



TP PHISHING(SOCIAL ENGINEERING TOOL KIT)



Timothé Icart

Sommaires

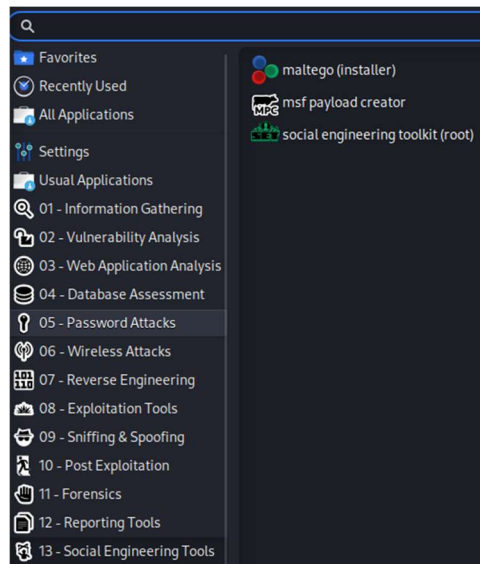
- Préparation côté attaquant
- Côté victime
- Résultat côté attaquant

Préparation côté attaquant :

Vous devez utiliser un système d'exploitation kali :

Kali Linux est spécialisée dans la sécurité informatique. Elle est basée sur Debian et comprend de nombreux outils de test de pénétration et de sécurité pour les professionnels de la sécurité informatique et les chercheurs en sécurité.

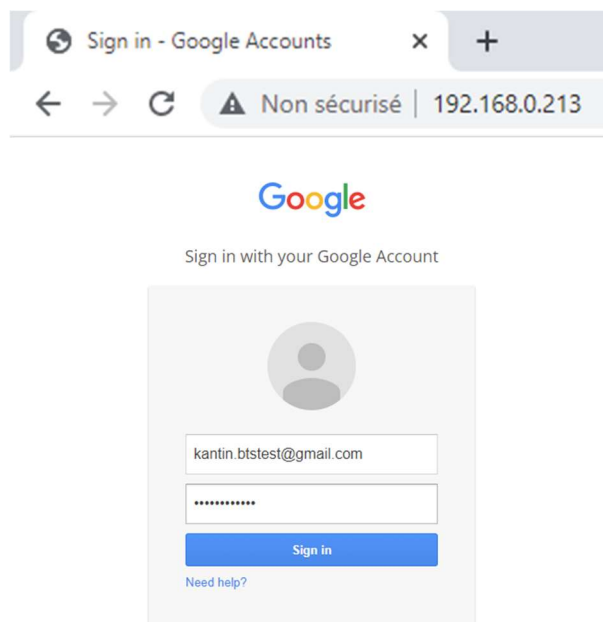
Lancez l'application social engineering toolkit



Entrez le mot de passe de votre session pour avoir accès à l'application

Côté victime

Je clique sur le lien que l'attaquant ma envoyé en usurpant l'identité de google



Entrez vos identifiants et après avoir validé, vous serez redirigé vers la page Google pour effectuer une recherche



Résultat côté attaquant

Dans la même console qu'au début vous verrez qu'elle s'actualisera et les identifiants et mot de passe vont apparaitre.

Vous avez gagné et la victime s'est faite avoir.

```
192.168.0.4 - - [06/Apr/2023 07:50:00] "GET / HTTP/1.1" 200 -
192.168.0.4 - - [06/Apr/2023 07:50:01] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLckfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWfBwd2JmV1hIcDhtUfdldzBENhIfVwsxSTdNLW9MdThibw1TMFQzVUZFc1BBaUR
uWmlRSQ%E2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRid3YTjX
PARAM: service=ls0
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=kantin.btstest@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=password123!
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```