AYI NEDJIMI Consultants

Pass-the-Ticket Active Directory : : Guide Complet

Catégorie : Attaques Active Directory Lecture : 11 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

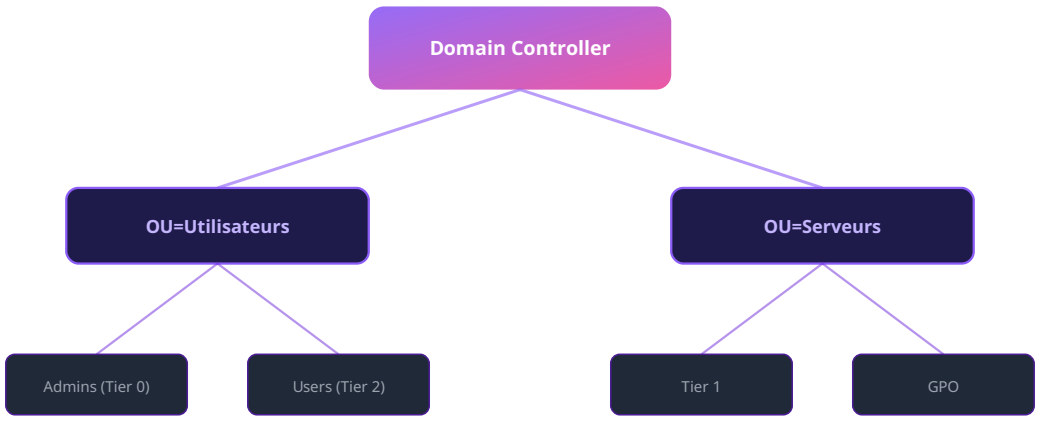
Guide expert sur l Pass-the-Ticket Active Directory : Attaque et Défense. Expert en cybersécurité et intelligence artificielle. Guide technique.

📑 Table des matières La securisation d'Active Directory represente un defi majeur pour les entreprises modernes. Les attaquants ciblent systematiquement ces infrastructures critiques, exploitant des configurations par defaut ou des privileges excessifs pour compromettre l'ensemble du systeme d'information. Cet article fournit une analyse technique approfondie des mecanismes d'attaque et des contre-mesures efficaces, basee sur des retours d'experience terrain et les recommandations des autorites de reference comme l'ANSSI et le MITRE. Guide expert sur l Pass-the-Ticket Active Directory : Attaque et Défense. Expert en cybersécurité et intelligence artificielle. Guide technique. Active Directory reste la cible privilégiée des attaquants en environnement Windows. Comprendre pass the ticket attaque defense est indispensable pour les équipes offensives comme défensives. Nous abordons notamment : introduction, méthodes de détection et contremesures et prévention. 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.

Introduction

Qu'est-ce que Pass-the-Ticket ?

Comment fonctionne l'attaque ?



Architecture Active Directory - Modele de tiering

Notre avis d'expert
Kerberos, conçu il y a des décennies, porte en lui des faiblesses architecturales que les attaquants exploitent quotidiennement. Le passage à une authentification moderne basée sur des certificats et FIDO2 n'est plus optionnel — c'est une question de survie numérique.

Méthodes de détection

Technique d'attaque	Tier cible	Difficulte	Impact
Kerberoasting	Tier 1-2	Facile	Eleve
DCSync	Tier 0	Moyen	Critique
Golden Ticket	Tier 0	Avance	Critique
NTLM Relay	Tier 1	Moyen	Eleve

Une compromission d'un seul poste de travail pourrait-elle mener à votre contrôleur de domaine ?

Contremesures et prévention

Cas concret
L'attaque ZeroLogon (CVE-2020-1472) permettait d'obtenir les privilèges d'administrateur de domaine en envoyant simplement des zéros dans le challenge Netlogon. Cette vulnérabilité critique, exploitable en quelques secondes, a rappelé que les protocoles historiques d'AD restent des surfaces d'attaque majeures.

Questions frequentes

Comment securiser un environnement Active Directory ?

La securisation d'Active Directory repose sur plusieurs piliers : l'implementation du modele de tiering, la restriction des privileges administratifs, la surveillance des evenements critiques, le deploiement du Protected Users group, la desactivation des protocoles obsoletes comme NTLM et la mise en place d'audits reguliers.

Qu'est-ce que le modele de tiering Active Directory ?

Le modele de tiering est une architecture de securite recommandee par Microsoft et l'ANSSI qui segmente les acces privilegies en trois niveaux : Tier 0 pour les controleurs de domaine, Tier 1 pour les serveurs membres et Tier 2 pour les postes de travail, empechant ainsi la propagation laterale des attaquants.

Pourquoi les attaques Active Directory sont-elles si frequentes ?

Les attaques Active Directory sont frequentes car AD reste le systeme d'authentification central de la majorite des entreprises. Les configurations par defaut sont souvent permissives, les privileges excessifs repandus et les techniques d'exploitation bien documentees, ce qui en fait une cible privilegiee pour les attaquants.

Conclusion

🎯 **Introduction**

L'attaque

Pass-the-Ticket

représente une menace critique pour les environnements Active Directory modernes. En matière de de la cybersécurité en 2025, cette technique d'attaque continue d'être largement exploitée par les acteurs malveillants, des cybercriminels opportunistes aux groupes APT (Advanced Persistent Threat) avancés.

Selon le

Verizon Data Breach Investigations Report 2024

, les attaques ciblant Active Directory représentent

plus de 80% des compromissions d'entreprise

. L'attaque Pass-the-Ticket fait partie du top 20 des techniques les plus observées en environnement réel.

⚠️ Impact critique

Vol et réutilisation de tickets Kerberos (TGT/TGS) capturés en mémoire

Maintenir une persistance long-terme dans le domaine

Escalader ses privilèges jusqu'au niveau Domain Admin

Déployer des ransomwares ou autres malwares

Ce guide expert, rédigé par

Ayi NEDJIMI

, consultant spécialisé en sécurité Active Directory, vous fournira une compréhension approfondie de cette attaque, des techniques **de détection** avancées et des stratégies de défense éprouvées.

📚 Qu'est-ce que Pass-the-Ticket ?

L'attaque

est une technique d'exploitation d'Active Directory qui permet à un attaquant de :

Vol et réutilisation de tickets Kerberos (TGT/TGS) capturés en mémoire

Contexte historique

Cette technique a été popularisée dans la communauté sécurité autour de 2015-2016, bien que les principes sous-jacents soient connus depuis plus longtemps. Elle a été documentée dans plusieurs frameworks d'attaque :

MITRE ATT&CK

: Technique référencée dans le framework de tactiques adversaires

Mimikatz
: Outil incluant des modules pour cette attaque (Benjamin Delpy)

BloodHound
: Capacité à identifier les chemins d'attaque potentiels

Impacket
: Suite Python incluant des outils d'exploitation

Prérequis

Pour qu'un attaquant puisse mener cette attaque avec succès, plusieurs conditions doivent généralement être réunies :

✅ Conditions d'exploitation

Accès initial
: Compromission d'au moins un compte utilisateur ou machine dans le domaine

Privilèges requis
: Selon l'attaque, des privilèges spécifiques peuvent être nécessaires

Outil

: Mimikatz, Rubeus, Impacket, ou outils personnalisés

Connaissance du domaine
: Compréhension de la topologie et des comptes sensibles

Différences avec d'autres attaques similaires

Caractéristique
Pass-the-Ticket

Autres techniques

Furtivité
Élevée - difficile à détecter

Variable selon la technique

Persistance
Long-terme possible
Souvent temporaire
Complexité
Modérée à élevée
Variable

Impact

Critique - accès privilégié

Dépend de la technique

Voir aussi notre article sur le

Top 10 des Attaques Active Directory

pour une vue d'ensemble complète du paysage des menaces.

🔒 Besoin d'un audit de sécurité Active Directory ?

Nos experts analysent votre environnement AD pour identifier les vulnérabilités critiques comme Pass-the-Ticket et vous fournissent un plan d'action prioritaire.

Demander un audit gratuit
⚙️ Comment fonctionne l'attaque ?

Comprendre le fonctionnement technique de l'attaque

Pass-the-Ticket
est essentiel pour mettre en place des défenses efficaces. Décomposons l'attaque en phases distinctes :

Phase 1 : Reconnaissance et énumération

L'attaquant commence par énumérer l'environnement Active Directory pour identifier les cibles potentielles. Outils et techniques couramment utilisés :

Énumération avec PowerView (PowerShell)

Import-Module PowerView.ps1 Get-DomainUser -Properties samaccountname,description

Get-DomainComputer
Get-DomainGroup
Énumération LDAP avec Python (ldap3)

```
from ldap3 import Server, Connection, ALL
server = Server('dc.exemple.local', get_info=ALL)
conn = Connection(server, user='DOMAIN\user', password='pass')
conn.search('dc=exemple,dc=local', '(objectClass=*)')
```

Énumération avec BloodHound
SharpHound.exe -c All -d exemple.local

Phase 2 : Exploitation

Une fois les cibles identifiées, l'attaquant procède à l'exploitation proprement dite. Les techniques varient selon les privilèges disponibles :

🔴 Techniques d'exploitation courantes

Utilisation de
Mimikatz
pour interagir avec LSASS

Exploitation via

Rubeus

pour les attaques Kerberos

Utilisation d' Pour approfondir, consultez Durcissement AD : Guide des Recommandations Microsoft.

Impacket
pour les opérations à distance

Scripts PowerShell personnalisés pour la furtivité

Phase 3 : Post-exploitation

Après une exploitation réussie, l'attaquant cherche à :

Maintenir l'accès

: Création de backdoors, comptes cachés

Escalader les privilèges
: Progression vers Domain Admin

Mouvement latéral
: Compromission d'autres systèmes

Exfiltration
: Vol de données sensibles

Chaîne d'attaque typique (Kill Chain)

Voici un scénario réaliste d'exploitation :

Initial Access
: Phishing avec macro malveillante → Beacon Cobalt Strike

Enumeration
: Découverte du domaine avec BloodHound

Privilege Escalation
: Exploitation de Pass-the-Ticket

Lateral Movement
: PsExec / WMI vers serveurs sensibles

Persistence
: Golden Ticket / Silver Ticket / Skeleton Key

Data Exfiltration
: Rapatriement via DNS tunneling ou HTTPS

Note forensique
: Les artifacts de cette attaque peuvent persister dans les logs pendant 90 à 180 jours selon votre politique de rétention. Une investigation rétrospective est souvent possible.

Pour approfondir les techniques d'investigation, consultez notre guide sur le

Forensics Windows et Active Directory

.

🔍 **Méthodes de** détection

La détection de l'attaque

Pass-the-Ticket
repose sur une approche multicouche combinant :

Surveillance des logs Windows et Active Directory

Corrélation d'événements via SIEM

Solutions EDR (Endpoint Detection and Response)

Produits spécialisés de protection d'identité (Microsoft Defender for Identity, etc.)

Event IDs Windows critiques
Utilisation de tickets Kerberos depuis IPs inhabituelles, EDR détectant accès mémoire LSASS

Event ID
Log Source
Description
Priorité
4768

Security
Ticket TGT Kerberos demandé
Haute

4769

Security
Ticket service Kerberos demandé

Haute

4662

Security
Opération effectuée sur un objet AD

Critique
4624

Security
Ouverture de session réussie
Moyenne
4672

Security
Privilèges spéciaux attribués
Haute

Requêtes SIEM (Splunk / Microsoft Sentinel)

Splunk Query
index=windows EventCode=4768 OR EventCode=4769 | stats count by src_ip, user, dest | where count > 50 | table _time, src_ip, user, dest, count | sort -count

Microsoft Sentinel (KQL)

SecurityEvent
| where EventID in (4768, 4769, 4662) | where TimeGenerated > ago(24h)

```
| summarize Count=count() by Account, Computer, IpAddress
| where Count > 50
| order by Count desc
```

Solutions EDR et Identity Protection

🛡️ Outils de détection recommandés

Microsoft Defender for Identity

: Détection native des attaques AD, alertes en temps réel

CrowdStrike Falcon
: EDR avec détection comportementale avancée

Vectra AI
: IA pour détection d'anomalies réseau et AD

Silverfort
: Protection d'identité unifiée pour AD hybride

Sysmon
: Logging avancé des événements système (gratuit)

Indicateurs de compromission (IOC)

Soyez attentif aux signes suivants :

Accès à LSASS par des processus non autorisés Pour approfondir, consultez DCShadow : Attaque Furtive.

Requêtes LDAP massives depuis workstations

Tickets Kerberos avec durées inhabituelles (> 10 heures)

Authentifications depuis adresses IP inconnues

Modifications d'attributs sensibles AD (ACL, groupes, SPN)

Consultez également notre article sur les

Top 5 Outils d'Audit Active Directory

pour découvrir les meilleurs outils de détection.

🛡️ **Contremesures et** prévention

La prévention de l'attaque

Pass-the-Ticket
nécessite une approche de défense en profondeur (Defense in Depth). Voici les mesures recommandées :

1. Architecture de sécurité (Tiered Administration)

Implémentez un modèle d'administration par niveaux (Tier 0/1/2) pour limiter l'exposition :

🏗️ Modèle Tiered Administration

Tier 0

: Domain Controllers, comptes Domain Admin, serveurs d'identité

Stations d'administration dédiées (PAW - Privileged Access Workstations)

MFA obligatoire
Pas de navigation Internet
Pas d'email

Tier 1

: Serveurs applicatifs, serveurs de fichiers

Comptes d'administration séparés de Tier 0

Jump servers pour l'accès

MFA recommandé
Tier 2

: Workstations utilisateurs

Comptes utilisateurs standard
Pas de privilèges admin locaux

UAC activé

2. Durcissement Active Directory

Credential Guard, HVCI, empêcher dump LSASS, contrôle d'exécution des outils non autorisés, réduire durée des tickets

Hardening Kerberos
Forcer AES pour Kerberos (GPO)

Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options Network security: Configure encryption types allowed for Kerberos

- Cocher uniquement AES128_HMAC_SHA1, AES256_HMAC_SHA1

Réduire la durée de vie des tickets (GPO)

Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Kerberos Policy Maximum lifetime for user ticket: 10 hours (default) Maximum lifetime for service ticket: 600 minutes Maximum lifetime for user ticket renewal: 7 days

Protected Users Group
Ajoutez les comptes privilégiés au groupe

Protected Users
(introduit dans Windows Server 2012 R2) :

Pas de chiffrement DES ou RC4 Kerberos

Pas de délégation Kerberos
Pas de cache des credentials NTLM

TGT max 4 heures (non renouvelable au-delà)

PowerShell : Ajouter utilisateurs au groupe Protected Users

Add-ADGroupMember -Identity "Protected Users" -Members "AdminDA01","AdminDA02"

3. Solutions techniques de protection

Microsoft LAPS (Local Administrator Password Solution)

Rotation automatique des mots de passe administrateur locaux :

Installation LAPS

msiexec /i LAPS.x64.msi /quiet

Configuration GPO LAPS

Computer Configuration > Policies > Administrative Templates > LAPS

Enable local admin password management: Enabled

Password Settings:

Length: 20 characters

Age: 30 days

- Complexity: Large letters + small letters + numbers + specials

Credential Guard (Windows 10/11 Enterprise, Server 2016+)

Protection

Activer Credential Guard (GPO ou script)

Computer Configuration > Administrative Templates > System > Device Guard

Turn On Virtualization Based Security: Enabled

- Credential Guard Configuration: Enabled with UEFI lock

Vérifier activation Credential Guard

```
Get-ComputerInfo | select DeviceGuardSecurityServicesConfigured
```

4. Surveillance et audit

✅ Checklist de prévention

☑️ Audit SACL activé sur objets sensibles AD

☑️ Rétention des logs Security minimum 180 jours

☑️ SIEM avec corrélation d'événements AD

☑️ EDR déployé sur tous les endpoints Pour approfondir, consultez CVE-2025-21293 : Escalade de Privileges AD DS.

☑️ Microsoft Defender for Identity configuré

☑️ Honeypots / Deception technologies déployés

☑️ Segmentation réseau (VLANs, micro-segmentation)

☑️ MFA pour tous les comptes privilégiés

☑️ Revue trimestrielle des ACL AD

☑️ Pentest annuel ciblé Active Directory

Pour un guide complet de sécurisation, consultez notre

Guide de Sécurisation Active Directory 2025

.

🚨 **Procédure de** remédiation

Si vous suspectez ou confirmez une compromission via

Pass-the-Ticket
, suivez cette procédure de réponse à incident :

⚠️ Avertissement critique

Ne prenez jamais de mesures précipitées qui pourraient alerter l'attaquant ou détruire des preuves forensiques.

Documentez chaque action et coordonnez-vous avec votre équipe IR (Incident Response).

Phase 1 : Containment (Confinement) ⏱️ 0-4 heures

Isoler les systèmes compromis
Déconnecter du réseau (physiquement si critique)

Désactiver les comptes compromis (ne pas supprimer)

Bloquer les adresses IP sources suspectes (firewall)

Préserver les preuves
Capturer images mémoire (RAM) avec FTK Imager ou WinPmem

Exporter les logs pertinents avant rotation

Prendre snapshots des VMs affectées

Activer le mode "Incident Response"

Augmenter le niveau de logging (verbose)

Activer monitoring continu (24/7)

Notifier le management et l'équipe juridique

Analyse mémoire avec Volatility

volatility -f memory.dmp --profile=Win10x64 psscan volatility -f memory.dmp --profile=Win10x64 dlllist -p

volatility -f memory.dmp --profile=Win10x64 malfind

Analyse disque avec PowerForensics

Get-ForensicTimeline -VolumeName C:\ | Export-Csv timeline.csv Get-ForensicEventLog -Path C:\Windows\System32\winevt\Logs\Security.evtx

Identifier la portée
Quels comptes ont été compromis ?

Quels systèmes ont été accédés ?

Quelles données ont été exfiltrées ?

Depuis combien de temps l'attaquant est-il présent ? (Dwell Time)

Phase 3 : Eradication ⏱️ 12-48 heures

Invalider sessions, forcer expiration des tickets, changer mots de passe si exposés

Supprimer la présence de l'attaquant

Réinitialiser mots de passe de tous les comptes compromis

Révoquer certificats et tokens compromis

Supprimer backdoors et malwares identifiés

Corriger les vulnérabilités exploitées

Réimager les systèmes critiques

Domain Controllers si compromission confirmée

Serveurs critiques (SQL, Exchange, etc.)

Workstations administratives
Phase 4 : Recovery (Récupération) ⏱️ 48-72 heures

Restauration des services
Validation de l'intégrité AD (dcdiag, repadmin)

Tests de fonctionnement

Retour progressif à la normale

Monitoring renforcé
Surveillance 24/7 pendant 30 jours minimum

Recherche de réinfection
Validation que l'attaquant n'a plus accès

Phase 5 : Lessons Learned ⏱️ Post-incident

📊 Post-Mortem

Rédaction d'un rapport d'incident détaillé

Identification des failles de sécurité exploitées Pour approfondir, consultez Computer Account Takeover Active.

Mise à jour du plan de réponse à incident

Formation des équipes sur les leçons apprises

Implémentation de contrôles compensatoires

Quand faire appel à un expert externe ?

Faites appel à un consultant spécialisé en réponse à incident Active Directory si :

Vous manquez d'expertise interne en forensics AD

L'attaque est élaborée (APT potentiel)

Vous avez besoin d'un regard externe impartial

Des obligations réglementaires l'exigent (RGPD, NIS2, etc.)

Consultez notre page
Investigation Forensics
pour plus d'informations sur nos services de réponse à incident.

Demander un devis
Voir les formations
🎓 Conclusion

L'attaque

Pass-the-Ticket
représente une menace réelle et actuelle pour les environnements Active Directory. Comme nous l'avons vu dans ce guide, cette technique peut avoir des conséquences critiques si elle n'est pas détectée et mitigée rapidement.

Points clés à retenir
✅ Synthèse des bonnes pratiques

Prévention
: Credential Guard, HVCI, empêcher dump LSASS, contrôle d'exécution des outils non autorisés, réduire durée des tickets

Détection

: Utilisation de tickets Kerberos depuis IPs inhabituelles, EDR détectant accès mémoire LSASS

Remédiation

: Invalider sessions, forcer expiration des tickets, changer mots de passe si exposés

Architecture

: Modèle Tier 0/1/2, PAW, MFA, LAPS

Surveillance
: SIEM, EDR, Microsoft Defender for Identity

Prochaines étapes recommandées

Évaluation de la posture actuelle

Audit de sécurité Active Directory complet

Analyse de vulnérabilités avec BloodHound

Pentest ciblé AD
Implémentation des **contremesures** prioritaires

LAPS sur toutes les workstations

Protected Users pour comptes privilégiés

Microsoft Defender for Identity

Credential Guard sur endpoints Windows 10/11

Formation et sensibilisation
Pour approfondir, consultez les ressources officielles : OWASP Testing Guide, CVE Details et ANSSI.

Sources et références : MITRE ATT&CK Privilege Escalation · ADSecurity.org

Formation des équipes IT aux attaques AD

Sensibilisation des utilisateurs (phishing, social engineering)

Exercices de simulation d'incidents (tabletop exercises)

Amélioration continue
Veille technologique sur les nouvelles menaces AD

Participation aux communautés sécurité (forums, conférences)

Tests réguliers (pentest annuel, purple teaming)

Ressources complémentaires
Pour approfondir vos connaissances sur la sécurité Active Directory, consultez nos autres ressources :

Top 10 des Attaques Active Directory 2025

Guide de Sécurisation Active Directory 2025

Top 5 Outils d'Audit Active Directory

Investigation Forensics Windows & Active Directory

Nos Formations Cybersécurité
Livres Blancs Gratuits
Citation
: "La sécurité n'est pas un produit, mais un processus." — Bruce Schneier

La protection contre Pass-the-Ticket et autres attaques Active Directory nécessite une approche holistique combinant technologie, processus et formation. N'attendez pas une compromission pour agir — la prévention est toujours plus efficace et moins coûteuse que la remédiation.

Besoin d'aide pour sécuriser votre Active Directory ?

Nos experts sont là pour vous accompagner.

Contacter un expert
Voir nos services
Article précédent
Article suivant
Ayi NEDJIMI Consultants
Experts en cybersécurité offensive et développement IA. Audits de sécurité Active Directory, Infrastructure Cloud, Kubernetes et Microsoft 365.

Nos Services
Audit Active Directory
Audit Infrastructure Cloud
Audit Kubernetes
Audit Microsoft 365

Audit Virtualisation
Forensics
Développement IA
Formations
Ressources
Tous les Articles
Articles Cybersécurité
Articles Intelligence Artificielle

Livres Blancs
Guides Gratuits
Blog

Top 10 Attaques AD

Guide Sécurisation AD
Contact
Demander un devis
Nous contacter
Mentions légales
Politique de confidentialité

Expert Cybersécurité & Intelligence Artificielle

```
Get-ComputerInfo | select DeviceGuardSecurityServicesConfigured
```

Ressources open source associées :

- KerberosTGTForensics — Forensics TGT Kerberos (C++)
- GoldenTicket-Detector — Détection de Golden/Silver tickets (C++)
- ad-attacks-fr — Dataset des attaques Active Directory (HuggingFace)

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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