

The logo for ESGI, featuring the letters 'ESGI' in a bold, black, sans-serif font. A blue eye-like shape is integrated into the letter 'E'.

école supérieure de
génie informatique



INTRINSEC
Innovative by design

Les phases de reconnaissance : clef du
succès d'un test d'intrusion interne



ESGI Security Day – 02/05/2023

Qui sommes-nous ?





Margaux **DABERT**



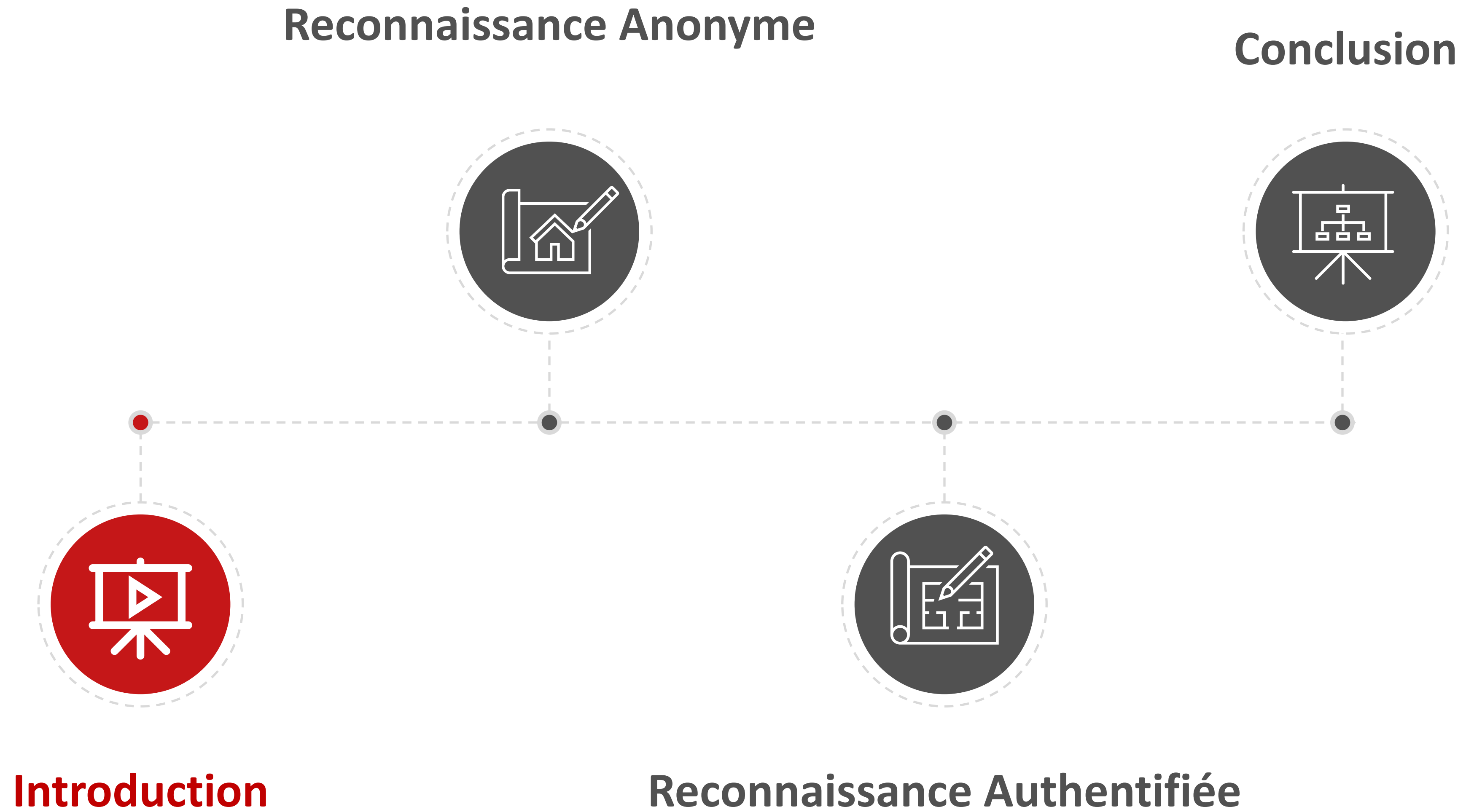
-  Consultante en cybersécurité - Pentester
-  Chez Intrinsec depuis 2021

Paul **SALADIN**



-  Consultant en cybersécurité - Pentester
-  Chez Intrinsec depuis 2021

Plan



Reconnaissance dans un milieu Active Directory

- Test d'intrusion : reconnaissance / exploitation / post exploitation
- Phases de reconnaissance
- Anonyme VS Authentifié : intrusion physique / phishing ou collaborateur malveillant

Pourquoi la reconnaissance est-elle la clef pour réussir un test d'intrusion interne ?

Reconnaissance dans un milieu Active Directory

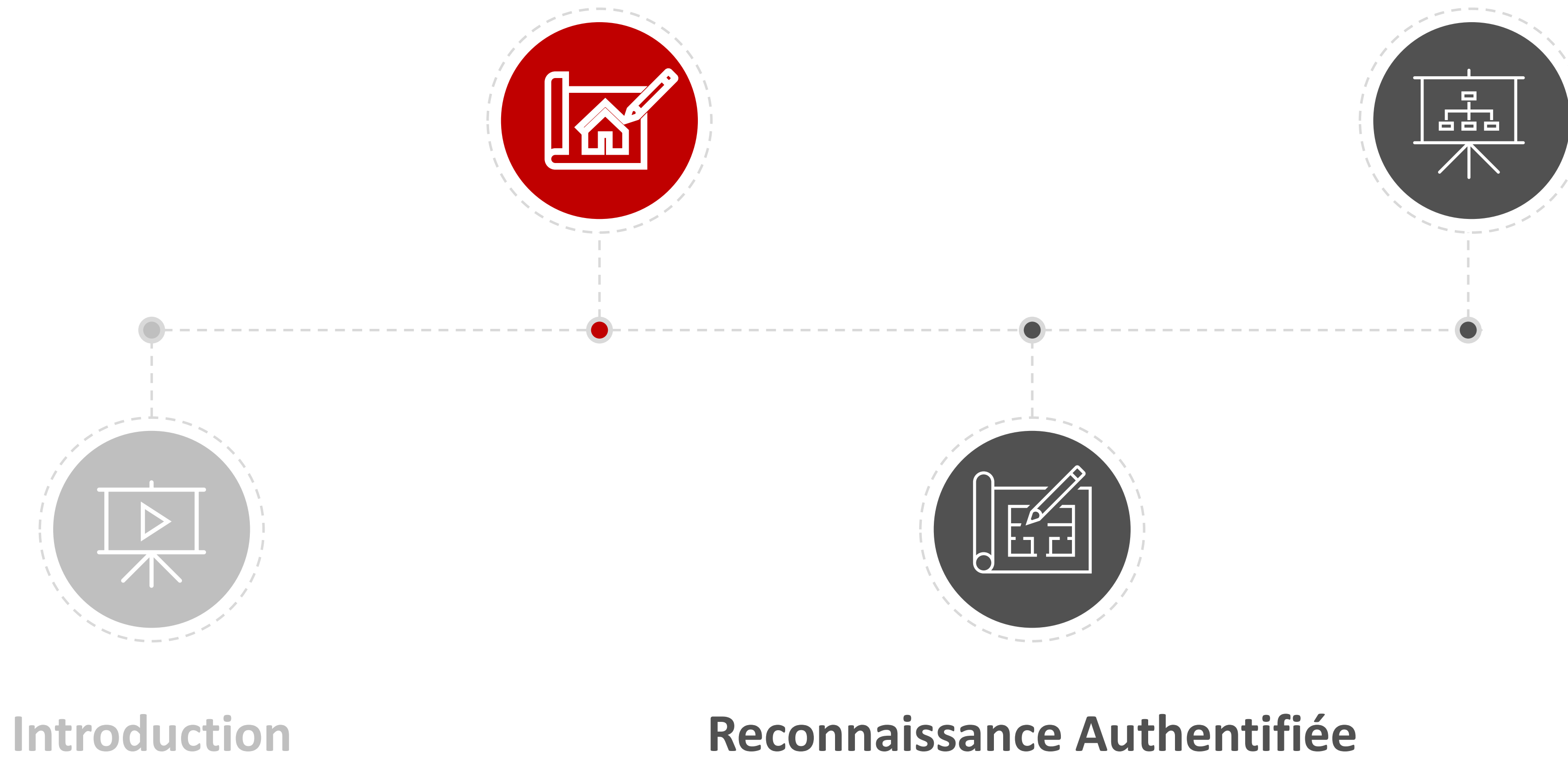
What's next

- Présentation d'un exemple de méthodologie
- Certains outils seront évoqués, il en existe beaucoup d'autres
- Les dimensions Azure et Microsoft 365 ne seront pas abordées
- Les exemples sont tirés du lab d'Intrinsec

Plan

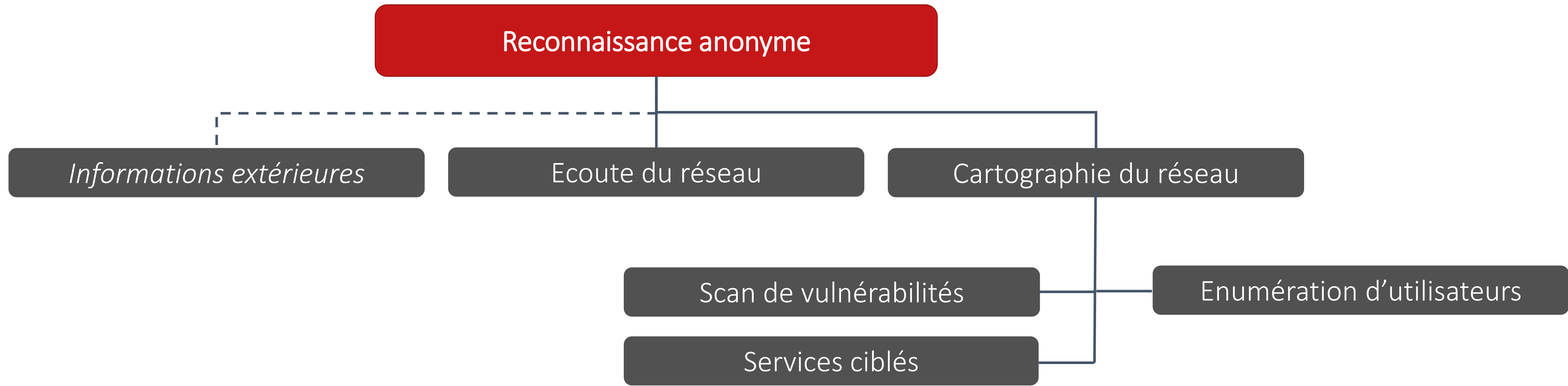
Reconnaissance Anonyme

Conclusion



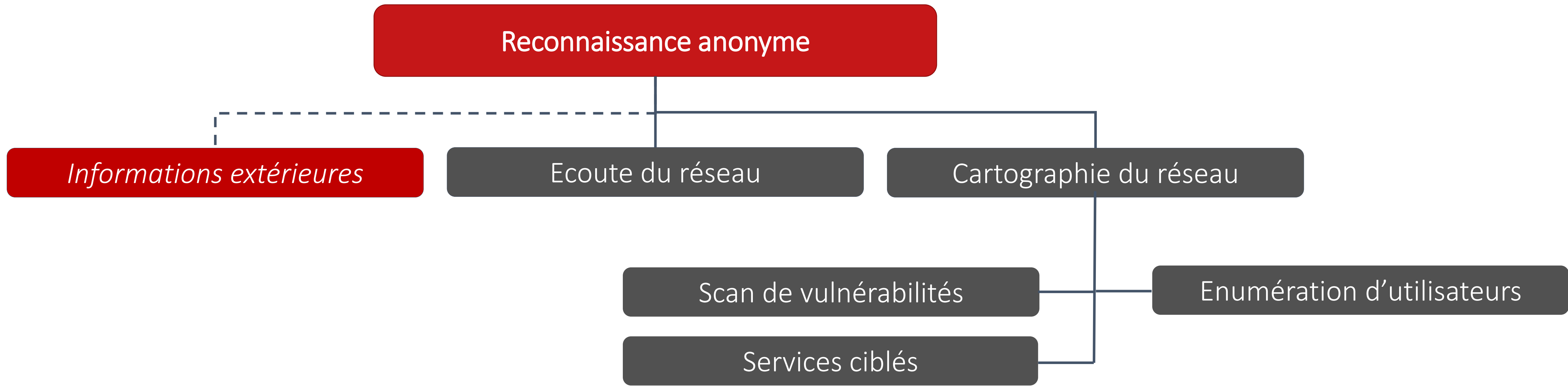
Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme



Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme



Reconnaissance dans un milieu Active Directory

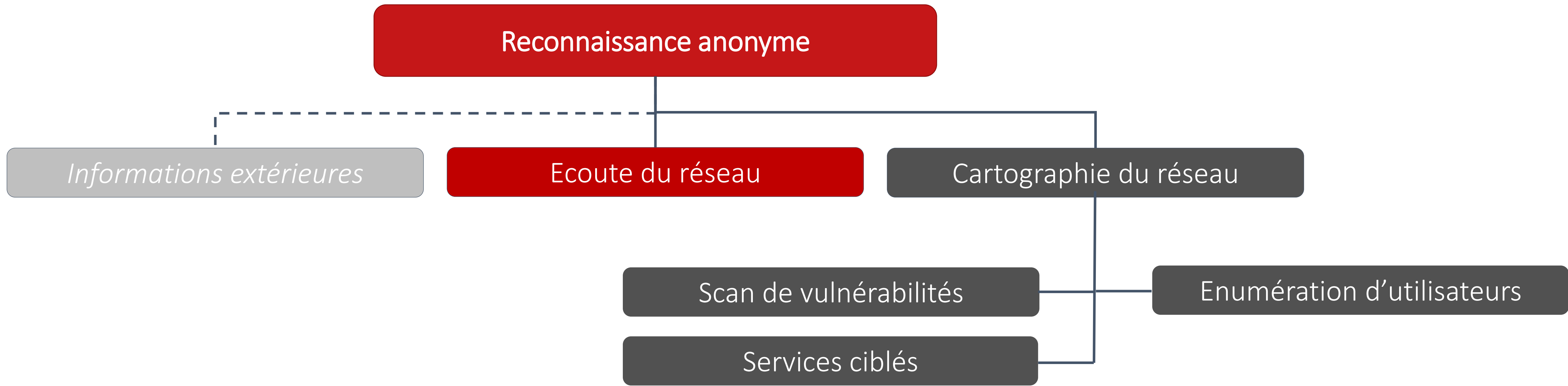
Reconnaissance anonyme – Informations extérieures

- Informations recherchées
 - Utilisateurs VIP
 - Données techniques / métiers

- Les recherches regroupent de multiples sources
 - Site vitrine
 - Réseaux professionnels
 - Fuites de données
 - Outils de collecte
 - ...

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme



Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme – Ecoute du réseau

- Ecoute passive
- Ecoute active (man-in-the-middle)
 - ✓ Mode silencieux
 - ✓ Redirection des flux
- Outils : Wireshark, Responder, Mitm6, ...

```
Sélection Windows PowerShell
PS C:\Users\isec-mdt> ipconfig /all

Carte inconnue OpenVPN TAP-Windows6 :

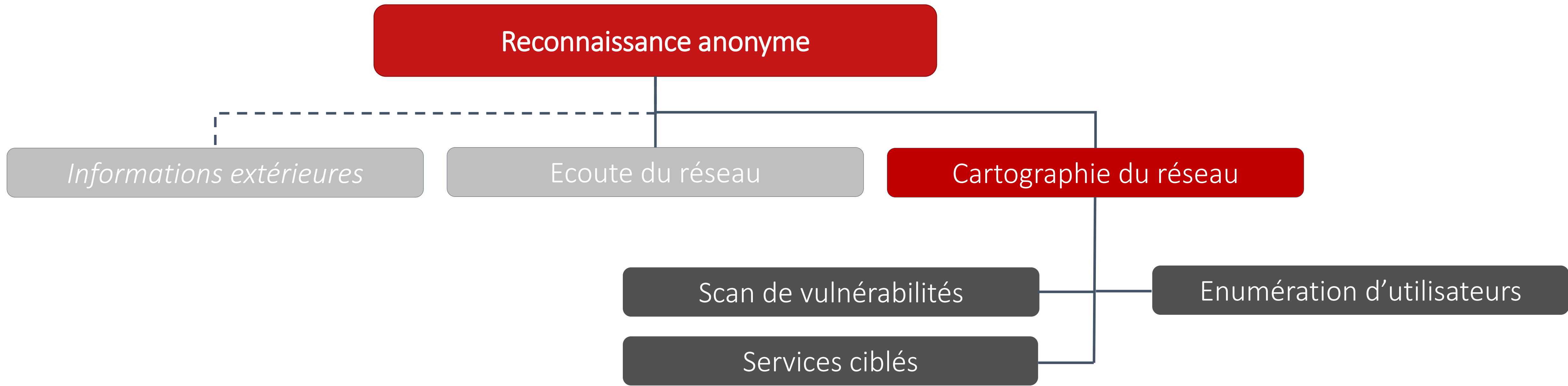
   Suffixe DNS propre à la connexion. . . : galaxy.lan
   Description. . . . . : TAP-Windows Adapter V9
   Adresse physique . . . . . : 00-FF-FB-EA-1A-95
   DHCP activé. . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . : fe80::1ca5:3338:2890:d0ce%17(préfééré)
   Adresse IPv4. . . . . : 10.26.10.4(préfééré)
   Masque de sous-réseau. . . . . : 255.255.255.0
   Bail obtenu. . . . . : mercredi 5 avril 2023 15:06:55
   Bail expirant. . . . . : jeudi 4 avril 2024 16:37:10
   Passerelle par défaut. . . . . :
   Serveur DHCP . . . . . : 10.26.10.0
   IAID DHCPv6 . . . . . : 184614907
   DUID de client DHCPv6. . . . . : 00-01-00-01-29-B3-A0-56-00-0C-29-B2-95-2A
   Serveurs DNS. . . . . : 10.26.1.201
   NetBIOS sur Tcpiip. . . . . : Activé
```

The image shows a Wireshark capture of a DHCP Offer packet. The packet list pane shows four packets: a DHCP Discover (No. 6), a DHCP Offer (No. 7), a DHCP Request (No. 8), and a DHCP ACK (No. 9). The packet details pane for the selected DHCP Offer (No. 7) shows the following information:

- Message type: Boot Reply (2)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0xd39a4af6
- Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 10.26.10.4
- Next server IP address: 10.26.10.0
- Relay agent IP address: 0.0.0.0
- Client MAC address: 00:ff:fb:ea:1a:95 (00:ff:fb:ea:1a:95)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Offer)
- Option: (54) DHCP Server Identifier (10.26.10.0)
- Option: (51) IP Address Lease Time
- Option: (1) Subnet Mask (255.255.255.0)
- Option: (15) Domain Name
 - Length: 10
 - Domain Name: galaxy.lan
- Option: (6) Domain Name Server
 - Length: 4
 - Domain Name Server: 10.26.1.201
- Option: (255) End
 - Option End: 255

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme



Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme – Cartographie du réseau

➤ Scan du réseau

- ✓ Découvertes des plages réseaux
- ✓ Découvertes des machines
 - Système d'exploitation
 - Services et versions

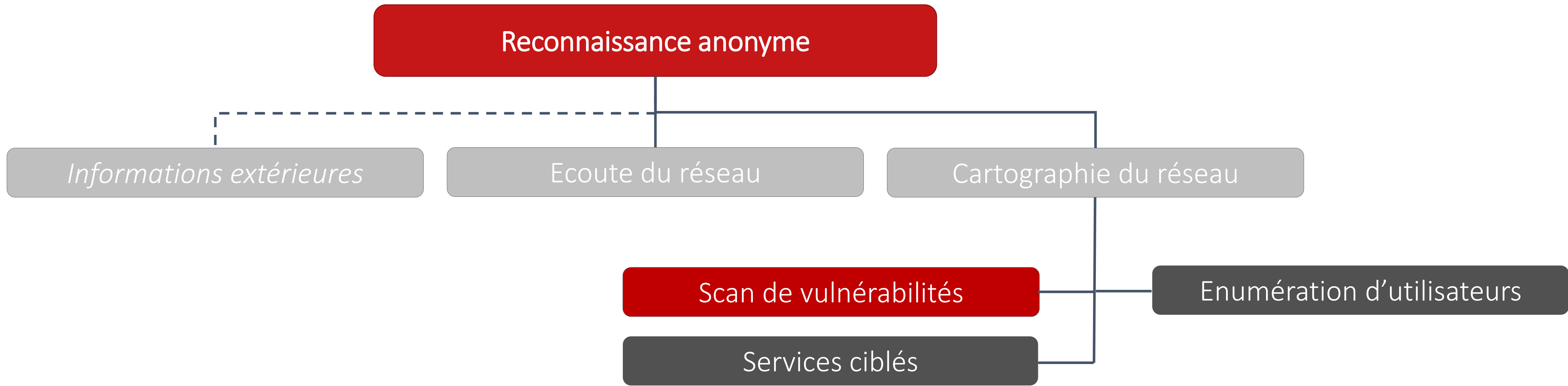
➤ Outils : Arpscan, Nmap, ...

```
└─$ nmap -T 5 -sV -A -oA ./tcp-output -p - 10.26.1.0/24
Nmap scan report for 10.26.1.212
Host is up (0.024s latency).
Scanned at 2023-04-15 18:56:57 CEST for 505s
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_ http-cookie-flags:
|   /:
|     PHPSESSID:
|_   httponly flag not set
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
135/tcp   open  msrpc          Microsoft Windows RPC
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ ssl-date: 2023-04-15T17:01:13+00:00; -4m06s from scanner time.
|_ ssl-cert: Subject: commonName=Gal-Kessel.galaxy.lan
| Issuer: commonName=Gal-Kessel.galaxy.lan
| Public Key type: rsa
| Public Key bits: 2048
|_ -----BEGIN CERTIFICATE-----
|_   MIIDBTCCAAGAMIBAgIqE92N74X1941AVD82QVSK2ANBgnKqk189A0BAQSPADAB
|_   VmXP3HNXOFT/GaYIM+dSk/UFHvz6wCa0pvdEWLxVuJiWgClB0Ds6svSyaKa3iaLU
|_   gg=
|_ -----END CERTIFICATE-----
5985/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
5986/tcp  open  ssl/http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ tls-alpn:
|   http/1.1
|_   MIIDBTCCAAGAMIBAgIqE92N74X1941AVD82QVSK2ANBgnKqk189A0BAQSPADAB
|_   VmXP3HNXOFT/GaYIM+dSk/UFHvz6wCa0pvdEWLxVuJiWgClB0Ds6svSyaKa3iaLU
|_   gg=
|_ -----END CERTIFICATE-----
8080/tcp  open  http           Apache Tomcat 9.0.70
|_ http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
|_ http-favicon: Apache Tomcat
|_ http-title: Apache Tomcat/9.0.70
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-time:
|   date: 2023-04-15T16:57:50
```

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme



Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme – Scan de vulnérabilités

➤ Scan de vulnérabilités

- En fonction des versions
- Basé sur des vulnérabilités connues
- Non intrusif

➤ Outils : Nmap, Metasploit, Nessus, Nuclei, ...

The screenshot shows the Nessus interface for a scan titled 'Scan nessus Lab'. It displays a summary of 17 hosts and 45 vulnerabilities. A table lists the top vulnerabilities, and a donut chart shows the distribution of severity levels.

Sev	Score	Name	Family	Count
MIXED	...	PHP (Multiple Issues)	CGI abuses	9
MIXED	...	Microsoft SQL Server (M...)	Databases	2
MIXED	...	Apache Tomcat (Multiple...)	Web Servers	4
MEDIUM	5.0	Network Time Protocol (NTP) ...	Misc.	1
MEDIUM	4.3	Terminal Services Doesn't Use...	Misc.	13
MIXED	...	Microsoft Windows (Mult...)	Windows	29
MIXED	...	SMB (Multiple Issues)	Misc.	11
INFO	...	SMB (Multiple Issues)	Windows	73

Scan Details

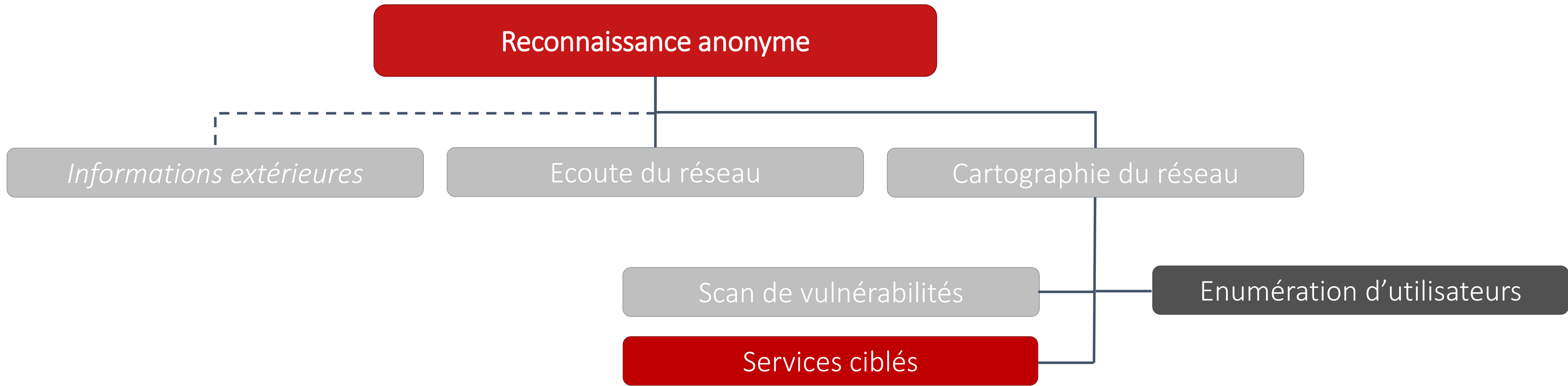
- Policy: Intrinsec-Default
- Status: Running
- Severity Base: CVSS v2.0
- Scanner: Local Scanner
- Start: Today at 11:38 AM

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme



Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme – Services ciblés

➤ Services / Protocoles

- FTP
- SSH
- Telnet
- HTTP(S)
- SMB
- SQL
- ...

➤ Outils : Nmap, Impacket, Burp, CrackMapExec, netscan, aquatone, ssh-audit, ...

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme – Services ciblés

➤ Services / Protocoles

- FTP
- SSH
- Telnet
- HTTP(S)
- SMB
- SQL
- ...

➤ Outils : Nmap, Impacket, Burp, CrackMapExec, netscan, aquatone, ssh-audit, ...

```
└─$ ftp 10.26.10.2
Connected to 10.26.10.2.
220 (vsFTPd 3.0.3)
Name (10.26.10.2:isec-mdt): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||53857|)
150 Here comes the directory listing.
```

```
└─$ nmap -p22 10.26.1.254 --script ssh-auth-methods --script-args="ssh.user=root"
Nmap scan report for 10.26.1.254
Host is up (0.025s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|   publickey
|   password
|_  keyboard-interactive

Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds
```

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme – Services ciblés

➤ Services / Protocoles

- FTP
- SSH
- Telnet
- HTTP(S)
- SMB
- SQL
- ...

➤ Outils : Nmap, Impacket, Burp, CrackMapExec, netscan, aquatone, ssh-audit, ...

```
└─$ cat ../../tcp-output.xml | ./aquatone -nmap

Targets      : 20
Threads     : 8
Ports       : 80, 443, 8000, 8080, 8443
Output dir  : .

http://GAL-KEPLER452B.GALAXY.LAN:5985/: 404 Not Found
http://10.26.1.1/: 200 OK
http://10.26.1.212:5985/: 404 Not Found
https://10.26.1.214:5986/: 404 Not Found
https://GAL-KEPLER452B.GALAXY.LAN:5986/: 404 Not Found
https://10.26.1.232/: 401 Unauthorized
http://10.26.1.232/: 200 OK
https://10.26.1.212:5986/: 404 Not Found
https://10.26.1.232:9200/: 401 Unauthorized
http://10.26.1.254/: 200 OK
https://10.26.1.214:8172/: 404 Not Found
http://10.26.1.214:5985/: 404 Not Found
http://10.26.1.212:8080/: 200 OK

https://10.26.1.214:5986/: screenshot successful
https://GAL-KEPLER452B.GALAXY.LAN:5986/: screenshot successful
https://10.26.1.232/: screenshot successful
http://10.26.1.232/: screenshot successful
https://10.26.1.212:5986/: screenshot successful
https://10.26.1.232:9200/: screenshot successful
https://10.26.1.214:8172/: screenshot successful
http://10.26.1.254/: screenshot successful
http://10.26.1.214/: screenshot successful
http://10.26.1.214:5985/: screenshot successful
http://10.26.1.212:8080/: screenshot successful
http://10.26.1.214:81/: screenshot successful
https://10.26.1.214:444/: screenshot successful
Calculating page structures ... done
Clustering similar pages ... done
Generating HTML report ... done
```

The screenshot shows the AQUATONE web interface with the title 'Pages by Similarity'. It displays a list of discovered pages with their URLs and status. The top entry is 'http://10.26.1.212:8080/' with a status of '200 OK' and a thumbnail of an Apache Tomcat/9.0.70 page. Below it are two entries for 'pfSense - LoginpfSense Logo' at 'http://10.26.1.1/' and 'http://10.26.1.254/', both with '200 OK' status and thumbnails showing the pfSense login page. The interface includes navigation arrows and buttons for 'View Details' and 'Visit Page' for each entry.



Reconnaissance dans un milieu Active Directory

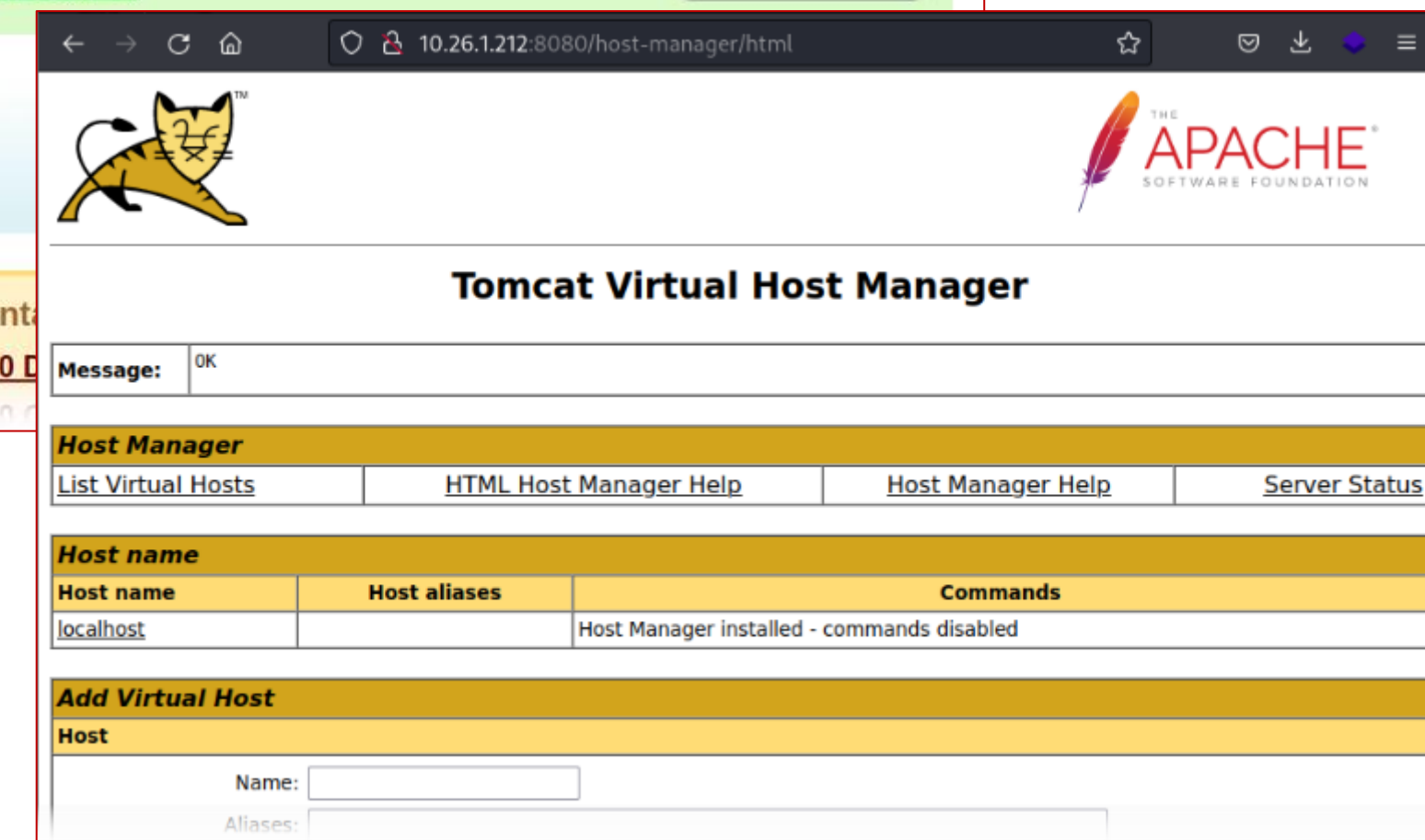
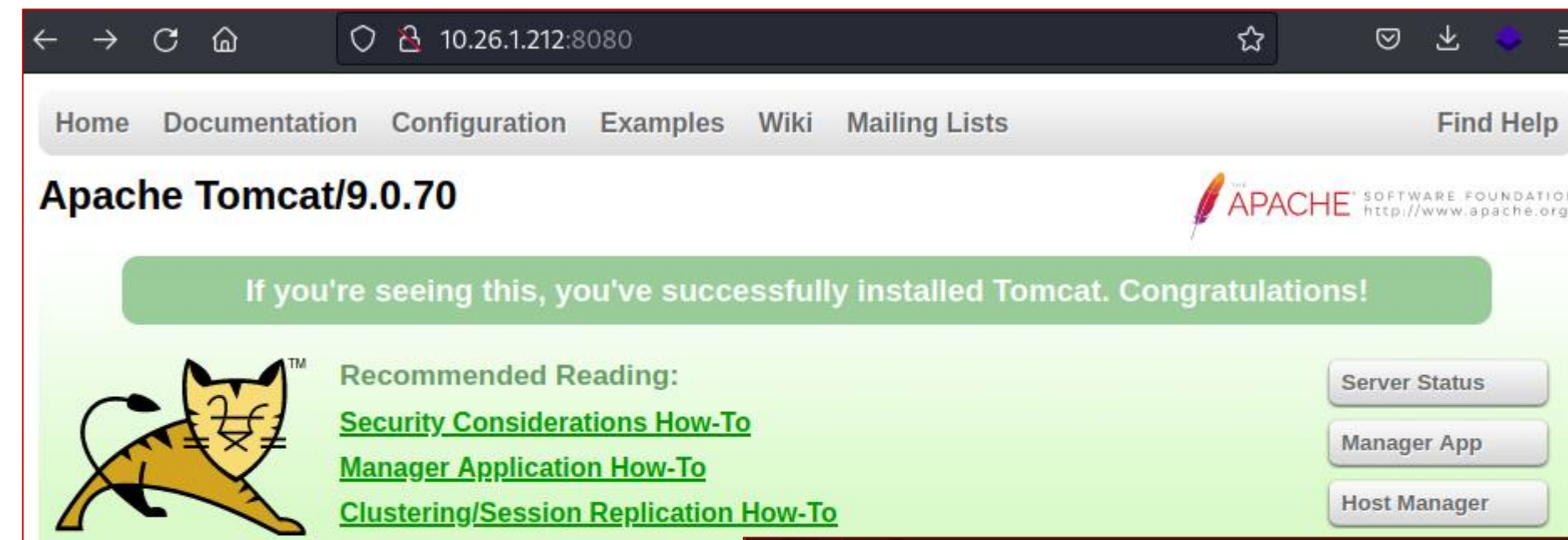
Reconnaissance anonyme – Services ciblés

➤ Services / Protocoles

- FTP
- SSH
- Telnet
- HTTP(S)
- SMB
- SQL
- ...

➤ Outils : Nmap, Impacket, Burp, CrackMapExec, netscan, aquatone, ssh-audit, ...

```
Nmap scan report for 10.26.1.212
Host is up (0.024s latency).
Scanned at 2023-04-15 18:56:57 CEST for 505s
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_ http-cookie-flags:
|   /:
|   PHPSESSID:
|   httponly_flag: not set
|_ gg==
|_ -----END CERTIFICATE-----
8080/tcp   open  http           Apache Tomcat 9.0.70
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-favicon: Apache Tomcat
```



Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme – Services ciblés

➤ Services / Protocoles

- FTP
- SSH
- Telnet
- HTTP(S)
- SMB
- SQL
- ...

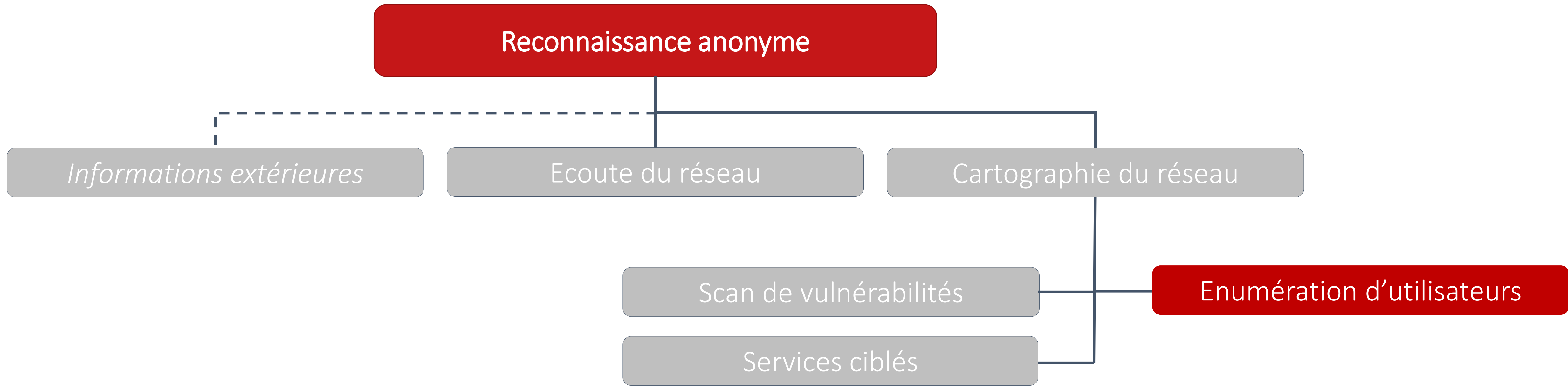
```
└─$ crackmapexec smb 10.26.1.0/24 --shares
SMB 10.26.1.53 445 GAL-KAMINO [*] Windows 10.0 Build 19041 x64 (name:GAL-KAMINO) (domain:galaxy.lan) (signing:False) (SMBv1:False)
SMB 10.26.1.52 445 GAL-CORELLIA [*] Windows 10.0 Build 19041 x64 (name:GAL-CORELLIA) (domain:galaxy.lan) (signing:False) (SMBv1:False)
SMB 10.26.1.53 445 GAL-KAMINO [-] Error enumerating shares: [Errno 32] Broken pipe
SMB 10.26.1.52 445 GAL-CORELLIA [-] Error enumerating shares: [Errno 32] Broken pipe
SMB 10.26.1.201 445 GAL-KORRIBAN [*] Windows 10.0 Build 17763 x64 (name:GAL-KORRIBAN) (domain:galaxy.lan) (signing:True) (SMBv1:False)
SMB 10.26.1.202 445 REBELS-GAL-YAVI [*] Windows 10.0 Build 17763 x64 (name:REBELS-GAL-YAVI) (domain:rebels4.galaxy.lan) (signing:True) (SMBv1:False)
SMB 10.26.1.201 445 GAL-KORRIBAN [-] Error enumerating shares: STATUS_USER_SESSION_DELETED
SMB 10.26.1.202 445 REBELS-GAL-YAVI [-] Error enumerating shares: STATUS_USER_SESSION_DELETED
SMB 10.26.1.205 445 KAAMELOTT [*] Windows 10.0 Build 17763 x64 (name:KAAMELOTT) (domain:logres.lan) (signing:True) (SMBv1:False)
SMB 10.26.1.205 445 KAAMELOTT [-] Error enumerating shares: STATUS_USER_SESSION_DELETED
SMB 10.26.1.214 445 GAL-MARIDUN [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:GAL-MARIDUN) (domain:galaxy.lan) (signing:False) (SMBv1:True)
SMB 10.26.1.214 445 GAL-MARIDUN [-] Error enumerating shares: [Errno 32] Broken pipe
SMB 10.26.1.213 445 GAL-KEPLER452B [*] Windows 10.0 Build 17763 x64 (name:GAL-KEPLER452B) (domain:galaxy.lan) (signing:False) (SMBv1:False)
SMB 10.26.1.213 445 GAL-KEPLER452B [-] Error enumerating shares: [Errno 32] Broken pipe
SMB 10.26.1.212 445 GAL-KESSEL [*] Windows 10.0 Build 17763 x64 (name:GAL-KESSEL) (domain:galaxy.lan) (signing:False) (SMBv1:False)
```

- Outils : Nmap, Impacket, Burp, CrackMapExec, netscan, aquatone, ssh-audit, ...



Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme

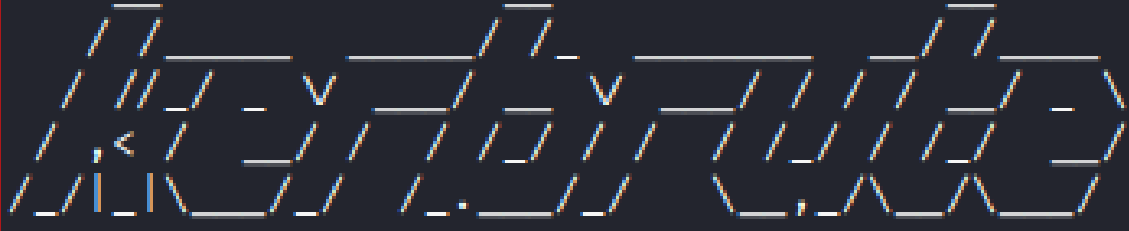


Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme – Enumération d'utilisateurs

- Recherche basée sur une *wordlist*
 - Liste générique
 - Liste personnalisée
- ⚠ *Politique de mot de passe encore inconnue à ce stade*

```
└─$ ./kerbrute_linux_amd64 userenum -d galaxy.lan --dc 10.26.1.201 usernames starwars.txt
```



```
Version: v1.0.3 (9dad6e1) - 04/15/23 - Ronnie Flathers @ropnop
```

```
2023/04/15 16:51:42 > Using KDC(s):
2023/04/15 16:51:42 > 10.26.1.201:88
```

```
2023/04/15 16:51:42 > [+] VALID USERNAME: anakin-skywalker@galaxy.lan
2023/04/15 16:51:42 > [+] VALID USERNAME: r2-d2@galaxy.lan
2023/04/15 16:51:42 > [+] VALID USERNAME: c3-po@galaxy.lan
2023/04/15 16:51:42 > [+] VALID USERNAME: jar-jar-binks@galaxy.lan
2023/04/15 16:51:42 > [+] VALID USERNAME: han-solo@galaxy.lan
2023/04/15 16:51:42 > [+] VALID USERNAME: leia-organa@galaxy.lan
2023/04/15 16:51:42 > [+] VALID USERNAME: comte-dooku@galaxy.lan
2023/04/15 16:51:42 > [+] VALID USERNAME: sheev-palpatine@galaxy.lan
2023/04/15 16:51:42 > Done! Tested 30 usernames (8 valid) in 0.194 seconds
```

- Outils : CrackMapExec, Enum4linux, Kerbrute

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme

Exploitation

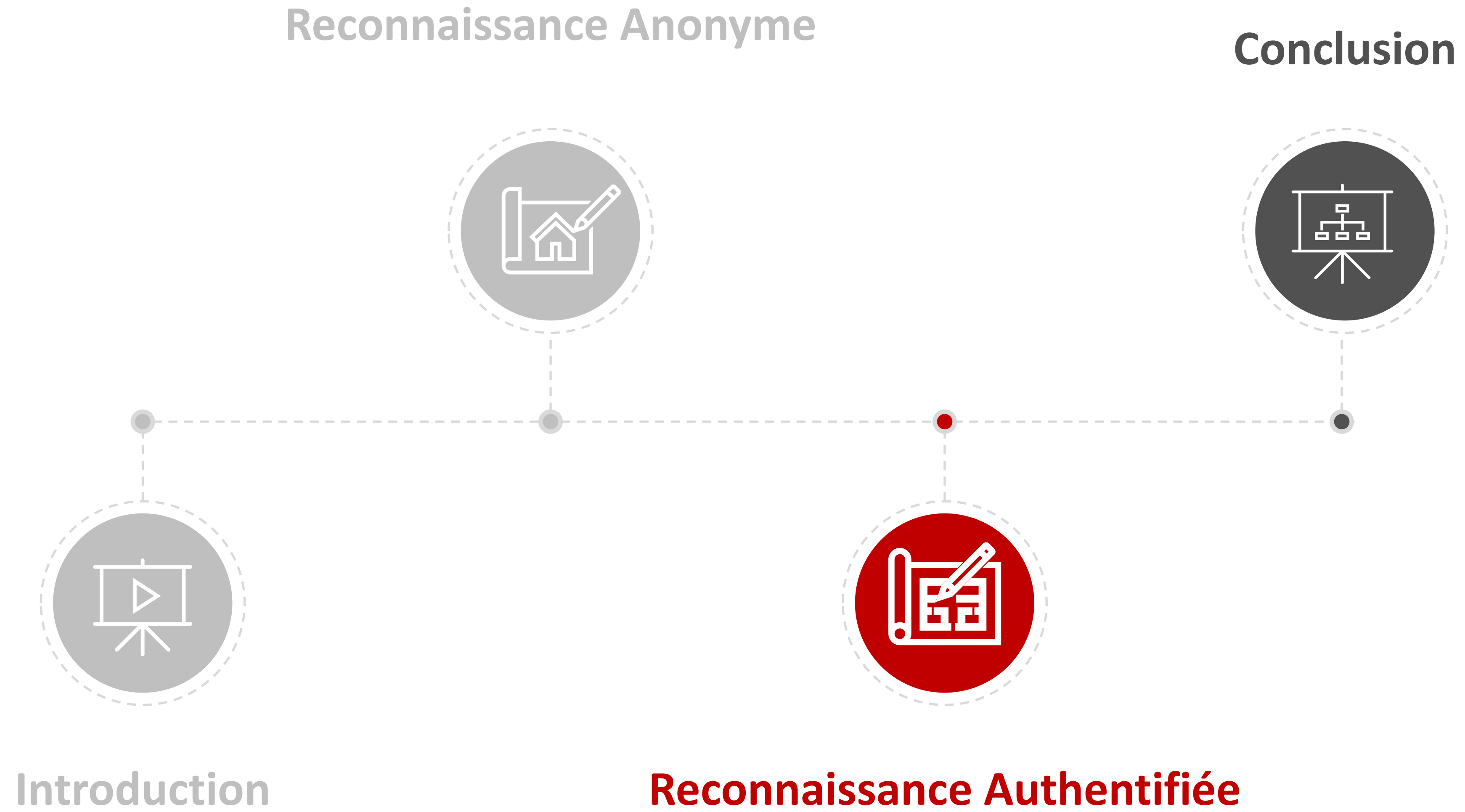


Anonyme

- Cassage d'un challenge obtenu lors de l'écoute active
- Relai d'une authentification reçue lors de l'écoute active
- Compromission d'une machine via un service vulnérable
- Récupération d'identifiants dans un partage
- Attaque par force brute sur les comptes identifiés

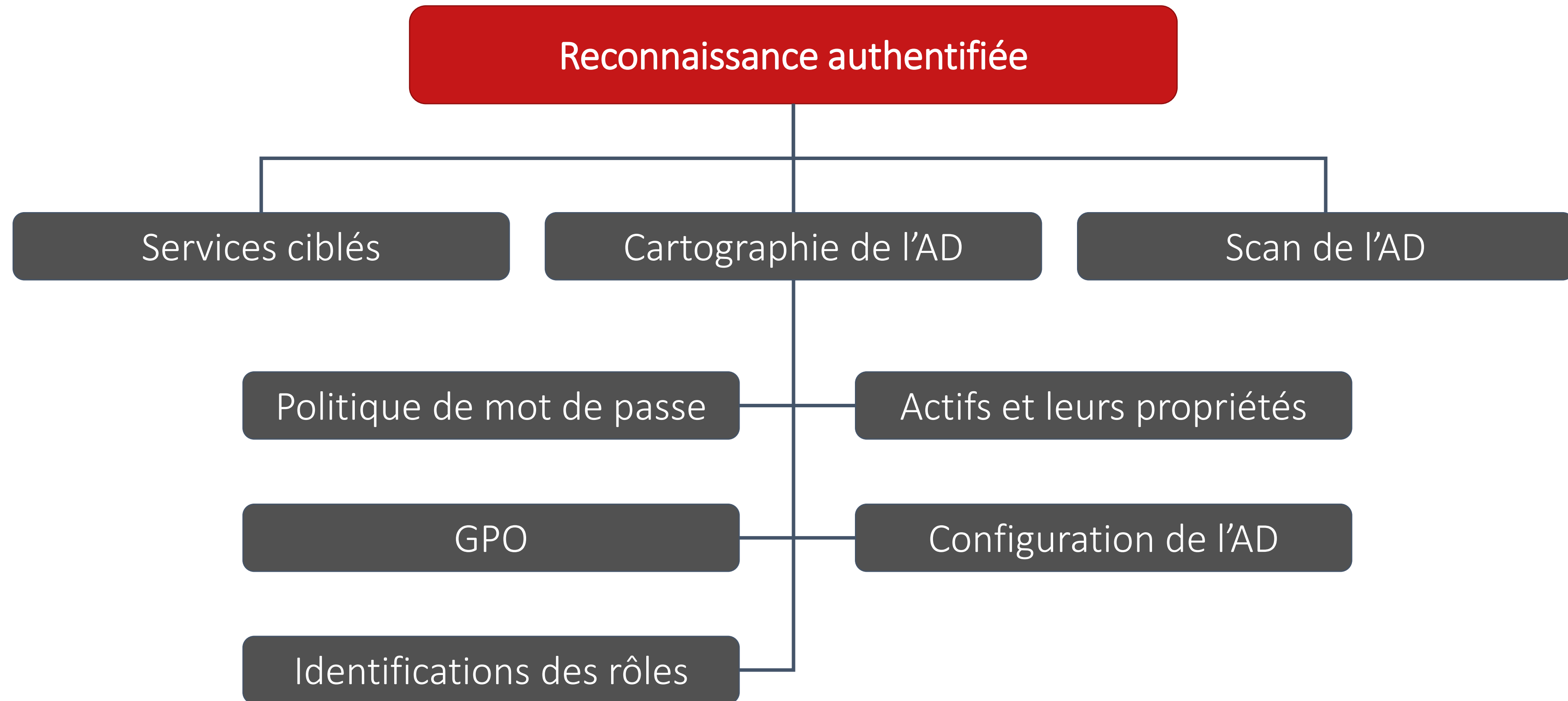
Accès initial
authentifié

Plan



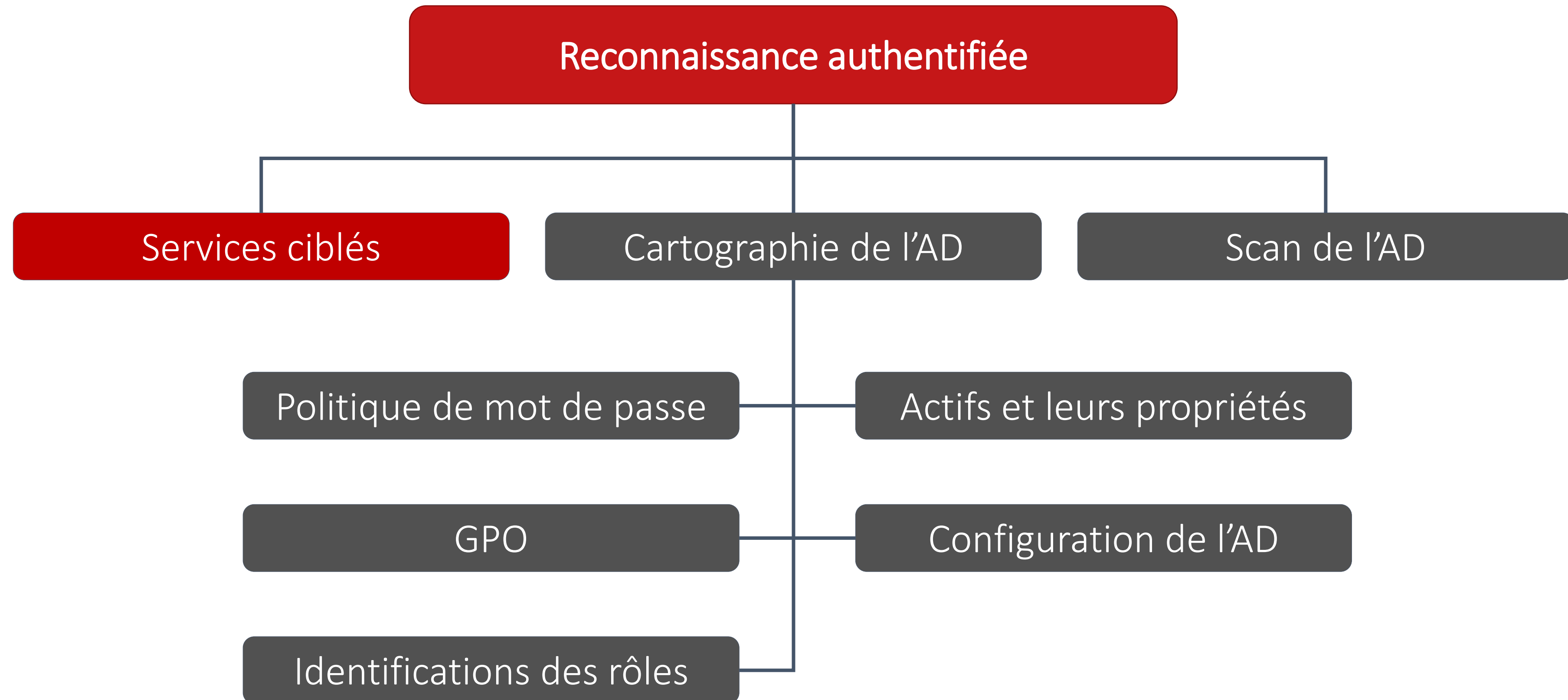
Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



Reconnaissance dans un milieu Active Directory

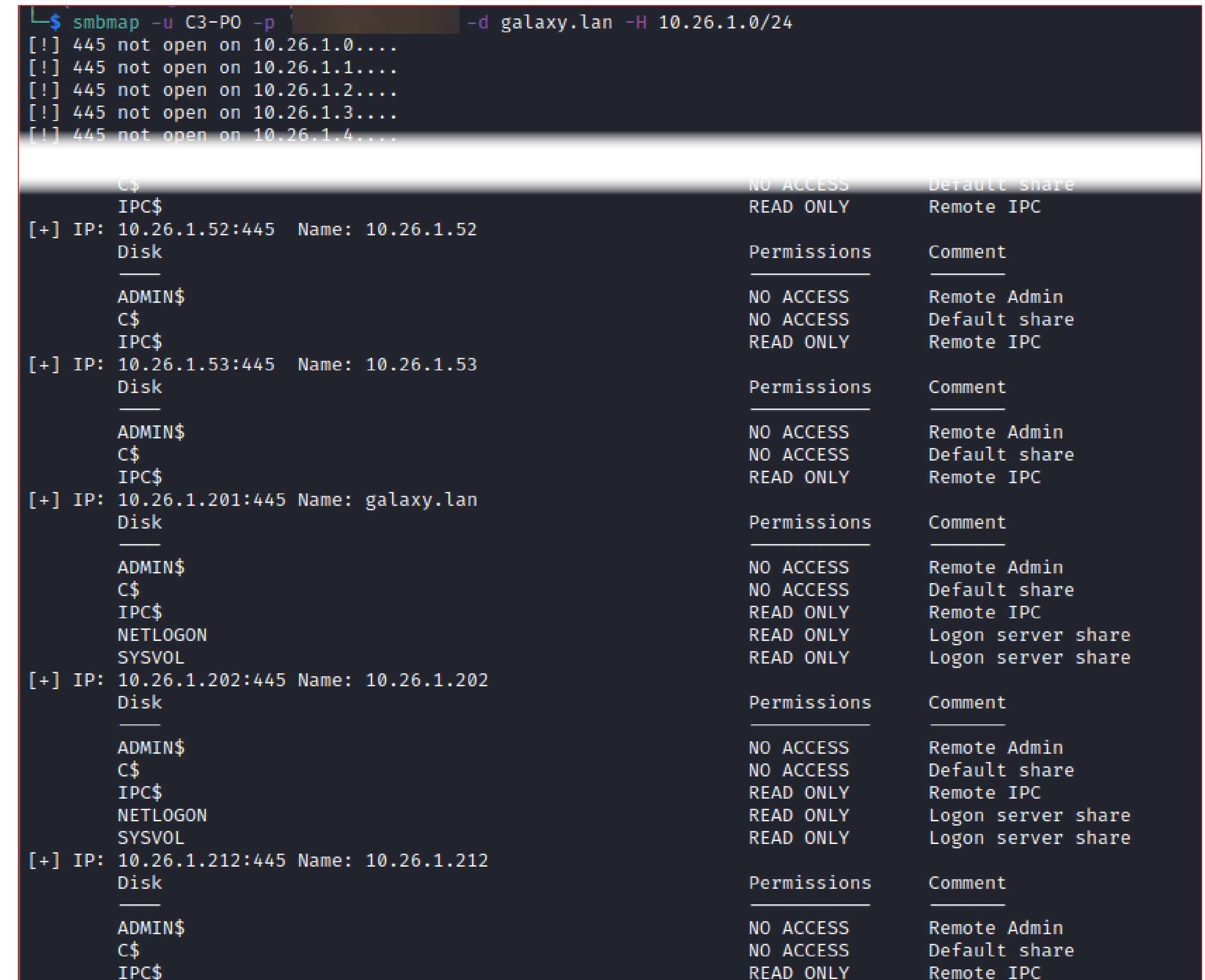
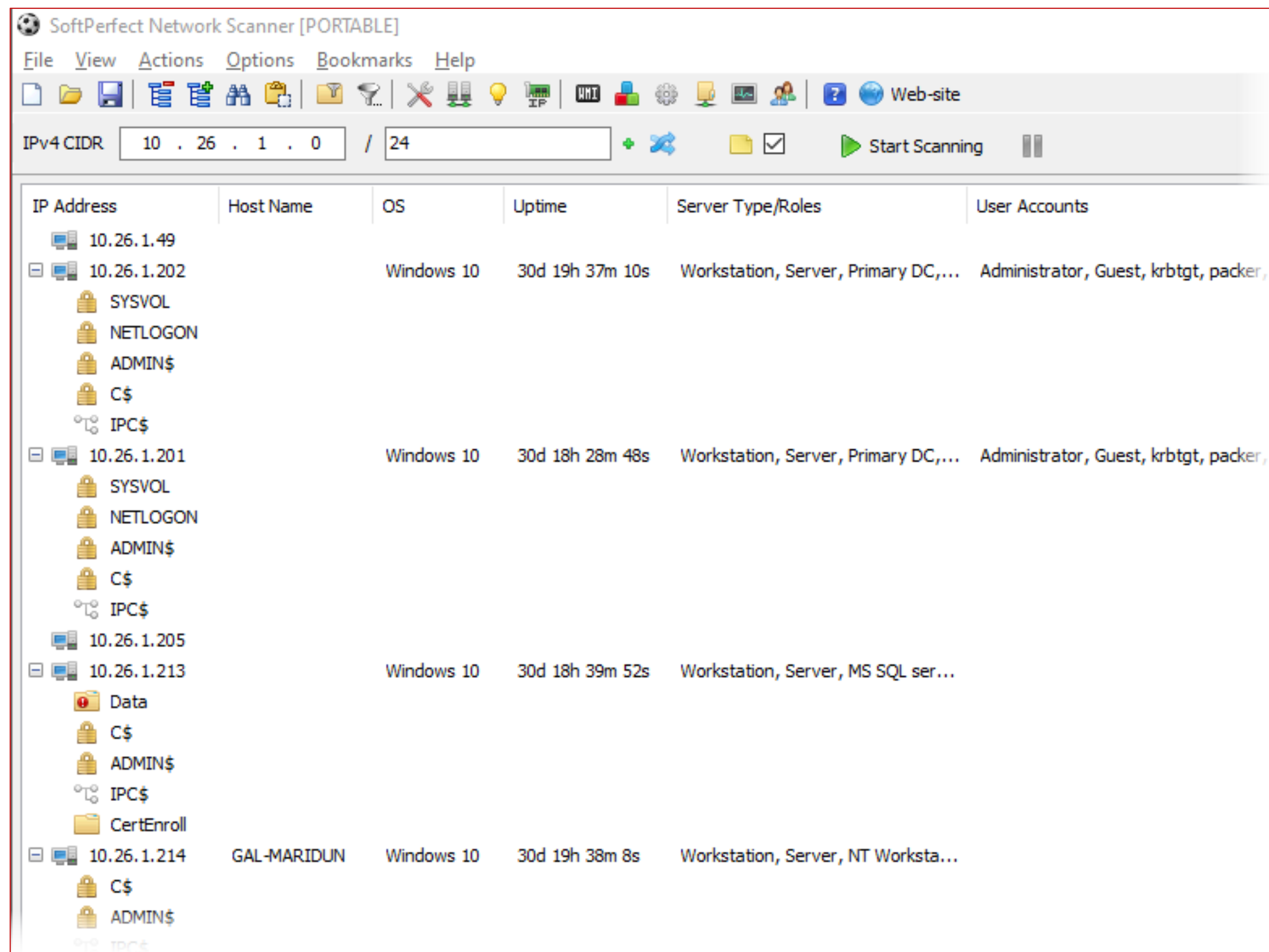
Reconnaissance authentifiée



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Services ciblés / Partages accessibles

- Réitération de l'étape anonyme
- Accès supplémentaires à l'aide des identifiants



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Services ciblés

- Réitération de l'étape anonyme
- Accès supplémentaires à l'aide des identifiants

```
PS C:\Users\isec-mdt\Documents> Get-SQLInstanceDomain

ComputerName      : Gal-Kepler452b.galaxy.lan
Instance          : Gal-Kepler452b.galaxy.lan,1433
DomainAccountSid  : 150000052100033252122582212232323623519020624488400
DomainAccount     : r5-d4
DomainAccountCn   : R5-D4
Service           : MSSQLSvc
Spn               : MSSQLSvc/Gal-Kepler452b.galaxy.lan:1433
LastLogon        : 16/04/2023 15:13
Description       : R5-D4 était un droïde astromécano de série R5 fabriqué par Industrial Auto
```

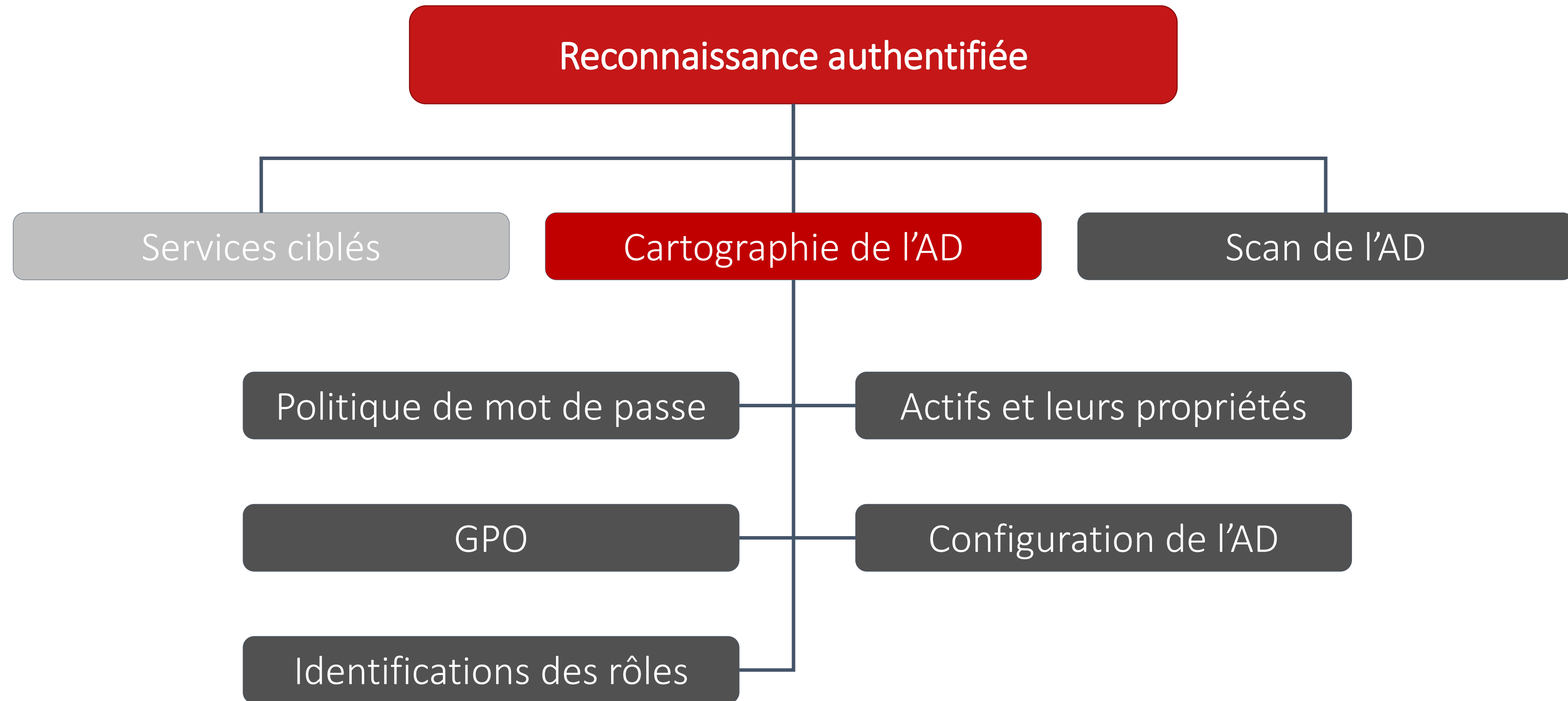
- Outils : Nmap, Impacket, CrackMapExec, PowerUPSQL, SMBMap, Netscan Portable, ...

```
PS C:\Users\isec-mdt\Documents> Get-SQLInstanceDomain | Get-SQLConnectionTest

ComputerName      Instance                                     Status
-----
Gal-Kepler452b.galaxy.lan Gal-Kepler452b.galaxy.lan,1433           Accessible
Gal-Kepler452b.galaxy.lan Gal-Kepler452b.galaxy.lan\SQLEXPRESS     Accessible
```

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Cartographie de l'AD

- Collecte d'informations globale de l'AD
- Représentations des données

- Outils : BloodHound, ADRecon, PowerView ...

Table of Contents
User Stats
Computer Stats
Privileged Group Stats
Operating System Stats
Computer Role Stats
Users
Group Members
Groups
User SPNs
OUs
Computers
Computer SPNs
LAPS
DNS Zones
DNS Records
gPLinks
GPOs
DAACLs
Domain Controllers
Default Password Policy
Sites
Trusts
Domain
Forest
About ADRecon

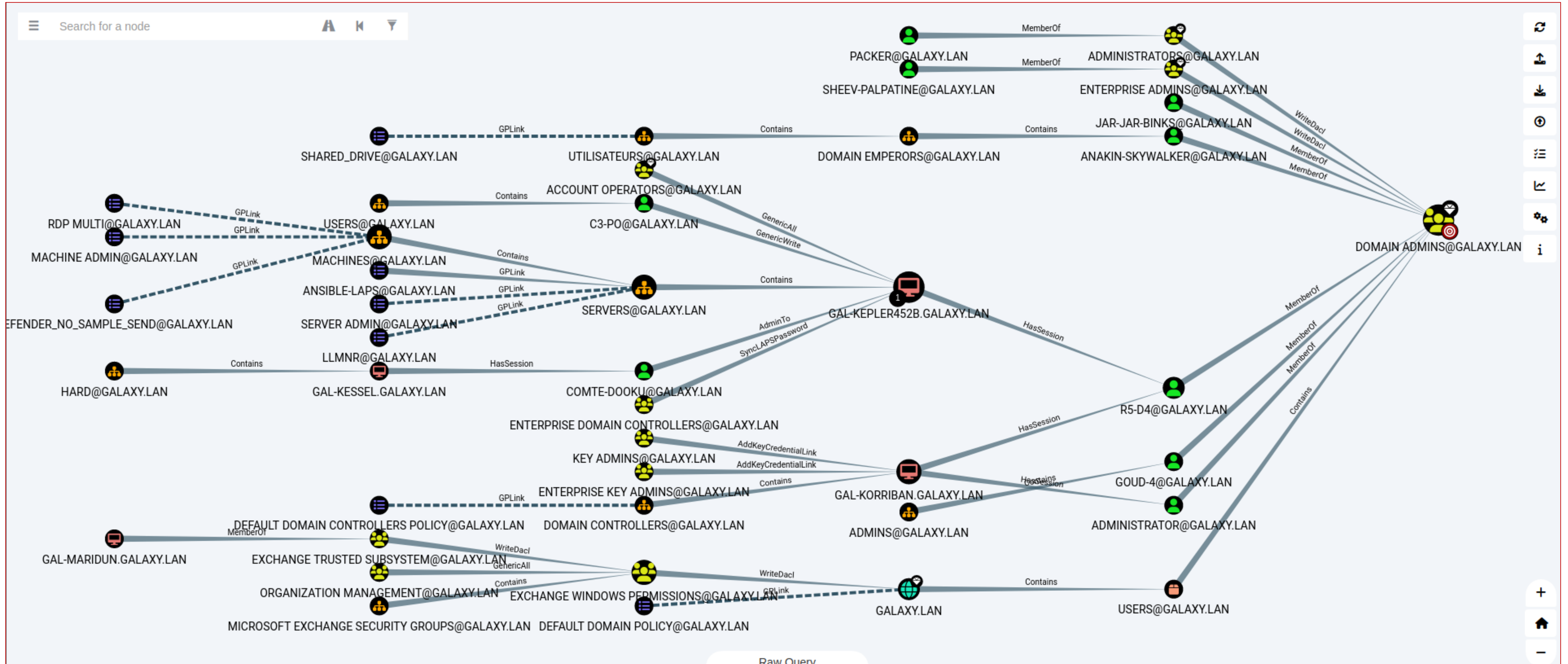
Classement des informations retrouvées à
grâce à ADRecon

Pre-Built Analytics Queries
Domain Information
Find all Domain Admins
Map Domain Trusts
Find Computers with Unsupported Operating Systems
Dangerous Privileges
Find Principals with DCSync Rights
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
Find Computers where Domain Users are Local Admin
Find Computers where Domain Users can read LAPS passwords
Find All Paths from Domain Users to High Value Targets
Find Workstations where Domain Users can RDP
Find Servers where Domain Users can RDP
Find Dangerous Privileges for Domain Users Groups
Find Domain Admin Logons to non-Domain Controllers
Kerberos Interaction
Find Kerberoastable Members of High Value Groups
List all Kerberoastable Accounts
Find Kerberoastable Users with most privileges
Find AS-REP Roastable Users (DontReqPreAuth)
Shortest Paths
Shortest Paths to Unconstrained Delegation Systems
Shortest Paths from Kerberoastable Users
Shortest Paths to Domain Admins from Kerberoastable Users
Shortest Path from Owned Principals
Shortest Paths to Domain Admins from Owned Principals
Shortest Paths to High Value Targets
Shortest Paths from Domain Users to High Value Targets
Find Shortest Paths to Domain Admins

Traitements des données avec Bloodhound
(pre-built queries)

Reconnaissance dans un milieu Active Directory

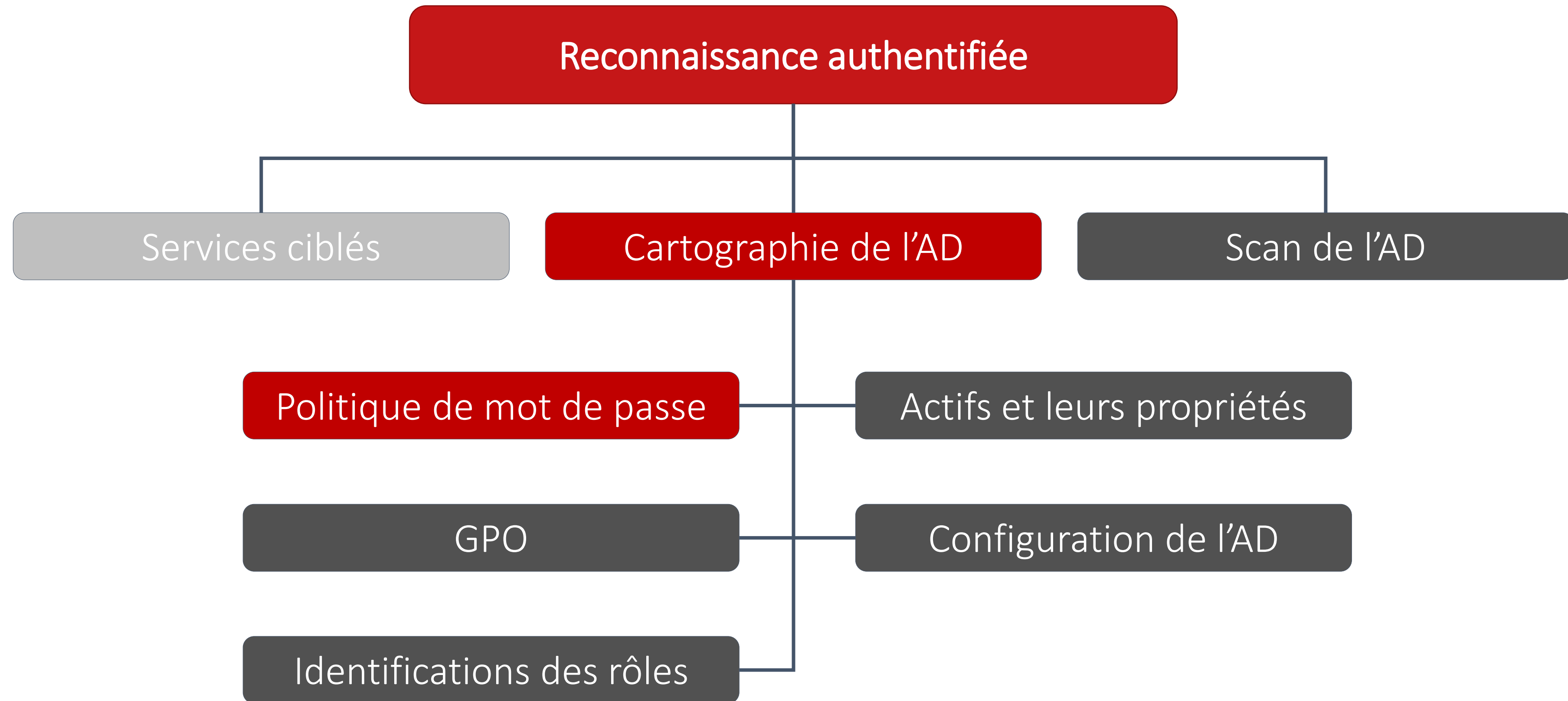
Reconnaissance authentifiée – Cartographie de l'AD



« Find shortest paths to domain admin »

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Politique de mot de passe

- Politique par défaut de l'Active Directory
 - Get-ADDefaultDomainPasswordPolicy
- ⚠ Politique de mot de passe affinée
 - Get-ADFineGrainedPasswordPolicy

- Outils : BloodHound, ADRecon, ...

	A	B
1	Policy	Current Value
2	Enforce password history (passwords)	24
3	Maximum password age (days)	42
4	Minimum password age (days)	1
5	Minimum password length (characters)	7
6	Password must meet complexity requirements	VRAI
7	Store password using reversible encryption for all users in the domain	FAUX
8	Account lockout duration (mins)	30
9	Account lockout threshold (attempts)	0
10	Reset account lockout counter after (mins)	30

```
PS C:\Windows\system32> Get-ADDefaultDomainPasswordPolicy
```

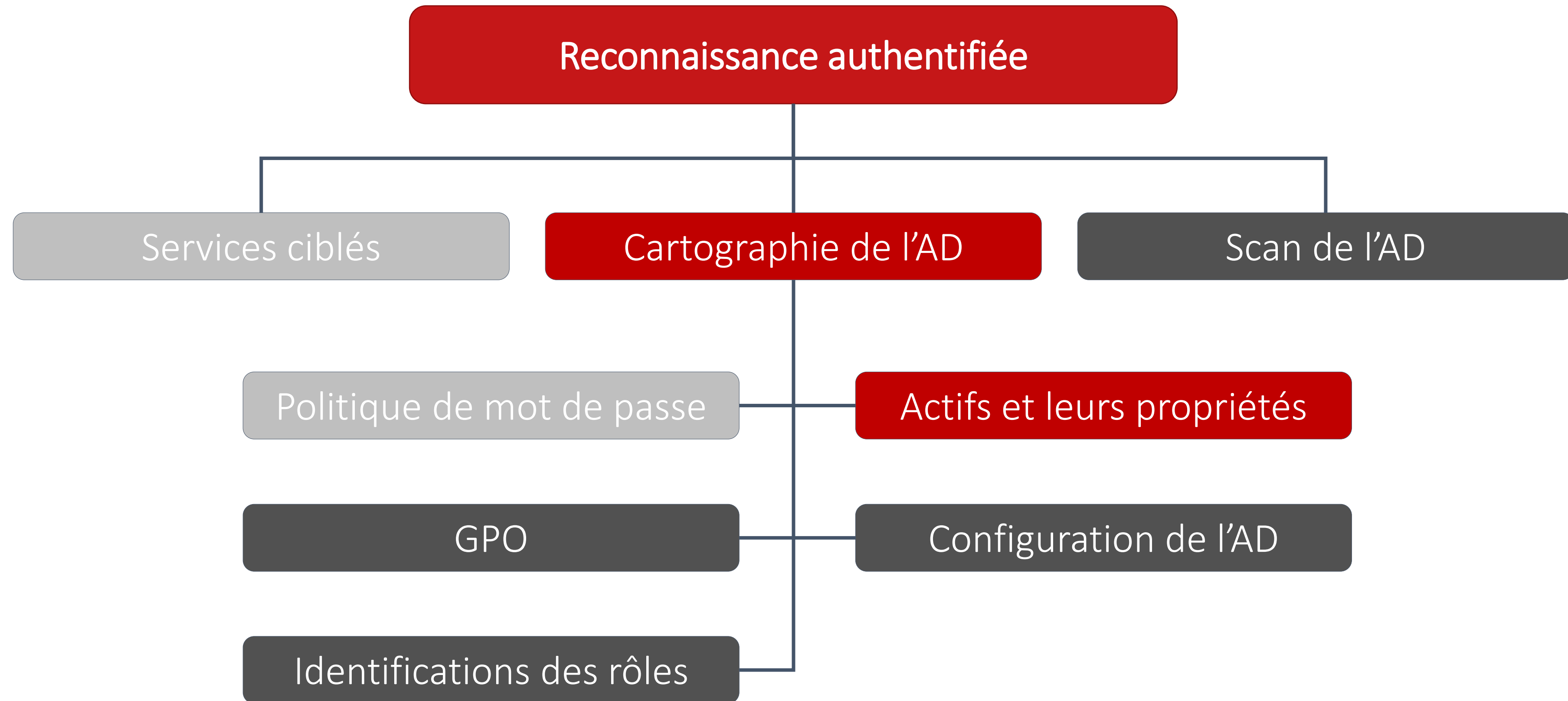
```
ComplexityEnabled           : True
DistinguishedName          : DC=galaxy,DC=lan
LockoutDuration             : 00:30:00
LockoutObservationWindow   : 00:30:00
LockoutThreshold            : 0
MaxPasswordAge              : 42.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 7
objectClass                  : {domainDNS}
objectGuid                   : 4b30365a-46f6-4f87-9238-9d14da7e560c
PasswordHistoryCount        : 24
ReversibleEncryptionEnabled : False
```

```
PS C:\Windows\system32> Get-ADFineGrainedPasswordPolicy -filter *
```

```
AppliesTo                   : {CN=Domain Users,CN=Users,DC=galaxy,DC=lan}
ComplexityEnabled           : True
DistinguishedName           : CN=Test Fine Grained Password Policy,CN=Password Settings
                             Container,CN=System,DC=galaxy,DC=lan
LockoutDuration              : 00:00:00
LockoutObservationWindow    : 01:00:00
LockoutThreshold             : 3
MaxPasswordAge               : 42.00:00:00
MinPasswordAge               : 1.00:00:00
MinPasswordLength            : 8
Name                         : Test Fine Grained Password Policy
ObjectClass                  : msDS-PasswordSettings
ObjectGUID                   : e345717a-c183-46b2-9396-00e91529f4f2
PasswordHistoryCount         : 24
Precedence                   : 1
ReversibleEncryptionEnabled  : False
```

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Actifs de l'AD et leurs propriétés

➤ Objets de l'Active Directory

- Utilisateurs
- Groupes
- Machines
- DACL
- GPO
- ...

➤ Propriétés

- Descriptions
- DistinguishedName
- ...

➤ Outils : BloodHound, ADRecon, ...

Status of User Accounts						
Category	Enabled Count	Enabled Percentage	Disabled Count	Disabled Percentage	Total Count	Total Percentage
Must Change Password at Logon	0	0.00%	10	0.83%	10	0.23%
Cannot Change Password	0	0.00%	0	0.00%	0	0.00%
Password Never Expires	29	0.91%	1	0.08%	30	0.68%
Reversible Password Encryption	0	0.00%	0	0.00%	0	0.00%
Smartcard Logon Required	0	0.00%	0	0.00%	0	0.00%
Delegation Permitted	32	1.00%	12	1.00%	44	1.00%
Kerberos DES Only	0	0.00%	0	0.00%	0	0.00%
Kerberos RC4	0	0.00%	0	0.00%	0	0.00%
Does Not Require Pre Auth	1	0.03%	0	0.00%	1	0.02%
Password Age (> 42 days)	1	0.03%	0	0.00%	1	0.02%
Account Locked Out	0	0.00%	0	0.00%	0	0.00%
Never Logged in	21	0.66%	12	1.00%	33	0.75%
Dormant (> 90 days)	0	0.00%	0	0.00%	0	0.00%
Password Not Required	1	0.03%	2	0.17%	3	0.07%
Unconstrained Delegation	0	0.00%	0	0.00%	0	0.00%
SIDHistory	0	0.00%	0	0.00%	0	0.00%

	A	B	C	D	E	F	G
1	UserName	Name	Enabled	GroupID	SID	Description	DistinguishedName
3	Administrator	Administrator	VRAI	513	S-1-5-21-4243601597-32924416	Built-in account for administering the computer	CN=Administrator,CN=Users,DC
4	anakin-skywalker	Anakin-Skywalker	VRAI	513	S-1-5-21-4243601597-32924416	Anakin-Skywalker ?tait un Chevalier Jedi qui	CN=Anakin-Skywalker,OU=Dom
5	bobba-fett	Bobba-Fett	VRAI	513	S-1-5-21-4243601597-32924416	Boba Fett ?tait un clone non alt?r? du chasse	CN=Bobba-Fett,OU=Admins,OU
6	C1-10P	C1-10P	VRAI	513	S-1-5-21-4243601597-32924416	C1-10P, plus connu sous le nom de Chopper,	CN=C1-10P,OU=Users,OU=Utili
7	C3-PO	C3-PO	VRAI	513	S-1-5-21-4243601597-32924416	C3-PO est un ? dro?de de protocole ? de la s	CN=C3-PO,OU=Users,OU=Utilis
8	comte-dooku	Comte-Dooku	VRAI	513	S-1-5-21-4243601597-32924416	Le Comte-Dooku ?tait un Jedi corrompu par	CN=Comte-Dooku,OU=Admins,
9	gial-ackbar	Gial-Ackbar	VRAI	513	S-1-5-21-4243601597-32924416	Gial-Ackbar ?tait un v?t?ran Mon Calamari e	CN=Gial-Ackbar,OU=Admins,OU
10	GOUD-4	GOUD-4	VRAI	513	S-1-5-21-4243601597-32924416	Exchange - GOUD-4 ?tait un dro?de travail	CN=GOUD-4,OU=Admins,OU=U
12	han-solo	Han-Solo	VRAI	513	S-1-5-21-4243601597-32924416	Han-Solo, se faisant appeler Han pendant sa	CN=Han-Solo,OU=Devs,OU=Uti

	A	B	C	D	E	F	G
1	Name	Username	Enabled	Service	Host	Password Last Set	Description
2	krbtgt	krbtgt	FAUX	kadmin	changepw	20/12/2022 14:57	Key Distribution Center Service Account
3	R5-D4	r5-d4	VRAI	MSSQLSvc	Gal-Kepler452b.	20/12/2022 15:18	R5-D4 ?tait un dro?de astrom?cano de s?rie R5 fabriqu?
4	R5-D4	r5-d4	VRAI	MSSQLSvc	Gal-Kepler452b.	20/12/2022 15:18	R5-D4 ?tait un dro?de astrom?cano de s?rie R5 fabriqu?
5	R5-D4	r5-d4	VRAI	SQL	run	20/12/2022 15:18	R5-D4 ?tait un dro?de astrom?cano de s?rie R5 fabriqu?



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Actifs de l'AD et leurs propriétés

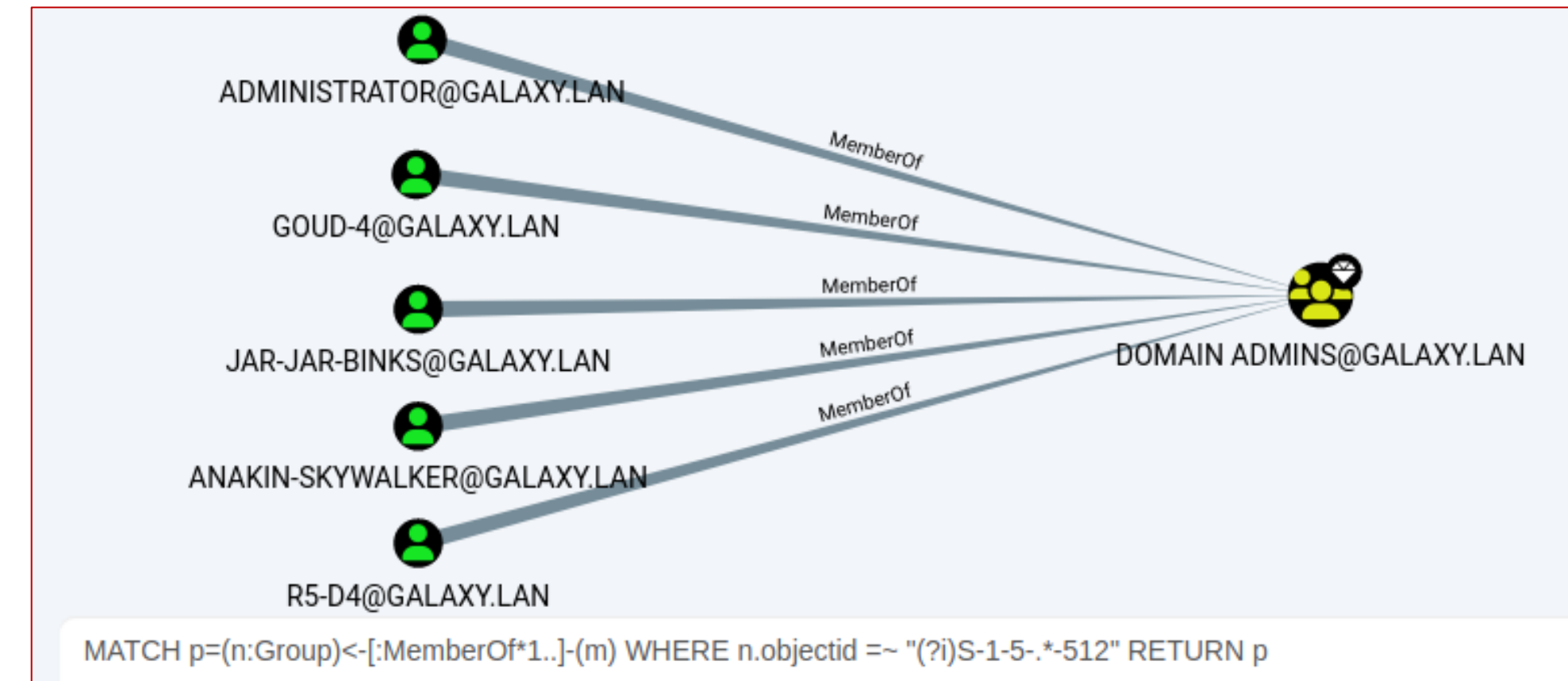
➤ Objets de l'Active Directory

- Utilisateurs
- **Groupes**
- Machines
- DACL
- GPO
- ...

➤ Propriétés

- Descriptions
- DistinguishedName
- ...

➤ Outils : BloodHound, ADRecon, ...



1	Name	AdminCount	GroupCategory	GroupScope	ManagedBy	SID
2	Access Control Assistance Operators		Security	DomainLocal		S-1-5-32-579
3	Account Operators	1	Security	DomainLocal		S-1-5-32-548
4	Administrators	1	Security	DomainLocal		S-1-5-32-544
5	Allowed RODC Password Replication Group		Security	DomainLocal		S-1-5-21-424360
6	Backup Operators	1	Security	DomainLocal		S-1-5-32-551
7	Cert Publishers		Security	DomainLocal		S-1-5-21-424360
8	Certificate Service DCOM Access		Security	DomainLocal		S-1-5-32-574

Group Members | **Groups** | User SPNs | OUs | Computers | Computer SPNs | LAPS | DNS Zones | DNS Records | ...



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Actifs de l'AD et leurs propriétés

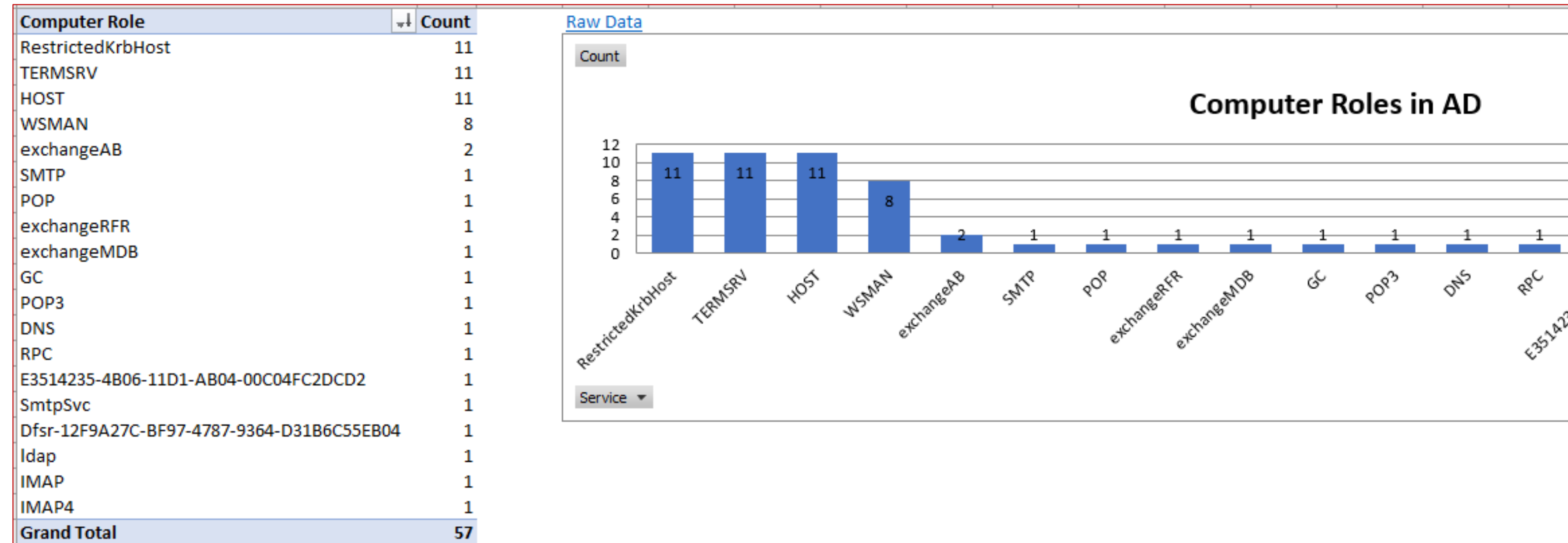
➤ Objets de l'Active Directory

- Utilisateurs
- Groupes
- **Machines**
- DACL
- GPO
- ...

➤ Propriétés

- Descriptions
- DistinguishedName
- ...

➤ Outils : BloodHound, ADRecon, ...



Hostname	Stored	Readable	Password	Expiration
Gal-Korriban.galaxy.lan	FAUX	FAUX		
Gal-Kepler452b.galaxy.lan	VRAI	FAUX		15/12/2023 17:51
Gal-Maridun.galaxy.lan	VRAI	FAUX		15/12/2023 17:20
Gal-Coruscant.galaxy.lan	VRAI	FAUX		15/12/2023 17:53
Gal-Kessel.galaxy.lan	VRAI	FAUX		15/12/2023 17:16
Gal-Kamino.galaxy.lan	FAUX	FAUX		
Gal-Tatooine.galaxy.lan	FAUX	FAUX		
Gal-Naboo.galaxy.lan	FAUX	FAUX		
Gal-Iokath.galaxy.lan	FAUX	FAUX		
Gal-Corellia.galaxy.lan	FAUX	FAUX		
Gal-Mustafar.galaxy.lan	FAUX	FAUX		

... | Users | Group Members | Groups | User SPNs | OUs | Computers | Computer SPNs | LAPS

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Actifs de l'AD et leurs propriétés

➤ Objets de l'Active Directory

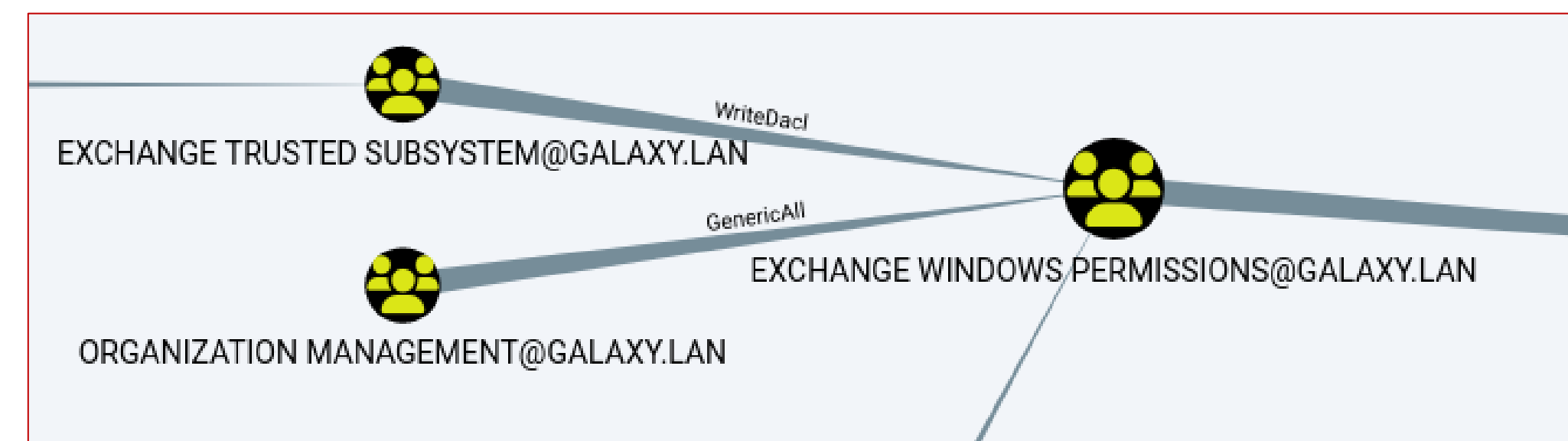
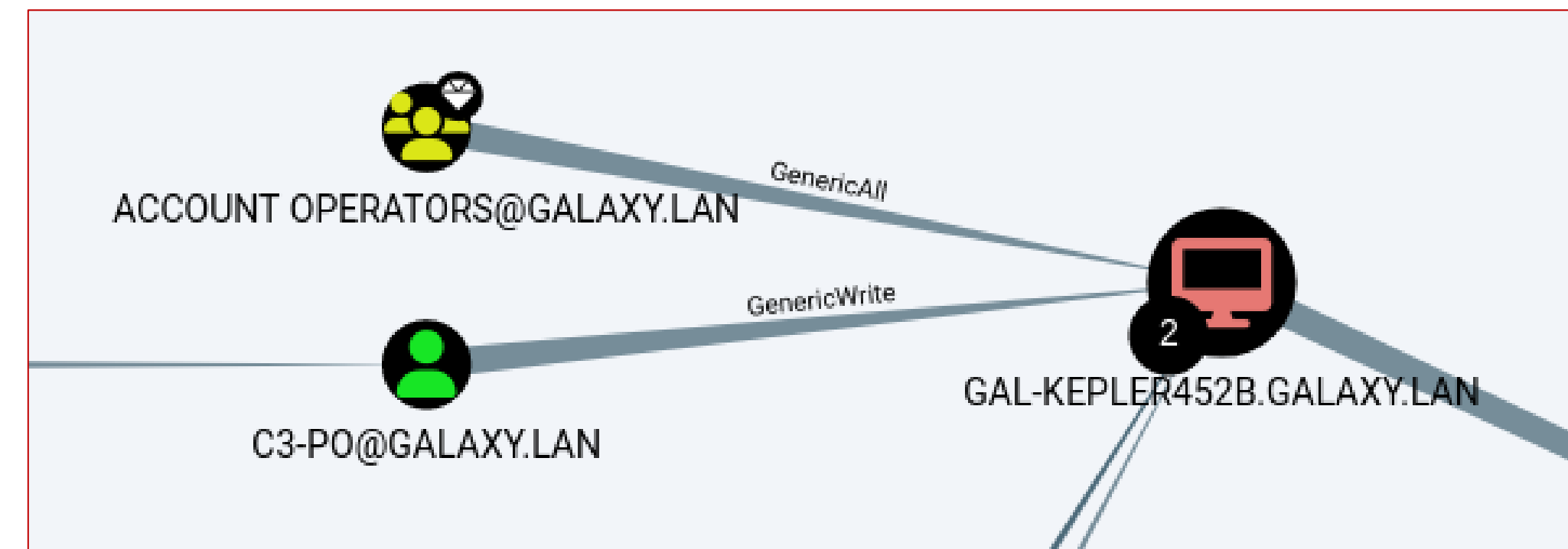
- Utilisateurs
- Groupes
- Machines
- **DAACL**
- GPO
- ...

➤ Propriétés

- Descriptions
- DistinguishedName
- ...

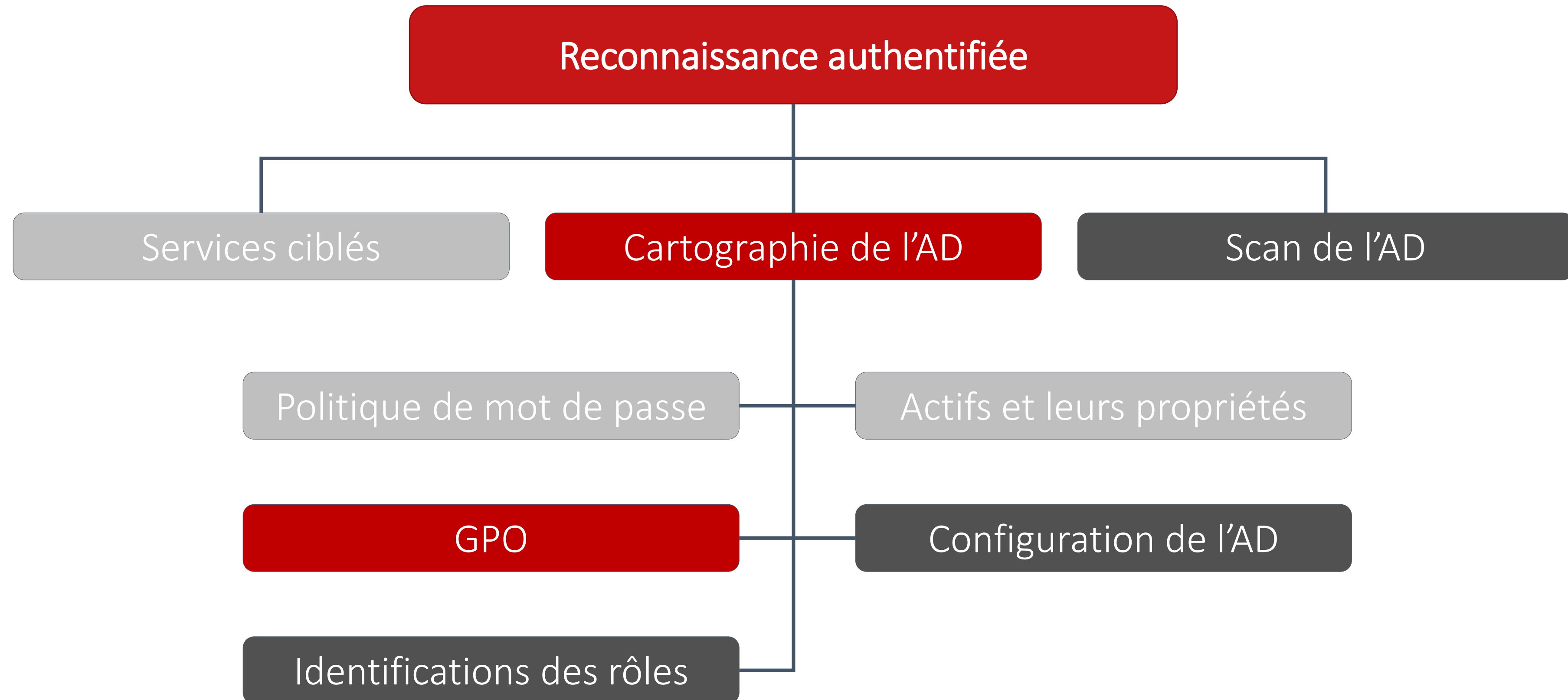
➤ Outils : BloodHound, ADRecon, ...

Discretionary Access Control List



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – GPO

- Group Policy Object
 - Mots de passe, cpassword
 - Privilèges trop permissifs
 - ...

Anomalies analysis

Anomalies : 92 / 100
It is about specific security control points

Anomalies rule details [16 rules matched on a total of 68]

Number of password(s) found in GPO: 1

Find Password GPO

Rule ID:
A-PwdGPO

Description:
The purpose is to alert when a password is present in a GPO. If a password is in a GPO, the password should be con

[\[MITRE\]T1552.006 Unsecured Credentials: Group Policy Preferences](#)

Details:
The detail can be found in the [Obfuscated Passwords](#)

GPO	login	password
Machine Admin	R2-D2	Q m

```
PS C:\Users\isec-mdt\Documents\Group3r-main\Group3r\bin\Debug> .\Group3r.exe -c 10.26.1.201 -d galaxy.lan -s -w
[...]
```

```
Gaze not into the abyss, lest you become recognized as an abyss domain expert,
and they expect you keep gazing into the damn thing... - @nickm_tor
```

```
Link | OU=LAPS,OU=Hard,OU=WorkStations,OU=Machines,DC=galaxy,DC=lan (Disabled, Enforced) |
```

```
2023-04-16 11:19:15 +02:00 [GPO]
GPO | Management Users {810C1139-6BF1-41A0-9815-20356A722282} Current
-----|-----
Date Created | 15/03/2023 14:04:05
Date Modified | 15/03/2023 14:04:05
Path in SYSVOL | \\galaxy.lan\sysvol\galaxy.lan\Policies\{810C1139-6BF1-41A0-9815-20356A722282}
Computer Policy | Enabled
User Policy | Enabled
Link | OU=WinRM,OU=WorkStations,OU=Machines,DC=galaxy,DC=lan (Enabled, Unenforced)
```

```
2023-04-16 11:19:15 +02:00 [GPO]
GPO | Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9} Current
-----|-----
Date Created | 15/03/2023 12:51:12
Date Modified | 15/03/2023 12:57:05
Path in SYSVOL | \\galaxy.lan\sysvol\galaxy.lan\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
Computer Policy | Enabled
User Policy | Enabled
Link | DC=galaxy,DC=lan (Enabled, Unenforced)
```

```
Setting - Computer Policy | Kerberos Policy |
-----|-----
MaxClockSkew | 5 |
```

```
Finding | Green
Reason | Non-default maximum Kerberos clock skew setting. 5
Detail | Dunno, bit interesting.
```

- Outils : Group3r, PingCastle, ADRecon, ...

Privileges

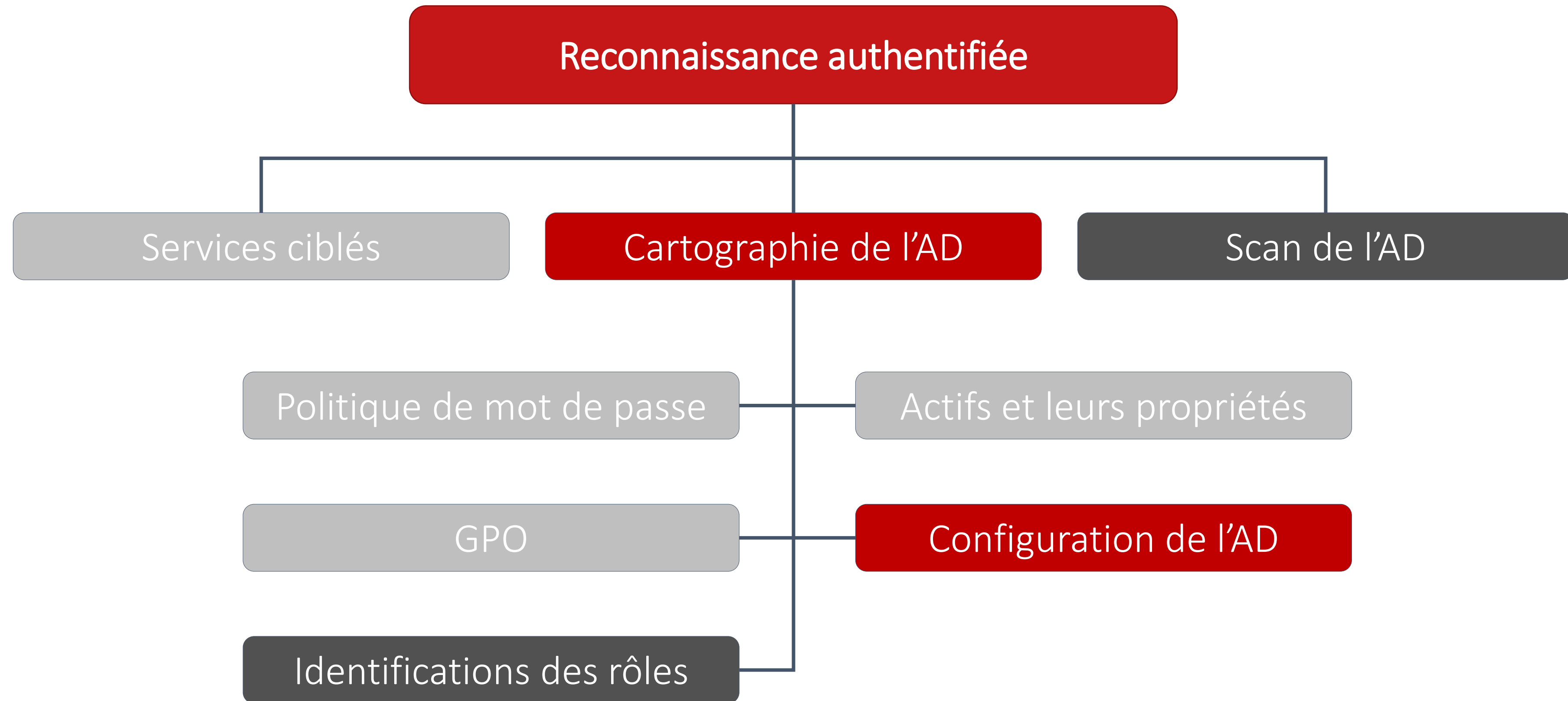
Giving privileges in a GPO is a way to become administrator without being part of a group.
For example, SeTcbPrivilege give the right to act as SYSTEM, which has more privileges than the administrator account.

GPO Name	Privilege	Members
Default Domain Controllers Policy	SeAssignPrimaryTokenPrivilege	NT AUTHORITY\LOCAL SERVIC
Default Domain Controllers Policy	SeAssignPrimaryTokenPrivilege	NT AUTHORITY\NETWORK SER
Default Domain Controllers Policy	SeLoadDriverPrivilege	BUILTIN\Print Operators
Default Domain Controllers Policy	SeMachineAccountPrivilege	Authenticated Users
Default Domain Controllers Policy	SeRestorePrivilege	Administrators

Showing 1 to 10 of 16 rows 10 rows per page

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Configuration de l'AD

- Méthodes d'administration
- Présence d'un AV / EDR
- ADIDNS
- Protocoles
- WSUS
- SCCM
- Nomenclature utilisée
- ...

Tier 0

Tier 1

Tier 2

- Outils : BloodHound, PingCastle, ADRecon, krbrelayx, LdapRelayScan, ...

```
└─$ crackmapexec smb 10.26.1.212 -u R5-D4 -p '...' --loggedon-users
SMB 10.26.1.212 445 GAL-KESSEL [*] Windows 10.0 Build 17763 x64 (name:GAL-KESSEL)
) (SMBv1:False)
SMB 10.26.1.212 445 GAL-KESSEL [+] galaxy.lan\R5-D4:P@ssw0rd (Pwn3d!)
SMB 10.26.1.212 445 GAL-KESSEL [+] Enumerated loggedon users
SMB 10.26.1.212 445 GAL-KESSEL galaxy\r5-d4 logon_server: GAL
SMB 10.26.1.212 445 GAL-KESSEL galaxy\r5-d4 logon_server: GAL
SMB 10.26.1.212 445 GAL-KESSEL galaxy\GAL-KESSEL$
SMB 10.26.1.212 445 GAL-KESSEL galaxy\GAL-KESSEL$
SMB 10.26.1.212 445 GAL-KESSEL galaxy\GAL-KESSEL$
```



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Configuration de l'AD

- Méthodes d'administration
 - Présence d'un AV / EDR
 - ADIDNS
 - Protocoles
 - WSUS
 - SCCM
 - Nomenclature utilisée
 - ...
-
- Outils : BloodHound, PingCastle, ADRecon, krbrelayx, LdapRelayScan, ...

```
└─$ impacket-smbclient Administrator@10.26.1.53 -hashes ""
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Type help for list of commands
# use C$
# cd Program Files
# ls
drw-rw-rw-    0 Sun Apr 23 14:21:02 2023 .
drw-rw-rw-    0 Sun Apr 23 14:21:02 2023 ..
drw-rw-rw-    0 Wed Mar 15 15:32:38 2023 Common Files
-rw-rw-rw-   174 Wed Mar 15 16:29:14 2023 desktop.ini
drw-rw-rw-    0 Wed Apr 12 02:40:37 2023 Elastic
drw-rw-rw-    0 Sun Apr  2 13:32:33 2023 Internet Explorer
drw-rw-rw-    0 Wed Mar 15 15:02:44 2023 LAPS
drw-rw-rw-    0 Thu Mar 30 13:34:53 2023 Microsoft
drw-rw-rw-    0 Wed Mar 15 13:33:51 2023 Microsoft Update Health Tools
drw-rw-rw-    0 Wed Mar 15 16:30:32 2023 ModifiableWindowsApps
drw-rw-rw-    0 Wed Mar 15 12:38:16 2023 MSBuild
drw-rw-rw-    0 Wed Mar 15 12:38:16 2023 Reference Assemblies
drw-rw-rw-    0 Wed Mar 15 16:16:36 2023 SentinelOne
drw-rw-rw-    0 Wed Mar 15 16:30:32 2023 Uninstall Information
drw-rw-rw-    0 Wed Mar 15 15:32:40 2023 VMware
```



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Configuration de l'AD

- Méthodes d'administration
- Présence d'un AV / EDR
- ADIDNS
- Protocoles
- WSUS
- SCCM
- Nomenclature utilisée
- ...

```
└─$ python3 dnstool.py -u 'galaxy.lan\C3-P0' -p '...' --record '*' --action 'query' 10.26.1.201
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[!] Target record not found!

(isec-mdt@isec-test)-[~/Tools/krbrelayx]
└─$ python3 dnstool.py -u 'galaxy.lan\C3-P0' -p '...' --record 'wpad' --action 'query' 10.26.1.201
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[!] Target record not found!
```

- Outils : BloodHound, PingCastle, ADRecon, krbrelayx, LdapRelayScan, ...

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Configuration de l'AD

- Méthodes d'administration
 - Présence d'un AV / EDR
 - ADIDNS
 - **Protocoles**
 - WSUS
 - SCCM
 - Nomenclature utilisée
 - ...
-
- Outils : BloodHound, PingCastle, ADRecon, krbrelayx, LdapRelayScan, ...

```
└─$ python3 LdapRelayScan.py -method BOTH -u C3-P0 -p '██████████' -dc-ip 10.26.1.201

~Domain Controllers identified~
Gal-Korriban.galaxy.lan

~Checking DCs for LDAP NTLM relay protections~
Gal-Korriban.galaxy.lan
[+] (LDAP) SERVER SIGNING REQUIREMENTS NOT ENFORCED!
```

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Configuration de l'AD

- Méthodes d'administration
 - Présence d'un AV / EDR
 - ADIDNS
 - Protocoles
 - **WSUS**
 - SCCM
 - Nomenclature utilisée
 - ...
-
- Outils : BloodHound, PingCastle, ADRecon, krbrelayx, LdapRelayScan, ...

WSUS settings

WSUS settings allow workstations and servers located on the intranet to be updated. The [reference documentation is here](#). Here are the settings found in GPO.

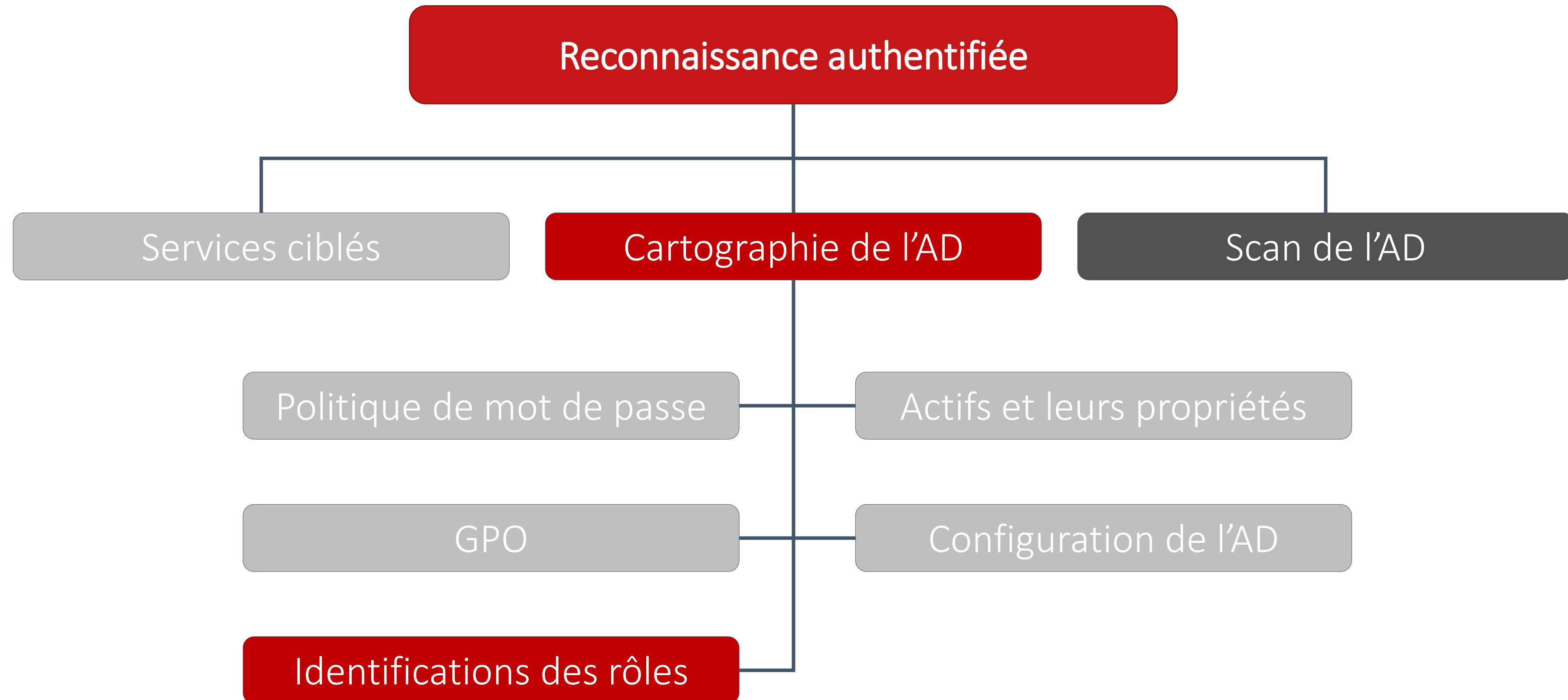
Search

Policy Name	WSUS Server	UseWUserver	ElevateNonAdmins	AUOptions	NoAutoUpdate	NoAutoRelay
No matching records found						



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Identifications des rôles

- ADCS
- ...
- Outils : Certify, Certipy, BloodHound, ADRecon, ...

```
PS C:\Users\isec-mdt\Documents> .\Certify.exe find /domain:galaxy.lan /vulnerable

Certify

v1.1.0

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=galaxy,DC=lan'

[*] Listing info about the Enterprise CA 'galaxy-GAL-KEPLER452B-CA'

Enterprise CA Name      : galaxy-GAL-KEPLER452B-CA
DNS Hostname           : Gal-Kepler452b.galaxy.lan
FullName               : Gal-Kepler452b.galaxy.lan\galaxy-GAL-KEPLER452B-CA
Flags                  : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
...
Allow ManageCA, ManageCertificates <UNKNOWN> S-1-5-21-981138465-6192414
Enrollment Agent Restrictions : None

[!] Vulnerable Certificates Templates :

CA Name      : Gal-Kepler452b.galaxy.lan\galaxy-GAL-KEPLER452B-CA
Template Name : StormTrooperEnrollement
Schema Version : 2
Validity Period : 1 year
Renewal Period : 6 weeks
mspki-Certificate-Name-Flag : ENROLLEE_SUPPLIES_SUBJECT
mspki-enrollment-flag : INCLUDE_SYMMETRIC_ALGORITHMS, PUBLISH_TO_DS
Authorized Signatures Required : 0
pkiextendedkeyusage : Authentification du client, Messagerie électronique sécurisée, Système
mspki-certificate-application-policy : Authentification du client, Messagerie électronique sécurisée, Système
Permissions
  Enrollment Permissions
  Enrollment Rights : AUTORITE NT\Utilisateurs authentifiésS-1-5-11
  Object Control Permissions
  Owner : <UNKNOWN> S-1-5-21-981138465-619241437-4107189995-512
  WriteOwner Principals : <UNKNOWN> S-1-5-21-981138465-619241437-4107189995-512
  WriteDacl Principals : <UNKNOWN> S-1-5-21-981138465-619241437-4107189995-519
  WriteProperty Principals : <UNKNOWN> S-1-5-21-981138465-619241437-4107189995-512
  WriteProperty Principals : <UNKNOWN> S-1-5-21-981138465-619241437-4107189995-519
```

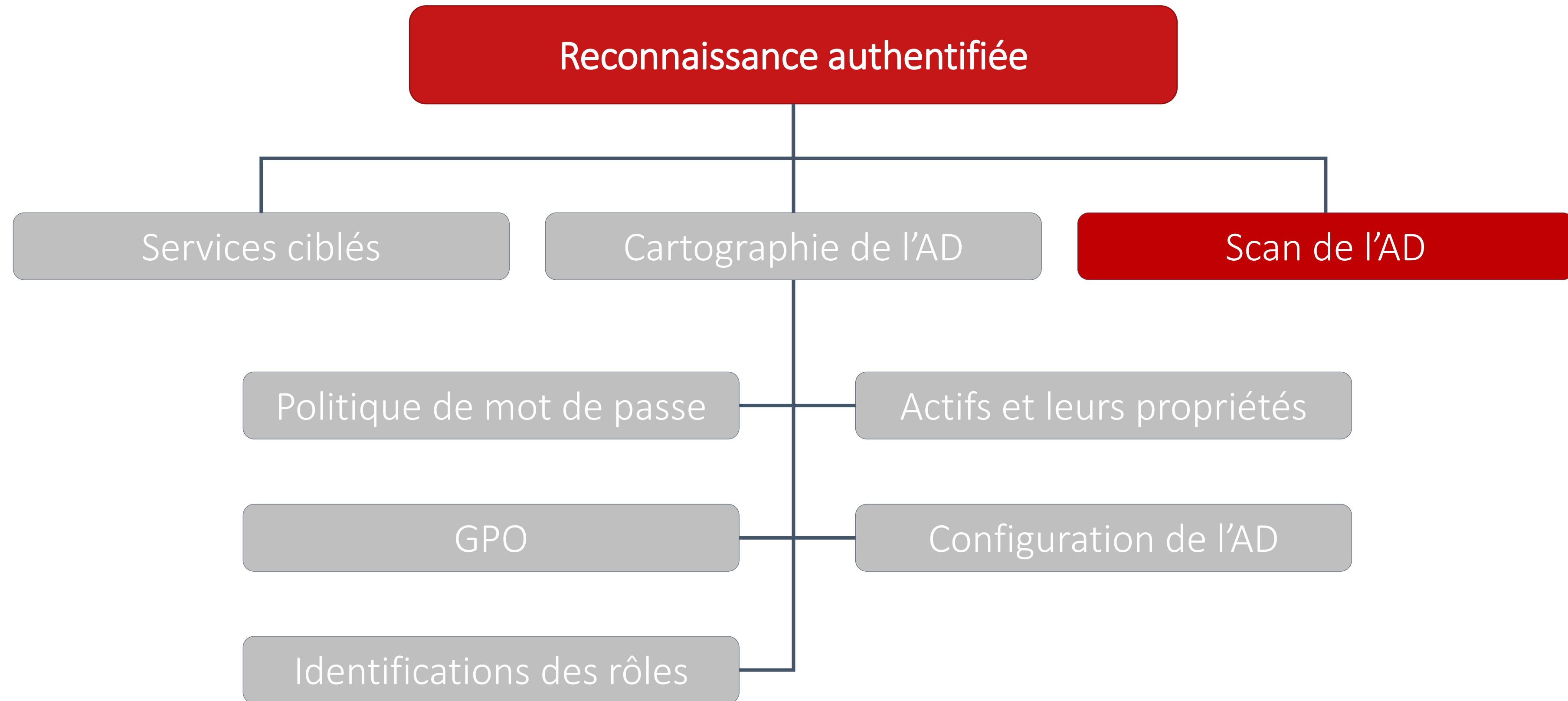
```
certipy find -u C3-P0@galaxy.lan -p 'sSTARWARS!@#$5' -dc-ip 10.26.1.201 -stdout -vulnerable
Certipy v4.3.0 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Trying to get CA configuration for 'galaxy-GAL-KEPLER452B-CA' via CSRA
[!] Got error while trying to get CA configuration for 'galaxy-GAL-KEPLER452B-CA' via CSRA: CASessionError: code: 0x80070005 - E_ACCESSDENIED - General access denied error.
[*] Trying to get CA configuration for 'galaxy-GAL-KEPLER452B-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Got CA configuration for 'galaxy-GAL-KEPLER452B-CA'
[*] Enumeration output:
Certificate Authorities
0
CA Name : galaxy-GAL-KEPLER452B-CA
DNS Name : Gal-Kepler452b.galaxy.lan
Certificate Subject : CN=galaxy-GAL-KEPLER452B-CA, DC=galaxy, DC=lan
Certificate Serial Number : 741F24E1D0059B944B95AA970812616E
Certificate Validity Start : 2023-03-15 15:02:56+00:00
Certificate Validity End : 2028-03-15 15:12:56+00:00
Enrollment Agent : GALAXY.LAN\Domain Admins
Enrollment Agent : GALAXY.LAN\Enterprise Admins
Enroll : GALAXY.LAN\Authenticated Users
[!] Vulnerabilities
ESC8 : Web Enrollment is enabled and Request Disposition is set to Issue
Certificate Templates
0
Template Name : StormTrooperEnrollement
Display Name : StormTrooper Enrollement
Certificate Authorities : galaxy-GAL-KEPLER452B-CA
Enabled : True
Client Authentication : True
Enrollment Agent : False
Any Purpose : False
Enrollee Supplies Subject : True
Certificate Name Flag : EnrolleeSuppliesSubject
Enrollment Flag : PublishToDs
IncludeSymmetricAlgorithms
Private Key Flag : ExportableKey
Extended Key Usage : Encrypting File System
Secure Email
Client Authentication
Requires Manager Approval : False
Requires Key Archival : False
Authorized Signatures Required : 0
Validity Period : 1 year
Renewal Period : 6 weeks
Minimum RSA Key Length : 2048
Permissions
Enrollment Permissions
Enrollment Rights : GALAXY.LAN\Authenticated Users
Object Control Permissions
Owner : GALAXY.LAN\Domain Admins
Write Owner Principals : GALAXY.LAN\Domain Admins
GALAXY.LAN\Enterprise Admins
Write Dacl Principals : GALAXY.LAN\Domain Admins
GALAXY.LAN\Enterprise Admins
Write Property Principals : GALAXY.LAN\Domain Admins
GALAXY.LAN\Enterprise Admins
[!] Vulnerabilities
ESC1 : 'GALAXY.LAN\Authenticated Users' can enroll, enrollee supplies subject and
template allows client authentication
```



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Scan de l'AD

- Relever les différents défauts
 - Privilèges permissifs
 - Configuration
 - ...

- Outils : PingCastle, ...

Active Directory Indicators

This section focuses on the core security indicators. Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators

Domain Risk Level: 92 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Compare with statistics
[Privacy notice](#)

Indicator	Score	Rules Matched
Stale Object	31 / 100	5 rules matched
Privileged Accounts	70 / 100	6 rules matched
Trusts	1 / 100	1 rules matched
Anomalies	92 / 100	16 rules matched

Risk model

Stale Objects	Privileged accounts	Trusts
Inactive user or computer	Account take over	Old trust protocol
Network topography	ACL Check	SID Filtering
Object configuration	Admin control	SIDHistory
Obsolete OS	Control paths	Trust impermeability
Old authentication protocols	Delegation Check	Trust inactive
Provisioning	Irreversible change	Trust with Azure
Replication	Privilege control	
Vulnerability management	Read-Only Domain Controllers	

Privileged Accounts

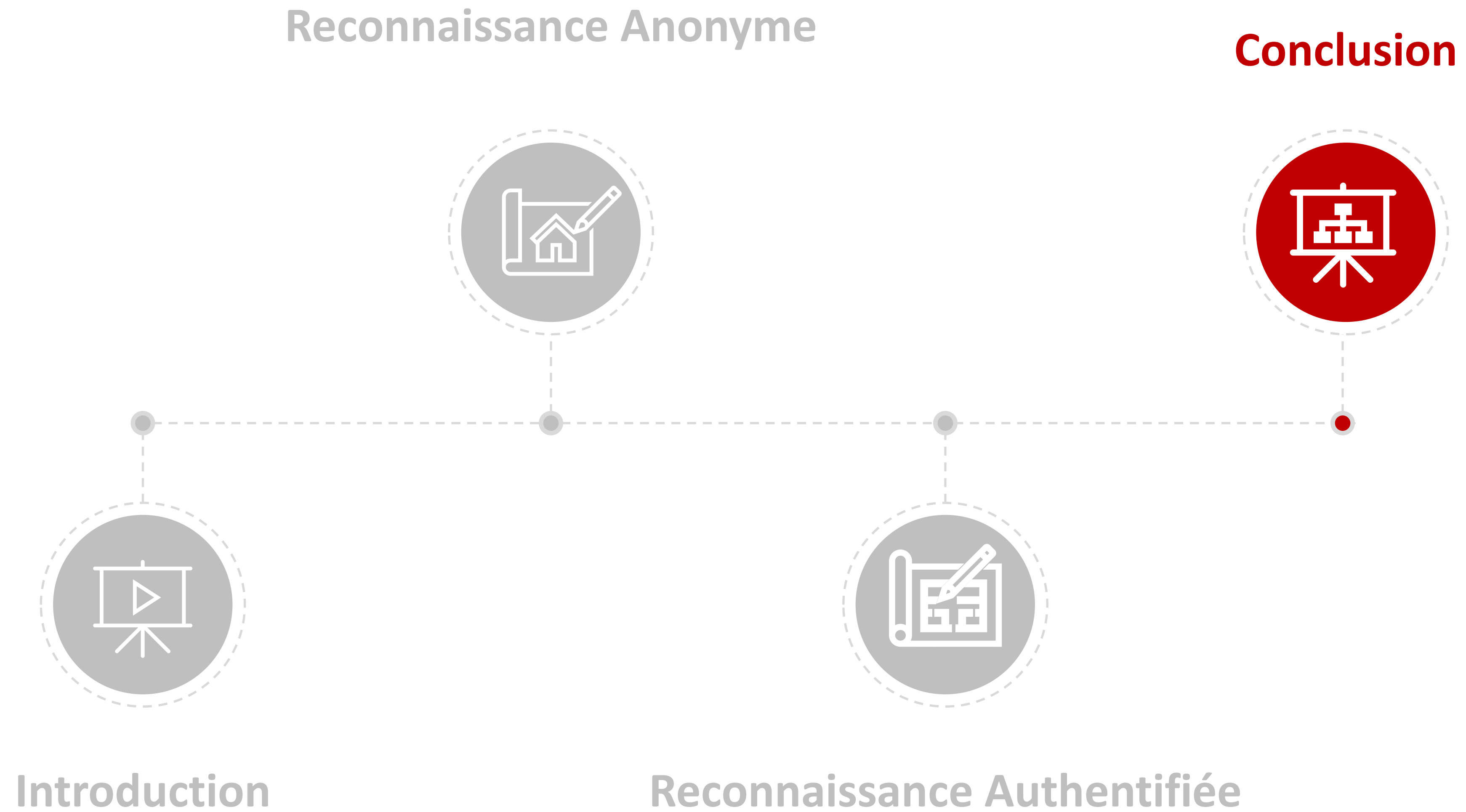
Privileged Accounts : 70 / 100

It is about administrators of the Active Directory

Privileged Accounts rule details [6 rules matched on a total of 42]

Presence of Admin accounts which do not have the flag "this account is sensitive and cannot be delegated": 7	+ 20 Point(s)
The group Exchange Windows Permissions has the right to change the security descriptor of the domain root	+ 15 Point(s)
Number of admins not in Protected Users: 7	+ 10 Point(s)
The Recycle Bin is not enabled	+ 10 Point(s)
The group Schema Admins is not empty: 2 account(s)	+ 10 Point(s)
Unconstrained delegations are configured on the domain: 1 account(s)	+ 5 Point(s)

Plan



Reconnaissance dans un milieu Active Directory

- *In the end, it matters ...*

