Introduction au *pentesting*

(Test d'intrusion + demo)

Jean-Patrick Gelas
Université Claude Bernard Lyon 1

Sources

- The Hacker Playbook 2, Peter Kim, Ed. Createspace
- Metasploit, David Kennedy et al. Ed. Pearson
- Wikipedia : https://fr.wikipedia.org/wiki/Test_d%27intrusion
- Youtube…
- TODO

Introduction

Test d'intrusion / *Penetration test / Pentest*

- Un test d'intrusion est une méthode d'évaluation de la sécurité d'un système ou d'un réseau informatique.
- Simulation d'un utilisateur (ou logiciel) malveillant.
- Le testeur adopte la position d'un attaquant potentiel.
- Le testeur analyse les risques potentiels du a :
  - Une mauvaise configuration d'un système
  - Un défaut de programmation

- Objectif : Trouver des vulnérabilités exploitables en vue de proposer un plan d'actions permettant d'améliorer la sécurité d'un système.

Trois types d'analyse

- **Blackbox** : Le testeur se met dans la peau de l'attaquant et ne possède a priori aucune information.
- **Greybox** : Le testeur possède un nombre limité d'informations (ex: un compte pour passer l'étape d'authentification).
- **Whitebox** : Le testeur possède les informations dont il a besoin (ex: schéma d'architecture, compte utilisateur, code source, …).

Les tests « *Red Team* »

- Test d'intrusion :
  - sans limite de temps (2 à 3 mois au lieu d'une ou deux semaines),
  - ni de périmètre précis défini par le commanditaire (le nom de l'entreprise seulement).
- En complément les testeurs peuvent user de techniques alternatives (ex: Social engineering, Intrusion physique,…)

Youtube: Watch hackers break into the US power grid (Durée : 15'50'')
`https://www.youtube.com/watch?v=pL9q2lOZ1Fw`

Quelques définitions

- **Social-engineering** (ingénierie sociale) : forme d'acquisition déloyale d'informations. Exploite les failles humaines. https://www.youtube.com/watch?v=lc7scxvKQOo

- **Phishing** : …
- **Spear phishing** : Contrairement au phishing le message est ici fortement personnalisé et envoyé à un nombre très limité d'utilisateurs (parfois un seul).

- TODO…

Principes fondamentaux nécessaire au bon déroulement d'un test (cf. PTES)

1. Préengagement
2. Collecte de renseignements
3. Détermination de la menace
4. Analyse des vulnérabilités
5. L'exploitation
6. Post exploitation
7. Le rapport

1. Préengagement

- Discussion à propos de la portée et des modalités du test d'intrusion avec le client.
- Présentation de vos objectifs, ce qui doit être attendu d'un test complet (sans restrictions) sur ce qui peut et sera testé.

2. Collecte de renseignements

- Une des compétences les plus importantes d'un testeur est sa capacité à acquérir le plus d'informations possible sur la cible.
- Peu importe les moyens. Adaptez vous. (via Internet, Réseau interne ou sans fil, ingénierie sociale)
- Identifiez les mécanismes qui protègent la cible en commençant par sonder lentement (ou avec une IP sacrifiable).

3. Détermination de la menace

- On examine la cible comme un adversaire.
- Requiert les informations obtenu lors de la phase de collecte afin d'identifier les vulnérabilités potentiels.

4. Analyse des vulnérabilités

- Vous déterminez les méthodes d'attaques les plus efficaces en combinant les informations apprisent lors des phases antérieurs.

- Example : scan de ports, consultation des bannières de services réseaux,…
- Des outils de scan de vulnerabilités : Nessus, NeXpose,...

5. L’exploitation

- La partie la plus sympa d’un test d’intrusion même si parfois réalisé par *brute force* plutôt qu’avec précision.
- Ne lancer que des *exploits* susceptible de réussir.

6. Post exploitation

- Après avoir compromis un (ou plusieurs) système(s).
- Visez des systèmes spécifiques, identifiez les infrastructures critiques, et les données que la cible a tenté de sécuriser.
- Essayez de démontrer les attaques qui auront le plus de répercussions sur les affaires de l'organisation ciblée.

7. Le rapport

- Documentez ce que vous avez fait, comment vous l'avez fait et comment l'organisation pourrait corriger les vulnérabilités découvertes.

Metasploit

Introduction à Metasploit

- Le framework Metasploit (MSF) est très utilisé par les professionnels de la sécurité de l'information.
- Gratuit, Open source + deux versions commerciales.
- C'est un cadre qui fournit l'infrastructure nécessaire pour automatiser les tâches routinières ou complexe.

Metasploit : Terminologie

- **Exploit** : c'est le moyen par lequel le pentester profite d'un défaut dans un système, une application ou un service. On l'utilise pour attaquer et produire un résultat que les développeurs n'avaient pas envisagé (injection sql, buffer overflow, …).
- **Payload** : code que l'on veux faire exécuter sur la cible (ex: reverse_shell)
- **Shellcode** : suite d'instructions utilisées par un payload qui fournit généralement un *shell* (ou *meterpreter shell*).
- **Module** : part de logiciel utilisé par le framework Metasploit.
- **Listener** : composant qui attend une connexion entrante.

Metasploit : MSFconsole

- MSFconsole fournit une interface pratique tout-en-un pour toutes les options et tous les réglages disponibles.
- On peut y lancer un exploit, charger un module auxiliaire, faire une énumération, créer des *listeners* ou lancer une exploitation massive contre tout un réseau.

Collecte de renseignements

La collecte permet d'obtenir des informations précises sur votre cible sans révéler vos intentions. Elle exige une préparation minutieuse (pour ne pas manquer des vecteurs d'attaque) et la faculté de penser tel un attaquant.

Notez tout ! Soyez méthodique et précis.

- Collecte d'information passive
  - Whois, Netcraft, nslookup, réseaux sociaux, moteurs de recherche,…
- Collecte d'information active
  - Scan de ports (nmap)
- Scan ciblé
  - SMB, Microsoft SQL, SSH, FTP, SNMP,…

Les joies de l'exploitation

- La possibilité de prendre enfin le contrôle total sur une machine cible (mais ne soyez pas stupide !)
- MSFconsole (demo)

  show exploits, show auxiliary, show options, search, use, show payloads, show targets, info, set/unset, setg/unsetg, save, …

Escalade de privilèges

Privilege escalation

- Parfois on compromet un compte utilisateur ayant des droits limités.
- Empêche l'exécution de commandes qui nécessitent des droits administrateurs.
- En élevant les droits d'un compte, nous surmonterons ces restrictions.

- Ex: http://resources.infosecinstitute.com/privilege-escalation-linux-live-examples/

La boîte à outils du social engineer (SET, Social Engineer Toolkit)

(demo)

Conclusion

- Les tests d'intrusion sont un moyen de simuler les méthodes d'un pirate.
- On ne peut pas devenir un expert de la sécurité informatique du jour au lendemain.
- Adoptez une méthodologie (ex: PTES)

For fun and profits…

- https://www.root-me.org/
- https://www.hackthebox.eu
- Youtube : Defcon 18 Pwned By the owner What happens when you steal a hackers computer zoz part https://www.youtube.com/watch?v=U4oB28ksiIo

- Mr Robot (Série TV/saison 1) https://fr.wikipedia.org/wiki/Mr._Robot_(s%C3%A9rie_t%C3%A9l%C3%A9vis%C3%A9e)

- http://www.exploit-db.com
- http://www.shodan.io (port:554 has_screenshot:true country:fr)