Conduisez un test d'intrusion

Partie I - Préparez votre test d'intrusion

1.1 *C'est quoi un test d'intrusion (ou pentest) ?*

Dans cette première partie, nous allons étudier comment préparer un test d'intrusion. Vous verrez ce qu'est un test d'intrusion ou *pentest*, les différents types de tests qui existent et apprendrez à installer votre environnement pour réaliser votre premier pentest.

1.2 Un pentest, c'est quoi ?

Commençons par la base : quelques définitions.

Un **test d'intrusion,** ou **test de pénétration,** ou encore **pentest,** est une méthode qui consiste à analyser une cible en se mettant dans la peau d'un attaquant (connu aussi sous le nom d'hacker malveillant ou pirate, mais nous y reviendrons). Cette cible peut être :

- **Une IP,**
- **Une application,**
- **Un serveur web,**
- **Ou un réseau complet.**

Dans ce cours, vous allez pratiquer sur un serveur web. **Le test d'intrusion** est donc une photographie à l'instant T de cette cible. Il ne doit donc pas être confondu avec le **scan de vulnérabilités**.

C'est quoi un **scan de vulnérabilité** ?

Le scan de vulnérabilité est une composante du test d'intrusion, c'est-à-dire une sous-partie. C'est plus précisément un **scan** (comme son nom l'indique) de la cible qui permet **d'énumérer les vulnérabilités,** sans tenter de les qualifier ou de vérifier si elles sont exploitables.

Contrairement à ce que certains pensent, le **test d'intrusion** n'est pas **un audit de sécurité**. Brièvement, l'audit permet d'établir un panorama de la sécurité d'un système d'information, mais il ne va pas tester la réalité et l'exploitabilité de chaque vulnérabilité. Il se concentre plutôt sur la sécurité fonctionnelle, opérationnelle et plus généralement la politique de sécurité du système d'information (**PSSI**) mise en place. D'un autre côté, le test d'intrusion est plus technique et pratique. Il va révéler par exemple, une application non à jour ou encore un port ouvert par erreur dans le firewall.

1.3 Un test d'intrusion, pour quoi faire ?

Depuis plusieurs années, le nombre de cyberattaques double, année après année. L'intention des pirates est variée, mais les principales motivations sont d'ordre :

- **Économique,**
- **Politique**
- **Ou juste pour le challenge de l'exercice !**

Cela dit, la grande majorité du temps, elle est économique. L'objectif étant de gagner de l'argent à l'insu ou sur le dos des entreprises, comme dans le cas du cheval de Troie « Ruthless » qui vole les numéros de cartes bancaires et accès aux comptes bancaires.
Il existe beaucoup de **groupes de hackers** plus ou moins malveillants dans le monde.

Il y a pas mal d'années, la sécurisation des systèmes coûtait cher et les chances de se faire pirater étaient minces. Cela dit, aujourd'hui la donne a changé car le pourcentage de chance de se faire pirater est élevé. Il faut absolument que chaque entreprise mette en place une sécurité adaptée.
Mais pourquoi faire des tests d'intrusion ?

Les objectifs sont clairs :

- Identifier les **vulnérabilités** de son SI ou de son application
- Évaluer le **degré de risque** de chaque faille identifiée
- Proposer des **correctifs** de manière priorisée

Grâce au test d'intrusion, nous pouvons qualifier :

- La **sévérité** de la vulnérabilité,
- La **complexité** de la correction,
- Et l'ordre de **priorité** qu'il faut donner aux corrections.

Le but n'est pas malveillant, mais il est de s'assurer que ces vulnérabilités sont bien réelles.
Par exemple, aujourd'hui certaines entreprises ont encore des vulnérabilités dans leurs réseaux permettant aux **rançongiciels** de se propager. Un rançongiciel (*ransonmware* en anglais), c'est un logiciel malveillant qui prend en « otage » vos données personnelles et qui les restitue uniquement contre le versement d'une « rançon ».

Un test d'intrusion permet d'en prendre conscience et de prioriser les corrections. Sinon la vulnérabilité risque de rester dans le système jusqu'à son exploitation malveillante. Une récente étude a établi que dans le monde, une entreprise se fait attaquer, en moyenne, toutes les 40 secondes par un rançongiciel.

1.4 Quand faire ce test ?

Afin de sécuriser l'infrastructure ou l'application, les tests d'intrusion peuvent être faits à différents moments :

- Lors de la **conception** du projet, afin d'anticiper les éventuelles attaques,
- Pendant la **phase d'utilisation,** à intervalle régulier
- **Suite à une cyberattaque** pour ne pas que ça se reproduise

La conduite d'un test d'intrusion est à l'initiative de l'entreprise qui veut se tester.

Le test d'intrusion peut se faire de **l'extérieur** (test d'intrusion externe). Ce test d'intrusion pourra être réalisé de n'importe quelle connexion Internet.

Le test d'intrusion peut également se faire de **l'intérieur** de l'infrastructure (test d'intrusion interne). Dans ce cas, le test sera opéré sur le LAN (réseau interne de l'entreprise).

1.5 Qui le fait ?

Vous vous demandez sûrement qui peut ou qui est en charge de réaliser un test d'intrusion ? Et bien c'est un expert en cybersécurité ou encore appelé **pentesteur** !

Pour devenir pentesteur, il faut avoir une large maîtrise des systèmes et réseaux, car le monde de la sécurité est transversal. Il faut connaître les différents matériels et technologies sur le marché pour pouvoir comprendre et exploiter les vulnérabilités qui y sont présentes.

Ce cours vous permettra de réaliser votre premier test pour ainsi avoir un aperçu d'ensemble de la sécurité de vos infrastructures ou applications. Si vous souhaitez aller plus loin, n'hésitez pas à vous former au métier d'expert ou de pentesteur. C'est un profil très recherché par les entreprises, mais ces professionnels ont en général au moins 5 à 10 ans d'expérience.

Voilà, nous venons de voir ensemble ce qu'est un test d'intrusion et à quoi cela sert. Dans le prochain chapitre, vous allez découvrir les différents types d'attaques ou intrusions possibles sur votre infrastructure.

En résumé

- Un test d'intrusion est un test pour **vérifier** et **identifier** les types de **vulnérabilités** ou **d'attaques** d'un SI (infrastructure, application…).
- Il est plus rapide et efficace qu'un audit de sécurité. Il donne également des résultats plus pertinents qu'un scan de vulnérabilité.
- Les tests d'intrusions peuvent être faits depuis l'infrastructure elle-même ou via Internet.
- Les professionnels du domaine sont appelés des experts en cybersécurité expérimentés ou des **pentesteurs.**

Conduisez un test d'intrusion

2.1 Maîtrisez les différents types de tests

Dans ce chapitre, nous allons voir les différents types de tests d'intrusion qui existent et comment sélectionner le bon en fonction de votre besoin.

Il existe deux types de tests d'intrusion :

- Les tests d'intrusion **externe**
- Les tests d'intrusion **interne**

Voyons cela ensemble !

2.2 Les 2 types de tests d'intrusion

Externe

Sur ce type d'intrusion, l'attaquant ou le pentesteur dans notre cas, est placé sur **Internet.** Il est donc dans la situation ou un pirate tenterait de pénétrer dans l'entreprise à partir de l'extérieur. L'adresse IP publique de la connexion internet du pentesteur et l'adresse IP publique de la connexion internet de l'entreprise sont utilisées dans ce scénario.

Interne

À l'inverse, dans ce cas-là, le pentesteur est sur le réseau interne de l'entreprise. Il est dans la situation d'une personne malveillante interne.

Par exemple, cela peut être le cas d'un **prestataire qui a accès physiquement** au bureau de l'entreprise comme un technicien télécom, un électricien, etc. C'est également le cas d'un **employé malveillant,** par exemple pour de l'espionnage industriel ou par vengeance. L'employé peut également être **inconscient** des risques, et cliquer sur une pièce jointe infectée ou communiquer des identifiants. Enfin, on peut également imaginer **un pirate** ayant

la possibilité de s'introduire physiquement dans l'entreprise et de se retrouver dans un de ces scénarios.

Il y a donc des deux types de tests que nous réalisons, interne et externe, car ce sont les deux types de scénarios qui se produisent dans la vie réelle des entreprises.

2.3 Conditions du test

En fonction du niveau de connaissance du pentesteur, trois qualificatifs différents sont utilisés pour identifier les tests d'intrusion :

- La boîte **noire**
- La boîte **grise**
- La boîte **blanche**

Voyons cela dans le détail.

Boîte noire

Dans ce cas, le pentesteur n'a **aucune information** sur le réseau cible au début du test et ne connaît aucun nom d'utilisateur ni mot de passe.

Il s'agit dans un premier temps de rechercher des informations sures :

- L'entreprise,
- Les employés,
- Connaître la situation géographique,
- Les informations générales,
- Le fournisseur d'accès à Internet,
- Et toutes autres données pour rassembler un maximum d'informations qui pourraient aider à trouver des vulnérabilités.

Nous sommes là dans le scénario d'un pirate qui souhaiterait s'introduire dans une entreprise qu'il ne connaît pas.

Boîte grise

Le testeur possède un **nombre limité d'informations.** En général, lors de tests d'intrusion en mode boîte grise, le testeur dispose uniquement d'un couple identifiant / mot de passe que l'entreprise cible lui a fourni avant de démarrer la phase de test. Cela permet notamment de passer l'étape d'authentification, et de pouvoir approfondir le test à l'intérieur de l'application ou du système.

L'objectif de ce type de test est de se mettre dans la peau d'un « utilisateur normal » de l'entreprise cible.

Boîte blanche

Enfin, dans cette condition, le pentesteur peut être en possession de **nombreuses informations.** Parmi elles, les plus courantes sont :

- Les schémas d'architecture,
- Un compte utilisateur permettant de s'authentifier,
- Le code source de l'application,
- etc.

Dans ce cas, le pentesteur va rechercher les failles en étant le plus exhaustif possible. Dans ce scénario, la recherche est très approfondie et très complète.

L'objectif de ce type de test est de se mettre dans la peau d'un « administrateur système et réseau » de l'entreprise cible.

2.4 Choix du test

Le choix du test d'intrusion qui va être conduit et très important, car il faudra le déterminer en fonction de ce que le client veut tester. En fonction de la stratégie adoptée, les résultats sont différents. Il faut donc bien identifier ce que l'entreprise cible veut protéger et de quel type d'attaque elle veut se prémunir. De là, il faut déterminer le meilleur type de scan et les meilleures conditions de connaissance du pentesteur avant le début du test.

Quelques exemples

1. Vous êtes RSSI pour l'entreprise SECURITYFIRST. Vous êtes soucieux qu'un pirate sur Internet vole les données que vous hébergez. Dans ce cas, vous devrez privilégier un test de type externe basé sur la boîte noire car c'est le scénario qui se rapproche le plus de la menace pour laquelle vous voulez vous protéger.

2. Vous êtes RSSI dans une entreprise qui traverse une période de crise sociale avec grèves et licenciements. Vous vous interrogez sur les conséquences que pourrait avoir un collaborateur malveillant. Le choix le plus judicieux sera un test d'intrusion interne en boîte grise. Le pentesteur possédera alors un login et mot de passe pour accéder au système comme un utilisateur standard et vous pourrez identifier les vulnérabilités internes dans ce scénario.

En résumé

- Il existe deux types de tests d'intrusion : **interne** et **externe**
- Il y a trois conditions de test d'intrusion : boîte **blanche,** boîte **grise,** et boîte **noire.**
- En fonction des conditions de départ, le pentesteur possède un niveau d'information qui lui permet de plus ou moins approfondir le test.

- Le choix du type de test et des conditions de connaissance de départ est très important. Il doit être fait en fonction de ce que l'entreprise veut protéger et également en fonction du risque contre lequel elle se protège.

3. Découvrez les systèmes d'exploitation adaptés

Conduisez un test d'intrusion

Nous venons de découvrir les différents types de tests d'intrusion possibles. Dans ce chapitre, nous allons découvrir les systèmes d'exploitation et les outils à disposition du pentesteur pour la réalisation d'un test d'intrusion. Il y a 3 systèmes principaux :

- **Sur Linux**
- **Windows**
- **Mobile avec Android.**

Voyons cela de plus près.

3.1 : Kali Linux

Kali Linux est une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information. Cette distribution a pris la succession de Backtrack.

Kali est disponible en plusieurs versions :

- 32 ou 64 bits
- Live CD
- Images Vbox et VMWare
- Versions pour processeurs ARM (utilisables sur matériel type Raspberry Pi)

Toutes les versions sont disponibles en téléchargement gratuit sur le site officiel.

Cette distribution rassemble plus de 600 programmes pré installés comme :

- **Nmap** : Le plus célèbre scanner de ports libre distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant.
- **Wireshark** : Analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques
- **Metasploit** : programme open source qui fournit des informations sur les vulnérabilités de systèmes informatiques et les exploite.
- **Burp Suite** : application utilisé pour la sécurisation ou les tests d'intrusion des applications web.

C'est vraiment la boîte à outils principale d'un pentesteur. Nous allons d'ailleurs nous attarder plus longuement sur ce système d'exploitation un peu plus loin dans le cours.

3.2 : Windows

Le système d'exploitation de Microsoft Windows 7, 8 ou 10 peut également être utilisé. Dans la grande majorité des cas, une version équivalente des outils de Kali Linux est disponible en version Windows. C'est évidemment le cas pour les plus connus d'entre eux :

- NMAP

- PuTTY
- Metasploit Framework
- Burp Suite
- OWASP Zed Attack Proxy
- Nessus
- John the Ripper

Étant donné que des versions similaires et en open source gratuit existent sur Kali Linux, nous n'utilisons pas de système d'exploitation Microsoft dans ce cours.

3.3 : Android

Les outils sur plateforme mobile sont parfois très pratiques quand on a besoin de tester de manière itinérante. Des outils très performants et très bien conçus sont disponibles pour l'utilisation sur Android :

- zANTI
- FaceNiff
- AndroRAT
- cSploit

Sachant que les outils installés sur Kali Linux couvrent les fonctionnalités de ses applications Android, nous ne les verrons pas dans ce cours.

En résumé

- La distribution la plus adaptée pour les tests d'intrusion est **Kali Linux.**
- Les principaux outils utilisés par les pentesteurs sont souvent disponibles sur les 3 plateformes Windows, Linux, et Android.

4. Configurez votre environnement LAB

5. Préparez votre pentest

6. Quiz : Préparez votre test d'intrusion