WinSec

DISCLAIMER: Travail fait par Marion Arnould - SRS 2023 - Il peut y avoir des fautes

NOTE - BONUS : Il faut apprendre une vulnérabilité sur Windows de l'année

Histoire

Connaître les différentes familles de systèmes Windows, leur version de noyau et leur état de support

Famille Historique - Basé sur MS-DOS :

- Windows 95, 98, Me

Famille NT (New Technology) :

- Client/serveur : Windows NT, 2000
- Client : XP (Noyau 5.1 ou 5.2 si x64), Vista (Noyau 6.0), 7(Noyau 6.1), 8 (Noyau 6.1), 8.1 (Noyau 6.3), 10 (Noyau 10), 11 (Noyau 11)
- Serveur : 2003 / 2003 R2 (Noyau 5.2) , 2008 (Noyau 6.0) / 2008 R2 (Noyau 6.1), 2012 (Noyau 6.2) / 2012 R2 (Noyau 6.3), 2016, 2019, 2022 (Noyau 10)

Support : le support c'est 5 ans actifs + 5 ans de sécu = 10 ans et après pour les entreprises peuvent payer 3 ans en plus donc en tout c'est 13 ans max

Architectures matérielles supportées et principales caractéristiques de Windows NT

Système d'exploitation exploitant pleinement les possibilités du processeur 386 (rings 0/3, Segmentation, pagination, adressage virtuel, multitâche préemptif, ...)

Fonctionne sur plusieurs architectures matérielles :

- À l'origine : x86, Alpha, PowerPC et MIPS
- Historiquement :
  - ARM : WOA (Windows on ARM) (Windows 8 RT)
  - Itanium : XP, 2003 et 2008/2008 R2
- Actuellement :
  - x86 : abandonné pour les serveurs depuis 2008 R2
  - x64 : de XP à Windows 10

Architecture

Catégories des différents types de processus (système, service, utilisateur)

- User : application (explorer.exe, userinit.exe, ...)
- Système : support, processes (lsass.exe, wininit.exe, ...)
- Services : processes (svchost.exe, spoolsv.exe, ...)

Définition d'un Sous système

Un Sous-système est composé de deux choses :

- Un processus jouant le rôle de « serveur »
- D'un ensemble de bibliothèque dynamiques offrant l'API aux processus

Connaître 3 sous-systèmes (Win, Posix, OS/2) et quelques exemples de processus de chaque catégorie

- Windows :
  - csrss.exe : Toujours démarré. Permet l'exécution de programme Windows 32/64 bits. Héberge les serveurs : csrsrv.dll, basesrv.dll ou encore winsrv.dll
- Posix :
  - psxss.exe : Initialement permet l'exécution de programmes POSIX 32 bits. Supprimé sous Windows 8/2012, remplacé sous 10 par Windows Subsystem for Linux (WSL) permettant l'exécution de binaire ELF64.
- OS/2 :
  - os2ss.exe : Support uniquement de programme OS/2 en invite de commande. Supprimé depuis XP/2003.

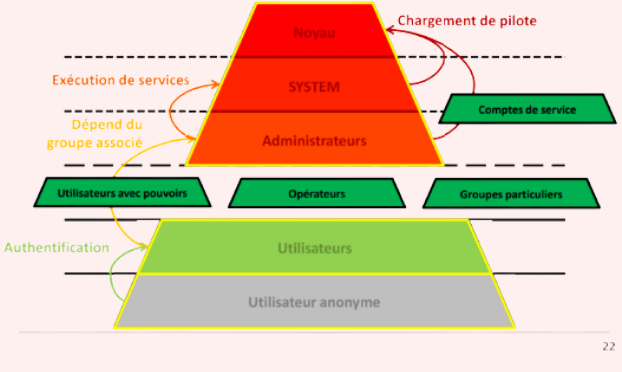
Session Windows : principe et isolation des services en session 0

Définition : Une session = Un processus + un Session ID. Elles sont mises en œuvre par le mécanisme Terminal Services. Utilisés pour le Fast User Switching, le bureau à distance ou les sessions étendues.

Apparue avec Windows NT4 TSE (Terminal Server Edition). Sert la connexion simultanée entre plusieurs users et un même système. Isolement pour le Système graphique et certains objets du noyau.

C'est Vista qui a introduit « l'isolation de la session des services » : la session 0 est réservée aux processus critiques du système et aux services. Pré-Vista, la session 0 était utilisée à la fois pour le système mais aussi pour le premier utilisateur.

Pyramide des droits



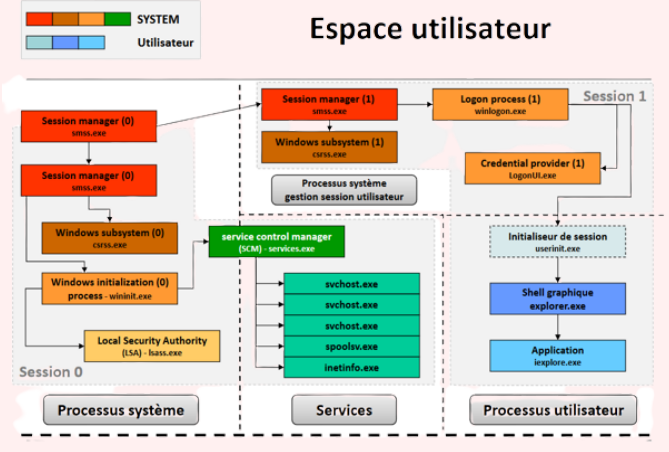
3 grands ensembles :

- Utilisateurs anonymes
- Utilisateurs authentifiés
- Utilisateurs privilégiés (Noyau, SYSTEM, Administrateurs)

Services

Introduction - Bonus

Processus du démarrage



Liste des processus importants

- smss.exe : Gestionnaire de sesssion Windows
- csrss.exe : Processus d'exécution client-serveur
- wininit.exe : Application de démarrage de Windows
- lsass.exe : Local Security Authority Process
- winlogon.exe : Application d'ouverture de session Windows
- svchost.exe : Processus hôte pour les services Windows. (utile pour charger les fichiers DLL)
- logonUI.exe - Windows Logon User Interface Host : gérer l'écran d'ouverture et de fermeture de sessions permettant de changer facilement d'utilisateur.
- spoolsv.exe : gère l'interaction avec l'imprimante
- inetinfo.exe : correspond au serveur web IIS (Microsoft Information Server)
- userinit.exe : User Session Initialization Application
- explorer.exe : gestionnaire de fichiers fourni avec l'OS Windows

Définition du SCM (Service Control Manager) - services.msc

Chargé de la gestion des services :

- Gestion de la base des services installés :
  - Ajout/suppression/configuration des services
  - Verrouillage de la base
- Démarrage (automatique/manuel) et arrêt des services
- Gestion de l'exécution des services (liste des services actifs, ...)

3 principaux comptes de service (droits, privilèges et capacité d'authentification réseau)

Chaque service applicatif s'exécute dans le contexte de sécurité d'un compte. Il est possible d'utiliser :

- Un compte user local ou de domaine
- Trois différents comptes de service et leur différence (privilégié ou non)
- Un compte de service virtuel
- Un compte de service géré (MSA)
- Un compte d'utilisateur authentifié interactivement

LocalSystem (S-1-5-18) : Entité de sécurité qui possède le plus haut niveau de droits et privilèges. Authentification à distance :

- Kerberos
- NTLM

LocalService (S-1-5-19) : Compte à droits restreints disponible à partir de XP. Peu de privilèges :

- AUDIT, CHANGE_NOTIFY, UNDOCK, IMPERSONATE
- Ceux de Utilisateurs et Utilisateurs authentifiés
- Ne peut pas s'authentifier à distance (session NULL / utilisateur anonyme)

NetworkService (S-1-5-20): Compte à droits restreints disponible à partir de XP. Peu de privilèges :

- AUDIT, CHANGE_NOTIFY, UNDOCK, IMPERSONATE
- Ceux de Utilisateurs et Utilisateurs authentifiés
- S'authentifie avec le compte de l'ordinateur lors des authentifications distantes (Kerberos et NTLM)

Principe de l'hébergement de services et rôle de svchost.exe

Pour les service du type SHARE_PROCESS un svchost.exe va être lancé, qui est l'hébergeur de services pour les services de type SERVICE_WIN32_SHARE_PROCESS, implémentés sous forme de bibliothèque (DLL). Plusieurs instances peuvent tourner simultanément.

Mise à jour

Principaux types de mises à jour de Microsoft

Les plus critiques :

- Critical Update : Problème spécifique, critique et non lié à la sécurité
- Security Update : Problème spécifique lié à la sécurité. Noté MSXX-YYY avec XX année sur deux chiffres et YYY numéro du correctif
- Update Rollup : Regroupement de hotfixes, critical updates, security updates et updates
- Service Pack : Update Rollup + Corrections + Ajout de nouvelles fonctionnalités
- Definition Update : Anti-virus, sites web malveillants, anti-spam
- [BONUS] Patch Tuesday : patch de sécurité tous les 2ème mardi du mois

Les autres :

- Update : Problème spécifique, non critique et non lié à la sécurité
- Feature Pack : Ajout de nouvelles fonctionnalités
- Tool
- Driver : Pilote

Politique de support : définition et durée des deux phases (principale et d'extension)

- Phase principale : support à l'incident, mises à jour de sécurité, hotfixes non relatifs à la sécurité. Environ 5 ans.
- Phase d'extension : support payant, mises à jour de sécurité, hotfixes non relatifs à la sécurité (payants via contrat), plus de changements de code ou de nouvelles fonctionnalités. Environ 5 ans.

Pour tout ce qui est grand public, matériel et multimédias ils ne bénéficie généralement pas de phase d'extension. Ce sont plus les logiciels d'entreprises et les logiciels de développements qui sont concernés

Windows 10 : Service Update et Feature Update - « Windows as a Service ».

- Service Update / Quality Update : ~ 1 par mois. Regroupement de correctif. 10.X.X.X
- Feature Update : ~ ½ par an. Nouvelle version de W10, Ajouts de fonctionnalité. Distribué sous forme d'une installation complète du système. 10.X.X.X

WSUS - Serveurs de déploiement (Update server)

- Microsoft update : postes isolés et connectés à internet
- WSUS (Windows Server Update Services) (ex. : SUS)
  - Sélection fine des mises à jour et du déploiement
    - Groupe avec des profiles différents
  - Inventaire des clients et déploiement des mises à jour :
    - Génération des rapports
    - Cascades de serveurs

Programmation avancée

Utilité des symboles et principe de fonctionnement

Les symboles sont créés par l'éditeur de liens. Ils sont utiles pour déboguer un programme, une bibliothèque ou un pilote (driver). Ils peuvent contenir :

- Le nom et type des variables : globales (Global syms), locales ou statiques
- Le nom des fonctions et des paramètres
- FPO records si applicable
- Le nom et les numéros de lignes de code (Line numbers)
- Les définitions des structures internes

Afin d'optimiser la taille du binaire, les symboles sont stockés dans un fichier séparé. Le principal format des fichiers de symboles est le Program Database (extension .pdb, anciennement .dbg). Il est possible de générer une version publique des fichiers de symboles (/PDBSTRIPPED). Celles-ci ne contiennent pas les informations sur le code source, les types et les données privées

Syntaxe : Module!NomFonction (La casse n'a pas d'importance)

Serveur de Symbole : L'API est implémentée dans dbghelp.dll. Les symboles sont recherchés dans un dépôt spécifié explicitement ou via des variables d'environnement (NT_SYMBOL_PATH)

Divers Symboles : dbh.exe, pdbcopy.exe, symchk.exe

Réseau

WNET : Notation UNC, Multiple Provider Router, Multiple UNC Provider

WNET permet l'accès et la gestion des systèmes de fichiers réseau. Mis en œuvre par :

- L'api WNET
- Le MPR (Multiple Provider Router) permettant de déterminer le fournisseur (Network provider)
- Le Multiple UNC Provider (MUP) (noyau) permettant de déterminer le redirecteur réseau (Network redirector)

Notation UNC (Uniform Naming Convention) : "**\\Serveur (nom de la machine distante)\Partage (nom du partage)\Chemin\fichier**"

Exemple de systèmes de fichiers réseau :

- Natifs : Lanman, WebDav, TS, (NFS)
- Tiers : VirtualBox, VMWare, etc

Network redirectors installés par défaut sous Windows (SMB, RDP et WebDav)

- Nom : Redirecteur RDPNP (RDP)
  - Principe : Utilisé par le service Terminal Services pour l'accès aux ressources disques du client
  - Exemple : \\tsclient\D
- Nom : Redirecteur WebClient (WebDAV)
  - Principe : Permet l'accès à des fichiers via HTTP(S) et les extensions WebDAV
  - Exemple : \\server@SSL\ ou \\server\share\
- Nom : Redirecteur LanmanWorkstation (SMB)
  - Principe : Permet l'accès à un système de fichiers via le protocole SMB
  - Exemple : net use \\localhost\c$

Fonctionnement de NetBios et des 3 sous-protocoles associés

Nommage des systèmes - deux formats :

- NetBios (max 15 caractères)
- DNS (hostname & FQDN)

Historique : protocole des années 80 toujours supporté via NetBT (NetBios over TCP/IP). Cela permet l'enregistrement, la libération et la résolution d'un nom NetBios sur un réseau local. Tout est en clair…

Nom NetBios = 15 caractères + 1 (Netbios Suffix).

Trois commandes : Registration, Release et Query. Cela offre trois services :

- NBNS (NetBios Name Service) : TCP/UDP 137
- NBDS (NetBios Datagram Service) : UDP 138
- NBSS (NetBios Session Service) : TCP 139

Rôle de SMB

SMB ou Server Message Block est un protocole de partage de fichiers apparu dans les années 80 où de nombreuses implémentations ont coexisté. SMB2 depuis **Vista**.

apports de SMB2 (de 2.0.2 à 3.1.1)

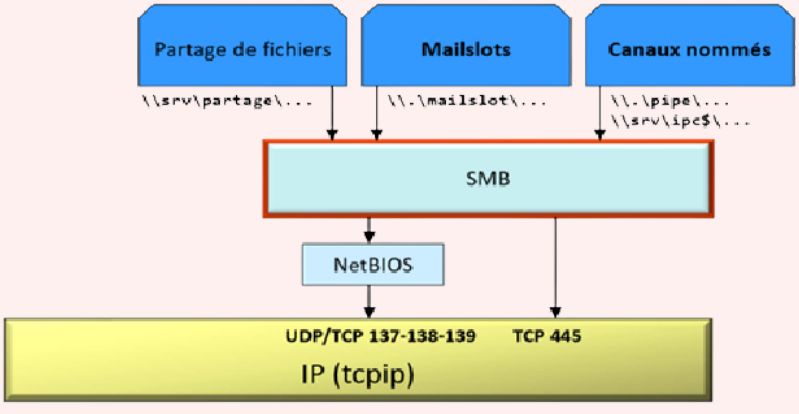
- SMB2 (Version) - SMB 2.0.2 (Famille) : Signature supporté et sécurisé (sur 16 octets) Abandon du transport NetBios, Changement complet, Simplification des commandes, Supports des handles et des symlink.
- SMB 3.0 - SMB 3.X : Chiffrement via AES-128-CCM, Signature avec AES-128-CMAC, Négociation sécurisée des dialectes entre v2 v3 (mais pas entre v2/v3 et v1) et Désactivation possible de SMB1.
- SMB 3.0.2 - SMB 3.X : Amélioration des opérations de connexion et d' I/O, partage de disque VHD, Administration avec PowerShell.
- SMB 3.1.1 - SMB 3.X : Négociation extensible, Pre-Authentication Intregrity, Possibilité pour le client à forcer le chiffrement, Support d'AES-128-GCM, Cluster DialectFencinget ClusterFailoverv2.

Transport de SMB et ports réseau associés

Transports disponibles :

- Tout système Windows :
  - NetBIOS Session Service (TCP 139) – OBSOLÈTE
    ⇨ Doit être désactivé
- À partir de Windows 2000 :
  - Direct Hosting (TCP 445)
- SMB 3.x :
  - RDMA (Remote Direct Memory Access)
- Windows 10 21Hx, Windows 11, Windows Server 2022 :
  - QUIC (UDP 443)

Named pipes et mailslots - Communication interprocessus



Rôle du partage IPC$ - Inter-Process Communication

Anonymes : permet une communication entre deux processus sur une même machine.

Nommés (namedpipe) : permet une communication entre processus éventuellement sur deux machines différentes.

- Le partage SMB est IPC$
- Chemin SMB : (insensible à la case) \\ServerName\pipe\PipeName
- Le canal nommé possède un descripteur de sécurité
- Utilisation possible d'alias : HKLM\SYSTEM\CurrentControlSet\Services\Npfs\Aliases

Définition des RPC (Remote Procedure Call) et importance dans les systèmes Windows

Définition : Mécanisme de gestion d'un modèle client/serveur réparti : Fonctions exportées par un serveur et appelées par un client. Permet l'appel, dans un processus client, d'une fonction s'exécutant dans un autre processus (dit serveur). La gestion des communications réseau est effectué par l'OS.

Chaque interface RPC est identifiée par :

- Un UUID (Universal Unique Identifier)
- Numéro de version

Les fonctions sont ensuite identifiées par un numéro d'opcode.

Principaux protocoles : ncacn_ip_tcp, ncadg_ip_udp, ncacn_np, ncacn_http, ncalrpc

RPC

Rôle du langage MIDL (Microsoft Interface Definition Language)

Définition :
Langage de définition des interfaces RPC. La compilation d'un fichier IDL génère :

- Un fichier d'en-tête commun
- Le stub client
- Le stub serveur

Principaux mécanismes de transport des RPC

Nom	Type
ncalrpc	Network Computing Architecture **local remote procedure call**
ncacn_x	Network Computing Architecture **connection-oriented** protocol
ncadg_x	Network Computing Architecture **datagram** protocol

Nom	Type	Option
ncalrpc	*Local Inter-Process Communication port*	Nom du LPC
ncacn_ip_tcp	Socket TCP	Port TCP
ncacn_np	Canaux nommés	Nom du canal nommé
ncacn_http	HTTP	Port et proxy
ncadg_ip_udp	Datagramme UDP	Port UDP

Authentification

Calcul hash LM/NTLM (grands principes, algos, faiblesses)

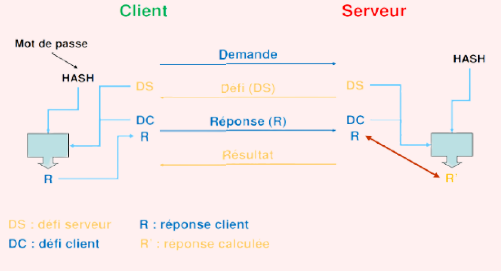
- LM (LAN Manager)
  - Apparition : Historique
  - Taille (en caractère) : 14
  - Alphabet : Restreint (OEM)
  - Algorithme de calcul : DES
  - Salt : Non
  - Stockage des empreintes des comptes locaux : Base SAM
  - Stockage des empreintes des comptes de domaine : Base Active Directory (Attribut dBCSPwd)

- NTLM (NT Lan Manager)
  - Apparition : Windows NT4 SP3
  - Taille (en caractère) : 255
  - Alphabet : Large (Unicode)
  - Algorithme de calcul : MD4
  - Salt : Non
  - Stockage des empreintes des comptes locaux : Base SAM
  - Stockage des empreintes des comptes de domaine : Base Active Directory (Attribut unicodePwd)

Problème : Pas de sel donc mot de passe identique pour empreinte identiques.
Utiliser LAPS qui permet de bloquer les flux entrants ou de réduire les droits UAC.

Calcul défi réponse LM/NTLM/NTLM2/LMv2-NTLMv2 (grands principes, algos, faiblesses)

Schéma général d'un défi / réponse



Protocole	Réponse	Empreinte utilisé	Défi Serveur	Défi Client	Algorithme Calcul Réponse	Taille de la réponse
NTLM	LM	LM	Oui	Non	DES	24 octets
	NTLM	NTLM	Oui	Non	DES	24 octets
NTLM Extended Session Security	NTLM	NTLM	Oui	Oui	DES	24 octets
NTLM v2	LM v2	NTLM	Oui	Oui	HMAC-MD5	24 octets
	NTLM v2	NTLM	Oui	Oui	HMAC-MD5	>24 octets

Calcul des clés Kerberos AES et Avantages de Kerberos par rapport à NTLM

	LM/NTLM	Kerberos
Type de Crypto	Symétrique	Symétrique
Plateformes Microsoft	Toutes	Depuis 2000
Montée en charge	Faible	Élevé
Authentification mutuelle	Non	Option
Délégation supportée	Non	Oui
Support carte à puce	Non	Extensions
Standard	Microsoft	IETF

Principales attaques sur NTLM

- Pass the hash : Il n'est pas nécessaire de retrouver le mot de passe d'un utilisateur pour pouvoir s'authentifier auprès d'un service (voir par la suite). Équivalent Kerberos : Pass the key
- La Reflexion NTLM : Le client discute directement avec l'attaquant qui se fait passer pour un serveur
- Le Relais NTLM : aussi nommé Credential Forwarding. Espèce de MitM
- Authentification mutuelle : NTLM ne peut pas assurer l'authentification mutuelle. Le client n'est donc jamais assuré qu'il s'est authentifié sur un serveur légitime

Kerberos : fonctionnement général et intérêts/apports en sécurité

Introduit dans Windows 2000, initialement standard du MIT avec des extensions en plus. Met en œuvre une authentification avec trois acteurs, disposant chacun d'un secret connu de lui et du KDC :

- Un utilisateur identifié par un UPN (User Principal Name) : KC
- Un service identifié par un SPN (Service Principal Name) : KS
- Un tiers de confiance, le KDC (Key Distribution Center) : KKDC

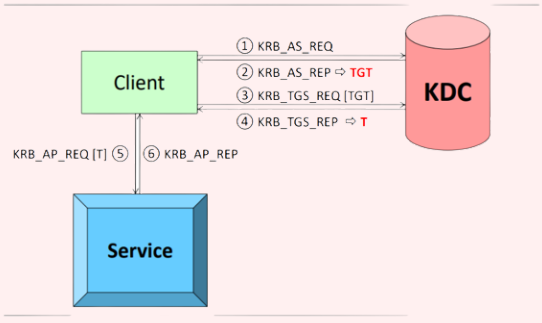
Kerberos est composé de trois services :

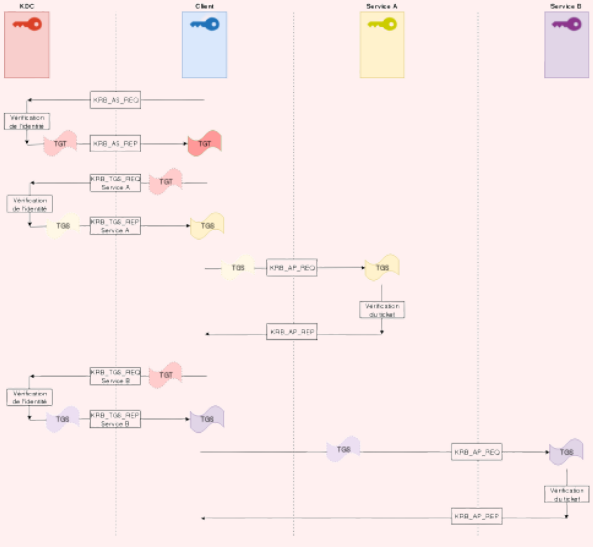
- Authentication Service (AS) qui délivre un TGT et une logon session key
- Ticket Granting Service (TGS) qui delivre un service ticket et un service session key
- Client/Server (CS) qui présente les tickets de service d'un client à un service

Kerberos permet de mettre en œuvre la délégation d'authentification (permet, à un client, de transmettre à un service tout ou partie de ses éléments d'authentification afin que le service puisse s'authentifier enson nom auprès d'un service tiers). Elle peut être :

- Non contrainte ou Complète
- Contrainte
- Contrainte avec transition de protocole
- Contrainte basée sur la ressource

Kerberos





Rôle de la PAC dans Kerberos

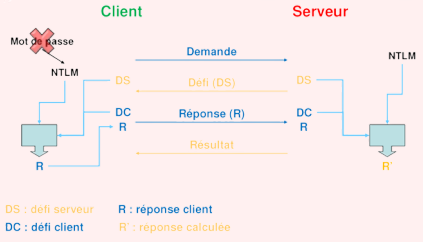
Privilege Attribute Certificate : Kerberos est un protocole d'authentification, il est également possible de l'utiliser pour transporter des données d'autorisation via un champ, transportant une structure de type KERB_VALIDATION_INFO, spécifiant les données d'autorisation de l'utilisateur (PAC). La PAC peut être validée par le KDC ou un système.

Fonctionnement de PKINIT

Public Key Cryptography for Initial Authentication (asymétrique), permet la mise en oeuvre d'échange de clés basés sur Diffie-Hellman et d'authentification basée sur RSA ou DSA. On peut alors utiliser des certificats numériques (x509), des cartes à puces et des tokens d'authentification.

Principe et conséquence de Pass-the-hash

Il y a deux formes d'authentification qui sont à distinguer, la locale et la distante



AP : rôle et connaître ceux de Microsoft

AP ou Authentication package va mettre en oeuvre l'authentification locale. Ça permet d'authentifier un utilisateur puis de créer une session d'authentification (composée d'un ID unique, nom de domaine, nom d'utilisateur, SID, nom de l'AP et type de session) et un contexte de sécurité.

Exemple d'AP Microsoft :

- Msv1_0 (NTLM) : authentification et (validation) des comptes locaux (via la base SAM) et pour les comptes d'un domaine si Kerberos peut pas être utilisé (validation via NetLogon). Possède un mécanisme de cache.
- Kerberos : Méthode privilégiée pour les comptes d'un domaine (demande au préalable d'un TGT)

SSP : rôle et connaître ceux de Microsoft (les principaux vus en cours)

SSP ou Security Support Provider va permettre l'authentification distante d'un utilisateur via la mise en œuvre d'un protocole d'authentification réseau.

- Côté Client, cela permet :
  - De spécifier le SSP à utiliser
  - De spécifier un contexte d'authentification à utiliser
  - De s'authentifier auprès d'un serveur

- Côté Serveur, cela permet :
  - De spécifier le SSP à utiliser
  - De valider l'authentification en provenance d'un client

Exemple d'SSP Microsoft : NTLM, Kerberos, Negociate, SSL/TLS, WDigest, CredSSP, TSSSP, NegoExtender, Pku2u

Si le SSP valide une authentification distante, il demande à son AP correspondant de réaliser une authentification locale de type réseau (3), ce qui permet :

- D'autoriser l'authentification de type réseau
- De créer une session d'authentification
- De créer un contexte de sécurité (token) représentant l'utilisateur distant authentifié par le réseau

Rôle de NetLogon

NetLogon permet d'interconnecter la base SAM d'une machine avec celle d'un CD d'un AD, grâce à un Secure Channel. Cela permet à la machine membre de pouvoir valider les authentifications auprès d'un tiers, ce qu'on appelle le Pass-Through Authentication. Ces authentifications peuvent être de deux types : Interactives ou distantes.

Mise en œuvre du SSO (authentification implicite/explicite)

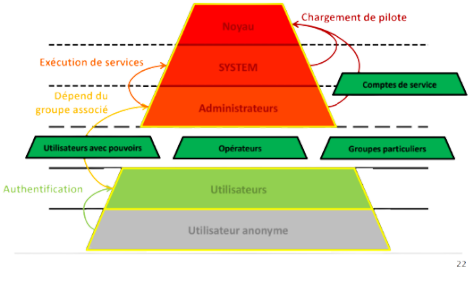
Côté client, trois contextes d'authentification sont possibles lors de l'initialisation du SSP :

- Authentification explicite : les authentifiants (credentials) sont fournis explicitement lors de l'appel. Ce mécanisme permet le changement d'identité lors d'une authentification distante
- Authentification implicite : aucun authentifiant n'est fourni lors de l'appel. Ceux-ci sont récupérés dans la session d'authentification de l'utilisateur effectuant l'appel (réalisation du SSO Windows)

Lors de la création de la session d'authentification locale, les credentials de l'utilisateur sont mis en cache par les SSP afin d'être utilisés implicitement lors des authentifications distantes. Ainsi, aucun nom d'utilisateur ni mot de passe n'est nécessaire lors des authentifications distantes réalisées par les SSP.

Modèle de sécurité

Pyramide des droits



SID : format générique et leur rôle dans le modèle de sécurité

S - REV - ID_AUTHORITY - (Sub...Sub) - RID

REV : Indique la version de la structure SID. Actuellement toujours à 1.
ID_AUTHORITY : Identifie le plus haut niveau d'autorité qui peut émettre des SID. 1 pour le monde et 5 pour Windows NT.

S-1-0-0 = nobody (NULL)
S-1-1-0 = everyone
S-1-5-18 = SYSTEM (admin local donc)

Un SID (Security ID) permet de décrire les interactions que peut avoir un objet (process/thread/fichier/...) dans le cadre d'un contrôle d'accès. Il sert aussi à identifier le propriétaire, le groupe d'un objet.

Principe de génération des SID des comptes locaux

SID des comptes locaux supérieur à S-1-5-21-999.

Dans un active directory c'est le FSMO RID qui s'en occupe.

Définition du Token et principaux composants

Les tokens, crées par les SSP, permettent de décrire le contexte de sécurité d'un objet. Par défaut, le système donne un token au programme qui est une copie de celui du user ou une copie plus restreinte. Les composants principaux d'un token sont :

- UsersAndGroups (tableaux) : contient des SID pour définir les accès en fontion du user et groupe.
- Privilèges : permissions spécifiques
- Owner
- RestrictedSids
- Default DACL, ...

Rôle de l'attribut DenyOnly

Le SID ne peut être utilisé que pour des ACE de refus d'accès

Définition du descripteur de sécurité et composants (owner, DACL, SACL)

C'est une chaine de caractère au format SDDL qui décrit les autorisations d'accès.
Owner : à qui appartient l'objet
DACL : Discretionary Access Control List - contient les ACEs d'accès
SACL : System Access Control List - Contient les ACEs d'audit et autres

Définition droits accès standard, spécifique, générique

Standard : Commun à tous les objets
Spécifique : différent pour chaque type d'objet
Générique : Accès regroupant les accès spécifiques en catégories

Fonctionnement général du contrôle d'accès

L'opération a un accessMask définissant les besoins en privilèges de l'opération. L'AccessMask est confronté au token puis à l'objet. Si tous les bits de l'accessMask sont à zéro après confrontation, l'opération peut avoir lieu sinon l'accès est refusé.

Rôle et fonctionnement des restricted SID

Permet de faire sauter le SID de l'owner. Dans le cas où une liste Restricted Sids existe, un deuxième contrôle d'accès est effectué avec la liste.

Connaître les privilèges sensibles

Privilèges sensibles :

- SeDebugPrivilege : avoir tous les droits sur n'importe quel process.
- SeRestorePrivilege : écrire un fichier/clé du registre quelque soient les droits (pour restauration)
- SeBackUpPrivilege : lire un fichier/clé du Registre quelque soient les droits (pour restauration)
- SeCreateTokenPrivilege : créer un Token
- SeTakeOwnershipPrivilege : prendre possession des objets avec contrôle d'accès (fichier, clé de reg...)
- SeLoadDriverPrivilege : charger et décharger des pilotes et périphériques
- SeTcbPrivilege : "agir en tant que partie du système d'exploitatopn" vérifié par diverses API
- SeAssignPrimaryTokenPrivilege : remplacer le token d'un processus

Définition du SDDL

Security Descriptor Definition Language : Permet de décrire un descripteur de sécurité.

Principe de l'impersonation

L'impersonation permet de représenter le contexte d'un utilisateur distant.

4 niveaux d'impersonation :

- Anonyme : représente un utilisateur anonyme
- Identification : Pas assignable à un thread
- Impersonation : Pas de délégation
- Délégation : assignable à un thread et délégation autorisée !

Définition et différences entre primary token et impersonate token

Un primary Token est un token affecté pour représenter un contexte de sécurité.
Un impersonate Token est un token créé pour capturer le contexte de sécurité d'un client.

Le primary Token est affecté à un processus.
L'impersonation Token ne peut être affecté qu'à un thread.

Fonction CreateRestrictedToken : modifications appliquées aux tokens

SIDs mis à Deny_Only.
Suppression de privilège.
Ajout de SIDs dans la liste des restricted SIDs.

Par défaut, un token a pour paramètre elevated = yes. Après l'UAC réduit le token en fonction des besoins (elvated = no), ce qui donne un restricted token.

AppContainer : principe et protections appliquées

Les AppContainer apportent de fortes restrictions sur un programme.

SID des appcontainers : S-1-15-2-XXXX
SID des capabilities : S-1-15-3-XXXX

Les AppContainers apportent des restrictions sur :

- Les tokens
- Control d'accès
- Kernel Namespace
- Graphique
- Réseau
- Fichier
- Registre
- Processus
- Credentials
- Périphériques

Nouveaux mécanismes

Rôle et intérêt de : /GS, DEP, ASLR, CFG, CET

/GS (Buffer Security Check) :
Mécanisme de compilation s'appliquant dans certains cas et amélioré à chaque version du compilateur. Protection à l'exécution contre les buffers overflows. Un cookie, vérifié à l'épilogue, est inséré sur la pile au prologue entre les informations liées à l'exécution de la fonction et les données utilisateurs.
La directive strict_gs_check, permet à /GS d'être plus agressif.

DEP ou Data Execution Prevention repose sur les fonctionnalités des processeurs :

- No Execute (NX) d'AMD
- Execute Disable Bit (XD) d'Intel

Afin de faire marcher le DEP, le PAE (Physical Address Extension) du processeur doit être activé. Le 64e bit des tables des pages PTE (Page Table Entry) est utilisé pour marquer les pages mémoires comme non exécutables. Plusieurs modes existent :

- AlwaysOff (0) : Protection Désactivée
- AlwaysOn (1) : Protection Activée pour tous les programmes
- OptIn (2) : Protections activées pour les programmes du système Par pour défaut les windows client. /NXCompat permet de marquer le module comme étant compatible avec DEP dans ce mode
- OptOut (3) : Protection activée pour tous les programmes sauf ceux listés dans les exceptions. Par défaut pour les Windows Server

ASLR (AddressSpaceLayout Randomization)
Permet de rendre aléatoire la position en mémoire des :

- Modules (EXE et DLL). /DynamicBase marque le module comme compatible avec l'ASLR
- Tas
- Piles
- Var d'Env
- Structure TEB et PEB

Avec Windows 8, de nouveaux mécanismes :

- HEASLR augmente l'entropie sur les systèmes x64
- ForceASLR qui force l'ASLR pour tous les modules
- Dissalow Stripped images qui ne chargent pas les images non relogeables

CFG (Control Flow Guard) : Permet de contrôler les appels indirects afin de s'assurer que les adresses de destination sont légitimes. Pour cela, il faut :

- L'ajout de la description des flux légitimes dans le module
- Le support par le système

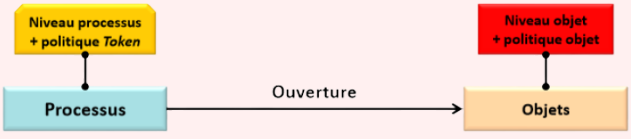
CET (Control-Flow Enforcement Technology
Protection au niveau du processeur contre les attaques dit de détournement de flot de contrôle (ordre d'exécution des opérations dans le CPU) utilisant abusivement du code légitime.

Integrity level : niveaux par défaut, politique sur les processus et objets

Windows Integrity Mechanism : Mécanisme de contrôle d'accès obligatoire, basé sur des niveaux appelés : niveaux d'intégrités.
Ce contrôle d'accès est traité avant le contrôle d'accès discrétionnaire

Principe :

- Chaque processus dispose d'un niveau d'intégrité explicite et d'une politique associée
- Chaque objet dispose d'un niveau d'intégrité explicite ou implicite et d'une politique associée



Niveaux d'intégrité prédéfinis :

Valeur	Nom	SID
0x0000	Non approuvé	S-1-16-0
0x1000	Faible	S-1-16-4096
0x2000	Moyen	S-1-16-8192
0x3000	Élevé	S-1-16-12288
0x4000	Système	S-1-16-16384

Donnant l'échelle pour le niveaux d'intégrité par défaut :

SID dans le token	Niveau d'intégrité
LocalSystem	Système
LocalService	Système
NetworkService	Système
Administrateurs	Élevé
Opérateurs de sauvegarde	Élevé
Opérateurs de configuration réseau	Élevé
Opérateurs de chiffrement	Élevé
Utilisateurs authentifiés	Moyen
Tout le monde	Faible
Anonyme	Non approuvé

Politique sur les tokens :

- TOKEN_MANDATORY_POLICY_NO_WRITE_UP (toujours activée) : le processus ne peut pas écrire dans un objet dont le niveau d'intégrité est supérieur
- TOKEN_MANDATORY_POLICY_NEW_PROCESS_MIN (activé pour les MOYEN et FAIBLE) : le niveau d'intégrité d'un processus fils sera le minimum entre :
  - Le niveau d'intégrité de ce processus (le père)
  - Le niveau d'intégrité du programme

Politique sur les objets :

- Chaque descripteur de sécurité d'un objet peut définir les politiques d'accès à l'objet : NO_WRITE_UP, NO_READ_UP, NO_EXECUTE_UP
- Si un objet ne définit pas de politique explicite, une politique implicite est appliquée :
  - NO_WRITE_UP & NO_READ_UP pour les processus et threads
  - NO_WRITE_UP pour tous les objets

Fonctionnement d'UAC et effets des 3 restrictions

UAC (User Account Control) permet de restreindre les droits et privilèges des admin pour leur permettre d'effectuer les tâches courantes en tant qu'utilisateur standard. Ainsi si ces droits sont à nouveaux demandés, l'utilisateur doit consentir à les retrouver (On parle d'élévation avec le token élevé).
Dans les faits quand un utilisateur membre d'un groupe "administratif" se connecte, deux tokens sont créés :

- Un élevé avec l'ensemble de ses droits et privilèges.
- Un épuré avec quelques privilèges conservés et les sid des groupes marqués DENY_ONLY. Lorsque les applications sont lancées par l'utilisateur c'est ce token-là qui est utilisé.

Une application, via son manifest et la directive requestedExecutionLevel, peut imposer le comportement d'UAC :

- asInvoker : pas de demande d'élévation
- highestAvailable : le «Token élevé» doit être utilisé
- requireAdministrator : l'application doit être lancée avec des droits administrateurs (élévation ou changement de compte)

Sécurisation des services : réduction des privilèges, SID de service (3 niveaux)

Un service peut avoir trois niveaux de protection par SID :

- None : Aucun changement
- Unrestricted : Ajout d'un SID (généré à partir du nom du service sous l'autorité NT Service) de service dans le jeton du processus hébergeant le service. Ce mécanisme permet la protection des objets manipulés par le service. Commande : sc showsid <nom>
- Restricted : Ajout d'un SID de service dans le jeton du processu hébergeant le service + utilisation des restricted SID pour perdre les droits du compte de service. Ajout des SID suivant dans la liste des SID restreints : LogonSID, S-1-1-0, Write-restricted SID et l'ensemble des RESTRICTED

Dans le cas d'un hébergeur de service, tous les privilèges et SID de service sont accordés au processus, dès sa création, même si les services ne sont pas en cours d'exécution.

Fonctionnement des Virtual Account et leur mise en œuvre

- Géré à partir de Windows 7/2008-R2
- Permet de démarrer un service (non mutualisé) sous une identité propre : NT SERVICE\servicename
- Le processus dispose des SID :
  - NT SERVICE\ALL SERVICES
  - SERVICE
- Le profile du compte est "c:\users\servicename"
- Le compte s'authentifie sur le réseau avec le compte de la machine

De Microsoft documentation :

Il s'agit de comptes locaux gérés qui simplifient l'administration des services en fournissant les avantages suivants :

- Le compte virtuel est géré automatiquement.
- Le compte virtuel peut accéder au réseau dans un environnement de domaine.
- Aucune gestion des mots de passe n'est requise.

Process Mitigation Option

Possibilité d'appliquer des restrictions aux processus via la fonction SetProcessMitigationPolicy()

- ProcessDEPPolicy - 8
- ProcessASLRPolicy - 8
- ProcessStrictHandleCheckPolicy - 8
- ProcessSystemCallDisablePolicy - 8
- ProcessExtensionPointDisablePolicy - 8
- ProcessDynamicCodePolicy - 8.1
- ProcessSignaturePolicy - 10
- ProcessFontDisablePolicy - 10
- ProcessImageLoadPolicy - 10
- ProcessUserShadowsStackPolicy - 10 - 2004

Windows Defender Exploit Guard (partie Exploit protection)

Composé de :

- Exploit protection - 1709
- Attack surface reduction (ASR) rules - 1709 WDAV
- Network protection - WDAV
- Controlled folder acces - WDAV

Divers

PP / PPL (Protected Process Light) : Possibilité d'activer les restrictions des droits sur les ouvertures des processus et des threads comme pour les PP, sur des processus non liés aux DRM et PMP. Plusieurs niveaux de PPL sont définis : Authenticode, CodeGen, Antimalware, Lsa, Windows, WinTcb.

Restrictions supplémentaires :

- Chargement de DDL dûment signé (WHQL)
- Conformité au développement SDL
- Désactivation des shims issus de la base de comptabilité

Si un processus d'un niveau PP ou PPL ouvre un processus ou un thread d'un niveau PP ou PPL supérieur, seuls les droits suivants sont autorisés :

- Processus :
  - PROCESS_QUERY_LIMITED_INFORMATION
  - PROCESS_SUSPEND_RESUME
  - PROCESS_SET_LIMITED_INFORMATION
  - [PROCESS_TERMINATE] : uniquement pour certains niveaux de PPL (ex : Authenticode)
- Thread :
  - THREAD_SET_LIMITED_INFORMATION
  - THREAD_QUERY_LIMITED_INFORMATION
  - THREAD_RESUME
  - [THREAD_SUSPEND_RESUME] : uniquement pour certains niveaux de PPL (ex : Authenticode)

Les services peuvent être configurés pour devenir des PPL (sc qprotection ou attribut LaunchProtected)

Protection VBS et exemples de mise en œuvre : Credential Guard et Device Guard (WDAC)

VirtualizationBasedSecurity (VBS) est apparu avec Windows 10/Server 2016. VBS permet l'apport de fonctions de sécurité via la mise en oeuvre de la virtualisation. Les mécanismes reposant sur VBS sont :

- CredentialGuard : les secrets devant être mis en cache par LSASS sont stockés dans le VSM par la TrustletLsaIso. Ces secrets deviennent alors inaccessibles depuis le système HLOS. Cela concerne les empreintes LM/NTLM/SHA-1 et les clés Kerberos
- DeviceGuard : Si activé à Les pages mémoires dans les noyaux ne peuvent être marquées « exécutables » que par le SKM et pour être marqué exécutable dans le HLOS, un code doit avoir sa signature validée par le HVCI (HyperVisorCode Integrity) et être approuvé par une politique de signature
- ShieldedFabric
- HyperGuard

Pour fonctionner correctement, les fonctionnalités VBS ont besoin :

- d'un module TPM pour assurer la protection de données (clé machine)
- de SecureBoot pour s'assurer que la chaîne de démarrage soit intègre
- d'UEFI pour pouvoir stocker des variables afin de s'assurer que les politiques de sécurité ne soient pas modifiées

AppLocker

AppLocker vous permet de contrôler les applications et fichiers que les utilisateurs peuvent exécuter.