IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 4)

Available online at: www.ijariit.com

SMTP attacks and detection using data mining (Information gathering)

S. Ranjitha
ranjithas14mss040@skasc.ac.in
Sri Krishna College of Arts and Science, Coimbatore, Tamil Nadu

A. Venugopal
venugopala@skasc.ac.in
Sri Krishna College of Arts and Science, Coimbatore, Tamil Nadu

M. Rajini Sri
rajinisrim14mss038@skasc.ac.in
Sri Krishna College of Arts and Science, Coimbatore, Tamil Nadu

A. Shobika
shobikaa14mss049@skasc.ac.in
Sri Krishna College of Arts and Science, Coimbatore, Tamil Nadu

ABSTRACT

The SMTP protocol is used to send and receive of e-mail messages and control headers the whole body of messages that are opposed to other protocols after the message is delivered a detailed record of the e-mail transactions in the receiver mailbox. SMTP headers can be used to map the networks and the information on the messaging software gateways.

Keywords— *Information gathering, Attack, SMTP security*

1. SMTP INFORMATION GATHERING

1.1 Introduction

SMTP takes information from the sender and the path a message from the network this information is used in the communication when problems arise and are superfluous and leaking very valuable secret information of the sender and the communication having to debug the information built into the protocol.

1.2 Control information

SMTP messages are very interesting for getting information which controls information as a part of the communication each message includes the content and the control information needed to get from the sender to the destination of the network. Controlling information is a vital part of the communication and the sender and recipient information the subject and the date of the message was sent all stored as a message header.

SMTP messages are fully available to the receiver to analyze the communications. An attacker needs access to the recipient storage.SMTP messages and control information which tell a tale of every sender. Mailing lists would keep an archive in **mailbox** format.

2. ATTACKS

(a) Bug- This happens because of the malicious tracking inside in the email links.

(b) Active Content attacks- using active HTML and scripting

(c) Buffer Overflow attacks: In this too large file are sent in emails so that it doesn't fit in the memory buffer of the email client.

(d) Trojan horse attacks- these come as an attachment in the email with file extension like an image, doc, spreadsheet etc.

2.1 Account enumeration

Good way attacker can get the information from the e-mail accounts to existing on. The VRFY command makes the server check a specific user ID exists or not. Spammers can automate this method to perform quick directory pirate attack which is a way of gleaning e-mail addresses from the server.

2.2 Attacks using account enumeration

SMTP command EXPN will allow the attackers to get information about what mailing lists exist from the server. We can simply telnet to the e-mail server on port 25 and implement EXPN on the system. Another method to automate the process is using the Email Verify program in TamiSoft’s Essential Net Tools. To get the valid e-mail addresses to use the Harvester to glean addresses via Google and other search engines.

2.3 Countermeasures against account enumeration

If we are running Exchange account census company e-mail addresses are not to be posted.

2.4 Relay

SMTP relay allows users to send e-mails from external servers. Open e-mail relays are not the problem they but we still need to check for them. Hackers can use an e-mail server to send malware through e-mail from the guise of the open-relay-owner.

3. AUTOMATIC TESTING

Here are few ways to test your server for SMTP relay. In Net ScanTools Pro, we simply enter values for the SMTP mail server name, Sending Domain Name. Message Settings; enter the Recipient Email Address and Sender's Email Address. When the test is complete click View Relay Test-Results.

4. MANUAL TESTING

We can manually test your server for SMTP relay by telling netting to the e-mail server on port 25. Follow these steps:

Step 1: Enter the following command at a Windows or UNIX command prompt: telnet mail server address 25.
Step 2: Give the command to the server Hi I'm connecting from this domain.
Step 3: Enter the command to the server your e-mail address.
Step 4: Enter the command to the server who to send the email -id to.
Step 5: Enter the command to the server that the message body is to follow.
Step 6: Enter the text as the body of the message.
Step 7: End the command with a period by itself.
Step 8: Check for relaying on your server: Look for a message to relay from the server.

5. COUNTERMEASURES AGAINST SMTP RELAY ATTACKS

We can tackle SMTP attack on the e-mail server to disable SMTP relaying Disable SMTP relay on your e-mail server. We can enable SMTP relay for particular hosts on the server. Enforce authentication if the e-mail server allows it. It must require password authentication on an e-mail address that matches the e-mail server's domain.

5.1 E-mail header disclosures

If the e-mail server is configured with defaults a hacker could find the precious information: Internal IP address of the e-mail server Software versions of the server.

5.2 Countermeasures against header explosions

The best measures to protect information exposures in the e-mail headers is to configure the e-mail server by changing the information shown. Check the e-mail server to see this option.

5.3 Malware

E-mail servers are regularly attacked by the malware. EICAR offers a safe option for analyzing antivirus software. The EICAR test string that transmits in the body of an e-mail so that we can see how the server responds

6. SMTP INTRUSION DETECTION

Companies that are offering email services to their employees and customers to facilitate service each other across the Internet. Every company that has a public domain allows SMTP traffic from their firewall to accept their email messages from other users on the Internet. We need to make sure that the email server is well protected from outside hackers and eliminate any harmful attacks.

6.1 SMTP Protocol - from a security perspective

Companies spend a huge amount of time making for their network to secure. And no outsiders with malicious can harm their system. SMTP is created to send and receive emails from other SMTP servers. When a user within you're an organization tries to send an email on the Internet the email client will forward the message to the SMTP server, which in turn will then forward it to the receiver.

7. HOW TO IDENTIFY A MALICIOUS USER

Companies find out disturbances after the system has been infected. The Hackers will find weaknesses by sending unexpected messages the data returned by the server. It is very difficult to find out such activity is taking place inside the server.

8. CONCLUSION

This paper explores how the SMTP Injection attack through a crafted recipient email address works and showed the examples of vulnerable SMTP clients and the possible further attacksStrip unneeded information whenever possible.

9. REFERENCES

[1] http://www.xeams.com/intrusiondetection.htm
[2] https://www.quora.com/What-are-the-common-attacks-on-SMTP-Server
[3] https://www.mbsd.jp/Whitepaper/smtpi.pdf
[4] https://www.blackhat.com/presentations/bh-europe-07/Mora/Whitepaper/bh-eu-07-mora-WP.pdf