Ethical Hacking: Phising Report

Jordi Nadeu Ferran

Abstract

In this lab, we performed email spoofing to end up simulating a phishing attack. The objective is to understand how the Simple Mail Transfer Protocol (SMTP) can be exploited to send spoofed emails. And also how to use the king phiser tool to make this type of attacks scalable.

1 Introduction

First of all, we will simulate an ethical hacking environment as in the previous labs using a Metasploitable machine (vulnerable SMTP server) and a Kali machine (attacker).

To introduce some context, let's look at the definitions of the important concepts related to this practice.

- **Phishing** is a type of cyberattack where attackers deceive victims by pretending to be a trusted entity, often to steal sensitive information.
- **Email spoofing**, a technique often used in phishing, involves falsifying the sender's identity.
- **SMTP**, the protocol responsible for sending emails, don't inherently verify the authenticity of the sender's address, making it susceptible to spoofing attacks.
- **King Phisher** is a popular phishing toolkit to automate phishing attacks and manage them at scale.

An SMTP server facilitates the sending of emails between users, but attackers can exploit this by connecting directly to the server and impersonating a legitimate sender. SMTP uses commands like HELO, MAIL FROM, RCPT TO and DATA which allows basic communication between the client (email sender) and the server. In this lab, we explored how these vulnerabilities can be exploited, first manually, then programmatically using Python.

2 Procedure

First of all we used the *dig mx gmail.com* command to retrieve Gmail's mail server information. This revealed the mail exchange (MX) records, which are responsible for handling emails for the domain. This is important to know how DNS is managed at the mail server level.

Figure 1: Output of command dig mx gmail.com

To simulate a phishing attack manually, we connect from the Kali machine to the SMTP server (Metasploitable) and start sending the commands to simulate an email. The following figures shows both what the attacker (Kali machine) sends and what the SMTP server (Metasploitable machine) receives.

Figure 2: Communication with the server using SMTP commands

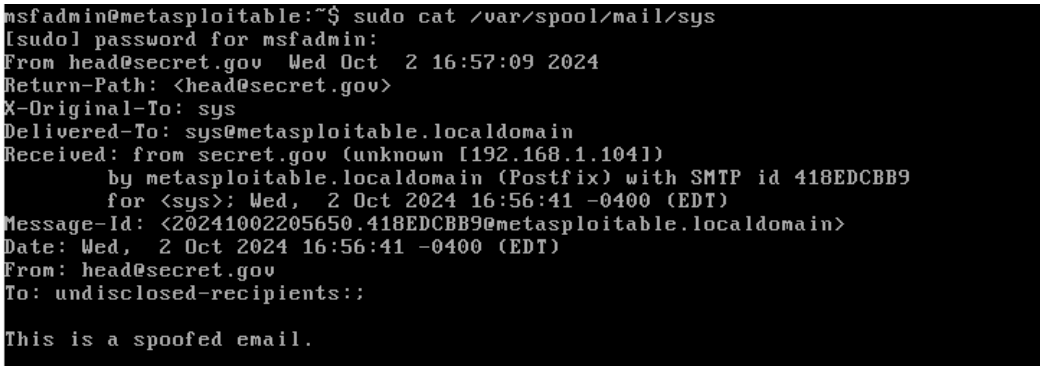

Figure 3: Messages received on the SMTP server

Then we tried a Python script to automate all the process explained above. The script opened a socket, connected to the SMTP server, and sequentially sent the necessary SMTP commands. We also tried another python script that does the same but adds an html template as the message body. This script use the Python smtplib library and OpenSSL to connect securely to Gmail's SMTP server using SMTPS. This method initiates a TLS (Transport Layer Security) session before sending the spoofed email, it how emails are sent in real life.

Then we have to train a deepfake model together with a voice to obtain a realistic video of a famous person and add this video to the email template to create a new bait to make phishing more probable to succeed. At this point I couldn't get the training done, after several hours trying to prepare all the environment, dependencies and other files needed for the training I couldn't finish. It seems that something is wrong with the cython package and other dependencies, I will keep looking to solve this. In the meantime I have used an external youtube video as an example.

I have added some social engineering techniques, such as urgency and call to action, to increase the chance of engagement. I have also added a bit of styling to the email to make it more attractive to click on the link, for example by making the link button colourful and highlighted. Below is the html code of the email to make the bait.

phisingEmail.html

```
<html>
<head>
    <style>
        .container {
```

```
            background-color: #FFFFFF;
            padding: 20px;
            border-radius: 10px;
            box-shadow: 0 4px 8px rgba(0, 0, 0, 0.1);
            max-width: 600px;
            margin: 0 auto;
        }
        h1 {
            color: #D9534F;
            font-size: 24px;
        }
        h3 {
            color: #5A5A5A;
            font-size: 18px;
        }
        a {
            display: inline-block;
            background-color: #D9534F;
            color: #FFFFFF;
            padding: 10px 20px;
            text-decoration: none;
            border-radius: 5px;
            font-weight: bold;
        }
    </style>
</head>
<body>
    <div class="container">
        <h1>Watch the video of Elon Musk doing the unthinkable!</h1>
        <h3>This video is going viral but will be removed soon!</h3>
        <p>Dear Georgios,</p>
        <p>A video of <strong>Elon Musk</strong> has been uploaded to Youtube
        and is quickly going viral. In the video, Elon Musk is seen in a highly
        controversial situation that has already sparked debates across social
        media and major news outlets.</p>
        <p>The video has gained <strong>over 1 million views</strong>
        in less than24 hours, and its impact is spreading rapidly.
        Georgios, you have to see the video now before they take it down
        and delete it permanently.</p>
        <p>To watch the video, click on the link below:</p>
        <a href="youtu.be/XuKUkyPegBE" target="_blank">Watch the Video</a>
```

```
        <p>Please note that due to the sensitive nature of the content, it may
        not be available for long. Don't miss your chance to see it!</p>
        <p>If you believe this message was sent in error,
        please contact us immediately.</p>
        <hr>
        <p>Best regards,</p>
        <p><strong>Viral Videos Team</strong></p>
    </div>
</body>
</html>
```

Finally, we use the king phiser tool, which by the way is not included in Kali, to escalate the attack and allow us to automatically send this email in massive amounts, thus further increasing the chances of a successful phishing attack.

To do the installation we have cloned the repository https://github.com/rsmusllp/king-phisher, and then we have executed the following command:

```
wget -q https://github.com/securestate/king-phisher/raw/master/tools/install.sh
sudo bash ./install.sh
```

we had a lot of problems to install the tool as the installation script uses pip without a virtual environment (as in 2019 it still worked correctly) but currently python does not allow to install in a simple way through pip and recommends to use the package manager of the OS itself, in the case of Kali using apt. More info at PEP 668.

I have tried to perform the manual installation following the steps of the installation script in the repository, but I have not had time to fix all the errors with the dependency package versions and use the python virtual environment. Here is the code of the installation script. I have watched videos on how to use this tool. Another option would have been to find an old Kali image and use it only to run this tool. I'm add a screenshot from repository to give an idea of how to set up a phishing campaign.

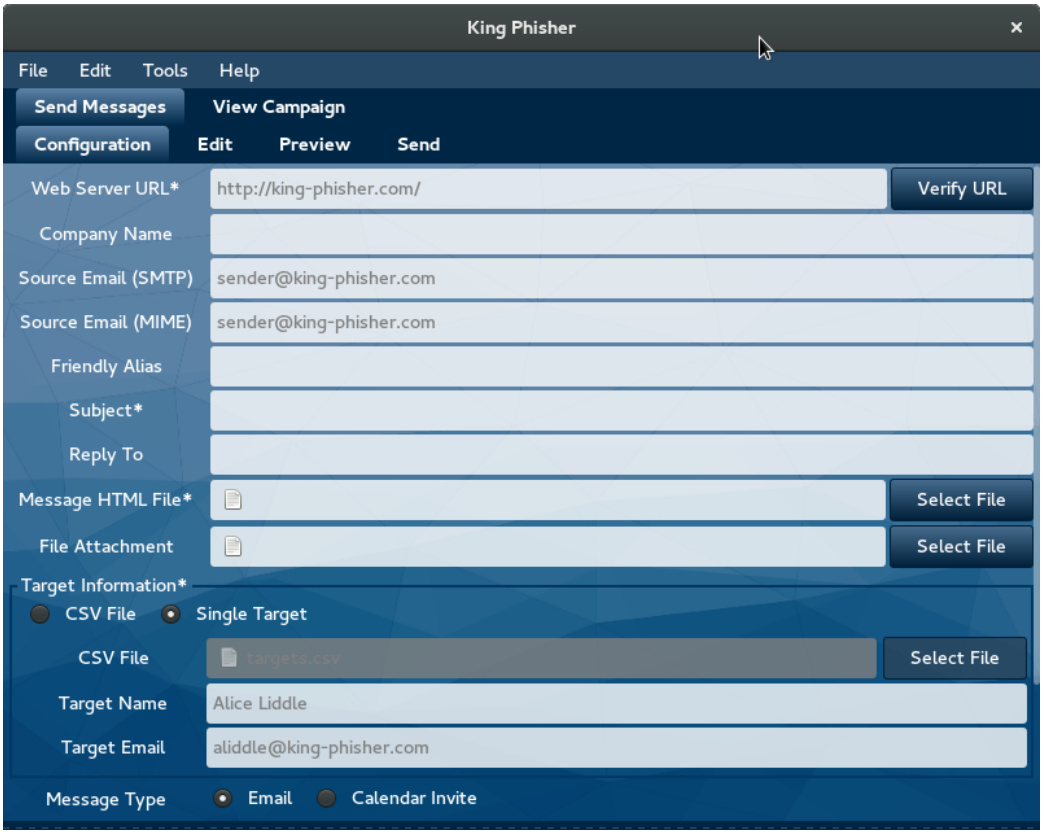

Figure 4: Screenshot of King phiser tool. Source

3 Conclusions

The lab demonstrated the vulnerabilities inherent in the SMTP protocol, how easily attackers can spoof emails without robust security mechanisms. The secure method using SMTPS illustrated the importance of encryption and verification in modern email systems. This experiment reinforces the need for organizations to implement email authentication protocols like SPF, DKIM, and DMARC to prevent email spoofing.

Regarding the deepfake part, I have found the whole process of getting an environment ready for AI training to be quite complicated. I guess once you have the set up ready, deepfake is a matter of having datasets.

It is very interesting the tools (like king phiser) that are available today to perform attacks in a scalable way and above all the simplicity of using them. However, this tool has been abandoned for 2 years now and is no longer maintained.