Cours 5 :

Introduction au test d'intrusion

JACQUEMIN Mathieu

Disclaimer

- Ce cours a été créé dans le but d'informer et d'éduquer les participants sur les sujets liés à la cybersécurité. L'ensemble des techniques présentées le sont à titre pédagogique et préventif afin de pouvoir se prémunir d'attaque potentiel.
- Certaines des techniques présentées sont illégales et dangereuses si elles sont utilisées à mauvais escient, sans maitrise, et sans consentement.
- Il est interdit d'utiliser ces techniques contre toute entité dont vous ne disposez pas le consentement. Dans le cadre d'un accord pour audit, il est obligatoire d'agir dans le cadre d'un contrat parfaitement défini, écrit, et signé par les deux parties.
- Vous devez respecter la loi en vigueur ainsi qu'utilisez les techniques avec éthique et responsabilité.
- Je me dédouane de toute responsabilité en cas de problème ou d'incidents à la suite de ce cours.
- Vous êtes seul responsable de l'usage fait des connaissances enseignées.

Le test d'intrusion

Qu'est-ce que c'est ?

Pourquoi ?

Le test d'intrusion

Tester des identifiants (d'utilisateurs mais même d'administrateur)
Tester un nouveau service qui vient d'être installé sur le système
Tester le personnel (une personne ciblée ou non)
Etc...

Tout ça dans le but de sécuriser son système, son réseau ou une application.

Les différents types de tests

Que voulons nous tester ?
- Application web
- Réseau
- Un appareil particulier (Ordinateur, smartphone, imprimante, etc..)

Le tout est encadré par un contrat !!!

Les 5 phases du pentest

Phase 1 : La reconnaissance

Phase 2 : Le scan réseau

Phase 3 : Gagner l'accès

Phase 4 : Maintenir l'accès

Phase 5 : Couvrir les traces

Phase 1 : La reconnaissance

Récupération des informations avant de passer à l'attaque

Passive ou active ?

Etape la plus facile mais la plus longue !

Phase 2 : Le scan réseau

Récupération des détails précis sur les systèmes

Ports ouverts ?

Vulnérabilités présentes ?

Phase 3 : Gagner l'accès

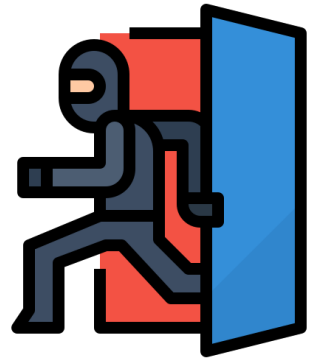
On a accès au système

Faiblesse exploitée

Phase 4 : Maintenir l'accès

On se facilite un accès futur

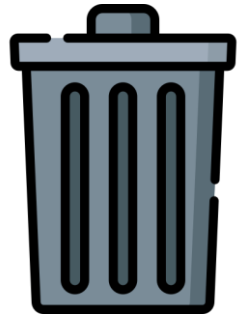
Backdoors (porte dérobée)



Phase 5 : Couvrir les traces

Destruction des preuves

Suppression des fichiers logs



En savoir plus

Plateforme en ligne de challenges de cybersécurité
https://tryhackme.com/

https://www.hackthebox.com/

https://www.root-me.org/?lang=fr

Hacktback, chaine Youtube
https://www.youtube.com/@HacktBack