then he may use it to propagate mass emails to produce spam attacks on other users. The email user may not even make out that his account is compromised and being used for bad purposes. Hackers may also infect browsers with malware to compromise their security and misuse them to send spoofed emails. It is easy to spoof because the protocol that is used called SMTP lacks authentication. If the site server is configured to allow SMTP connections then the attackers may exploit this and issue commands to send some emails that may appear to originate from choice of the attacker. This email address may be either of two – a correct email address or any address that is of the choice of the attacker that is correctly formatted. There are email service providers that may be vulnerable to attacks of forged or spoofed emails. If there are a lot of bounced emails , one should be alert and analyse the logs to make proper remedial measures. However, if your email address is being spoofed, you may experience large numbers of messages appearing in your inbox that have bounced back because the original spam message was undeliverable to the intended recipients. These messages are referred to as "backscatter."

The motivation of making this project is from a research paper : “Email Spoofing” by Kunal Pandove. The motive is to develop a fully undetectable email spoofing tool which will help intelligence and investigation agencies in capturing suspects.

Methodology/Approach Adopted

The methodology adapted by us is offensive in terms of working of our prepared tool.
The pattern followed to develop this tool is taken from a research paper named as “Email Spoofing”, author “Kunal Pandove”.
The technologies used to develop this project are mentioned below in detail :

- SMTP Server
- Web Server : Apache2
- Cloud Machine : GCP (Google Cloud Platform) VM Instance

SMTP Server

An SMTP (Simple Mail Transfer Protocol) server is an application that’s primary purpose is to send, receive, and/or relay outgoing mail between email senders and receivers.

An SMTP server will have an address (or addresses) that can be set by the mail client or application that you are using, and is generally formatted as smtp.serveraddress.com. (For example, Gmail’s SMTP server address is smtp.gmail.com, and Twilio SendGrid’s is smtp.sendgrid.com. You can generally find your SMTP server address in the account or settings section of your mail client.)

When you send an email, the SMTP server processes your email, decides which server to send the message to, and relays the message to that server. The recipient’s inbox service provider, such as Gmail or AOL then downloads the message and places it in the recipient’s inbox.

Web Server

Web server is a program that uses HTTP to serve files that create web pages to users in response to their requests, which is sent by their computer's HTTP connection.

Any server that delivers an XML document to another device can be a web server. A better definition might be that a web server is an Internet server that responds to HTTP requests to deliver content and services.

In the open market there are different types of web servers available. Let's discuss the most popular web servers. Apache, IIS, Nginx and LiteSpeed are few of them.

Apache Server

One of the most popular web servers in the world developed by the Apache Software Foundation. Apache is an open source software which supports almost all operating systems including Linux, Unix, Windows, FreeBSD, Mac OS X and more. About 60% of machines run on Apache Web Server.

Customization of apache web server is easy as it contains a modular structure. It is also open source which means that you can add your own modules to the server when required and make modifications that suit your requirements.

It is more stable than any other web servers and is easier to solve administrative issues. It can be installed on multiple platforms successfully.

Cloud Machine

A machine type is a set of virtualized hardware resources available to a virtual machine (VM) instance, including the system memory size, virtual CPU (vCPU) count, and persistent disk limits. In Compute Engine, machine types are grouped and curated for different workloads. You can choose from general-purpose machine types, memory-optimized machine types, and compute-optimized machine types.

Google Cloud Platform

Google Cloud Platform (GCP), offered by Google, is a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search and YouTube. Alongside a set of management tools, it provides a series of modular cloud services including computing, data storage, data analytics and machine learning. Registration requires a credit card or bank account details,

Google Cloud Platform provides infrastructure as a service, platform as a service, and serverless computing environments.

In April 2008, Google announced App Engine, a platform for developing and hosting web applications in Google-managed data centers, which was the first cloud computing service from the company. The service became generally available in November 2011. Since the announcement of App Engine, Google added multiple cloud services to the platform.

Google Cloud Platform is a part of Google Cloud, which includes the Google Cloud Platform public cloud infrastructure, as well as G Suite, enterprise versions of Android and Chrome OS, and application programming interfaces (APIs) for machine learning and enterprise mapping services.

Note : We have adapted the web application framework to develop this tool whereas this can also be developed as a desktop application using the most popular language Python.

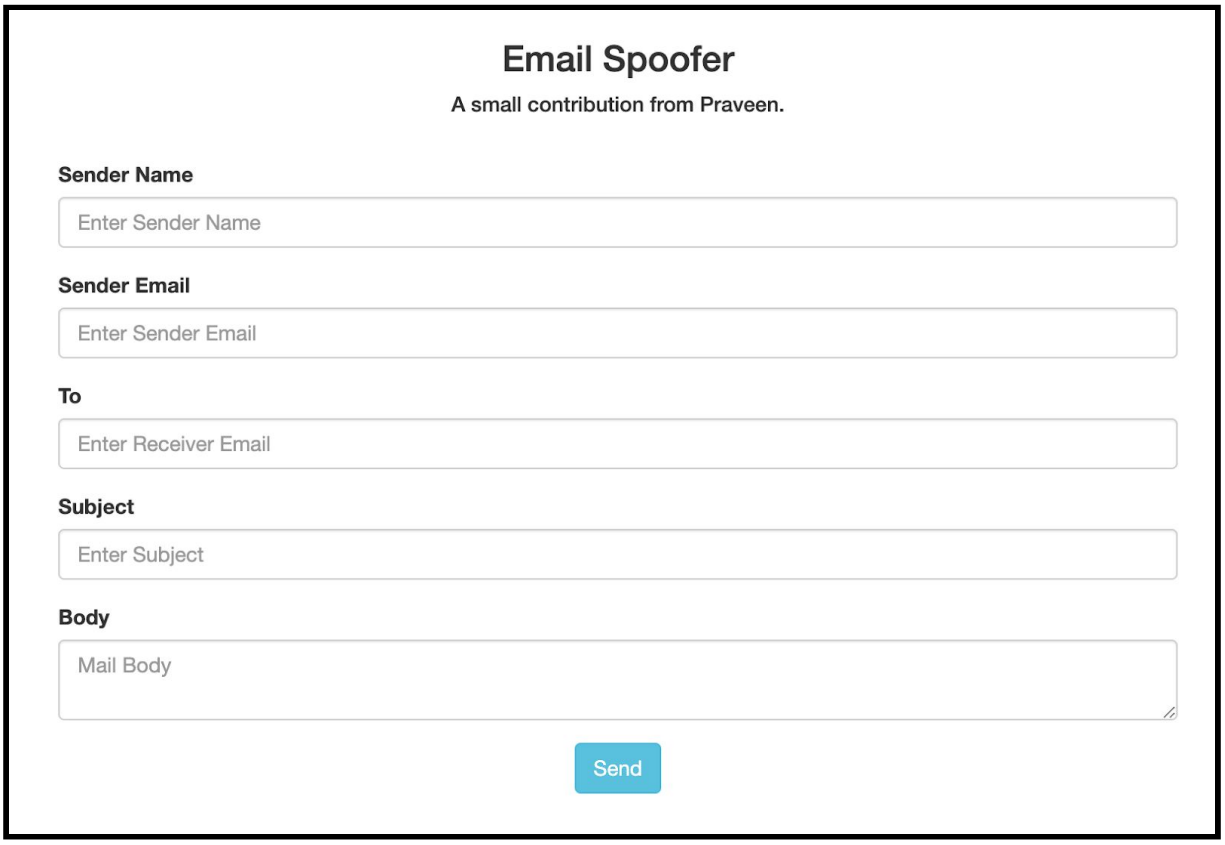
The most challenging situation in this project or tool is to stop emails to move into spam when reaching the recipient's mailbox. We have taken many test cases where we tested the number of emails being sent from our tool to the victim's mailbox.
The setup for the whole working is :

- An SMTP server which is activated based upon a working domain's SPF record.
- The Web Server which is used to host the mail spoofer web pages.
- PHP mail function (phpmailer())

The only step which was disturbing a lot was the SMTP server part, It often stops working as per expectation. So, at every stage of development we needed to perform testing so that we must get the information about errors.
The testing performed by us in the development of this project involves sending a number of emails to an email using an authentic and existing user's email id with his full consent.

Results and Discussions

The result which is produced after completion of this project is a running web application with a page having form which includes the sender's address, receivers address, subject, body text boxes and a send button . On successful filling this form and clicking on submit button, the mail will be sent to the receiver.
The intelligence agencies can use this tool to impersonate anyone’s email address and can send it to anyone.
This tool can be used by organisations who are doing their great work in Cyber Threat Intelligence and running Phishing Campaigns.



Conclusion and Future Enhancement

We conclude that this tool which is web based is for official purpose and can be used by intelligence industries and departments of any Nations with due permissions.
This application can be used as a service and embedded into any other websites too as an iframe.

There will be a requirement of sending fully formatted mails having images and graphics. This new feature can be added to the tool further for making the mails look more original, this capability will be implemented by using html.

References

1. http://en.wikipedia.org/wiki/E-mail_spoofing
2. http://en.wikipedia.org/wiki/Phishing
3. http://www.cert.org/tech_tips/email_spoofing.html
4. “Email Spoofing” by Kunal Pandove