Réseaux avancés et sécurité

Sidi Biha

SupNum

2023-2024

Protection informatique

- Ensemble de techniques et systèmes pour se prémunir contre les attaques informatique.
- Les systèmes de protection informatique les plus connus sont :
  - Les Antivirus
  - Les Firewalls
  - Les systèmes de détection (et prévention) d'intrusion (IDS)

Antivirus

- Logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (virus, vers, . . .)
- Signature : un programme malveillants possède une ou plusieurs empreintes.
- Lorsqu'un fichier infecté est détecté, il peut être :
  - Supprimer totalement.
  - Supprimer le code malicieux.
  - Déplacer en quarantaine pour un traitement futur.

Antivirus : fonctionnement

- Un Antivirus vérifie :
  - fichiers et courriers électroniques
  - secteurs de démarrage
  - mémoire/RAM de l'ordinateur
  - médias amovibles (clefs USB, CD, DVD, etc...)
  - données transmises sur le réseau

Antivirus : fonctionnement

- Différentes méthodes de détections de programme malveillant.
  - Approche classique : se concentrent sur les fichiers et comparent la signature virale au contenu du fichier.
    - Taux de détection limitée.
  - Approche par heuristique : tend à découvrir un code malveillant par son comportement.
    - plus puissante.
    - Peut générer des de fausses alertes false positives.
  - Approche par filtrage : basée sur des expressions régulières.
    - efficace pour les serveurs de messageries, pour la détection de spam ou phishing...

Antivirus : techniques

- **Scanning des empreintes (signatures)** : la détection des virus consiste à la recherche de signatures à partir d'une base de données de définitions de virus.
  - Avantage : permet de détecter le virus avant son activation.
  - Inconvénient : il est nécessaire que la signature soit connue. De plus, la base doit être toujours à jour.
- **Liste blanche (Whitelisting)** : au lieu de rechercher les logiciels connus comme malveillants, on empêche l'exécution de tout logiciel à l'exception de ceux qui sont considérés comme fiables par l'administrateur système.
  - De plus en plus utilisée pour lutter contre les logiciels malveillants.
  - Difficile d'un point de vue administration

Antivirus : techniques

- **Analyse de comportement** : contrôler/vérifier en continu toute les activités suspecte.
  - Exemple d'activités suspecte :
    - lectures et écritures dans des fichiers exécutables
    - tentatives d'écriture dans les secteurs de partitions et de boot du disque.
  - Peut réduire les ressources disponible de la machine
- **Contrôle d'intégrité** : maintenir une liste des fichiers exécutables associés à leur taille, leur date de création, de modification, voire un hash.
  - Ceci permet de vérifier qu'un exécutable n'a pas été modifié avant et après son exécution.
  - Efficacité limitée aux virus modifiant du contenu sur disque.

Antivirus : techniques

- **Analyse heuristique** : détecter les virus avant leur exécution.
  - Analyse statique : recherche dans le code des commandes suspectes, typiques pour les programmes malveillants, par exemple, recherche et modification des fichiers exécutables.
  - Analyse dynamique : émule le lancement d'un programme dans un espace virtuel spécial (VM, Sandbox). Si une activité suspecte est détectée, le programme est identifié comme malveillant et son lancement est bloqué.

Firewalls

Définition

Logiciel et/ou un matériel permettant de faire respecter la politique de sécurité au niveau réseau.

Objectif principal

Surveiller et contrôler les applications et les flux de données (paquets), en empêchant les connexions non-autorisées sur un réseau.

Firewalls

Deux types de politiques de filtrage :

- **politique restrictive** : ce qui n'est pas explicitement autorisé est interdit (souvent ce qui est mis en place dans les entreprises)
- **politique permissive** : ce qui n'est pas explicitement interdit est autorisé (e. g. les réseaux à la maison, certains réseaux d'université)

Firewalls : types

- **Sans état (stateless firewall)** : regarde chaque paquet indépendamment des autres et le compare à une liste de règles pré-configurées.
- **Avec états (stateful firewall)** : vérifie que chaque paquet est bien la suite d'un précédent paquet et/ou la réponse à un paquet dans l'autre sens.
- **Applicatif** : vérifie la complète conformité du paquet à un protocole attendu.

Firewalls : niveau de filtrage

- **Adresses IP** : accepter les flux de données provenant d'une plage d'adresses, ou d'une seule adresse.
- **Noms de domaine** : bloquer l'accès à certaines adresses Internet.
- **Protocoles** : empêcher tout transfert FTP, tout accès ssh, ou encore pour éviter la navigation sur Internet (HTTP).
- **Ports** : supprimer l'accès FTP en refusant les connexions sur le port 21.
- **Contenu** : refuser la transmission de paquets dont le contenu renferme des séquences de caractères données, expressions régulière.