Méthodologie d’une attaque réseau

[sommaire]

1. ## Objectifs

- Savoir la méthodologie généralement retenue par les pirates pour s’introduire dans un système informatique

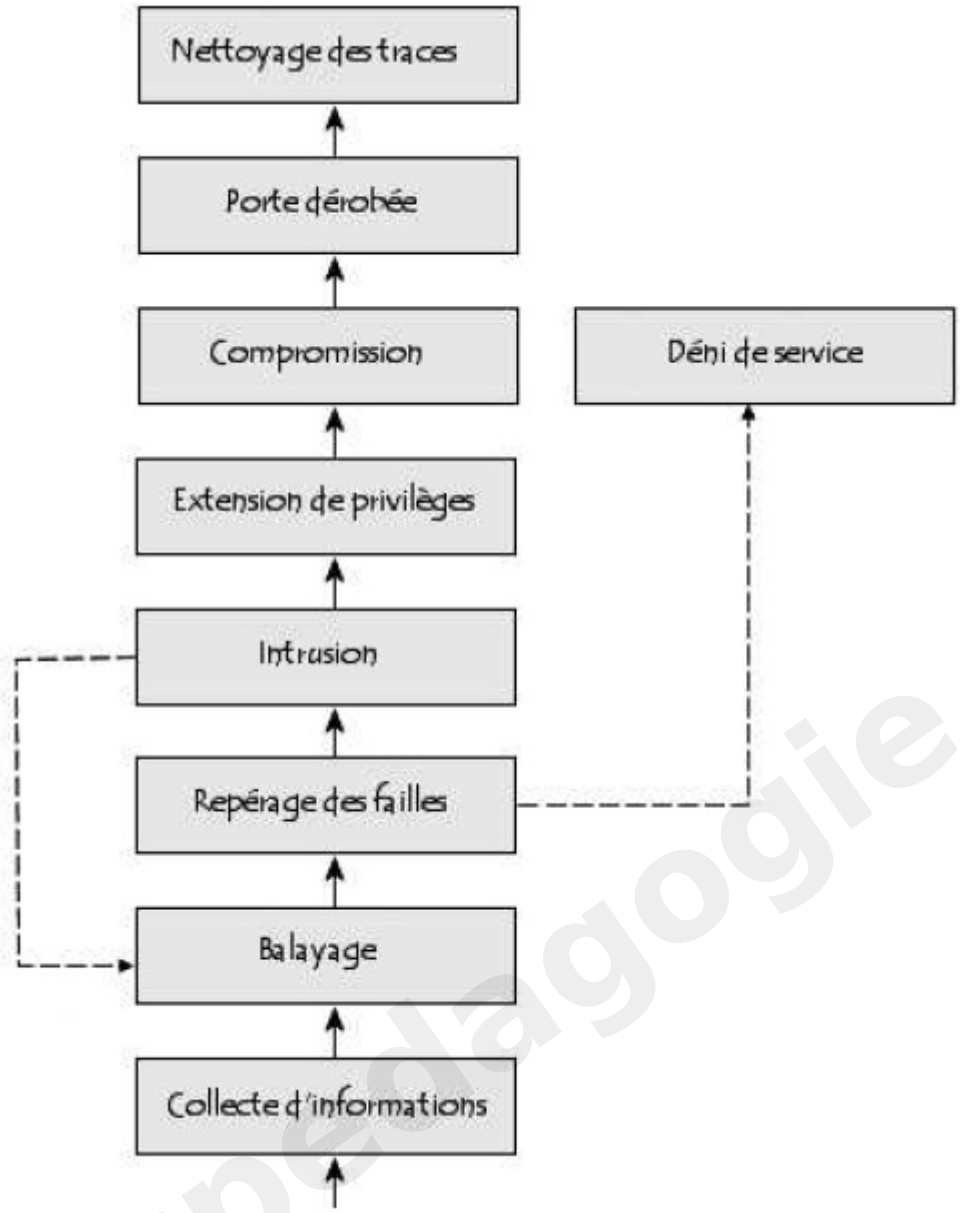
- ## Présentation

  - Ce tutoriel a pour vocation d’expliquer la méthodologie généralement retenue par les pirates pour s’introduire dans un système informatique ainsi que les principales techniques utilisées.
  - Il ne vise en aucun cas à expliquer comment compromettre un système mais à comprendre la façon dont il peut l’être afin de mieux pouvoir s’en prémunir.
  - En effet, la meilleure façon de protéger son système est de procéder de la même manière que les pirates afin d’être en mesure d’identifier les vulnérabilités du système. Ainsi cette section ne donne aucune précision sur la manière dont les failles sont exploitées, mais explique comment les déceler et les corriger.

- ## Méthodologie globale

  - Les hackers recherchent dans un premier temps des failles, dans les protocoles, les systèmes d'exploitations, les applications ou même le personnel d'une organisation! Note: vulnérabilité = trou de sécurité (security hole).
  - Pour pouvoir mettre en œuvre un exploit (exploiter une vulnérabilité), la première étape du hacker consiste à récupérer le maximum d'informations sur l'architecture du réseau et sur les systèmes d'exploitations et applications fonctionnant sur celui-ci.
  - Le schéma suivant récapitule la méthodologie complète.

apcpedagogie.com



- Les **hackers** ayant l'intention de s'introduire dans les systèmes informatiques recherchent dans un premier temps des failles, c'est-à-dire des vulnérabilités nuisibles à la sécurité du système, dans les protocoles, les systèmes d'exploitations, les applications ou même le personnel d'une organisation ! Les termes de vulnérabilité, de brèche ou en langage plus familier de trou de sécurité (security hole) sont également utilisés pour désigner les failles de sécurité.
- Pour pouvoir mettre en œuvre un exploit (il s'agit du terme technique signifiant « exploiter une vulnérabilité »), la première étape du hacker consiste à récupérer le maximum d'informations sur l'architecture du réseau et sur les systèmes d'exploitation et les applications fonctionnant sur celui-ci.
- La plupart des attaques sont l'œuvre de script kiddies essayant bêtement des exploits trouvés sur Internet, sans aucune connaissance du système, ni des risques liés à leur acte.

apcpedagogie.com

- Une fois que le hacker a établi une cartographie du système, il est en mesure de mettre en application des exploits relatifs aux versions des applications qu’il a recensées.
- Un premier accès à une machine lui permettra d’étendre son action afin de récupérer d’autres informations, et éventuellement d’étendre ses privilèges sur la machine.
- Lorsqu’un accès administrateur (le terme root est généralement utilisé) est obtenu, on parle alors de compromission de la machine (ou plus exactement root compromise), car les fichiers systèmes sont susceptibles d’avoir été modifiés. Le hacker possède alors le plus haut niveau de droit sur la machine.
- S'il s'agit d’un pirate, la dernière étape consiste à effacer ses traces, afin d’éviter tout soupçon de la part de l'administrateur du réseau compromis et conserver ainsi le plus longtemps possible le contrôle des machines compromises.

Déroulement d’une intrusion

- **La récupération d'informations sur le système**
  - **Préalable à toute attaque**.
    - Rassembler le maximum d'informations sur le réseau cible.
    - L'obtention d'informations sur l'adressage du réseau visé, généralement qualifiée de prise d'empreinte, est un préalable à toute attaque. Elle consiste à rassembler le maximum d'informations:
      - adressage IP,
      - noms de domaine,
      - protocoles de réseau,
      - services activés,
      - architecture des serveurs, etc.
  - **Consultation de bases publiques**
    - En connaissant l'adresse IP publique d'une des machines du réseau (ou le nom de domaine de l'organisation), un pirate est potentiellement capable de connaître l'adressage du réseau tout entier. Il suffit de consulter les bases publiques d'attribution des adresses IP et des noms de domaine:
      - http://www.ina.net
      - http://www.ripe.net pour l'Europe
      - http://www.arin.net pour les Etats-Unis
    - Note: La simple consultation des moteurs de recherche permet parfois de rassembler des informations sur la structure d'une entreprise.
  - **Consultation de moteurs de recherche**

apcpedagogie.com

- Informations sur la structure d'une entreprise, le nom de ses principaux produits, voire le nom de certains personnels.

- **Balayage du réseau**

  - Lorsque la topologie du réseau est connue par le pirate, il peut le scanner, c'est-à-dire déterminer à l'aide d'un outil logiciel quelles sont les adresses IP actives sur le réseau, les ports ouverts correspondant à des services accessibles, et le système d'exploitation utilisé par ces serveurs.
  - L'un des outils les plus connus pour scanner un réseau est Nmap. Cet outil agit en envoyant des paquets TCP et/ou UDP à un ensemble de machines sur un réseau, puis il analyse les réponses.

- **Le repérage des failles**

  - Il existe des scanneurs de vulnérabilité permettant aux administrateurs de soumettre leur réseau à des tests d'intrusion afin de constater si certaines applications possèdent des failles de sécurité.
  - Les deux principaux scanneurs de failles sont :
    - Nessus (http://www.tenable.com)
    - SAINT (http://www.saintcorporation.com)

- **Intrusion**

  - Pour pouvoir s'introduire dans le réseau, le pirate a besoin d'accéder à des comptes valides sur les machines qu'il a recensées. Pour ce faire, plusieurs méthodes sont utilisées par les pirates :
    - L'ingénierie sociale, c'est-à-dire en contactant directement certains utilisateurs du réseau (par mail ou par téléphone) afin de leur soutirer des informations concernant leur identifiant de connexion et leur mot de passe. Ceci est généralement fait en se faisant passer pour l'administrateur réseau.
    - La consultation de l'annuaire ou bien des services de messagerie ou de partage de fichiers, permettant de trouver des noms d'utilisateurs valides.
    - Les attaques par force brute (brute force cracking), consistant à essayer de façon automatique différents mots de passe sur une liste de compte (par exemple l'identifiant, éventuellement suivi d'un chiffre, ou bien le mot de passe password, ou passwd, etc).

apcpedagogie.com

- **Extension de privilèges**
  - Lorsque le pirate a obtenu un ou plusieurs accès sur le réseau en se logeant sur un ou plusieurs comptes peu protégés, celui-ci va chercher à augmenter ses privilèges en obtenant l'accès root .
  - Dès qu'un accès root a été obtenu sur une machine, l'attaquant a la possibilité d'examiner le réseau à la recherche d'informations supplémentaires.
  - Il lui est ainsi possible d'installer un sniffeur, c'est-à-dire un logiciel capable d'écouter le trafic réseau en provenance ou à destination des machines situées sur le même brin.
  - Grâce à cette technique, le pirate peut espérer récupérer les couples identifiants/mots de passe lui permettant d'accéder à des comptes possédant des privilèges étendus sur d'autres machines du réseau afin d'être à même de contrôler une plus grande partie du réseau.
  - Les serveurs NIS (Network Information Service) présents sur un réseau sont également des cibles de choix pour les pirates car ils regorgent d'informations sur le réseau et ses utilisateurs.
- **Compromission**
  - Grâce aux étapes précédentes, le pirate a pu dresser une cartographie complète du réseau, des machines s'y trouvant, de leurs failles et possède un accès root sur au moins l'une d'entre-elles. Il lui est alors possible d'étendre encore son action en exploitant les relations d'approbation existant entre les différentes machines.
  - Cette technique d'usurpation d'identité, appelée spoofing, permet au pirate de pénétrer des réseaux privilégiés auxquels la machine compromise a accès.
- **Porte dérobée**
  - Lorsqu'un pirate a réussi à infiltrer un réseau d'entreprise et à compromettre une machine, il peut arriver qu'il souhaite pouvoir revenir. Pour ce faire celui-ci va installer une application afin de créer artificiellement une faille de sécurité, on parle alors de porte dérobée.
- **Nettoyage des traces**
  - Lorsque l'intrus a obtenu un niveau de maîtrise suffisant sur le réseau, il lui reste à effacer les traces de son passage en supprimant les fichiers qu'il a créés et en

apcpedagogie.com

nettoyant les fichiers de logs des machines dans lesquelles il s'est introduit.

- Il existe des logiciels, appelés “kits racine” (rootkits) permettant de remplacer les outils d'administration du système par des versions modifiées afin de masquer la présence du pirate sur le système.
- En effet, si l'administrateur se connecte en même temps que le pirate, il est susceptible de remarquer les services que le pirate a lancé ou tout simplement qu'une autre personne que lui est connectée simultanément. L'objectif d'un rootkit est donc de tromper l'administrateur en lui masquant la réalité.

Cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/methodologie-dune-attaque-reseau · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com