Responsable du cours (ST2EH) : Yousfi Souheib

TP Ingénierie Sociale

1 Présentation des outils Ngrok et Storm-Breaker :

Objectif du TP : L'objectif de ce TP est de vous familiariser avec deux outils qui pourraient être utilisés dans votre projet du Ethical Hacking : Ngrok et Storm-Breaker. Vous apprendrez comment les utiliser efficacement pour exposer des applications locales à Internet et pour simuler des attaques d'ingénierie sociale, dans **un cadre éthique** et de **test de sécurité**.

FIGURE 1 – Reverse Proxy

FIGURE 2 – Outil d'ingénierie sociale

1.1 Ngrok : Exposition d'applications locales sur le Web

Ngrok est un outil puissant qui permet de créer des tunnels sécurisés vers vos serveurs locaux. Cet outil est très pratique pour tester des applications locales, partager des prototypes, ou configurer des **webhooks**. Il évite d'avoir à configurer un serveur externe ou à modifier des pare-feu et autres paramètres réseau.

Pourquoi utiliser Ngrok ?

- **Tester des applications locales en ligne :** Exposez rapidement une application web qui tourne sur votre ordinateur à des collaborateurs ou clients, où qu'ils soient.
- **Recevoir des webhooks :** Testez des intégrations avec des services externes en exposant vos endpoints locaux.
- **Facilité d'utilisation :** Aucune configuration complexe nécessaire, un simple exécutable et une commande suffisent à créer un tunnel HTTPS sécurisé.

Exemple d'utilisation dans ce TP :

Nous allons utiliser Ngrok pour exposer une application locale (comme un serveur web) à l'internet. Cela vous permettra de voir comment on peut partager un projet web en temps réel avec une URL publique.

1.2 Storm-Breaker : Ingénierie sociale et simulation d'attaques

Storm-Breaker est un outil de sécurité qui permet de simuler des attaques d'ingénierie sociale. Il est capable de collecter des informations sensibles sur les appareils cibles à distance via des liens malveillants. Cet outil est destiné à être utilisé dans un cadre éthique, lors de tests de pénétration pour évaluer les failles humaines et techniques dans la sécurité.

Pourquoi utiliser Storm-Breaker ?

- **Tester la vigilance face aux attaques de phishing :**Vérifiez comment les utilisateurs réagissent à des scénarios de phishing et comment leurs appareils peuvent être compromis via des liens malveillants.
- **Collecte d'informations :** Simulez des attaques qui révèlent des informations sur l'appareil cible (comme l'IP, la géolocalisation, et parfois l'accès à la caméra ou au micro).
- **Éducation à la cybersécurité :** C'est un excellent moyen de sensibiliser les utilisateurs aux risques associés à l'ingénierie sociale.

2 Scénario :

Clonez le dépôt GitHub officiel de Storm-Breaker et installez les dépendances nécessaires.

```
ubuntu@ubuntu:/opt$ sudo git clone https://github.com/ultrasecurity/Storm-Breaker.git
Cloning into 'Storm-Breaker'...
remote: Enumerating objects: 493, done.
remote: Counting objects: 100% (129/129), done.
remote: Compressing objects: 100% (70/70), done.
remote: Total 493 (delta 73), reused 60 (delta 57), pack-reused 364 (from 1)
Receiving objects: 100% (493/493), 7.79 MiB | 20.93 MiB/s, done.
Resolving deltas: 100% (245/245), done.
```

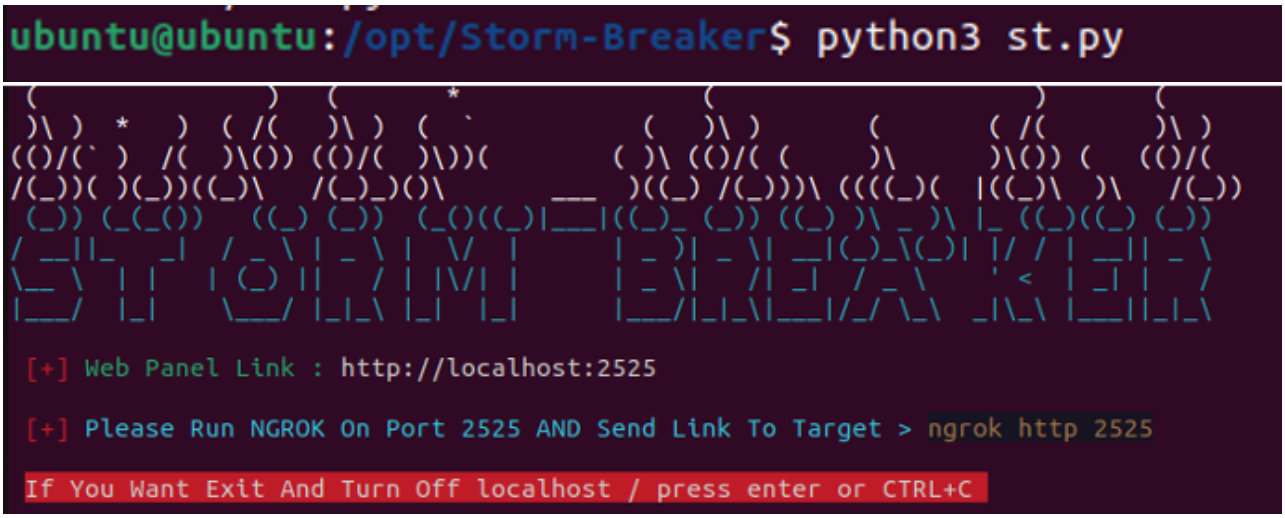
```
ubuntu@ubuntu:/opt$ cd Storm-Breaker/
ubuntu@ubuntu:/opt/Storm-Breaker$ ls
install.sh  modules  README.md  requirements.txt  Settings.json  storm-web  st.py
```

```
ubuntu@ubuntu:/opt/Storm-Breaker$ sudo bash install.sh
[sudo] password for ubuntu:

                --      --
             .:"  | .:'" |
          --   ___    ___   -        Storm-Breaker's dependencies installer
         /:.  /   .\ /.   \ .\
        |:|. ;\___/O\___/   :|  Github: https://github.com/ultrasecurity/Storm-Breaker/
        |:|. |   `__|__'    | .|
        |:|.  \_,       ,_/   /
         \______        |__/
          |:.             \
         /.:,|   |         \
        /.:,.|   |          \
        |::.. \_;_\-;        |
 _____|::..     .::|        |
/    ----,      .::/__,     /__,
\_______|,...____;_;_|../_;_|
```

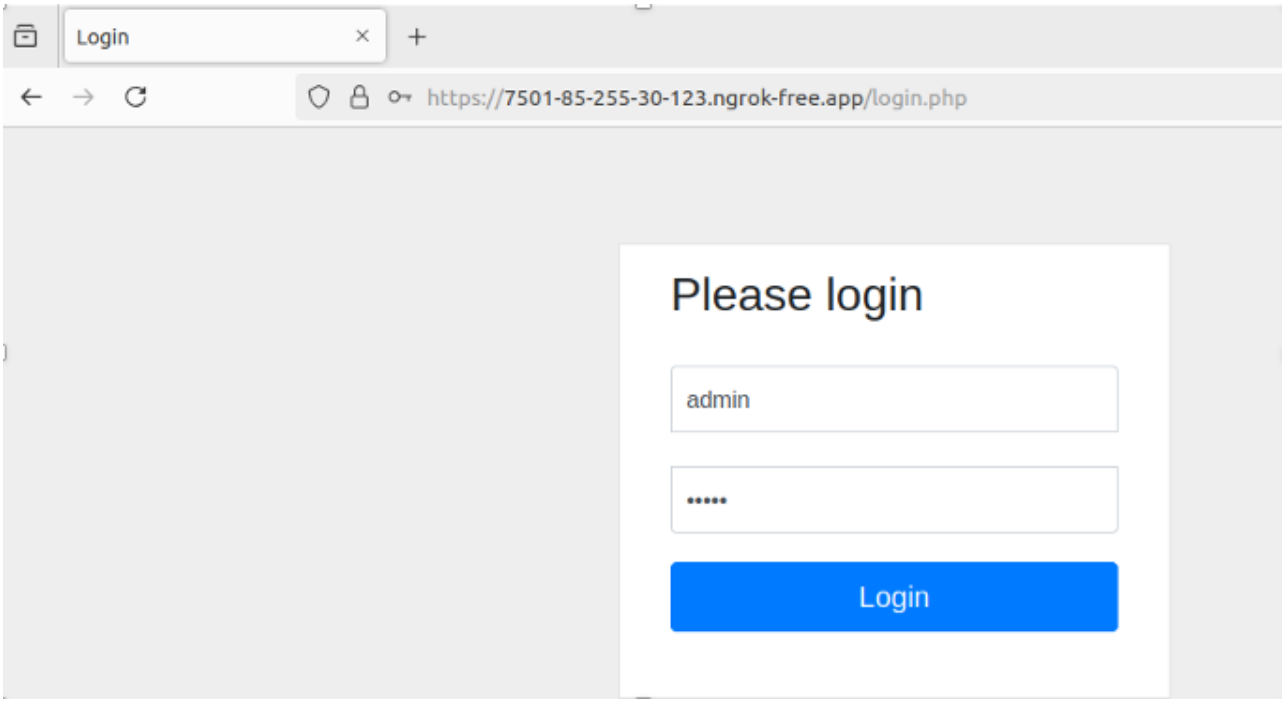
```
ubuntu@ubuntu:/opt/Storm-Breaker$ sudo python3 -m pip install -r requirements.txt
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r req
uirements.txt (line 1)) (2.25.1)
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from -r req
uirements.txt (line 2)) (0.4.4)
Requirement already satisfied: psutil in /usr/local/lib/python3.10/dist-packages (from
 -r requirements.txt (line 3)) (6.0.0)
```

- Téléchargez et installez Ngrok depuis le site officiel.
- Créez un compte Ngrok pour obtenir votre authtoken et configurez-le.



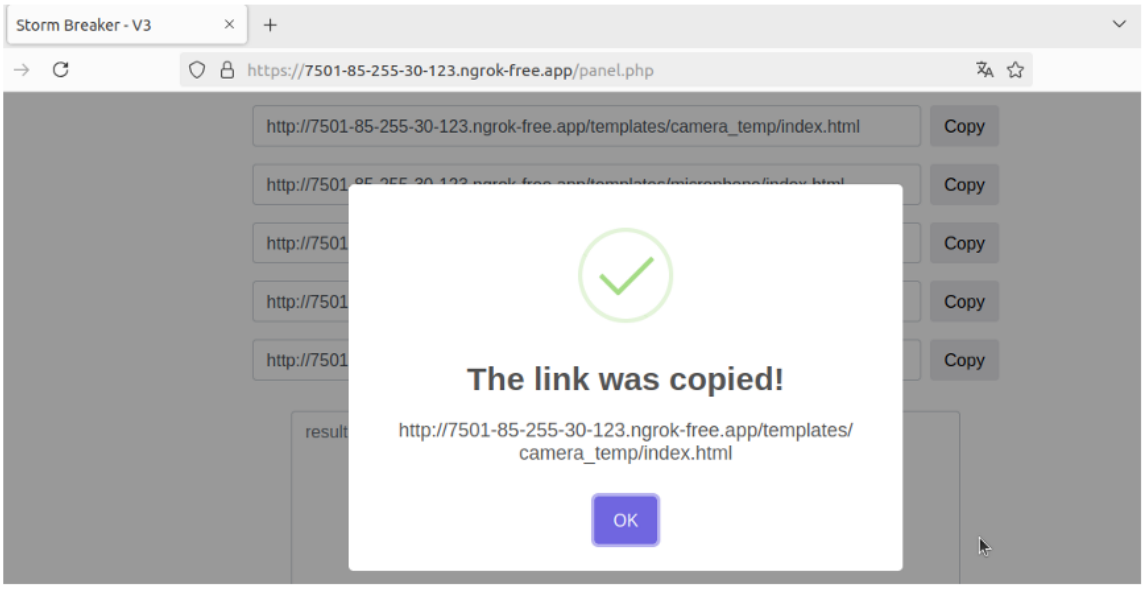
Sur un autre terminal, lancez la commande Ngrok http 2525 :

Une URL publique sera générée, que vous pouvez partager pour accéder à votre application locale depuis n'importe où. Le credential est (admin, admin)



Simulez une attaque en accédant au lien depuis un autre appareil ou via un navigateur. Col-

lectez les informations sur l'appareil cible et discutez des failles possibles ainsi que des moyens de s'en protéger.



En simulant l'attaque, j'ai pu avoir l'adresse ip (sans même une autorisation) et une fois la caméra autorisé je peux avoir des snapchat sur ma victime.

ip : 85.[redacted]
os name : Mac OS
Version : 10.15.7
Browser Name : Chrome
Get Browser Version : 128.0.0.0
Cpu Name : undefined
Resolution : 1440x900
Time Zone : heure d'été d'Europe centrale
Language : fr-FR
Number Of CPU Core : 8

Image File Was Saved ! > /images/cam24Sep2024091156.png

3 Conclusion :

À travers ce TP, vous aurez découvert comment exposer une application locale avec Ngrok et comment simuler des attaques de phishing avec Storm-Breaker dans un environnement sécurisé et contrôlé. Ces outils vous aideront à mieux comprendre les défis liés à la cybersécurité, ainsi que les bonnes pratiques à adopter pour sécuriser vos applications et infrastructures.
Pour votre projet final en matière d'ethical hacking, n'hésitez pas à appliquer les connaissances acquises avec ces outils. Ils vous fourniront des perspectives pratiques sur la sécurité informatique et renforceront votre capacité à concevoir des solutions de sécurité robustes.

Rappel important :Storm-Breaker et Ngrok doivent être utilisés à des fins éducatives et éthiques uniquement. L'utilisation de ces outils à des fins malveillantes est strictement illégale et peut avoir des conséquences graves.

♣ S.Y. ♣
Bon travail