M346, Sicherheit, Phishing-Demo.

Thema:
Cloud, Sicherheits-Aspekte

Lernziele
- Sie sind überzeugt, dass Username und Passwort nicht genügen, um ein Benutzerkonto zu schützen.
- Sie festigen Ihren Umgang mit VM's in der Cloud.

Sozialform
Arbeit im Zweierteam

Warnhinweis:
SocialFish ist eine Awareness-Tool und darf nur zur Sensibilisierung verwendet werden!
Die Verwendung zum Stehlen von Passwörtern ohne vorherige Zustimmung ist illegal und strafbar!

Aufgabe 1: Phishing-Server bereitstellen

Ubuntu VM erstellen
Erstellen Sie eine Ubunto EC2 Instanz, die per SSH erreicht werden kann:

- Name: **MyPhishingServer**
- Machine Image: **Ubuntu Server 22.04 LTS**
- Instance type: **t2.micro**
- Key pair (login): Wahlweise kann ein neuer oder ein bestehender Key verwendet werden.
- Network settings: **[X] Allow SSH traffic from**

Fügen Sie unter «Advanced details» | «user data» folgendes Initialisierungs-Skript ein.

```
#!/bin/bash
sudo apt-get update
sudo apt-get -y install python3-pip
sudo apt-get -y install nmap
pip install PyLaTeX==1.4.1
pip install python3-nmap==1.6.0
pip install qrcode==7.4.2
pip install Werkzeug==2.3.7
pip install Flask==2.3.3
pip install Flask_Login==0.6.2
pip install python-secrets==23.4.2
pip install python-nmap==0.7.1
git clone https://github.com/UndeadSec/SocialFish.git
cd SocialFish
chmod +x SocialFish.py
./SocialFish.py gbs myPassword
```

Mit Launch Instance wird die Server-Instanz erstellt.

Firewall-Einstellungen
In den Security-Einstellungen der Instanz muss eine Inbound-Rule erstellt werden, um den TCP-Zugriff auf Port 5000 zu erlauben.

Öffnen Sie dazu die Instanz und öffnen Sie die im Folder «Security» verlinkte Security-Group.
Wechseln Sie mit Edit inbound rules in den Edit-Modus und erstellen Sie eine Firewall-Regel mit folgenden Eigenschaften:

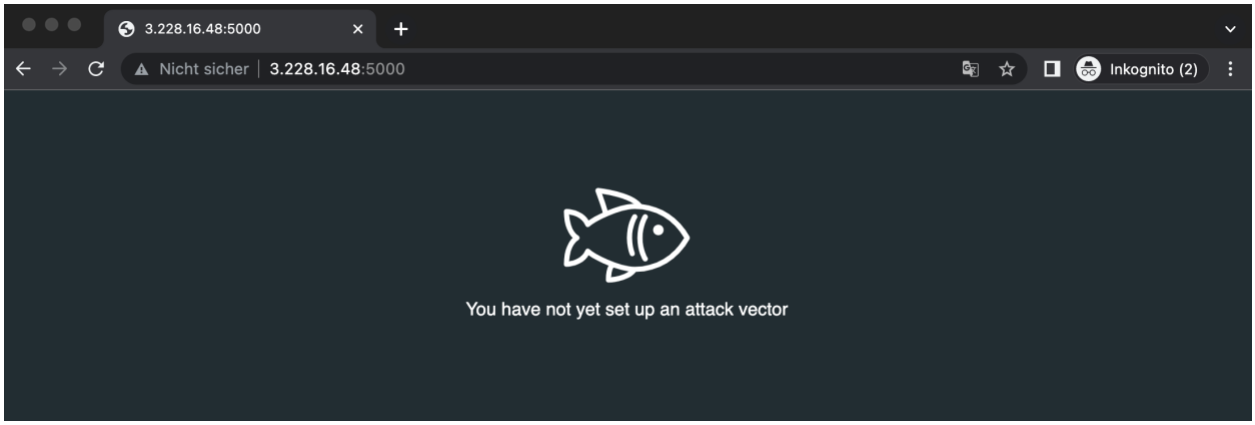
- Type: **Custom TCP**
- Port range: **5000**
- CIDR block: **0.0.0.0/0**

Server testen

Öffnen Sie nun in einem Browser folgende URL: [Public IP der Ubuntu-Instanz]:5000

Hinweis: Die Verarbeitung des Initialisierungs-Skripts dauert ca. 2-3 Minuten. Erst danach ist die Anwendung verfügbar.

Folgende Seite zeigt, dass de Phishing-Server bereits ist:



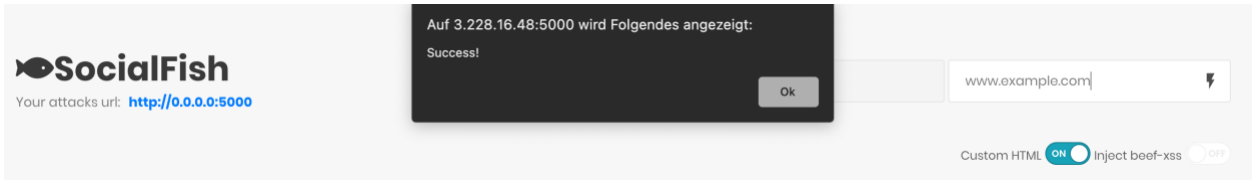
Aufgabe 2: Phishing-Attacke mit statischer Seite

Öffnen Sie das Dashboard mit folgender URL: [Public IP der Ubuntu-Instanz]:5000/neptune und melden Sie sich mit den im Initialisierungsskript übergebenen Login-Daten (gbs | myPassword) an.

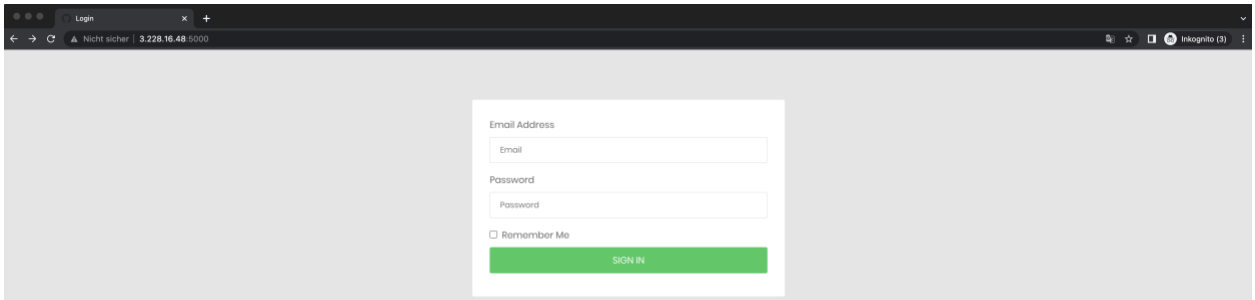
Parametrieren Sie Ihren ersten Angriff wie folgt:

- Aktivieren Sie die Option Custom HTML auf on. Dadurch wird das Feld Clone gesperrt.
- Geben Sie unter Redirection eine URL an, auf die Ihr Phishing-Opfer nach einem erfolgreichen Angriff weitergeleitet werden soll. z.B. www.example.com und schliessen Sie die Eingabe mit [Enter] ab.

Eine Messagebox mit dem Text Success! zeigt, dass Ihre Attacke nun parametriert ist.



Öffnen Sie nun in einem neuen Browser den Opfer-Link [Public IP der Ubuntu-Instanz]:5000. Er führt das Opfer zu einem in SocialFish statisch definierten Anmeldefenster.



Hat das Opfer seine Zugangsdaten eingegeben wird es auf die parametrierte Seite weitergeleitet.

Nach einem Refresh des SocialFish-Dashboards, wird die erfolgreiche Attacke aufgelistet:

Über den View-Link werden die vom Opfer gefischten Daten im Json-Format angezeigt.

Der Angreifer loggt sich mit den gefischten Daten an und wechselt das Passwort. Danach kann er im Namen des Opfers bestellen, Social-Media-Aktionen durchführen etc.

Dass auf diesem Weg auch heute noch Benutzerkonten gestohlen werden, zeigen die folgenden Mediennerichte

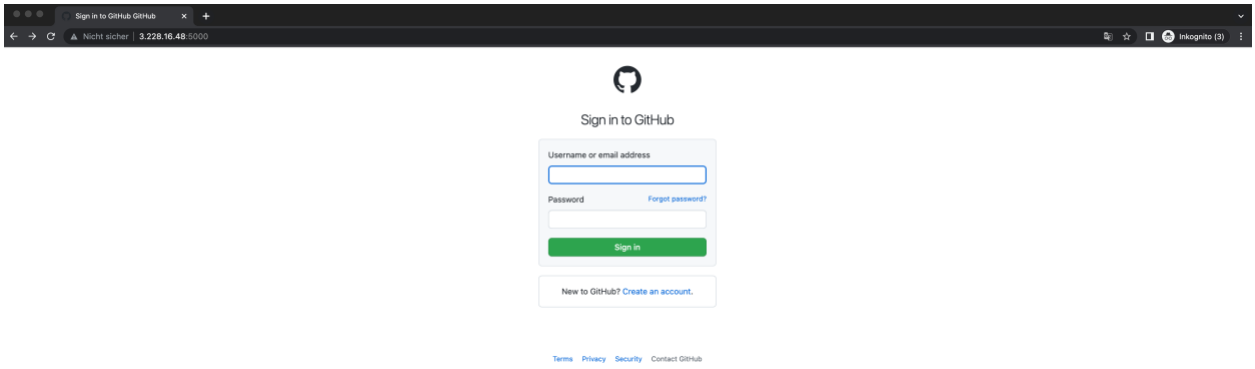
- St. Galler wird gehackt – Galaxus lässt ihn den Schaden zahlen (20.09.2023)
- Kriminelle attackierten Digitec-Galaxus-Kunden (03.10.2019)

Aufgabe 3: Phishing-Attacke mit dynamischer Seite

Parametrieren Sie nun Ihren zweiten Angriff. Es soll ein Gitub-Account gefischt werden.

- Deaktivieren Sie die Option Custom HTML.
- Geben Sie unter Clone die URL des Github-Anmeldefensters ein: https://github.com/login
- als Redirection-URL können Sie eine beliebige URL eingeben. Schliessen Sie die Eingabe wieder mit [Enter] ab.

Ihr 2. Angriff ist nun bereit und der Opfer-Link zeigt nun eine Kopie des Github-Anmeldefensters an.



Hinweis:
In letzter Zeit sind verschiedene Web-Anwendungen gegen Phishing-Angriffe mit automatisch kopierten Login-Seiten abgesichert worden. Dadurch lassen sich Anmeldedaten von Instagram, LinkedIn, Digitec etc. nicht mehr ganz so einfach “fischen”.
Gegen ein gut nachgebautes statisches Anmeldefenster (wie in Attacke 1) schützen solche Abwehrmassnahmen natürlich nicht.