La sécurité périmétrique

- Introduction

- La sécurité périmétrique est l'ensemble des mécanismes et stratégies visant à protéger les **frontières d'un réseau informatique** contre les intrusions, attaques et accès non autorisés.
- Elle constitue la première ligne de défense dans une architecture de sécurité.

- Avec la généralisation du cloud, du télétravail et des objets connectés, la notion de périmètre devient plus complexe et nécessite une approche **multi-couches**.

La sécurité périmétrique

- **Périmètre réseau** : zone frontière séparant un réseau interne (de confiance) d'un réseau externe (non fiable, comme Internet).
- **Objectif** : contrôler et filtrer le trafic entrant et sortant, détecter les menaces, et réduire la surface d'attaque.
- **Principe clé : « Trust but verify »** – autoriser uniquement ce qui est explicitement nécessaire, tout le reste est bloqué.

Les principaux mécanismes de sécurité périmétrique

- **Les pare-feu (Firewalls)**
- **Rôle** : filtrer les paquets selon des règles prédéfinies.
- Types :
  - **Pare-feu statique (packet filtering)** : contrôle basique sur adresses IP, ports, protocoles.
  - **Pare-feu dynamique / Stateful Inspection** : garde l'état des connexions pour décider si un paquet est légitime.
  - **Next Generation Firewall (NGFW)** : inclut des fonctions avancées (filtrage applicatif, détection d'intrusions, VPN, antivirus).
- Exemple : Bloquer tout accès externe au port 3389 (RDP), sauf pour un administrateur via

Les principaux mécanismes de sécurité périmétrique

- Les systèmes de détection et prévention d'intrusions (IDS/IPS)

- **IDS (Intrusion Detection System) :**
  - détecte des activités suspectes (signature, anomalies).

- **IPS (Intrusion Prevention System) :**
  - agit en temps réel pour bloquer l'attaque.

- **Limite :**
  - peuvent générer de faux positifs / faux négatifs, nécessitent un ajustement constant.

Les principaux mécanismes de sécurité périmétrique

- **Les DMZ (Demilitarized Zones)**
  - Zone intermédiaire entre le réseau interne et Internet.
  - On y place les serveurs accessibles **publiquement** (web, mail, DNS).
- **Avantage :**
  - si une machine en DMZ est compromise, l'attaquant n'accède pas directement au réseau interne.

Les principaux mécanismes de sécurité périmétrique

- **Les VPN (Virtual Private Networks)**
- **But :**
  - assurer une communication sécurisée via Internet.
- **Mécanismes :**
  - chiffrement (IPSec, SSL), authentification forte.
- **Exemple :**
  - un employé distant se connecte au réseau de l'entreprise via un tunnel sécurisé.

Les principaux mécanismes de sécurité périmétrique

- **Les proxies et reverse-proxies**

- **Proxy :**
  - agit comme intermédiaire entre utilisateur et Internet, filtrant et journalisant les requêtes.

- **Reverse proxy :**
  - protège les serveurs internes en interceptant et filtrant le trafic entrant (ex : Nginx, HAProxy).

Les principaux mécanismes de sécurité périmétrique

- **Filtrage DNS et Web**
- Empêche l’accès à des sites malveillants ou non autorisés.
- Complément essentiel aux pare-feu et proxies.

Architectures de sécurité périmétrique

- **Architecture en « Bastion »**
  - Une machine fortement sécurisée sert de point d'entrée unique.

- **Architecture en « couches d'oignon »**
  - Superposition de plusieurs mécanismes (pare-feu, IDS, proxy, authentification multifactorielle).
  - Défense en profondeur.

- **Architecture Zero Trust**
  - Remise en question du périmètre classique.
  - Principe :
    - ne jamais faire confiance, même à l'intérieur du réseau.

- Contrôle d'accès basé sur l'identité, le contexte et la conformité des appareils.

Menaces et défis actuel

- **Bypass des pare-feu :**
  - via protocoles tunneling, ports non filtrés.
- **Attaques DDoS :**
  - saturent le périmètre pour empêcher le fonctionnement normal.
- **Shadow IT :**
  - applications ou équipements non autorisés échappant au périmètre.
- **Mobilité et Cloud :**
  - le périmètre devient flou, obligeant à combiner périmétrique et sécurité applicative.

Bonnes Pratiques

- Mettre en place une politique de sécurité stricte (« Deny by default »).
- Segmentation du réseau (VLAN, microsegmentation).
- Surveillance et journalisation du trafic (SIEM).
- Tests réguliers (pentests, red team).
- Mise à jour continue des règles et signatures.
- Sensibilisation des utilisateurs (phishing, BYOD).

Conclusion

- La sécurité périmétrique reste indispensable, mais elle ne suffit plus seule.
- Elle doit être intégrée dans une stratégie globale de défense en profondeur, complétée par des contrôles au niveau des applications, des données et des identités.
- Le futur s'oriente vers le Zero Trust et la sécurité cloud-centric, mais comprendre les bases périmétriques est fondamental pour tout ingénieur en réseaux et sécurité.

Introduction : pourquoi durcir Active Directory ?

- **Active Directory est un composant central dans l'infrastructure Microsoft :**
  - **annuaire des utilisateurs, groupes, contrôleurs de domaine, authentification, etc.**
- **Si un attaquant compromet AD (ou obtient des droits élevés dessus), cela lui donne un contrôle massif sur tout le SI (exfiltration, sabotage, persistance).**
- **L'ANSSI observe que beaucoup d'attaques réussissent par mauvaises pratiques d'administration, par défaut mal configurés ou par cloisonnement insuffisant**
- L'objectif du durcissement est de réduire les chemins d'attaque, limiter l'exposition des objets sensibles, segmenter les fonctions critiques et éviter les escalades de privilèges non contrôlées.

Modèle de tiers / cloisonnement (Tiering)

- **L'un des piliers recommandés est le cloisonnement du SI en niveaux de confiance, souvent appelé « Tier 0 / Tier 1 / Tier 2 » dans le contexte d'AD.**

- **Tier 0 : cœur de confiance** — les ressources les plus critiques (contrôleurs de domaine, comptes de service AD sensibles, comptes d'administration AD).

- **Tier 1** : services métiers, serveurs applicatifs ou de données ayant une valeur métier élevée, mais moins sensibles que le cœur AD.

- **Tier 2** : postes de travail, endpoints, ressources moins sensibles, etc.

Principes de cloisonnement

- Une ressource d'un Tier inférieur ne doit pas pouvoir compromettre un Tier supérieur via des chemins d'attaque directs ;
- on doit analyser et bloquer les chemins d'attaque entre Tiers.
- On applique des politiques de sécurité plus strictes pour le Tier 0, avec un nombre restreint d'interactions autorisées.
- Le cloisonnement ne se limite pas au réseau : il doit être logique, matériel, système et organisationnel.
- Ce cloisonnement est un processus itératif :
  - on commence avec une catégorisation initiale, puis on affine au fil de la détection de nouveaux chemins et des évolutions du SI.

Par exemple : identifier les chemins d'attaque (trajectoires qu'un attaquant pourrait emprunter) comme base pour le cloisonnement.

Analyse des chemins d'attaque

- Pour durcir AD, il faut savoir par où un attaquant pourrait progresser de façon latérale ou verticale.
- L'analyse des chemins d'attaque est donc centrale.
- Types de chemins
  - **Relations de contrôle AD (transitivité)** : si A contrôle B, et B contrôle C, la compromission de A peut permettre la compromission de C.
  - **Exploitation de protocoles AD / Windows légitimes** (RPC, SMB, Kerberos, LDAP) dans un contexte détourné ou mal configuré.
  - **Secrets d'authentification** (mots de passe, hashes, clés), réutilisation de comptes locaux, serviescripteurs d'authentification, etc.
  - **Agents de gestion centralisée**, services installés, scripts automatisés, etc.
  - **Chemins hors AD**, via infrastructure physique, virtuelles ou cloud, pouvant rétroagir sur AD.

Analyse des chemins d’attaque

- **Étapes de l’analyse**
  - Identification initiale des ressources sensibles (Tier 0 en priorité)
  - Cartographie des relations légitimes entre objets AD / systèmes
  - Détection des liens transitifs ou implicites
  - Évaluation de la difficulté d’exploitation de chaque chemin (coût, conditions, faisabilité)
  - Priorisation des chemins à traiter (ceux les plus exploitables / critiques)
  - Mise en place de mesures pour briser ou atténuer ces chemins
- Cette analyse doit être réévaluée régulièrement lorsque le SI évolue.

Bonnes pratiques d’administration sécurisée

- **L’ANSSI** propose plusieurs recommandations sur la façon d’administrer en sécurité un SI reposant sur AD.

- **Séparation des usages :**
  - Séparer les postes bureautiques et les postes d’administration.
  - Ne pas utiliser un compte d’administration pour des usages courants.
  - Ne pas mutualiser les usages d’administration entre Tiers sans mesures de sécurité renforcées.
  - Comptes, postes et méthodes d’administration dédiés pour chaque zone de confiance (Tier) pour éviter les chemins d’attaque inter-Tiers.
  - Mutualisation possible sous conditions, mais avec des contrôles stricts et sans générer de nouveaux vecteurs d’attaque.

- Cette séparation est une condition forte pour le cloisonnement des Tiers.

Gestion des comptes administrateurs locaux

- Les droits de lecture du mot de passe local ne doivent être attribués qu'à des comptes du même Tier ou d'un Tier supérieur.
- Si LAPS n'est pas utilisable, chaque mot de passe local doit être unique, complexe, et stocké dans un coffre-fort sécurisé.
- Délégation d'administration
- Ne pas utiliser des comptes Tier 0 pour des tâches d'administration courantes sur Tier 1 ou Tier 2.
- Déléguer les tâches d'administration à des comptes de Tiers moindres via délégation fine, groupes AD, ACLs, etc.
- Utiliser le modèle RBAC (Role-Based Access Control) pour assigner des permissions selon des rôles ou groupes plutôt qu'aux comptes individuels.
- Pour PowerShell, recourir à JEA (Just Enough Administration) pour limiter les cmdlets/actions possibles selon le profil d'administrateur.

Politique de mot de passe et MFA (authentification forte)

- Pour les comptes à privilèges, l'usage de l'authentification multifacteur (MFA) est fortement encouragé.
- Appliquer des politiques de mot de passe robustes (longueur, complexité, renouvellement) selon le contexte de risque.
- Ne jamais exposer les comptes administrateurs via des accès externes sans contrôle renforcé.

Durcissement système / logiciel

- **Le durcissement (hardening)** consiste à paramétrer les systèmes et logiciels pour réduire les vulnérabilités.

- Principes généraux :
  - Activer les fonctions de sécurité natives (audit, contrôle d'accès, chiffrement) des systèmes et services utilisés.

  - Désactiver les services non nécessaires, ports ouverts inutiles, modules superflus.

  - Appliquer régulièrement les correctifs de sécurité (patch management).

  - Ne pas recourir à des configurations affaiblissantes, même si elles sont souvent présentes par défaut.

  - Surveiller et corriger les configurations AD sensibles (ex : attributs DsHeuristics, réglages LDAP anonymes).

Durcissement du Tier 0 prioritaire

- Le Tier 0 doit bénéficier d'un durcissement maximal car c'est le cœur de confiance.
- Réduire l'exposition des contrôleurs de domaine :
  - limiter les services, applications et agents installés dessus.
- Réduire la surface d'attaque par les agents de gestion centralisée, scripts, services tiers sur les contrôleurs.
- Restreindre les flux réseau externes vers les contrôleurs AD.
- Contrôler les accès physiques aux serveurs ; isolation physique et logique renforcée.

Délégation fine des droits et principe de moindre privilège

- **Le principe de moindre privilège est fondamental :**
  - donner uniquement les droits strictement nécessaires pour une tâche, rien de plus.
- Les comptes à haut privilège (Tier 0) doivent être utilisés rarement et uniquement pour des tâches critiques (extensions de schéma, relations d'approbation, etc.)
- Le reste des tâches doit être délégué à des comptes de Tier 1 ou Tier 2 via des droits bien définis.
- Pour la délégation, privilégier l'attribution de droits via des groupes plutôt qu'au niveau compte individuel.
- JEA en PowerShell peut limiter les capacités des administrateurs (modules, cmdlets, scripts) pour réduire les risques liés à l'exécution arbitraire de commandes.

Journalisation et détection

- La journalisation et la détection ne sont pas directement du durcissement, mais elles sont essentielles pour repérer les attaques ou tentatives de contournement.

- L'ANSSI a aussi publié un guide dédié à la journalisation en environnement AD (paramétrage Windows, Sysmon, collecte centralisée)

Remédiation du Tier 0

- Lorsqu'une compromission est avérée ou suspectée, l'ANSSI conseille :
- Identifier les pilliers conceptuels de la remédiation pour AD Tier 0.
- Réinitialiser ou remplacer les objets compromis, couper les chemins d'attaque identifiés, restaurer l'intégrité des contrôleurs de domaine, valider les ACL, les comptes sensibles et les configurations critiques.
- Reprendre le contrôle du cœur AD, puis étendre la remédiation progressivement aux zones moins sensibles une fois la confiance restaurée.
- Effectuer une refonte (si nécessaire) du cloisonnement, des comptes et des droits après l'incident pour éviter une récidive.

Synthèse & conclusion

- Le durcissement d'Active Directory est critique car AD est un point de rupture puissant dans les infrastructures Microsoft.
- Le cloisonnement en Tiers, l'analyse des chemins d'attaque, la séparation des usages, le durcissement des systèmes, la délégation fine et la journalisation/détection constituent les volets majeurs du durcissement selon l'ANSSI.
- Ces mesures doivent être mises en place dans une démarche itérative, adaptée au contexte de l'organisation (taille, maturité, contraintes) et réévaluées à chaque évolution du SI.