RESUME SECURITE

Chapitre: MALWARES

Définition:Un malware est un programme conçu pour altérer le fonctionnement normal d'un ordinateur de manière plus ou moins grave

Cycle de vie:

1. Phase de recherche : recherche des victimes potentielles.
2. Phase d'implantation : implantation discrète sur l'ordinateur cible.
3. Phase de contamination : infection du système cible et établissement d'une présence persistante.
4. Phase d'incubation : période pendant laquelle le malware reste silencieux et ne montre aucun signe d'activité.
5. Phase d'exécution : activation du malware pour effectuer sa tâche programmée tout en cherchant de nouvelles victimes
6. Phase d'hibernation : période de latence pendant laquelle le malware reste caché et peut réapparaître plus tard pour poursuivre son activité malveillante.

VIRUS:

- Un virus informatique est un petit programme qui vit à l'intérieur d'un hôte, généralement une application.
- Le virus injecte son code dans le code d'un programme sur l'ordinateur cible, et ne peut se répliquer sans l'aide du programme hôte.
- Le virus est programmé pour se répliquer autant que possible vers d'autres cibles et déclencher la charge virale sur un critère donné.
-Un virus arrive toujours sur un ordinateur dans un fichier exécutable.

Extension	Programme
.exe	écrit en langage machine, directement interprétable par l'ordinateur
.com	écrit en langage machine, directement interprétable par l'ordinateur
.vbs	écrit en langage Visual Basic et exécutable sous Windows
.doc	destiné au logiciel de traitement de textes Word. Il peut contenir des programmes (des macros) exécutables par Word
.xls	destiné au tableur Excel. Il peut contenir des programmes (des macros) exécutables par Excel
.bat	destiné à l'interpréteur de commandes
.cmd	destiné à l'interpréteur de commandes
.scr	destiné à réaliser un écran de veille
.pif	destiné à d'anciennes versions de Windows et contenant des informations nécessaires à l'exécution de certaines programmes et/ou des instructions exécutables sous Windows
.zip	éventuellement compressé et exécutable après décompression par un utilitaire de type IZarc, WinZip,...

Effets des virus :

- Les virus peuvent s'auto-envoyer par e-mail aux contacts de l'ordinateur infecté.
- Les virus peuvent collecter des données confidentielles et les envoyer sur Internet.
- Les virus peuvent utiliser l'ordinateur infecté pour lancer une attaque contre un autre ordinateur.
- Les virus peuvent modifier ou supprimer des données dans l'ordinateur infecté.
- Les virus peuvent provoquer une panne matérielle, ralentir ou bloquer l'ordinateur, et même le faire s'éteindre à intervalles réguliers.

Transmission des virus :

- Les clés USB et les pièces jointes aux courriers électroniques sont des vecteurs courants de transmission de virus.
- Les documents transmis par des personnes connues peuvent contenir des virus de macros.
- Le téléchargement de logiciels ou de fichiers de nature inconnue sur des sites non fiables peut amener des virus.
- Les logiciels piratés téléchargés sur des réseaux de pair à pair (peer-to-peer) peuvent contenir des virus.

Pourquoi les virus :

- crime organisé et de racket, où une entreprise est ciblée par un virus qui menace de l'attaquer si elle ne paie pas.
- D'autres motivations financières, tels que l'envoi de millions de courriers électroniques publicitaires (spam) à partir d'ordinateurs infectés.
- Certains auteurs de virus cherchent à obtenir une reconnaissance dans des groupes criminels.
- D'autres cherchent à marquer leur empreinte dans le cyberespace.
- Certains ont des motivations politiques ou idéologiques.

VERS:

Un ver est un type de logiciel malveillant plus avancé que les virus, capable de se propager automatiquement à travers les réseaux en exploitant des vulnérabilités dans les applications ou des configurations incorrectes.
Contrairement aux virus, les vers sont indépendants et n'ont pas besoin d'un hôte pour se dupliquer. De plus, ils se propagent généralement plus rapidement que les virus.

Certains virus ou vers sont **polymorphes**: ils changent légèrement de forme pour se rendre plus difficiles à identifier.

Cette modification peut être faite en ajoutant des instructions sans conséquence ou en exploitant d'instructions machines.

Buts de vers:

- Pur vandalisme gratuit : saturation d'un réseau par la multiplication exponentielle du ver.
- Attaque ciblée : attente discrète au sein de milliers d'ordinateurs, puis chaque ver se connecte à un serveur pour le mettre hors service à une date précise.
- Prise de commande à distance de l'ordinateur.
- Espionnage des frappes au clavier
- Ouverture de portes de l'ordinateur pour faciliter l'accès par d'autres vers ou virus.
- Envoi de milliers de courriers électroniques publicitaires à partir de l'ordinateur infecté.
- Effacement de fichiers, envoi de fichiers confidentiels sur Internet, etc.

Exemples de vers:

- Le ver Sasser se propage en exploitant une erreur de conception dans le traitement des commandes sur les ordinateurs vulnérables. Il s'installe dans le système et se propage rapidement à d'autres ordinateurs présentant la même faiblesse.

- Le ver Netsky utilise une faille dans Outlook pour infecter les ordinateurs, et peut s'auto-envoyer par courrier électronique. Les ordinateurs infectés servent également de « zombies » pour attaquer d'autres sites web. L'infection par Netsky peut entraîner un ralentissement important de l'ordinateur.

Trojan horses:

- Un cheval de Troie est un type de logiciel malveillant qui se présente comme un programme utile ou une application intéressante.
- Contrairement aux vers, les chevaux de Troie n'essaient pas de se multiplier ou de se propager.
- Les chevaux de Troie peuvent être utilisés pour des activités malveillantes telles que la récupération de mots de passe, la destruction de fichiers, l'espionnage ou le vol d'informations.
- Les chevaux de Troie peuvent être introduits dans un système via des e-mails, des téléchargements de logiciels piratés ou des sites web malveillants.
- Les mesures de prévention contre les chevaux de Troie incluent l'utilisation de logiciels antivirus et pare-feu, ainsi que la prudence lors du téléchargement ou de l'ouverture de fichiers provenant de sources inconnues.
- Un cheval de Troie est un type de logiciel malveillant qui se présente comme un programme utile ou une application intéressante.
- Contrairement aux vers, les chevaux de Troie n'essaient pas de se multiplier ou de se propager.

Example :
"Le ver "ILOVEYOU" se présente comme un courrier électronique amical. Une fois installé, il envoie les mots de passe qu'il trouve sur l'ordinateur vers une adresse électronique. Ver écrit en Visual Basic.

BACKDOORS:

- Les Backdoors sont des chevaux de Troie qui permettent de se connecter à distance sur un ordinateur infecté.
- Une fois les portes ouvertes, l'ordinateur peut être utilisé par d'autres logiciels malveillants ou par des pirates.
- Il suffit d'ouvrir un port non utilisé pour pénétrer dans un ordinateur, et dès qu'un port est ouvert, il est possible de prendre le contrôle total de la machine depuis n'importe quel ordinateur connecté à Internet.

Buts :

- Ils peuvent être utilisés pour espionner et voler des informations sensibles sur un réseau.
- Les informations visées incluent les détails des comptes, les documents confidentiels, les adresses email, les images ou conceptions confidentielles, les informations sur l'emploi du temps et les déplacements des utilisateurs, ainsi que les informations de cartes de crédit.
- Les chevaux de Troie peuvent être utilisés pour des activités illégales, telles que le hacking, le scanning, l'infiltration d'autres machines sur le réseau ou sur Internet.

Exemple :

- BackOrifice est une application client/serveur permettant de surveiller, administrer et effectuer à distance toutes les actions sur la machine infectée.
- Il a été développé en 1998 par un groupe de hackers nommé "Cult of the Dead Cow" (cDc) dans le but de mettre en évidence les failles de sécurité dans Windows 95/98 et de dévaloriser ce système.
- BackOrifice a été diffusé rapidement sur Internet après sa création.

SPYWARES:

- Les spywares sont des programmes malveillants qui collectent des informations sur l'utilisateur d'un ordinateur et les envoient à leur concepteur ou un commanditaire.
- La collecte d'informations permet de créer et de vendre des bases de données à des sociétés publicitaires pour l'envoi de spam.
- Certains spywares sont intégrés à des logiciels gratuits ou tentent de s'installer lors de la visite d'un site web.

- Plusieurs centaines de spywares peuvent cohabiter ensemble et affecter les performances de l'ordinateur.
- Les spywares peuvent afficher des publicités ciblées en fonction des informations collectées.

ADWARES:

• Les adwares sont des logiciels qui s'installent généralement sans le consentement de l'utilisateur.
• Ils ajoutent des publicités dans les pages web visitées ou dans des fenêtres séparées.
• Contrairement aux spywares, les adwares ne communiquent pas d'informations vers un serveur, ils peuvent donc travailler même si l'ordinateur n'est pas connecté à Internet.
• Les adwares utilisent des ressources de l'ordinateur, comme la mémoire et le processeur, ce qui peut ralentir l'ordinateur.
• Ces programmes sont souvent mal écrits et peuvent contenir des bugs qui font planter l'ordinateur.

Installation d'ADware:

- Les adwares peuvent s'installer sans prévenir si le niveau de sécurité du navigateur web est trop faible.
- Certains utilisateurs peuvent cliquer trop facilement sur le bouton qui donne leur accord sans avoir compris à quoi ils s'engagent.
- Certains adwares ou spywares se font passer pour des anti-spywares et persuadent les utilisateurs que leur ordinateur est infesté de spywares.
- Les utilisateurs téléchargent alors le logiciel qui ne fait que leur ajouter des spywares, adwares ou dialers supplémentaires.

KEYLOGGERS:

- Les Keyloggers sont des logiciels commerciaux qui permettent d'espionner tout ce que fait l'utilisateur d'un ordinateur.
- Ils enregistrent les frappes au clavier, y compris les mots de passe, numéros de carte de crédit, sites web visités, copies d'écran, etc.
- Les informations sont ensuite transmises à une adresse de courrier électronique.
- Les Keyloggers sont souvent présentés comme des solutions discutables pour les parents ou les patrons qui souhaitent surveiller l'activité de leur enfant ou de leurs employés.
- Certains virus ou chevaux de Troie peuvent contenir des Keyloggers.

DIALERS:(composeurs téléphoniques)

• Les dialers peuvent être utilisés pour appeler des numéros surtaxés.

• Le fournisseur de service peut proposer de télécharger un logiciel pour effectuer l'appel surtaxé.
• Les utilisateurs doivent faire attention, car ils ne connaissent pas le numéro qui sera appelé par le logiciel.
• Les dialers peuvent connecter l'utilisateur à un serveur situé à l'étranger.

PHISHING (ou hameçonnage)

• Technique d'escroquerie où des malfaiteurs créent un site web qui ressemble à celui d'une banque ou d'un service en ligne pour piéger les clients.
• Ils envoient des courriers électroniques aux utilisateurs, souvent de manière aléatoire, pour les persuader de fournir des informations confidentielles telles que des numéros de carte de crédit ou des informations de connexion.
• Les fraudeurs peuvent ensuite utiliser ces informations pour effectuer des achats ou des retraits d'argent à partir du compte bancaire de la victime.
• Les cibles sont souvent des utilisateurs non méfiants qui ne remarquent pas les signes indiquant qu'il s'agit d'un site web fake.

SPAM:

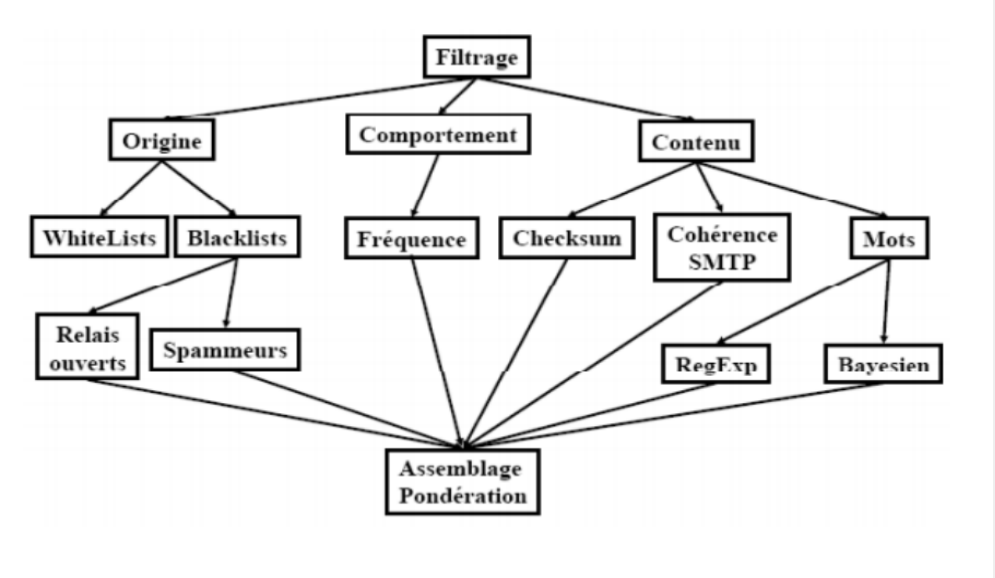
- Le spam est l'envoi massif et répété de courriers électroniques non sollicités à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière.
- Les adresses électroniques peuvent être captées grâce à des moteurs de recherche, des espaces publics sur Internet tels que les sites web, les forums de discussion, les listes de diffusion, les chats, ou encore en cédant les adresses sans le consentement des personnes concernées.
- Les spammeurs peuvent utiliser des ordinateurs répartis sur la planète pour envoyer leurs courriers en contrôlant ces ordinateurs à distance et en y implantant des serveurs de courrier électronique.
- Pour prendre le contrôle d'un ordinateur distant, ils peuvent utiliser des virus ou des vers qui ouvrent des ports des ordinateurs qu'ils infectent.

Les différentes catégories de Spam : Health, Products ,Financial ,Scams ,Internet, Leasure,Spiritual…

Solutions :

- Utiliser des règles pour détecter les spams sur le serveur de courriel
- Utiliser plusieurs règles avec une logique "floue" pour déterminer si un message est un spam ou non
- Combinaison des résultats des règles pour produire un "score"
- Définir un seuil pour considérer le message comme spam

- Utiliser des filtres bayésiens pour les corrélations



HOAXES (canulars):

- Les hoaxes sont des canulars qui circulent sous forme de courriers électroniques pour informer de faits graves, importants ou urgents qui sont souvent inexistants.
- Il s'agit souvent de chaînes de courriers que l'on vous invite à relayer à tous vos contacts.
- Il ne faut jamais renvoyer ces messages car cela pourrait simplement provoquer une saturation du réseau.

Les solutions

• Antivirus : un outil indispensable
• Pare-feu : pour éviter les intrusions.
• Anti adwares : pour éviter les publicités envahissantes et les espiogiciels.
• Anti-pourriels : des filtres pour éviter les courriers indésirables.
• Logiciels moins sensibles : certains logiciels sont moins sensibles aux pestes de l'Internet (Linux, Firefox,...).
• Comportements : les comportements à éviter, ceux qui sont recommandés

---

Chapitre : FIREWALLS

- Un firewall est un système physique ou logique qui contrôle et bloque la circulation des paquets de données entre un ou plusieurs réseaux.
- Il analyse les informations contenues dans les couches 3, 4 et 7 du modèle OSI.
- Il s'agit d'une machine qui a au minimum deux interfaces réseau : une pour le réseau interne à protéger et une pour le réseau externe.
- Le firewall est souvent situé à l'entrée du réseau dans les entreprises pour protéger le réseau interne contre les intrusions en provenance des réseaux externes, notamment internet.

Pourquoi un firewall?

Contrôle : Gérer les connexions sortantes à partir du réseau local.
Sécurité : Protéger le réseau interne des intrusions venant de l'extérieur.
Vigilance : Surveiller/tracer le trafic entre le réseau local et internet

Zone Démilitarisée:

- La DMZ est une zone démilitarisée permettant d'isoler des machines du réseau interne pour qu'elles soient accessibles de l'extérieur sans compromettre la sécurité de l'entreprise.
- La DMZ est créée en configurant une nouvelle interface vers un réseau isolé et accessible aussi bien du réseau interne que de l'extérieur.
- Des applications mises à disposition du public peuvent être hébergées dans la DMZ, comme un serveur web, un serveur de messagerie ou un serveur FTP public.

Le principe de filtrage de paquet :

- Le filtrage de paquets est utilisé par les firewalls pour sécuriser les réseaux.
- Les firewalls agissent comme des filtres entre les réseaux locaux et externes.
- Ils examinent les paquets de données en fonction de règles préétablies.
- Les firewalls détectent les tentatives d'intrusion et fournissent des informations sur les auteurs.
- Ils ne sont pas efficaces contre les attaques de virus.

a. **Filtrage de paquets simple (stateless)**
   - il est utilisé par les systèmes pare-feu, souvent intégrés aux routeurs.
   - Il repose sur l'analyse des en-têtes des paquets IP échangés entre machines.
   - Les en-têtes contiennent des informations telles que les adresses IP émettrice et réceptrice, le type de paquet, le numéro de port, etc.
   - Les adresses IP identifient les machines et les ports donnent des indications sur les services utilisés.
   - Certains ports courants, tels que les ports 25, 110 et 80, sont généralement autorisés, mais il est recommandé de bloquer les ports non essentiels selon la politique de sécurité adoptée.

- Les règles des firewalls sont définies dans un fichier et utilisent les informations des paquets pour décider de leur traitement.
- Il y a deux approches pour définir la politique par défaut du filtre :
  1. **Tout ce qui n'est pas interdit explicitement est autorisé**
  2. **Tout ce qui n'est pas autorisé explicitement est interdit**

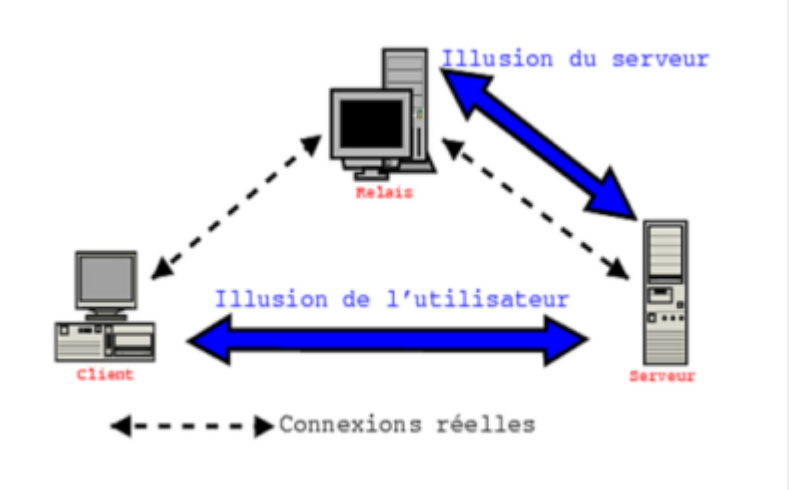
- La deuxième méthode est plus sécurisée, mais nécessite une définition précise des besoins en termes de communication.
- L'ordre des règles dans le fichier est important, car les paquets sont évalués successivement selon les règles. Si un paquet est rejeté par une règle, il ne sera pas accepté même s'il est accepté plus loin dans le fichier.
(remember cours reseau Acl).

b. **Le filtrage dynamique et adaptatif (stateful inspection)**, permet de suivre les transactions entre le client et le serveur.
- Contrairement au filtrage statique, ce système examine les couches 3 et 4 du modèle OSI pour assurer la circulation correcte des données de la session en cours.
- Les sessions et les connexions sont conservées dans des tables d'états internes au firewall, ce qui lui permet de prendre des décisions en fonction de l'état des connexions.
- Ce type de filtrage offre une meilleure protection contre les attaques de type DoS (Denial of Service).
- Pour certains protocoles tels que UDP, ICMP, et FTP, où les ports peuvent être dynamiquement ouverts, le filtrage dynamique est particulièrement utile pour gérer l'état de ces connexions.
- Le firewall doit connaître le protocole FTP et d'autres protocoles similaires pour permettre le passage du flux de données associé au flux de contrôle.
- Cela garantit que le firewall fonctionne de manière appropriée pour ces protocoles spécifiques.

c. **Le filtrage applicatif (type proxy)**, fonctionne au niveau de la couche 7 du modèle OSI pour filtrer les communications application par application.

- Un firewall utilisant le filtrage applicatif est appelé passerelle applicative ou serveur mandataire (proxy) et permet de relayer les informations entre deux réseaux tout en effectuant un filtrage détaillé du contenu des paquets.
- Il nécessite une connaissance de l'application et de la structure des données échangées.
- Le proxy HTTP est l'exemple le plus courant, mais il existe également d'autres types de serveurs proxy pour différents protocoles tels que SMTP, POP3, IMAP et FTP.
- Les fonctions du proxy incluent le relais des échanges, la masquage des informations des machines internes, la tenue d'un journal, le filtrage basé sur des critères tels que les adresses, les ports, le contenu, et la possibilité d'inclure une fonction de cache.

- Le proxy permet de protéger les informations du réseau en cachant les adresses IP des postes internes, mais nécessite la configuration des applications pour les utiliser.
- Pour rendre son utilisation transparente, une redirection de port sur le firewall est souvent nécessaire.



La traduction d'adresse:

- La traduction d'adresse permet de substituer d'autres valeurs aux adresses et ports source ou destination dans les paquets traversant un routeur.
- La redirection permet de rediriger un flux entrant vers une autre adresse et éventuellement un autre port.
- Le camouflage IP (ip masquerading) substitue une adresse IP source du réseau local par une adresse IP publique, permettant aux utilisateurs d'un réseau privé d'accéder à Internet sans que leur adresse soit visible de l'extérieur.
- La traduction d'adresse est réversible, ce qui signifie que l'opération effectuée dans un sens sera inversée dans l'autre sens.

La redirection d'adresse : et de port, redirige les flux entrants de l'interface externe vers un serveur interne spécifique. Par exemple, le flux arrivant à l'adresse publique du routeur sur le port 80 est redirigé vers l'adresse IP du serveur Web interne du réseau local. Cela permet d'accéder au serveur Web interne en utilisant l'adresse publique du routeur.

La traduction d'adresse réseau (NAT) : permet à un routeur d'établir une correspondance entre les adresses IP internes et les adresses IP publiques.d'une manière statique ou dynamique. un routeur peut permettre à plusieurs hôtes internes d'accéder à Internet en utilisant une seule adresse IP publique.donc le nombre d'hôtes simultanés est limité par le nombre d'adresses IP publiques disponibles.

Deux types de NAT :
Statique : association entre n adresses publiques et n adresses privées.
Intérêt : Uniformité de l'adressage dans la partie privée du réseau

Sécurité accrue (tous les flux passent par la passerelle NAT) .
Inconvénient : Problème de pénurie d'adresses IP publiques non-résolu

Dynamique : association entre 1 adresse publique et n adresses privées
Intérêt : Plusieurs machines utilisent la même adresse IP publique pour sortir du réseau privé
Inconvénient :
Les machines du réseau interne ne sont pas accessibles de l'extérieur
L'association de n adresses privées à 1 adresse publique nécessite, au niveau de la passerelle, de : Modifier l'adresse source et destination des paquets sortant et entrants et le numéro de port source pour les flux sortant

Pourquoi avoir des adresses privées?

- Gérer la pénurie d'adresses au sein d'un réseau
- Masquer l'intérieur du réseau par rapport à l'extérieur
- Améliorer la sécurité pour le réseau interne
- Assouplir la gestion des adresses du réseau interne
- Faciliter la modification de l'architecture du réseau interne

Le routeur différencie les paquets qui lui sont destinés de ceux qu'il doit relayer en utilisant la translation d'adresse réseau (NAT) en suivant cet algorithme:

1: Modifier l'adresse source et le port source :*(@source_privée,port_source)* → *(@publique,port_source)*
2: Sauvegarder l'association dans la table NAT Pour chaque paquet entrant
3: Chercher une association correspondant au couple (@destination, port_destination)
4: Si ∃ une association dans la table NAT Alors :
5: Modifier l'adresse de destination et le port de destination
6: Relayer le paquet
7: Sinon /* Erreur de routage */

- Dans le cas de protocoles sans numéro de port, des méthodes spécifiques doivent être mises en place((identifiant ICMP pour ICMP par exemple).
- Pour rendre les machines du réseau local joignables, la redirection de port est utilisée, redirigeant les connexions entrantes d'un port donné vers une machine spécifique du réseau privé.

Autres fonctions:

- Les pare-feu ont évolué pour inclure des fonctionnalités telles que (VPN), permettant la création d'extranets et la sécurisation de l'accès distant aux ressources internes.
- La haute disponibilité est assurée grâce à la synchronisation des tables de filtrage, pour garantir la continuité des services .
- Certains équipements intègrent des filtres au niveau applicatif, tels qu'un antivirus, une recherche de contenus licencieux ou une sonde de détection d'intrusion. Cependant, ces

fonctionnalités peuvent affecter les performances globales et augmenter la consommation de ressources.
- Il est important de minimiser la taille du code pour réduire les risques de failles résiduelles et assurer la sécurité du pare-feu.

Les limites de Firewalls:

- Les firewalls ne garantissent pas une sécurité absolue,ils protègent uniquement les communications qui passent à travers eux.
- Les accès au réseau extérieur qui ne passent pas par le firewall représentent des failles de sécurité, comme les connexions effectuées via un modem.
- L'introduction de supports de stockage externes sur les machines internes au réseau peut compromettre la sécurité.
- La mise en place d'un firewall doit être accompagnée d'une politique de sécurité globale.
- Il est important de rester informé des failles de sécurité et de prendre des mesures pour les minimiser, même avec un système de firewall en place.

Chapitre: Les systèmes de détection d'intrusion (IDS)

Definitions:

Intrusion : Violation d'une politique de sécurité d'un système, impliquant la compromission de la confidentialité, de l'intégrité ou de la disponibilité du système.
Attaque : Tentative de violer la politique de sécurité d'un système, distincte d'une intrusion réussie qui est une violation effective de cette politique.
IDS (Intrusion Detection System) : Mécanisme d'écoute du trafic réseau pour détecter des activités anormales ou suspectes, déclenchant des alarmes en cas de détection d'une attaque.
IPS (Intrusion Prevention System) : IDS actif qui, en cas de détection d'une attaque, prend des mesures pour bloquer ou corriger les risques d'intrusion, comme le blocage de l'adresse IP de l'attaquant présumé.

- **Les méthodes de détection d'intrusions** reposent sur l'observation d'événements et leur analyse.
- Pour cela, on collecte les informations à analyser, qui proviennent des fichiers de journalisation du système ou de sondes telles que les "sniffers" réseau.
- Les événements enregistrés sont ensuite examinés pour détecter des schémas, des comportements anormaux ou des signatures d'attaques connues.
- Cette analyse permet d'identifier les potentielles intrusions et de déclencher des alarmes pour une réponse appropriée.

Classification des IDS:

- IDS Réseaux (ou NIDS) : Ces IDS analysent en temps réel le trafic réseau en utilisant une sonde qui aspire les paquets du réseau. Les paquets sont ensuite décortiqués et analysés pour détecter des comportements ou des signatures d'attaques.
- IDS Systèmes (ou HIDS) : Ces IDS analysent le fonctionnement et l'état des machines sur lesquelles ils sont installés. Ils surveillent l'intégrité des systèmes en vérifiant périodiquement leur état et en générant des alertes en cas d'activités suspectes.
- IDS Hybrides : Les IDS hybrides combinent les caractéristiques des NIDS et des HIDS. Ils surveillent à la fois le réseau et les terminaux en utilisant des sondes placées à des points stratégiques. Les alertes remontent vers une machine centrale qui les agrège et les lie pour une corrélation plus précise. Les IDS hybrides permettent une meilleure détection avec moins de faux positifs et une réaction plus efficace.

Classification par methode de detection:

- ***IDS à signatures (ou à scénarios)*** : Ces IDS se basent sur la recherche de scénarios d'attaques connues à travers l'analyse de l'activité de l'élément surveillé, comme le flux réseau. Trois familles de méthodes sont utilisées :
  - **Systèmes Experts** : Utilisent des règles pour détecter ce qui est suspect, les failles et vulnérabilités connues, ainsi que le savoir-faire de l'administrateur réseau.
  - **"Pattern matching"** (reconnaissance de formes) : Identifie dans les paquets analysés des suites d'événements ou de caractères caractéristiques d'une attaque connue.
  - **Algorithmes génétiques** : Utilisent la sélection naturelle pour générer des règles de détection basées sur les flux anormaux, en s'appuyant sur les logs récoltés par le sniffeur de réseaux.

  L'objectif est de correspondre les connexions à des règles établies, évaluer leur pertinence et remplacer les règles moins efficaces par de nouvelles règles issues de fusions de règles "bonnes".

Avantages:
- Déclenchement d'alertes pertinentes permettant de détecter le type d'attaque et la vulnérabilité exploitée, ce qui facilite les actions de l'administrateur réseau pour rétablir l'état initial du système.
- Utilisation efficace des ressources, notamment pour les IDS réseaux (NIDS), car ils ne fonctionnent pas sur les machines rendant des services dans le système, minimisant ainsi l'impact sur les performances.
- Facilité de mise en œuvre grâce à la disponibilité de logiciels performants en open source et d'une documentation abondante.

inconvenients:
- ils ne peuvent pas détecter les intrusions non connues, même si elles sont basiques.
- Ils nécessitent une maintenance et une mise à jour constantes pour assurer une protection optimale, ce qui peut être complexe.

Les IDS comportementaux : ont les caractéristiques suivantes :

- Leur objectif principal est la détection des anomalies.
- Ils nécessitent une phase d'apprentissage pendant laquelle l'outil observe le comportement "normal" des flux applicatifs présents sur le réseau.
- Lorsqu'un flux anormal est détecté, l'IDS émet une alerte, mais il ne spécifie pas la gravité de l'attaque.
- Cette approche peut être appliquée non seulement aux utilisateurs, mais aussi aux applications et aux services.
- Plusieurs métriques peuvent être utilisées pour déterminer la normalité du trafic, telles que la charge CPU, le volume de données échangées, le temps de connexion sur des ressources, la répartition statistique des protocoles et applications utilisés, les heures de connexion, etc.

Les approches des IDS comportementaux:

***Approche probabiliste* :** Elle consiste à prédire la probabilité d'un événement en se basant sur la séquence des événements précédents.
Par exemple, si une demande de connexion est suivie d'une requête GET, on peut supposer qu'elle sera suivie d'une réponse HTTP.
Si ce schéma n'est pas respecté, une anomalie est détectée.
Cette approche permet une construction simple et dynamique du profil et réduit les faux positifs, mais elle peut être déformée progressivement par des attaques répétées.

Approche statistique : Cette approche consiste à effectuer des tests sur des éléments tels que l'occupation de la mémoire, l'utilisation des processeurs, la charge réseau, le nombre d'accès à l'Intranet par jour, etc.
Elle permet de détecter des attaques inconnues et d'apprendre automatiquement les habitudes des utilisateurs, mais elle peut être complexe en termes de maintenance et générer de nombreux faux positifs.

Approche immunologique : Cette approche s'inspire du fonctionnement du système immunitaire pour différencier ce qui est considéré comme normal (le "soi") de ce qui ne l'est pas (le "non-soi").
Elle propose de détecter les anomalies en recherchant ce qui est considéré comme malveillant, tout en connaissant ce qui est considéré comme normal.
Elle nécessite une période d'apprentissage prolongée, mais présente l'avantage d'une nouvelle approche basée sur la détection d'anomalies.

Avantages des IDS comportementaux:
- La construction du profil de trafic est simple et dynamique, ne nécessitant pas de configuration complexe.
- Les nouvelles attaques sont directement prises en compte, car il n'y a pas de dépendance sur une base de signatures.
- Cette approche est particulièrement adaptée pour des trafics réguliers où la période d'apprentissage est favorisée, tant en termes de durée que de corrélation des protocoles utilisés.

inconvénients :

- Ils sont sensibles au bruit, ce qui peut entraîner un fort taux de fausses alarmes, rendant le système difficile à utiliser voire inutilisable.
- Les comportements et activités des utilisateurs pendant la phase d'apprentissage peuvent ne pas être suffisamment statiques pour offrir un modèle de comportement normal fiable, ce qui rend l'IDS inefficace.
- Un utilisateur malveillant peut modifier lentement son comportement pour s'adapter au modèle d'apprentissage de l'IDS, rendant les attaques plus difficiles à détecter.
- il est possible que le système subisse une attaque pendant la phase d'apprentissage, ce qui peut compromettre l'efficacité de l'IDS.

Criteres du choix d'un outil IDS:

1. Fiabilité :générant des alertes justifiées et en ne laissant aucune intrusion passer inaperçue.

2. Réactivité : L'IDS doit être capable de détecter rapidement les nouveaux types d'attaques. Il doit être constamment mis à jour et disposer de capacités de mise à jour automatique.

3. Facilité de mise en œuvre et adaptabilité : doit être facile à déployer et à configurer, s'adapter au contexte spécifique dans lequel il sera utilisé (matériel, réseau, etc.).

4. Performances : L'IDS ne doit pas impacter négativement les performances des systèmes surveillés. Il doit être capable de traiter efficacement toutes les informations à sa disposition.

5. Multi-canal :émettre des alertes via plusieurs canaux (email, pager, téléphone, fax, etc.) pour garantir la réception des alertes par les responsables de sécurité.

6. Information : L'IDS devrait fournir un maximum d'informations sur les attaques détectées, pour permettre une réponse efficace.

7. Classification : Il devrait être possible de classer la gravité des attaques détectées, afin de pouvoir adapter les mesures de réponse en fonction de leur importance.

Exemple d'un IDS:
SNORT est l'un des IDS les plus populaires avec plus de 2 millions de téléchargements.
Il offre des mises à jour en temps réel pour une réactivité élevée, ainsi qu'une architecture modulaire qui peut être personnalisée.
SNORT dispose d'un décodeur de paquets intégré pour analyser le trafic réseau. Il est largement utilisé pour la détection d'intrusion et la surveillance du trafic réseau.

Nom de l'IDS	HIDS	NIDS	Comportementale	Scénario	Payant	Libre
Attack Mitigator		X		X	X	
BlackIce		X		X	X	
Bro		X		X		X
Cisco IPS				X	X	
Dragon		X		X	X	
Prelude-IDS	X	X		X		X
SNORT		X	X	X	X	X

Chapitre: SANDBOXING

Definition: Le sandboxing est un module de sécurité récent qui analyse les fichiers entrants (emails, téléchargements, sites web) avant qu'ils n'interagissent avec les systèmes de l'entreprise, permettant ainsi une meilleure détection des malwares et une prévention des infections.

Fonctionnement:
- Le sandboxing exécute les fichiers suspects dans un environnement virtuel isolé.
- Il observe le comportement du fichier pour détecter les actions malveillantes.
- Si le fichier se comporte normalement, il est considéré comme sûr.
- Si le fichier effectue des actions suspectes, il est identifié comme une menace.
- En utilisant la sandbox, les menaces sont contenues et ne peuvent causer de dommages.
- Les sandboxes sont personnalisables et peuvent être dimensionnées selon les besoins de l'entreprise.
- Le processus de test dans la sandbox est généralement rapide (environ cinq minutes).
- Les techniques d'évitement utilisées par les pirates sont connues et contournées par les sandboxes.
- Les sandboxes peuvent accélérer virtuellement le temps pour contrer les actions malveillantes programmées avec un délai.

Notes:
- Le sandboxing est une technologie efficace et de plus en plus accessible grâce à la virtualisation et au cloud.
- Son coût d'entrée est réduit et la gestion de la puissance de traitement est externalisée grâce au cloud.
- Le sandboxing peut être utilisé sur des clouds publics, privés ou en configuration locale pour une isolation totale.
- Il complète d'autres mesures de sécurité telles que l'antivirus, le firewall, l'IPS, le filtrage web, etc.
- La sandbox travaille en coordination avec l'antivirus pour une protection plus complète.
- Certaines techniques de détection des sandbox sont intégrées dans les agents de protection avancés des postes utilisateurs ou serveurs.

impplementation de sandbox:

- commence par la définition des besoins, tels que les flux à surveiller et les environnements à virtualiser.
- Il est possible de configurer des règles pour le traitement des fichiers douteux et définir le niveau de sensibilité.
- L'implémentation prend moins d'une heure pour une version de sandbox dans le cloud et quelques jours pour une configuration sur site.
- Le coût de l'implémentation dépend de la puissance et de la capacité de traitement de la sandbox.

- Le cloud a contribué à rendre le sandboxing plus abordable, contrairement à sa réputation passée de technologie coûteuse.

obfuscation de code: *(rendre le code source ou le programme plus difficile à comprendre ou à analyser)*

Le mécanisme viral :
stratégies utilisées par les virus informatiques pour se propager et infecter les systèmes. Cela inclut l'obfuscation de code, la furtivité et le polymorphisme.

L'obfuscation : rendre le code viral difficile à comprendre en utilisant des transformations pour le rendre plus complexe. Cela complique la détection et l'analyse par les antivirus.
La furtivité permet aux virus de se cacher et de se déplacer discrètement sur les systèmes infectés pour éviter la détection.
Le polymorphisme permet aux virus de modifier leur structure et leur code à chaque infection, rendant difficile leur identification par des signatures uniques.

le mécanisme cryptographique:
utilise des techniques de cryptographie dans le contexte des infections informatiques.
Il protège les clés de chiffrement et le contenu du virus en les chiffrant .
Cela rend la compréhension et l'analyse du code viral plus difficiles.
Les techniques cryptographiques sont utilisées pour assurer la confidentialité des clés et empêcher leur utilisation non autorisée.

(le mécanisme viral se concentre sur les stratégies de propagation des virus, le mécanisme cryptographique utilise des techniques de cryptographie pour protéger le code viral et ses éléments clés contre la détection et l'analyse.)

Chapitre: HONEYPOTS

honeypot est un ordinateur ou un programme volontairement vulnérable destiné à attirer et à piéger les pirates informatiques.

Types de honeypots:

Honeypots de production :
- Utilisés pour sécuriser un réseau opérationnel en déroutant les attaques des services de production vers le honeypot.
- Renforcent la sécurité en complément des autres mécanismes de sécurité tels que les firewalls et les IDS.
- Permettent la détection d'attaques grâce aux fichiers d'audit, qui peuvent également être utilisés pour corriger les vulnérabilités.
- Rôle dans la protection du système : prévention (attirer les attaquants vers le honeypot au lieu des systèmes de production), détection (toute connexion avec le honeypot est

considérée comme une tentative d'intrusion) et recouvrement (offrent une continuité des services après une attaque, fournissent des informations pour la récupération du système).

Honeypots de recherche :

- Utilisés pour étudier et comprendre les techniques et l'évolution de la communauté des hackers.
- Plus complets que les honeypots de production, le système entier peut être attaqué.
- Offrent des renseignements précieux sur les attaquants et leur comportement.
- Aident les professionnels de la sécurité informatique à améliorer les méthodes et mécanismes de protection en fournissant une meilleure connaissance de la communauté des hackers.

les honeypots de production sont utilisés pour sécuriser un réseau opérationnel en déroutant les attaques, tandis que les honeypots de recherche sont utilisés pour étudier les techniques des hackers et fournir des informations pour améliorer la sécurité.

Classification des "honeypots" :

1. Honeypots à faible interaction :
- Interaction limitée avec les attaquants, simulant les services d'un système réel mais en enregistrant simplement les paquets reçus.
Avantages : Facilité de déploiement, gestion simplifiée des journaux, conservation de la sécurité du système.
Inconvénients : Facilité de détection par les attaquants en raison de réponses incomplètes, peu d'informations sur l'attaquant.
Utilisation principale : Détection des tentatives de connexion non autorisées.
Exemples : Honeyd, Specter.

2. Honeypots à moyenne interaction :
- Simulation améliorée des services avec la capacité de renvoyer des réponses aux attaquants, généralement fausses.
- Offre également quelques services réels mais sans permettre à l'attaquant de prendre le contrôle total du système.
Avantages : Gestion des journaux plus facile, fourniture d'informations intéressantes pour l'analyse.
Inconvénients : Difficulté de mise en œuvre en termes de développement, risque de sécurité accru.
Utilisation principale : Fournir des informations supplémentaires pour l'analyse des attaques.
Exemples : homemade honeypots, Deception Toolkit.

3. Honeypots à haute interaction :
- Utilisation d'un véritable système d'exploitation avec de réelles failles de sécurité pour une interaction étroite avec l'attaquant.
- Utilisés principalement dans la recherche pour observer les activités des pirates.

Avantages : Difficulté de détection par les pirates, fourniture d'informations détaillées sur les activités des attaquants.
Inconvénients : Risque élevé pour le système hôte, gestion complexe des journaux.
Utilisation principale : Observation approfondie des activités des pirates.
Exemples : Honeynet CDROM ROO, ManTrap.

Architecture des "honeypots" :

1. Architecture réelle :
- Chaque honeypot est installé sur sa propre machine physique, représentant un système réel.
Avantages : Administration simplifiée.
Inconvénients : Nécessite plusieurs machines physiques pour plusieurs honeypots, surveillance complexe sans être détecté, réinstallation fréquente du système.

2. Architecture virtuelle :
- Le honeypot est installé sur une machine virtuelle, créée à l'aide d'outils de virtualisation tels que VMWare, UML (User-Mode-Linux) ou Jail.
- Les machines virtuelles permettent d'émuler un ou plusieurs systèmes sur une seule machine physique, permettant d'installer plusieurs honeypots virtuels.
Avantages : Sécurité de la machine virtuelle, économie de machines physiques, facilité de monitoring en temps réel, facilité de réinstallation par sauvegarde des disques virtuels, invisibilité du système hôte pour les pirates.
Inconvénients : Charge importante sur le système hôte, restriction du choix des systèmes virtuels compatibles.

Chapitre : DAC et MAC

Discretionary Access Control/ Mandatory Access Control

les contrôles d'accès discrétionnaires (DAC) utilisent les notions de propriété et de droits d'accès pour restreindre l'accès aux objets.
-Les sujets peuvent conférer des droits d'accès à d'autres utilisateurs, mais cela nécessite une confiance envers les utilisateurs du système.
- Les politiques DAC ne peuvent pas garantir l'interdiction d'accès à un objet pour un sujet et ne peuvent pas contrôler les canaux cachés de stockage utilisés par les chevaux de Troie.

Modeles DAC:

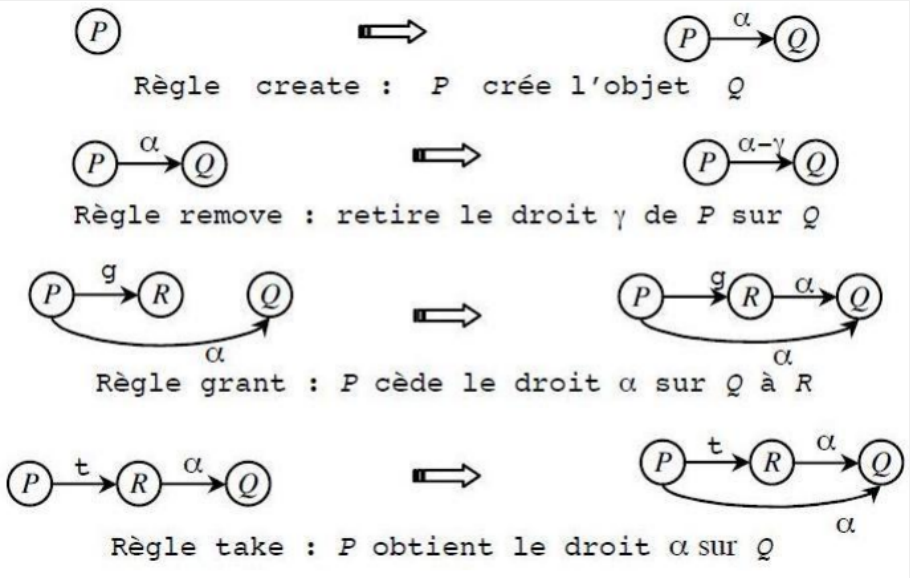
Modele de lampson:
-le modèle de Lampson utilise une matrice de contrôle d'accès pour représenter les droits d'accès des sujets sur les objets.
-il présente des limitations en termes de mise à jour des autorisations et ne permet pas d'exprimer directement des interdictions ou des obligations. Il a servi de base à d'autres modèles plus avancés tels que HRU et Take-Grant.

Modèle HRU :

-le modèle HRU se concentre sur la vérification des propriétés d'une politique d'autorisation. Il utilise une matrice d'accès et définit des opérations spécifiques.
-Le problème de protection dans HRU peut être indécidable dans le cas général, mais décidable pour les systèmes à mono-opération.donc il est incapable de couvrir des politiques de sécurité plus complexes,(t la création d'objets et l'attribution de droits spécifiques)

Modèle Take-Grant :

- Le modèle Take-Grant est une évolution du modèle HRU visant à représenter des politiques d'autorisation sophistiquées tout en maintenant la décidabilité du problème de protection.
- Il utilise un graphe où les nœuds représentent des sujets ou des objets, et des règles de modification de ce graphe.
- Les commandes du modèle Take-Grant sont réparties en quatre catégories : create (création d'un objet avec un droit initial attribué à un sujet), remove (retrait d'un droit d'accès d'un sujet sur un objet), take (permet à un sujet de prendre tous les droits d'un autre sujet) et grant (permet à un sujet de céder un droit à un autre sujet).
- Le graphe représentant l'état de protection du système dans ce modèle peut être assimilé à la matrice d'accès, et les règles de réécriture correspondent aux commandes.
- L'application successive de ces règles peut conduire à des états d'insécurité où des sujets obtiennent des droits supplémentaires, compromettant ainsi certains objectifs de sécurité.
- Le modèle Take-Grant permet de définir le prédicat "P can Q", qui est vrai s'il existe une séquence de graphes où P possède le droit sur Q.



Modèle TAM (Typed Access Matrix) :

le modèle TAM utilise des types d'objets et de sujets, ainsi qu'une matrice de contrôle d'accès, pour gérer les autorisations d'accès aux objets. Cela permet de contrôler qui peut faire quoi dans le système informatique.

1. Types d'objets : Dans TAM, chaque objet appartient à un type spécifique qui ne peut pas être modifié. Par exemple, un objet peut être de type "fichier", "dossier" ou "base de données". Les types aident à définir les autorisations d'accès pour les objets.

2. Types de sujets : Les utilisateurs (sujets) sont également associés à des types spécifiques. Par exemple, un utilisateur peut être de type "administrateur", "utilisateur régulier" ou "invité". Les types de sujets déterminent les commandes qu'ils peuvent exécuter sur les objets.

3. Matrice de contrôle d'accès : Pour définir les autorisations d'accès, une matrice de contrôle d'accès est utilisée. Cette matrice relie les types de sujets aux types d'objets et spécifie les droits d'accès pour chaque combinaison sujet-objet. Par exemple, un administrateur peut avoir le droit d'écrire dans un fichier, tandis qu'un invité peut seulement avoir le droit de le lire.

4. Schéma d'autorisation : Le schéma d'autorisation est constitué des droits d'accès, des types d'objets et des types de sujets. Il définit les opérations que les sujets peuvent effectuer sur les objets. Par exemple, les opérations primitives peuvent inclure "lire", "écrire" et "supprimer".

L'objectif principal du modèle TAM est de contrôler l'accès aux objets en fonction des types de sujets et d'objets, en utilisant une matrice de contrôle d'accès. Cela permet de définir des règles de sécurité précises et de gérer les autorisations de manière efficace.

—----------

Le contrôle d'accès obligatoire (MAC)
est un mécanisme de sécurité qui restreint l'accès aux ressources en se basant sur des règles prédéfinies, indépendamment des préférences individuelles des utilisateurs.

Politiques MAC:

La politique de Bell-LaPadula :

1. Niveaux de sécurité : Les informations et les utilisateurs sont classés en différents niveaux de sécurité. Par exemple, les informations peuvent être classées comme "non classifiées", "confidentielles" ou "secrètes", et les utilisateurs peuvent avoir des habilitations correspondantes.

2. Règle de la propriété simple : Selon cette règle, un utilisateur ne peut accéder à une information que si son niveau de sécurité est égal ou supérieur à celui de l'information. En

d'autres termes, un utilisateur classifié comme "confidentiel" ne peut pas accéder à des informations classifiées comme "secrètes".

3. Règle de la propriété étoile : Cette règle interdit la divulgation d'informations d'un niveau de sécurité élevé vers un niveau de sécurité inférieur. Par exemple, un utilisateur classifié comme "confidentiel" ne peut pas écrire dans un document classifié comme "non classifié", car cela pourrait permettre la divulgation d'informations confidentielles.

L'objectif principal de cette politique:

- éviter les fuites d'informations sensibles
- garantir que seules les personnes autorisées y ont accès.
- cette politique vise à empêcher les utilisateurs d'accéder à des informations pour lesquelles ils n'ont pas les autorisations nécessaires et à éviter la divulgation d'informations sensibles à des niveaux de sécurité inférieurs.

La politique d'intégrité de Biba: vise à prévenir la propagation d'informations vers des niveaux d'intégrité supérieurs et à empêcher les modifications non autorisées des objets.
-Elle utilise des labels d'intégrité et des règles d'autorisation pour garantir la protection de l'intégrité des informations.

1. Objectifs de sécurité *:* Les objectifs principaux de cette politique sont les suivants :
- Empêcher la propagation d'informations d'un objet à un niveau d'intégrité inférieur vers un objet à un niveau d'intégrité supérieur.
- Empêcher tout sujet à un certain niveau d'intégrité de modifier un objet à un niveau d'intégrité supérieur.

2. Schéma d'autorisation : Le schéma d'autorisation repose sur des labels d'intégrité et des classes d'opérations. Les classes d'opérations comprennent l'observation, la modification et l'invocation.
- Un sujet ne peut modifier un objet que si son label d'intégrité domine le label d'intégrité de l'objet.
- Un sujet ne peut observer un objet que si le label d'intégrité de l'objet domine le label d'intégrité du sujet.
- Un sujet ne peut invoquer un autre sujet que si le label d'intégrité du sujet émetteur domine le label d'intégrité du sujet cible.

3. Protection contre la pollution : Ces règles garantissent qu'une information à un niveau d'intégrité inférieur ne peut pas "polluer" une information à un niveau d'intégrité supérieur. Ainsi, les modifications non autorisées de l'information sont empêchées.

4. Dégradation des niveaux d'intégrité : Un inconvénient de la politique de Biba est similaire à celui de Bell-LaPadula. Si une information à un certain niveau d'intégrité est utilisée par un sujet à un niveau inférieur, tous les objets modifiés ou créés par ce sujet auront un niveau d'intégrité inférieur. Il peut être nécessaire de remonter artificiellement le niveau d'intégrité de certains objets par des sujets "de confiance" pour permettre leur accès.

La politique de Clark et Wilson: vise à assurer deux besoins principaux :

1. Cohérence des données : maintenir la cohérence des données à l'intérieur du système informatique. les données doivent être conformes aux règles et procédures spécifiques pour préserver leur intégrité.

2. Cohérence avec le monde réel ; Cela implique que les procédures informatiques doivent correspondre aux procédures du monde réel, et les opérations de transformation doivent être contrôlées et validées.

Les principes clés de la politique de Clark et Wilson sont les suivants :

1. Transactions bien formées : Les utilisateurs ne sont pas autorisés à manipuler les données de manière arbitraire. Ils doivent utiliser des procédures de transformation spécifiques qui préservent l'intégrité des données.
Par exemple, une opération de transformation doit respecter les principes comptables pour assurer l'intégrité des données financières.

2. Séparation des pouvoirs : Ce principe consiste à répartir les opérations entre différentes parties et à attribuer des droits différents mais complémentaires à différentes catégories de personnes.
Par exemple, dans certaines entreprises, l'achat d'une marchandise nécessite l'intervention du service commercial, du service de contrôle et du service financier, assurant ainsi une vérification croisée pour éviter les fraudes et les erreurs.

(En résumé, la politique de Clark et Wilson vise à maintenir la cohérence et l'intégrité des données, en utilisant des procédures de transformation certifiées et en appliquant le principe de séparation des pouvoirs. Elle sépare les données en données contraintes et non contraintes, et met en place des mécanismes de contrôle et de certification pour garantir la sécurité du système.)

Chapitre :RBAC et OrBAC

RBAC (Role-Based Access Control) et ORBAC (Organizational-Based Access Control) sont deux modèles de contrôle d'accès largement utilisés dans la sécurité informatique pour gérer les autorisations d'accès aux ressources.

1. RBAC (Role-Based Access Control):

- RBAC repose sur l'attribution de rôles aux utilisateurs et sur la définition des autorisations associées à ces rôles.
- Les utilisateurs se voient attribuer des rôles en fonction de leurs responsabilités ou de leurs fonctions au sein de l'organisation.
- Les autorisations d'accès sont définies au niveau des rôles plutôt qu'au niveau des utilisateurs individuels.

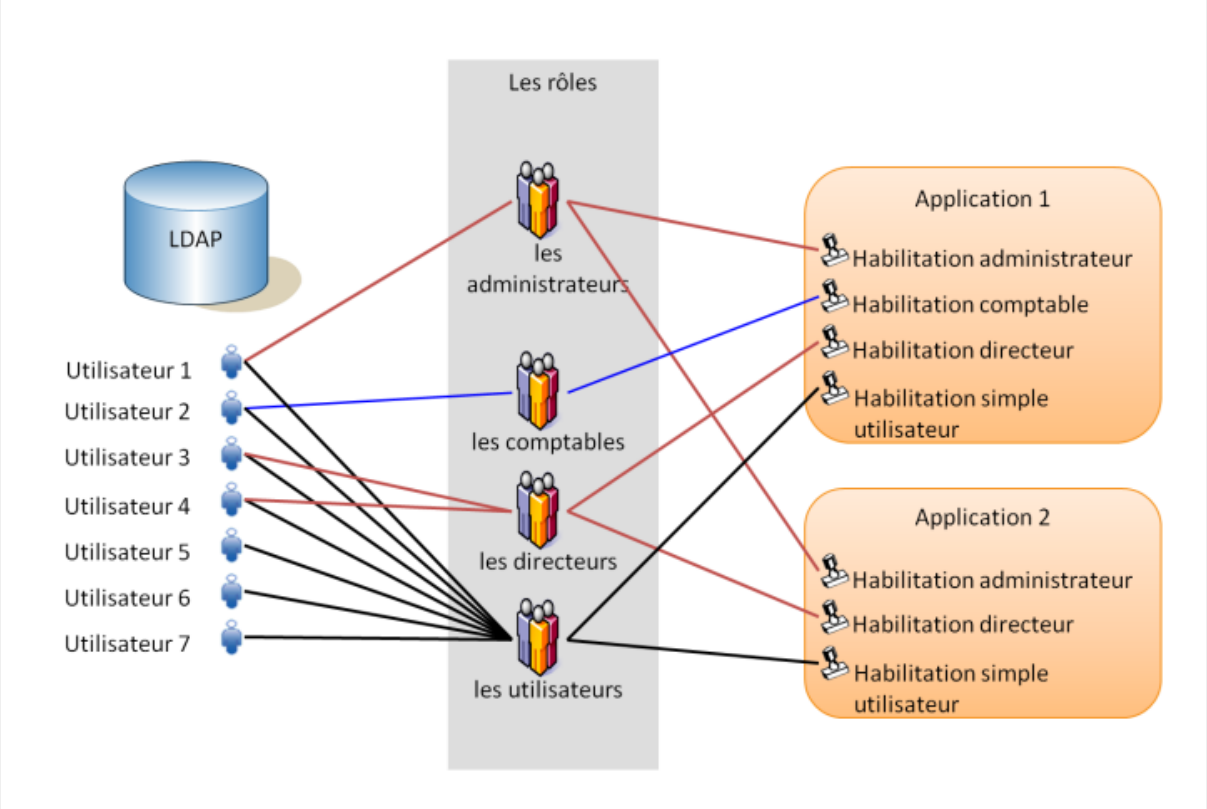
- Cela simplifie la gestion des autorisations en permettant d'attribuer, de modifier ou de révoquer des droits d'accès en fonction des rôles plutôt que des utilisateurs spécifiques.

Contraintes:

1. Séparation des droits : Dans la plupart des organisations, un individu n'est pas autorisé à être membre de deux rôles simultanément. Cette contrainte garantit une séparation claire des droits entre les différents rôles, évitant ainsi les conflits d'intérêts et les autorisations inappropriées.

2. Contrainte de cardinalité : Cette contrainte concerne à la fois les rôles et les membres. Elle spécifie qu'un rôle peut avoir un nombre maximum de membres, par exemple, un seul individu peut occuper le rôle de "chef de département". De plus, un individu peut être limité à un nombre restreint de rôles auxquels il peut appartenir.

L'hiérarchie de rôle peut aussi être considérée comme une contrainte



Avantages :

- RBAC permet aux utilisateurs d'effectuer un large éventail d'opérations et offre une grande souplesse et flexibilité d'application.
- Il permet le contrôle des actions des utilisateurs en définissant les rôles, la hiérarchie des rôles, les relations et les contraintes.

Inconvénients :

- Le modèle RBAC atteint rapidement ses limites lorsque les utilisateurs sont géographiquement dispersés ou lorsque l'entreprise est composée de services indépendants.

- Par exemple, dans une société de services, un commercial attaché à un secteur spécifique ne peut pas effectuer des actions pour un client dans un autre secteur.
- De même, un conseiller clientèle d'une banque peut avoir des droits de gestion de patrimoine et de gestion immobilière, mais l'étendue de ses droits dépend de l'agence dans laquelle il travaille. Dans une agence donnée, il peut n'avoir que les droits de gestion immobilière, tandis que dans une autre agence, il peut avoir à la fois les droits de gestion de patrimoine et de gestion immobilière.

Ces limitations montrent que le modèle RBAC peut présenter des difficultés lorsque des distinctions géographiques ou des structures organisationnelles particulières sont impliquées.

2. ORBAC (Organisational-Based Access Control):

- ORBAC étend le modèle RBAC en prenant en compte les structures organisationnelles et hiérarchiques des entreprises.
- Il permet de définir des règles d'accès basées sur les relations organisationnelles, telles que les départements, les groupes de travail ou les relations de supervision.
- Les autorisations sont attribuées en fonction de l'appartenance à des unités organisationnelles spécifiques ou à des relations de supervision.
- ORBAC permet une gestion plus flexible des autorisations, en tenant compte des changements dans la structure organisationnelle sans avoir à modifier les autorisations individuelles des utilisateurs.

Contexte:

L'OrBAC utilise des contextes pour exprimer des permissions ou des interdictions dans certaines circonstances spécifiques. :

1. Contexte temporel : Il régule la durée de validité des privilèges accordés.
2. Contexte spatial : Il peut être lié à l'appartenance à un réseau, à la position géographique ou à toute autre situation spatiale.
3. Contexte déclaré par l'utilisateur : Ce type de contexte est activé par l'utilisateur lui-même dans des situations exceptionnelles, telles qu'une urgence médicale ou une demande d'audit. Dans ces cas, des permissions spécifiques peuvent être accordées même si elles sont normalement interdites.
4. Contexte prérequis : Ils permettent de contraindre les sujets concernés par les permissions en fonction de certains contextes, ce qui peut étendre ou restreindre les droits d'accès hérités du rôle associé.
5. Contexte provisionnel : Il permet d'accorder des privilèges en fonction de l'historique. Par exemple, un contexte "accès limité à 2 fois" peut vérifier si un document a été consulté au moins 2 fois.

L'utilisateur qui déclare un contexte doit également fournir un compte-rendu des opérations effectuées et des raisons qui ont motivé la déclaration de ce contexte.

Hierarchie de role:
Il existe deux façons de définir la hiérarchie de l'héritage :

1. Hiérarchie organisationnelle : Un rôle R1 est considéré comme un rôle supérieur (senior) par rapport à un rôle R2 s'il existe une relation hiérarchique supérieure-inférieure entre les utilisateurs jouant ces rôles. Par exemple, si un utilisateur occupant le rôle R1 est le supérieur hiérarchique d'un utilisateur occupant le rôle R2, alors R1 est considéré comme un rôle senior de R2.

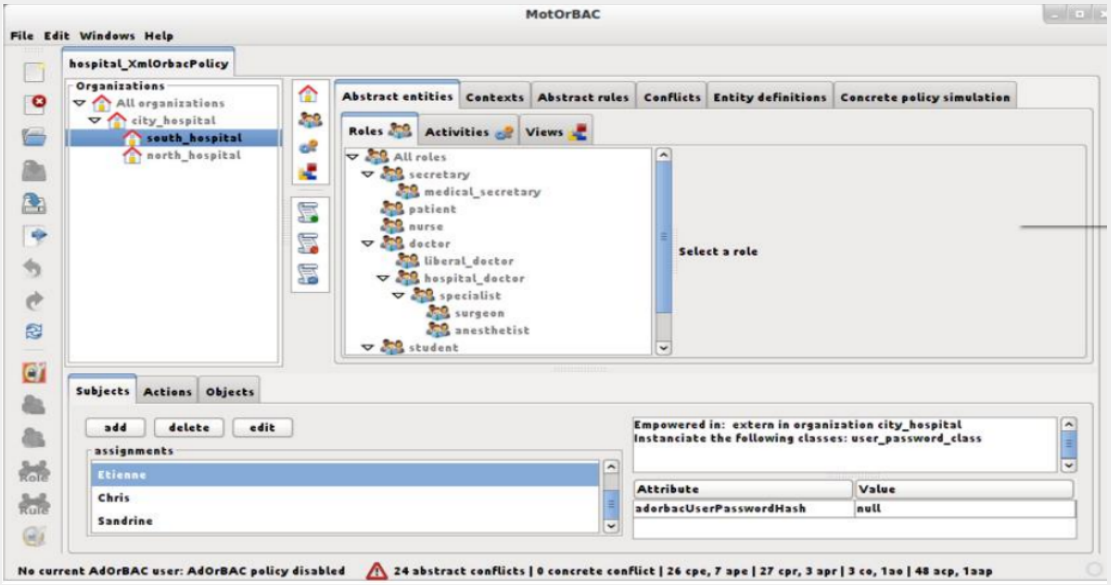
2. Hiérarchie de spécification/généralisation : Une hiérarchie est établie en spécifiant que chaque fois qu'un utilisateur joue le rôle R1, il joue également le rôle R2. Ainsi, R1 est considéré comme un rôle supérieur (senior) de R2. Cela signifie que chaque fois qu'un utilisateur se voit attribuer le rôle R1, il hérite également des permissions associées au rôle R2.

Par exemple, si nous prenons la hiérarchie présentée dans le schéma, où le rôle de chirurgien est également un rôle de médecin, cela signifie que chaque fois qu'un utilisateur est associé au rôle de chirurgien, il joue également le rôle de médecin. Le rôle de chirurgien est donc considéré comme un rôle supérieur (senior) par rapport au rôle de médecin, ce qui implique que le rôle de chirurgien hérite des permissions attribuées au rôle de médecin.

Délégation:
• La délégation permet de donner à un utilisateur particulier un privilège, sans donner ce privilège à toutes les personnes ayant le même rôle que lui.

MotOrBAC:

- est un prototype d'outil de saisie de la politique de sécurité abstraite qui permet de définir une politique de sécurité basée sur le modèle OrBAC.
- Il offre la possibilité de créer des organisations, des rôles, des activités, des vues, des contextes et les règles qui leur sont associées.
- MotOrBAC permet également de simuler la politique en saisissant les sujets, les actions et les objets liés à la politique.



summary

Chapitre :malwares

virus , vers , trojans, spywares, adwares, spams, phishing, ransoms, hoaxes,backdoors, dialers

—----------

Chapitre: firewalls

- Definition
- interet ,
- zone dematerialisé
- Filtrage de paquet (stateful , stateless, proxy)
- Traduction & redirection d'adresse
- NAT
- Limites de firewalls

—----------

Chapitre : IDS

- Definition
- Classification (*par signature* : systeme expert , pattern matching , algo genetique
  par comportement : probabiliste, statistique , immunologique)
- Criteres de choix d'un IDS :(fiabilité , reactivité,adaptabilité, performance,multicanale,information et classification)

—----------

Chapitre: sandboxing

- Definition
- Fonctionnement
- Implementation
- Obfuscation de code (**virale**: polyorphisme , obfuscation,furtivité , **cryptographique**)

—----------

Chapitre : honeypots

- Definition
- Types (de production , de recherche)
- Classification (faible ,moyenne et haute interaction)
- architecture(réelle et virtuelle)

—----------

Chapitre: DAC&MAC

- Definitions
- Modeles DAC (lampson ,HRU , take grant, TAM)
- Politiques MAC(bell-lapadula ,biba,clark et wilson)

—----------

Chapitre :RBAC & ORBAC

- **RBAC :**
  Contrainte (separation de droits , cardinalité , hiérarchie)
- **ORBAC:**
  -Contextes (temporelle , spatial ,déclaré par utilisateur , prérequis, provisionnel)
  -Hierarchie de role (organisational ,specification/ generalisation)
  -Delegation
  -MotORBAC
