Leçon 3 – Principales techniques d'attaques et logiciels malveillants dans le réseau

Équipe Pédagogique Réseau Informatique@ UVCI
2018

Juin 2018
Version 1.0

Table des matières

Objectifs

A la fin de cette leçon, vous serez capable de :

- Identifier les techniques d'intrusion
- Identifier les techniques Déni de service

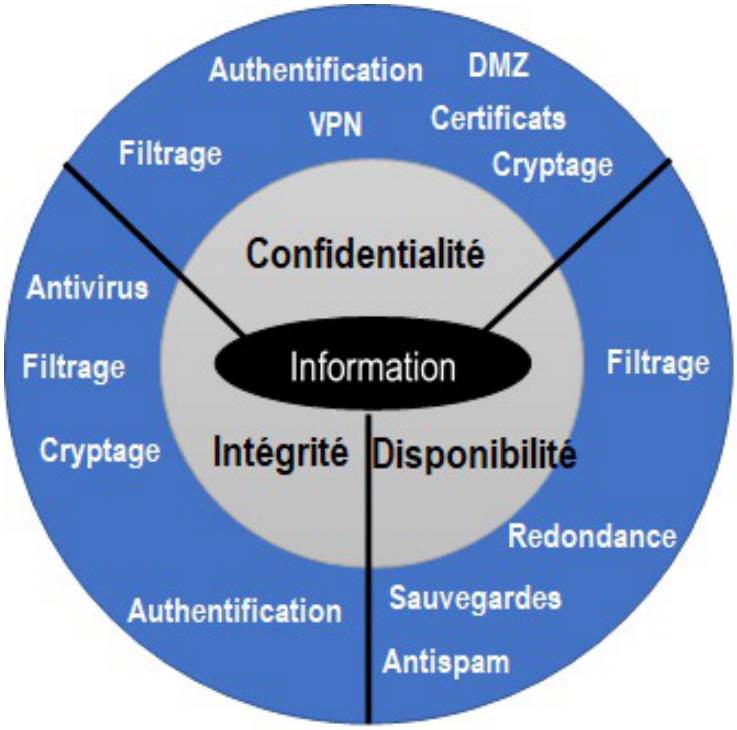
Introduction

Les attaques visant à pirater un système en réseau dans le but de récupérer des informations sensibles ou d'altérer les services existent à tous les niveaux. Les points d'entrée les plus vulnérables sont les *navigateurs* (lien malveillant) et les *clients de messagerie* (faux lien intégré et pièces jointes). Les services récents sont également concernés : les nouvelles menaces impliquent *les blogs, le partage des fichiers multimédia et les sites des réseaux sociaux.*

Quelle que soit leur place ou leur rôle dans une architecture de réseau local ou sur Internet, les systèmes (serveurs, PC, routeurs, systèmes de stockage...) sont donc tous vulnérables à un certain niveau :

- émergence en permanence de nouveaux usages et de nouvelles technologies, et donc de nouvelles vulnérabilités (réseaux sociaux, peer to peer, messagerie instantanée, réseaux sans fil, smartphone connectés en WiFi ou en 3G, téléphonie sur IP, stockage sur clé USB...) ;
- les politiques de sécurité sont complexes car elles doivent opérer simultanément sur tous les éléments d'une architecture réseau et pour différents types d'utilisateurs (firewall sur les routeurs d'accès et sur les serveurs d'extrémité, cryptage de certains fichiers, droits accrus pour les administrateurs sur certaines ressources...) ;
- les politiques de sécurité mises en place sont basées sur des jugements humains qui doivent de plus être révisés en permanence pour s'adapter aux nouvelles attaques ;
- la sécurisation est coûteuse en moyens, en temps et surtout en ressources humaines.

Pour limiter les risques, la sécurité informatiques visent trois objectifs principaux présentés dans la figure ci-dessous.



Objectifs de sécurité

Les attaques peuvent être classées en deux grandes catégories : les *techniques d'intrusion* dont l'objectif principal est de s'introduire sur un réseau pour découvrir ou modifier des données et les *dénis de service*

qui ont pour but d'empêcher une application ou un service de fonctionner normalement. Cette deuxième catégorie agit donc sur la disponibilité de l'information tandis que la première concerne essen-tiellement la confidentialité et l'intégrité. Une autre classification existe : elle distingue les *attaques passives* basées sur l'écoute et l'interception qui concernent seulement la confidentialité et les *attaques actives* qui altèrent également les données ou les services et concernent donc la disponibilité et l'intégrité.

Techniques d'intrusion

Objectifs

Identifier les techniques d'intrusion

Ces techniques peuvent être classées suivant le niveau d'intervention :

- les accès physiques vont du vol de disque dur ou de portable à l'écoute du trafic sur le réseau (sniffing) ;
- l'ingénierie sociale (social engineering) permet de retrouver ou de récupérer directement des couples identifiant/mot de passe en envoyant par exemple des messages falsifiés (phishing) ;
- l'interception de communications permet l'usurpation d'identité, le vol de session (session hijacking), le détournement ou l'altération de messages (spoofing) ;
- les intrusions sur le réseau comprennent le balayage de ports (port scan), l'élévation de privilèges (passage du mode utilisateur au mode administrateur) et surtout les logiciels malveillants ou malwares (virus, vers et chevaux de Troie).

Les principales attaques de ce type sont détaillées dans les paragraphes suivants.

1. Le sniffing

Sur la plupart des réseaux, les trames sont diffusées sur tout le support (câble Ethernet, transmission radio WiFi...). En fonctionnement normal, seul le destinataire reconnaît son adresse (adresse MAC destination sur un réseau Ethernet) et lit le message. La carte Ethernet ou WiFi d'un PC peut être reprogrammée pour lire tous les messages qui traversent le réseau (promiscious mode). La limite dans ce cas est le dispositif d'interconnexion utilisé sur le LAN ou le segment de LAN (hub, switch, point d'accès WiFi, routeur...). Les hackers utilisent des « sniffers » ou analyseurs réseau qui scannent tous les messages qui circulent sur le réseau et recherchent ainsi des identités et des mots de passe.

2. Le « craquage » de mot de passe

Le hacker utilise un dictionnaire de mots et de noms propres construit à partir d'informations personnelles et privées qui ont été collectées (social engineering). Ces chaînes de caractère sont essayées une à une à l'aide de programmes spécifiques qui peuvent tester des milliers de mots de passe à la seconde. Ce type d'attaque est souvent nommé attaque par force brute car le mot de passe est deviné grâce à des milliers d'essais successifs à partir d'un dictionnaire, et non pas retrouvé à l'aide d'un programme capable de décrypter une chaîne de caractères.

3. Le phishing

Ce néologisme anglais provient de la contraction de fishing (pêcher) et de phreaking (pirater le réseau téléphonique). Il s'agit de conduire des internautes à divulguer des informations confidentielles, notamment bancaires, en usant d'un hameçon fait de mensonge et de contrefaçon électronique (identité visuelle d'un site connu, en-têtes, logo...). Le cas le plus classique est celui d'un mail usurpant l'identité de votre banque et contenant un lien vers un faux site où l'on vous demandera de confirmer votre numéro de carte visa par exemple.

4. Le spoofing

Le spoofing consiste à faire passer pour, à usurper .

Les falsifications peuvent intervenir sur tous types de serveur, en particulier sur les serveurs DNS et web.

1) Le DNS spoofing

Le pirate utilise les faiblesses du protocole DNS et de son implémentation sur les serveurs de noms de domaine pour rediriger des internautes vers des sites falsifiés. Le but du pirate est donc de faire correspondre l'adresse IP d'une machine qu'il contrôle à l'URL réel d'une machine publique.

2) Le web spoofing

Le web spoofing est une version élaborée de l'IP spoofing : il s'agit de remplacer un site par une version pirate du même site. Cette technique est notamment utilisée dans la dernière étape du phishing. La falsification se déroule en plusieurs temps :

- amener la victime à entrer dans le faux site web (grâce à l'utilisation du DNS spoofing par exemple) ;
- intercepter les requêtes HTTP ;
- récupérer les vraies pages web et modifier ces pages ;
- envoyer de fausses pages à la victime.

5. Les malwares

Le terme « virus » est souvent employé abusivement pour désigner toutes sortes de logiciels malveillants (les virus ont été historiquement les premiers malwares).

1) Virus

Un virus est un programme qui se propage à l'aide d'autres programmes ou de fichiers. Il est souvent simple et facile à détecter à partir de son code (signature) mais néanmoins efficace lorsqu'il se propage plus rapidement que la mise à jour des anti-virus. Un virus passe le plus souvent par la messagerie et est activé par la sélection d'un lien sur le message ou l'ouverture d'un fichier attaché. Les conséquences de l'exécution du virus peuvent aller de la simple modification des paramètres d'une application (page par défaut du navigateur) ou de la base de registre du système (exécution automatique d'un programme commercial à chaque démarrage) à l'effacement de données ou de fichiers essentiels au système d'exploitation.

2) Ver

Un ver (worm) est un programme plus sophistiqué capable de se propager et de s'auto-reproduire sans l'utilisation d'un programme quelconque (d'un vecteur) ni d'une action par une personne. La particularité des vers ne réside pas forcément dans leur capacité immédiate de nuire mais dans leur facilité pour se propager grâce par exemple aux listes de contacts présentes sur les PC ou les smartphones.

3) cheval de Troie

Un cheval de Troie (troyan) est un programme caché dans un autre programme qui s'exécute au démarrage du programme « hôte ». Il permet donc de s'introduire sur le système à l'insu de la victime (ouverture d'une « porte dérobée » ou backdoor) ; le cheval de Troie devient alors autonome et peut agir comme un virus en infectant des données ou des programmes.

6. Exercice

[Solution n°1 p 13]

Exercice : 1

Lequel des éléments suivants permet de faire un backdoor caché pour accéder aux postes de travail sur Internet ?

- ◯ a)Cheval de troie
- ◯ b)Bombe logique
- ◯ c)Firmware
- ◯ d)Ver

Exercice : 2

Quelle technique permet de collecter des identifiants et mots de passe ?

- ☐ A) Sniffing
- ☐ B) SYN Flood
- ☐ C) Ingénierie sociale
- ☐ D) DoS

Exercice : 3

Parmi ces attaques, lesquelles réalisent une attaque par intrusion ?

- ☐ A) phishing
- ☐ B) web flooding
- ☐ C) web spoofing
- ☐ D) DoS
- ☐ E) attaque par force brute

Exercice : 4

Donner dans la liste ci-dessous les objectifs d'une attaque par intrusion :

- ☐ A) découvrir les données
- ☐ B) empêcher une application de fonctionner
- ☐ C) modifier des données
- ☐ D) Arrêter le fonctionnement d'un service

Déni de service

II

Objectifs

Identifier les techniques Déni de service

Ce type d'attaque nommé en anglais Dénial of Service ou DoS empêche par saturation un service de fonctionner correctement sur une machine.

1. SYN Flood

Cette attaque consiste à inonder (flooding) la cible à l'aide de demande successive d'ouverture de connexion TCP. Lors d'une ouverture normale (figure a) :

- le premier segment TCP est transmis par le client avec le bit SYN à 1 pour demander l'ouverture ;
- le serveur répond avec dans son segment TCP les bits SYN et ACK à 1;
- le client demandeur conclut la phase avec le bit ACK à 1.

Les abus interviennent au moment où le serveur a renvoyé un accusé de réception (SYN ACK) au client mais n'a pas reçu le « ACK » du client. C'est alors une connexion semi-ouverte et l'agresseur peut saturer la structure de données du serveur victime en créant un maximum de connexions partiellement ouvertes. Le client autorisé ne pourra alors plus ouvrir de connexion.

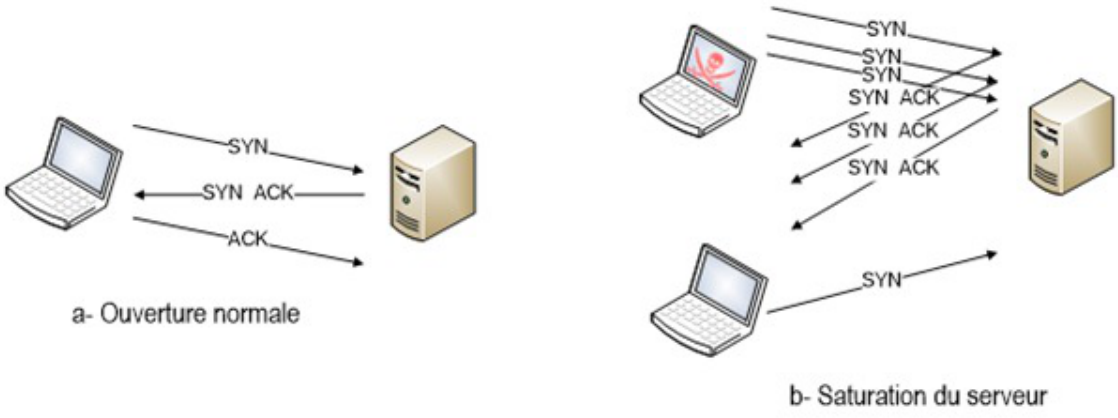


Figure 2 : Principe du SYN Flood

2. Ping flooding

cette attaque consiste à envoyer un flux maximal de « ping » vers une cible. • Attaque Ping of Death : le principe est d'envoyer un paquet ICMP avec une quantité de données supérieure à la taille maximale d'un paquet IP. Si la cible n'est pas adaptée à gérer ce type de paquet, il peut se produire un crash.

3. Smurfing

Elle consiste à envoyer un ping en diffusion sur un réseau (A) avec une adresse IP source correspondant à celle de la cible (B). Le flux entre le port ping de la cible (B) et du réseau (A) sera multiplié par le nombre de machines sur le réseau (A), conduisant à une saturation de la bande passante du réseau (A) et du système de traitement des paquets de (B).

4. UDP Flood

L'attaquant envoie un grand nombre de requêtes UDP sur une machine. Le trafic UDP étant prioritaire sur le trafic TCP, ce type d'attaque peut vite troubler et saturer le trafic transitant sur le réseau.

5. L'attaque ARP

Elle consiste à s'attribuer l'adresse IP de la machine cible, c'est-à-dire à faire correspondre son adresse IP à l'adresse MAC de la machine pirate dans les tables ARP des machines du réseau. Pour cela il suffit en fait d'envoyer régulièrement des trames ARP REPLY en diffusion, contenant l'adresse IP cible et la fausse adresse MAC. Cela a pour effet de modifier les tables dynamiques de toutes les machines du réseau. Celles-ci enverront donc leurs trames Ethernet à la machine pirate tout en croyant communiquer avec la cible.

6. DDOS

Le déni de service distribué ou DDoS (Distributed Déniai of Service) a les mêmes effets que le DOS traditionnel excepté que ce n'est plus une seule machine qui attaque les autres mais une multitude de machines nommées zombies contrôlées par un maître unique. L'attaque se déroule en plusieurs étapes (figure 3) :

- recherche sur Internet d'un maximum de machines vulnérables qui deviendront des complices involontaires, des « zombies ». Les réseaux de zombies (botnet en anglais) ainsi formés sont une ressource précieuse pour les hackers ;
- installation sur ces machines de programmes dormants (daemons) et suppression des traces éventuelles (logs). Les daemons sont basés sur les attaques DOS classiques (paquets UDP multiples, SYN Flood, buffer ovetflow...) ;
- activation du dispositif à l'heure et au jour programmé.

Parmi les attaques DDOS très populaires, on connaît l'attaque sur les sites Yahoo, CNN, Amen et eBay qui ont subi une inondation de leur réseau.

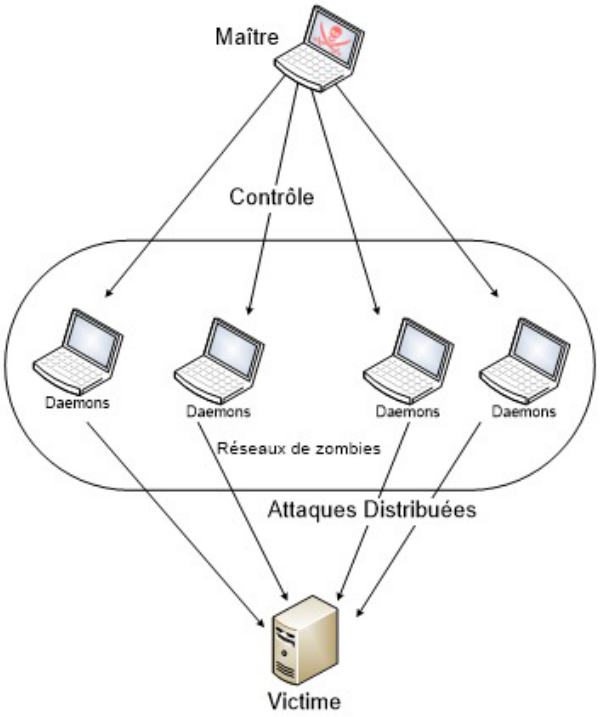


Figure 3 : Principe du DDoS

7. Exercice

[Solution n°2 p 13]

Exercice : Question 1

Lequel des éléments suivants est utilisé pour effectuer un déni de service (DoS) ?

- ◯ A)Rootkit
- ◯ B)Bombe logique
- ◯ C)Botnet
- ◯ D)Port redirection

Exercice : Question 2

L'objectif d'une attaque par déni de service (attaque DoS) est :

- ◯ A) Voler des informations secrètes
- ◯ B) de bloquer un serveur ou d'empêcher l'accès à un site Web
- ◯ C) Modifier les données

Exercice : Question 3

Parmi ces attaques, lesquelles réalisent un déni de service ?

- ☐ A) SYN flooding
- ☐ IP spoofing
- ☐ C) Ping of Death
- ☐ D) DNS spoofing

Solutions des exercices

> Solution n°1

Exercice p. 8

1

- (•) a)Cheval de troie
- ( ) b)Bombe logique
- ( ) c)Firmware
- ( ) d)Ver

2

- [x] A) Sniffing
- [ ] B) SYN Flood
- [x] C) Ingénierie sociale
- [ ] D) DoS

3

- [x] A) phishing
- [ ] B) web flooding
- [x] C) web spoofing
- [ ] D) DoS
- [x] E) attaque par force brute

4

- [x] A) découvrir les données
- [ ] B) empêcher une application de fonctionner
- [x] C) modifier des données
- [ ] D) Arrêter le fonctionnement d'un service

Exercice p. 12

> Solution n°2

Question 1

- ○ A)Rootkit
- ○ B)Bombe logique
- ◉ C)Botnet

  Ensemble de machines compromises.
- ○ D)Port redirection

Question 2

- ○ A) Voler des informations secrètes
- ◉ B) de bloquer un serveur ou d'empêcher l'accès à un site Web
- ○ C) Modifier les données

Question 3

- ☑ A) SYN flooding
- ☐ IP spoofing
- ☑ C) Ping of Death
- ☐ D) DNS spoofing

Bibliographie

1. Stéphane Lohier, Dominique Présent ; Réseaux et transmissions, 6è édition, DUNOD 2016

2. Danièle Dromard, Dominique Seret ; Architecture des réseaux, collection Synthex, 2009 Pearson Education France, ISBN : 978-2-7440-7385-4