AYI NEDJIMI Consultants

Livre Blanc Détaillé : Guide Pratique Cybersecurite

Catégorie : Livres Blancs Lecture : 7 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

Guide complet et détaillé pour 2025 sur la sécurisation d Livre Blanc Détaillé : Sécuriser Active Directory. Expert en cybersécurité et.

Livre Blanc

Sécuriser Active Directory : Guide Complet Contre les Attaques Modernes (Édition 2025)

En 2025, l'Active Directory, qu'il soit sur site (on-premise) ou hybridé avec Microsoft Entra ID (anciennement Azure AD), reste la cible numéro un des attaquants une fois à l'intérieur d'un réseau. Ce guide détaillé a pour but de démystifier les techniques d'attaque les plus courantes et de vous fournir une feuille de route claire pour renforcer la sécurité de votre annuaire. Guide complet et détaillé pour 2025 sur la sécurisation d Livre Blanc Détaillé : Sécuriser Active Directory. Expert en cybersécurité et. Ce guide technique sur livre blanc securite active directory s'appuie sur des retours d'expérience terrain et des méthodologies éprouvées en environnement de production. Nous abordons notamment : sécuriser active directory : guide complet contre les attaques modernes (édition 2025), chapitre 1 : reconnaissance, la phase fondamentale de la compromission et chapitre 2 : les techniques d'attaque sur les identifiants. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Chapitre 1 : Reconnaissance, la phase fondamentale de la compromission

La première action d'un attaquant est de comprendre l'environnement. Par défaut, l'AD est permissif : tout utilisateur authentifié peut énumérer une quantité massive d'informations via le protocole LDAP. C'est le fondement de la technique **T1087.002 (Domain Account Discovery)** du framework MITRE ATT&CK.

Des outils comme **PowerView**, **SharpHound** (le collecteur de données pour BloodHound), ou même des commandes PowerShell natives, permettent de collecter des informations sur :

- Les utilisateurs et leurs attributs (descriptions, appartenances à des groupes).
- Les groupes à privilèges (Admins du Domaine, Admins de l'Entreprise, etc.).
- Les ordinateurs et leurs systèmes d'exploitation.
- Les politiques de mots de passe du domaine.
- Les relations de confiance entre domaines.
- Les Listes de Contrôle d'Accès (ACLs) sur les objets critiques.

Ces informations sont ensuite ingérées par **BloodHound**, qui visualise les chemins de compromission. En quelques secondes, l'attaquant sait quel utilisateur standard a des droits sur quel ordinateur, qui est connecté à cette machine, et si cette chaîne mène à un compte à privilèges.

La défense contre cette phase ne consiste pas à bloquer ces requêtes (ce qui est quasi impossible sans casser des fonctionnalités légitimes), mais à réduire la surface d'attaque en nettoyant les permissions qui créent ces chemins d'attaque directs. Un audit régulier de la configuration AD est la seule solution.

Notre avis d'expert

L'approche holistique de la cybersécurité est au cœur de nos publications. Chaque livre blanc traite non seulement les aspects techniques, mais aussi les dimensions organisationnelles, humaines et réglementaires. La sécurité est un problème systémique qui exige des réponses systémiques.

Vos guides de bonnes pratiques sont-ils lus et appliqués par les équipes opérationnelles ?

Chapitre 2 : Les techniques d'attaque sur les identifiants

Kerberoasting (T1558.003)

Cette technique vise les comptes de service utilisés par les applications (ex: un compte pour un service SQL). Si un tel compte a un Service Principal Name (SPN) et, surtout, n'est pas configuré pour utiliser un mot de passe fort, un attaquant peut demander un ticket de service Kerberos (TGS) pour ce compte. Ce ticket est chiffré avec le hash du mot de passe du compte de service. L'attaquant peut alors, hors ligne, tenter de craquer ce hash pour retrouver le mot de passe en clair à l'aide d'outils comme **Hashcat** ou **John the Ripper**. Pour approfondir, consultez Sécurité LLM Adversarial : Attaques, Défenses et Bonnes.

Défense :

- Utiliser des mots de passe longs (plus de 25 caractères, générés aléatoirement) pour tous les comptes de service.
- Utiliser des comptes de service administrés (gMSA) lorsque c'est possible, car Windows gère automatiquement leurs mots de passe complexes.
- Surveiller l'événement de sécurité **4769** sur vos contrôleurs de domaine pour détecter un grand nombre de demandes de TGS depuis une seule source, surtout si le type de chiffrement du ticket est **0x17 (RC4-HMAC)**, qui est plus facile à craquer.

AS-REP Roasting

Similaire au Kerberoasting, cette attaque cible les comptes utilisateurs pour lesquels l'option "Ne pas requérir la pré-authentification Kerberos" est activée. Un attaquant peut demander directement un ticket d'authentification pour cet utilisateur, et la partie chiffrée de la réponse (l'AS-REP) peut être craquée hors ligne pour retrouver le mot de passe.

Défense : Auditez régulièrement votre AD pour trouver les comptes avec cette option activée et désactivez-la, sauf cas d'usage legacy absolument indispensable et documenté.

Pass-the-Hash (T1550.002) & Pass-the-Ticket (T1550.003)

Ces attaques exploitent la manière dont Windows gère les identifiants en mémoire (via le processus LSASS). Au lieu de voler un mot de passe en clair, l'attaquant, déjà présent sur une machine, utilise des outils comme **Mimikatz** pour extraire un hash NTLM ou un ticket Kerberos valide de la mémoire. Il peut ensuite réutiliser ces artéfacts pour s'authentifier sur d'autres systèmes au nom de l'utilisateur, sans jamais connaître le mot de passe. Pour approfondir, consultez Evasion d'EDR/XDR : techniques.

Défense :

- **Segmentation des privilèges (Tiering) :** La mesure la plus efficace. Un administrateur ne doit jamais se connecter avec son compte à privilèges sur une machine moins sécurisée (ex: un poste utilisateur). Cela empêche le vol de ses identifiants.

- **Microsoft LAPS (Local Administrator Password Solution) :** Pour gérer et renouveler aléatoirement les mots de passe des administrateurs locaux des postes de travail et serveurs, empêchant le mouvement latéral avec un seul et même mot de passe.
- **Credential Guard :** Une fonctionnalité de Windows 10/11 et Server 2016+ qui isole le processus LSASS dans un environnement virtualisé pour le protéger, même d'un attaquant avec les droits SYSTEM.
- **Remote Credential Guard :** Pour les connexions RDP, cela empêche les identifiants d'être envoyés au serveur distant, limitant l'exposition.

Votre Active Directory est-il vulnérable à ces attaques ?
La seule façon de le savoir est de le tester. Nos experts simulent ces attaques dans un environnement contrôlé pour identifier vos faiblesses avant que les vrais attaquants ne le fassent.

Demander un audit de sécurité

Chapitre 3 : La persistance, l'objectif ultime de l'attaquant

Une fois qu'un attaquant obtient des privilèges élevés, son objectif est de s'assurer un accès durable et furtif.

Golden Ticket (T1558.001)

C'est le Saint Graal pour un attaquant. Après avoir compromis un contrôleur de domaine, il peut extraire le hash du compte `KRBTGT`. Ce compte est utilisé pour signer tous les tickets Kerberos du domaine. Avec ce hash, l'attaquant peut forger des tickets Kerberos à volonté (Golden Tickets). Il peut se faire passer pour n'importe quel utilisateur (y compris un administrateur), avec n'importe quels privilèges, pour une durée quasi-illimitée (10 ans par défaut) et de manière très difficile à détecter car le ticket est techniquement valide. Pour approfondir, consultez Kubernetes offensif (RBAC abuse,.

Défense :

- Protéger les contrôleurs de domaine comme les joyaux de la couronne. L'accès physique et logique doit être extrêmement restreint.
- Changer le mot de passe du compte `KRBTGT` deux fois de suite, en suivant la procédure documentée par Microsoft. C'est une procédure à réaliser avec précaution, mais elle invalide tous les tickets Kerberos existants et le hash volé.
- Surveiller les anomalies dans les tickets Kerberos, comme des durées de vie anormalement longues ou l'utilisation d'un SID inexistant dans l'attribut SIDHistory.

DCSync & DCShadow

Un attaquant avec les bons privilèges (`GetChanges` et `GetChangesAll`) peut utiliser une attaque **DCSync** pour demander à un contrôleur de domaine de répliquer les secrets des mots de passe, comme le ferait un autre DC. Il n'a même pas besoin d'exécuter de code sur le DC lui-même. **DCShadow** est une technique encore plus avancée où l'attaquant enregistre une fausse machine en tant que DC pour pousser des modifications malveillantes dans l'AD.

Défense : Surveiller de très près qui possède ces privilèges de réplication. Détecter les requêtes de réplication provenant de machines qui ne sont pas des contrôleurs de domaine déclarés.

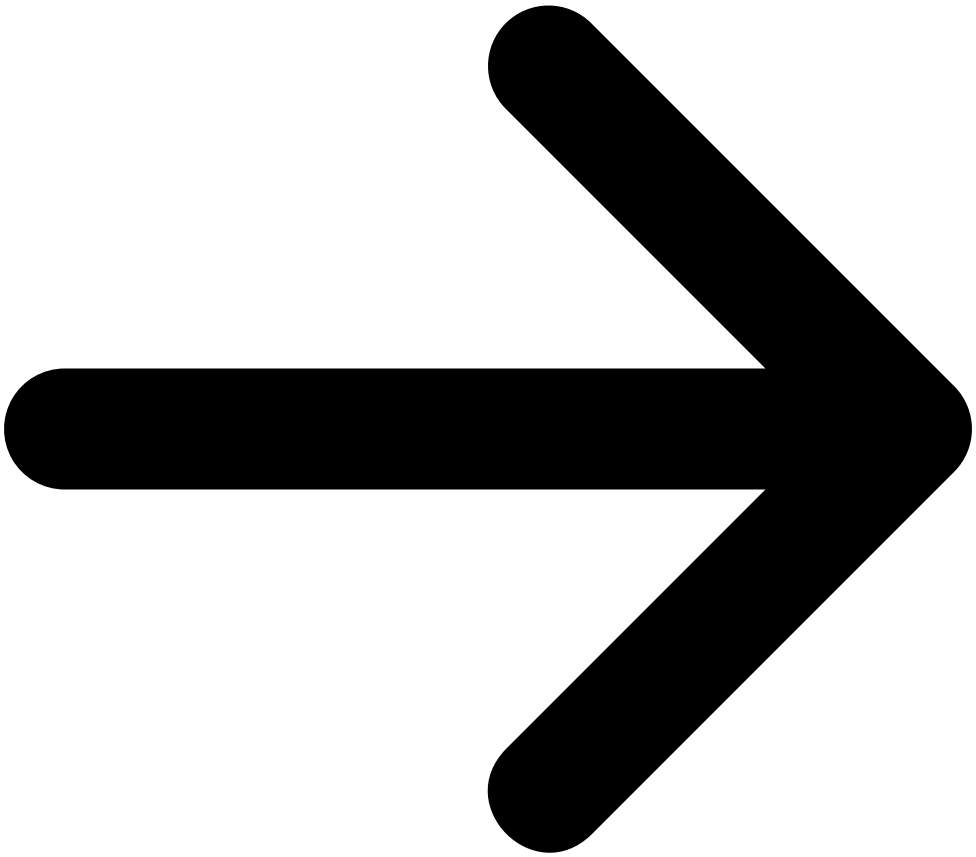
Attaques sur AD CS (Active Directory Certificate Services)

Si votre domaine utilise une infrastructure à clé publique (PKI) via AD CS, une mauvaise configuration peut être catastrophique. Des modèles de certificats mal configurés (par exemple, permettant à un utilisateur standard de demander un certificat qui peut être utilisé pour l'authentification en tant qu'administrateur) sont des vecteurs d'escalade de privilèges et de persistance extrêmement puissants (cf. les attaques ESC1, ESC8, etc., documentées par SpecterOps). Pour approfondir, consultez Livre Blanc : Directive.

Passez au niveau supérieur

Maintenant que vous comprenez les menaces sur AD, découvrez comment les principes de sécurité s'appliquent aux environnements Cloud.

Lire le livre blanc suivant : Pentest Cloud



Ressources open source associées :

- ADauditor — Toolkit d'audit de sécurité Active Directory (PowerShell)
- ADBloodHound-AI — Analyse BloodHound avec IA
- ad-attacks-fr — Dataset des attaques Active Directory (HuggingFace)

Cas concret
La publication du référentiel NIST Cybersecurity Framework 2.0 en 2024 a introduit la fonction Govern, reconnaissant que la gouvernance de la cybersécurité est indissociable de sa mise en œuvre technique. Cette évolution reflète la maturité croissante de l'approche risque dans l'industrie.

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, mettre en place des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Les experts recommandent une approche basee sur les risques, incluant l'evaluation reguliere de la posture de securite, la mise en place de controles techniques et organisationnels, la formation continue des equipes et l'adoption des referentiels de securite reconnus comme ceux du NIST, de l'ANSSI et de l'OWASP.

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Conclusion

Cet article a couvert les aspects essentiels de Chapitre 1 : Reconnaissance, la phase fondamentale de la compromission, Chapitre 2 : Les techniques d'attaque sur les identifiants, Chapitre 3 : La persistance, l'objectif ultime de l'attaquant. La mise en pratique de ces recommandations permet de renforcer significativement la posture de securite de votre organisation.

Sources et références : ANSSI · CERT-FR

Outils et Ressources Securite Active Directory

Decouvrez nos outils open source et modeles d'IA developpes pour les professionnels de la cybersecurite :

Outil / Ressource	Description	Lien
ADReplicationInspector	Inspecteur de replication AD pour detecter les attaques DCSync	Voir sur GitHub
WMIEventConsumerHunter	Chasseur de consumers WMI malveillants pour la persistance	Voir sur GitHub
TokenPrivilegeForensics	Analyse forensique des privileges de tokens Windows	Voir sur GitHub
Awesome Cybersecurity Tools	Collection d''outils de cybersecurite incluant des outils AD	Voir sur GitHub
AlternateDataStreamScanner	Scanner d''ADS NTFS pour la detection de donnees cachees	Voir sur GitHub

Tous ces outils sont disponibles en open source sur notre profil GitHub et nos modeles d'IA sur notre espace HuggingFace. N'hesitez pas a contribuer et a signaler les issues.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr