sécurité réseau

Les menaces

Sommaire

- **Les risques**
- **Les attaques**
- **Références**

Dispositions légales

- Le chapitre III du Code pénal relatif aux atteintes des systèmes de traitement automatisé de données (on y trouve 7 articles):
  - **Article 323-1:** le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni **d'un an d'emprisonnement** et de **100 000 F d'amende**. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 200 000 F d'amende**.**
  - **Article 323-2 :** le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de **trois ans d'emprisonnement** et de **300 000 F d'amende**.
  - **Article 323-3 :** le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de **trois ans d'emprisonnement** et de **300 000 F d'amende**.

Dispositions légales (1)

- Le 323-1 concerne l'intrusion en elle-même. La peine est majorée lorsque cette intrusion induit une altération des données.
- Le 323-2 porte sur des nuisances faites au réseau (virus, mail bombing, dénis de services …).
- Le 323-3 punit les modifications faites volontairement aux données présentes sur le réseau.
- …

Les risques

- Qui protéger ?
  - **Les données**
    - Confidentialité : protection contre le risque de divulgation ;
    - Intégrité : protection contre l'altération ou perte d'informations ;
    - Disponibilité : protection contre la dégradation ;
  - **Les ressources**
    - Serveur, disques, réseau,…
    - Protection contre le refus de service (Denis de service)
  - **L'entreprise et les personnes**
    - Usurpation d'identité, …
- **Diverses origines** : fraude, sabotage matériel, indiscrétion, détournement d'informations, piratage,…

Les attaques

- **Consistent à trouver un point d'entrée (ou une faille) sur un système informatique, le plus souvent à partir d'un accès distant**.
- **Intrusion**
  - La plus connue et la plus pratiquée,
  - Problèmes d'authentification.
- **Dénis de service**
  - Empêcher l'utilisation des machines, du réseau,…
  - Empêcher, par *saturation* ou *inondation*, un service de fonctionner.
- **Vols d'informations**
  - **Attaques passives**: écoute du réseau (*Sniffing*)
  - **Attaques actives** : interrogation par envoie de paquets sur la machine cible pour obtenir des informations telles que: les @IP des machines, la liste des services disponibles, l'état des ports (ouvert, fermé ou filtré),…

Description d'une attaque

- **Attaque** :
  - Recherche systématique d'informations
    - DNS, whois, moteurs de recherche, …
  - Recherche de vulnérabilités connues
    - Services ouvert (SMTP, HTTP, etc),
    - type de système d'exploitation, versions
  - Tentative d'intrusion par exploitation des vulnérabilités
  - Systèmes d'écoutes du réseau
  - Tentative de déni de service
- **Intrusion** :
  - Prise de contrôle partielle ou totale du système distant

Recherche d'information (1)

- **Requêtes indirectes** :
  - Principe : apprendre sur la cible sans la contacter directement
  - Interrogation des bases whois : BD des renseignements fournis lors de l'enregistrement d'un nom de domaine
    - **whois unicaen.fr**
  - En particulier la base whois de RIPE pour découvrir par exemple les classes des @IP allouées
    - **whois 193.55.130.2**

Recherche d'information (2)

- **Requêtes directes** :
  - Principe : lancer des sondes en direction de la cible pour apprendre des informations plus importantes.
  - Interrogation des DNS avec dig.
  - Découverte du réseau :
    - **traceroute** : **obtenir @IP d'un routeur d'accès aux machines cibles;**
    - **balayage des @IP avec nmap** : **Ping scan (nmap –sP)**
    - **hping** : **Port scan et leur états.**
  - Découverte des services ouverts sur une machine (**scans furtifs**):
    - **Scan en connexion demi-ouverture (syn-scan) : nmap –sS**
  - Découverte des versions logicielles : telnet n°_port_du_service permet de récupérer les **bannières des serveurs.**

Social engineering

- **Désigne des techniques d'intrusion basées sur les points faibles des personnes en lien avec le SI.**
- **Principe** :
  - Faire croire aux utilisateurs du système que leur mot de passe est demandé d'urgence par l'administrateur (usurpation d'identité par e-mail)
  - Deviner le mot de passe d'un utilisateur par des informations personnelles (prénom et date de naissance des enfants, …)

Sniffing des mots de passes

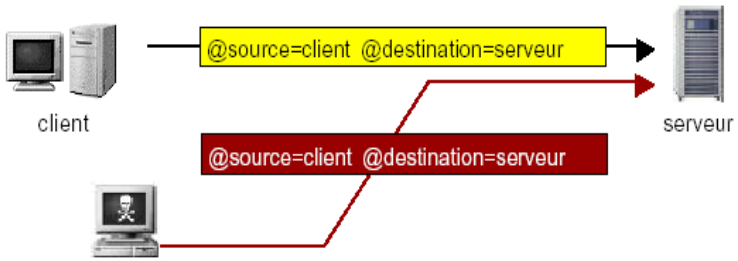
- **Principe** :
  - Chaque paquet transmis sur le réseau peut être lu par n'importe quel machine sur le réseau (broadcasting)
  - En fonctionnement normal, seul le destinataire lit le message. Une carte réseau peut donc être programmée pour lire tous les messages qui traversent le réseau.
  - Utilisation de **sniffers** pour scanner tous les segments circulant sur le réseau, rechercher les identités et des mots de passes (**dsniff**).
  - Une parade pour déjouer le sniffing est de "**tunneler** " (ou **encrypter**) toutes les transactions, avec IPSec ou des VPN.

Crack de mot de passe

- **Principe** :
  - L'attaque consiste à encrypter différentes combinaisons de caractères et de comparer cette forme encryptée à celle du mot de passe à découvrir.
  - **L'attaque par dictionnaire** : basée sur un dictionnaire de mots et de nom propres. Un programme les encrypte un par un avec un algorithme d'encryptage adéquat et les compare au mot de passe encrypté.
    - Crack4.1 utilise un dictionnaire de 50000 mots
  - **Le brute forcing** : en cas d'échec de l'attaque par dictionnaire, générer des mots de passe avec une suite aléatoire de caractères, les encrypter et les comparer au mot de passe à découvrir.

IP Spoofing (Kevin Mitnick)

- **Principe** : Usurper l'adresse IP en envoyant un paquet avec une fausse adresse IP source



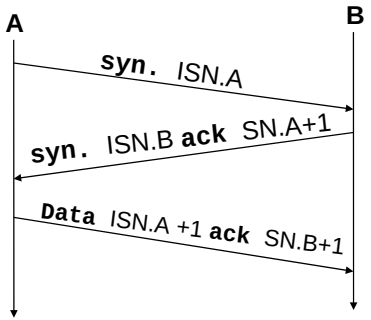
  - Il est impossible de trouver la véritable source du paquet
  - Utilisé dans de nombreuses attaques :
    - Dénis de service
    - Pour profiter d'une relation de confiance entre deux machines (authentification basée sur l'@ IP)

IP spoofing avec TCP

- Les application que nous voulons pirater (rlogin, rsh, ..) utilisent TCP
- TCP est un protocole à fenêtre.
- Il utilise des numéros de séquence pour suivre les données envoyées et reçues.
- Pour éviter de réutiliser les mêmes numéros de séquence, un numéro de initial aléatoire (ISN) est choisi pour chaque nouvelle connexion.

IP spoofing avec TCP

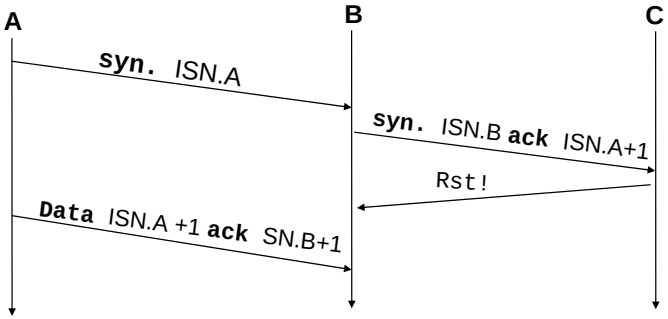
- TCP rappel : établissement de la connexion (3-way handshake)



Difficulté du spoofing TCP

- A envoie ses paquets en utilisant l'@ de C

→ Il doit deviner l'ISN que B va proposer à C!



- C, qui n'a rien demandé à personne, envoie un reset à B

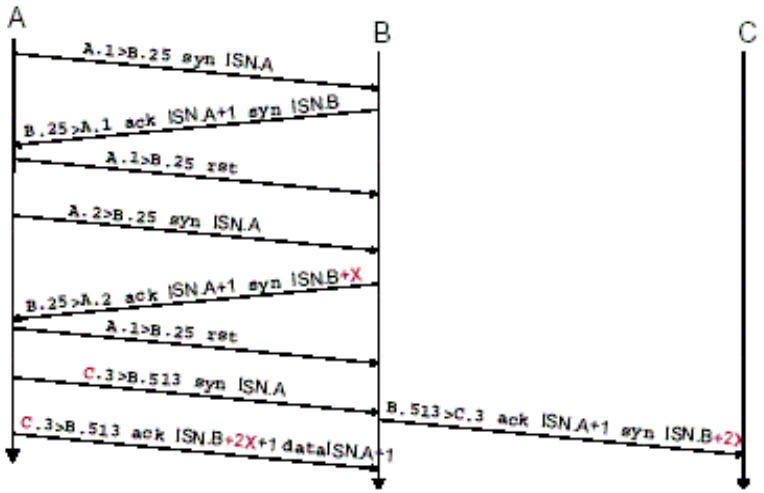
→ Le pirate doit empêcher C de répondre!

Génération de l'ISN TCP

- Le standard (RFC 793) indique qu'il faut incrémenter l'ISN de 1 toutes les 4 microsecondes

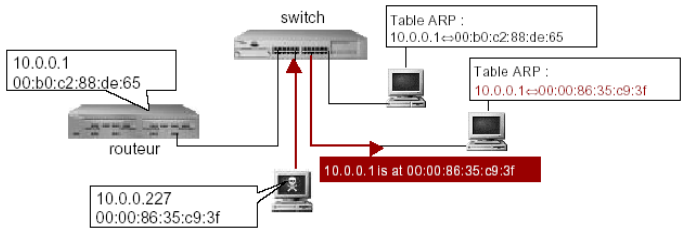
- Procédé du pirate:
  - Il ouvre quelques connexions réelles (par exemple SMTP) pour obtenir un ISN actuel et des échantillons d'incréments
  - Il lance sa connexion forgée en utilisant le dernier ISN plus un incrément déduit de ces échantillons
    - Il peut lancer de multiples connexions forgées avec des incréments variés en espérant avoir juste au moins une fois.

TCP spoofing : Exemple



ARP-Poisoning

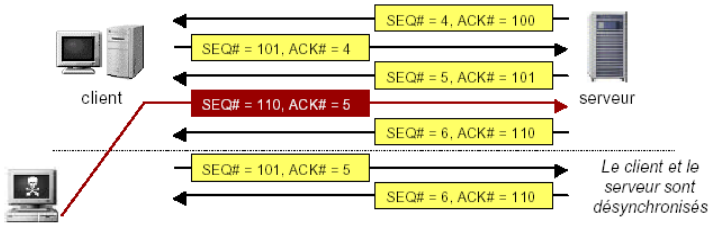
- **Principe** : rediriger le trafic réseau d'une ou plusieurs machines vers la machine de l'attaquant, en corrompant le cache ARP du récepteur.
  - L'attaquant envoie un message de réponse ARP avec son adresse physique correspondant à l'@ IP du récepteur.



  - Solution pour déjouer l'attaque :
    - mettre en place un serveur DHCP avec une liste "fermée" de correspondance entre @ MAC et @ IP.
    - Utilisation d'un mécanisme d'authentification.

TCP session Hijacking

- **Principe** : Voler une session IP en prenant le contrôle d'une communication au milieu de celle-ci :
  - Permet de profiter de l'authentification en début de session TCP



  - L'attaquant crée un **état de désynchronisation**, faisant croire au client qu'il a perdu la connexion et stoppera ses échanges avec le serveur. Mais si l'attaquant envoie les bons numéros de séquences au serveur, il récupèrera la connexion pour lui.

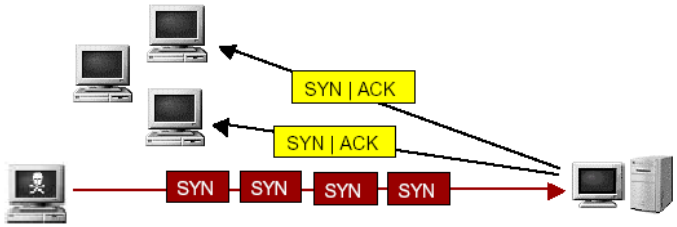
Les dénis de service

- Attaques aboutissant à l'indisponibilité du service ou de la machine visée

- Deux types :
  - **Dénis de service applicatifs**
    - Exploitation des vulnérabilités d'une application : débordement debuffer (*buffer overflow*) par exemple
    - Indisponibilité par saturation des ressources ou par crash de l'application
  - **Dénis de service réseaux**
    - exploitation des faiblesses d'un protocole

SYN-flooding

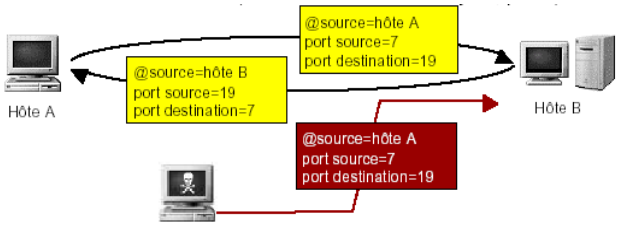
- **Principe** : Envoyer massivement des demandes de connexion (**flag SYN à 1**) vers la machine cible avec des adresses sources aléatoires.
- La machine cible renvoie les SYN-ACK en réponse à chaque SYN reçu



- Aucun ACK n'est renvoyé pour établir la connexion : connexions semi-ouvertes consomment des ressources mémoire ;
- Au bout d'un moment, la machine cible est saturée et ne peut plus accepter de connexions ;

UDP-flooding

- **Principe** : générer une grande quantité de paquets UDP (**UDP paquet storm**) à destination d'une machine ou entre deux machines.
- Utilise le fait qu'UDP ne possède pas de mécanisme de contrôle de congestion.
- Entraîne une congestion du réseau et une saturation des ressources des hôtes victimes.



- Exemple le plus connu : *Chargen Denial of Service Attack*
  - Faire communiquer le service chargen (génération de caractères, port 19) d'une machine avec le service echo (rémission des données reçues, port 7) d'une autre.

Smurf

- **Principe** : Noyer la cible à l'aide d'amplificateurs de trafic
- Cas typique: ICMP echo-request (ping)
- Le pirate envoie un paquet ping avec l'adresse de la cible comme source
- La machine "pingée" envoie sa réponse à la cible
- Si le pirate envoie le paquet à une adresse broadcast, ce sont toutes les machines du réseau qui vont répondre à la cible

L’abus de scripts Web

- Les sites web interactifs (e-commerce, etc.) sont réalisés avec des scripts.
- Des formulaires sont écrits en HTML.
- Le client les remplit et clique sur un bouton.
- Le bouton génère la requête d'une URL garnie des paramètres donnés dans le formulaire.
- La requête appelle un script qui fait une opération avec les paramètres et rend une page web en résultat.
- Exemple connu d’attaque : SQL injection

SQL injection

- Exemple connu d’attaque : SQL injection
  - Un formulaire d'un site de e-commerce demandait un nom et un mot de passe
  - Il construisait une chaîne de caractères représentant une requête SQL du type :

```
query$ =‘SELECT nom, pw FROM database
 WHERE nom = " ‘+nom$+‘ " AND pw =" ‘+password$+‘ " ‘
```

  - La requête était exécutée, si le résultat n'était pas nul, l'authentification était ok

```
Result = SQLquery(query$);
IF Result <> 0 then ok ….
```


Problème

- Pour nom = " OR TRUE OR nom = " et pw =bidon

```
query$ =‘SELECT nom, pw FROM database
        WHERE nom = " " OR TRUE OR nom = " "
        AND  pw = " bidon " ‘
```

- La requête va toujours retourner un résultat <>0 et l'utilisateur est accepté!

Références

- http://www.hsc.fr/
- Transparents DESS DCISS 2002/2003 (*bulfone@icp.inpg.fr)*
- Les systèmes pare-feu, polycopie LT La Salle Avignon