ESGI
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 ?

INTRINSEC
Innovative by design

Margaux DABERT

- Consultante en cybersécurité - Pentester
- Chez Intrinsec depuis 2021

Paul SALADIN

- Consultant en cybersécurité - Pentester
- Chez Intrinsec depuis 2021

Plan

Reconnaissance Anonyme

Conclusion

Introduction

Reconnaissance Authentifiée

INTRINSEC

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

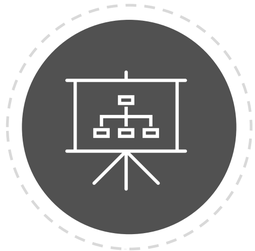
What's next

- 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



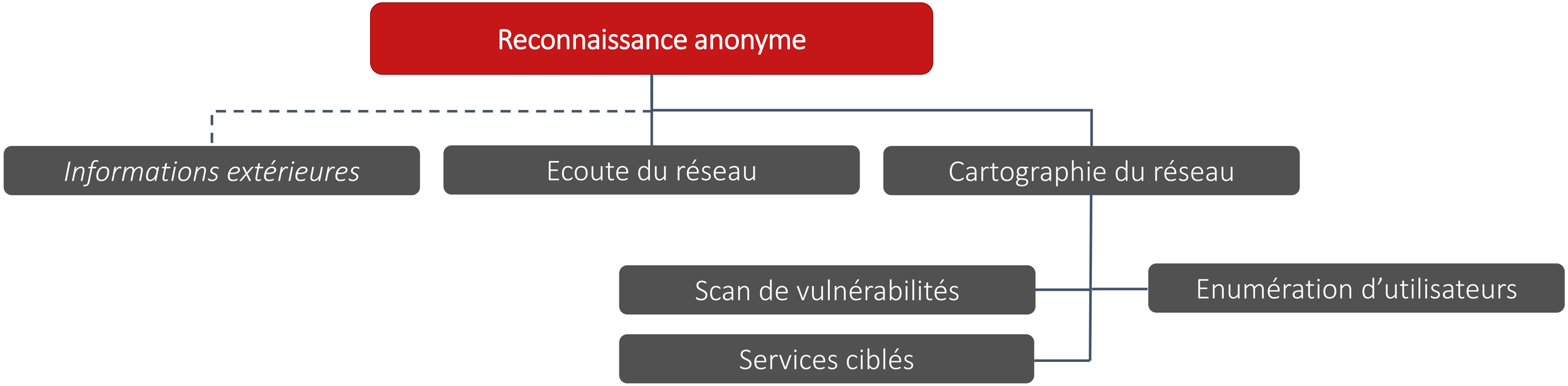
Introduction

Reconnaissance Authentifiée

INTRINSEC

Reconnaissance dans un milieu Active Directory

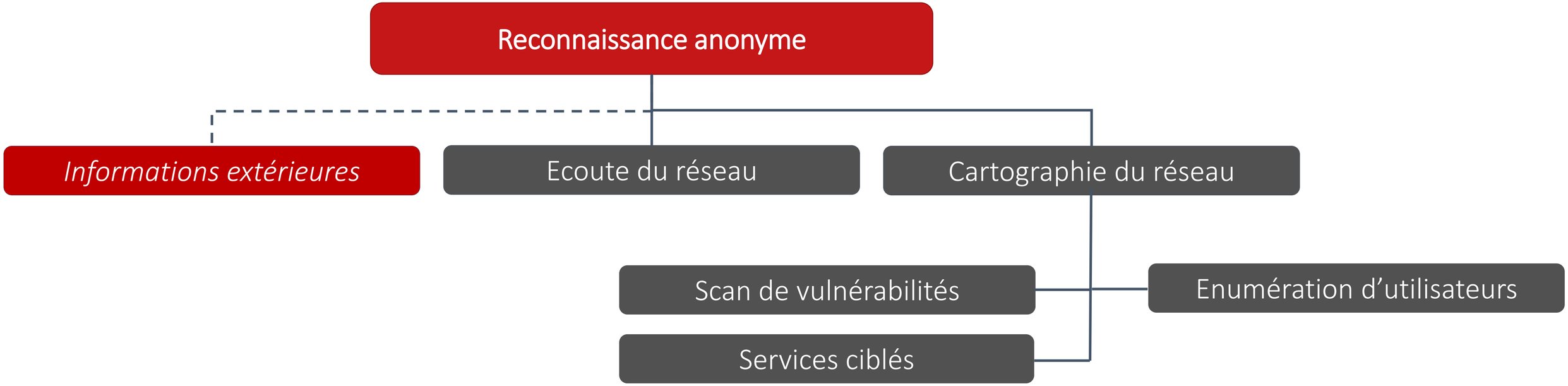
Reconnaissance anonyme



INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme



INTRINSEC

Reconnaissance dans un milieu Active Directory

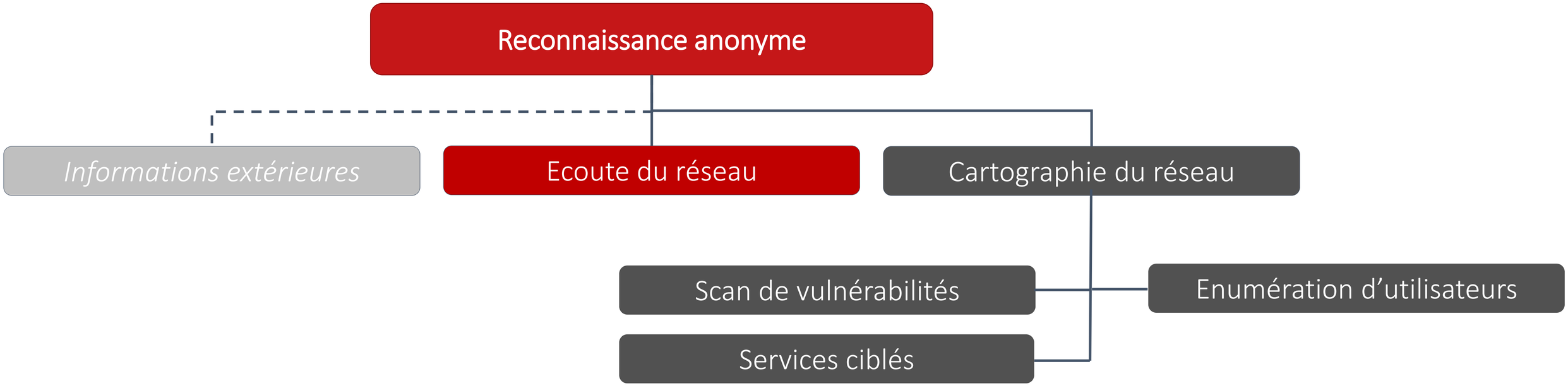
Reconnaissance anonyme – Informations extérieures

- **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

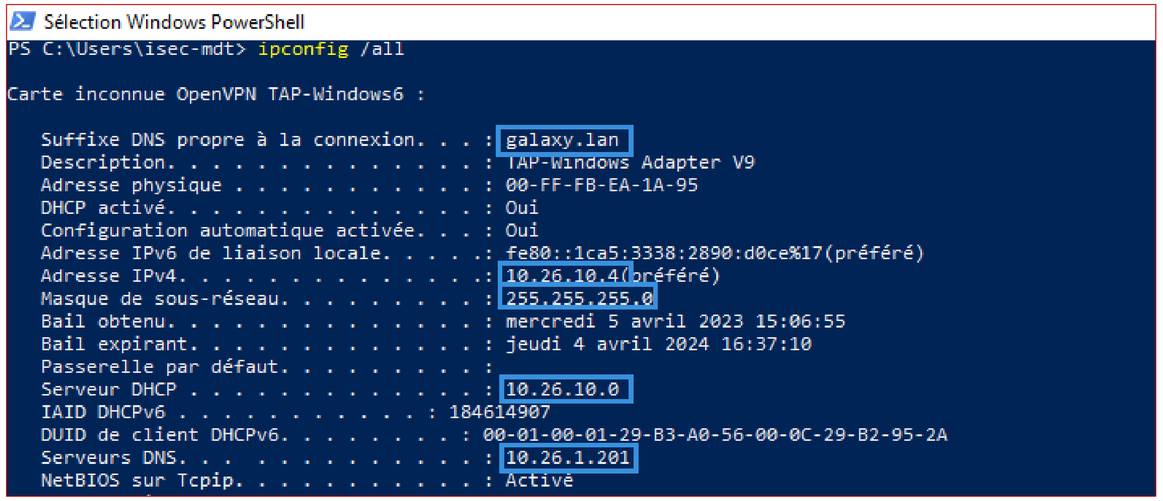


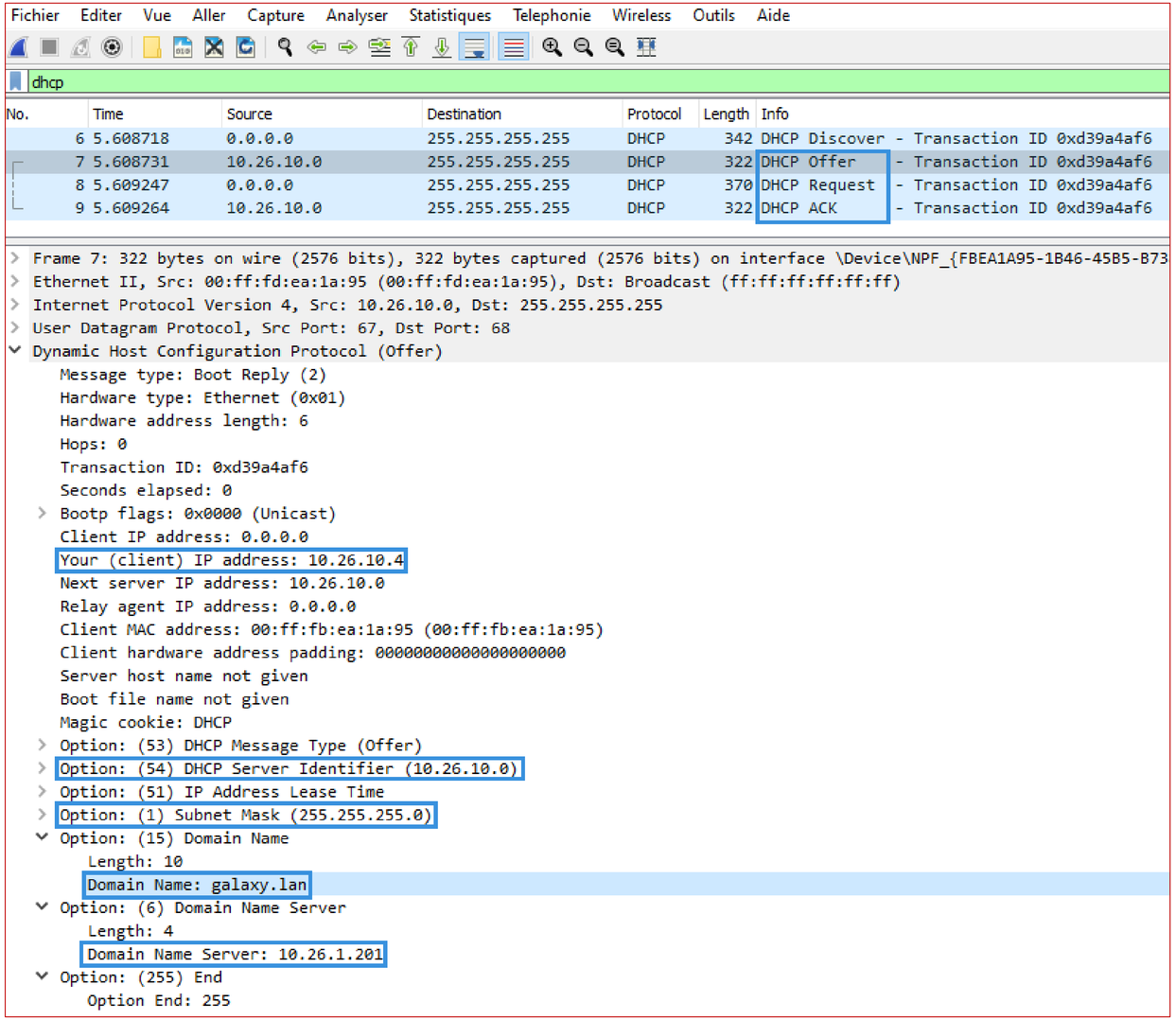
INTRINSEC

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, …



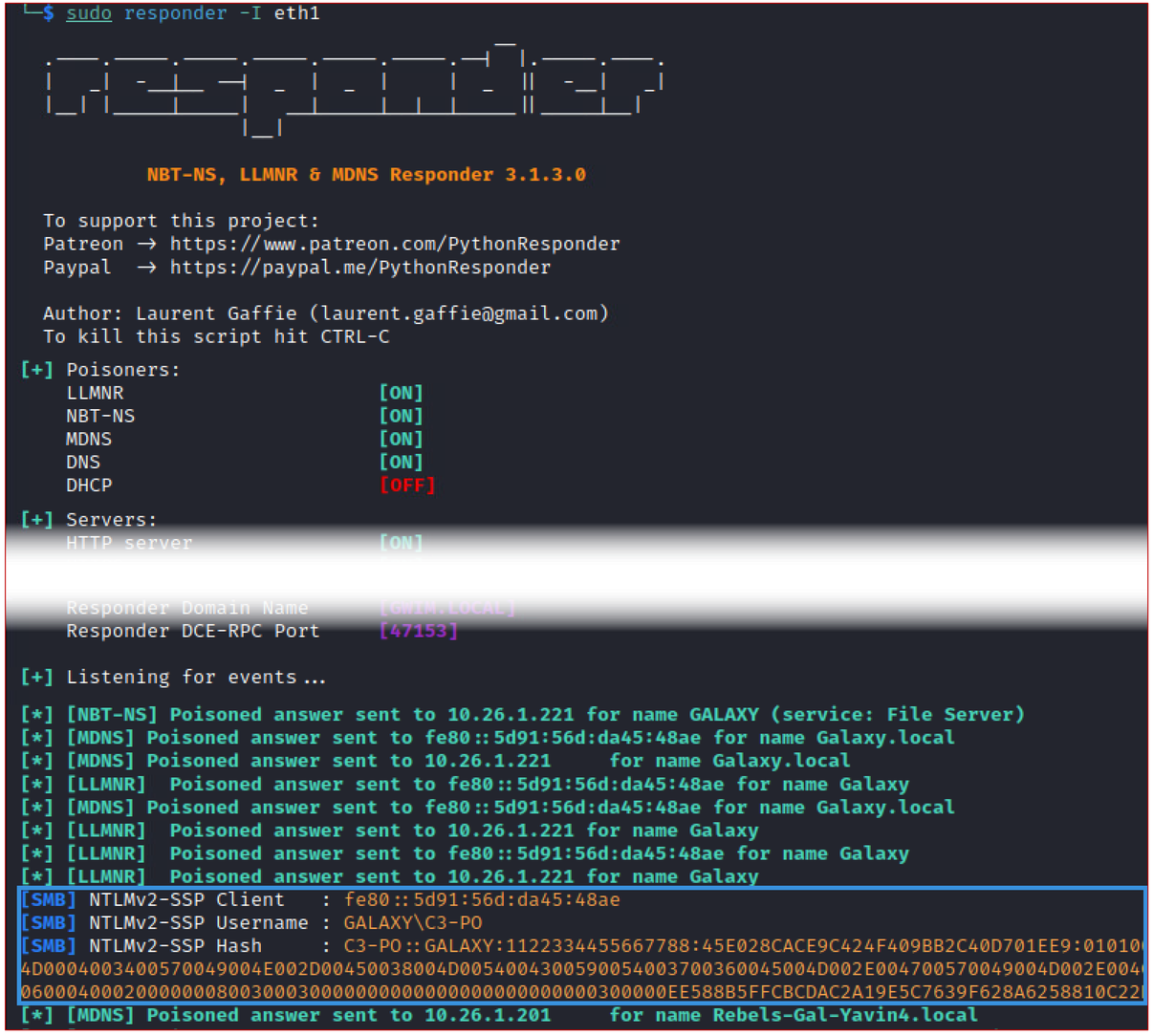


INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme – Ecoute du réseau

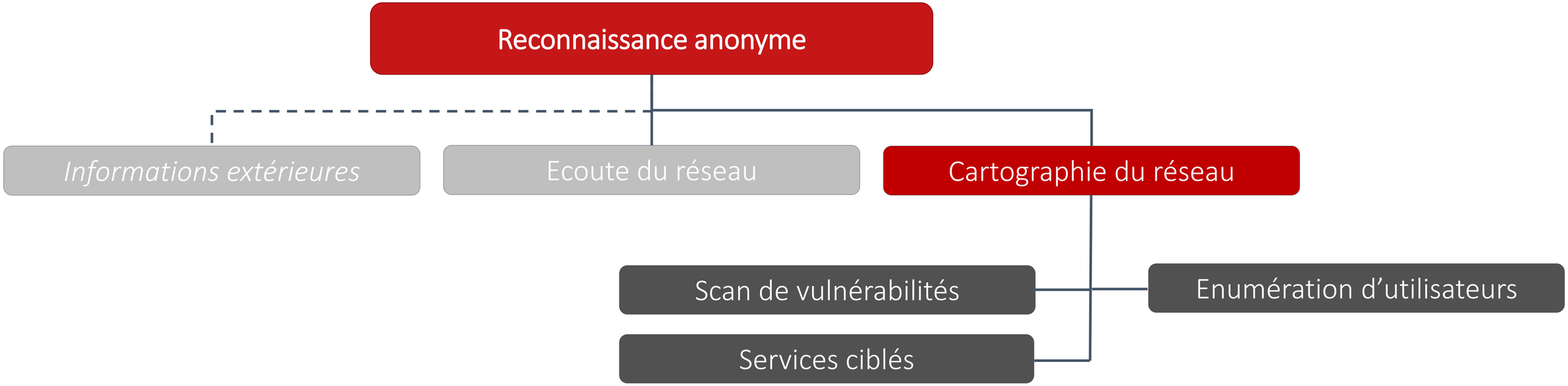
- **Ecoute passive**
- **Ecoute active** (man-in-the-middle)
  - ✓ Redirection des flux
    - Protocoles non sécurisés
    - Interceptions les flux et empoisonnement
    - Demande d'authentification
    - Récupération des challenges (générés à partir du mot de passe)
    - Exploitation de la pile IPv6
- **Outils** : Wireshark, Responder, Mitm6, …



INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme



INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme – Cartographie du réseau

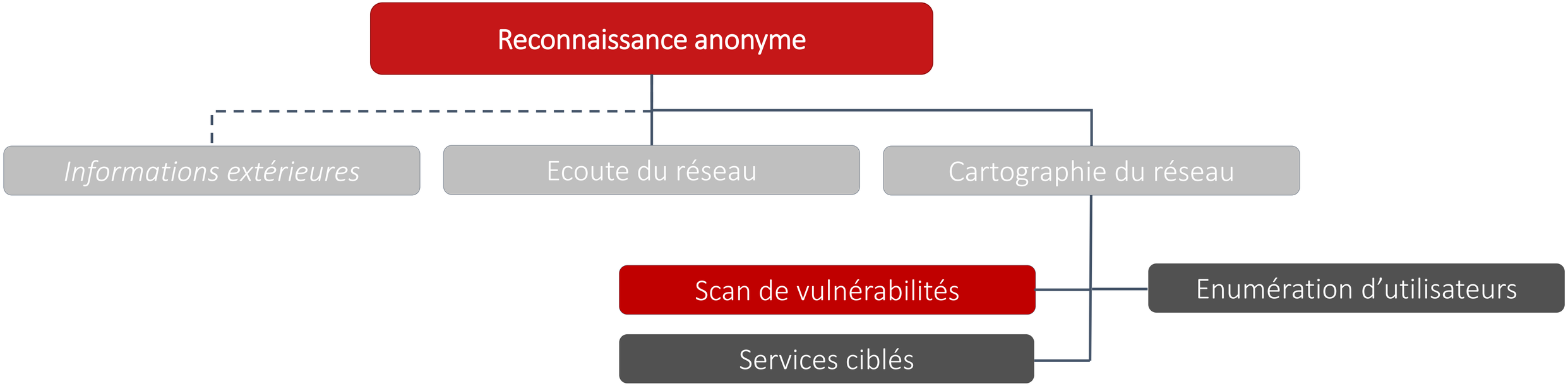
- Scan du réseau
  - ✓ Découvertes des plages réseaux
  - ✓ Découvertes des machines
    - Système d'exploitation
    - Services et versions
- Outils : Arpscan, Nmap, …

```
└─$ 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
|   Product_Version: 10.0.17763
|_  System_Time: 2023-04-15T16:57:43+00:00
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:
| VmXP3HNXOFT/GaYIM+dSk/UFHvz6wCaOpvdEWLxVuJiWgClBODs6svSyaKa3iaLU
| 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
```


INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme



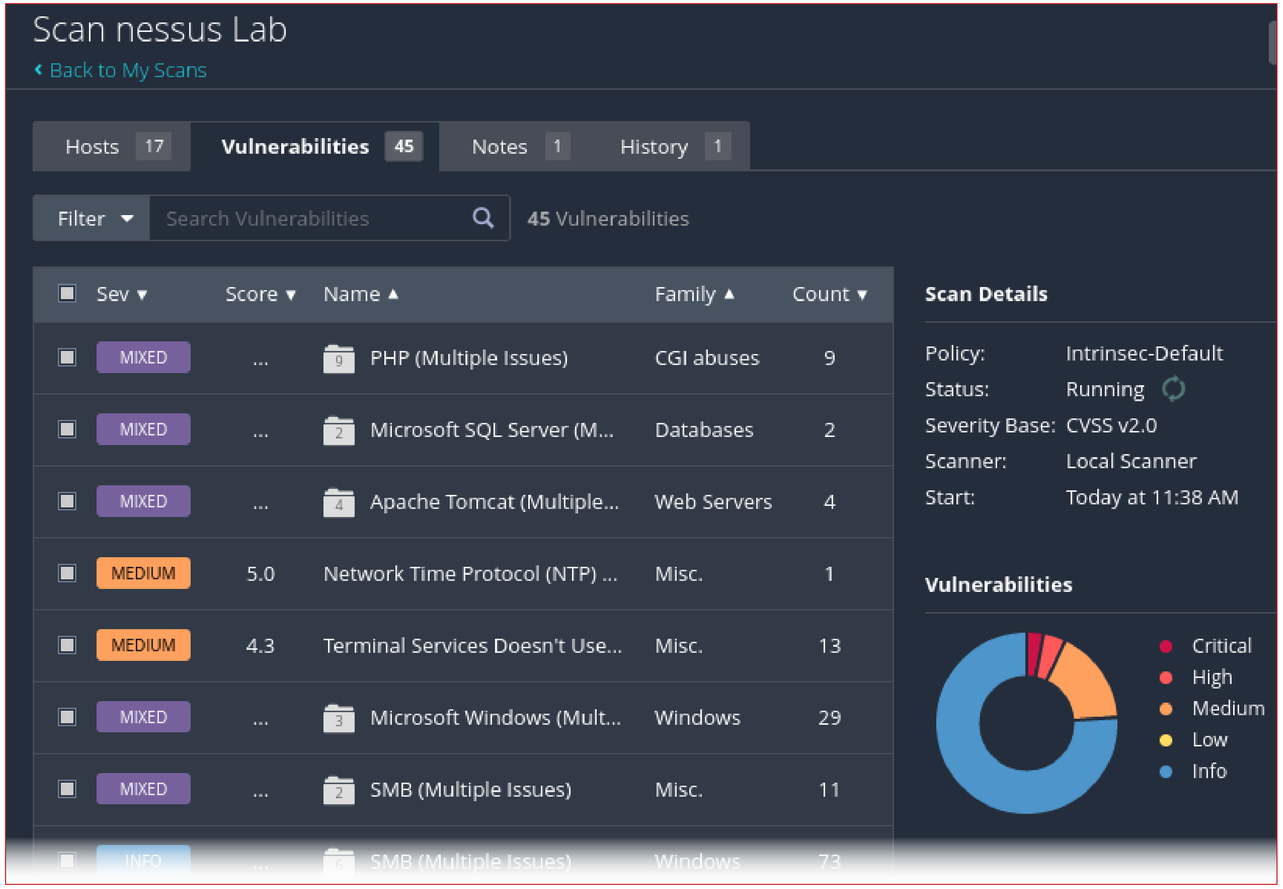
INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme – Scan de vulnérabilités

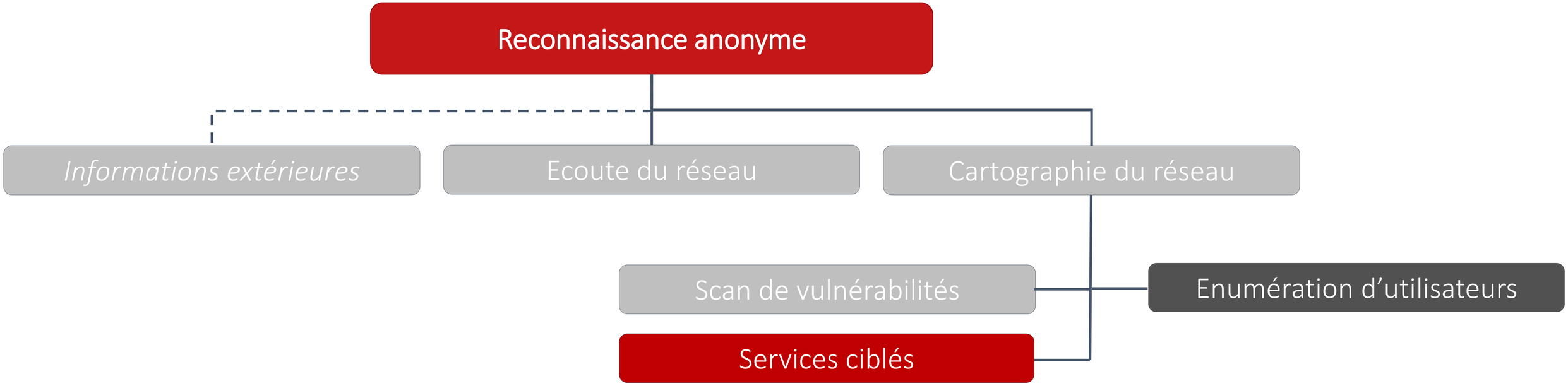
- Scan de vulnérabilités
  - En fonction des versions
  - Basé sur des vulnérabilités connues
  - Non intrusif

- Outils : Nmap, Metasploit, Nessus, Nuclei, …



Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme



INTRINSEC

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, …

INTRINSEC

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
```

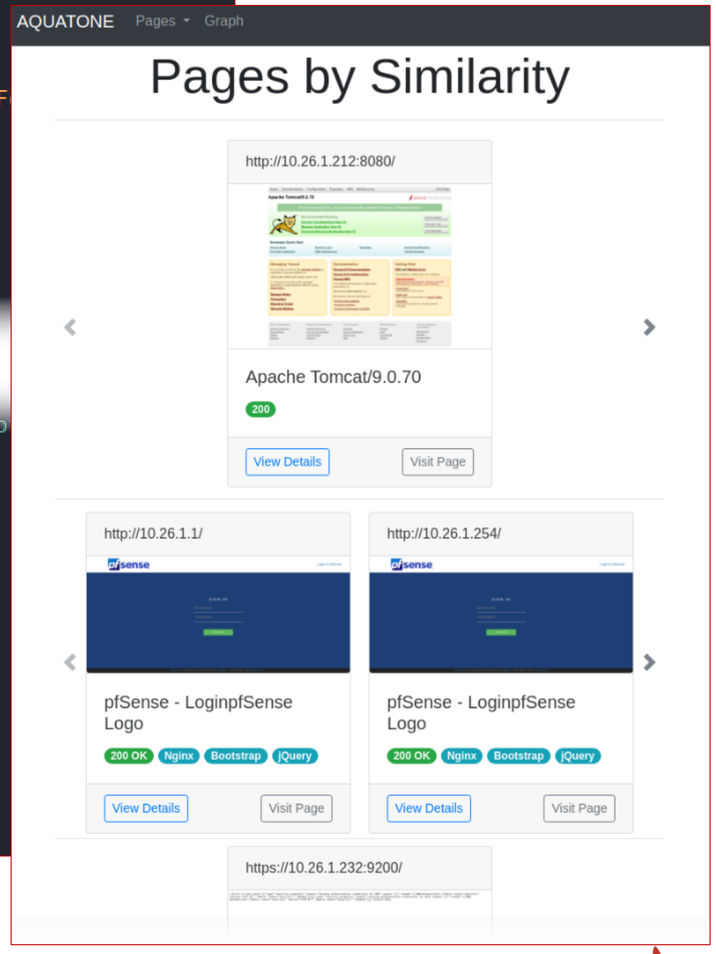

INTRINSEC

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 F
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

https://10.26.1.214:5986/: screenshot successful
https://GAL-KEPLER452B.GALAXY.LAN:5986/: screensho
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
```



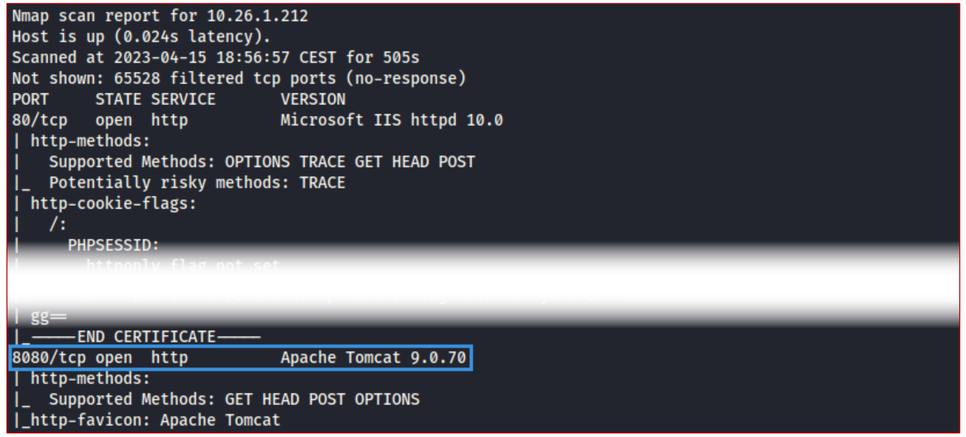
INTRINSEC

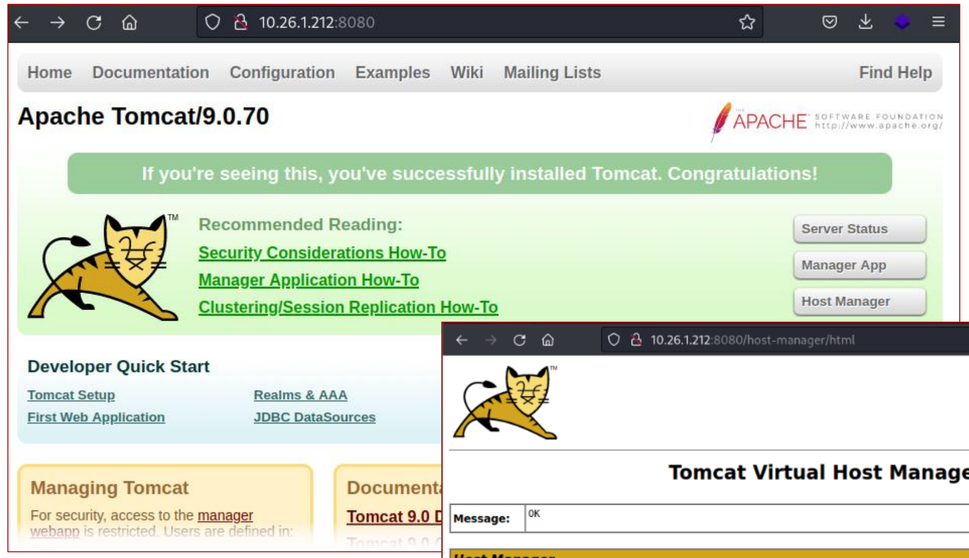
Reconnaissance dans un milieu Active Directory

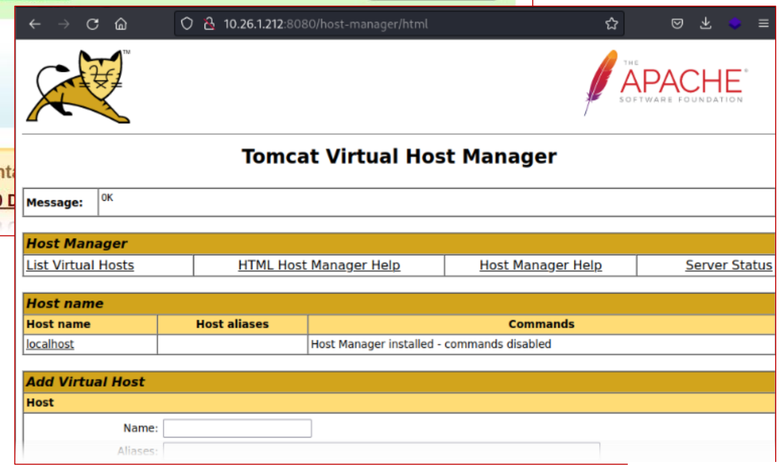
Reconnaissance anonyme – Services ciblés

- Services / Protocoles
  - FTP
  - SSH
  - Telnet
  - **HTTP(S)**
  - SMB
  - SQL
  - …

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







INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme – Services ciblés

- Services / Protocoles
  - FTP
  - SSH
  - Telnet
  - HTTP(S)
  - **SMB**
  - SQL
  - …

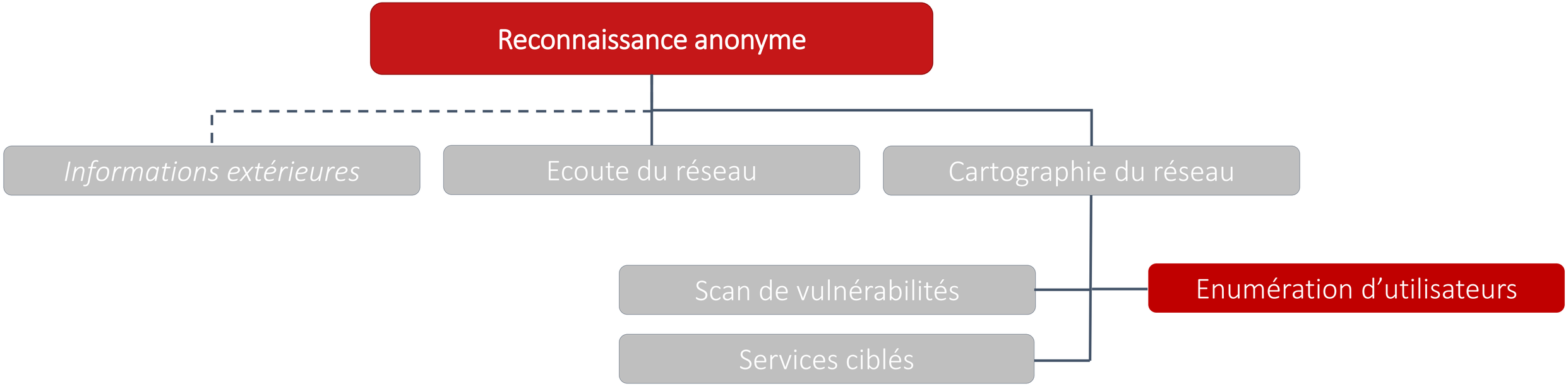
```
└─$ crackmapexec smb 10.26.1.0/24 --shares
SMB         10.26.1.53      445    GAL-KAMINO       [*] Windows 10.0 Build 19041 x64 (name:GAL-KAMINO) (domain:galaxy
.lan) (signing:False) (SMBv1:False)
SMB         10.26.1.52      445    GAL-CORELLIA     [*] Windows 10.0 Build 19041 x64 (name:GAL-CORELLIA) (domain:gala
xy.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:gala
xy.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:r
ebels4.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-M
ARIDUN) (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:ga
laxy.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, …

INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme



INTRINSEC

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*

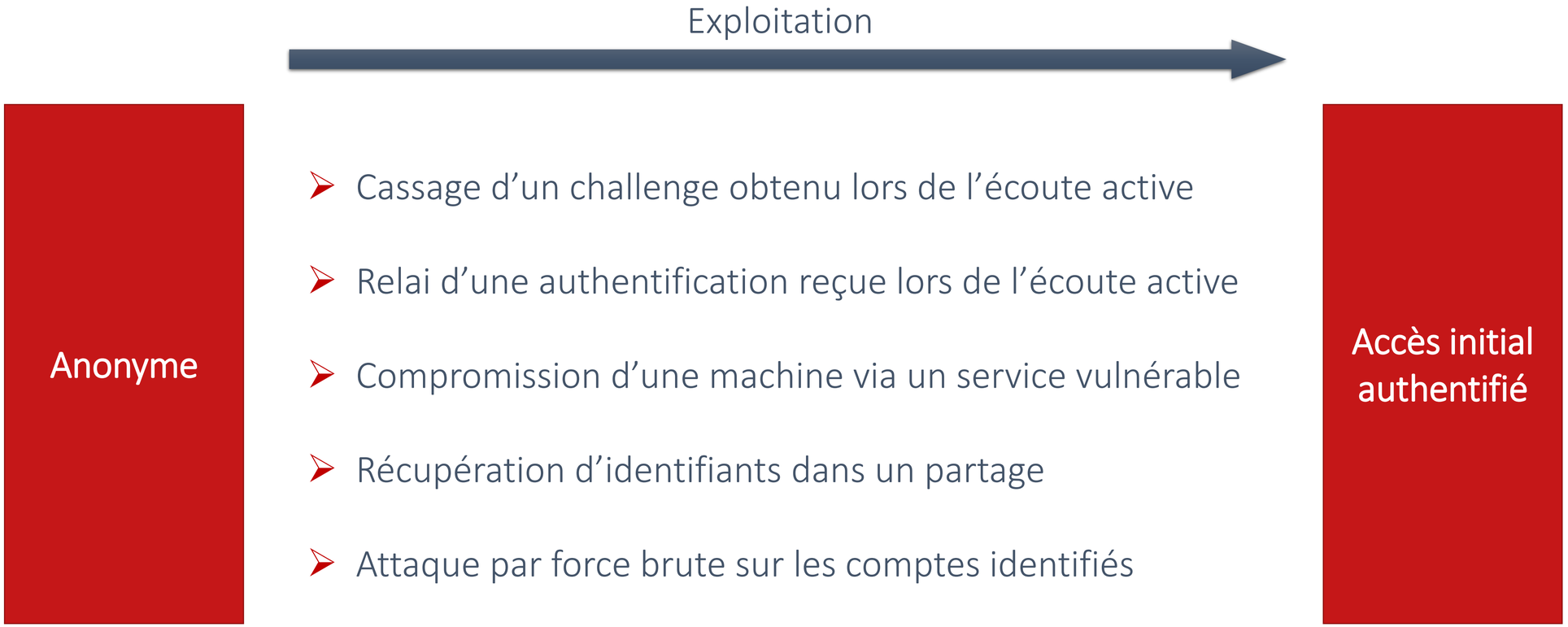
```
└─$ ./kerbrute_linux_amd64 userenum -d galaxy.lan --dc 10.26.1.201 usernames_starwars.txt

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

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

INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance anonyme



INTRINSEC

Plan

Reconnaissance Anonyme

Conclusion

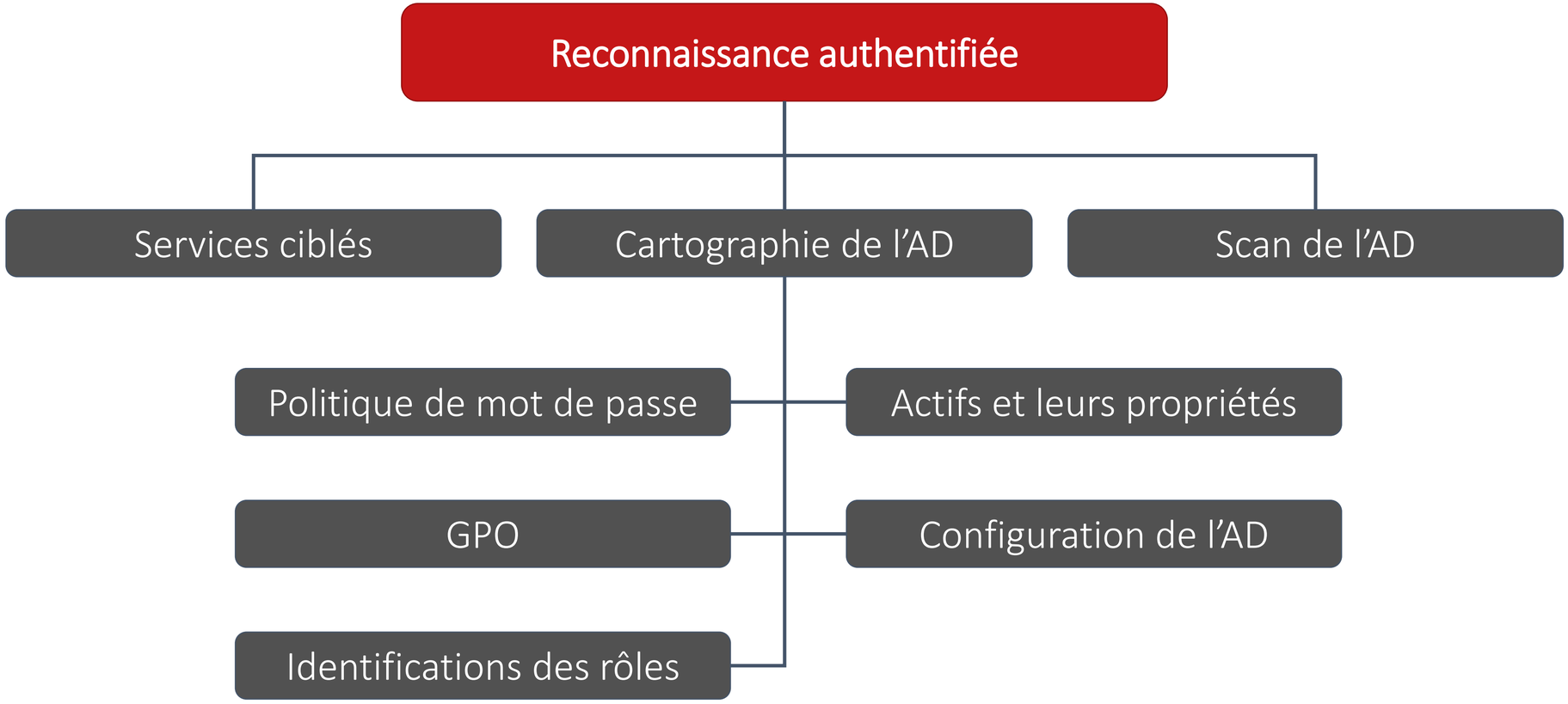
Introduction

Reconnaissance Authentifiée

INTRINSEC

Reconnaissance dans un milieu Active Directory

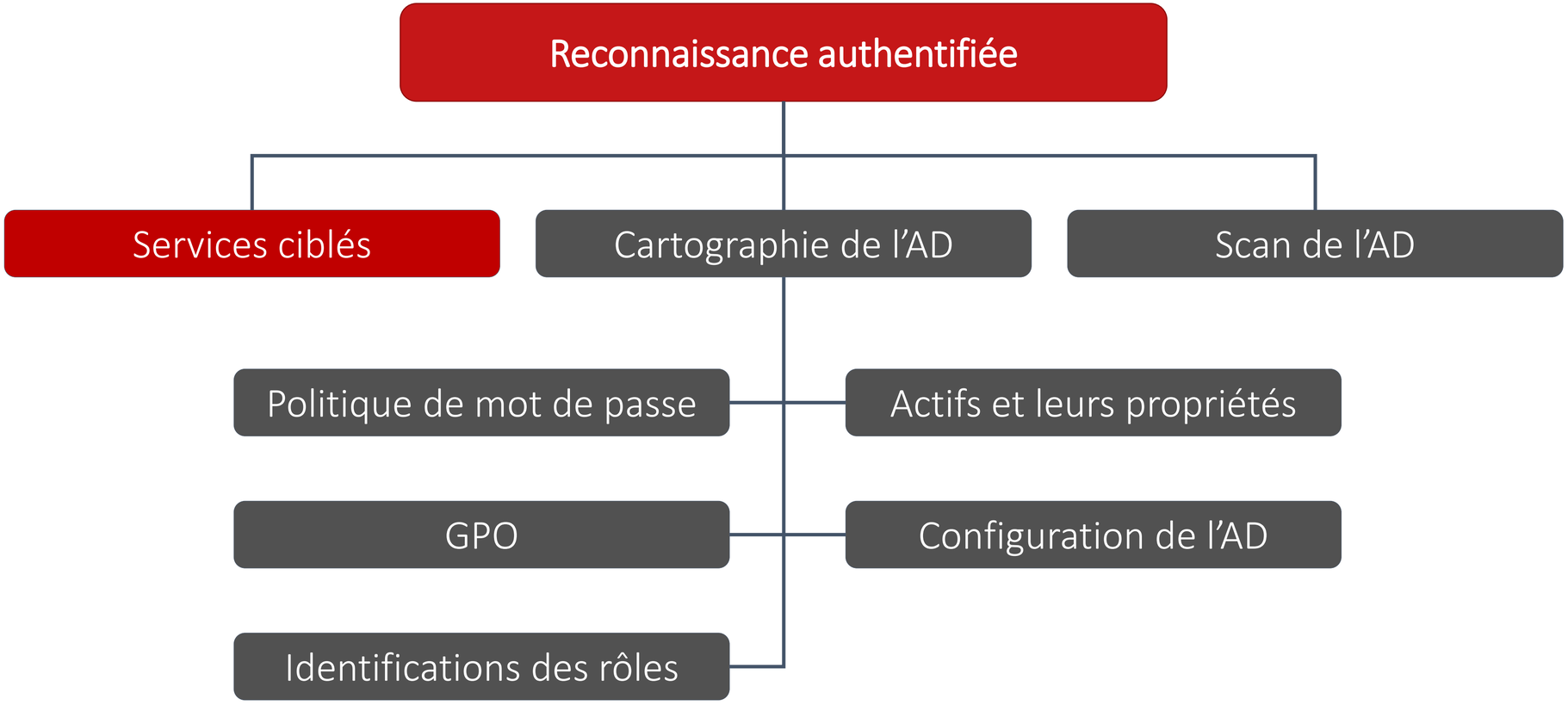
Reconnaissance authentifiée



INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée

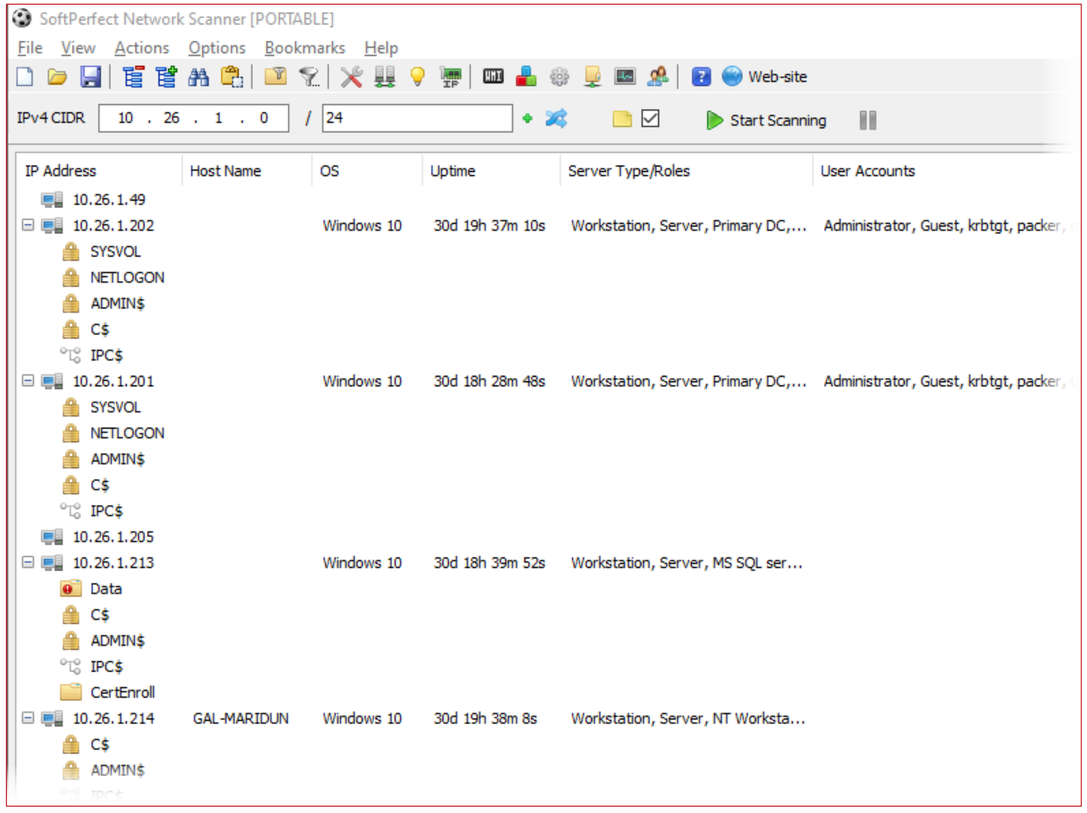


INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Services ciblés / Partages accessibles

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




```
└─$ smbmap -u C3-PO -p [redacted] -d galaxy.lan -H 10.26.1.0/24
[!] 445 not open on 10.26.1.0....
[!] 445 not open on 10.26.1.1....
[!] 445 not open on 10.26.1.2....
[!] 445 not open on 10.26.1.3....
[!] 445 not open on 10.26.1.4....

        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
[+] IP: 10.26.1.52:445  Name: 10.26.1.52
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
[+] IP: 10.26.1.53:445  Name: 10.26.1.53
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
[+] IP: 10.26.1.201:445 Name: galaxy.lan
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
[+] IP: 10.26.1.202:445 Name: 10.26.1.202
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
[+] IP: 10.26.1.212:445 Name: 10.26.1.212
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
```


INTRINSEC

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
```

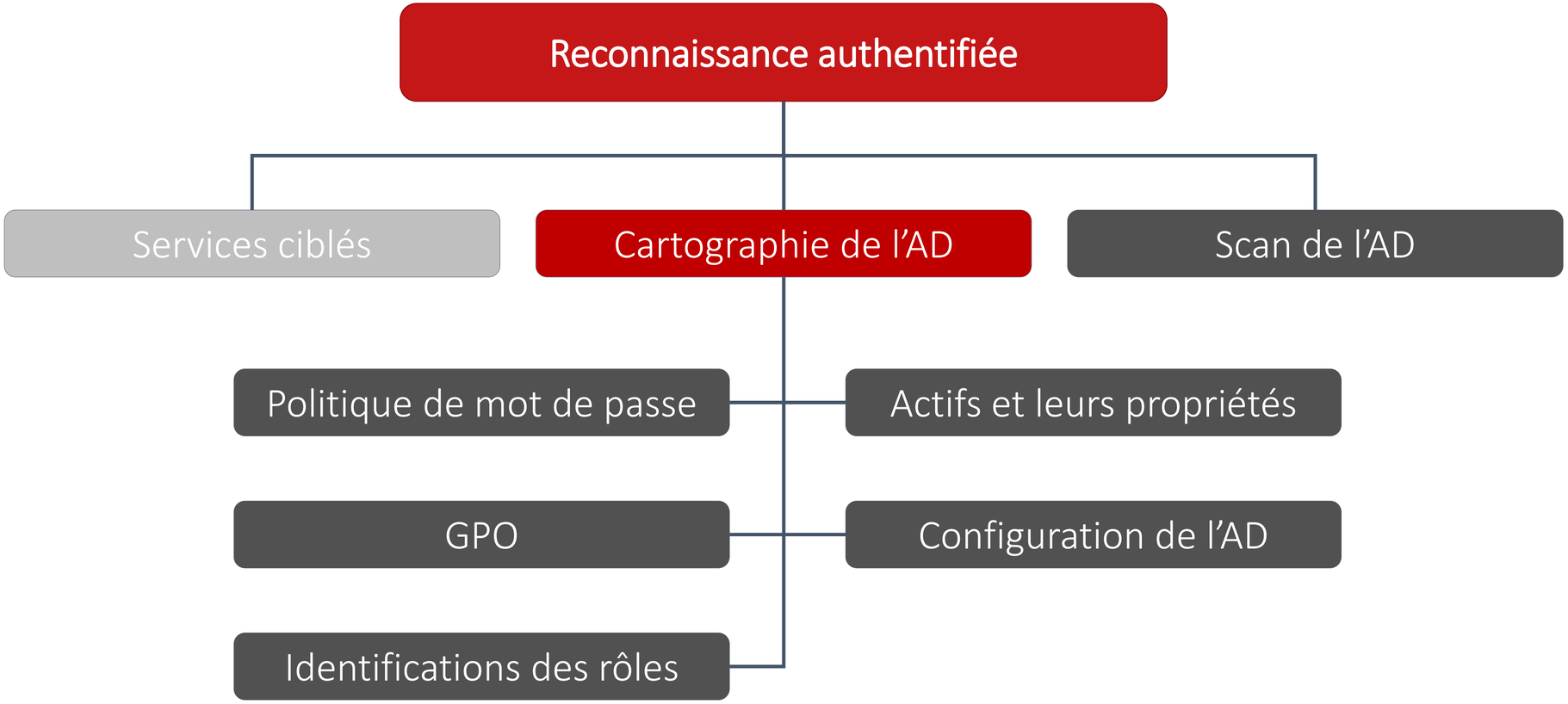
```
PS C:\Users\isec-mdt\Documents> Get-SQLInstanceDomain | Get-SQLConnectionTest

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

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

INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



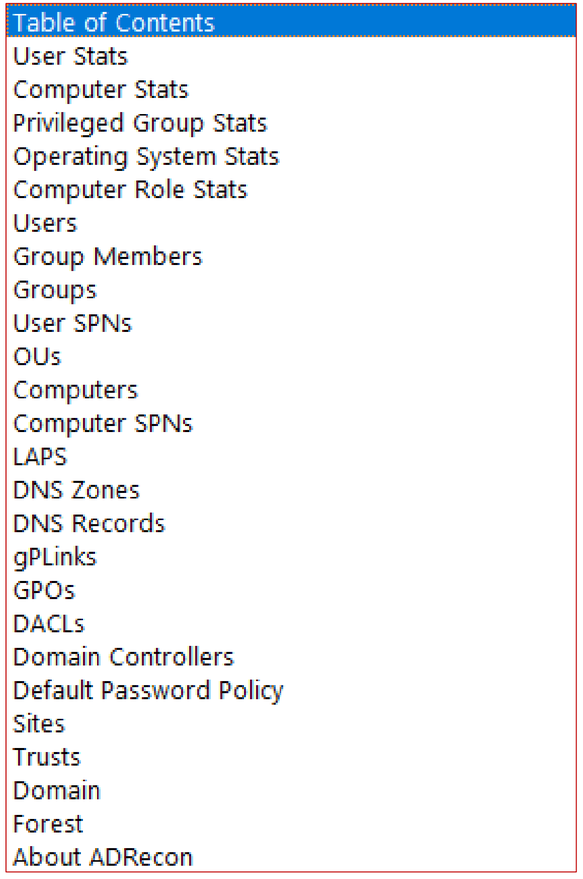
INTRINSEC

Reconnaissance dans un milieu Active Directory

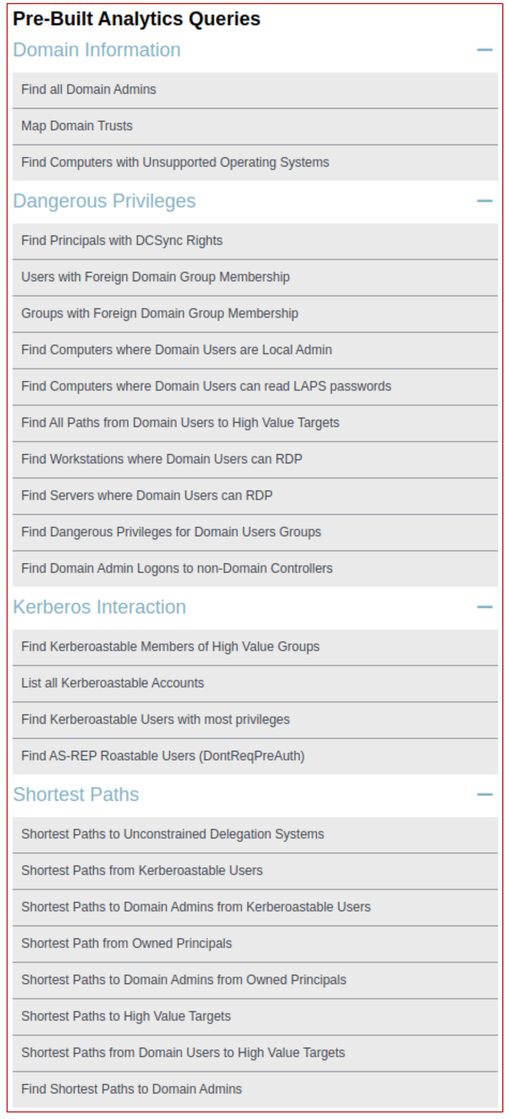
Reconnaissance authentifiée – Cartographie de l'AD

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

- Outils : BloodHound, ADRecon, PowerView …



Classement des informations retrouvées à grâce à ADRecon

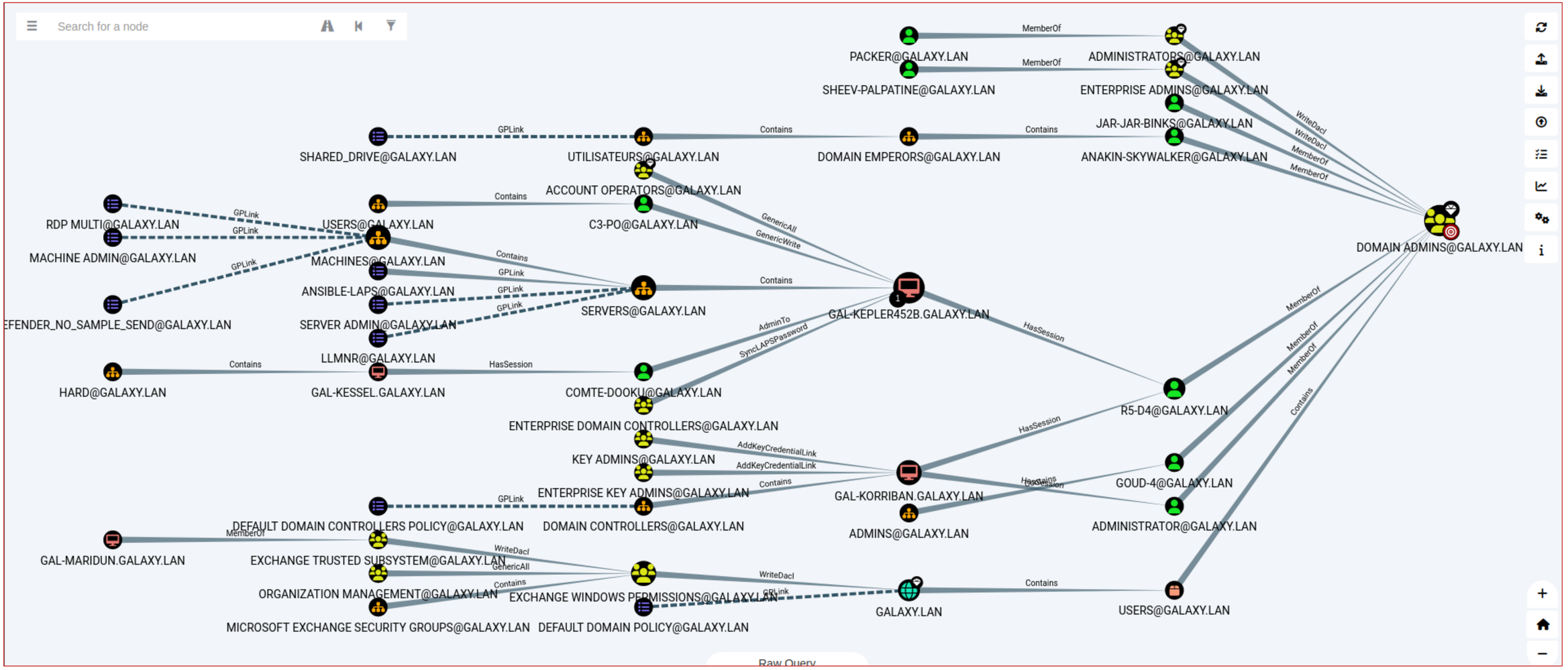


Traitements des données avec Bloodhound (pre-built queries)

INTRINSEC

Reconnaissance dans un milieu Active Directory

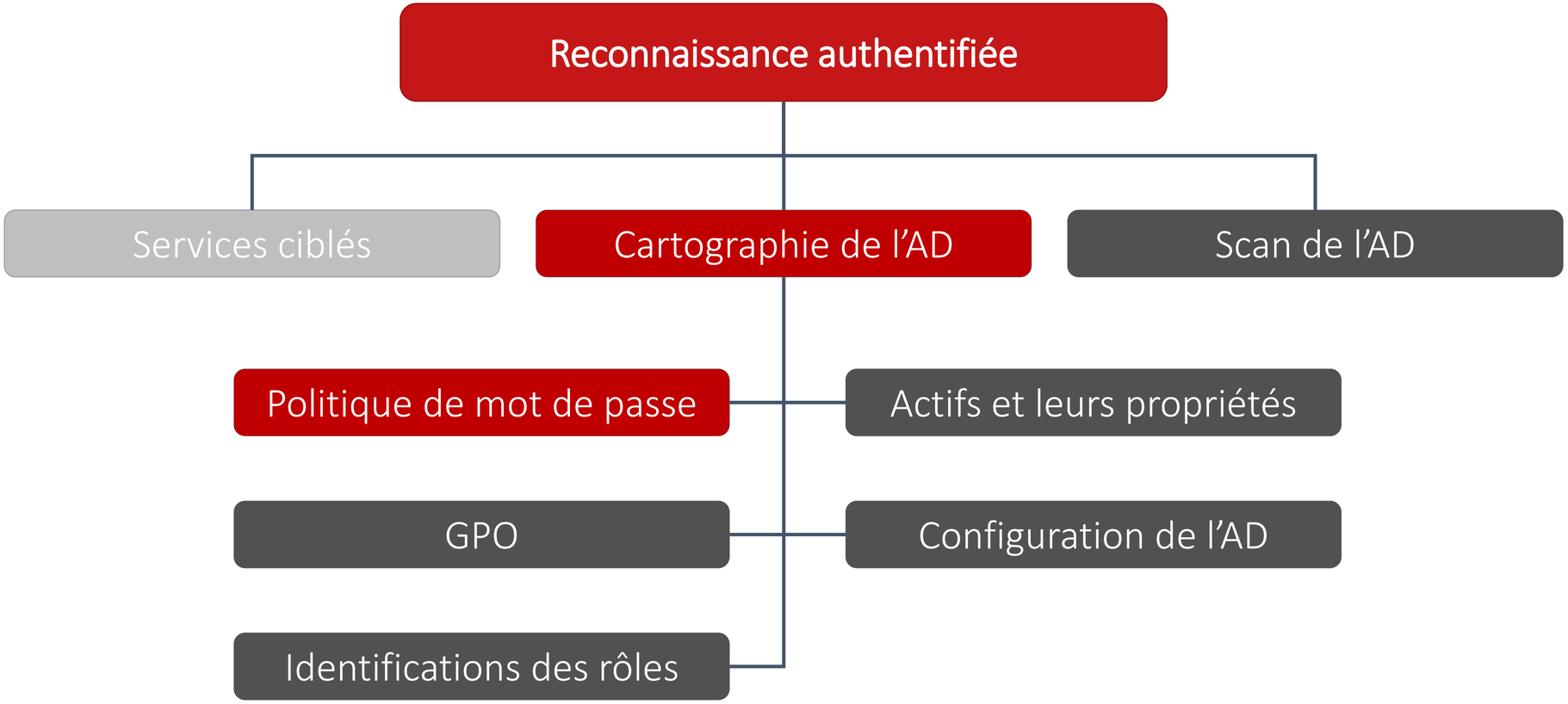
Reconnaissance authentifiée – Cartographie de l'AD



« Find shortest paths to domain admin »

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



INTRINSEC

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

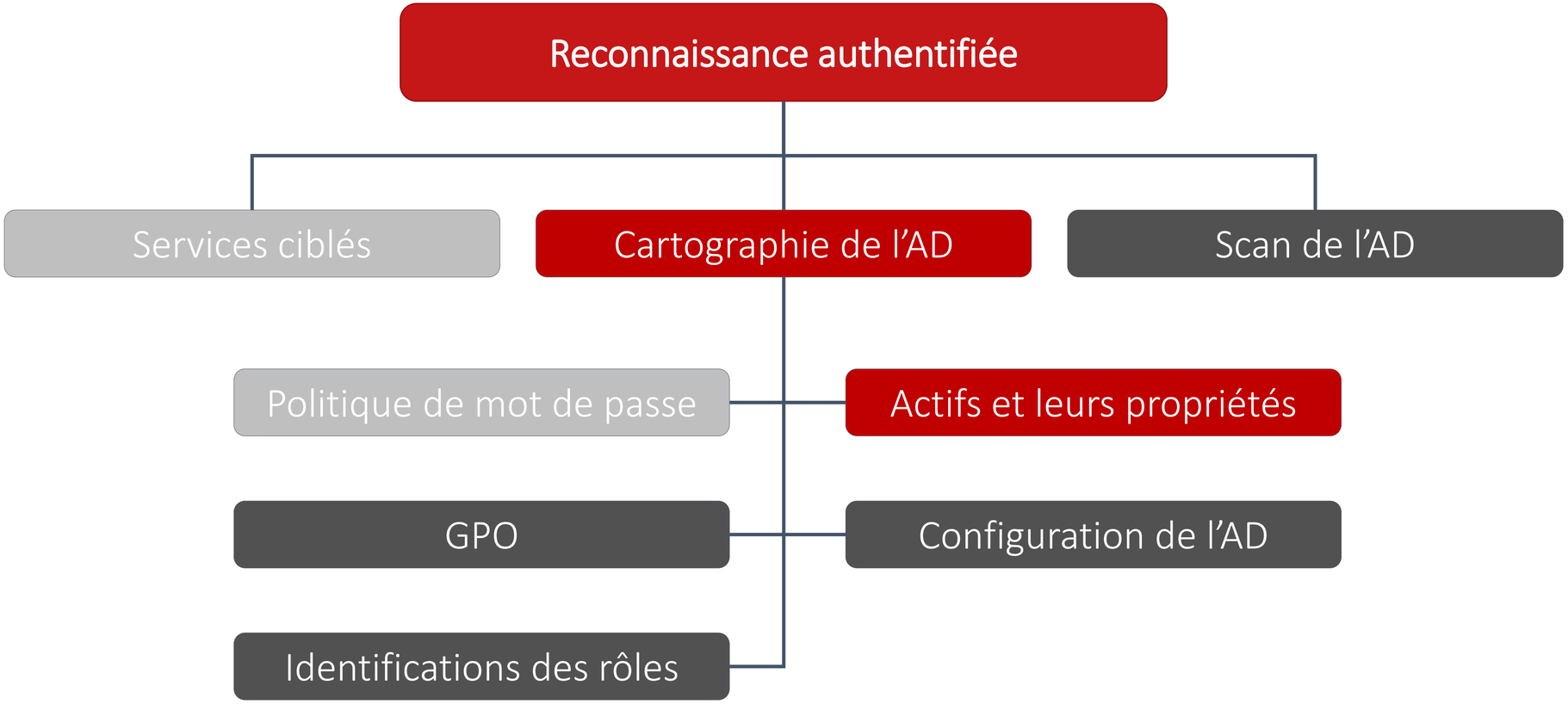
```
PS C:\Windows\system32> Get-ADDefaultDomainPasswordPolicy


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
```


INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



INTRINSEC

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			
1	UserName	Name	Enabled	upID	SID	Description	DistinguishedName
3	Administrator	Administrator	VRAI	513	S-1-5-21-4243601597-32924416	Built-in account for administering the comp	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 chass	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 travailla	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	
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?

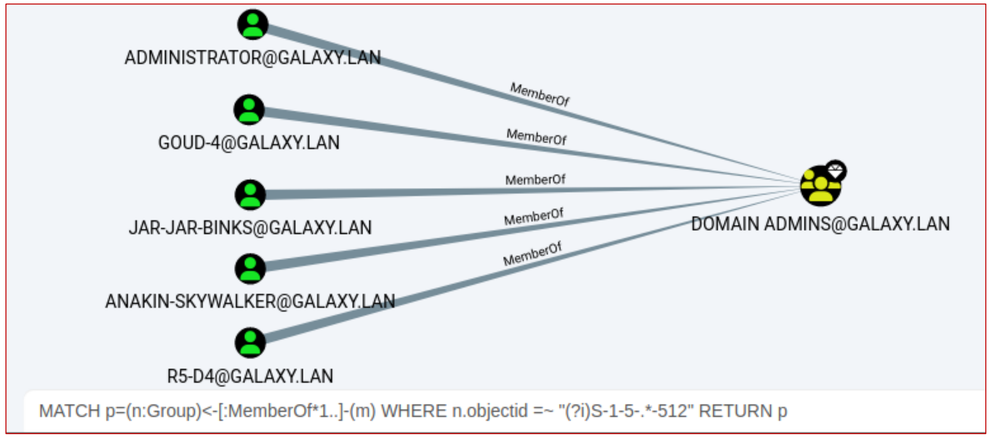
… | Computer Role Stats | Users | Group Members | Groups | User SPNs | OUs | Computers | Computer SPNs | LAPS

INTRINSEC

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
  - …



	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 | …

- Outils : BloodHound, ADRecon, …

INTRINSEC

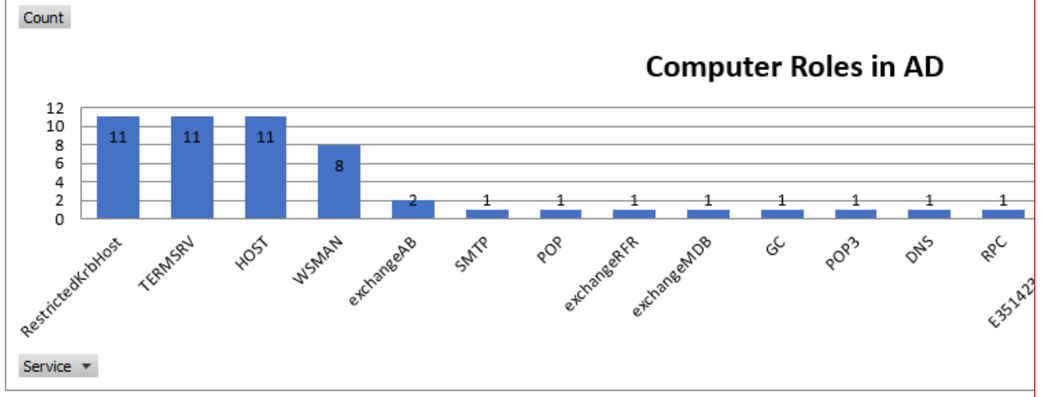
Reconnaissance dans un milieu Active Directory

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, …

Computer Role	Count
RestrictedKrbHost	11
TERMSRV	11
HOST	11
WSMAN	8
exchangeAB	2
SMTP	1
POP	1
exchangeRFR	1
exchangeMDB	1
GC	1
POP3	1
DNS	1
RPC	1
E3514235-4B06-11D1-AB04-00C04FC2DCD2	1
SmtpSvc	1
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04	1
ldap	1
IMAP	1
IMAP4	1
Grand Total	**57**



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

INTRINSEC

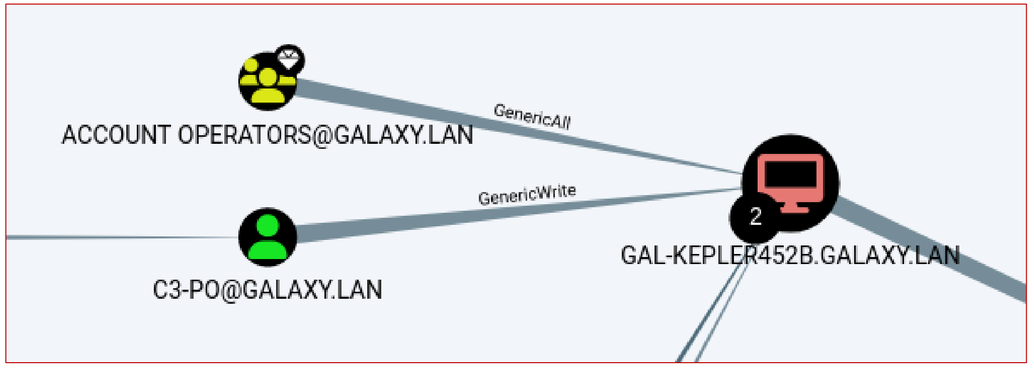
Reconnaissance dans un milieu Active Directory

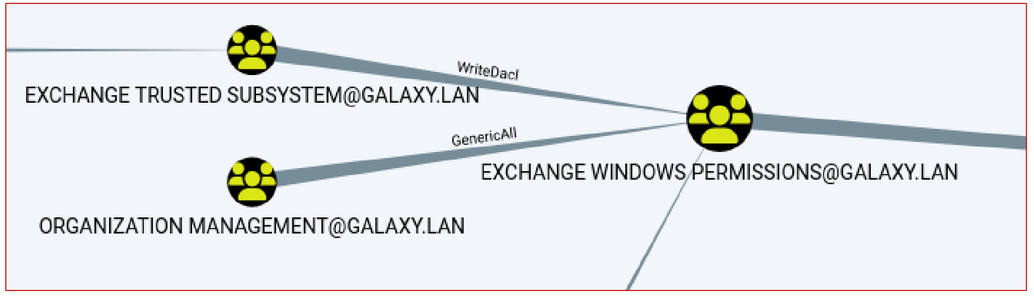
Reconnaissance authentifiée – Actifs de l'AD et leurs propriétés

- Objets de l'Active Directory
  - Utilisateurs
  - Groupes
  - Machines
  - DACL
  - GPO
  - …
- Propriétés
  - Descriptions
  - DistinguishedName
  - …

- Outils : BloodHound, ADRecon, …

Discretionary Access Control List

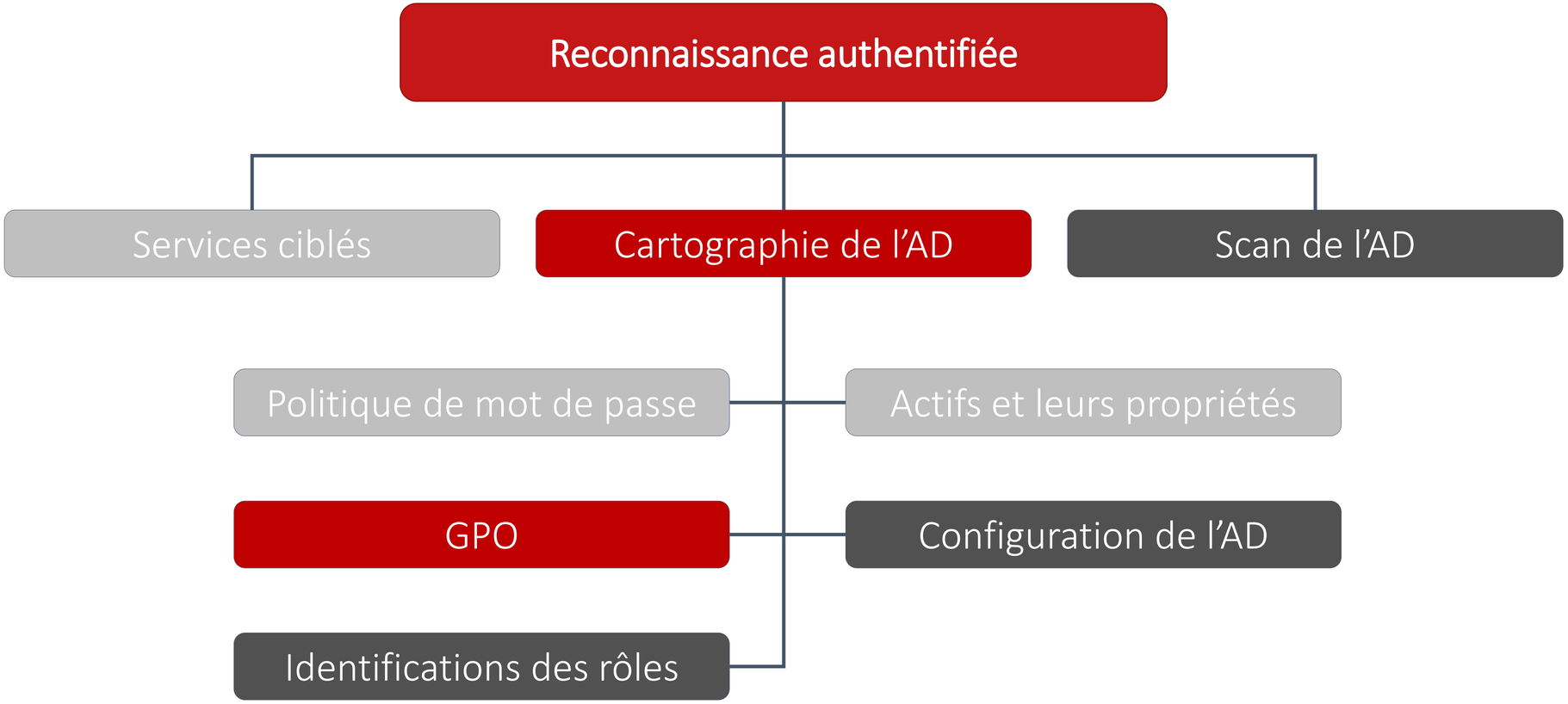




INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée

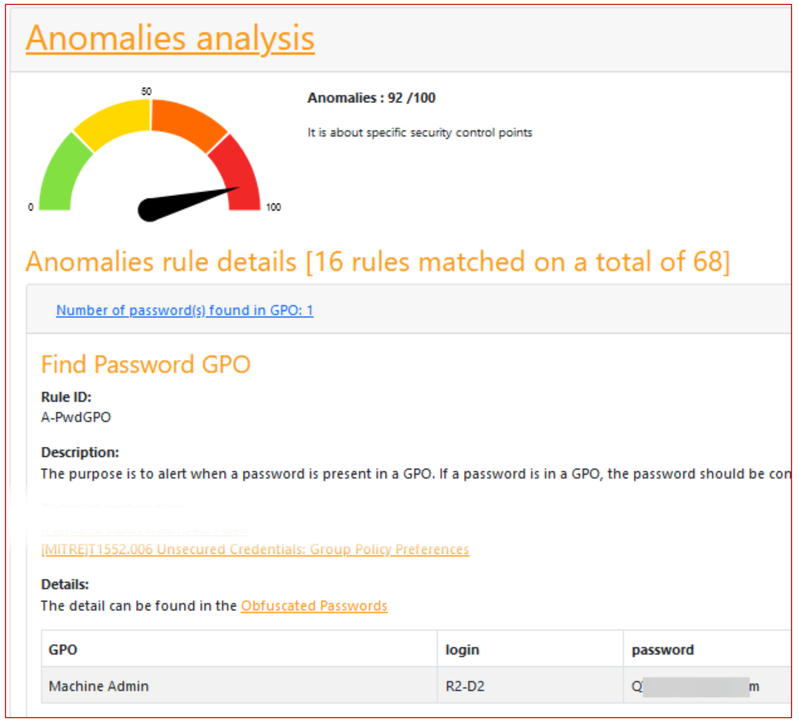


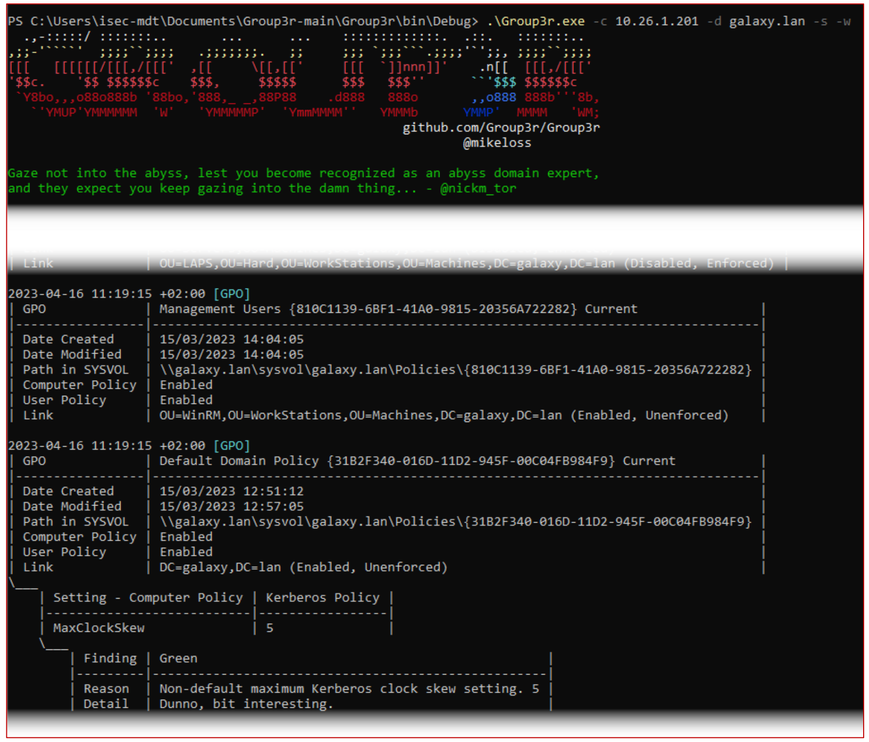
INTRINSEC

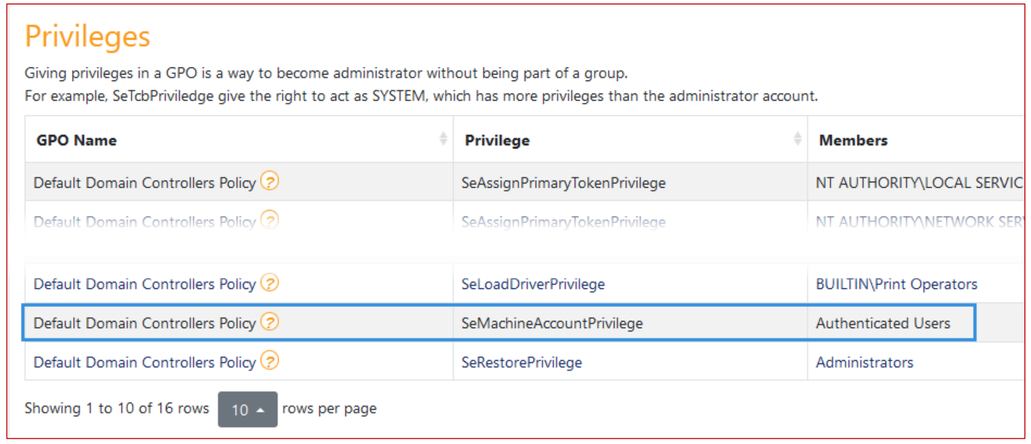
Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – GPO

- Group Policy Object
  - Mots de passe, cpassword
  - Privilèges trop permissifs
  - …
- Outils : Group3r, PingCastle, ADRecon, …

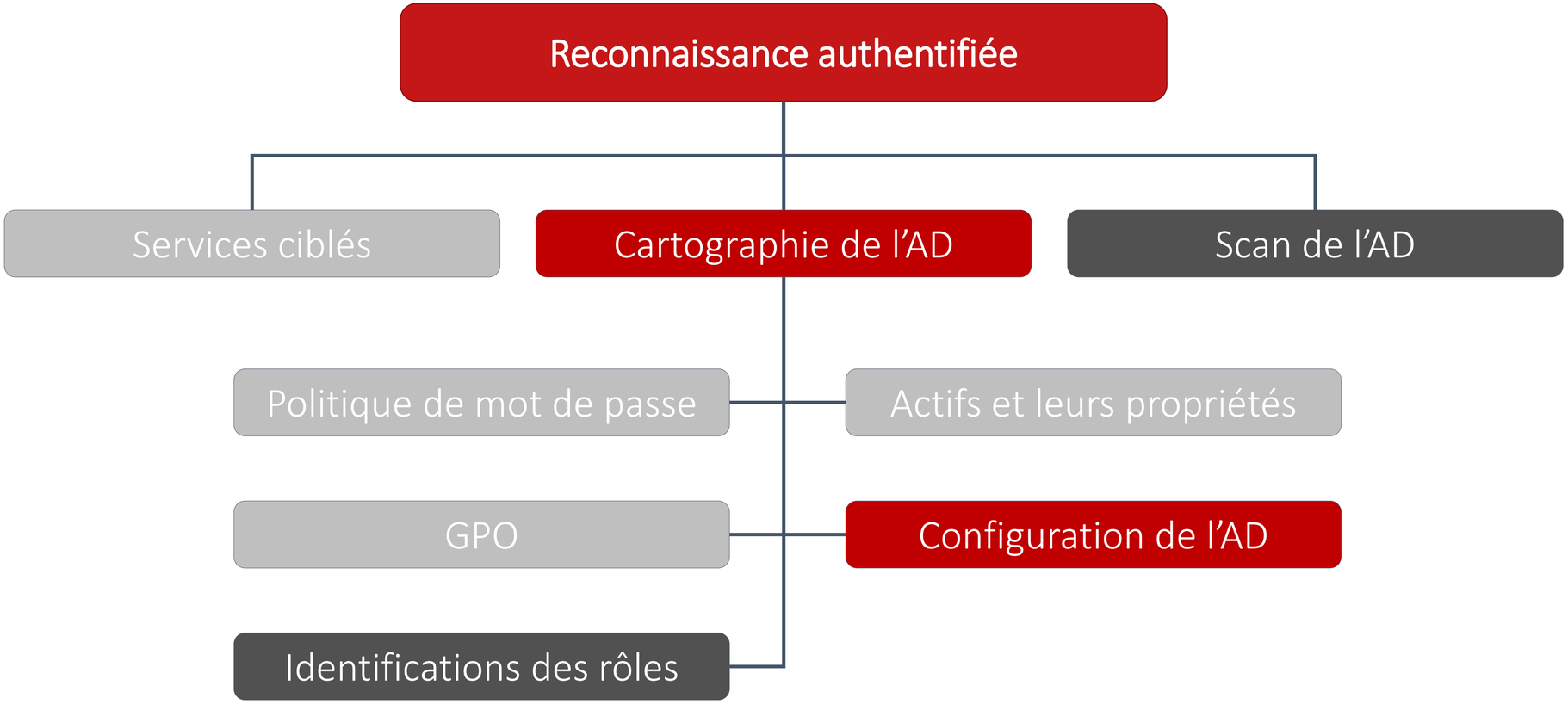






Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



INTRINSEC

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, …

Tier 0

Tier 1

Tier 2

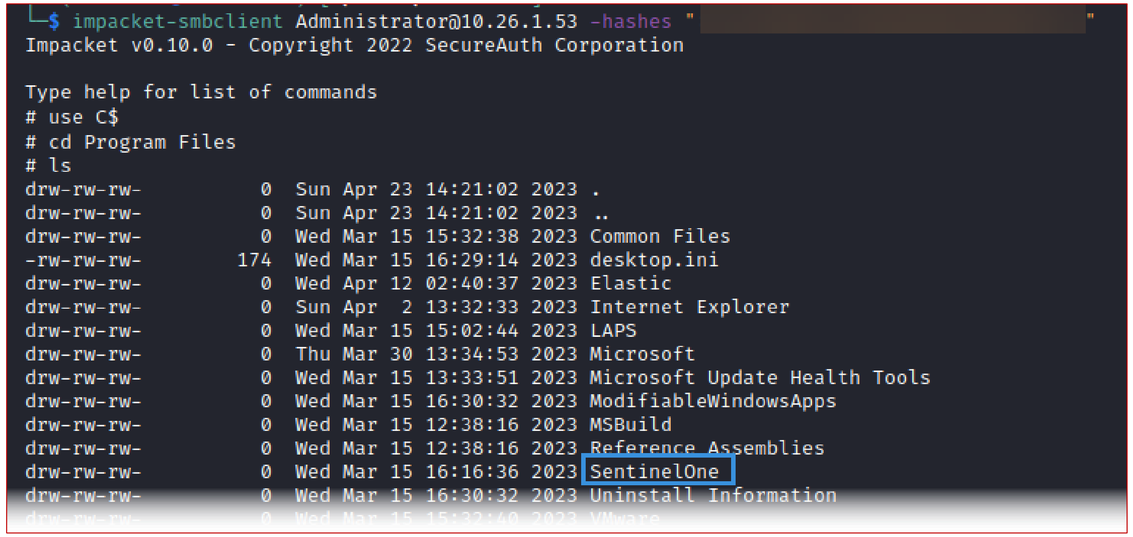
```
└─$ crackmapexec smb 10.26.1.212 -u R5-D4 -p '[redacted]' --loggedon-users
SMB         10.26.1.212     445    GAL-KESSEL       [*] Windows 10.0 Build 17763 x64 (name:GAL-KESSEL)
) (SMBv1:False)
SMB         10.26.1.212     445    GAL-KESSEL       [+] galaxy.lan\R5-D4:P@ssw0rd (Pwn3d!)
SMB        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


INTRINSEC

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
- …



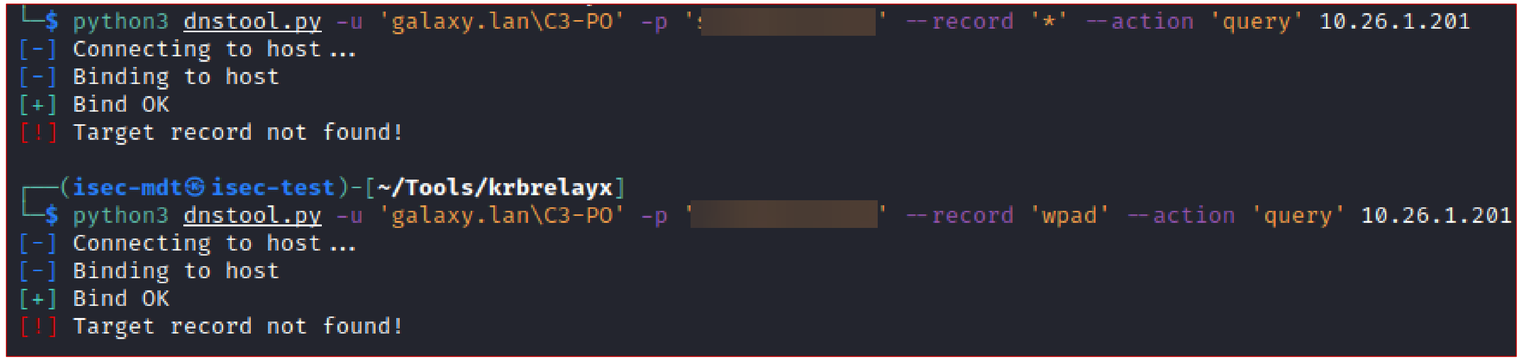
- Outils : BloodHound, PingCastle, ADRecon, krbrelayx, LdapRelayScan, …

INTRINSEC

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, …

INTRINSEC

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 LdapRelayScan.py -method BOTH -u C3-PO -p '[redacted]' -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!
```

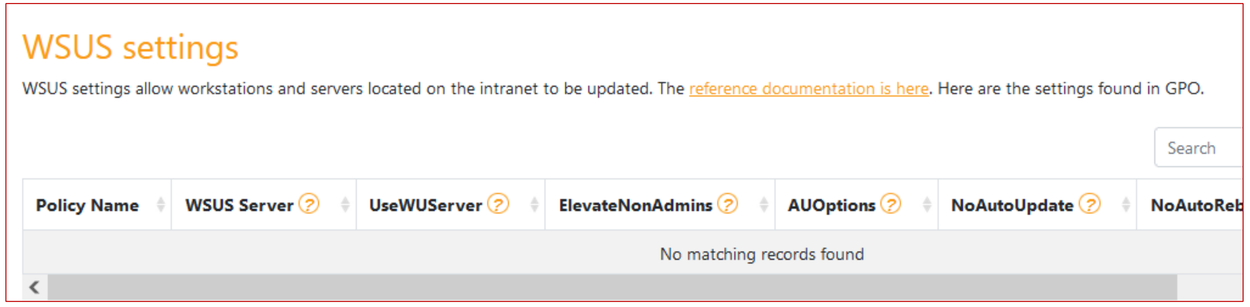
- Outils : BloodHound, PingCastle, ADRecon, krbrelayx, LdapRelayScan, …

INTRINSEC

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
- …

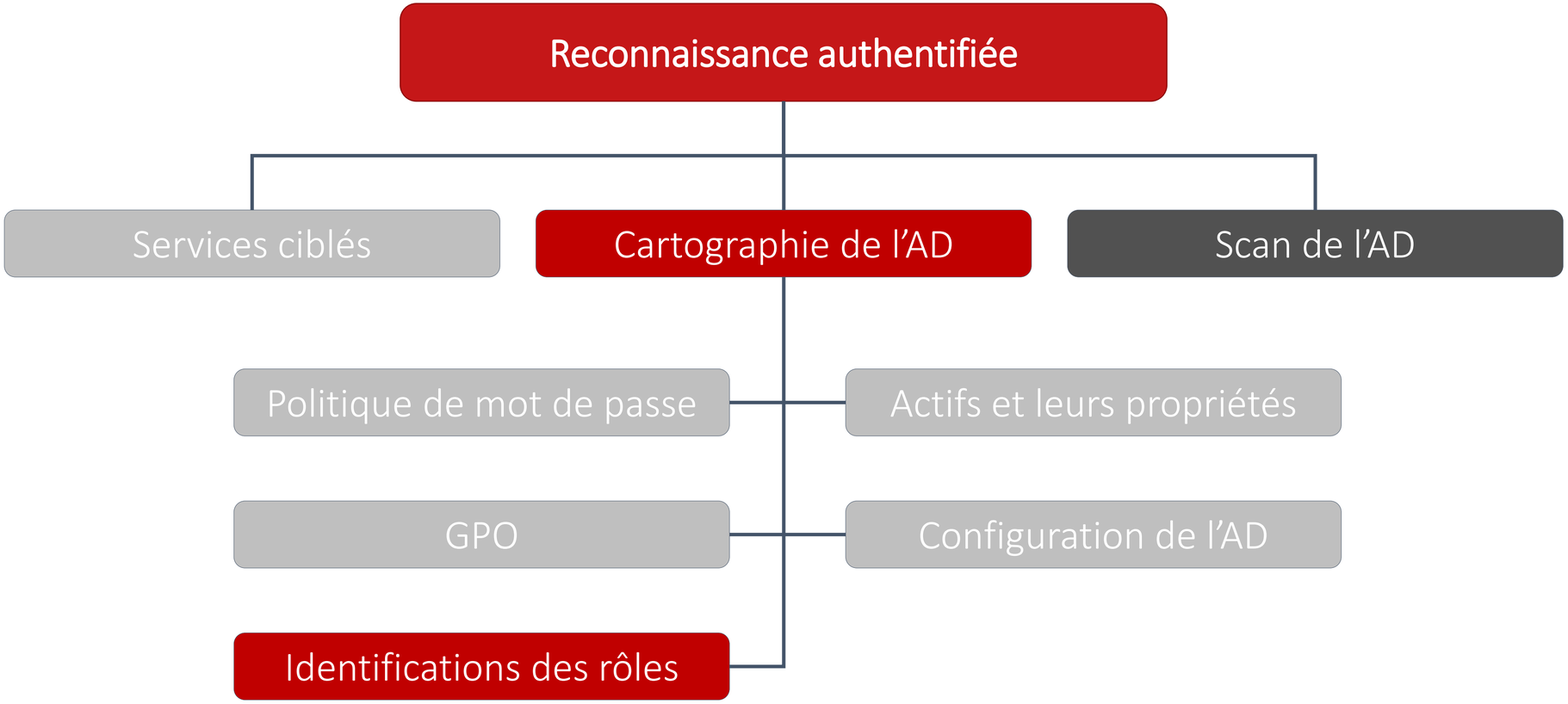


- Outils : BloodHound, PingCastle, ADRecon, krbrelayx, LdapRelayScan, …

INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée



INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Identifications des rôles

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

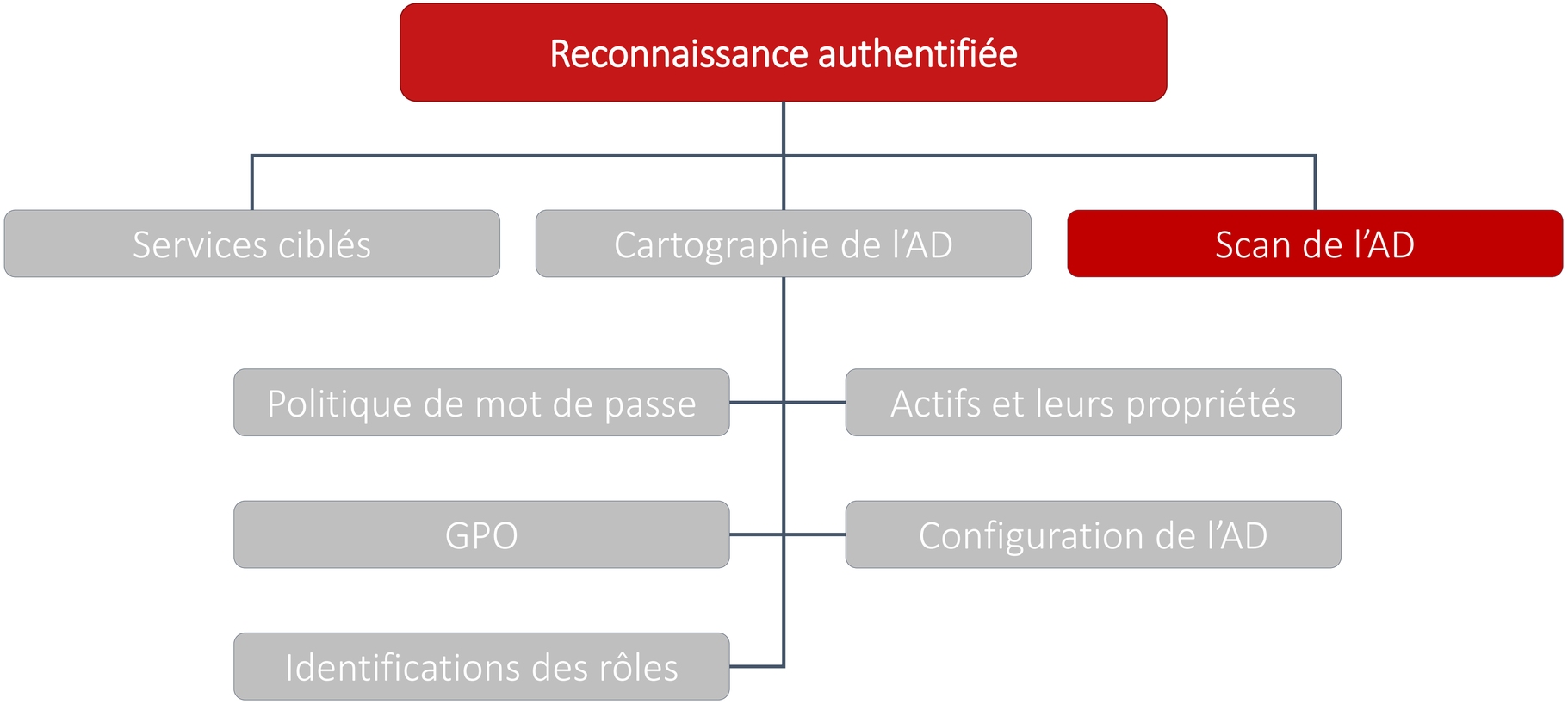
```
PS C:\Users\isec-mdt\Documents> .\Certify.exe find /domain:galaxy.lan /vulnerable

  _____          _   _  __
 / ____|        | | (_)/ _|
| |     ___ _ __| |_ _| |_ _   _
| |    / _ \ '__| __| |  _| | | |
| |___|  __/ |  | |_| | | | |_| |
 \_____\___|_|   \__|_|_|  \__, |
                            __/ |
                           |___./
  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-1-5-21-981138465-619241
    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, Systè
    mspki-certificate-application-policy  : Authentification du client, Messagerie électronique sécurisée, Systè
    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
                                      <UNKNOWN>                    S-1-5-21-981138465-619241437-4107189995-519
        WriteDacl Principals        : <UNKNOWN>                    S-1-5-21-981138465-619241437-4107189995-512
                                      <UNKNOWN>                    S-1-5-21-981138465-619241437-4107189995-519
        WriteProperty Principals    : <UNKNOWN>                    S-1-5-21-981138465-619241437-4107189995-512
                                      <UNKNOWN>                    S-1-5-21-981138465-619241437-4107189995-519
```

```
└─$ certipy find -u C3-PO@galaxy.lan -p 'sTARWARS!@#$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: 0x8
0070005 - 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

                                          GALAXY.LAN\Domain Admins
                                          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
```


INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée

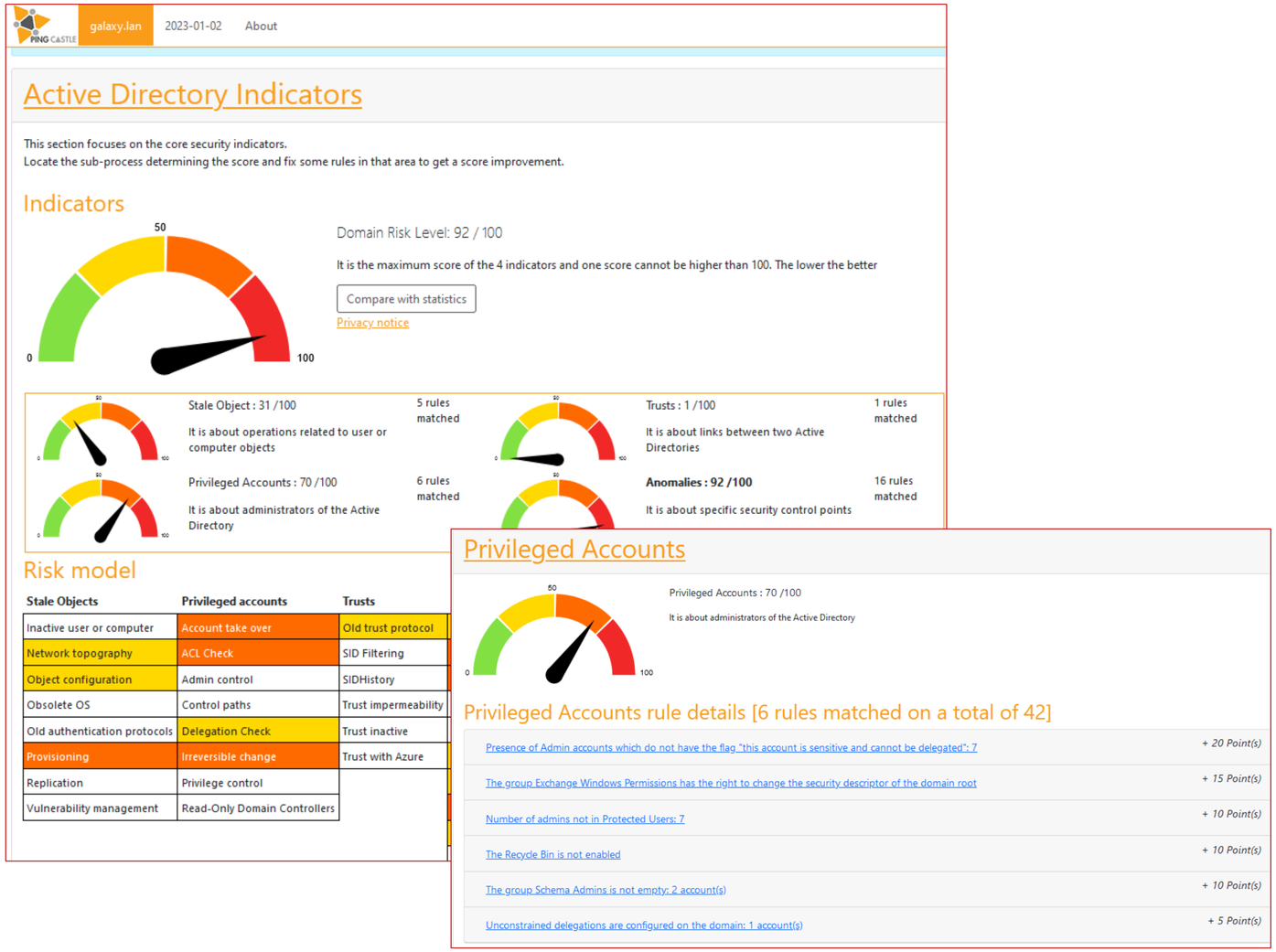


INTRINSEC

Reconnaissance dans un milieu Active Directory

Reconnaissance authentifiée – Scan de l'AD

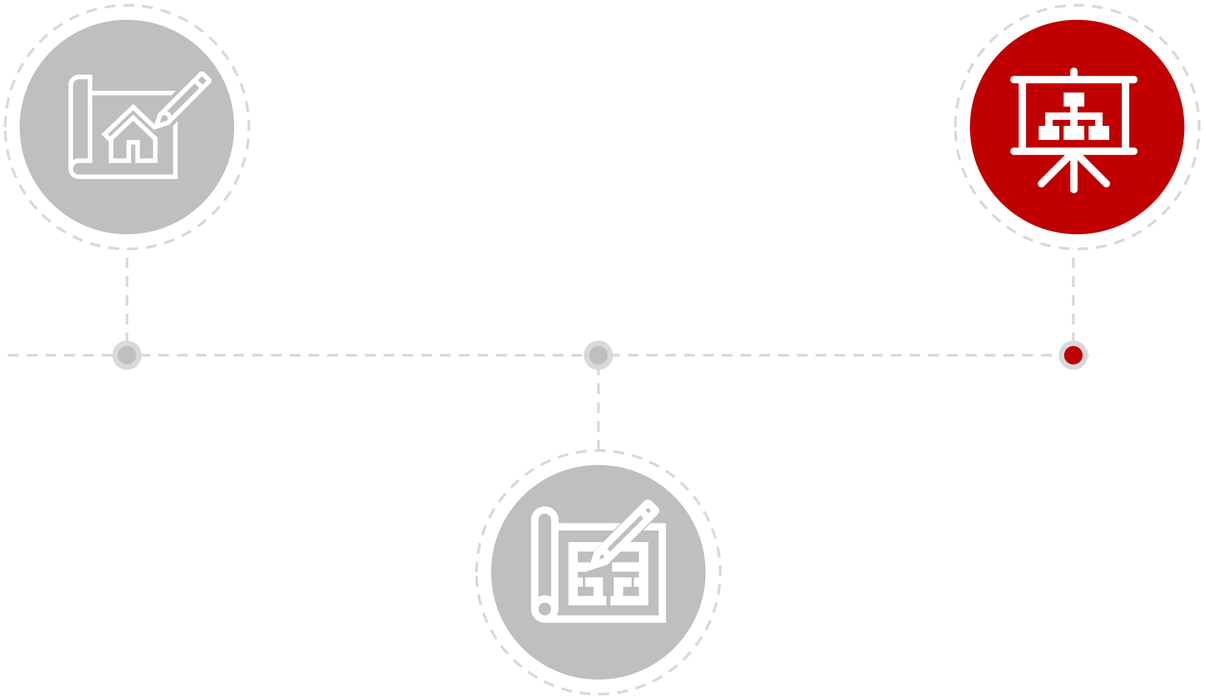
- Relever les différents défauts
  - Privilèges permissifs
  - Configuration
  - …
- Outils : PingCastle, …



Plan

Reconnaissance Anonyme

Conclusion



Introduction

Reconnaissance Authentifiée

INTRINSEC

Reconnaissance dans un milieu Active Directory

- *In the end, it matters …*