Launching Email Spoofing Attacks

Kunal Pandove
Project Assistant
CSRC, PEC,
Sector 12, Chandigarh.

Amandeep Jindal
Project Assistant
CSRC, PEC,
Sector 12, Chandigarh.

Rajinder Kumar
Research Associate
CSRC, PEC,
Sector 12, Chandigarh.

ABSTRACT

To launch a spoofing attack with emails we need to have knowledge of the techniques to launch an email spoofing attack. Spoofing has been widely discussed in documents on the Internet. Email spoofing is termed as an attack on email users who are sent emails from email addresses that are fake or altered. An attacker may pose as other legitimate user to fool or cheat an user.

Keywords

Email spoofing, SMTP, PHP

1. INTRODUCTION

This is an effort towards postulating way to launch a email spoofing attack. Spoofing emails is thought of as in innocent activity just fool friends but it may take heinous forms when it is applied to terrorism related activities. Many other crimes like extortion, and threats may be committed by email spoofing. A saying goes that all crimes are traceable and shall be traced. It is therefore advised that the techniques advised in this article not be used for criminal purposes, and be limited to educational purposes only.

Email spoofing was started in by programmers for tricking their friends or playing pranks on them. As time progressed the postulated efforts were stared to be used by mischivious elements to do crimes also.

Type of attack	Purpose of Attack
Programming by pal	Pranks
Phishing	Fianancial
Warning	Threats
Extortion	Fear and Fianance
Terrorism	Extortion and heinous activity

Fig 1. Severity of attacks

Security mechanisms have been devised to detect spoofing and trace the origins of spoofed emails. Professional hackers make use of servers located at unreachable places to avoid security personnel to track the attack back to the original attacker.

2. Methods of Email Spoofing

I wonder sometimes how the spoofing initiative has found usage so widely that loads of spam is generated which is almost untraceable. The methods that have been devised to propogate this attack have been postulated here and shall be explained in the section that follow. The thing to consider before launching the attacks is that we should implement them taking care of the language in which these are implemented. The methods of Email Spoofing are being postulated here.

First and formost email spoofing attacks are launched by using the vulnerability that is present in SMTP protocol. Here the problem is that it does not provide a strong authentication mechanism and therefore may be misused. The details of the attack shall be explained later in the doc.

Secondly we may configure accounts in a web server that has hosted PHP to send spoofed emails to users anywhere on the Internet.

Let us investigate into email model that is used for emails.

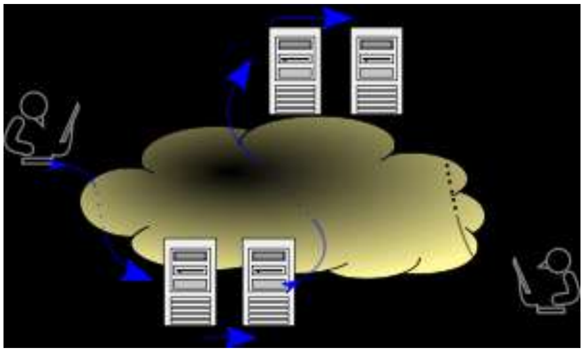

Fig2. Message Flow

3. SMTP vulnerability

There is a big flaw that is present in the SMTP protocol which allows once logged in users to send illegitimate emails. The connection to a SMTP server is established using the telnet command.

```
telnet smtp.exampe.com 25
```

This command opens a connection to the server providing email server at port number 25.

Usually the response is of the form: 220 smtpmailserver.ontheinternet.com Microsoft ESMTP MAIL Service, Version: 5.0.2195.6713 ready at Mon, 11 Apr 2005 11:15:50 -0400

This means you are successfully connected to the Server!

Next we issue a command to say hello to the gateway .

"helo"

Response: "250 smtpmailserver.ontheinternet.com [10.1.1.x]"

This means that the gateway greets you!

Then the rcpt to command is issued to specify the Recipient.

"rcpt to: person@targetdomain.com": Who are we sending the e-mail to?

Response: "250 2.1.5 person@targetdomain.com"
This means that we are close to sending our spoofed e-mail message!!!

Action: "data (then hit enter)": Tell the smtp server we are writing our message next!
Response: "354 Start mail input; end with <CRLF>.<CRLF>": The mail server is telling us to write our message then type "enter" a period ".", then "enter" again
Result: You type your message
Action: "(Hit enter) type "." (Hit enter)": Tell the smtp server we are finished writing our message!
Response: "250 2.6.0 <smtpmailserver WQm21OesnsI0000148e@smtpmailserver.ontheinternet.com> Queued mail for delivery"
Result: The SMTP mail server has just accepted your e-mail for delivery and has queued it for sending!

It is evident from the above example that the mail server does not authenticate the sender email ID and it may be duplicated. Sending fake emails from SMTP server is therefore a common practice.

4. Sending spoofed email from PHP

A webserver that allows hosting of PHP scripts may be used to send spoofed emails to any email user. This type of attack uses the mail method provided in PHP to launch spoofing attack. A html page is used as index to fetch the details of fake email to be used. The data is pushed onto the php script which executes the sending of the fake email.
The scripts to launch this attack is as follows:

```
<?php
$toemail = $_POST['toemail'];
$fromname = $_POST['fromname'];
$fromid = $_POST['fromid'];
$subject = $_POST['subject'];
$message = $_POST['message'];
$headers = "From: $fromname <$fromid>";
mail($toemail,$subject,$message,$headers);
echo "Mail Sent!";
exit();
?>
```

Fig3. Script for email spoofing

A webserver that allows hosting PHP may be used for uploading this script. When the parameters are passed, the mail method of php sends email to any email address and posing from any email address.

5. CONCLUSION

We have discussed techniques to launch email spoofing attack. These may be used by users to send fake emails to users across the Internet. Firstly proper mechanism of logging may act as a deterrent to user to not send spoofed emails from servers. Intrusion detection systems may allow issuing warnings at appropriate time and to appropriate people regarding any malicious activity. The servers should be checked for any malicious scripts that may be uploaded for execution by the users. This allows application of good security policy. Hereby we have concluded that prevention mechanisms may be employed to prevent against these attacks.

6. REFERENCES

[1] www.cert.org/tech_tips/home_networks.html

[2] http://en.wikipedia.org/wiki/Spoofing_attack

[3]http://searchsecurity.techtarget.com/.../0,,sid14_gci840262,00. html

[4] www.wisegeek.com/what-is-spoofing.htm

[5] www.ethicalhackers.in/tag/email-spoofing-attack

[6] http://www.consumerfraudreporting.org/spoofing.php