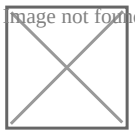

Comment un test d'intrusion est-il réalisé ?

Question / réponse publié le **27/03/2020**, vu **2268 fois**, Auteur : Droit de la sécurité informatique

Un test d’intrusion est réalisé en principe dans les conditions réelles. Les conditions dans lesquelles serait un pirate essayant de s’introduire sur un système informatisé.

L’objectif étant de démontrer l'existence de failles de sécurité dans l’application ou service audité.

Toutefois, quelques différences subsistes. Dans le cadre d’une mission d’audit le client est informé de la date de début des tests, de la date de fin et le périmètre de l’audit. Il est également invité à réaliser des sauvegardes avant le début de la mission afin de pouvoir récupérer des données qui seraient éventuellement endommagées.

Le pentester ne réalisera pas la même mission d’une mission à l’autre. Un test d’intrusion sur une application mobile sera différent d’un pentest sur du woocommerce. Toutefois, la méthodologie d’audit restera la même. Dans un premier temps il essayera d’identifier les vulnérabilités présentes sur l’application (code, port, configuration…).

S’il réussit il récupérera un maximum d’informations puis essayera de récupérer des accès à droits élevés. Sauf demande explicite du client, il ne procédera pas à des attaques DDOS visant à rendre HS l’application auditée.

En tout état de cause, le test d'intrusion ne peut être automatisé. L'humain est essentiel dans cette démarche. C'est la reproduction d'une vraie attaque informatique. Les scans de vulnérabilités sont bien évidemment utilisés par le pentester, mais il ne se limitera pas à ces outils. Les scans donnent des pistes mais sont limités et n'abordent pas l'ensemble d'un périmètre d'attaque.

A l’issue de la période de test, le spécialiste en sécurité informatique procédera à la rédaction des livrables à remettre au commanditaire. Parfois, lorsque cela est demandé il présentera les résultats de l’audit lors d’une réunion de restitution.