1

Tests d'intrusion

Introduction

Un test d'intrusion peut être vu comme une tentative légale et autorisée de localiser des systèmes informatiques et de réussir à y pénétrer dans le but d'améliorer leur niveau de sécurité. La procédure comprend la recherche de vulnérabilités ainsi que la mise en place d'attaques en tant que preuves de concept (POC, *proof of concept*) afin de démontrer la réalité des vulnérabilités. Un test d'intrusion correct se termine toujours par des recommandations précises qui permettent de traiter et de corriger les problèmes découverts. En résumé, la procédure est utilisée pour aider à sécuriser les ordinateurs et les réseaux afin de les prémunir contre les attaques futures. L'idée générale est de trouver les problèmes de sécurité en utilisant les mêmes outils et techniques que les pirates. Ils seront ensuite corrigés avant qu'un véritable pirate ne les exploite.

Les tests d'intrusion sont parfois appelés pentest, hacking, hacking éthique, hacking white hat ou sécurité offensive.

Il est important de comprendre les différences entre test d'intrusion et évaluation de la vulnérabilité. De nombreuses personnes (y compris les fournisseurs) impliquées dans la sécurité les emploient à tort de façon interchangeable. L'évaluation de la vulnérabilité consiste à examiner les services et les systèmes à la recherche de problèmes de sécurité éventuels, tandis qu'un test d'intrusion réalise des exploits et des attaques POC réels afin de démontrer l'existence d'un problème de sécurité. Les tests d'intrusion vont au-delà de l'évaluation de la vulnérabilité en simulant les actions d'un pirate et en plaçant de véritables attaques. Dans cet ouvrage, l'évaluation de la vulnérabilité constitue l'une des étapes qui permettent d'aller au bout d'un test d'intrusion.

Préparer le terrain

Pour avoir une vision globale, il est indispensable de comprendre les différents acteurs et situations que l'on rencontre dans le monde du hacking et des tests d'intrusion. Nous allons commencer par tracer les grandes lignes du sujet. Sachez que les explications suivantes constituent une simplification excessive. Toutefois, elles devraient vous aider à voir les différences entre les divers groupes de personnes impliqués.

Nous allons nous placer dans l'univers de *Star Wars*, avec les deux côtés de la "force" : les Jedi et les Sith (les bons et les méchants). Chaque camp dispose d'une puissance incroyable. Le premier l'utilise pour protéger et servir, l'autre, à des fins personnelles.

Apprendre le hacking peut se comparer à apprendre à utiliser la force (enfin, j'imagine). Plus vous progressez dans votre apprentissage, plus votre puissance augmente. À un moment donné, vous devez décider si vous allez l'exploiter pour faire le bien ou le mal. Des images de l'épisode 1 de *Star Wars* montrent Anakin en jeune garçon. Si vous regardez attentivement son ombre, vous verrez qu'elle correspond à celle de Darth Vader (vous trouverez ces images en effectuant une recherche sur les termes "Anakin Darth Vader ombre"). Il est important de comprendre pourquoi ces images ont un intérêt. En tant que petit garçon, Anakin n'aspire pas à devenir Darth Vader, mais cela se produira néanmoins.

Nous pouvons supposer à juste titre que les personnes qui entrent dans le monde du hacking sont peu nombreuses à vouloir devenir des superméchants. Le problème est que le chemin vers le côté obscur est en pente glissante. Cependant, si vous voulez être grand, être respecté par vos pairs et faire partie des forces de sécurité, vous devez vous engager à utiliser vos pouvoirs dans le but de protéger et de servir. Ajouter un crime à votre casier revient à acheter un aller simple pour une autre profession. Même s'il existe actuellement une pénurie d'experts en sécurité, peu d'employeurs sont prêts à prendre le risque d'embaucher une personne qui a commis des crimes informatiques. Les règles et les contraintes deviennent encore plus strictes si vous envisagez un poste qui requiert des habilitations de sécurité.

Dans le monde des tests d'intrusion, il est fréquent d'entendre les termes *white hat* et *black hat* pour décrire les Jedi et les Sith. Tout au long de cet ouvrage, les termes *white hat*, "hacker éthique" et "testeur d'intrusion" seront employés sans distinction pour représenter les Jedi (les bons garçons). Les Sith seront désignés sous les termes *black hat*, *cracker*, "pirate" ou "assaillant malveillant" (les méchants garçons).

Il est important de noter que les hackers éthiques et les pirates réalisent les mêmes activités en employant quasiment les mêmes outils. Dans pratiquement toutes les situations, un hacker éthique doit agir et réfléchir comme un véritable assaillant malveillant. Plus le test d'intrusion est proche d'une attaque réelle, plus le résultat présentera un intérêt pour le client qui l'a commandé.

Vous l'aurez remarqué, dans le paragraphe précédent nous avons mentionné "dans pratiquement toutes les situations". Bien que les testeurs d'intrusion mettent en place les mêmes actions avec les mêmes outils, il existe tout un monde de différences entre les deux côtés. Elles peuvent se réduire à trois points essentiels : autorisation, motivation et intention. Ils ne sont pas exhaustifs, mais ils seront utiles pour déterminer si une activité entre ou non dans le cadre éthique.

L'autorisation est la première façon de différencier les white hat et les black hat. Elle consiste à obtenir un accord pour mener des tests et des attaques. Lorsque c'est fait, le testeur d'intrusion et l'entreprise auditée doivent définir l'étendue du test. Cela comprend des informations précises sur les ressources et les systèmes impliqués dans le test. Elle définit explicitement les cibles autorisées. Il est important que les deux côtés comprennent parfaitement l'accord et l'étendue du test d'intrusion. Les white hat doivent toujours respecter l'autorisation qui leur a été accordée et rester dans les limites du test. Ces contraintes ne s'appliquent pas aux black hat.

INFO

Il est essentiel de définir clairement et de comprendre parfaitement l'étendue du test. Celle-ci établit de façon formelle les règles d'engagement du testeur d'intrusion et du client. Elle doit comprendre une liste des cibles et préciser les systèmes ou les attaques que le client refuse d'inclure dans le test. Elle doit être rédigée sur un papier et signée par le personnel autorisé, à la fois de l'équipe de test et du client. Il peut arriver qu'elle ait besoin d'être amendée pendant le test d'intrusion. Dans ce cas, soyez certain de l'actualiser et de la signer de nouveau avant de procéder à des tests sur les nouvelles cibles.

La deuxième façon de différencier un hacker éthique et un hacker malveillant concerne leur motivation. Si l'assaillant est motivé par des fins personnelles, y compris un profit au travers d'extorsion ou d'autres méthodes illégales auprès de la victime, par une volonté de revanche, un besoin de renommée ou autre, il doit être considéré comme un black hat. *A contrario*, si les actions de l'assaillant ont été autorisées et si son objectif est d'aider l'entreprise à améliorer sa sécurité, il doit être considéré comme un white hat. Par ailleurs, un hacker malveillant peut en général consacrer à l'attaque de l'entreprise tout le temps nécessaire. Dans la plupart des cas, un testeur d'intrusion n'aura au mieux que quelques semaines. En fonction de la durée laissée à la réalisation du test d'intrusion, un white hat pourra ne pas découvrir les vulnérabilités élaborées qui demandent plus de temps.

Enfin, si l'intention est de proposer à l'entreprise une simulation d'attaque réaliste afin qu'elle puisse améliorer sa sécurité en corrigeant les vulnérabilités découvertes, l'assaillant doit être considéré comme un white hat. Il est également important de comprendre que les découvertes effectuées lors d'un test d'intrusion doivent rester confidentielles. Jamais un hacker éthique ne partagera les informations sensibles découvertes au cours d'un test d'intrusion avec une personne autre que son client.

En revanche, si l'intention est d'exploiter des informations à des fins personnelles, l'assaillant doit être considéré comme un black hat.

Il est également important de comprendre que tous les tests d'intrusion ne sont pas menés de la même manière ni n'ont le même objectif. Les tests d'intrusion par boîte blanche, ou "transparents", sont très rigoureux et complets. L'objectif d'un tel test est d'examiner le système ou le réseau cible dans ses moindres recoins. Il permet d'évaluer la sécurité globale de l'entreprise. Puisque la discrétion n'est pas de mise, nombre des outils présentés dans cet ouvrage peuvent être exécutés en mode verbeux. En privilégiant la rigueur à la discrétion, le testeur d'intrusion est souvent en mesure de découvrir un plus grand nombre de vulnérabilités. Cependant, cette approche a pour inconvénient d'être moins fidèle à la façon de travailler des pirates expérimentés. Par ailleurs, elle n'offre pas à l'entreprise la possibilité de tester ses systèmes de réponse aux incidents et d'alerte précoce. N'oubliez pas que le testeur a l'intention d'être non pas discret mais rigoureux.

Les tests d'intrusion par boîte noire, ou "cachés", se fondent sur une stratégie radicalement différente. Un tel test constitue une simulation beaucoup plus réaliste d'une attaque menée par un pirate expérimenté pour obtenir un accès au système ou au réseau cible. Il met de côté la rigueur et la possibilité de détecter de multiples vulnérabilités pour privilégier la discrétion et la précision. Dans ce cas, le testeur se contentera de trouver une seule vulnérabilité qu'il pourra exploiter. L'avantage de ce type de test est qu'il s'approche plus des attaques réelles. Peu de pirates effectueront aujourd'hui un scan des 65 535 ports d'une cible. Cette opération est plutôt bruyante et sera à coup sûr repérée par les pare-feu et les systèmes de détection d'intrusion. Les hackers malveillants intelligents seront beaucoup plus discrets. Ils pourront scanner un seul port ou interroger un seul service afin de trouver une manière de compromettre la cible et de se l'approprier. Les tests par boîte noire ont également l'avantage de donner à l'entreprise l'occasion de tester ses procédures de réponse aux incidents et de déterminer si ses défenses sont capables de détecter une attaque ciblée et de l'arrêter.

Introduction à Kali et à BackTrack Linux

Il y a quelques années, une discussion ouverte sur les techniques de hacking et leur enseignement aurait fait l'objet d'un certain tabou. Les temps ont heureusement changé et la valeur d'une sécurité offensive est à présent comprise. Elle est aujourd'hui adoptée par les entreprises, quels que soient leur taille et leur secteur d'activité. Les gouvernements la prennent également au sérieux. Ils sont nombreux à avoir annoncé sa mise en place.

Un test d'intrusion doit jouer un rôle important dans la sécurité globale de l'entreprise. À l'instar des politiques, de l'évaluation du risque, de la planification

de la continuité d'activité et du plan de reprise d'activité, qui font désormais partie intégrante d'une stratégie de sécurité, il faut y ajouter les tests d'intrusion. Ils permettent de voir l'entreprise au travers des yeux de l'ennemi. Ils peuvent mener à des découvertes surprenantes, en donnant le temps de corriger les systèmes avant qu'un pirate n'entre en scène.

Lorsque l'on souhaite apprendre le hacking, on a aujourd'hui à sa disposition de nombreux outils. Non seulement ils sont prêts à l'emploi, mais nombre d'entre eux font également preuve d'une grande stabilité car ils bénéficient de plusieurs années de développement. Pour certains d'entre vous, le plus important sera peut-être que la plupart sont disponibles gratuitement. Les outils présentés dans cet ouvrage sont tous gratuits.

S'il est facile de savoir qu'un outil est gratuit, il peut en aller tout autrement pour le trouver, le compiler et l'installer avec tous les autres utilitaires requis pour mener à bien un test d'intrusion même de base. Si la procédure se révèle relativement simple sur un système d'exploitation Linux moderne, elle reste un tantinet intimidante pour les novices. En général, les gens sont plus intéressés par apprendre à utiliser les outils qu'à explorer Internet pour les trouver et ensuite les installer.

Pour être franc, vous devrez apprendre à compiler et à installer manuellement les logiciels sur une machine Linux. Tout au moins, vous devez vous familiariser avec l'outil `apt-get` (ou équivalent).

Aller plus loin

APT (*Advanced Package Tool*) est un système de gestion de paquetages. Il permet d'installer, d'actualiser et de supprimer rapidement et facilement des logiciels à partir de la ligne de commande. Outre sa simplicité, il présente l'intérêt de résoudre automatiquement les problèmes de dépendance. Autrement dit, si le paquetage en cours d'installation a besoin d'un logiciel supplémentaire, APT va se charger de localiser et d'installer automatiquement celui-ci. Cette possibilité constitue une nette amélioration par rapport aux outils plus anciens.

L'installation d'un logiciel à l'aide d'APT est très simple. Par exemple, supposons que nous souhaitions installer l'outil Paros Proxy sur notre machine Linux locale. Paros peut servir, entre autres, à évaluer la sécurité des applications web. Nous examinerons les proxies au Chapitre 6, mais, pour le moment, concentrons-nous sur l'installation de l'outil plutôt que sur son utilisation. Si nous connaissons le nom du paquetage, il suffit d'exécuter `apt-get install` depuis la ligne de commande en lui précisant ce nom. Il est toujours préférable d'exécuter `apt-get update` avant d'installer un logiciel car nous sommes ainsi certains de disposer de la dernière version. Dans le cas de Paros, il suffit de lancer les commandes suivantes :

```
apt-get update

apt-get install paros
```

Avant que l'installation du paquetage ne débute, la quantité d'espace disque requise est affichée et APT demande si nous souhaitons poursuivre. Dans l'affirmative, nous saisissons **o** et appuyons sur la touche `Entrée`. Lorsque l'installation du programme est terminée, nous revenons à l'invite `#`. Nous pouvons alors lancer Paros en exécutant la commande suivante depuis la console :

```
paros
```

Pour le moment, fermons simplement le programme Paros, car notre objectif était non pas de lancer ou d'utiliser Paros, mais de montrer l'installation d'un nouveau logiciel.

Si vous ne souhaitez pas passer par la ligne de commande, sachez qu'il existe plusieurs applications graphiques qui s'interfacent avec APT. La plus répandue se nomme Aptitude. D'autres gestionnaires de paquetage sont disponibles, mais ils sortent du cadre de cet ouvrage.

APT nous oblige à connaître le nom exact du logiciel à installer avant d'exécuter la commande `apt-get install`. Si nous ne sommes pas certains du nom ou ne connaissons pas son orthographe exacte, la commande `apt-cache search` va nous être utile. Elle affiche tous les paquetages ou outils qui correspondent au critère de recherche et en donne une courte description. Grâce à `apt-cache search`, nous pouvons arriver rapidement au nom du paquetage que nous recherchons. Par exemple, pour obtenir le nom officiel donné au paquetage de Paros, nous commençons par exécuter la commande suivante :

```
apt-cache search paros
```

Dans les noms et les descriptions obtenus, nous devrions trouver le paquetage recherché. Il suffira ensuite d'exécuter la commande `apt-get install` appropriée.

Si vous choisissez la distribution Kali Linux, Paros sera déjà installé. Même dans ce cas, la commande `apt-get install` reste un outil puissant pour l'installation des logiciels.

Des connaissances de base sur Linux vous seront profitables et vous en tirerez de nombreux bénéfices sur le long terme. Dans le cadre de cet ouvrage, nous ne supposons aucune expérience préalable avec Linux. Toutefois, pour votre propre bien, n'hésitez pas à vous engager à devenir plus tard un gourou Linux. Inscrivez-vous à des formations, lisez des livres ou découvrez par vous-même. Vous nous en remercierez. Si vous vous intéressez aux tests d'intrusion ou au hacking, vous n'avez d'autre choix que de maîtriser Linux.

Heureusement, le monde de la sécurité profite d'une communauté très active et très généreuse. Plusieurs organismes ont travaillé inlassablement à la création de distributions Linux adaptées à la sécurité. Une distribution est de façon générale une variante, un type ou une marque dérivé de Linux.

Parmi les distributions les plus connues adaptées aux tests d'intrusion, il existe BackTrack. Elle représente votre guichet unique pour l'apprentissage du hacking et la mise en place de tests d'intrusion. BackTrack Linux me fait penser à cette scène

du premier épisode de *Matrix* où Tank demande à Neo : "Alors, de quoi t'as besoin, à part d'un miracle ?" Neo réplique alors : "Des armes, un maximum d'armes." À ce moment du film, de nombreux râteliers d'armes apparaissent. Tous les types d'armes imaginables sont proposés à Neo et à Trinity : des pistolets, des fusils, des fusils de chasse, des semi-automatiques, des automatiques, des explosifs et d'autres encore. Lorsqu'ils démarrent BackTrack ou Kali, les débutants se trouvent dans la même situation : des outils, un maximum d'outils.

BackTrack Linux et Kali Linux sont le rêve réalisé de tout hacker. Ces distributions ont été conçues pour les testeurs d'intrusion. Elles viennent avec des centaines d'outils de sécurité déjà installés, configurés et prêts à l'emploi. Qui plus est, elles sont gratuites ! Vous pouvez en télécharger un exemplaire à l'adresse **http://www.backtrack-linux.org/downloads/**.

INFO

Au printemps 2013, les membres d'Offensive Security ont sorti une version redéfinie et revue de BackTrack appelée "Kali Linux". Elle est également disponible gratuitement et est fournie avec de nombreux outils pour l'audit de la sécurité. Vous pouvez la télécharger à l'adresse **http://www.kali.org**.

Si vous débutez dans les tests d'intrusion et le hacking, les différences entre BackTrack et Kali risquent d'être confuses. Toutefois, pour apprendre les bases et expérimenter les exemples de cet ouvrage, les deux distributions feront l'affaire. Kali Linux sera parfois plus facile à utiliser que BackTrack car tous les outils sont installés de façon à pouvoir être exécutés depuis n'importe quel répertoire. Il suffit d'ouvrir une fenêtre de terminal et de saisir le nom de l'outil, avec les options souhaitées. Si vous utilisez BackTrack, il vous faudra souvent aller dans le répertoire qui correspond à un outil avant de pouvoir lancer celui-ci.

Si ces explications vous laissent un tantinet perplexe, ne vous inquiétez pas. Nous y reviendrons progressivement dans les chapitres suivants. Pour le moment, vous devez simplement choisir entre Kali et BackTrack. Quelle que soit votre décision, elle sera de toute façon bonne.

En vous rendant sur ce site, vous aurez le choix entre un fichier `.iso` et une image VMware. Si vous choisissez le fichier `.iso`, vous devrez le graver sur un DVD. Il vous suffira de placer ce DVD amorçable dans le lecteur et de redémarrer l'ordinateur. Dans certains cas, vous devrez d'abord modifier l'ordre de démarrage dans le BIOS afin de donner la priorité au lecteur optique.

Si vous choisissez de télécharger l'image VMware, vous aurez besoin d'un logiciel capable de l'ouvrir et de la déployer ou de l'exécuter. Par chance, il existe plusieurs outils pour y parvenir. En fonction de vos préférences, vous pouvez opter pour VMware Player de VMware, VirtualBox d'Oracle ou Virtual PC de Microsoft.

Si ces propositions ne vous conviennent pas, il existe d'autres logiciels capables d'exécuter une image VMware. Prenez simplement celui qui vous correspond.

Les trois solutions de virtualisation mentionnées sont disponibles gratuitement et vous permettront d'exécuter des images de machines virtuelles. Vous devez simplement décider de la version à employer. Dans cet ouvrage, nous utilisons principalement l'image VMware de BackTrack et l'application VMware Player. Au moment de l'écriture de ces lignes, VMware Player est disponible à l'adresse **http://www.vmware.com/fr/products/player/**.

Si vous ne savez pas quelle option choisir, nous vous conseillons d'opter pour la solution VMware. Non seulement cette technologie vaut la peine d'être maîtrisée, mais les machines virtuelles vous permettront également de mettre en place un laboratoire complet pour les tests d'intrusion en utilisant une seule machine. S'il s'agit d'un ordinateur portable, vous pourrez mener vos expériences à partir d'un laboratoire de voyage, à tout moment et en tout lieu.

Si vous décidez de lancer BackTrack à partir d'un DVD amorçable, vous verrez apparaître un menu initial que vous devez examiner attentivement car il propose plusieurs articles différents. Si vous rencontrez des difficultés à faire démarrer BackTrack, choisissez BackTrack Debug - Safe Mode. Le menu propose plusieurs autres options, mais elles sortent du cadre de cet ouvrage. Pour sélectionner une option, servez-vous des touches de direction puis validez en appuyant sur `Entrée`. La Figure 1.1 montre un exemple d'écran de démarrage de Kali (en haut) et de BackTrack (en bas).

Figure 1.1

Les options du menu de démarrage de Kali et de BackTrack.

Kali Linux fonctionne de façon comparable. Vous devez choisir entre le téléchargement d'une image ISO (à graver sur un DVD) et celui d'une image VMware déjà configurée. Quelle que soit la version sélectionnée, vous pouvez simplement accepter l'option par défaut (en appuyant sur la touche `Entrée`), lorsque vous arrivez au menu GRUB de Kali Linux.

BackTrack ou Kali n'est pas indispensable à la lecture de cet ouvrage ni à l'apprentissage des bases du hacking. N'importe quelle version de Linux fera l'affaire. Toutefois, en utilisant ces distributions, tous les outils nécessaires sont déjà installés. Si vous optez pour une autre version de Linux, vous devrez commencer par les installer avant de lire les chapitres. Par ailleurs, puisque cet ouvrage se focalise sur les bases, la version de BackTrack ou de Kali n'a pas d'importance. Tous les outils que nous présenterons et emploierons dans cet ouvrage sont disponibles dans toutes les versions.

Machine d'attaque

Que vous exécutiez BackTrack ou Kali à partir d'une machine virtuelle ou d'un DVD amorçable, le chargement du système initial se termine par une invite d'ouverture de session. Le nom d'utilisateur par défaut est `root`, avec le mot de passe `toor`.

Ce nom d'utilisateur et ce mot de passe par défaut sont utilisés depuis la première version de BackTrack ; ils seront certainement conservés dans les futures versions. Après que vous avez entré ces informations, vous devez voir apparaître l'invite `root@bt:~#`. Bien que vous puissiez exécuter la plupart des outils décrits dans cet ouvrage directement à partir de la console, les débutants préféreront souvent utiliser le système X Window. Pour démarrer cet environnement graphique, saisissez la commande suivante à l'invite `root@bt~#` :

```
startx
```

Appuyez sur la touche `Entrée` pour lancer le chargement de X Window. Cet environnement doit être vaguement familier à la plupart des utilisateurs. Au terme de son chargement, vous obtenez un bureau, des icônes, une barre de tâches et une zone de notification. Comme dans Microsoft Windows, vous pouvez interagir avec ces éléments en déplaçant le pointeur de la souris et en cliquant sur l'objet concerné. Si vous avez adopté Kali Linux, l'ouverture de session réussie avec le nom d'utilisateur et le mot de passe par défaut déclenche automatiquement le chargement de l'environnement graphique de bureau GNOME.

Les programmes utilisés dans cet ouvrage seront principalement exécutés depuis la console. Avec la plupart des distributions Linux, vous pouvez ouvrir celle-ci en utilisant le raccourci clavier `Ctrl+Alt+T`. En général, les systèmes proposent également une icône qui représente une boîte noire avec les caractères `>_` à l'intérieur.

Cette icône se trouve dans la barre des tâches ou le menu du système. La Figure 1.2 illustre cette icône dans GNOME.

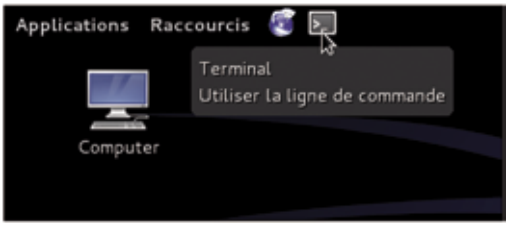

Figure 1.2

L'icône qui permet d'ouvrir une fenêtre de terminal.

Contrairement à Microsoft Windows et à de nombreuses distributions Linux modernes, certaines versions de BackTrack viennent avec un réseau non configuré. Il s'agit d'un choix de conception. En tant que testeurs d'intrusion, nous essayons souvent de rester discrets ou invisibles. Un ordinateur qui démarre en envoyant immédiatement des requêtes réseau pour obtenir un serveur DHCP et une adresse IP revient à crier : "Coucou, coucou, je suis là !!!" Pour éviter ce problème, les interfaces réseau de l'ordinateur BackTrack sont désactivées par défaut.

Pour activer le réseau, la solution la plus simple passe par la console. Ouvrez une fenêtre de terminal en cliquant sur l'icône indiquée à la Figure 1.2 ou, si vous utilisez BackTrack, appuyez sur `Ctrl+Alt+T`. Ensuite, dans la console, exécutez la commande suivante :

```
ifconfig –a
```

Elle énumère les interfaces disponibles sur la machine. En général, vous verrez au moins les interfaces `eth0` et `lo`. L'interface `lo` correspond à la boucle de retour. L'interface `eth0` désigne la première carte Ethernet. En fonction du matériel, vous verrez des interfaces supplémentaires ou des numéros d'interface différents. Dans le cas d'une machine virtuelle BackTrack, l'interface principale sera généralement `eth0`.

Pour activer la carte réseau, saisissez la commande suivante :

```
ifconfig eth0 up
```

`ifconfig` est une commande Linux qui signifie "je souhaite configurer une interface réseau". Nous l'avons déjà indiqué, `eth0` correspond au premier dispositif réseau du système (n'oubliez pas que les ordinateurs comptent souvent à partir de 0, non de 1). Le mot clé `up` signifie que l'interface doit être activée. Autrement dit, la commande signifie "je veux activer la première interface".

Puisque l'interface est à présent active, nous devons obtenir une adresse IP. Pour cela, il existe deux façons de procéder. La première consiste à affecter manuellement l'adresse en l'indiquant à la fin de la commande précédente. Par exemple, pour attribuer l'adresse IP 192.168.1.23 à la carte réseau, nous saisissons la commande suivante :

```
ifconfig eth0 up 192.168.1.23
```

L'ordinateur possède alors une adresse IP, mais nous devons préciser une passerelle et un serveur DNS (*Domain Name System*). Une simple recherche Google des termes "configuration interface réseau linux" donnera des résultats qui expliquent comment procéder. Pour vérifier la validité de votre configuration, exécutez la commande suivante dans une fenêtre de terminal :

```
ifconfig -a
```

Les paramètres actuels des interfaces réseau s'affichent alors. Puisque ce guide est destiné aux débutants, et pour des questions de simplicité, nous supposons que la discrétion n'est pas un aspect important, tout au moins pour le moment. Dans ce cas, la solution la plus simple pour obtenir une adresse passe par DHCP. Pour cela, il suffit d'exécuter la commande suivante :

```
dhclient
```

Notez que `dhclient` tentera d'attribuer automatiquement une adresse IP à la carte réseau et de configurer tous les éléments requis, notamment les informations du DNS de la passerelle. Si vous exécutez Kali ou BackTrack Linux dans VMware Player, le logiciel VMware jouera le rôle de serveur DHCP.

Que l'adresse soit obtenue de manière dynamique avec DHCP ou qu'elle soit affectée de manière statique, la machine doit à présent avoir sa propre adresse IP. Dans le cas de Kali Linux, le réseau est préconfiguré. Cependant, en cas de difficultés, la section précédente pourra se révéler utile.

Enfin, nous devons apprendre à éteindre BackTrack ou Kali. Comme souvent sous Linux, il existe plusieurs manières d'y parvenir. L'une des plus simples consiste à exécuter la commande suivante dans une fenêtre de terminal :

```
poweroff
```

ATTENTION

Il est toujours préférable d'éteindre ou de redémarrer la machine d'attaque lorsque vous avez achevé un test d'intrusion. Vous pouvez également exécuter `shutdown` ou `shutdown now` pour arrêter votre machine. Cette bonne habitude évite de laisser par inadvertance un outil en cours d'exécution ou d'envoyer du trafic sur votre réseau alors que vous n'êtes pas devant l'ordinateur.

Vous pouvez également remplacer `poweroff` par la commande `reboot` afin de redémarrer le système au lieu de l'arrêter.

Avant d'aller plus loin, prenez le temps de revoir les étapes décrites jusqu'à présent et de les mettre en pratique, notamment :

- démarrer et arrêter BackTrack ou Kali ;
- ouvrir une session avec le nom d'utilisateur et le mot de passe par défaut ;
- lancer l'environnement graphique X Window ;
- afficher toutes les interfaces réseau de l'ordinateur ;
- activer l'interface réseau souhaitée ;
- attribuer manuellement une adresse IP ;
- examiner l'adresse IP attribuée manuellement ;
- attribuer une adresse IP à l'aide de DHCP ;
- examiner l'adresse IP attribuée dynamiquement ;
- redémarrer la machine depuis l'interface en ligne de commande ;
- arrêter la machine depuis l'interface en ligne de commande.

Mettre en place un laboratoire de hacking

Un hacker éthique doit disposer d'un endroit où pratiquer et découvrir. La plupart des débutants se demandent comment apprendre à utiliser les outils de hacking sans violer la loi ni attaquer des cibles interdites. En général, la solution consiste à créer son propre "laboratoire de hacking". Il s'agit d'un environnement isolé du trafic réseau, et les attaques n'ont aucune chance de sortir ni d'atteindre des cibles interdites ou accidentelles. Dans cet environnement, vous avez toute liberté pour étudier les différents outils et techniques sans craindre que du trafic ou des attaques ne sortent de votre réseau. Le laboratoire comprend au moins deux machines : celle de l'assaillant et celle de la victime. Il est également possible de déployer simultanément plusieurs victimes afin de simuler un réseau plus réaliste.

Il est important que l'utilisation et la configuration du laboratoire de hacking soient correctes car il représente l'une des meilleures façons de se former à ces techniques par l'expérimentation. L'apprentissage et la maîtrise des bases des tests d'intrusion se passent de la même manière.