Université Internationale de Casablanca

LAUREATE INTERNATIONAL UNIVERSITIES

Sécurité des SI

Dr Mohammed BOUTABIA

introduction

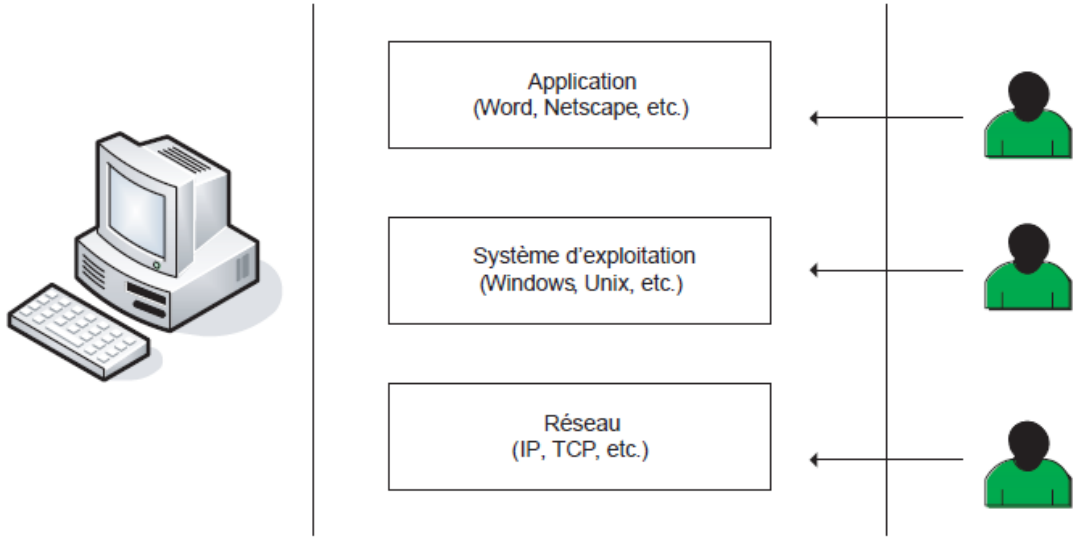
- L’information est primordiale dans l’activité de n’importe qu’elle entreprise
- Les données comportent des informations critiques de l’entreprise (chiffre d’affaires, stratégie marketing, secrets industriels, états des comptes…)
- La perte ou la divulgation de ces données peut avoir des conséquences graves pour l’entreprise
- La disponibilité de cette information a la même importance que l’information elle-même (une information qui n’est pas accessible aux utilisateurs n’est pas utile)
- Le système d’information dans sa globalité (réseaux, systèmes d’exploitations, bases de données) doit être protégé

introduction

- Les équipement réseaux et les terminaux sont des entités vulnérables: bugs dans les programmes, mal configuration
- Les protocoles réseaux ne sont pas conçu pour supporter la sécurité
- Le protocole IP ou TCP ne comportent aucune couche de sécurité
- Ces protocoles de communications présentent plusieurs faiblesses ou failles de sécurité qui peuvent être exploité par des personnes mal intentionnées

Les attaques

- Les attaques exploitent les faiblesses d'un système
- Les attaques touchent :
  - Le réseau et ses protocoles
  - Les systèmes d'exploitation
  - Les applications



Les attaques

- Les premières vulnérabilités d'un système informatique sont les virus, les vers et les chevaux de Troie:
  - Un virus est un programme malicieux attaché à un autre programme qui exécute une fonction non légitime sur un ordinateur
  - Un ver exécute un code arbitraire et installe des copies de lui même sur la mémoire de la machine infectée et qui infecte d'autres machines
  - Un cheval de Troie est une application écrite d'une manière à ressembler à une autre application (légitime) quand l'application est téléchargée et exécuté il attaque la machine

Catégories des attaques

- Les attaques essayent toujours d'exploiter une faiblesse d'un système
  - Attaques de reconnaissance
  - Attaques d'accès
  - Attaques de déni de service

Attaques de reconnaissance

- Attaques de reconnaissance: Une découverte non autorisé des services et une cartographies des systèmes et des vulnérabilités. L'attaque de reconnaissance utilise en générale le sniffing des paquets et un scan des ports qui sont très largement disponible sur internet.
- L'attaque de reconnaissance prépare en générale le terrain pour une attaque ultérieure
- L'attaque de reconnaissance est semblable à un voleur qui surveille un quartier pour localiser les maisons vulnérables sans résidents

Attaques de reconnaissance

- Packet sniffers: capteur de paquets dans un réseau permettant de rassembler tout le trafic qui circulent dans un domaine de collision. Même avec l'utilisation d'un commutateur et une adresse MAC spoofé
- Ping sweeps: un balayage des adresses ip d'une manière aléatoires. Ceux qui existent sur le réseaux répondront aux pings

Attaques de reconnaissance

- Port scans: un balayage des ports pour découvrir les ports ouverts. Un message est envoyé en TCP ou UDP à tout les port, la réponse révèle est ce que la machine est à l'écoute sur ce port
- Attaque par cartographie des réseau: l'architecture du réseau est révélé par des outils comme traceroute en se basant sur les message d'erreur de ICMP qui permettent de cartographier un réseau

Attaques d’accès

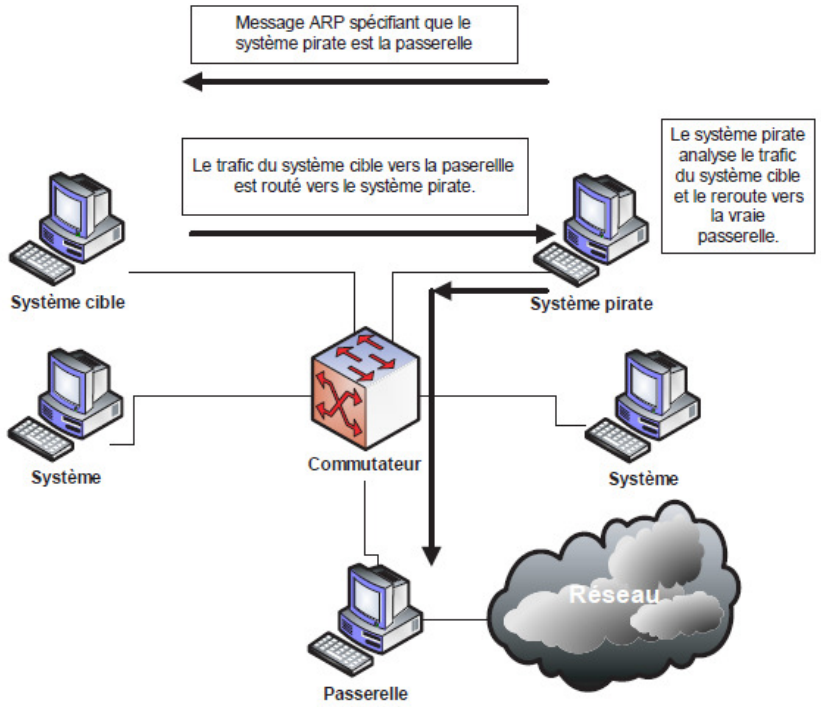
- Attaques d’accès: ces attaques exploitent des vulnérabilités connues pour accéder à un service ou une information sensible.
- Un exemple d’attaque d’accès tente de casser le mot de passe d’un compte pour accéder à une base de données.

Attaques d’accès

- Password attack : un attaquant essaye de deviner le mot de passe d’un système. Un exemple typique est basé sur un dictionnaire de mot de passe
- Redirection de port: un système est utilisé comme un pont pour attaquer un autre système. Un outil d’intrusion est installé dans le système attaqué pour rediriger la session.

Attaques d’accès

- ARP spoofing: attaque qui permet de répondre à une requête ARP avec une adresse MAC non légitime



Attaques d’accès

- IP spoofing: L’attaque IP spoofing consiste à se faire passer pour un autre système en falsifiant son adresse IP. Le pirate commence par choisir le système qu’il veut attaquer. Après avoir obtenu le maximum de détails sur ce système cible, il détermine les systèmes ou adresses IP autorisés à se connecter au système cible.
- Étant donnée que les connexions TCP/IP se basent sur les adresses IP et numéro de port comme identifient de la session l’IP spoofing constitue une attaque d’acces à des ressources critiques

Attaques d'accès: attaques man in the middle

- Cette attaques consistent à faire passer les échanges entre deux systèmes par un troisième selon trois formes:
  - Relais transparent: la machine pirate transforme les données à la volée (ne modifie pas les adresse sources et destination de la session)

  - Relais applicatif: les deux machines n'échangent jamais de données directement (ex: session SSL)

Attaques man in the middle

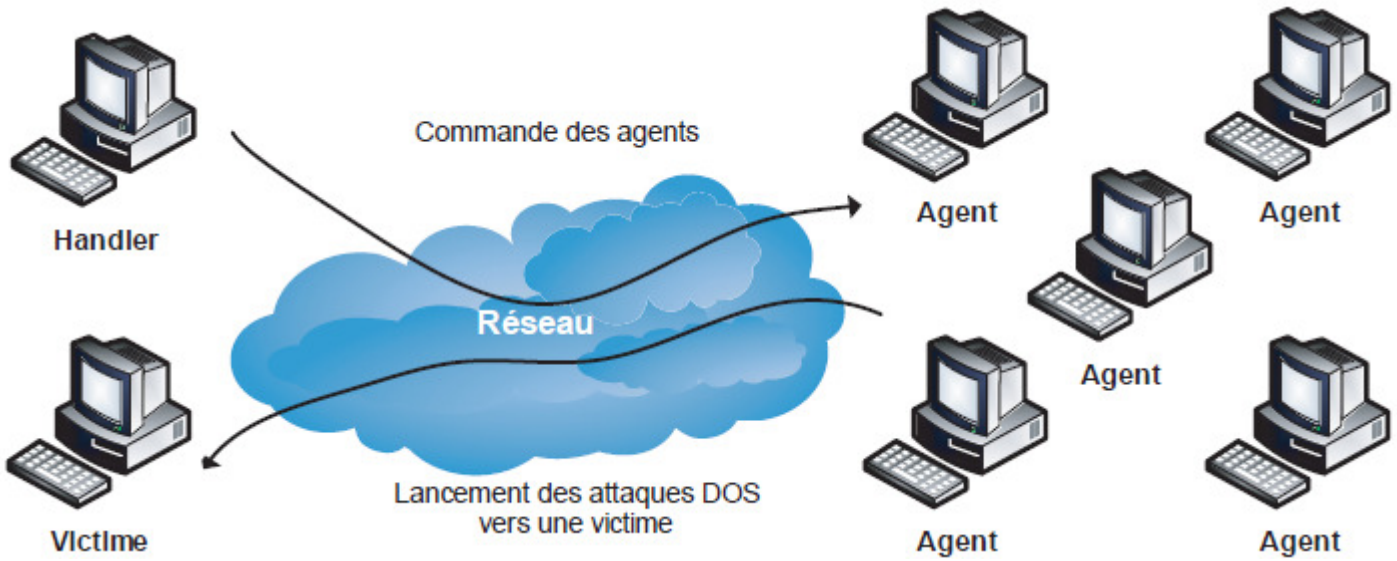
- Hijacking: la machine pirate détourne la session déjà engagée entre A et B pour que ce soit elle qui est en session avec B. A perd la session avec B et la session continue entre B et la machine pirate
- Le hijacking exige une connaissance parfaite de la session TCP (adresse IP , numéro port, numéro de séquence, numéro Ack, falgs…)

Déni de service

- Attaques de déni de service (denial of service): les attaques de déni de service envoie un large nombre de requête sur le réseau. Cet envoi excessif de requête ralenti les systèmes => les systèmes deviennent indisponible pour les utilisateurs légitimes
- Son principe de fonctionnement est le suivant :
  - Une ou plusieurs machines inondent le réseau avec des paquets réseau afin de saturer la bande passante de celui-ci
  - Une fois que toute la bande est occupée, les autres machines ne peuvent plus travailler, ce qui génère une situation de déni de service.

Déni de service

- Les attaques de déni de service distribués (DDoS) est similaire à un DoS sauf que DDoS est lancée depuis plusieurs machines complices ce qui amplifie l'effet de l'attaque.



Les attaques de Déni de service

- **Ping of Death**: Envoie des fragment de ICMP request sans jamais compléter les fragment. Un envoi excessif de ping avec des adresses différentes remplies la mémoire de réassemblage
- **Smurf Attack**: Il s'agit d'un ping vers une adresse de broadcast d'un réseau. Toutes les machines répondent en même temps ce qui sature le réseau. Les routeurs doivent arrêter des ping de braodcast
- **TCP SYN Flood**: Dans ce type d'attaque, la machine victime est inondé avec des message TCP SYN qui annoncent le début d'une session TCP. Le serveur répond a chaque message avec un message TCP SYN ACK sauf que le three way handshake n'est pas finalisé par l'attaquant et la machine victime reste à l'attente d'un Ack qui n'arrivera jamais. En faisant ceci avec plusieurs adresse spoofé le serveur alloue des ressources qui pour chaque connexion sans pouvoir les libérer jusqu'à sa saturation.

Évaluation des risques et politique de sécurité

Évaluation de la sécurité

- L'objectif de la sécurité est de protéger les éléments critiques d'une entreprise
- La détermination de ces ressources à protéger est primordiale pour l'élaboration d'une politique de sécurité cohérente.
- Les ressources peuvent être de plusieurs natures:
  - matériel (ordinateurs, équipements réseau, etc.) ;
  - données (bases de données, sauvegardes, etc.) ;
  - logiciels (sources des programmes, applications spécifiques, etc.) ;
  - personnes (salariés, personnel en régie, etc.).
- En suite il faut déterminer les objectifs de sécurité en spécifiant les besoins en terme de confidentialité, d'intégrité et de disponibilité des éléments critiques de l'entreprise.

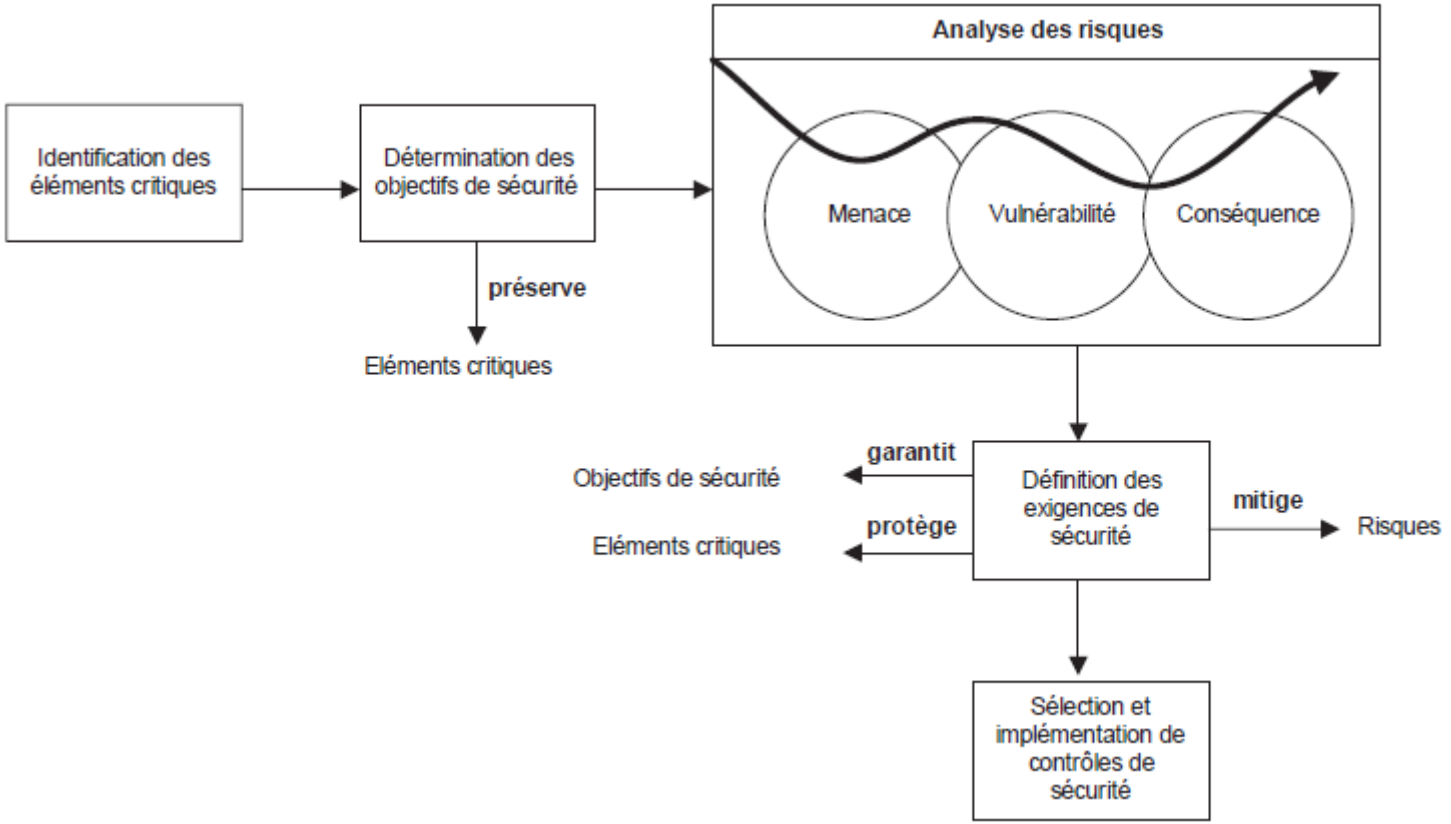
Évaluation des risques

- Une fois les éléments critiques et les objectifs de sécurité identifiés, il convient, pour chacune des ressources vitales, d'associer les trois éléments (vulnérabilité, menace, conséquences), qui visent à définir l'analyse de risques proprement dite, telle que définie par l'ISO comme la combinaison de la probabilité d'un événement et de ses conséquences.

Évaluation des risques

- **Vulnérabilité:** Il s'agit d'une faiblesse de sécurité qui peut être de nature logique ou physique. exemple: une erreur d'implémentation, une mauvaise configuration ou une insuffisance de moyens de protection
- **Menace:** La menace désigne l'exploitation d'une faiblesse de sécurité (vulnérabilité) par un attaquant interne ou externe => La probabilité d'une menace de sécurité est généralement évaluée par des études statistiques.
- **Conséquence**: Il s'agit de l'impact (perte financière, dommages sur l'image de marque, etc.) sur l'entreprise de l'exploitation d'une faiblesse de sécurité. Estimer une conséquence d'une faiblesse de sécurité nécessite généralement une connaissance approfondie de l'entreprise et requiert la participation de l'ensemble des experts

Stratégie de sécurité



Stratégie de sécurité

- La prévention consiste à diminuer la probabilité d'occurrence des menaces
- la correction des faiblesses de sécurité consiste à diminuer les impacts de sécurité sur l'activité de l'entreprise.

Évaluation des risque

la stratégie sécuritaire répond aux principes suivants :

- Les risques ayant **une occurrence faible et une conséquence faible** sur l'entreprise ne sont pas pris en compte *a priori. On peut cependant mitiger ce point par le fait que la* combinaison de risques faibles peut engendrer un risque fort. Ils doivent donc être pris en compte.
- Les risques ayant **une occurrence forte et une conséquence forte** ne doivent pas exister par nature, car ils mettraient en cause les activités de l'entreprise. Si de tels risques existent, il est probable que les coûts nécessaires pour les réduire seront trop importants pour l'entreprise. Il est donc nécessaire de faire appel à des assurances pour les couvrir.

Évaluation des risques

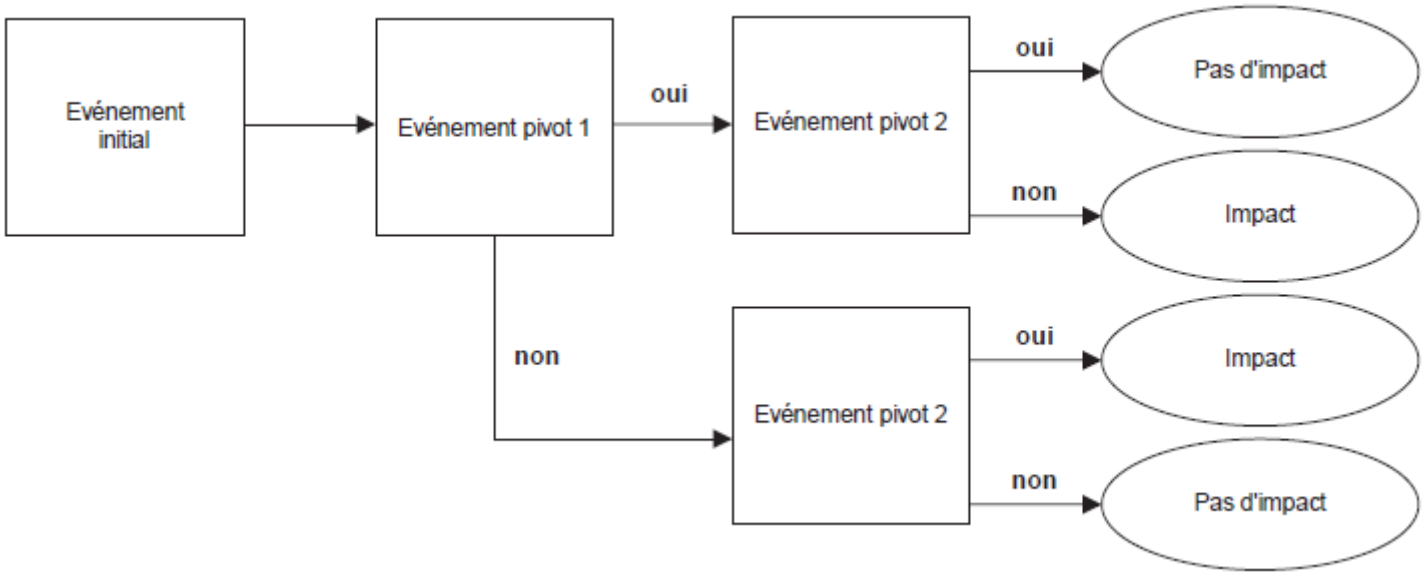
- Les risques ayant **une occurrence forte et une conséquence faible** doivent être pris en compte et faire l'objet d'une analyse coût/acceptation du risque.
- Les risques ayant **une occurrence faible et une conséquence forte** doivent être pris en compte et faire l'objet d'une analyse coût/acceptation du risque. Il est probable qu'il faille faire appel à des assurances pour les couvrir.

Analyse probabiliste des risques

- Analyser le risque revient à répondre aux trois questions suivantes :
  - Qu'est-ce qui peut tourner mal ? => définir un ensemble de scénarios d'accidents possibles
  - Quelle est la probabilité que cela se produise ? => l'évaluation des probabilités associées à ces scénarios
  - Quelles en sont les conséquences ? => Estimer les conséquences

Analyse probabiliste des risques

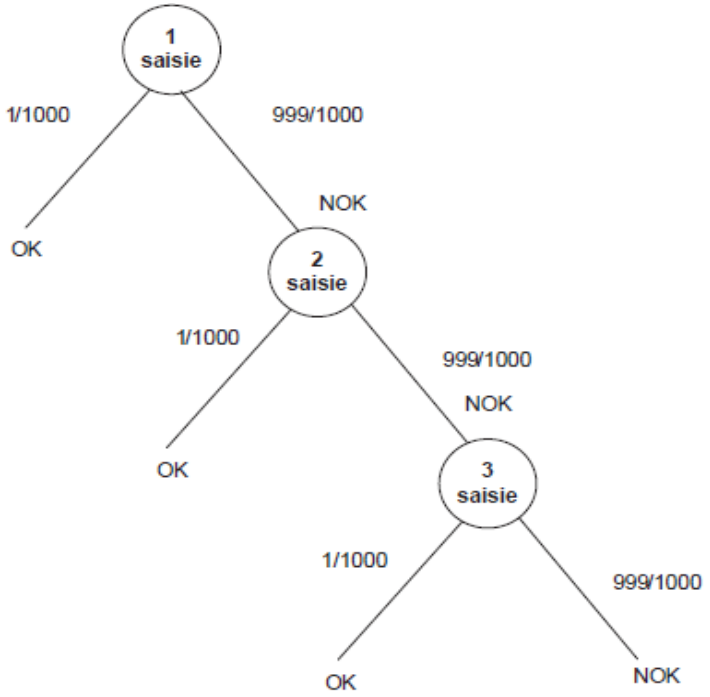
- **Modélisation des scénarios**: Chaque scénario d'accident doit être modélisé à l'aide d'un arbres d'événements. *Un arbre d'événements* commence par un événement initial et s'étend en fonction de la progression du scénario.



exemple

- si un distributeur de billets a calculé qu'un individu essayant un code au hasard est refoulé 999 fois sur 1 000 et que l'ordinateur n'accepte que trois essais consécutifs, quelle est la probabilité de retirer des billets par hasard ?

arbre d'événements



Principes génériques d'une politique de sécurité

- **Identification:** Information permettant d'indiquer qui vous prétendez être. Une identification élémentaire est le nom d'utilisateur que l'on saisit dans un système informatique. Une identification plus évoluée peut être fournie par un relevé d'empreinte digitale, une analyse faciale ou rétinienne, etc.
- **Authentification:** Information permettant de valider l'identité pour vérifier que vous êtes celui que vous prétendez être. Une authentification élémentaire est le mot de passe que vous entrez dans le système informatique. Une authentification forte combine une chose que vous possédez et une chose que vous connaissez (numéro de carte bancaire et code personnel, par exemple).
- **Autorisation:** Information permettant de déterminer quelles sont les ressources de l'entreprise auxquelles l'utilisateur identifié et autorisé a accès, ainsi que les actions autorisées sur ces ressources. Cela couvre toutes les ressources de l'entreprise.

Principes génériques d'un politique de sécurité

- **Confidentialité:** Ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données.
- **Intégrité:** Ensemble des mécanismes garantissant qu'une information n'a pas été modifiée.
- **Disponibilité:** Ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles, que ces dernières concernent l'architecture réseau, la bande passante, le plan de sauvegarde, etc.

Principes génériques d'un politique de sécurité

- **Non-répudiation:** Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire et que l'émetteur ne peut pas nier son envoie.
- **Traçabilité:** Ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise. Cela suppose que tout événement applicatif soit archivé pour investigation ultérieure.

Politique de sécurité

- **Distinguer la politique de la procédure**
  - La politique est l'expression du besoin. L'objectif d'une politique de sécurité est d'énoncer des résultats attendus, et non les moyens par lesquels les obtenir
  - La procédure, ou recommandation technique, est l'implémentation du besoin.

Exemple de politique

- *« L'accès à distance au réseau interne de l'entreprise (intranet) est autorisé à la condition exclusive d'une authentification forte de l'individu via une connexion réseau chiffrée»*
- *« L'accès à Internet depuis le réseau interne de l'entreprise (intranet) est protégé contre les attaques éventuelles, incluant les virus informatiques. »*

Exemple de procédure

- *« L'accès externe au réseau interne de l'entreprise (intranet) est authentifié par un certificat électronique validé auprès de la PKI de l'entreprise. De plus la connexion réseau est chiffrée par le protocole IPsec. »*
- *« L'accès à Internet traverse un pare-feu filtrant le protocole IP. De plus, le pare-feu est couplé à un système antivirus, qui analyse tous les e-mails et attachements transitant entre Internet et le réseau interne de l'entreprise (intranet) afin de détecter d'éventuels virus. »*

Access control list (ACL)

- C’est l’outil de base pour le filtrage des paquets IP (niveau 3)
- Interdire certaines actions à certains utilisateurs
- Une ACL indique au routeur quels sont les paquets qu’il doit accepter ou refuser
  - ➔contrôle du trafic (seuls les paquets autorisés circulent)
  - ➔amélioration de la performance du réseau (limitation du trafic)

Access control list (ACL)

- Une ACL est une collection séquentielle d'instructions d'acceptation ou d'interdiction qui s'applique
  - aux adresses IP
  - aux protocoles de couche supérieure
- Une ACL s’applique à une interface orientée d’un routeur
- Sur une interface, on peut mettre deux ACL :
  - une en entrée
  - une en sortie

Access control list (ACL)

- L'acceptation ou le refus peuvent être fondés sur :
  - l'adresse IP d'origine
  - l'adresse IP de destination
  - le numéro de port
- Tous les paquets qui arrivent sur l’interface d’un routeur où une ACL a été activée sont confrontés à cette ACL
- Un paquet refusé est tout simplement abandonné

Access control list (ACL)

- L'ordre des instructions qui composent les ACL est très important
- Pour chaque paquet, les instructions de l'ACL sont scrutées dans l'ordre où elles ont été écrites
- Dès que le paquet correspond à l'une des instructions de l'ACL, la décision est prise et les suivantes ne sont pas consultées
- Toutes les ACL doivent se terminer par une instruction du genre :
  - Dans tous les autres cas faire …
  - Une ACL incomplète se termine par défaut par « deny any »

Access control list (ACL)

- Il existe deux familles d'ACL :
  - les ACL standards qui ne vérifient que l'adresse IP source du paquet filtré (de 1 à 99 et de 1300 à 1999)
  - les ACL étendues qui vérifient :
    - l'adresse IP source
    - l'adresse IP destination
    - le protocole de niveau 3 ou 4
    - le numéro de port
    - De 100 à 199 et de 2000 à 2699

ACL standard

Syntaxe générale:
R1(config)#access-list access-list-number [deny | permit] source [source-wildcard] [log]

Exemple:

```
R1(config)#  access-list 50 deny 172.16.1.1
R1 (config)# access-list 50 permit 172.16.0.0 0.0.255.255
```

Nombre compris entre 1 et 99, ou entre 1300 et1999 (IOS recent) c'est une ACL standard

Refuser ou autoriser

Pas de masque générique : par défaut 0.0.0.0

Masque générique

Exercice

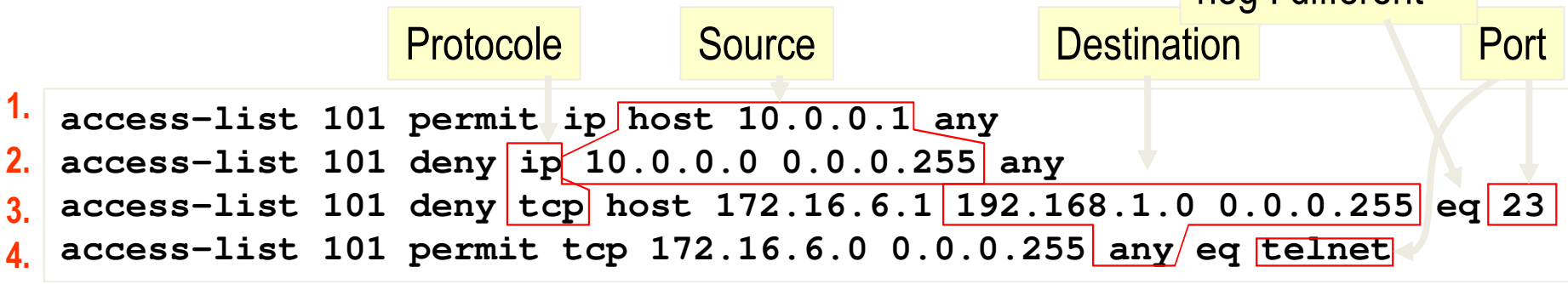
- Écrire une ACL qui autorise seulement le trafic venant de la machine 192.168.1.3
- Écrire une ACL qui refuse seulement le trafic venant de la machine 192.168.1.3
- Ecrire une ACL permettant le trafic du réseau 192.168.1.0/24 et refuser le trafic venant de la machine 192.168.1.3

ACL étendue

Syntaxe générale:
R1(config)#access-list access-list-number [deny | permit] protocol source [source-wildcard] operator port destination [destination-wildcard] operator port [log]

Exemple:

eq : equal
gt : greater than
lt : less than
neg : different



1. **autorise tout le trafic IP venant de l'hôte 10.0.0.1, quelle que soit la destination**
2. **refuse le trafic venant du réseau 10.0.0.0/24, quelle que soit la destination**
3. **interdit à l'hôte 172.16.6.1 (only) l'accès telnet au réseau 192.168.1.0/24**
4. **autorise tous les hôtes du réseau 172.16.6.0/24 à utiliser telnet vers tous les réseaux**

exercice

- Écrire une ACL qui autorise le trafic venant de n'import quel machine vers le serveur web sur la machine 200.190.1.12
- Écrire une ACL qui refuse l'acces à Telnet de toutes les machines externes et l'autoriser pour les machines interne du réseau 179.10.0.0/16