Systèmes Windows

- Plan
  - Objectifs
  - Quelques notions
  - Cartographie
  - Récupération d’informations à distance
  - Récupération d’informations locales
  - Authentification sous Windows
  - Elévation de privilèges

objectifs

Objectifs

- Prise de contrôle d'une machine ou d'un domaine
- Techniques ?
  - Élévation des privilèges
- Vers les privilèges d'administration locale
  - Sur une machine isolée : poste client ou serveur
- Vers les privilèges d'administration du domaine
  - Sur un contrôleur de domaine

Techniques

- Découvrir le mot de passe d'un administrateur
- Obtenir l'empreinte d'un compte privilégié
- Exploiter une vulnérabilité pour obtenir un accès privilégié
  - Par exemple, une invite de commande exécutée avec les droits d'un administrateur ou de l'identité LOCAL SYSTEM
- Créer un compte et l'ajouter au groupe des administrateurs locaux ou du domaine

Quelques notions

Histoire de Windows

- Préhistoire
  - MS-DOS, Windows 3.1, Windows 95/98/Me
- Famille NT : Branche maintenue
  - 1 ère génération : Windows NT4 SP6a, Windows 2K SP4
  - 2nd génération : Windows XP SP3, Windows 2003 SP2
  - 3éme génération : Windows Vista / Seven / Huit SP1, server 2008 R2
  - 4éme génération : Windows 10, serveur 2012
- Autres :
  - Windows CE
  - Windows Embedded
  - Windows Cloud
  - Windows Phone
  - Hyper-V

Modèle de sécurité

- Principaux et SID
  - Entités qui s'authentifient auprès du système
  - Utilisateurs, machines, processus…
- Groupes
  - Groupes de principaux, groupes soit locaux au système, soit globaux (domaine)
- Domaine
  - Espace de confiance géré par un/des contrôleur(s) de domaine, prenant en charge les demandes d’authentification et de distribution de configurations
- Relations de confiance
  - Relations entre systèmes et contrôleurs, entre domaines

Notion de SID

(Security Identifier)

- Un SID est une valeur numérique de longueur variable constituée
  - `S-V-I-XXX-XXX-XXX`
    - `S` = La chaîne de caractères est un SID
    - `V` = numéro de version du format (1)
    - `I` = entier identifiant la source du SID
    - `XXX-XXX`... chaîne de longueur variable de sous-autorités ou d'identifiants relatifs (RID)

- Exemple SID d'un Administrateur :
  - `S-1-5-21-7623811015-3361044348-030300820-500`
  - `5` = SECURITY_NT_AUTHORITY
  - `21` = sous-autorité
  - `7623811015-3361044348-030300820` = identifiant de l'ordinateur ou du domaine
  - 500 = RID (Relative Identifiers) de l'administrateur
    - > 500 et < 1000 : builtin; > 1000 : users ou groupes non natifs;
      500 = administrateur ; 501 = guest

Notion de SID

(Security Identifier)

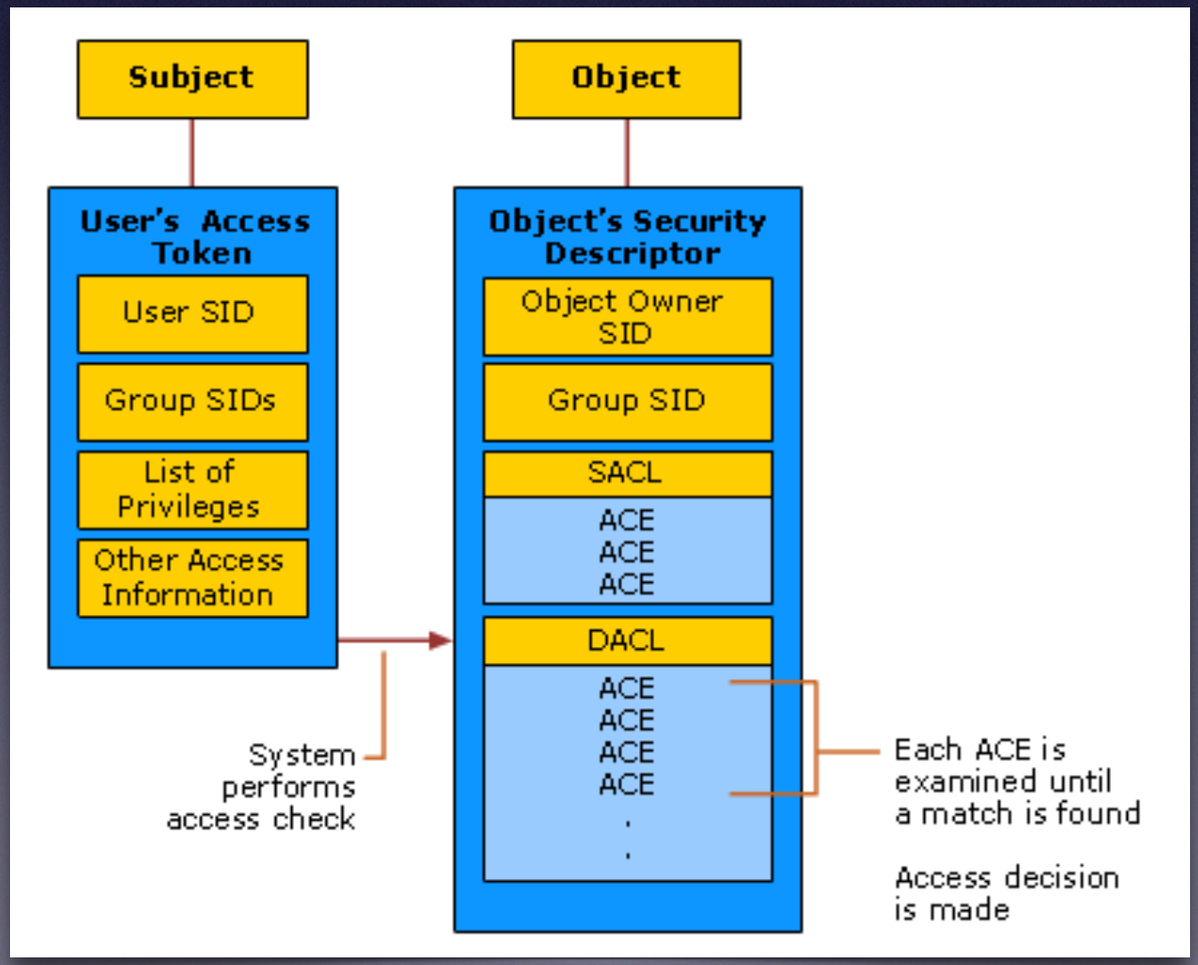
- Pour visualiser les SIDs
  - `psgetsid.exe`
    - http://www.microsoft.com/sysinternals
  - `wmic useraccount get name,sid`

```
Name                SID
Administrateur      S-1-5-21-1343024091-842925246-839522115-500
ASPNET              S-1-5-21-1343024091-842925246-839522115-1004
BvSsh_VirtualUsers  S-1-5-21-1343024091-842925246-839522115-1005
HelpAssistant       S-1-5-21-1343024091-842925246-839522115-1000
Invité              S-1-5-21-1343024091-842925246-839522115-501
john                S-1-5-21-1343024091-842925246-839522115-1003
SUPPORT_388945a0    S-1-5-21-1343024091-842925246-839522115-1002
```

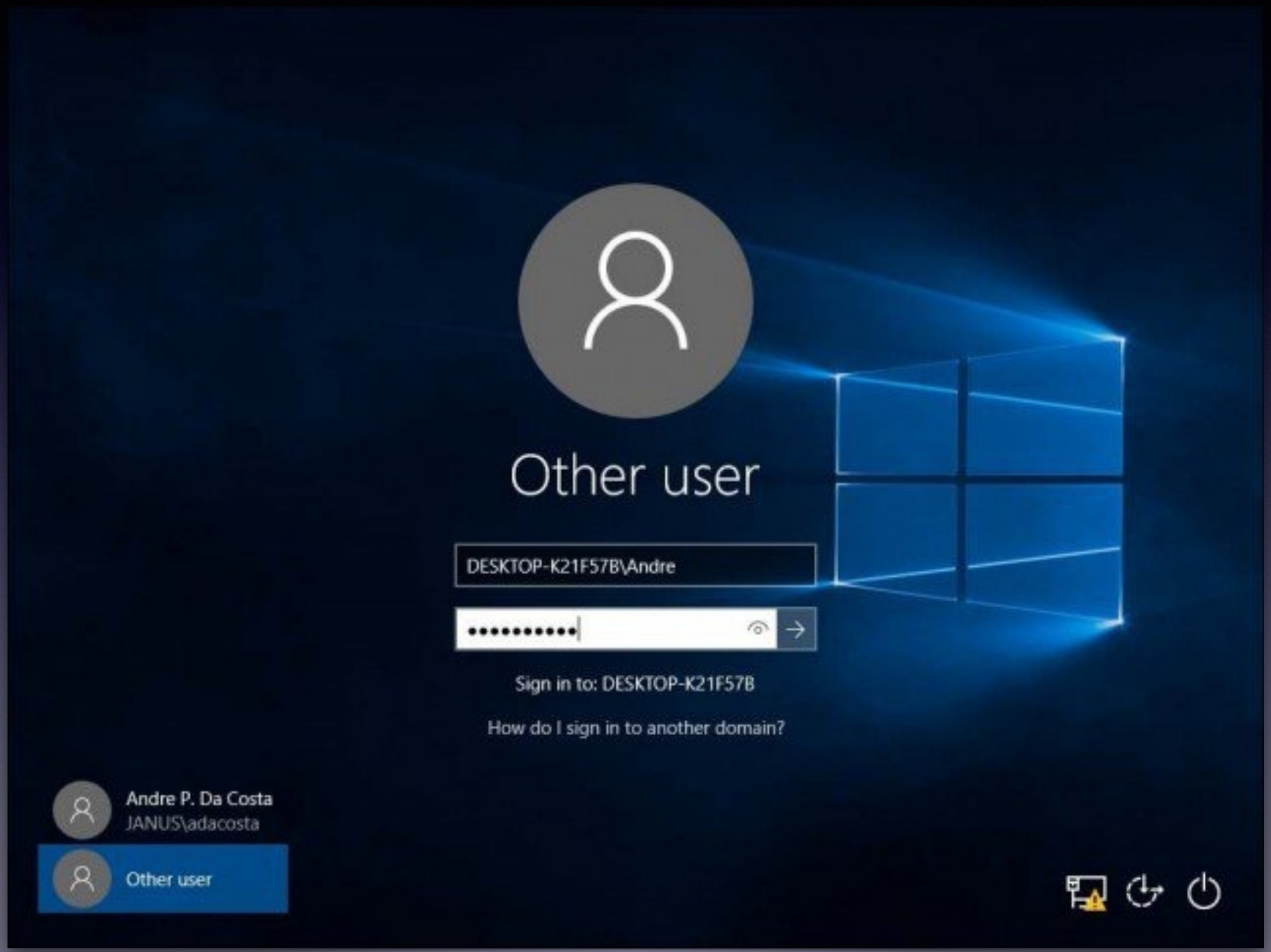
- Les “well known” : communs à tous les systèmes
  - S-1-3-0 : creator owner
  - S-1-5-10 : self
  - S-1-5-21 : domain user
  - S-1-5-18 : local system account
  - S-1-5-19 : NT authority : local service

Jetons d’accès

- Lorsque un utilisateur a été authentifié au sein de sa session, il se voit remettre un jeton d’accès (token) ;
- Ce jeton est utilisé pour toute la durée de la session ;
- Il est utilisé pour représenter l’utilisateur dans toutes les demandes d’accès aux ressources du système.



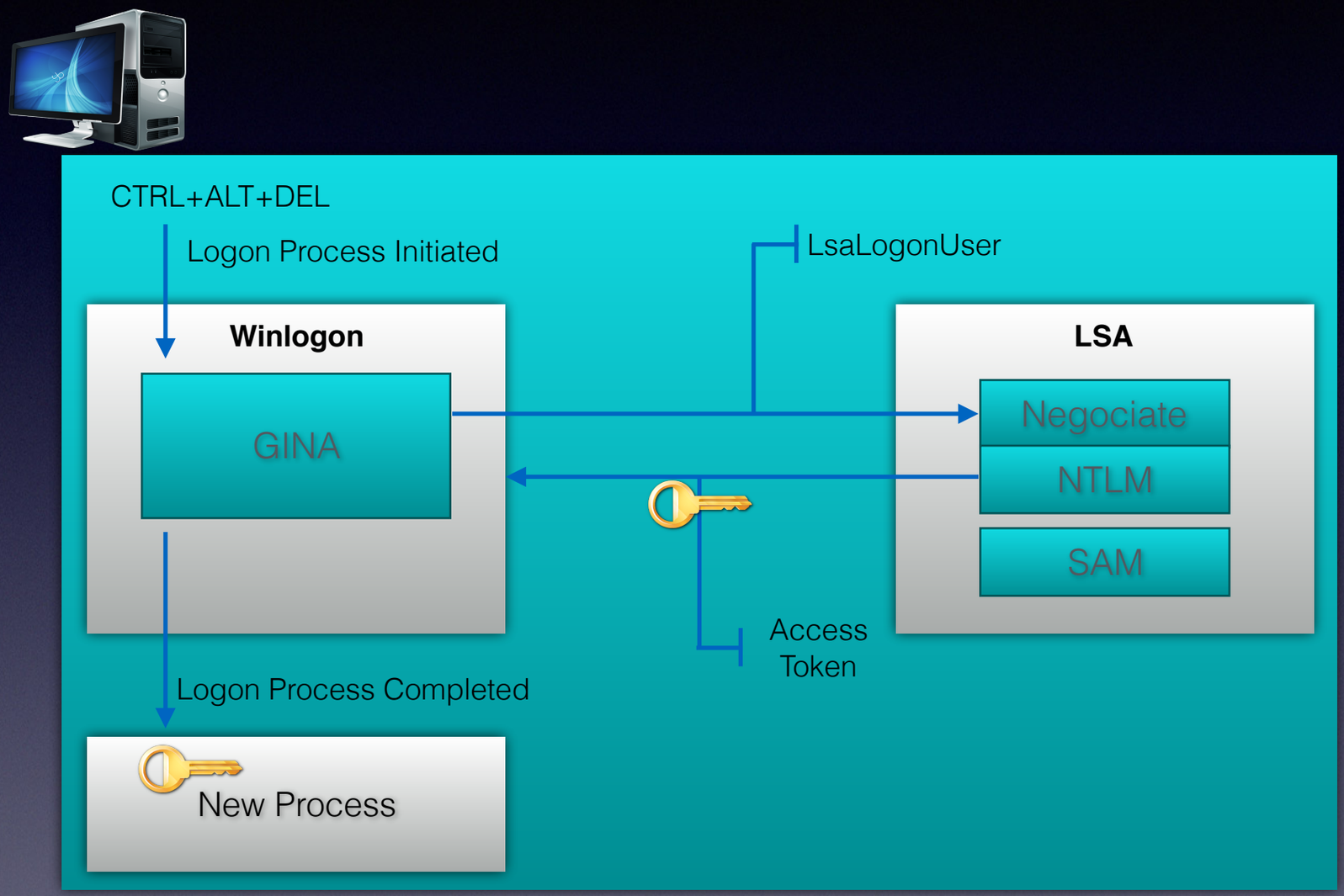
Authentification locale



Authentification locale

- Base d'authentification des utilisateurs locaux = SAM
- Service de sécurité local = LSA (Local Security Authority)
  - Service permettant d'authentifier et d'enregistrer les utilisateurs sur le système local.

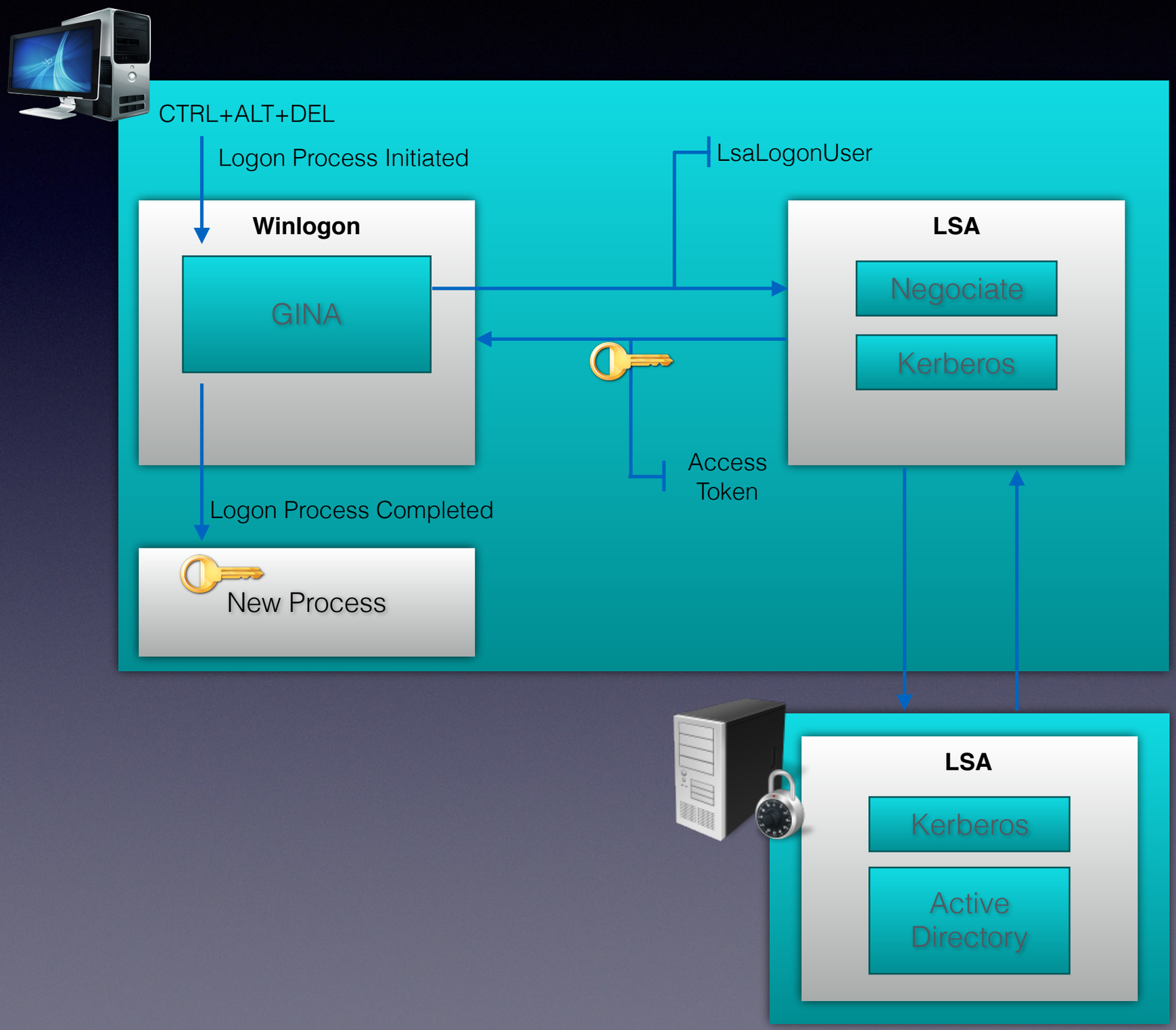
Authentification locale



Base SAM

- Fichier binaire localisé dans %WINDIR% \system32\config
  - Dans le même répertoire que les ruches SYSTEM et SOFTWARE de la base des registres
    - Copie de secours sous forme compressée SAM._ dans le même répertoire
- Contient comptes locaux et mots de passe sous forme hashée
- Récupération du contenu de la SAM intéressant pour cassage des mots de passe

Authentification locale



Authentification locale à un système

- Les mots de passes sont stockés sous forme d'emprunte (SAM ou Active Directory)
- LM : `2 * 7 caractères + Uppercase + DES`
- NTLM : `14 caractères MD4`

Authentification à distance

- Via la mise en œuvre d'un protocole d'authentification
  - Clair
  - Défi / réponse
    - Protocole historique, basé sur le condensat LM :
      - LM
    - Nouveaux protocoles, basés sur le condensat NTLM :
      - NTLM
      - NTLM2
      - NTLMv2

Mécanisme des domaines

- Réseaux Windows organisés en domaines de confiances
- Deux types de domaines, avec fonctionnalités et protocoles propres :
  - Domaines NT4 (historiques)
  - Organisations Active Directory (AD, versions récentes)
- Services de base : gestion d’objets et authentification des utilisateurs

Domaines NT4

- Domaine de confiance pour authentification auprès de contrôleurs
- Deux types de contrôleurs :
  - PDC (Primary Domain Controler)
  - BDC (Backup Domain Controler)
- Synchronisation des deux effectuée manuellement ou automatiquement
- Protocoles des domaines NT4
  - Protocoles propriétaires Microsoft
    - SMB / CIFS
    - MSRPC
  - Authentification LM ou NTLM réseau

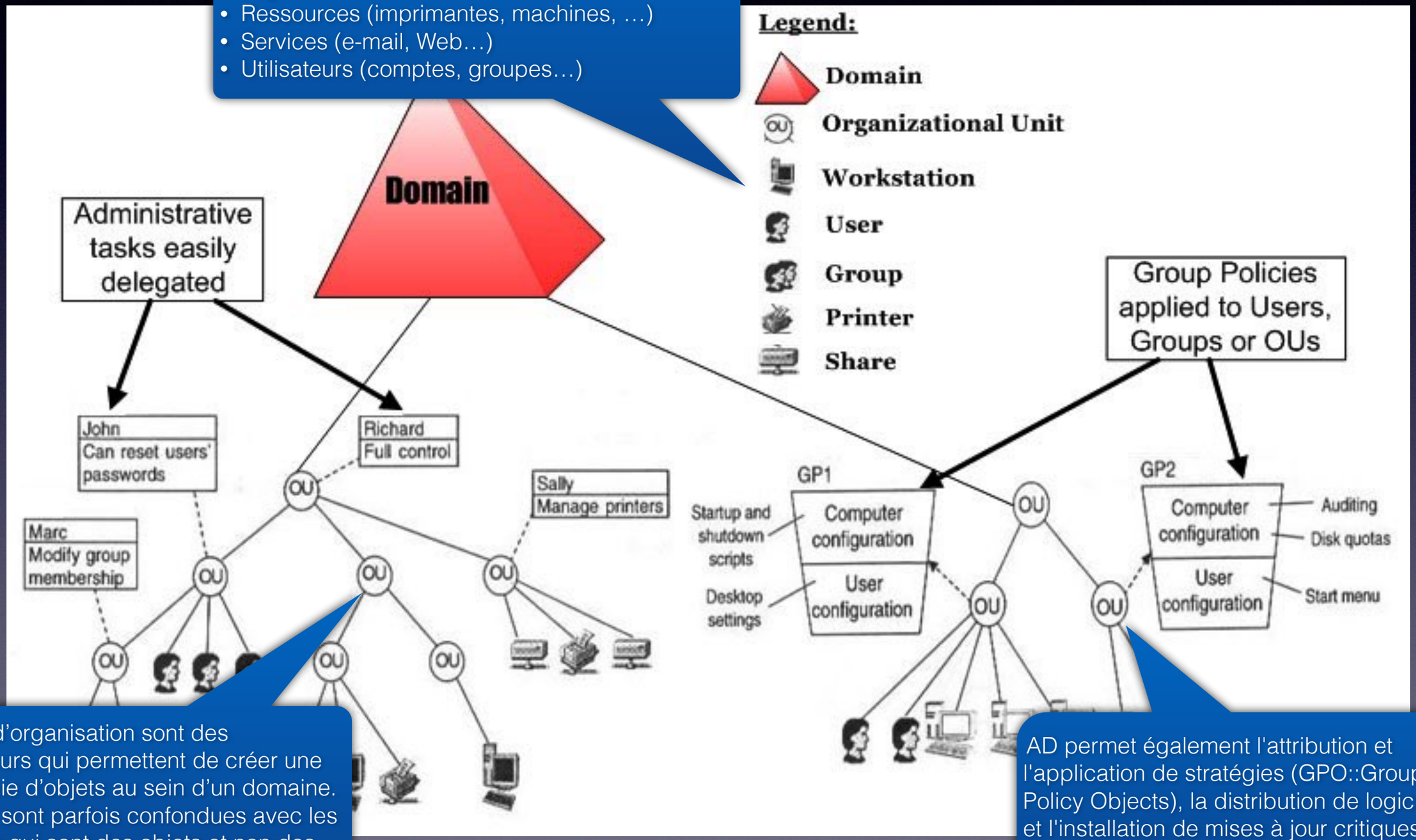
Protocoles d'Active Directory

- AD s'appuie sur des standards Internet
  - DNS
  - Kerberos
  - LDAP
  - NTP
- AD utilise massivement DNS, qui est obligatoire
- AD permet une granularité très importante des rôles et privilèges

Quelques notions sur le domaine

L'AD est une organisation hiérarchisée d'objets. Les objets sont classés en trois grandes catégories

- Ressources (imprimantes, machines, …)
- Services (e-mail, Web…)
- Utilisateurs (comptes, groupes…)



L'unité d'organisation sont des conteneurs qui permettent de créer une hiérarchie d'objets au sein d'un domaine. Les OU sont parfois confondues avec les groupes qui sont des objets et non des conteneurs.

AD permet également l'attribution et l'application de stratégies (GPO::Group Policy Objects), la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs.

Cartographie

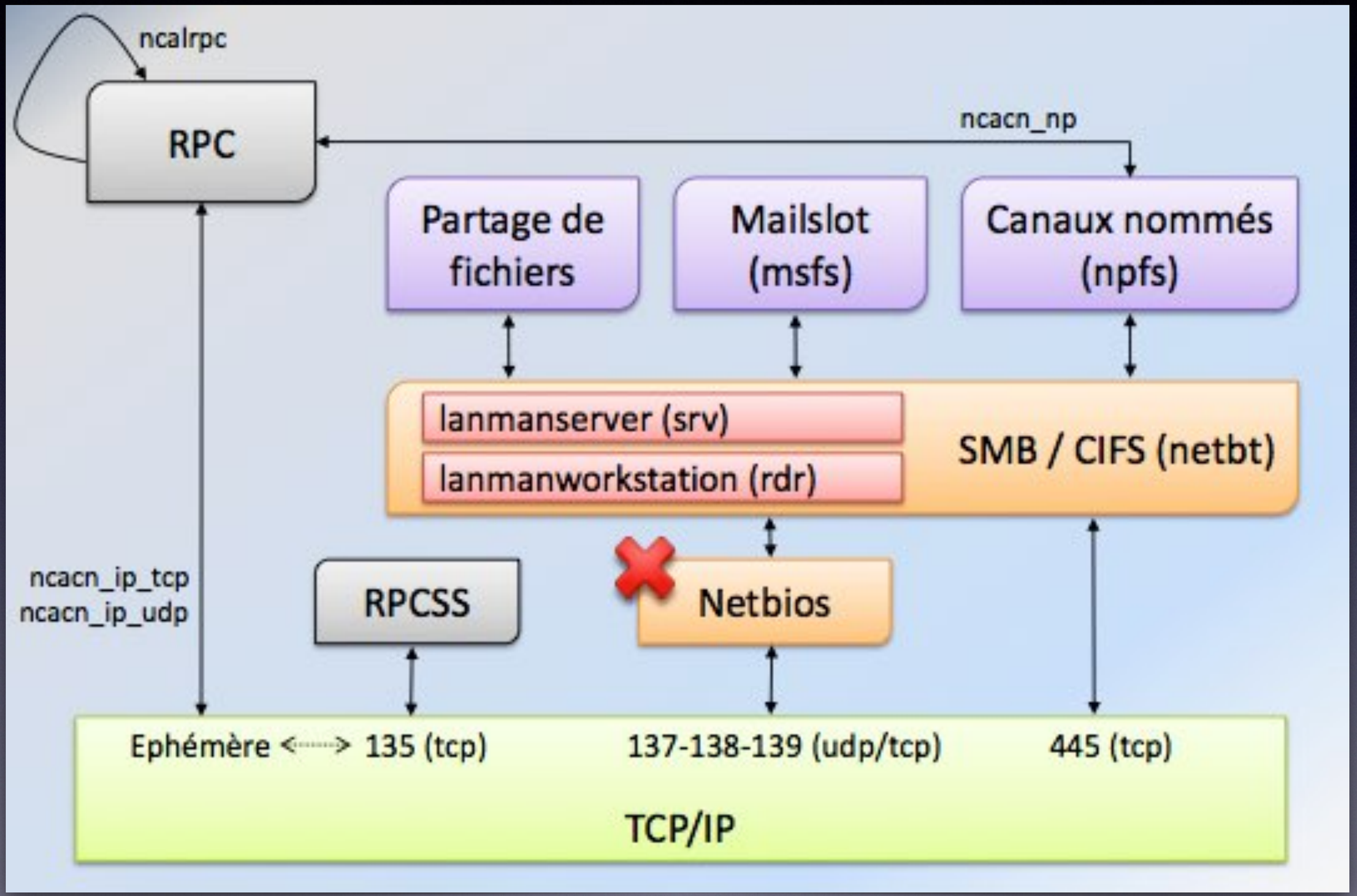
Par quelle machine commencer ?

- Identification des machines intéressantes
  - nmap (éventuellement hping) et metasploit
- Quelles sont-elles ?
  - Les contrôleurs de domaine
  - Les serveurs d'application
  - Les postes clients
- Nécessité d'effectuer une classification des machines découvertes
- La source d'information principale
  - Les services en écoute sur le réseau

Protocoles réseaux natifs Windows

- NBT
  - Encapsulation de Netbios sur TCP/IP
- SMB / CIFS (Partage de fichiers)
- MS RPC (Communication interprocess)
  - Protocole d’appel de fonctions et d’échange de données entre processus locaux ou distants

Les services Windows en écoute



Identification des services en écoute

- Services en écoute caractéristiques des machines Windows
  - Portmapper MS-RPC - `135/TCP`
    - Service Location : Service permettant la réalisation des appels de procédures distantes
  - Service de noms NETBIOS – `137/UDP`
    - NetBios Name Service : Utilisé pour enregistrer les noms NetBios dans la base Wins.
  - Service de transport NETBIOS sur UDP - `138/UDP`
    - NetBios Datagram Service : Utilisé par le service explorateur réseau (SMB browser service)
  - Service de transport NETBIOS sur TCP - `139/TCP`
    - NetBios Session Service : Utilisé pour accéder aux ressources réseaux (partages de fichiers et d'imprimantes)
  - Service SMB/CIFS – `445/TCP`
    - Microsoft DS : Protocole SMB (Server Message Block) est utilisé entre autres pour le partage de fichiers dans Windows. Détaché de NetBios depuis Windows 2K/XP.
  - Service Terminal Server – `3389/TCP`

Identification des services en écoute

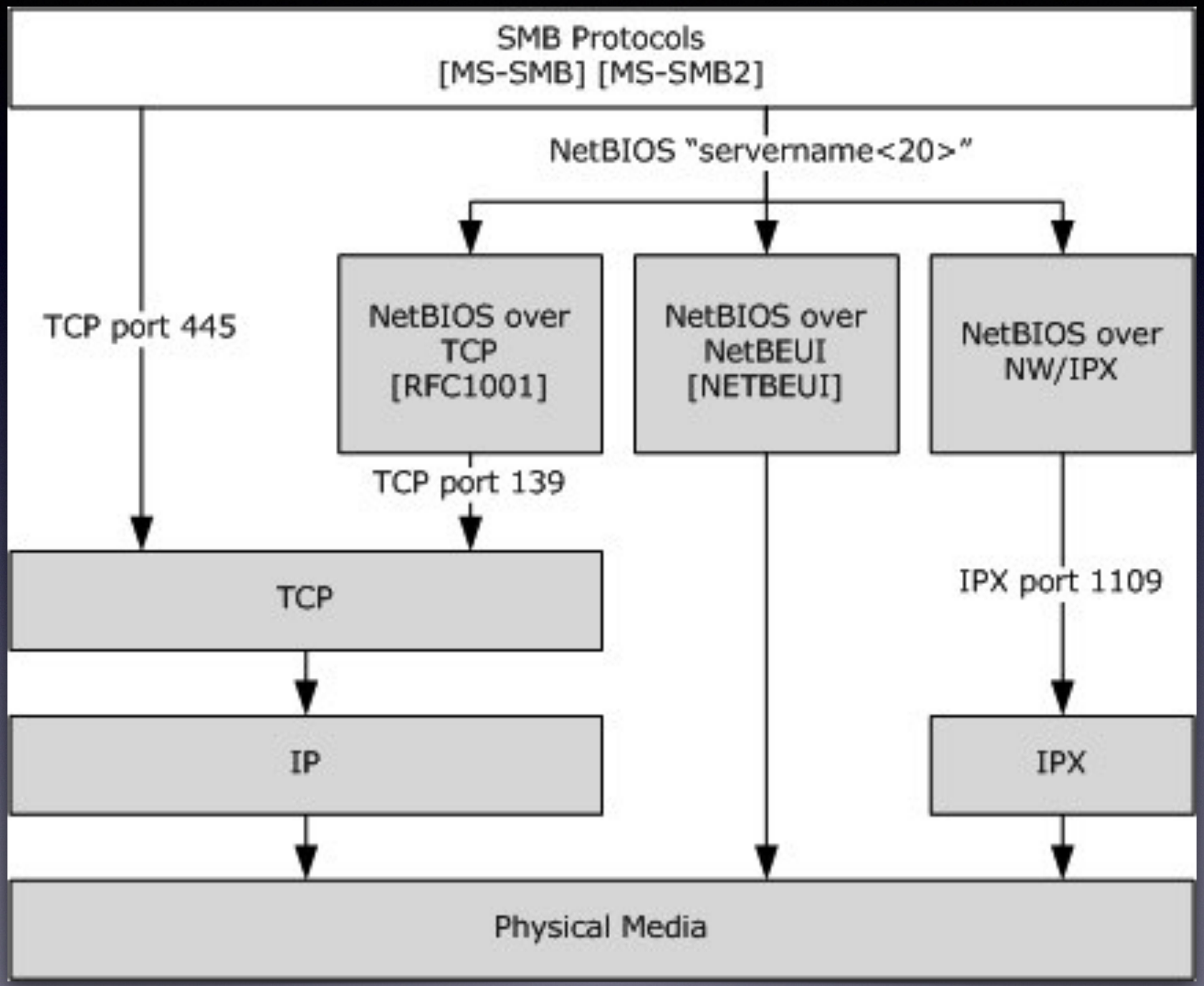
- Services classiques hébergés par des serveurs Windows
  - Serveur WINS – `42/TCP`
  - Serveur DNS – `53/UDP`
  - Serveur HTTP – `80/TCP et/ou 81/TCP`
  - Serveur HTTPS – `443/TCP`
  - Mandataire HTTP – `8080/TCP`
  - KDC Kerberos – `88/UDP`
  - Serveur LDAP – `389/TCP (et LDAPSSL - 636/TCP)`
  - Serveur RDP – `3389/TCP`
  - Serveur VNC – `5900/TCP`
- `88/UDP et 389/TCP` == AD DS (contrôleur de domaine)

Récupération d’informations à distance

Sessions nulles

- Principe, déroulement et tubes nommés
  - Possibilité de connexion sans login/password
    - utilisées lorsqu'une machine cherche à accéder aux informations d'une autre machine sans faire partie de son domaine ou de son groupe de travail.
  - Transport sur SMB
    - Port `139/TCP` (via `TCP sur NetBIOS`)
    - Port `445/TCP` (directement en TCP)
- Accès et configuration
  - Récupération des comptes, groupes, partages …
- Outils
  - `Cain, rpcclient`
- L’accès anonyme aux tubes nommés est interdit depuis Windows XP SP2 et 2003

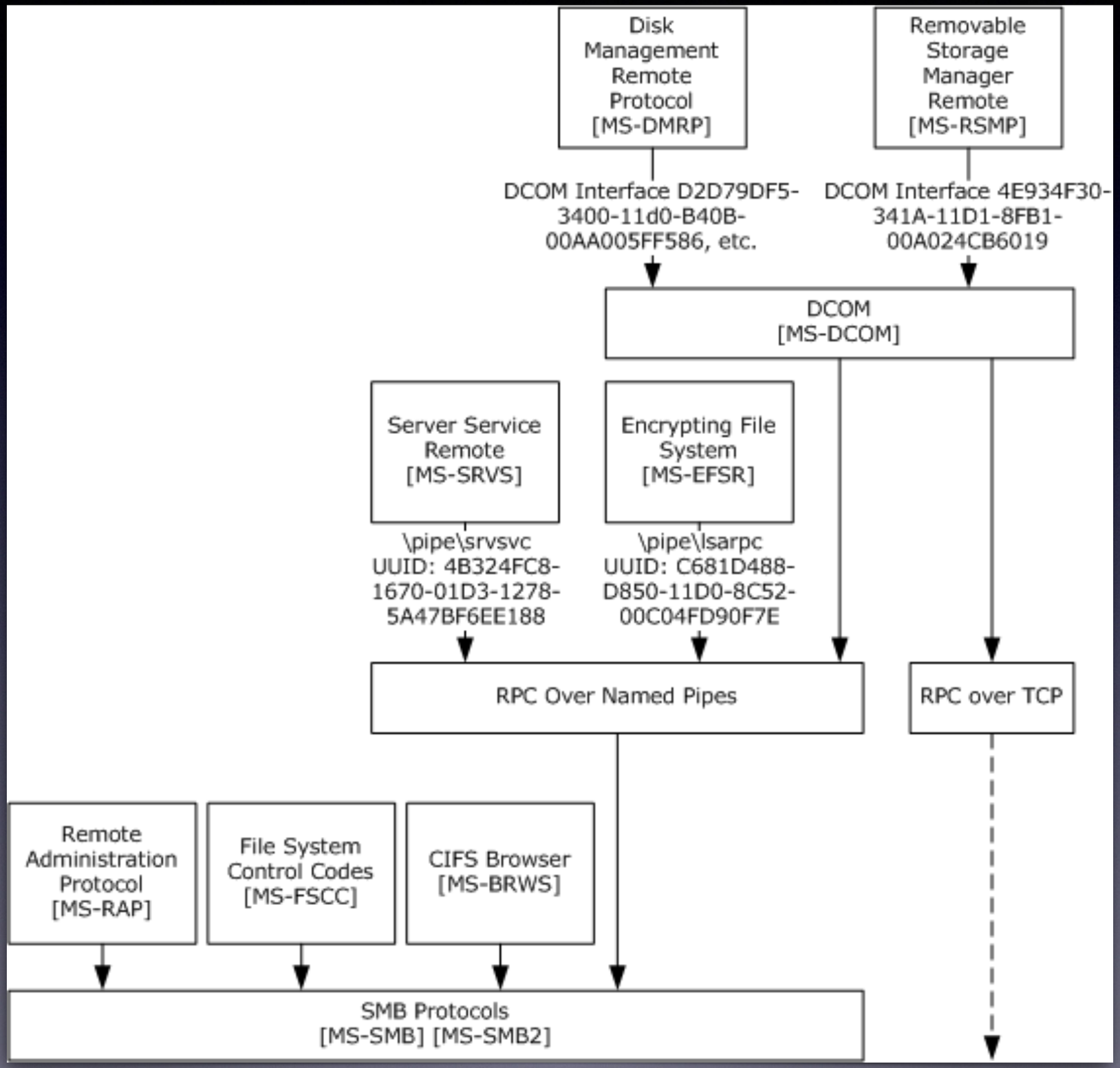
Sessions SMB



Sessions nulles

- Connexion TCP au port 445 ou 139
- Etablissement d'une session SMB avec identifiant et mot de passe vides
  - Seule étape d'authentification
- Connexion au partage `IPC$`
- Ouverture d'un tube nommé
- Association à une interface `RPC`
- Chaque interface `RPC(remote procedure call)` est identifiée par un identifiant (`UUID`) `(Universal Unique Identifier)`
- Lancement de requêtes `RPC`

Association à une interface RPC



Accès authentifié

- Objectifs
  - Récupérer des informations fournies par des interfaces Windows avec un compte légitime du domaine
- Les informations à récupérer
  - Liste des sites, réseaux…
  - Liste des utilisateurs du domaine
  - Appartenance des utilisateurs aux groupes privilégiés
  - …
- Outils d'administration
  - `rpcclient`
  - `Cain & Abel`
  - `Clients WMI`
    - WMI offre un mécanisme de gestion à distance d'un système d'exploitation ou des composants installés
      - `Wmic /node:[TargetIPaddr] /user:[User] /password:[Passwd] process list full`
    - `wbemtest`
  - `Dsquery` (cible l'annuaire Active Directory)

Partage réseau : principes

- Partages de fichiers
- Transport sur TCP via le protocole SMB (445/TCP)
- Authentification
  - Utilise les protocoles d'authentification classiques disponibles sous Windows et sélectionnées par le `SSP Negociate`
    - NTLM ou Kerberos, le plus souvent
- Outils
  - Pour lister les partages SMB
    - `rpcclient` et la commande `netshareenum`
    - `rpcclient-tng` et la commande `share list`
  - `smbclient` pour y accéder
    - `%smbclient -U <identifiant> \\\\<cible>\\<partage>`

Exécution de code à distance

1. Service Control Manager (SCM)

ex. : `sc REMOTECOMPUTERNAME create myservicename binPath= executableToRun start= auto`

Writing to the svcctl named pipe (a.k.a. srvsvc) on remote computer over SMB. (TCP port 139 or 445 owned by kernel, forwarded to srvsvc pipe). srvsvc pipe hosted by Server service in `svchost.exe` running as `SYSTEM`.

2. Task scheduler

Ex. : `AT \\REMOTECOMPUTERNAME 12:34 "command to run"`

Writing to atsvc named pipe on remote computer over SMB. (TCP port 139 or 445 owned by kernel, forwarded to atsvc pipe). atsvc pipe hosted by Task Scheduler (Schedule) service in `svchost.exe` running as `SYSTEM`.

3. WMI

Ex. : `WMIC /node:REMOTECOMPUTERNAME PROCESS call create "command to run"`

Connecting to remote procedure call interface (RpcSs service in `svchost.exe` directly listening on `TCP port 135`)

4. Remote Registry

Ex. : `REG ADD \\REMOTECOMPUTERNAME\HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v myentry /t REG_SZ /d "command to run"`

Writing to the winreg named pipe on remote computer over SMB. (TCP port 139 or 445 owned by kernel, forwarded to winreg pipe). The winreg pipe is hosted by Remote Registry service in `svchost.exe`

Exécution de code à distance

5. Remote File Access

Ex. :`xcopy executabletorun.exe "\\REMOTECOMPUTERNAME\C$\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\e.exe"`

Writing to remote administrative shares using SMB. (`TCP port 139 or 445` owned by kernel)

6. Remote Desktop

Ex. : `rdesktop 1.2.3.4`

Hosted by the TermService service (“Remote Desktop Services”) in `svchost.exe` by a server socket listening on `TCP port 3389`.

7. Windows Remote Management

Ex. : `winrs -r:REMOTECOMPUTERNAME` command to run

Hosted by Windows Remote Management service (`svchost.exe`), listens on `TCP/80 or TCP/5985` and can share port with `IIS`

Récupération d'informations locales

Récupération d'informations locales

- Si un poste client est accessible ou rendu accessible …
- Les informations à récupérer
  - Liste des utilisateurs locaux
  - Appartenance des utilisateurs aux groupes privilégiés
  - Appartenance de la machine à un domaine
  - Liste des applications installées
  - Droits sur les fichiers locaux
  - Cache netbios
  - Liste des derniers documents ouverts
  - Liste des process et services actifs
  - Si possible extraits des registres

Informations sur les comptes

- Première étape de l'attaque sur les moyens d'authentification
- Lister les utilisateurs
  - `net user; net user /domain`
- Obtenir des informations individuelles sur les utilisateurs
  - `net user <login_utilisateur>`
- Lister les groupes locaux
  - `net localgroup`
- Lister les groupes du domaine
  - `net group`
- Identifier les membres d'un groupe
  - `net localgroup <nom_du_groupe>` ou `net group <nom_du_groupe>`

Manipulation des comptes

- Après avoir obtenu des droits élevés
- Il est possible de
  - Créer un utilisateur
    - `c:\> net user <login utilisateur> /add`
  - Ajouter un utilisateur dans un groupe
    - Pour le domaine local
      - `c:\net localgroup <nom_du_group> <login_utilisateur> /add`
    - Dans le domaine AD DS
      - `c:\net group <nom_du_group> <login_utilisateur> /add`

Informations d'environnement

- Lister les informations d'environnement
  - La commande `set` affiche :
    - Le nom de l'utilisateur connecté : `USERNAME`
    - Le nom de la machine : `COMPUTERNAME`
    - Le nom du domaine : `USERNAME`
- Les partages réseaux: `net use`
- Configuration des interfaces réseaux
  - `ipconfig /all`
- Voisinage réseau
  - `net view`

Le service de noms NETBIOS

- Service utilisé par défaut en environnement Windows
- Permet l'identification des machines
- Utilise le port `137/UDP`
- Fournit des informations sur le rôle des systèmes

- Outils `nbtstat`
  - `c:\> nbtstat -a <nom_de_la_machine>`
  - `c:\> nbtstat -A <adresse_ip_de_la_machine>`
- Accès au cache Netbios
  - `c:\> nbtstat -c`
- Sous linux, il existe `nbtscan`
  - `$ nbtscan -v <adresse_ip_de_la_machine>`

Le service de noms NETBIOS

- Informations intéressantes obtenues
  - Nom de la machine, Domaine, Utilisateur authentifié
  - Adresse MAC de la machine
  - Certains services démarrés :
    - <00> : service Workstation
    - <03> : service Messenger
    - <20> : service Server
  - Rôle
    - <1C> : Contrôleur de domaine
    - <Inet~Services> : Serveur IIS
    - <22>, <23>, <24>,<87>,<6A> : Serveur Exchange
  - Référence : http://support.microsoft.com/kb/163409

Liste des applications installées

- Objectif : identifier des applications vulnérables
- S'intéresser à la version installée
  - Permettra l'exécution d'exploits locaux

- En mode graphique
  - Ajout/Suppression de programmes
  - `regedit` et afficher la ruche `HKLM\SOFWARE`

- En ligne de commande
  - `c:\> reg query HKLM\SOFTWARE`

Liste des process et services

- Objectif : identifier des processus « hostiles » (pare-feu, antivirus), les services vulnérables, prévoir la pérennisation de l'accès

- En mode graphique
  - Possible mais à éviter si possible

- En ligne de commande
  - `Tasklist (taskkill), sc (cf. aussi schtasks)`

Extraction des registres

- Objectif : extraire les informations utiles en vue du cassage des mots de passe locaux

- En ligne de commande
  - `Reg save HKLM/SECURITY, HKLM/SAM, HKLM/SYSTEM`

Récupération des accréditations

- Récupération locale
  - Des empreintes
    - Dans la base SAM
    - Dans la mémoire
  - Des données d’authentification en cache
  - Des mots de passe dans la mémoire
- Récupération à distance

Récupération locale des empreintes

- Dans la base SAM
- Outils
  - Metasploit
    - meterpreter> run hashdump
  - PwdumpX 1.4
    - c:\> PwdumpX –ph <cible> <identifiant> <mot_de_passe>
    - L'identifiant et le mot de passe peuvent être remplacés par « + + » pour utiliser les accréditations de l'utilisateur qui exécute le programme
  - Fgdump
    - c:\> fgdump –c –h <cible> -u <identifiant> -p <mot_de_passe>
  - Wce (windows credentials editor)
  - Cain
    - Onglet Cracker
    - Clic gauche « Add to list »

Récupération locale des empreintes

- Dans la mémoire
  - Metasploit
    - meterpreter> use incognito
    - meterpreter> list_tokens -u
    - meterpreter> impersonate token <DOMAIN\
      \username>
  - wce
  - PSH Toolkit de Core Security (<Seven et 2K08)
    - whosthere permet de lister les sessions de connexion présentes en mémoire
      - whosthere.exe ou whosthere-alt.exe
  - MSVCTL (<Seven et 2K08)

Récupération locale des données d'authentification

- Les données d'authentification en cache (`mscash`)
- Outils
  - `Metasploit`
    - `meterpreter> run post/windows/gather/cachedump`
  - `PwdumpX 1.4`
    - `c:\> PwdumpX -c <cible> <identifiant> <mot_de_passe>`
  - `Fgdump`
    - `c:\> fgdump -w -h <cible> -u <identifiant> -p <mot_de_passe>`
  - `Cain`
    - Onglet Decoders, LSA Secrets, Bouton « + »
- Anciennement
  - `Cachedump`
  - `Lsadump2 (avant Windows XP et 2003)`
  - `lsadump <PID_de_lsass.exe>`

Récupération locale des mots de passe

- Dans la mémoire
- Outils
  - `Wce`
  - `Mimikatz`
  - `CachedPasswordDumper` (pour Windows XP SP1 et 2003 SP0
    - cpd
  - `PasswordReminder` (avant Windows XP)
  - `FindPass` (avant Windows XP)
    - `c:\ Findpass <nom_de_domaine> <identifiant> <PID_de_winlogon.exe>`
    - Le `PID` peut être obtenu avec `pslist` (`pstools` de systinternals)

Récupération à distance

- Directement par le réseau
- Outils
  - `psexec, meterpreter` et `hasdump`
  - `fgdump` ou `pwdump`
  - `Cain & Abel` (méthode employée sous Windows)
    - Onglet Network
    - Clic droit sur Quick List : Add to Quick List
    - Clic droit sur l'adresse de la machine : Connect As
    - Clic droit sur Services : Install Abel
    - Double clic sur l'adresse de la machine
    - Abel\Hashes
      - L'historique des empreintes est affichée

Authentification sous Windows

Les attaques

Authentification avec des empreintes

- Objectifs
  - Utiliser les empreintes des mots de passe pour s'authentifier sur un server ou un poste de travail sans connaître les mots de passe !
- Techniques
  - Méthode Pass the hash
    - Disposer des empreintes de mot de passe (SAM, mémoire, cache)
    - Accéder à un serveur/service acceptant l'authentification NTLM
- Outils
  - Metasploit :
    - exploit/windows/smb/psexec
  - Pass The Hash Toolkit
    - C:\> iam.exe <identifiant> <domain> <empreinte_LM> <empreinte_NT>
  - Msvctl (<Seven et 2K08)
    - C:\> msvctl <domain>\<user> [lm <lm hash>] [ntlm <ntlm hash>] run <cmd>
  - Wce

Découverte de mots de passe

- Objectifs
  - Découvrir le clair d'une empreinte
  - Identifier des comptes et mots de passe valides
- Techniques
  - Cassage d'empreinte
    - Par dictionnaire
      - Test des mots de passe usine
      - Constitution d'un dictionnaire (noms communs, multilingues ...)
    - Par force-brute
      - Test des possibilités en direct, selon un jeu de caractères prédéterminé (charset)
    - Par les tables « rainbow »
      - Génération de tables de hash et de mots de passe selon un algorithme "optimisé",
      - Nécessite une table par type d'algorithme, en fonction du nombre de caractères, et du charset composant le mot de passe recherché.
    - Attaque sur l'authentification SMB
      - Attention à la politique de blocage des comptes
      - Penser à vérifier avec rpcclient ou wmi
- Outils
  - `John` (formats : LM, NT et mscash)
  - `Rcrack` (formats : LM et NT)
  - `Cain` (formats : LM, NT et mscash)
  - `Medusa` (`medusa -h <adresse_de_la_cible> -U <fichier_identifiants> _P <dictionnaire> -M smbnt`)

Protocoles d’authentification

- Challenge fixe + Rainbow table
  - Outils : `Cain, OphCrack`
- Prédiction des nombres pseudo-aléatoires/défi
  - Corrigé par le patch MS10-012
- SMB Relay et NTLM Reflection
  - Corrigé par le patch MS08-068
  - Outils : `Metasploit`

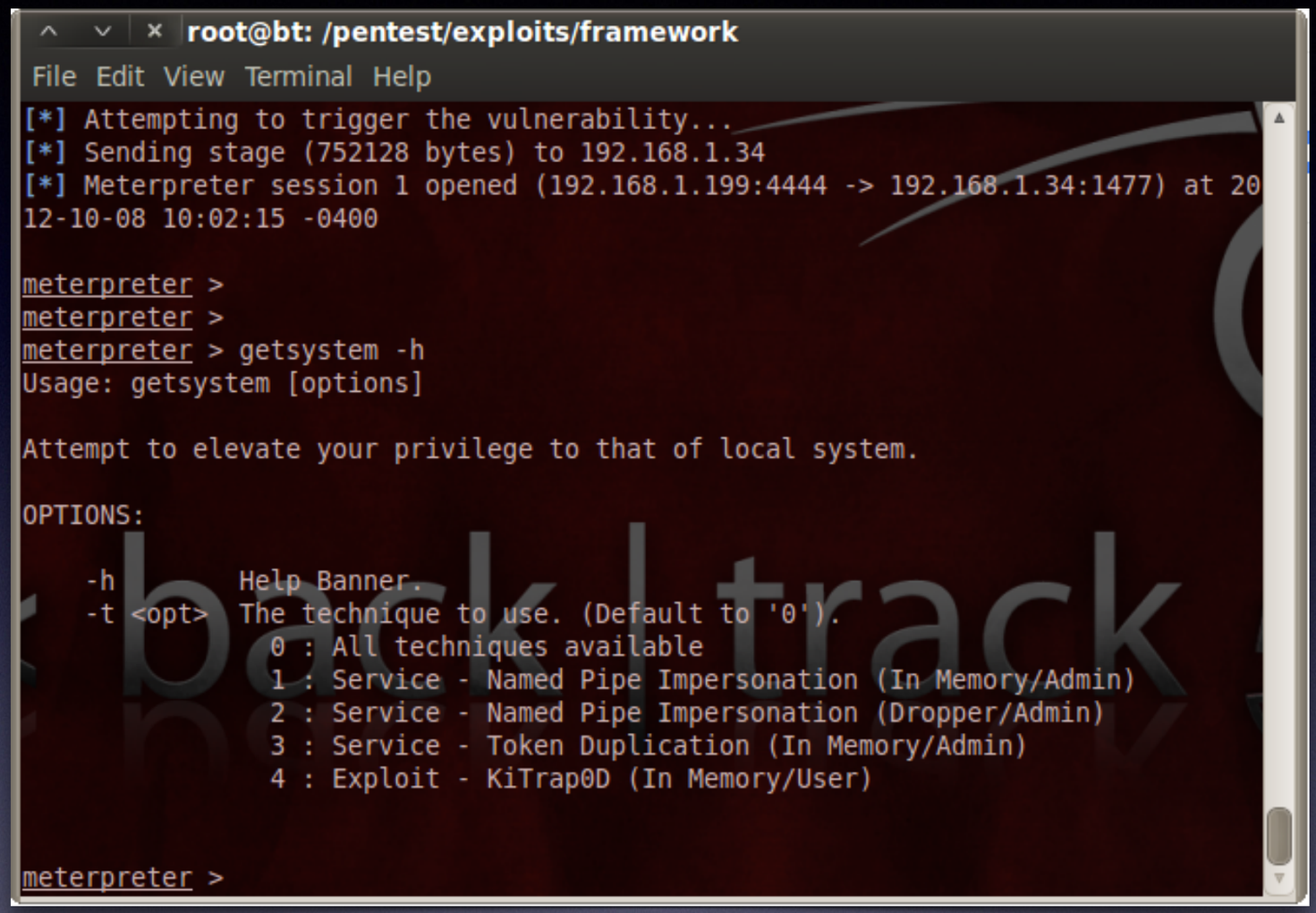
Elevation de privilèges

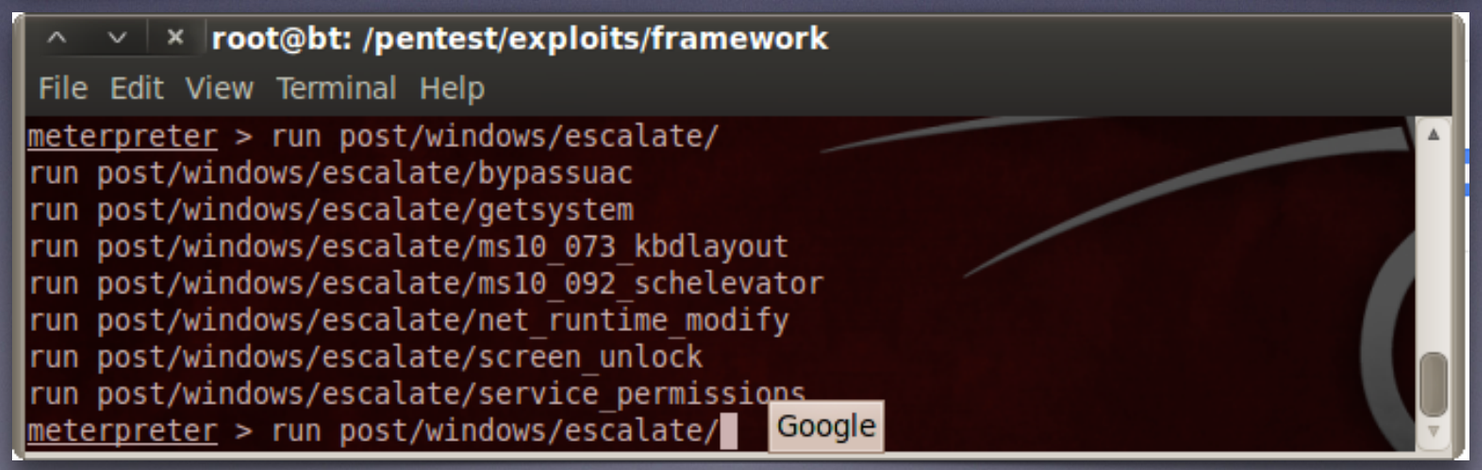
Elévation des privilèges

- Utilisation d'exploits
  - Disponibles pour
    - Les systèmes d'exploitation
    - Les applications internet
    - Les applications tierces
- Deux types
  - Locaux
  - A distance (remote)

Elévation des privilèges

- Metasploit





ExploitDB

```
root@bt:/pentest/exploits/exploitdb# ./searchsploit windows | grep remote | grep MS08
Windows Media Encoder wmex.dll ActiveX BOF Exploit (MS08-053)                /windows/remote/6454.html
MS Windows GDI (EMR_COLORMATCHTOTARGETW) Exploit MS08-021                    /windows/remote/6656.txt
MS Windows Server Service Code Execution Exploit (MS08-067) (Univ)           /windows/remote/6841.txt
MS Windows Server Service Code Execution Exploit (MS08-067)                  /windows/remote/7104.c
SmbRelay3 NTLM Replay Attack Tool/Exploit (MS08-068)                         /windows/remote/7125.txt
MS Windows Server Service Code Execution Exploit (MS08-067) (2k/2k3)         /windows/remote/7132.py
Microsoft XML Core Services DTD Cross-Domain Scripting PoC MS08-069          /windows/remote/7196.html
Microsoft XML Core Services DTD Cross-Domain Scripting PoC MS08-069          /windows/remote/7196.html
```

Questions ?