Netzwerksicherheit

Phshing, Spam und Homebanking

vorgelegt von

Tommy Bui (Matrikelnummer: 84366)

Studiengang IT-Sicherheit
Semester WS23/24

Hochschule Aalen

Hochschule für Technik und Wirtschaft

Betreut durch Prof. Roland Hellmann

12.02.24

Für die Bearbeitung der Übungsaufgaben benötigen Sie eine Linux VM(am besten die bekannte Kali Linux VM) mit folgender Software:

- Docker, falls man mit Container arbeiten möchte
- GoPhish ggf. als Docker Container
- MailHog oder einen anderen Mailserver ggf. als Docker Container

1 Installation

1.1 Docker

Docker sollte bereits auf der Kali VM installiert sein. Sollte Ihre VM kein Docker installiert haben, können Sie Docker über die offizielle Dokumentation installieren. https://docs.docker.com/engine/install/debian/
Allgemeiner Hinweis: Um Docker ohne Root Rechte zu verwenden, muss der Benutzer der Gruppe docker hinzugefügt werden.
Dazu führen Sie folgende Befehle aus:

```
1  sudo usermod –aG docker $USER
2  newgrp docker
```

1.2 MailHog

Richten Sie sich an die offizielle Dokumentation von MailHog https://github.com/mailhog/MailHog oder richten einen Docker Container ein.

1.3 GoPhish

Richten Sie sich an die offizielle Dokumentation von GoPhish https://docs.getgophish.com/user-guide/installation oder richten einen Docker Container ein.

2 Phishing Kampagne starten

Bevor man GoPhish und MailHog startet, sollte man in Docker ein Netzwerk erstellen:

```
1        docker network create phishingNet
```

Dieses Netzwerk wird später benötigt, damit die Container miteinander kommunizieren können.

2.1 MailHog

MailHog bietet eine einfache Möglichkeit einen Mailserver für Testzwecke zu starten und kann mit Docker einfach aufgesetzt werden.
Laden Sie das Docker Image mit folgendem Befehl herunter:

```
1            docker pull mailhog/mailhog
```

Anschließend starten Sie den Docker Container mit folgendem Befehl:

```
1            docker run --network pishingNet -p 8025:8025 -p
                1025:1025 mailhog/mailhog
```

Damit man vom Host-System Zugriff auf die im Container laufenden Dienste hat, müssen die Ports `8025` und `1025` weitergeleitet werden. Der Port `8025` ist der Webserver Port und der Port `1025` ist der SMTP Port. Mit `--network` wird der MailHog Container dem Netzwerk zugewiesen.

2.2 Gophish

GoPhish bietet ein Docker Image an welches eine einfache Möglichkeit bietet GoPhish zu verwenden.
Laden Sie das Docker Image mit folgendem Befehl herunter:

```
1            docker pull gophish/gophish
```

Um nun GoPhish zu starten, führen Sie folgenden Befehl aus:

```
1 docker run --network pishingNet -p 3333:3333
    gophish/gophish
```

Im Terminal wird neben einen Link, der zum Webinterface führt, auch ein Passwort für den Admin **admin** angezeigt. Mit dem Link und dem Passwort können Sie sich in GoPhish einloggen.

```
1 time="2023-12-20T23:15:22Z" level=info msg="Please login with
    the username admin and the password dfe2753dcc994b76"
2 time="2023-12-20T23:15:22Z" level=info msg="Starting phishing
    server at http://0.0.0.0:80"
3 time="2023-12-20T23:15:22Z" level=info msg="Starting IMAP
    monitor manager"
4 time="2023-12-20T23:15:22Z" level=info msg="Creating new self-
    signed certificates for administration interface"
5 time="2023-12-20T23:15:22Z" level=info msg="Starting new IMAP
    monitor for user admin"
6 time="2023-12-20T23:15:22Z" level=info msg="Background Worker
    Started Successfully - Waiting for Campaigns"
7 time="2023-12-20T23:15:22Z" level=info msg="TLS Certificate
    Generation complete"
8 time="2023-12-20T23:15:22Z" level=info msg="Starting admin
    server at https://0.0.0.0:3333"
```

Klicken Sie auf den Link und geben Sie Anmeldedaten ein. Beim erstmaligen Anmelden werden Sie aufgefordert Ihr Passwort zu ändern.

Um nun zu verifizieren, dass GoPhish und MailHog miteinander kommunizieren können, erstellen Sie unter **Sending Profiles** ein neues Profil.
Die Felder sind wie folgt auszufüllen:

- Name: Name des Profils
- SMTP From: hier wird die Absenderadresse eingetragen, z.B. **phisher@web.de**
- Host: hier wird die Adresse unseres MailHog Servers eingetragen, also: **namemailhogcontainer:1025** (hier ist namemailhogcontainer der Name des MailHog Containers, welche von Docker automatisch aufgelöst wird)
- Username und Passwort: können leer gelassen werden, da dies von MailHog nicht erlangt wird
- man kann auch Custom Headers hinzufügen, dies ist aber optional

Hat man sein Sender Profil fertigestellt, kann man dieses unter **Send Test Mail** testen. Es sollte eine Bestätigung erscheinen, dass die Mail erfolgreich versendet wurde. Dies kann auch über das MailHog Webinterface unter **http://0.0.0.0:8025/** eingesehen werden. Ansonsten muss man seine Angaben überprüfen, wie z.B den Host oder die E-Mail. Sind alle Angaben richtig kann man für den Host auch **0.0.0.0:1025** oder **containerid:1025** eintragen. Ansonsten muss das Docker Netzwerk überprüft und Notfalls die Container neu gestartet werden.

3 Phishing Kampagne erstellen

Im folgenden wird der Workflow von GoPhish erklärt um eine Kampagne zu erstellen.

3.1 Sending Profiles

Zunächst erstellt man Profile von Absendern, von denen vermeintlich die E-Mails stammen. Gehen Sie wie beim testen der Verbindung vor und erstellen Sie 1-2 Sender Profile

3.2 Users and Groups

Je nach Szenario können Sie hier Benutzer und Gruppen erstellen. GoPhish bietet hier an manuell einzelne ziele einzutragen oder eine größere Gruppe durch eine CSV-Datei zu importieren. Die CSV-Datei sollte dabei folgendes Format haben:

```
1 First Name, Last Name, Position, Email
2 Willi, Wollte, Dozent, wwollte@hs-aalen.de
```

Fügen Sie eigene Personen in Ihre Gruppe ein. Sie können auch die **test_csv** Datei verwenden um mehrere Einträge zu erstellen.

3.3 E-Mail Templates

Unter **E-Mail Templates** können Sie E-Mail Vorlagen erstellen, die für die Kampagne genutzt werden. Zu den Feldern:

- Subject: Betreff der E-Mail
- Envelope Sender: Absender der E-Mail der angezeigt wird(nicht bei jedem E-Mail Client)
- HTML: HTML Code der E-Mail
- Text: Text der E-Mail

Hier kann man sich sein gewünschtes E-Mail Template erstellen. Allerdings bietet GoPhish es auch an E-Mails zu importieren (hier wird **Raw Email Source** importiert).
Verwenden Sie die E-Mail Vorlage **phishing_email.txt** um eine Phishing Mail zu erstellen.
Hinweise zum erstellen von E-Mail Vorlagen:

- GoPhish bietet die Möglichkeit Variablen zu verwenden, die später durch die Daten der Benutzer ersetzt werden. Hier eine Übersicht der Variablen: https://docs.getgophish.com/user-guide/template-reference
- Im Editor kann zwischen **Text** und **HTML** gewechselt werden. Fügen Sie die Vorlage in **Text** ein und bearbeiten diese.
- Um Links zu erstellen markieren Sie den Text und klicken auf das Kettensymbol. Hier können Sie dann die URL (der Phishing Seite) eintragen. Für den GoPhish Server sollte **http** ausgewählt sein.
-

3.4 Landing Pages

Um eine Landing Page zu erstellen, klicken Sie auf **New Landing Page**, dort können Sie dann eine gewünschte HTML Seite Importieren oder erstellen.
Erstellen Sie eine Landing Page für die Anmelde Seite unserer Hochschule.
Hinweise zum erstellen von Landing Pages:

- wählt man die Box **Capture Credentials** aus, werden die eingegebenen Daten in GoPhish gespeichert und es erscheint eine neue Box **Capture Passwords**. Klickt man diese auch an kann man unter **Redirect to** die URL der echten Webseite angeben. So wird der Benutzer nach der Eingabe der Daten auf die echte Seite weitergeleitet und verdächtigt unter Umständen kein Phishing.

3.5 Kampagne starten

Um eine Kampagne zu starten, klicken Sie auf **New Campaign**. Dort können Sie dann die eben erstellten Gruppen und Templates angeben. GoPhish übernimmt hier, da momentan wenige Gruppen usw. vorhanden sind, die Einstellungen automatisch.
Wichtig ist nur die URL des Phishing Servers anzugeben. Hier **http://0.0.0.0:80**.
Man kann noch einen Zeitplan erstellen, wann die Kampagne starten soll oder im welchen Zeitraum. Zusätzlich kann man hier wieder Test E-Mails versenden um zu überprüfen ob alles richtig eingestellt ist.

- Starten Sie die Kampagne.

- Was können Sie im Dashboard sehen?
- Klicken Sie auf die Links in der E-Mail. Was fällt auf.

3.6 Zusatzaufgabe

Versuchen Sie Ihre eigene Kampagne zu erstellen. Sie können z.B für PayPal eine Phishing Seite erstellen. Im Netz finden Sie E-Mail Source Code für die E-Mail Templates