

CRACKINTELLIGENCE



100 PRINCIPALES  
MÉTHODES  
POUR PIRATER UN AD

MICROSOFT

FROM INVERSEHACKER



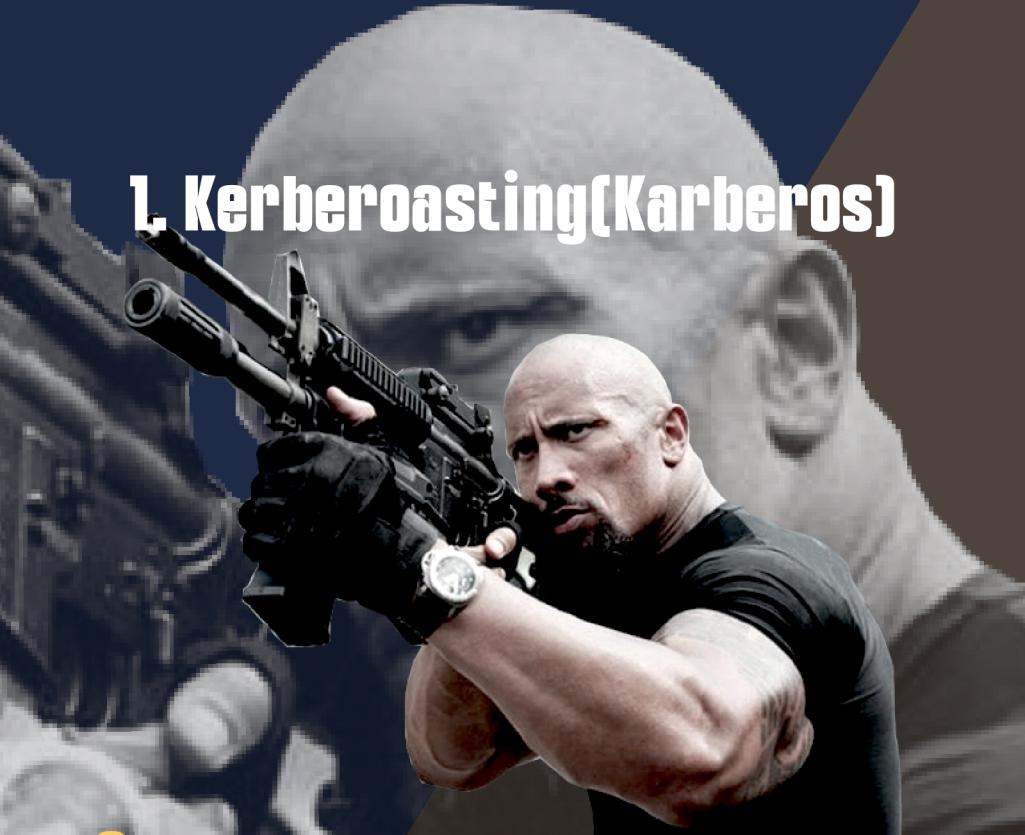
IRJEANL



JEANLUCK NDATO



# L'Kerberoasting(Karberos)

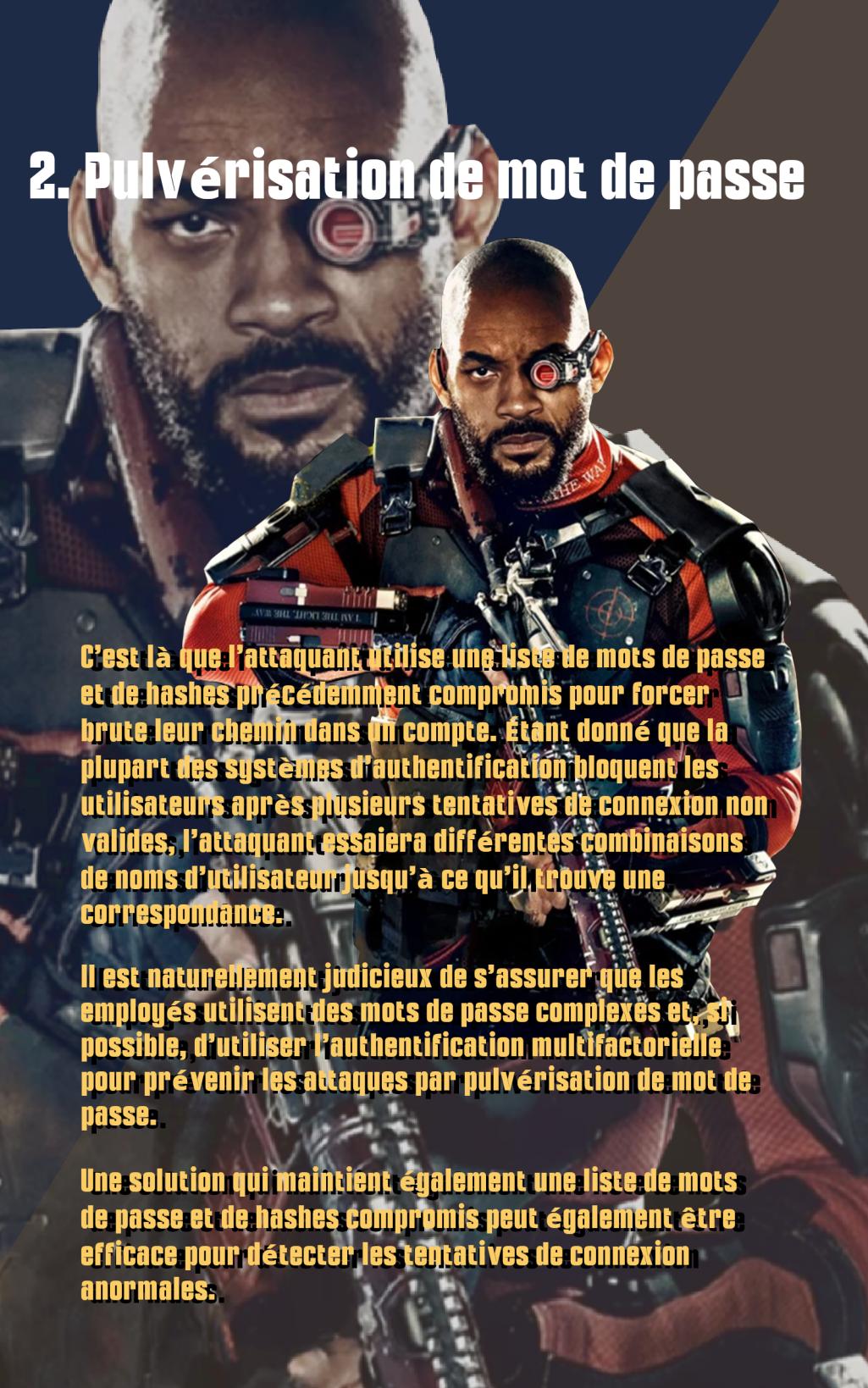


**C**es attaques ciblent les comptes de service dans Active Directory en exploitant l'attribut SPN (ServicePrincipalName) des objets utilisateur.

**L**es services publient leurs SPN dans les objets AD lorsqu'ils s'authentifient, et les adversaires essaieront de cibler ces comptes de service et de modifier les valeurs SPN pour répondre à leurs besoins, en particulier si le compte appartient à des groupes privilégiés.

**L**es organisations doivent surveiller en permanence les objets utilisateur pour détecter des modifications anormales apportées aux valeurs SPN et les comptes de service doivent être protégés par des mots de passe forts.

## 2. Pulvérisation de mot de passe

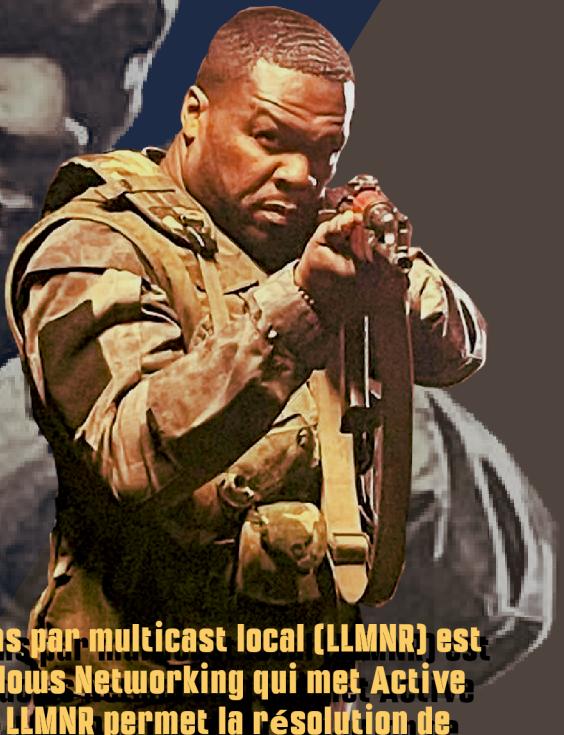


C'est là que l'attaquant utilise une liste de mots de passe et de hashes précédemment compromis pour forcer brute leur chemin dans un compte. Étant donné que la plupart des systèmes d'authentification bloquent les utilisateurs après plusieurs tentatives de connexion non valides, l'attaquant essaiera différentes combinaisons de noms d'utilisateur jusqu'à ce qu'il trouve une correspondance.

Il est naturellement judicieux de s'assurer que les employés utilisent des mots de passe complexes et, si possible, d'utiliser l'authentification multifactorielle, pour prévenir les attaques par pulvérisation de mot de passe.

Une solution qui maintient également une liste de mots de passe et de hashes compromis peut également être efficace pour détecter les tentatives de connexion anormales.

### **3. Résolution de noms par multicast local (LLMNR)**



**La résolution de noms par multicast local (LLMNR) est une fonction de Windows Networking qui met Active Directory en danger. LLMNR permet la résolution de noms sans l'exigence d'un serveur DNS.**

**Des paquets multicast sont diffusés sur le réseau, demandant l'adresse IP d'un nom d'hôte donné. Les attaquants peuvent intercepter ces paquets et affirmer que l'adresse IP est liée à leur nom d'hôte.**

**Cette fonctionnalité n'est pas nécessaire si le Domain Name System (DNS) est correctement configuré. Par conséquent, la meilleure façon de mitiger cette menace consisterait à simplement désactiver LLMNR.**

## 4. Pass-the-hash avec Mimikatz

**Pass-the-hash est une technique utilisée pour voler des informations d'identification à partir d'Active Directory et facilite également le mouvement latéral dans l'environnement.**

**Les attaquants utilisent un outil appelé Mimikatz, qui exploite le protocole d'authentification NTLM pour s'identifier en tant qu'utilisateur et extraire les hachages de jeton de mémoire.**

**Les organisations doivent s'assurer que les hachages de jeton de comptes privilégiés ne sont pas stockés dans un endroit où ils peuvent être facilement extraits.**

**Ils devraient également envisager d'activer la protection LSA et d'utiliser le mode administrateur restreint pour les connexions Bureau à distance.**

## **5. Mots de passe par défaut**

**Les entreprises oublient souvent de changer les mots de passe par défaut sur les appareils/systèmes, et les attaquants rechercheront ces appareils/systèmes pour pénétrer dans votre réseau.**

**Les organisations doivent s'assurer qu'elles changent les mots de passe par défaut et qu'elles conservent une liste à jour de tout le matériel réseau.**

**Il peut également être utile d'adopter une solution qui crée des mots de passe aléatoires pour les utilisateurs et les appareils de l'entreprise.**

## 6. Identifiants codés en dur



Dans certains cas, les développeurs de logiciels codent en dur des identifiants dans des scripts, ce qui est évidemment un risque pour la sécurité, en particulier si les identifiants fournissent un accès privilégié.

Les développeurs ont peut-être codé en dur les identifiants pour tester la fonctionnalité du script et les ont ensuite oubliés de les supprimer.

Quelle qu'en soit la raison, les attaquants essaieront de trouver des scripts qui contiennent des identifiants codés en dur, qu'ils peuvent exploiter. Les administrateurs doivent garder un œil attentif sur tous les comptes d'utilisateur pour s'assurer qu'ils sont utilisés aux fins prévues.

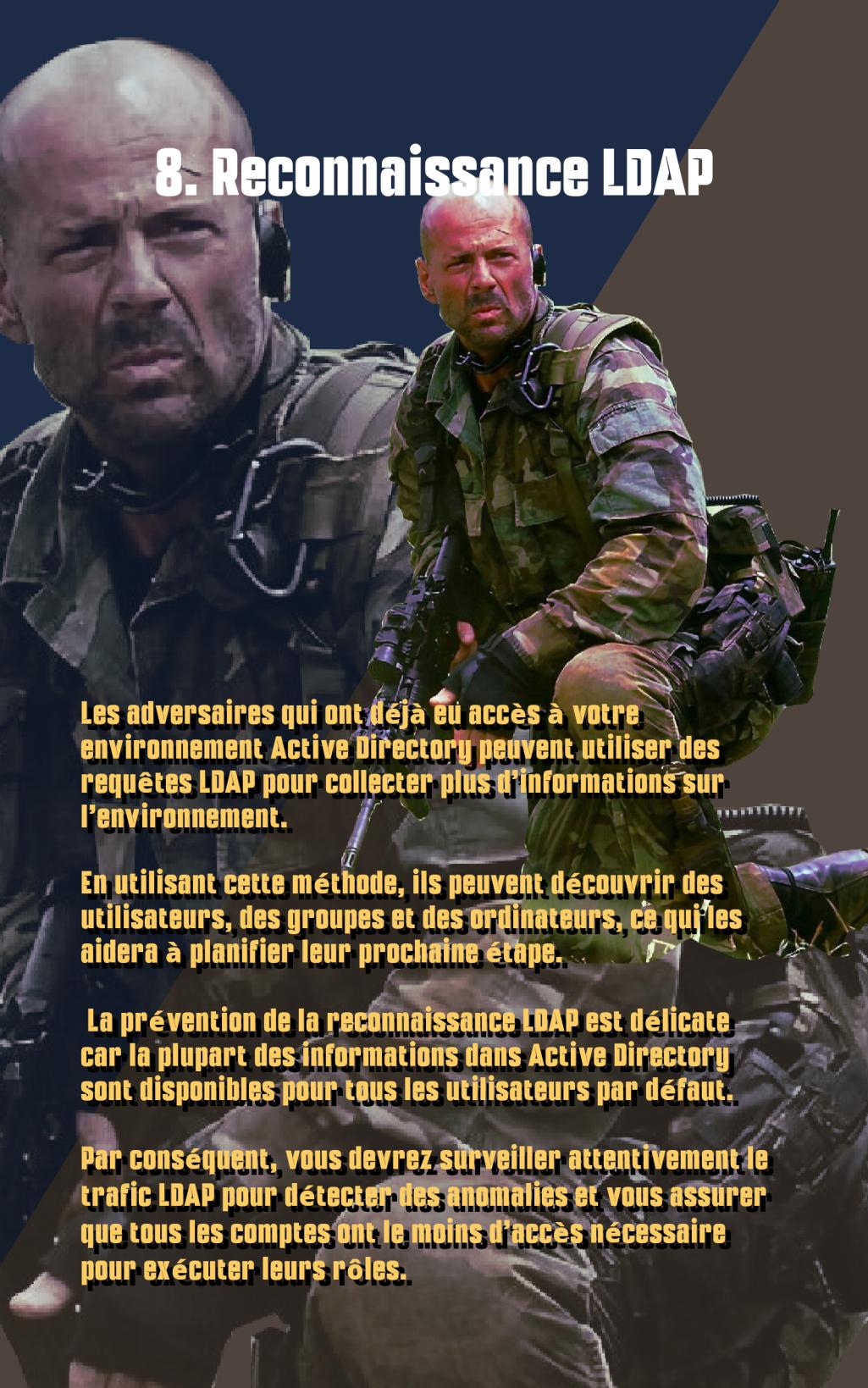
## 7. Élévation des privilèges

**Les cybercriminels essaieront généralement d'accéder à un compte utilisateur standard en exploitant de mauvaises pratiques en matière de mots de passe.**

**Une fois qu'ils ont eu accès, ils essaieront d'élever leurs privilèges par l'ingénierie sociale, l'exploitation de vulnérabilités logicielles/matérielles, les configurations erronées, l'installation de logiciels malveillants, etc.**

**Les organisations doivent tenir à jour une liste des comptes qui ont accès aux ressources, en particulier aux ressources critiques. Les comptes doivent avoir les privilèges les plus bas dont ils ont besoin pour exécuter leur rôle, et toute activité de compte privilégié doit être surveillée en permanence, avec des alertes en temps réel envoyées à l'administrateur.**

## 8. Reconnaissance LDAP



**Les adversaires qui ont déjà eu accès à votre environnement Active Directory peuvent utiliser des requêtes LDAP pour collecter plus d'informations sur l'environnement.**

**En utilisant cette méthode, ils peuvent découvrir des utilisateurs, des groupes et des ordinateurs, ce qui les aidera à planifier leur prochaine étape.**

**La prévention de la reconnaissance LDAP est délicate car la plupart des informations dans Active Directory sont disponibles pour tous les utilisateurs par défaut.**

**Par conséquent, vous devrez surveiller attentivement le trafic LDAP pour détecter des anomalies et vous assurer que tous les comptes ont le moins d'accès nécessaire pour exécuter leurs rôles.**

## 9. Reconnaissance BloodHound

**La reconnaissance LDAP est une technique utilisée par les attaquants pour collecter des informations sur un environnement Active Directory.**

**Cela peut être fait en envoyant des requêtes LDAP au serveur Active Directory, qui peuvent révéler des informations telles que les noms d'utilisateur, les groupes d'appartenance et les autorisations.**

**La reconnaissance BloodHound est une technique plus sophistiquée qui permet aux attaquants de visualiser les relations entre les objets Active Directory.**

**Cela peut leur aider à identifier les chemins d'attaque potentiels et à planifier leurs attaques.**

# 10. Extraction de NTDS.dit

**Les contrôleurs de domaine stockent toutes les données Active Directory dans un fichier appelé ntds.dit, ou "le dit", comme certains l'appellent.**

**Par défaut, ce fichier se trouve dans le chemin suivant : C:\Windows\NTDS. Si un attaquant accède à Active Directory, il peut accéder au fichier ntds.dit ou compromettre la solution de sauvegarde de l'organisation et extraire le fichier ntds.dit de la sauvegarde.**

**Pour empêcher les attaquants d'extraire le fichier ntds.dit, vous devez minimiser le nombre de comptes qui peuvent se connecter aux contrôleurs de domaine, contrôler l'accès aux machines physiques des contrôleurs de domaine et prendre toutes les mesures nécessaires pour sécuriser votre environnement Active Directory."**



<https://jeanlucndato.blogspot.com>  
<https://geekstudyn.blogspot.com>