LOGIN SÉCURITÉ

RETEX Internal Pentesting

LOGIN SÉCURITÉ

CONSEIL & GOUVERNANCE	AUDIT & TEST D'INTRUSION	FORMATION	INTEGRATION DE SOLUTION	SECURITE OPERATIONNELLE

Accompagner la DSI dans la définition et la mise en œuvre de leur stratégie de ***Confiance Numérique****.*

30
COLLABORATEURS

3
M€ DE CA

14
ANS D'EXPÉRIENCE

CYBERSECURITÉ & RÉSEAU

Nos équipes délivrent des prestations de conseil, d'intégration, de services managés et de formation, **sur site** ou depuis notre **centre de Cybersécurité (SOC).**

Login Sécurité apporte des réponses opérationnelles dans une **démarche de gestion des risques**, créatrice de valeur à long terme pour ses clients.

AB8

AGENDA

+ Pentest ?
+ Démarche technique
+ Vulnérabilités récurrentes
+ Nos Conseils

Slide 3

AB8 todo

Alexis Beaufils; 11/10/2018

POURQUOI ORGANISER UN PENTEST

Tester vos défenses dans des conditions « presque » réelles.

Objectifs :

- Identifier les faiblesses de mon SI
- En comprendre les risques, les impacts
- Recevoir des conseils précis de correction pour une sécurité pragmatique

C’est un vision très opérationnelle de la sécurité du SI ,

Beaucoup plus concrète que l’analyse de risque.

PENTEST, QUELLE APPROCHE CHOISIR ?

Différentes approches selon votre maturité :

- Blackbox, Greybox, Whitebox ?
- RedTeam ?
- Une approche collaborative du Pentest offre un meilleur ROI.

DÉMARCHE TECHNIQUE

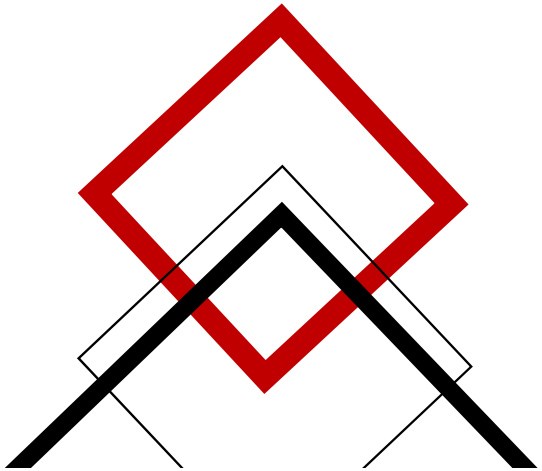
METHODOLOGIE TRADITIONNELLE

- Information gathering
- Cartographie et énumeration
- Recherche de vulnérabilité
- Exploitation
- Élévation de privilège
- Maintien d'accès
- Propagation

APPROCHE SPÉCIFIQUE

- Chaque machine du SI est une cible potentielle

- Peut on compromettre toutes les machines d'un coup ?



DÉMARCHE TECHNIQUE

Le Pentest débute traditionnellement avec l'accès à une prise réseau.

- Pas de compte sur le Domain => 1° Objectif
- Connaissance restreinte de l'infra interne => Scan de vulnérabilité

A partir d'un premier compte utilisateur, on cherche à élargir sa connaissance du SI

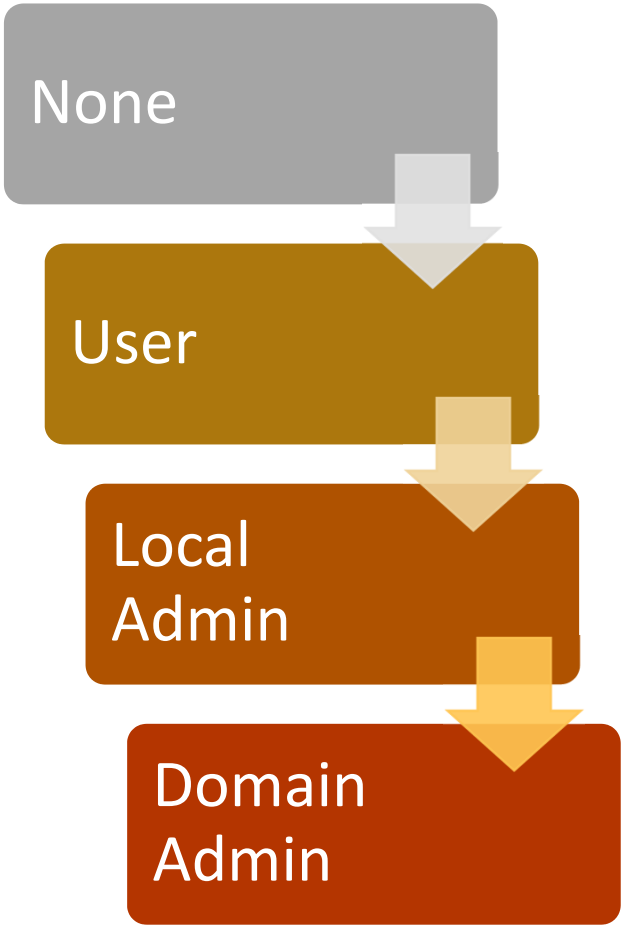
- Lister les utilisateurs, machines, services, droits … => Trouver un cheminement pour élever nos droits sur le SI

Exploitation de vulnérabilités :

- Accès Admin local => Credential Gathering

Escalade de privilèges AD :

- Accès d'Administration sur le domain




LES ATTAQUES
TRADITIONNELLES

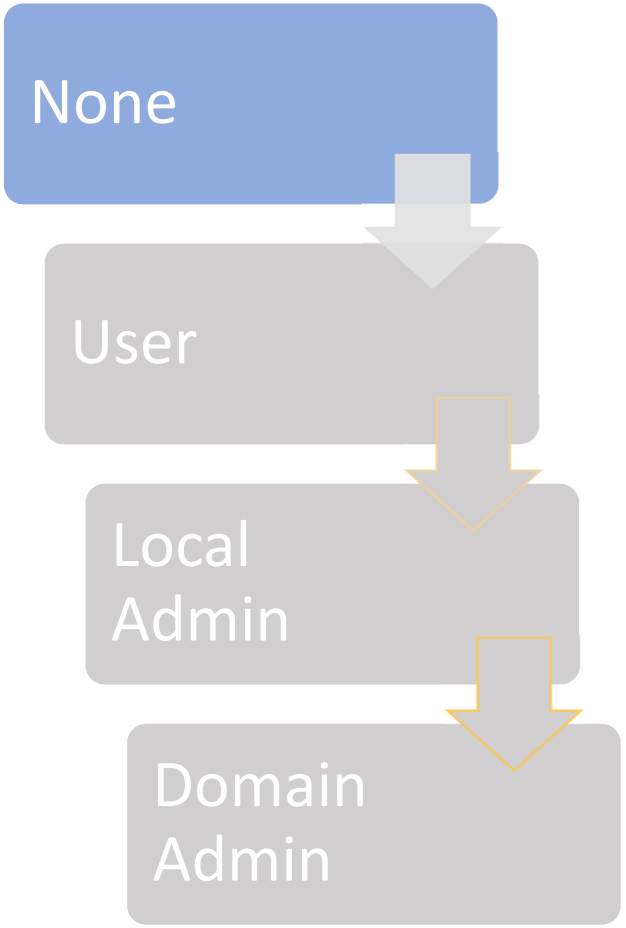
DÉMARCHE TECHNIQUE

Le Pentest débute traditionnellement avec l'accès à une prise réseau.

- Pas de compte sur le Domain => 1° Objectif
- Connaissance restreinte de l'infra interne => Scan

Scénarios potentiels :

- Mots de passe faible

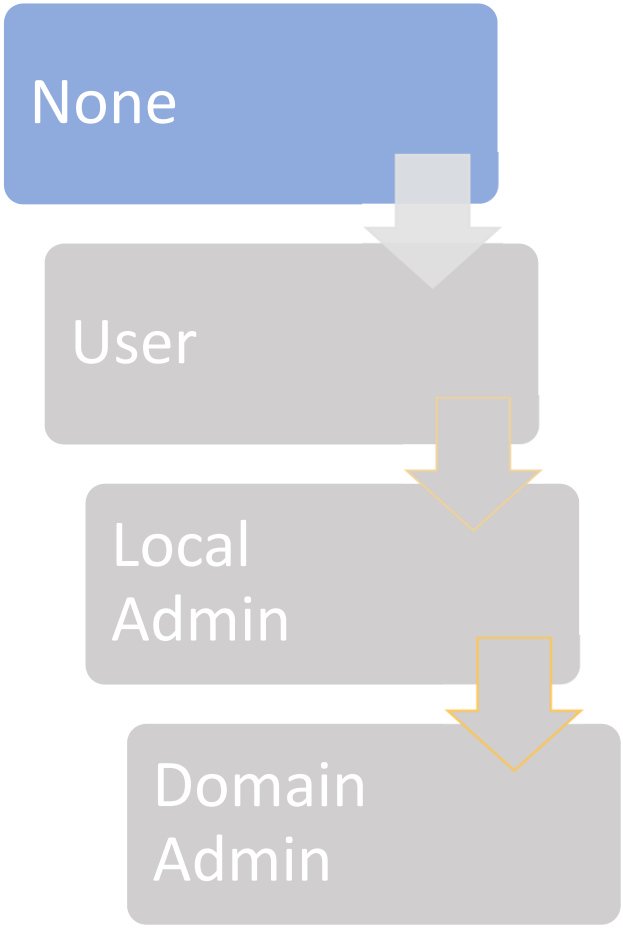


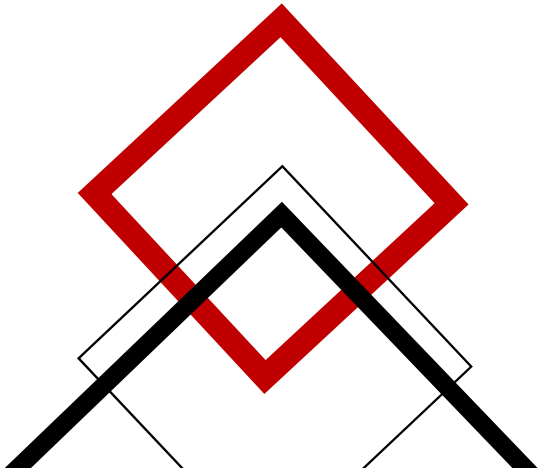
WEAK PASSWORD

On retrouve presque toujours des passwords faibles au sein d'un SI

- Comptes génériques, comptes partagés
- Politique de MDPasse inadapté

- Attaque par Password Spraying
  - MachineName = login = pass
  - Societe2019 :-/





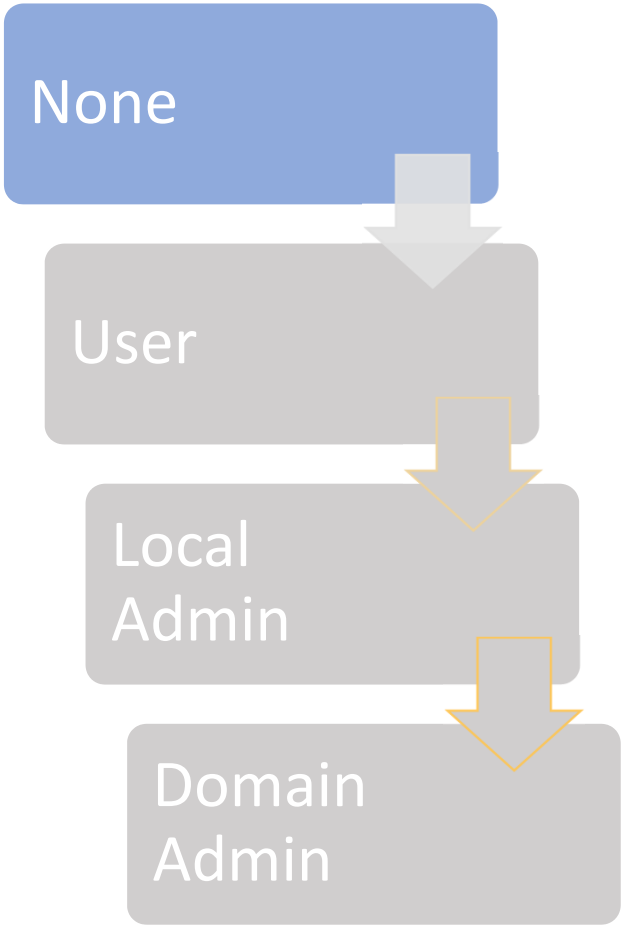
DÉMARCHE TECHNIQUE

Le Pentest débute traditionnellement avec l'accès à une prise réseau.

- Pas de compte sur le Domain => 1° Objectif
- Connaissance restreinte de l'infra interne => Scan

Scénarios potentiels :

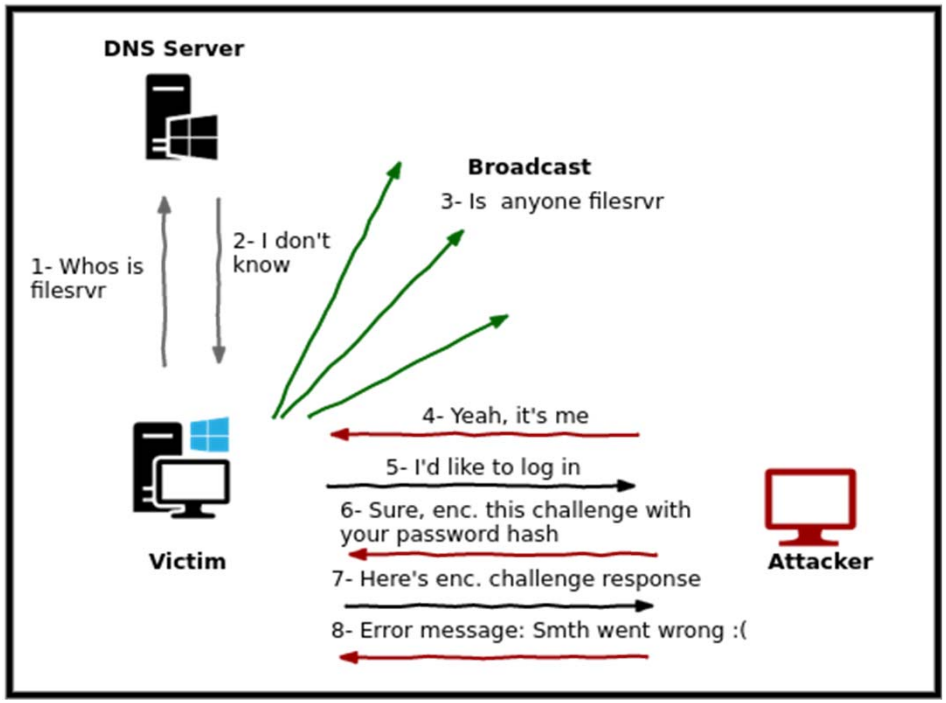
- Mots de passe faible
- Interception / MITM

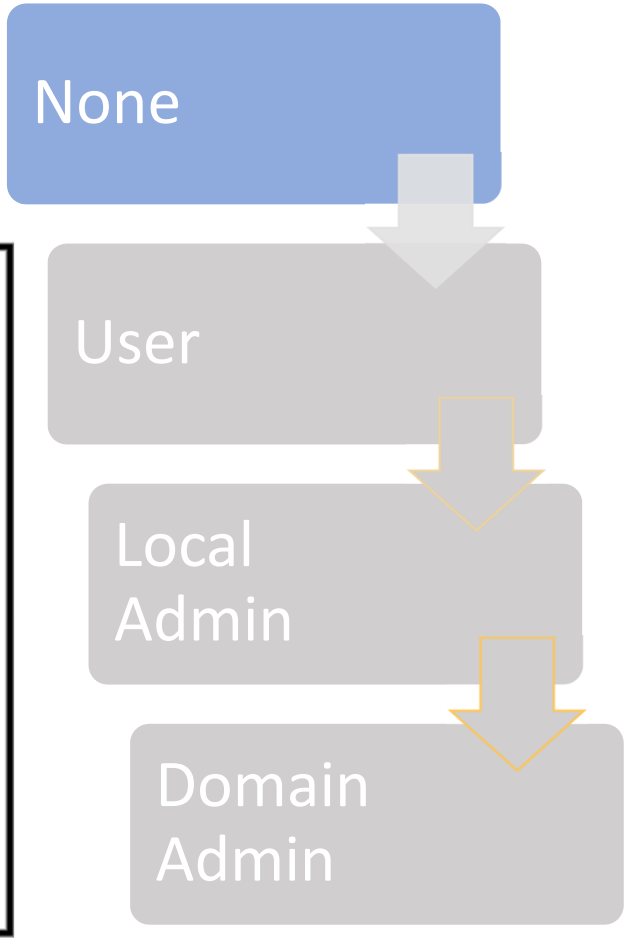


INTERCEPTION & RELAYING

De nombreuses possibilités pour capturer du traffic :

- ARP spoofing
- LLMNR-NBNS (Responder -Laurent Gaffie)
- MITM6 (@_dirkjan)





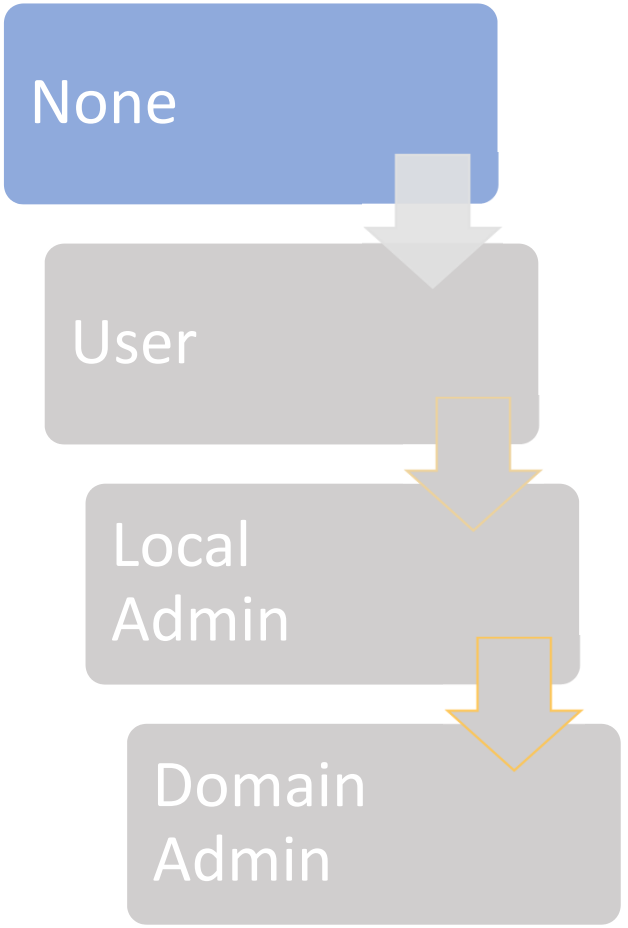
INTERCEPTION & RELAYING

De nombreuses possibilités pour capturer du traffic :

- ARP spoofing
- LLMNR-NBNS (Responder -Laurent Gaffie)
- MITM6 (@_dirkjan)

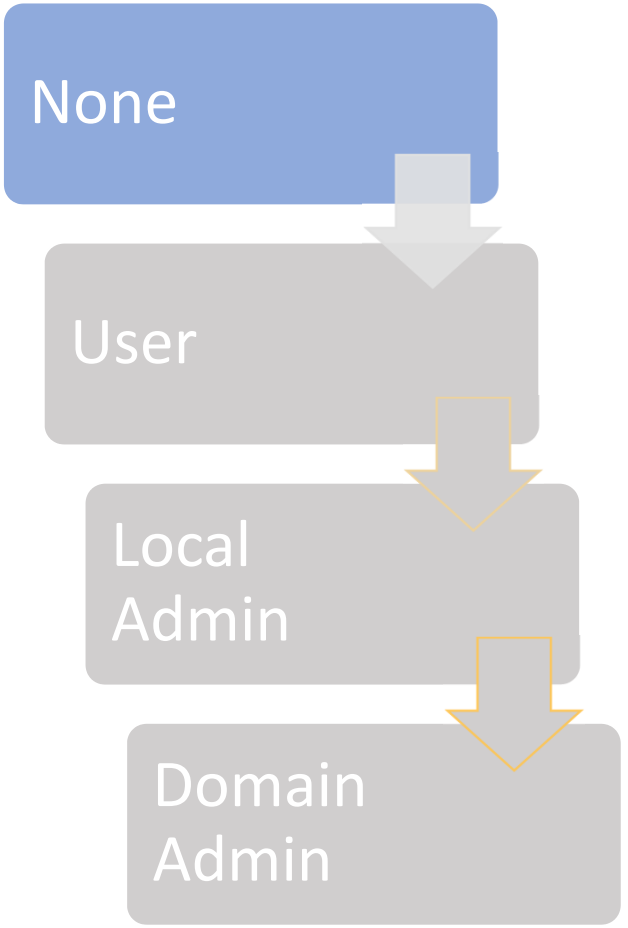
Possibilité de générer du traffic :

- Partage réseau
- Phishing



WEAK PASSWORD

- BruteForce de MDP offline
  - 100 Milliards de hash NTLM/sec
  - 25 Milliards de hash NetNTLMv2/sec
    - 8 caractères random
      - => 72h
    - Mot du dictionnaire + 4chiffres + 1 spécial + 2 permutations
      - <3minutes
- Un bon mot de passe c'est :
  - Un MDP unique !
    - Utilisez un gestionnaire de MDP/Coffre fort (Keepass, lastpass, dashlane …)
  - Complexité de 12caratères, réellement aléatoire
    - Faites une phrase
  - Durée de vie plus longue



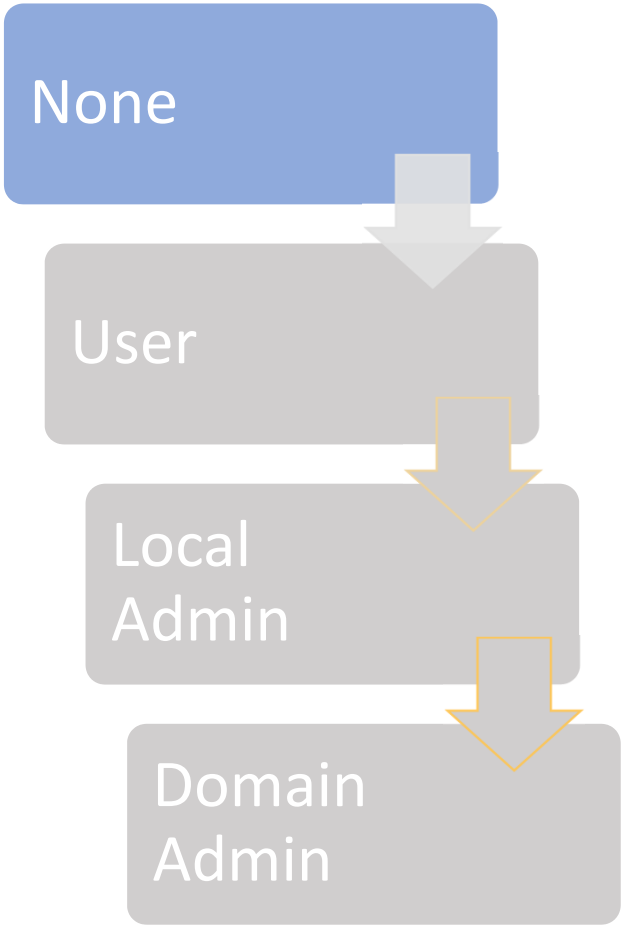
DÉMARCHE TECHNIQUE

Le Pentest débute traditionnellement avec l'accès à une prise réseau.

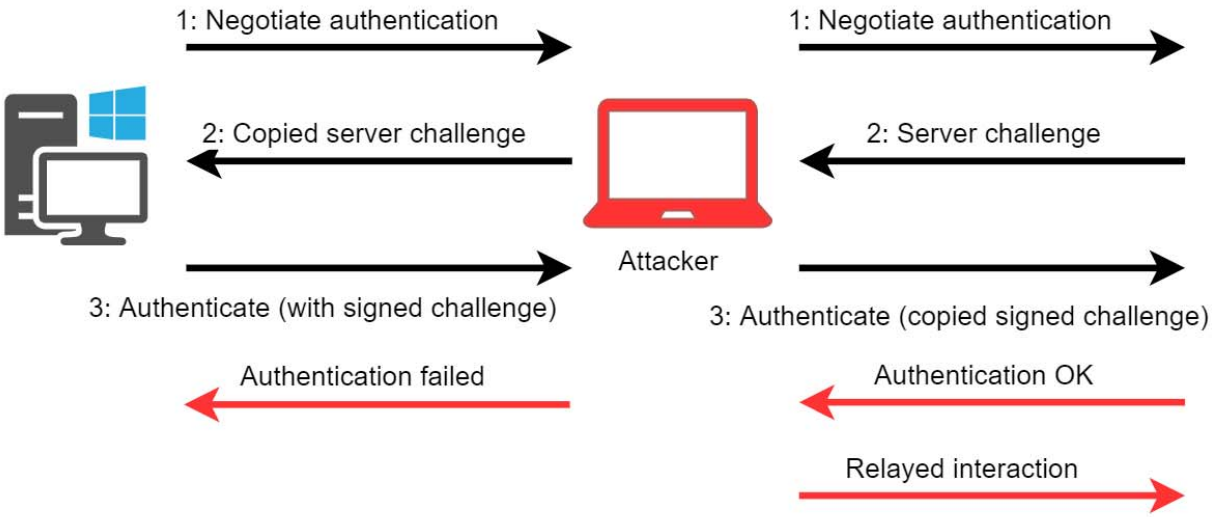
- Pas de compte sur le Domain => 1° Objectif
- Connaissance restreinte de l'infra interne => Scan

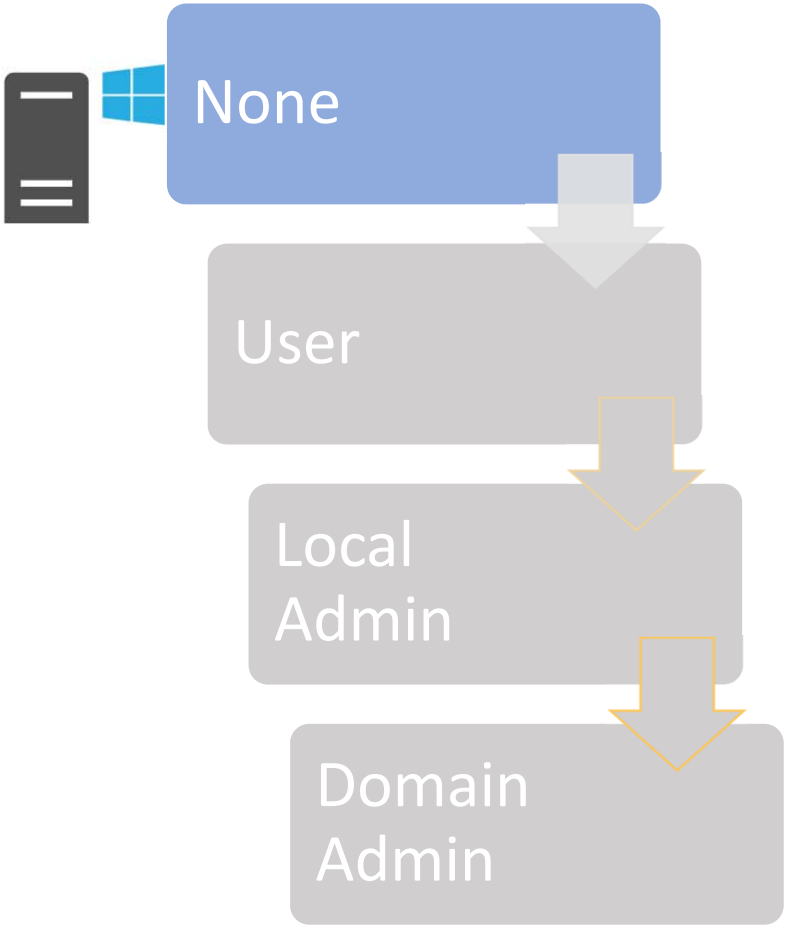
Scénarios potentiels :

- Mots de passe faible
- Interception / MITM
  - Relaying



INTERCEPTION & RELAYING





Pour contrer cela, Microsoft introduit le SMB Signing … dans Windows 98 !

Il est activé par défaut sur les Domain Controllers à partir de Windows 2003

Est-ce suffisant ?

- **CVE-2019-1166 : Drop the MIC (**https://www.preempt.com/**)**
- **CVE-2019-1338 : Drop the MIC 2**

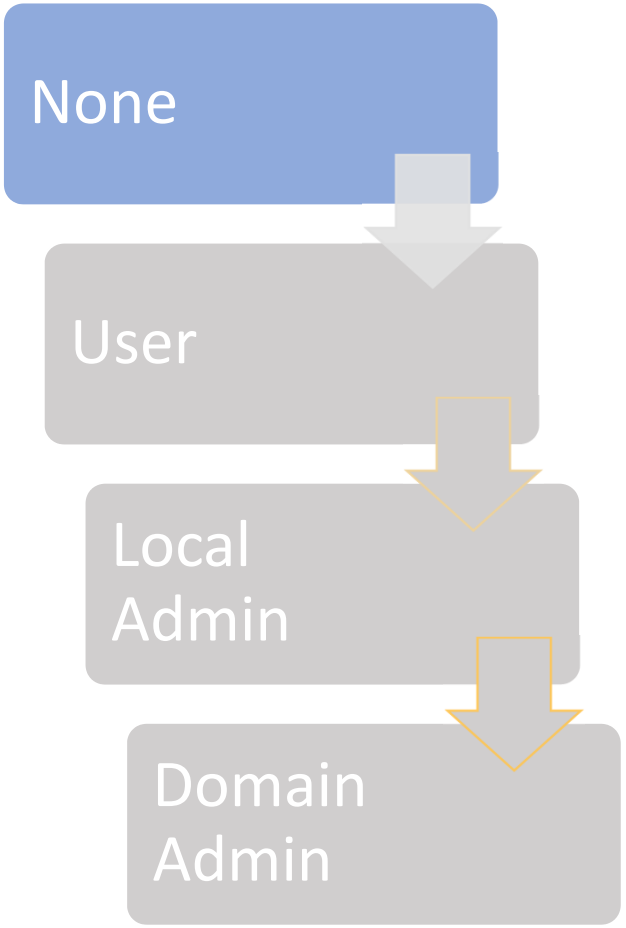
DÉMARCHE TECHNIQUE

Le Pentest débute traditionnellement avec l'accès à une prise réseau.

- Pas de compte sur le Domain => 1° Objectif
- Connaissance restreinte de l'infra interne => Scan

Scénarios potentiels :

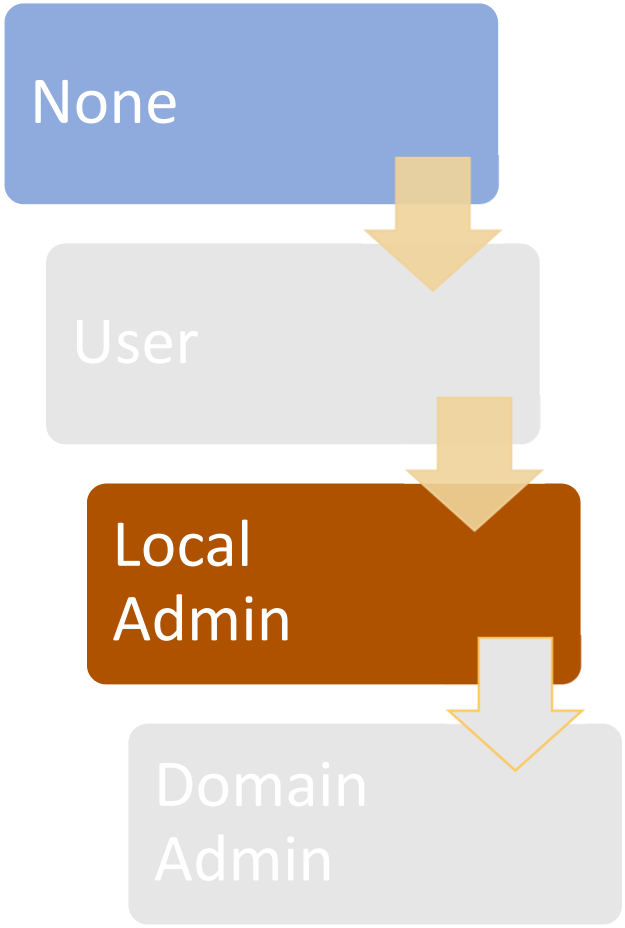
- Mots de passe faible
- Interception / MITM
  - Relaying
- Manque de mise a jour



MANQUE DE MAJ == VULNÉRABILITÉ LOGICIELLE CONNUE

- On retrouve encore des postes vulnérable à MS17_010 chez 75% de nos clients.
- Cette vulnérabilité permet, en exploitant SMBv1, d'obtenir un Remote Code Execution ayant les droits d'accès SYSTEM

- Plus de 200 vulnérabilités par jour (https://www.cvedetails.com/)
- 50K exploits sur exploit-db.com
- UPDATE !
- Mettre en place un process de patch managment
- S'outiller en conséquence : Cyberwatch



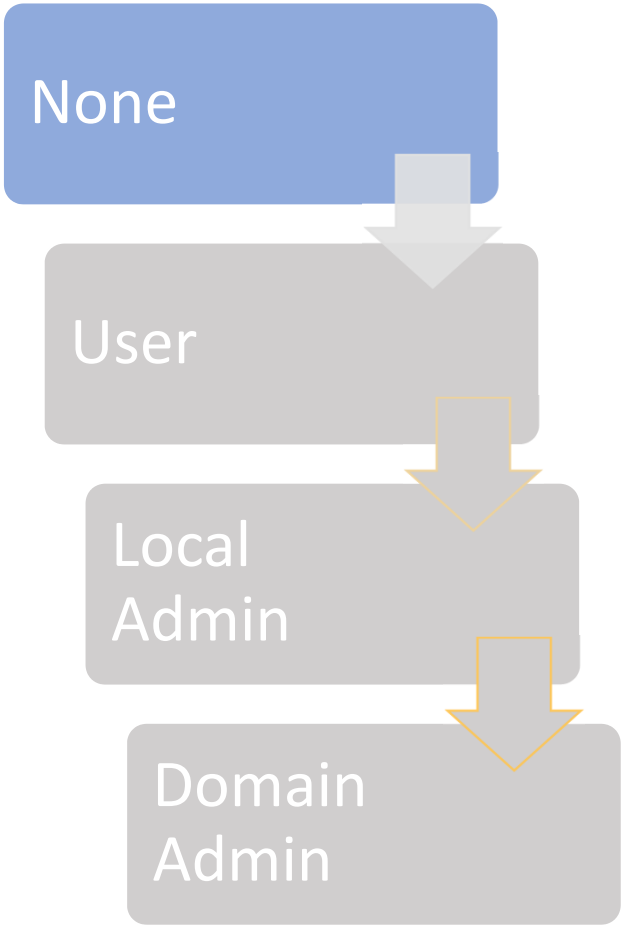
DÉMARCHE TECHNIQUE

Le Pentest débute traditionnellement avec l'accès à une prise réseau.

- Pas de compte sur le Domain => 1° Objectif
- Connaissance restreinte de l'infra interne => Scan

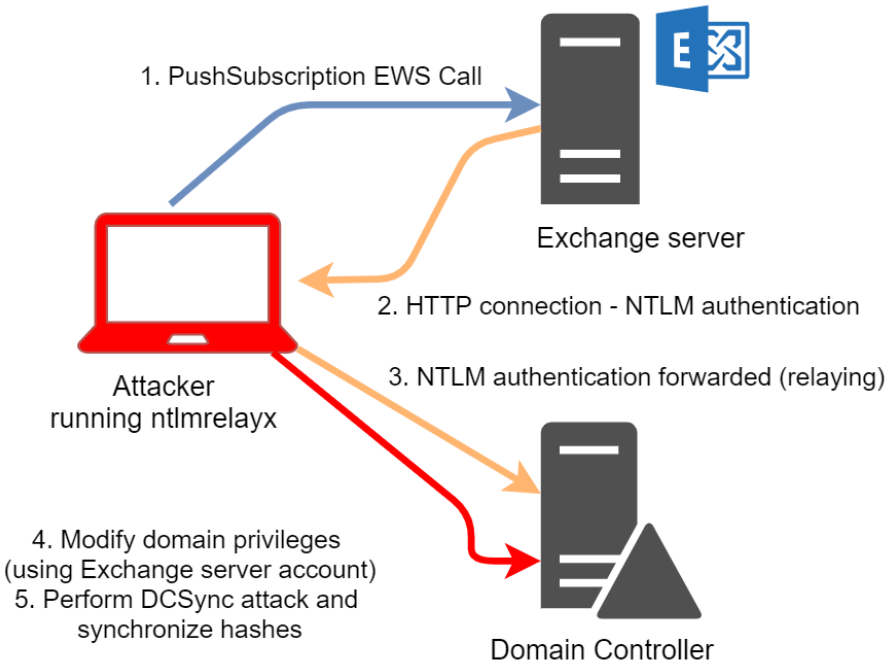
Scénarios potentiels :

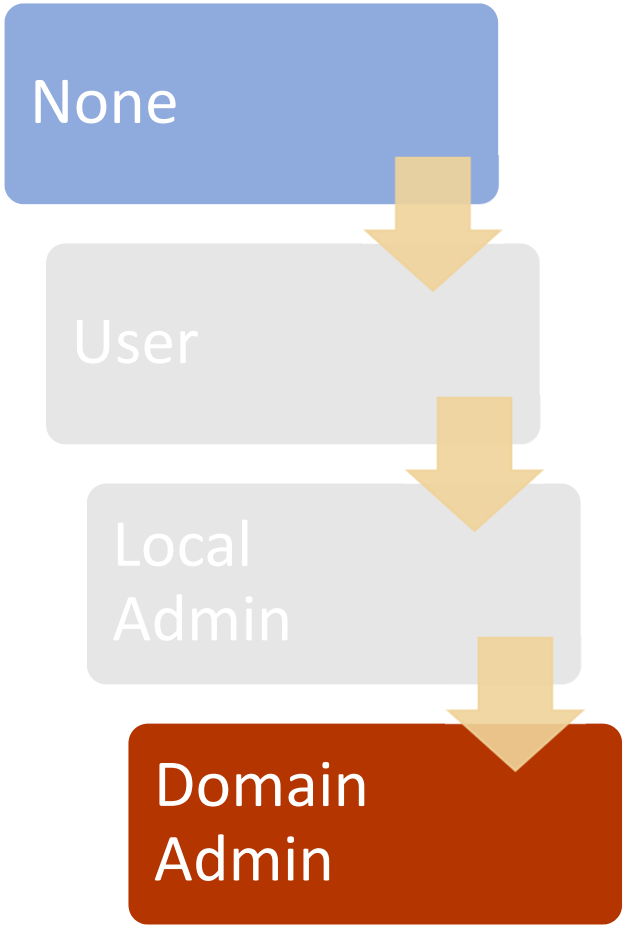
- Mots de passe faible
- Interception / MITM
  - Relaying
- Manque de mise a jour
- Mot de passe par défaut
- Applicatifs web interne



MANQUE DE MAJ + NTLM RELAYING == ¯_(ツ)_/¯

- PrivExchange + NTLM Relay + DropTheMic == ?





- https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/

DÉMARCHE TECHNIQUE

A partir d'un premier compte utilisateur, on cherche à élargir sa connaissance du SI

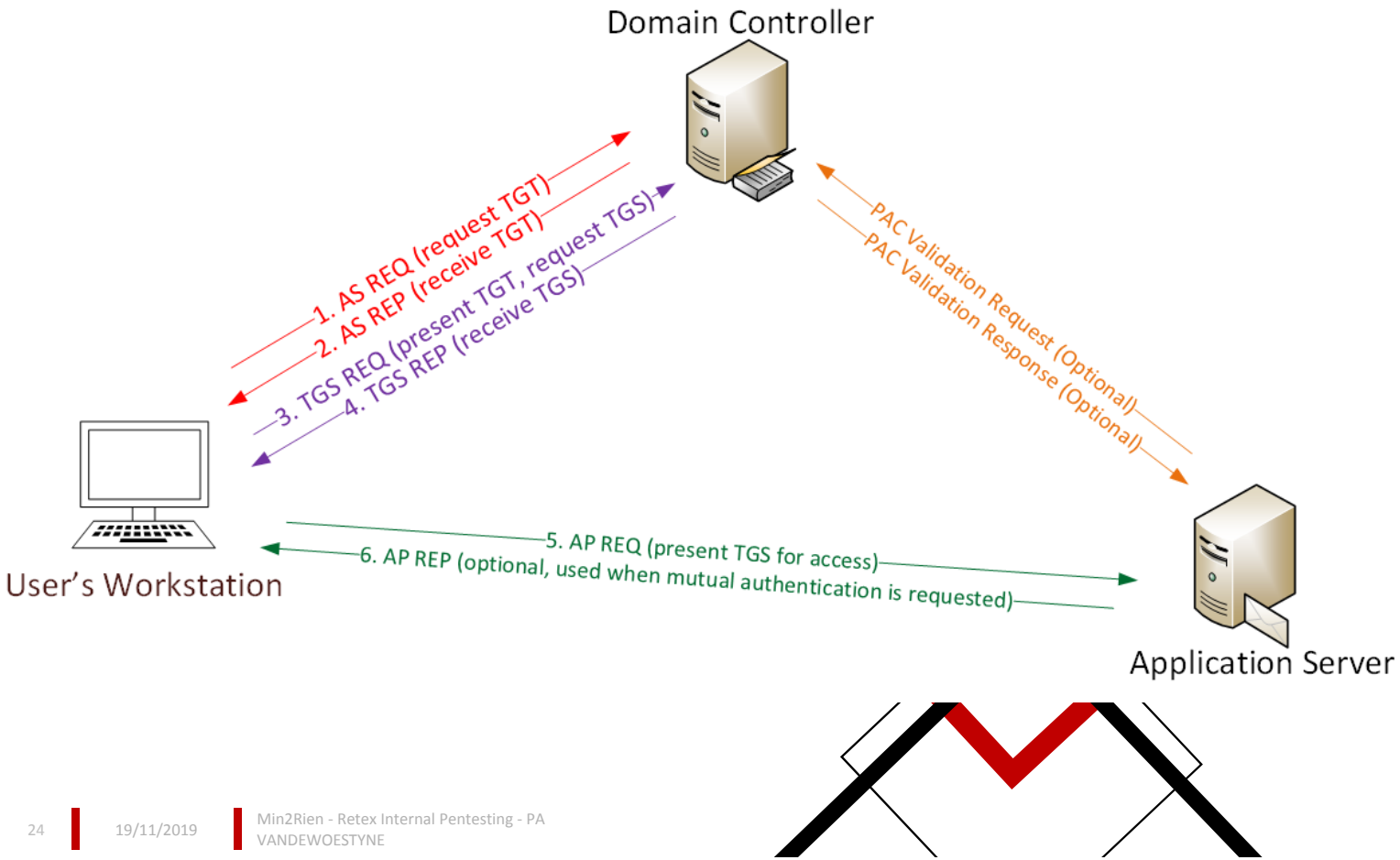
- Lister les utilisateurs, machines, services, droits … => Trouver un cheminement pour élever nos droits sur le SI

Scénarios potentiels :

- AD Enumeration :
  - Domains, DomainControllers, DNSNodes, DNSZones
  - OU, Forest, GPLink
  - Subnets, Sites, Trusts
  - Groups, GroupMembers
  - Users, UserSPNs
- Kerberoasting

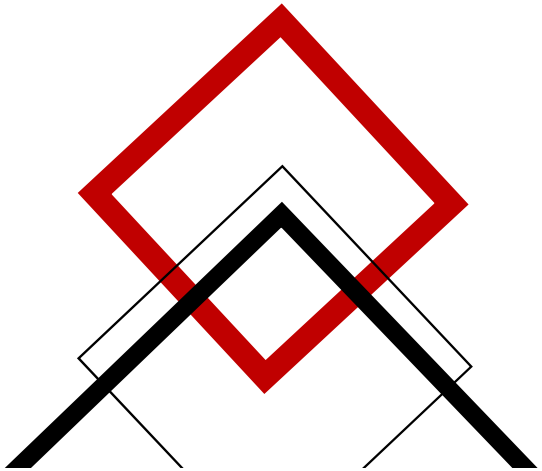
KERBEROASTING

- Dès que l'on a un compte sur l'AD, on peut demander à s'authentifier à des services



KERBEROASTING

- Dès que l'on a un compte sur l'AD, on peut demander à s'authentifier à des services
- Les services sont attachés à un SPN (ServicePrincipalName)
  - Ce SPN peut être lié à un « computer account » ou à un « user account »
- Pour cela on demande au DC un TGS, qui est chiffré avec le password du Server. On peut alors tenter de cracker le password Offline

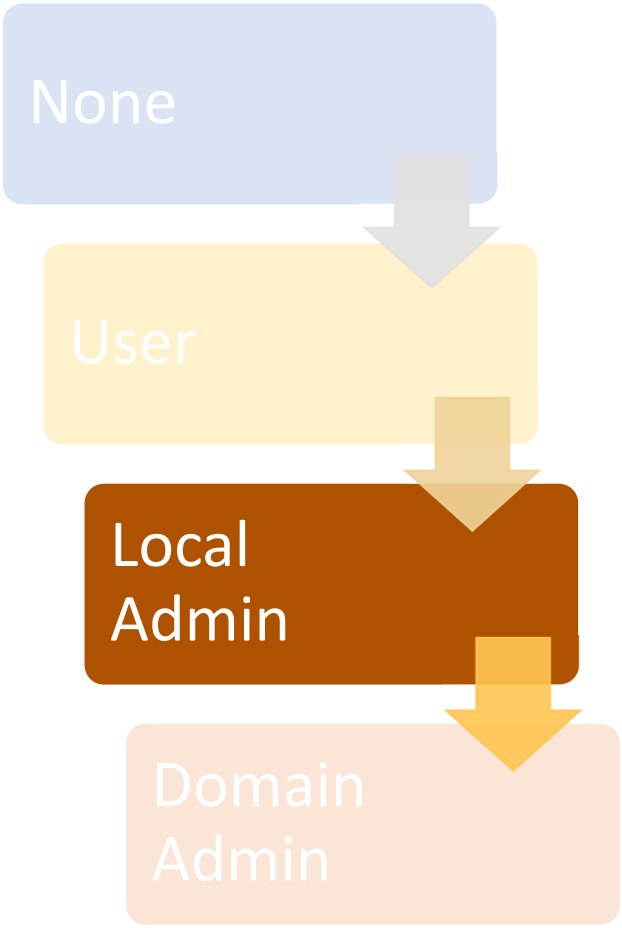


DÉMARCHE TECHNIQUE

Mes utilisateurs sont admin de leurs postes ?

Scénarios potentiels avec un Accès Admin local :

- Local Passwords Dumping



LOCAL PASSWORD DUMPING

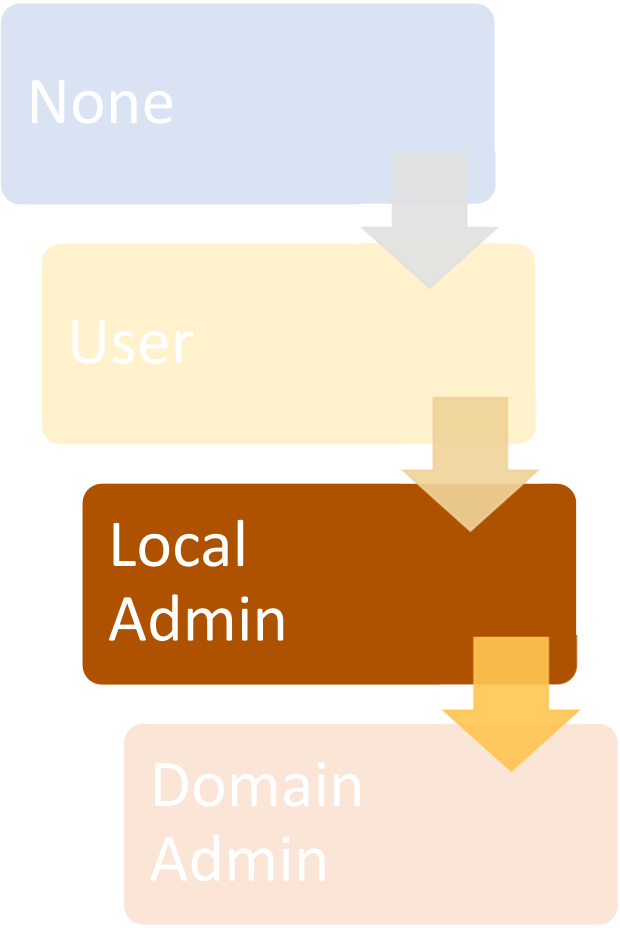
Avec des droits système on peut accéder à

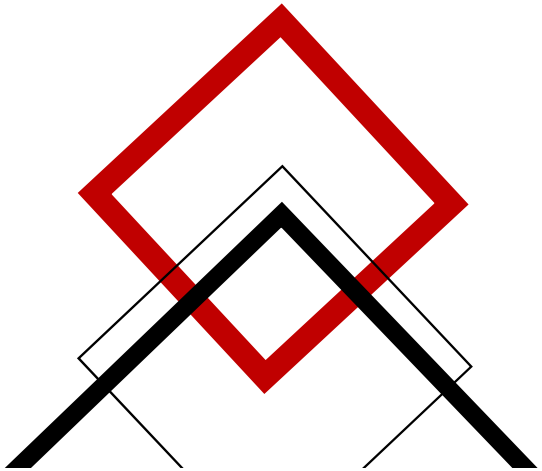
- Base de hash locale (SAM)
- Passwords locaux (VNC, Wifi, VPN, RDP, navigateurs …)
- Mémoire de LSASS (Mimikatz – benjamin delpi)

Risques de password reuse

Meme avec un MDPass complexe, il sera possible de se connecter avec le hash.

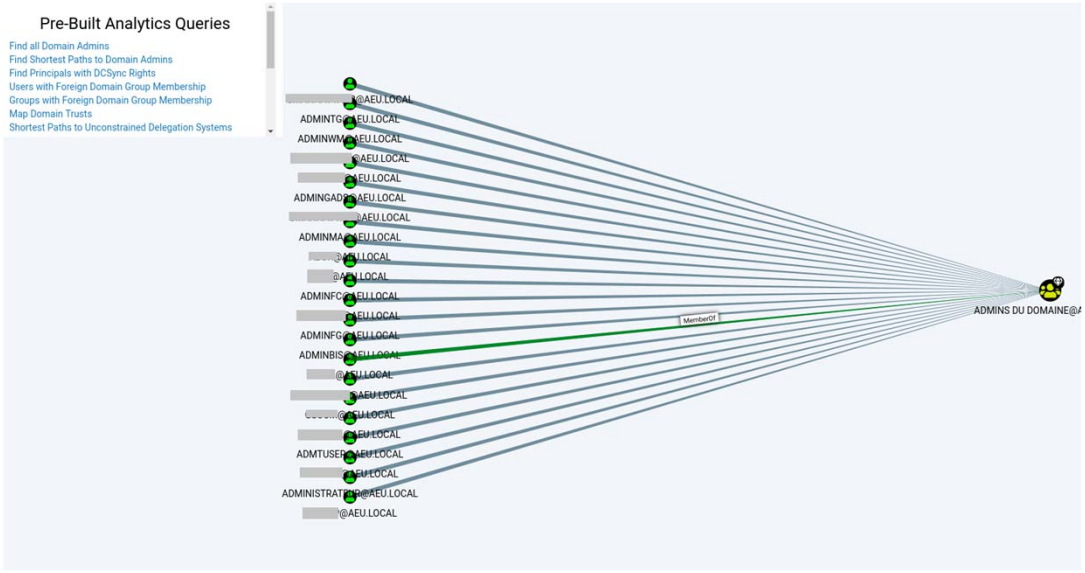
- Psexec, Smbexec …

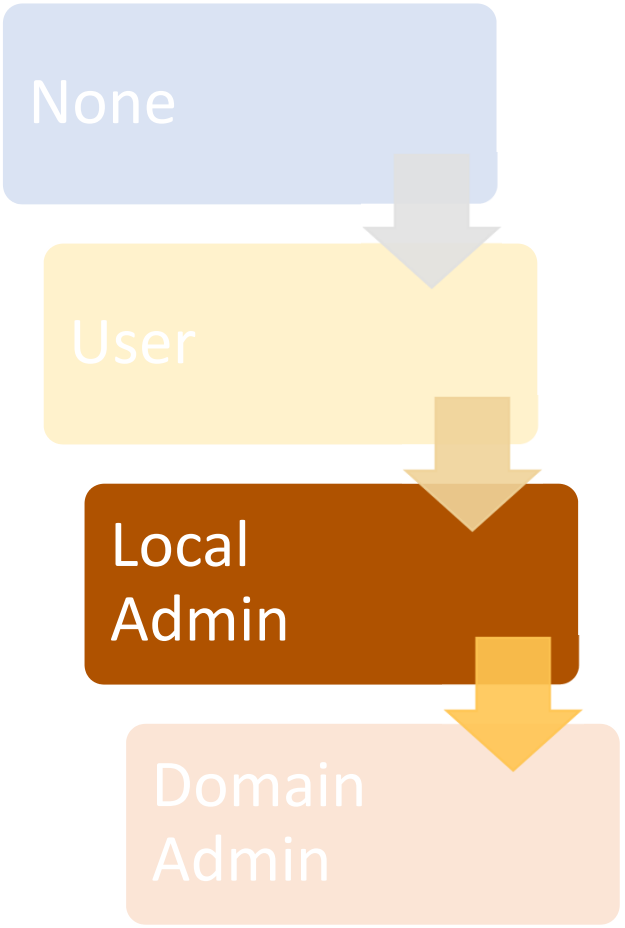




PRIVILEGE ESCALATION AD

- Nous avons collecté beaucoup d'informations sur l'AD, les machines, les droits, les utilisateurs, les sessions …
- On modélise ces informations : BloodHound (@wald0, @CptJesus, @harmj0y)





CREDENTIAL ESCALATION

Avec un compte administrateur local, il est possible de récupérer des identifiants conservés sur le poste :

- Accès direct a LSASS
- Mimikatz

Depuis Windows 8.1 et 2012R2 il est possible d'interdire le stockage des mots de passe en clair ou sous forme de hash LM en modifiant la clef de registre suivante:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest "UseLogonCredential"(DWORD) à 0

Mimikatz va permettre d'interagir avec ce service LSASS pour en extraire les informations importantes.
Exemples :

```
mimikatz "privilege::debug" "sekurlsa::logonpasswords" exit
```


NOS CONSEILS

CONSEILS

- UPDATE
- Politique de mot de passe cohérente :
  - 12 caractères, pas de mot du dictionnaire, durée de vie allongée
- Seriously … UPDATE !
- Utilisateur != Administrateur
- Credential Reuse => LAPS
- Faites tester vos développements internes.
- UPDATE ☺
- Prévenir / Limiter / Surveiller
  - Prévenir : identifier les vulnérabilités pour les faire disparaitre
  - Limiter : pour les risques « non patchables », limiter le scope de leur impact
  - Surveiller : tout ce que l'on ne peut garantir doit être surveillé.

SOURCES

- Harmj0y : https://www.harmj0y.net/
- Dirk-jan Mollema **:** https://dirkjanm.io/
- Pixis : https://beta.hackndo.com/
- Byt3bl33d3r : https://byt3bl33d3r.github.io/
- Responder : Laurent Gaffie
- Mimikatz : Benjamin Delpy @gentilkiwi
- Impacket : http://secureauth.com/

MERCI

?

pav@login-securite.com

www.login-securite.com