
# Exploitation d'Active Directory 101

28 novembre 2020

# À propos d'Active Directory (AD)

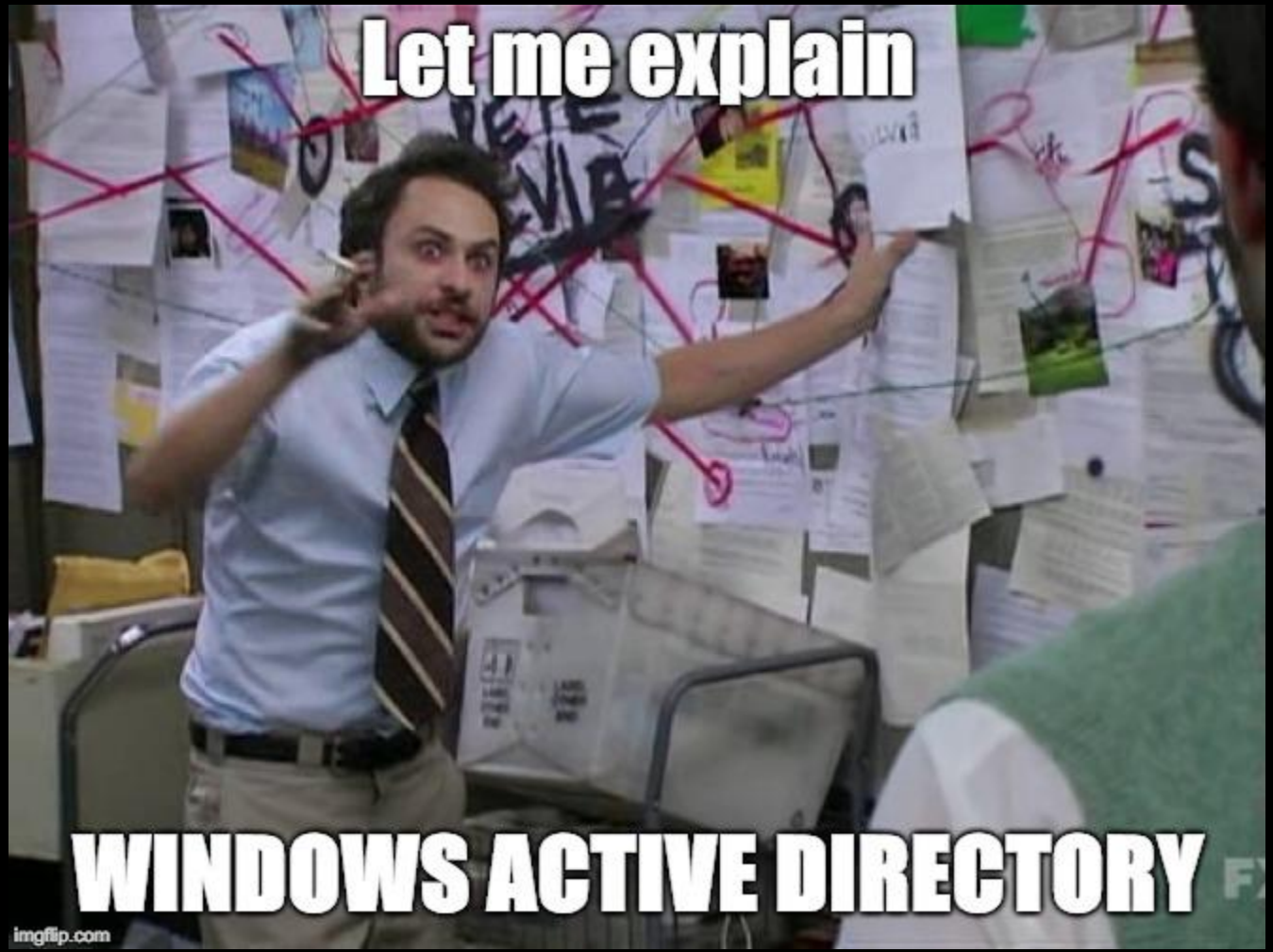
- Service d'annuaire (base de données d'utilisateurs, d'ordinateurs, de groupes, ...) fonctionnant en réseau
- *Utilisé par plus de 90% des compagnies dans le classement Fortune 1000*
- Compagnies, écoles, hôpitaux, gouvernements l'utilisent
- Plus plus compétiteur proche: Novell (eDirectory, ZENWorks)
- Service central d'authentification, application des politiques d'accès et de configuration, installation de programmes, partage de ressources, ...
- Souvent AD est utilisé conjointement avec plusieurs autres services Microsoft:
    - MS-SQL Server (base de données) , Internet Information Services (IIS, serveur web), autorité de certification (CA Root), AD Federated Service (Single sign-on)
- Peut également fonctionner avec Linux et macOS (plutôt rare)
- Dans les dernières années, montée en popularité de Azure AD et des comptes Office 365 (dans le Cloud)

# Au programme

- Bases d’Active Directory et fondements de Windows
- Reconnaissance de réseau
- Outils et méthodes d’exploitation
- Crackage de mots de passe
- Une méthode d’élever ses privilèges
- Ressources pour en apprendre davantage

# Éléments requis

- Machine virtuelle Kali Linux/ParrotOS sur votre PC
- Client OpenVpn (`sudo apt-get install openvpn`)
- Profil OpenVPN pour accéder au lab (*polyhx-ad-lab.ovpn*)


Let me explain
WINDOWS ACTIVE DIRECTORY
imgflip.com

# Domain controller (DC)

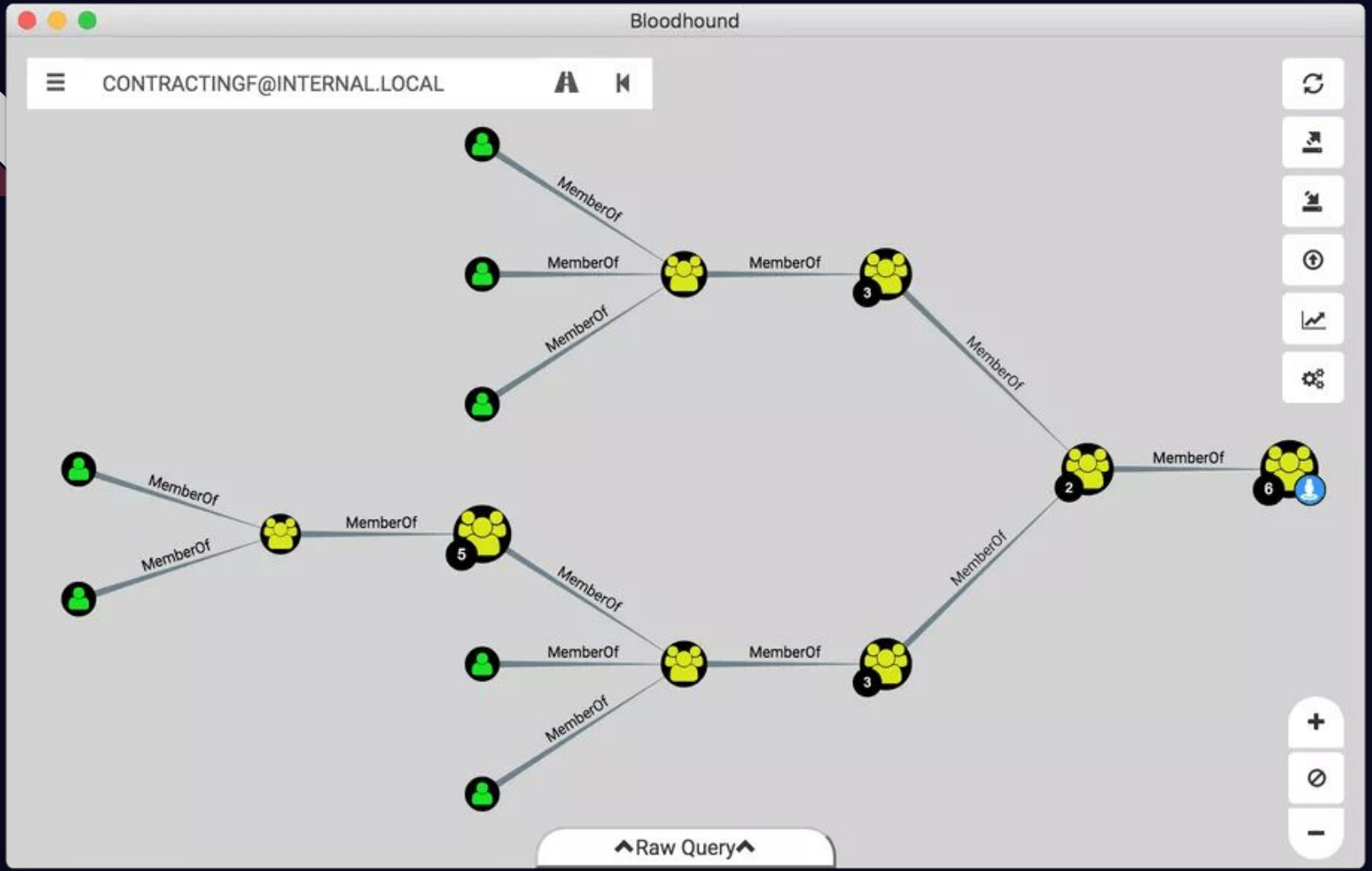
- Édition Windows Server ( != Windows Enterprise, Pro, NT, ...) contient le logiciel requis pour AD
- Contient l'annuaire (base de données des utilisateurs, groupes, permissions, ordinateurs, ...)
- Gère plusieurs stations de travail qui exécutent Windows Enterprise
- Le domaine a un nom et il est essentiel de le connaître pour utiliser plusieurs outils d'exploitation de vulnérabilités d'AD
- Les stations de travail doivent le joindre pour avoir accès à son contenu
    - Pour le joindre, on a besoin d'un compte utilisateur du domaine
- Selon la compagnie, il pourrait y avoir plusieurs domain controllers, à ce moment-là, on appelle l'ensemble du domain une forêt
- Le DC est géré par les domain admins
- En tant qu'attaquant, le but ultime est d'obtenir l'accès à un domain admin
- Généralement lui qui exécute les services comme
    - IIS, ADFS, MS-SQL, Certification Authority, Network Shared Drives, Email Server
- D'un point de vue réseau
    - serveur DNS (port 53/TCP)
    - le service d'authentification Kerberos est actif (port 88/TCP)
    - Panoplie de ports ouverts pour assurer le fonctionnement du réseau

# Stations de travail

- OS == Windows Pro/Enterprise qui est authentifié au domain controller (domain-joined workstation)
- Comptes locaux: peuvent être utilisés que sur la machine sur laquelle ils sont présents
- Comptes domaines: peuvent être utilisés pour se connecter aux machines qui
- Une station de travail qui a joint le domaine possède une copie de presque l'intégralité du domaine (ex. : utilisateurs, groupes, …)
- Il y a un admin local qui a tous les droits sur la machine mais qui n'a pas d'accès spéciaux dans le domaine
- Utile de discerner les comptes locaux des comptes du domaine: ils n'ouvrent pas les mêmes portes
- On se connecte à un compte domaine généralement dans ce format: DOMAINNAME\username

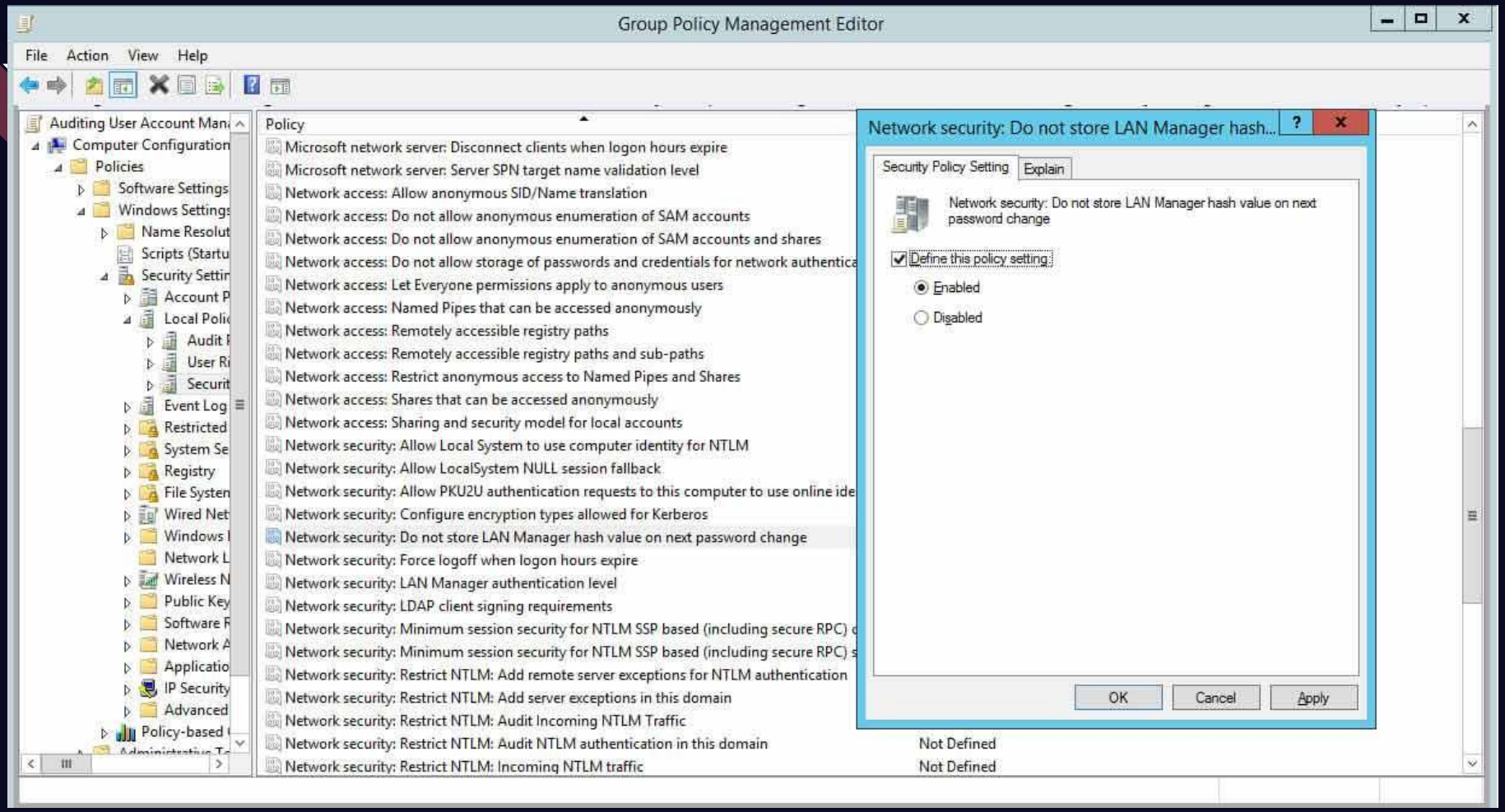
# Groupe

- Outil pour gérer plusieurs utilisateurs
- Restreint les actions qu'un utilisateur d'un groupe peut faire (créer de nouveaux comptes, modifier le serveur web, etc.)
- Définit les permissions des fichiers (*r-w-x*)
- Il peut devenir très compliqué de déterminer les permissions d'un utilisateur car il peut appartenir à plusieurs groupes
    - On utilise des outils comme Bloodhound évaluer ces permissions
- Les administrateurs du domaine peuvent appliquer des GPO aux groups (*slide suivante*)


Bloodhound
CONTRACTINGF@INTERNAL.LOCAL
MemberOf
MemberOf
MemberOf
MemberOf
3
MemberOf
MemberOf
2
MemberOf
6
MemberOf
MemberOf
MemberOf
5
MemberOf
MemberOf
MemberOf
3
MemberOf
MemberOf
Raw Query

# Group policies

- Outils de gestion des configurations (réseau, domaine, workstations, utilisateur)
- GPO (Group policy object)
- Peut s'appliquer à plusieurs entités (ex.: un groupe, un utilisateur, un ordinateur, un domaine)
- Gère surtout les paramètres des fonctionnalités de Windows
  - Désactiver des fonctionnalités
  - Vérouiller des réglages
  - Password length
  - Niveau de sécurité (UAC) sur les machines
  - Firewall
  - Type de hash à utiliser dans le réseau
  - Activation du compte Guest
  - Déconnexion après x heures d'inactivité
  - Configuration des protocoles qu'utilise Windows
  - Mesures de sécurité
  - Audit et log des activités du système et des utilisateurs
- Under the hood, modifie généralement une clé du registre de Windows (regedit.exe)


Group Policy Management Editor
File Action View Help
Auditing User Account Mana
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Security Settir
Account P
Local Polic
Audit
User Ri
Securit
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows
Network L
Wireless N
Public Key
Software R
Network A
Applicatio
IP Security
Advanced
Policy-based
Policy
Microsoft network server: Disconnect clients when logon hours expire
Microsoft network server: Server SPN target name validation level
Network access: Allow anonymous SID/Name translation
Network access: Do not allow anonymous enumeration of SAM accounts
Network access: Do not allow anonymous enumeration of SAM accounts and shares
Network access: Do not allow storage of passwords and credentials for network authentica
Network access: Let Everyone permissions apply to anonymous users
Network access: Named Pipes that can be accessed anonymously
Network access: Remotely accessible registry paths
Network access: Remotely accessible registry paths and sub-paths
Network access: Restrict anonymous access to Named Pipes and Shares
Network access: Shares that can be accessed anonymously
Network access: Sharing and security model for local accounts
Network security: Allow Local System to use computer identity for NTLM
Network security: Allow LocalSystem NULL session fallback
Network security: Allow PKU2U authentication requests to this computer to use online ide
Network security: Configure encryption types allowed for Kerberos
Network security: Do not store LAN Manager hash value on next password change
Network security: Force logoff when logon hours expire
Network security: LAN Manager authentication level
Network security: LDAP client signing requirements
Network security: Minimum session security for NTLM SSP based (including secure RPC)
Network security: Minimum session security for NTLM SSP based (including secure RPC)
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication
Network security: Restrict NTLM: Add server exceptions in this domain
Network security: Restrict NTLM: Audit Incoming NTLM Traffic
Network security: Restrict NTLM: Audit NTLM authentication in this domain
Network security: Restrict NTLM: Incoming NTLM traffic
Not Defined
Not Defined
Network security: Do not store LAN Manager hash...
Security Policy Setting
Explain
Network security: Do not store LAN Manager hash value on next password change
Define this policy setting
Enabled
Disabled
OK
Cancel
Apply

# Protocoles

- Psexec, wmiexec: semblable à SSH mais pour Windows, accès à une invite de commande sur un ordinateur distant,
- RPC: un API pour récupérer des informations sur le domaine ou une machine Windows, port 139
- SMB: Small Messaging Block, couramment utilisé pour l'accès à des fichiers sur un serveur, port 445
- RDP: Remote Desktop Protocol, session graphique à distance, port 3389,
- Kerberos, NetBIOS, et beaucoup plus...

**Lightweight Directory Access Protocol (LDAP):**

- Protocole pour effectuer des recherches et d'autres actions (ajout, retrait, ...) dans un annuaire (en l'occurrence, Active Directory)
- Pour les recherches, on utilise généralement la notation pour spécifier ou chercher:
  `("CN=Dev-India,OU=Distribution Groups,DC=gp,DC=gl,DC=google,DC=com");`
  - Common name: le nom de l'objet
  - Organizational unit: dossier dans lequel se trouve l'objet (ex.: ordinateurs, utilisateurs, logiciels et réglages
  - Domain component: le domaine AD dans lequel on cherche (ici: gp.gl.google.com)

# Hash de mots de passe

- Au fil des années plusieurs types de hash de mot de passe se sont succédés pour permettre l'authentification dans le domaine.
  - LM (LAN Manager, ~1994)
  - NTLMv1 (NT Lan Manager)
  - NTLMv2  (version moderne)
- Les versions plus anciennes sont rarement utilisées et posent des risques en raison de leurs failles cryptographiques.
- Windows retient les hash des mots de passe des utilisateurs connectés depuis le démarrage de l'ordinateur dans la mémoire RAM. (*lsass.exe*)

# Déroulement de l’atelier de ce soir

- Machines vulnérables, privées, hébergées sur Azure
- Pentest de ces machines Azure permis (https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing)
- Possible d’y accéder à l’aide du profil VPN (.ovpn) et Openvpn
- Défis hands-on pour vous familiariser avec les outils
- Les seules IP que vous pouvez scanner sont:
  - 10.0.1.0/24
- N’hésitez pas à poser de questions dans le chat ou dans le voice channel
- Pour le bon déroulement de l’atelier
  - Ne pas interagir (reconnaissance, attaques, connexions, …) avec les machines qui ne sont pas font pas partie des challenges, comme celles d’autres participants
  - Aucune attaque de dénis de service
  - Pas de connexions RDP (graphiques)
  - Pas d’utilisation de CVE (Zerologon)

# Challenge /x00:

# Reconnaissance initiale

En utilisant nmap ou tout autre outil de scan de réseau, déterminez

1. Les ports intéressants ouverts sur les machines
2. Quelle est l'IP du DC?
3. Nom du domaine

IP: 10.0.1.0/24

# Challenge /x00 - Solution

1. Commandes nmap possibles:
   a. Nmap -Pn -sC  -v -oN polyhx-ad.txt 10.0.1.0/24
2. Nom de domaine: THEOFFICE
3. Port 53 -> service du serveur DNS
4. Port 88 -> Kerberos (on peut être certain que c'est le domain controller)
5. Port 389, 636 -> LDAP, LDAP Secure (LDAPS)
6. Port 445 -> SMB
7. Ports 443, 80 -> serveur web (HTTPS)
8. Port 5895 -> WinRM
9. Port 3890 -> RDP
10. Noms des workstations: WKS-01, WKS-02, THE-OFFICE-DC
11. On observe que des dossiers partagés sont disponibles sur le DC (SMB Drives) : accounting, hr

# Challenge /x01:

# Interrogeons les ports

Parmi les ports que vous venez de scanner, déterminez à quels protocoles ceux-ci appartiennent et tentez d'en extraire des informations juteuses.

Vous pourriez avoir besoin de smbclient, ldapsearch, rpcclient, nmap, ...

Hint: certains protocoles admettent que les utilisateurs ne soient pas connectés pour accéder à leurs informations (null authentication)

# Challenge /x01 - Interrogeons les ports

1. `rpcclient -U '' 10.0.1.20`
2. `smbclient -L 10.0.1.20`
3. `smbclient //10.0.1.20/hr`
4. `ldapsearch -h 10.0.1.20 -s base namingcontexts`
5. `ldapsearch -h 10.0.1.20 -x -b "DC=theoffice,DC=lab"`
6. `ldapsearch -h 10.0.1.20 -x -b "DC=theoffice,DC=lab" '(ObjectClass=Person)'`
7. `GetADusers.py -all -dc-ip 10.0.1.20`

# LLMNR Poisoning

*(Link-Local Multicast Name Resolution)*

1. Plusieurs services de Windows utilisent des noms pour identifier les machines (ex.: vous accédez au serveur \\serveur-fichiers-partage\ pour accéder à des fichiers sur un disque réseau partagé
2. Tout nom doit être traduit en IP. Windows se base sur ces protocoles en ordre : DNS, LLMNR, NBT
3. Parfois il arrive qu'on tente de traduire un nom qui n'existe pas. (typo, ancien nom, etc. )
4. Les requêtes de traduction de nom par LLMNR sont envoyées à tous les ordinateurs du réseau et tous peuvent répondre
5. Lorsqu'un attaquant voit passer une requête LLMNR, il y répond avec son IP
6. Le service envoie le hash du mot de passe de l'utilisateur pour authentifier l'utilisateur et lui permettre de compléter son action (ex. : serveur de partage de fichiers)

# Challenge /x02:

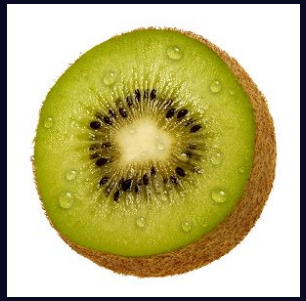
# Password Spray

En utilisant crackmapexec, essayez de vérifier si le mot de passe par défaut des nouveaux employés de la compagnie est valide pour un utilisateur de la liste trouvée.

1. Créez une liste d’utilisateurs contenant seulement les noms d’utilisateurs
2. Trouver la commande de crackmapexec qui permet de faire un password spray

Ajouter d.schrute

# Mimikatz



- Comme mentionné précédemment, Windows garde les hash des mots de passe des utilisateurs connectés depuis la mise en marche de la machine dans la mémoire RAM du processus lsass.exe (Local Security Authority Subsystem Service).
- Certains processus ont accès à la mémoire de processus pour le débogage par exemple.
- 1+1=2! On a développé Mimikatz pour accèder à la mémoire et y récupérer les hash.
- Aussi utile pour récupérer des certificats cryptographiques, des mots de passe de navigateur web, des tickets, ...

```
C:\Users\root\Desktop\mimikatz\x64
λ mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Jul 10 2019 23:09:43
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Key import
```

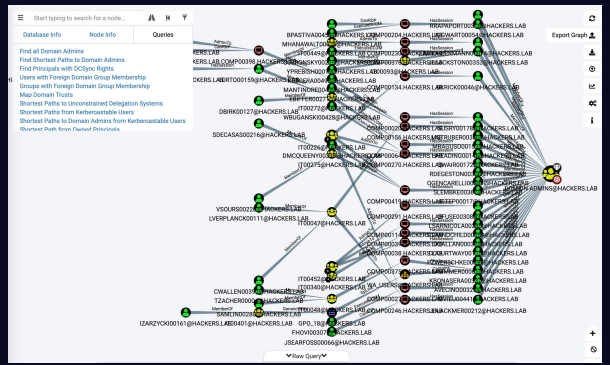
# Challenge /x03:

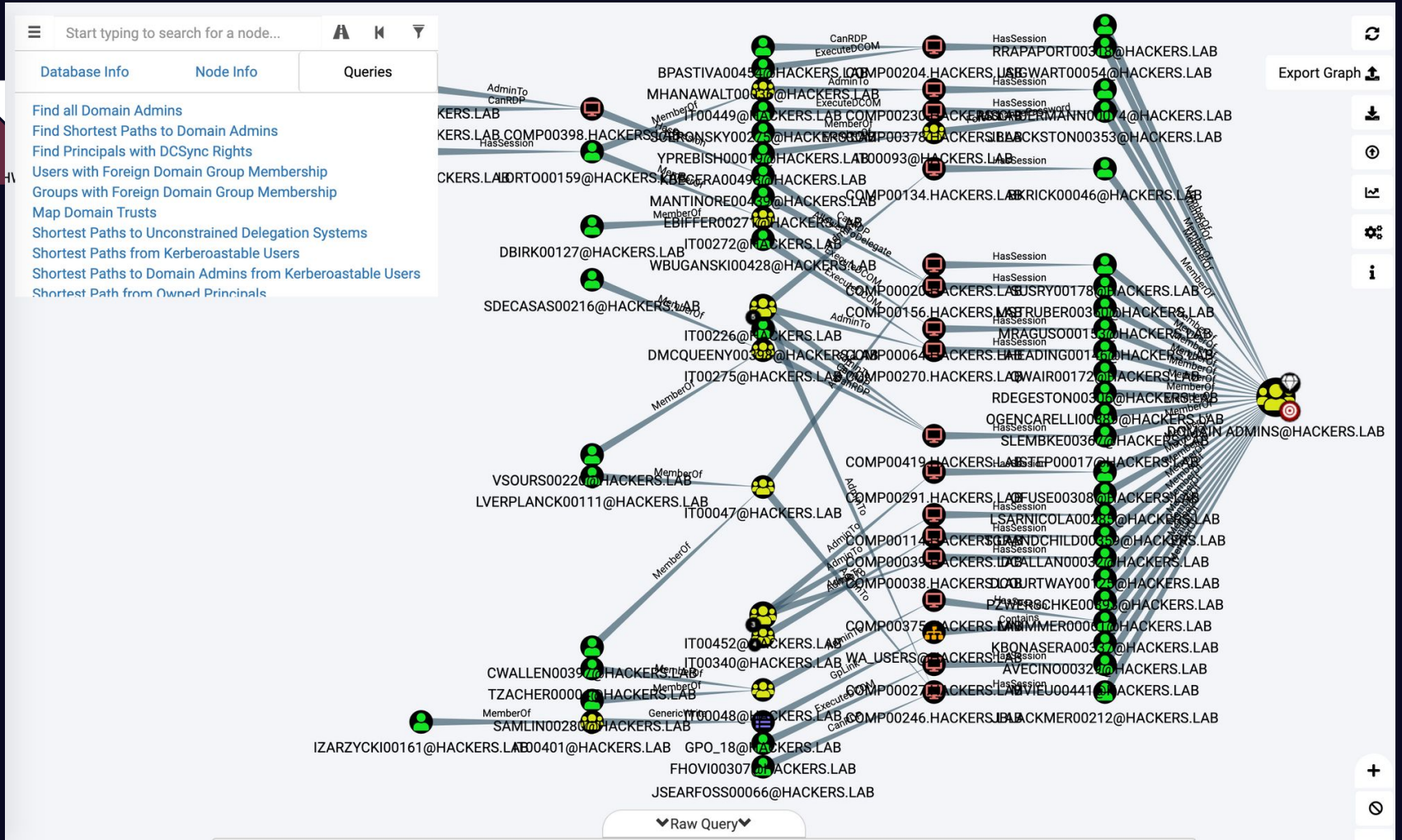
# Reconnaissance interne

Maintenant en possession d’un mot de passe d’un utilisateur, on peut s’authentifier sur une machine en son nom. Tentez de trouver des informations intéressantes sur les machines… comme des hash de mots de passe en mémoire ou encore le graphe du domaine…

# Bloodhound

- Programme très utile qui utilise la théorie des graphes pour trouver des chemins d'exploitation sinon compliqués à trouver et des informations sur le domaine (ex.: trouver le plus court chemin pour être admin, trouver utilisateur "kerberoastable", ...)
- Toute machine connecté au domaine peut demander les infos du domaine au DC.
- En installant Sharphound sur une machine, on peut récupérer ces infos juteuses et les importer dans Bloodhound




Start typing to search for a node...
Database Info
Node Info
Queries
Find all Domain Admins
Find Shortest Paths to Domain Admins
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Map Domain Trusts
Shortest Paths to Unconstrained Delegation Systems
Shortest Paths from Kerberoastable Users
Shortest Paths to Domain Admins from Kerberoastable Users
Shortest Path from Owned Principals
Export Graph
DOMAIN ADMINS@HACKERS.LAB
Raw Query

# Pass-the-hash

- De nombreux protocoles utilisés par Windows comme SMB, psexec, wmiexec et rpc permettent à un utilisateur d'être authentifié sous présentation du hash de son mot de passe (pass-the-hash)
  - Pass-the-hash: si un acteur malicieux met la main sur un hash d'un mot de passe il peut s'authentifier comme l'utilisateur
  - Plus besoin de voler le plaintext password ou besoin de le cracker pour l'utiliser
  - Cela n'est pas une faille, c'est juste le modèle de fonctionnement qui nécessite cette fonctionnalité
- Conditions pour pass-the-hash
  - Compte utilisateur actif
  - Compte administrateur

# Challenge /x04:

# Crackage de hash de mot de passe

À l’aide de hashcat ou de John the Ripper, il est possible d’effectuer une dictionary attack sur le hash capté en spécifiant la wordlist rockyou.txt.

*Hint: il faut trouver le type de hash et le spécifier à Hashcat/JohnTheRipper*

# Challenge /x04 - Crackage

1. Locate rockyou.txt pour le chemin d'accès à la wordlist pour brute-force
2. La commande *hashid* vous permet de déterminer le numéro associé au type de hash afin de le spécifier à Hashcat ou encore https://hashcat.net/wiki/doku.php?id=example_hashes
3. hashcat -m 5600 hashes.txt rockyou.txt -o cracked.txt
4. john --format=netntlmv2 --wordlist=rockyou.txt hash.txt

# Challenge /x06:

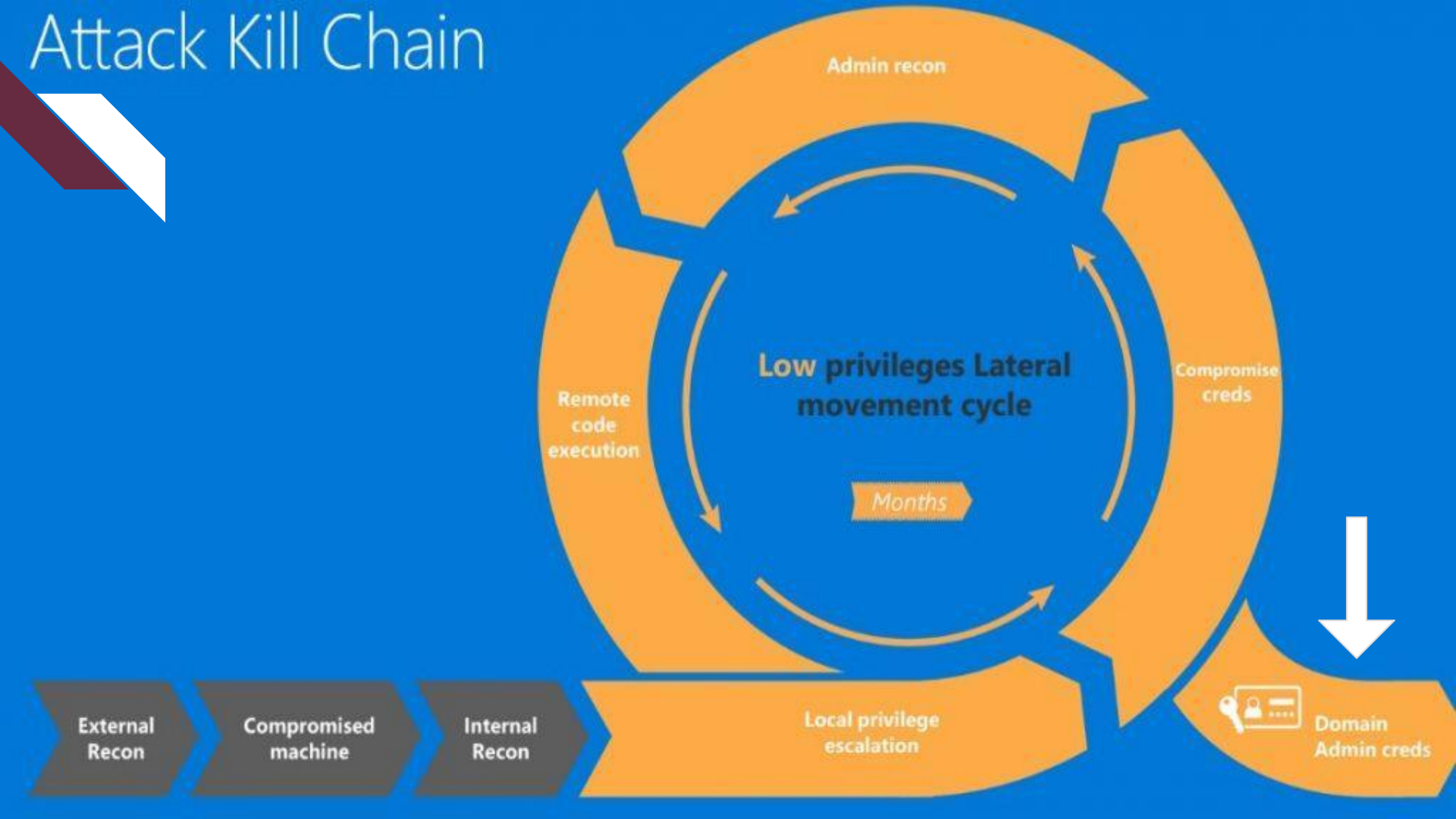
# Élévation de privilèges

À l’aide des informations du domaine (fichiers JSON) récupérées à l’aide de Sharphound, explorez avec Bloodhound quel chemin vous permettrait d’obtenir les droits du groupe Domain Admin

# Challenge /x06 - Privilege Escalation

1. On remarque que l'utilisateur que nous avons compromis (helpdesk) est membre du groupe Organization Management, Exchange Windows Permissions, Exchange Trusted Subsystem Service
2. En cherchant sur Internet, on découvre que ces groupes confèrent suffisamment de pouvoir à l'utilisateur pour qu'il puisse écrire dans le Discretionary Access Control List
3. Exchange Windows Permission est un groupe qui est créé par le programme Exchange Server, un service de serveur mail développé par Microsoft et couramment utilisé en entreprises
4. Le service nécessite beaucoup de privilèges et fonctionne avec Active Directory
5. Tout utilisateur qui est membre de ces groupes peut créer un nouveau compte utilisateur et l'ajouter au groupe Domain Admins
6. L'attaquant crée donc un nouvel utilisateur Domain Admin, s'y connecte et c'est game over pour les sysadmins!
7. En right-cliquant sur le lien du groupe Exchange Windows Permission et Domain Admin dans Bloodhound, on peut choisir l'option Help. Dans le menu qui apparaît, il y a un tab qui mentionne les étapes pour exploiter l'appartenance de l'utilisateur compromis à ce groupe
8. On doit télécharger le script PowerView.ps1 via psexec/wmiexec/evil-winrm puis exécuter les commandes affichées dans Bloodhound

# Attack Kill Chain



# One last thing: DCSync

1. Désormais en possession des privilèges Domain Admins,  on a suffisamment de droits pour faire une attaque DCSync.
2. On prétend être un domain controller en répliquant (*impersonate*) son comportement  de réplication du domaine lorsqu'un DC doit transférer son contenu vers un autre DC qui se joint à la forêt afin que ce dernier puisse fonctionner correctement et soit indépendant pour fonctionner.
3. Le Directory Replication Service Remote Protocol par les outils d'exploitation
4. But: obtenir les hash de mots de passe des utilisateurs du domaine et d'autres info sur ces comptes
5. Exemple d'outils
    a. mimikatz "lsadump::dcsync /domain:theoffice.lab"
    b. Secretsdump.py de Impacket

# Résumé

1. Bases d'Active directory et de Windows (types de comptes, permissions et groupes, hash)
2. Reconnaissance de systèmes AD
3. Attaques communes:
    - LLMNR poisoning
    - Pass-the-hash
    - password spraying
    - Mimikatz
    - privilege escalation
    - DCSync
4. Outils: impacket scripts, crackmapexec, bloodhound et sharphound, mimikatz

# Boîtes à outils

D’autres outils  fréquemment utilisés

1. Impacket scripts
2. Responder
3. Crackmapexec
4. Evil-winrm
5. Rubeus
6. Kerbebrute
7. Mimikatz
8. Metasploit Framework
9. Bloodhound & Sharphound
10. Powerview
11. ntlmrelayx
12. Panoplie d’autres scripts adaptés à vos besoins se retrouvent sur Github

# Créez votre propre laboratoire AD

Meilleure façon d'apprendre le fonctionnement d'AD, comment l'installer le configurer, l'attaquer et le défendre

1. VMWare/VirtualBox sur votre PC avec au moins trois VM (Domain controller, client and attaquant):
    a. ~16 GB of RAM (2 GB ea.)
    b. 60 GB of hard drive (20 GB ea.)
    c. CPU
    d. Windows Evaluation Versions (.iso) expirent après 180 jours (Microsoft Evaluation Center)
    e. 2 cartes réseau (réseau du laboratoire, l'autre pour accéder à Internet pour l'installation et màj)
2. Azure (ou Amazon Web Services):
    a. En utilisant les abonnements étudiants et les démos gratuites
    b. Plus flexible (nombre de machines) et meilleures performances

# Désireux(se) d’en apprendre plus?

1. Environnements d’apprentissage
   a. Hack the Box : lisez les write-ups et faites des machines Windows!
   b. PentesterAcademy : Attacking and Defending Active Directory course (intermédiaire)
   c. TryHackMe : Throwback Network Labs : Attacking Windows Active Directory
2. Liste bien garnie de méthodes d’exploitation
3. Playlist de VBScrub sur les fondements d’AD pour les CTF
4. Explications simplifiées de plusieurs attaques
5. Framework d’attaques des groupes persistants
6. Bon blog pour apprendre certains fondements de l’exploitation
7. Blog traitant régulièrement d’attaques et de défense d’AD
8. NSEC 2019 Windows Track Walkthrough: exploitation réaliste et avancée d’un réseau AD