Reconnaissance

Guillaume Pillot

Club de Hacking de l'Université Laval

27 Septembre 2016

Sommaire

Qu'est ce que la reconnaissance ?

- Recueil d'informations sur une cible, principalement des adresses IP
- Première étape d'un test d'intrusion et la plus importante, mais souvent négligé
- "Que l'on me donne six heures pour couper un arbre, j'en passerai quatre à préparer ma hache." A.Lincoln
- Reconnaissance active : interaction directe avec la cible. La cible peut vous détecter
- Reconnaissance passive : Aucune interaction avec la cible. Informations disponibles sur le Web. La cible ne peut pas vous détecter
- Documentation : Les bases du hacking. Chapitre 2 : La reconnaissance p. 21 à 25

Opérateurs Google

- Permet d'extraire de façon plus précise les pages indexé par Google
- Voici quelques exemples :
  - Pages contenant les mots "guillaume pillot" sur le site hacking.fsg.ulaval.ca :
    `site:hacking.fsg.ulaval.ca guillaume pillot`
  - Sites web dont les titres de pages comprennent tous les mots "club hacking ulaval" :
    `allintitle:club hacking ulaval`
  - Sites web contenant le mot "admin" dans leur URL :
    `inurl:admin`
  - Afficher le site web hacking.fsg.ulaval.ca contenu dans le cache de Google (pensez à désactiver la recherche instantanée de google) :
    `cache:http://hacking.fsg.ulaval.ca`
  - Fichiers PDF contenus sur le site web hacking.fsg.ulaval.ca :
    `site:hacking.fsg.ulaval.ca filetype:pdf`

Google Hacking DataBase (GHDB)

- Un Google Dork est une recherche Google qui permet de découvrir des vulnérabilités sur une cible
- Google Hacking DataBase (GHDB) est une base de données maintenue par Offensive-Security contenant plusieurs Google Dork accessible via cette URL : https ://www.exploit-db.com/google-hacking-database/
- Pour en savoir plus sur le Google Hacking, consulter le livre Google Hacking for Penetration Testers de Johnny Long

HTTrack

- HTTrack est un outil qui permet de copier en local un site web
- Moins on passe du temps sur le site web de la cible, moins on laisse de traces
- NB : Le clonage d'un site web est facile à repérer et est considéré comme fortement offensif, on ne peut utiliser HTTrack sans autorisation préalable

```
# apt-get install httrack
```

- Ensuite il suffit de lancer la commande :

```
# httrack
```

- Il suffit de suivre les instructions, pour les options, choisissez l'option 2 pour cloner le site ou l'option 4 pour cloner les autres sites liés dans notre cible.
- Documentation : Lien

The Harvester

- The Harvester permet de cataloguer rapidement les courriels et les sous-domaines directement liés à la cible
- L'outil passe par les serveurs de Google,Bing,PGP et Exalead pour effectuer ses recherches
- Il est intégré à Kali et son utilisation est très simple :

```
# theharvester -d ringzer0team.com -b google -f /home/myuser/test
```

On effectue une collecte sur le site ringzer0team.com en utilisant Google et on enregistre les résultats dans le fichier test.html dans /home/myuser

`-b all` permet d'effectuer la recherche dans tous les référentiels reconnus (Google,Bing,PGP et Exalead)

- Documentation : Lien

Whois

- Whois permet de recueillir les informations publiques d'un site web tels ses serveurs DNS, son IP, le registrar, etc.
- L'outil est intégré par défaut dans Linux et son utilisation est triviale :

```
# whois ringzer0team.com
```

- Vous pouvez aussi utiliser le site web : https ://whois.net/
- Documentation : Lien

Netcraft

- Netcraft est une entreprise qui mène des sondages automatisés d'Internet par nom de domaine à la recherche de serveurs HTTP
- On peut effectuer des recherches sur son site à partir de cette URL : http ://toolbar.netcraft.com/site_report/
- Documentation : Lien

Host

- Grâce aux outils précédant, on a pu collecter plusieurs DNS, il faut maintenant obtenir leur adresse IP
- Host permet de traduire des noms d'hôte en adresse IP
- L'outil est installé dans la plupart des distributions Linux et son utilisation est triviale :

```
# host NS17.DOMAINCONTROL.COM
```

- L'option `-a` permet d'obtenir plus d'informations
- Documentation : `# man host`

Internet Archive

- Internet Archive est un organisme à but non lucratif consacré à l'archivage du Web
- On peut accéder aux anciennes versions d'un site web via cette URL : https ://archive.org/web/
- Documentation : Lien

RobTex

- RobTex est une sorte de couteau suisse d'Internet
- Il centralise à peu près toutes les recherches faites précédemment
- https ://www.robtex.com
- Documentation : Lien

Transfert de zone (AXFR)

- Les serveurs DNS peuvent contenir de précieuse informations (surtout quand ils sont mal configuré)
- Rappel : Le DNS permet de traduire les nom de domaine (hacking.fsg.ulaval.ca) en adresse IP
- Pour assurer une redondance et une répartion de la charge, plusieurs DNS peuvent être déployés dans un réseau. Pour partager des informations entre eux, les serveurs utilisent un mécanisme nommé transfert de zone (ou AXFR). Au cours de ce transfert, un serveur envoie toutes les correspondances hôtes-IP qu'il contient à un autre serveur DNS assurant ainsi la synchronisation entre tous les serveurs.
- Réaliser un transfert de zone sur un serveur DNS permet donc d'obtenir beaucoup d'informations.
- Documentation : Les bases du hacking. Chapitre 2 : La reconnaissance p. 43 et 44

NSLookup

- Outil très connu permettant d'interroger les serveurs DNS
- Intégré sur la plupart des Linux et disponible pour Windows
- `# nslookup 132.203.210.235`
- NSLookup fonctionne en mode intéractif :

  `# nslookup`

  `> server 8.8.8.8` <= L'IP du serveur

  `> set type=any` <= Le type de recherche

  `> google.com` <= domaine cible
- Documentation : Lien

Dig

- Dig permet d'extraire des informations du DNS :

```
# dig hacking.fsg.ulaval.ca
```

- Cet outil permet d'effectuer des transferts de zone si la cible les autorise et ne les limite pas :

```
# dig @132.203.210.235 hacking.fsg.ulaval.ca -t AXFR
```

- Documentation : Lien

Fierce

- Fierce est un autre outil permettant d'interroger le DNS
- `# fierce -dns ringzer0team.com`
- Il commence par tenter un transfert de zone, puis vérifie l'existence d'un "Wildcard DNS record" et effectue plusieurs tests
- Documentation : `# fierce -h`
  Lien

MetaGooFil

- Une métadonnée est une information sur une donnée (auteur, taille,titre, format, etc.)
- MetaGooFil cherche sur Internet tout document appartenant à la cible et les télécharge
- La version par défaut de Kali ne fonctionne pas, il faut donc télécharger celle-ci : https ://github.com/opsdisk/metagoofil
  Il faut installer le package de google dans Python comme ceci :
  `# pip install google`
  Ensuite, il suffit d'extraire le .zip et exécuter le fichier python :
  `# python metagoofil.py -d guillaume-pillot.ca -t pdf,doc -w mondossier`
  Pour extraire les métadata, on peut utiliser pdfinfo :
  `# pdfinfo monfichier.pdf`
  Pour extraire les métadata de tous les PDFs, on peut utiliser la commande suivante :
  `# for f in ``ls *.pdf``; do pdfinfo $f; done`
- Documentation : `# metagoofil.py -h`

FOCA

- FOCA est un outil d'extraction de métadonnée très populaire pour Windows
- Documentation : Lien

SearchDiggity

- SearchDiggity est un autre outil pour Windows
- Documentation : Lien1 Lien2
  Dans la GUI : Help -> Content

Ingénierie sociale

- Obtenir des informations via les courriels des employés
- Bien d'autres techniques
- Un domaine à part entière
- Livre : Social Engineering : The Art of Human Hacking

Advanced Reconnaissance Framework

- Site web regroupant un bon nombre d'outils de reconnaissance
- http ://osintframework.com/

Maltego

- Maltego collecte toutes informations publiques sur la cible (site web, personne, etc.) que contient internet
- Il relie toutes ses informations sous forme de graphe
- Il est possible de rajouter à la main d'autres informations collectées par les autres outils permettant de tout regrouper en un seul point
- Documentation : Lien

Challenge Time

- Quel est le registar du site ringzer0team.com ?
- Quel est son adresse IP ?
- Il y a un flag dans l'un des PDF du site de hacking.
- https ://ringzer0team.com/challenges/160
- https ://ringzer0team.com/challenges/217