

- Souv Réf Monitor (SRM) (ntoskrnl.exe): composant écrit en C qui définit la structure de données selon accès + effectuer contrôles accès objets + manipuler priviléges et droits users + générer messages audits. Seul résponsable pour politiques d'accès.
- Local Secu Authority SubSyst (LSASS) (lsass.exe): processus user mode, gérer politiq. Secu locale (users autorisés) + authent. Local Secu Auth. Server (LSSASrv.exe) (lsasrv.dll) chargée par LSASS qui implemente la plus grande partie des fonc de LSASS.
- ↳ Secu Accounts Manag Server (SAM Serv) (sam.srv, dll) chargée par LSASS gère la bdd SAM (noms + empreintes md5) → HKEYLM/SAM
- ↳ Active Directory Server (ntds.dll) chargée par LSASS - implemente le Directory System Agent (DSA) fait Active directory control des objets.
- ↳ Service Network Logon, composé netlogon, serviceW pr localiser contrôleur domaine + canal secu avec + effectuer logon + recuperer mots de passe.
- ↳ packages d'authent - permet d'authentifier utilisateurs et communiquer à LSASS identité user (pr générer token) ex: msvcrt-1-0.dll
- Winlogon (winlogon.exe) processus pr hép au SAS (Secure Attention Sequence) CTRL+ALT+SUPPR + gérer session interactif + 1er processus.
- LogonUI (LogonUserInterf) (logonui.exe): processus qui présente l'interface aux user pr s'authent sur le système et utilisation de Credential Providers pr récup authentifiants utilisateurs (ID + md5 authz). DLL se P:\Nuice\Smartcard\CredentialProvider.dll
- fichiers importants:
 - hal.dll: module moyen implementant la couche d'abstraction matérielle. ntoskrnl.exe = registre hal.dll
 - win32k.sys: pilote périph. réseau + gestionnaire fenêtres, affichage écran, saisies clavier/souris) + ntdll.dll : DLL exportant plusieurs points d'entrée vers services sys. Kernel32.dll : DLL exportant fonc fondamentales comme gestion fichiers, création de processus, pr empêcher applis users d'avoir accès ou modif données critiq OS → Kernel Mode : processus donne accès à toute le mem et intér. C
 - User Mode : accès partie mémoire + bloqué accès à certaines introm. = appeler SYSCALL pr passer en mode moyen pr appeler certaines instr.
- base de registre (regedit en reg) : bdd qui contient la config du système, des applications, des profils utilisateurs, des valo.
- service (services.msc en sc) : daemon. appli service + prog control service (scmgr) pr gérer demon cont.
- objet : ressources associées progr. mode user représentées comme objet au niveau regen. Le contexte prop entité. Les objets sont manipulés en user mode avec des handles. DAC = Discretionary Access Control
- SID : permet identifier les entités (users et leurs process, groupes, groupes, domaines, ordinateurs locaux) d'un système. Il le monde entier : S-1-5-sid4-sid2-sid3 - RID → S = autorité SECURITY_NT_AUTHORITY ; 1ere RID = 1er user pr système. S-1-1-0 : nul. S-1-5-7 : anonyme. S-1-5-11 : utilisateur auth. S-1-5-18 : système local. S-1-5-domain-500 : admin local. S-1-5-dom-501 : guest.
- jeton d'accès : identifie contexte sécurisé processus user (privileges + id). Généré à l'authent user Winlogon qui l'attache au 1er process user. Tous les prog lancé par user héritent du jeton. Il est possible de générer jeton (LogonUser) et de lancer process avec ce jeton (CreateProcessAsUser).
- ↳ primary token = identité sécurisé user associé process. La impersonation token = pr prendre temps.
- ↳ autre identité (thread) Le jeton restreint : limitation accès objets et priviléges (CreateRestrictedToken)
- privileges : droit d'un compte de faire actions sys sur objets (enable / disabled), concerne les objets.

- actions non autorisées à la clé en portefeuille (ex: charger monnaie) le présent dans le jeton d'accès → tokens / priv
- droits utilisateurs → secpol.msc : priviléges qui concernent les types ouverture de session autorisé (vérifié par LSA) le m
présent dans le jeton accès la se: interdit connexion en tant que Service. Il définit quelles infos sont enregistrées de journal
- descripteur de sécurité → secdl.exe (je vois DACL) le définit qui peut faire quoi sur l'objet et quelles il sont attachés.
le stockage de la clé SECURITY_DESCRIPTOR: revision number: version modifiée sécurité SACL flags: bits contenant descripteurs
- owner SID = SID propriétaire • gris SID • DACL: spécifie qui a quel accès à l'objet • SACL: spécifie quelles opérations enregistrées, journ
(d'accès)
- ACL (access control list): collection d'ACE. - ACE (access control entry): association d'un compte (user ou group) à une
règle d'autorisation ou interdiction sur une ressource. - DACL (Discretionary Access Control List): gère les permissions
sur l'objet, spécifiant qui est autorisé et à qui est interdit de faire certaines actions sur l'objet. - SACL (System Access Con

- ACL syntaxe : `acl Reader: comp(ace_1)(ace_2) ... avec acl_header(D pr, DACL et S pr, SACL) et comp° PAI (bloquer héritage), AI (autoriser)` - ACE Syntax : `ace_type; ace_flags; rights; object_guid; inherit object_guid; account_sid`
- ↳ `ace_type` : A (access allowed), D (denied), AL (sys alarm), OU (obj audit)
- ↳ `ace_flags` : C (objet enfants conteneurs héritage)
- ↳ `Oi` (obj enfants non conteneurs héritage), ID (héritage)
- ↳ `rights` : GA (All), GR (Read), GW (Write), GX (exec), WC (write owner), F (file access), FR (file generic read) le account_sid = SID complet ou SID string → BA (gradmin), SY (sys local), WD (creer)
- Système de contrôle d'accès aux objets : descripteur seen possédé par 1 obj (ex: fichier, dossier, processus). - Jeton possédé par un user (en réalité leurs processus) ↳ quand un processus veut un handle d'un objet, le SRM vérifie le jeton du processus de l'utilisateur et le descripteur de sécurité de l'objet.

① gestionnaire sessions (smss) démarre Winlogon (au démarrage de Windows) ② Winlogon crée un objet Windows Statique (représentant écran, clavier, souris) ③ Winlogon crée 2 objets Desktop (desktop sec et desktop d'appli) ④ Winlogon se connecte à LSASS (avec la fonction RegisterLogonProcess) pour échanger infos login, log off, mdp. ⑤ Winlogon enregistre son serveur RPC qui écoute notif du SAS (lancé appli malveillante sur le SAS) ⑥ connexion user : ① user va sur le SAS (CTRL+ALT+SUP) ② Winlogon décode l'authentification ③ Winlogon récup handles sur packages authent. → Kerberos, NTLM, digest, DLL (avec LsaLookupAuthent Package) ④ Winlogon trouve dans LSASS l'authentifiant à chaque pack. d'authent (avec LsaLogonUser) ⑤ LSASS vérifie que user droit se connecter (en regardant ses droits) ⑥ LSASS crée un jeton accès et retourne 1 handle sur le jeton à Winlogon ⑦ Winlogon exécute userinit.exe en y attachant jeton ⑧ userinit.exe charge le profil et exécute le shell de l'utilisateur. | * NTLmv1 = LM ; NTLmv2 = NTLM | hash1 hash2 envoyer au client - authent local (msv 1.0.dll) → vérif base SAM hash mdp. Is possible de s'authent direct avec un hash → attaque穷举 - authent distante (msv 1.0.dll → protocole LM et NTLM ; kerberos.dll ; wedigest.dll) uti l'option de netlogon pr communiquer client / serveur - authent protoc. NTLM (NT Lan Manager) : ① msv 1.0.dll du client récupère les infos et calcule le hash du mdp. ② msv 1.0.dll du client envoie le login de l'user au serveur. ③ msv 1.0.dll du serveur génère et envoie un challenge chell. ④ msv 1.0.dll du client chiffre le login avec le hash du mdp et l'envoie au serveur. ⑤ msv 1.0.dll chiffre le chell avec hash de sa base SAM et compare avec réponse du serveur. NTLmv1 : hash LM ou NTLM - chell serveur = hash NTLM - chell client / user ; hashLM théorique (PSK) ; hash NTLM (MTRN)

- Single Sign-On : Windows garde en mémoire (table de LSASS) certains contenus d'un jeton en dehors des droits de l'utilisateur, des tickets Kerberos
 L'attaque tire la mémoire LSASS (minimally) (notamment avec privilège admin SeDebugPrivilege)

- stockage des secrets : les comptes locaux ds HKLM\SAM & comptes domaine ds base NTDS & mdp en hash LM ou NTDS.

S - système : mécanisme de protection de la base SAM pour protéger d'un attaquant accès physique (2-3) : le mode 1 : secrets chiffrés avec clé dérivée d'1 de HKLM\SYSTEM le mode 2 : secrets chiffrés avec une clé donnée par user au démarrage le mode 3 : secrets chiffrés avec clé stockée sur support amovible (ex: USB) - mécanisme de protection : User Account Control : permet à tous les utilisateurs de s'exécuter avec des droits limités (non admin) même si l'user possède des droits administrateurs.

1. la création de 2 jetons (WinDBG !token) → jeton filtré de droits admin : suppression des SIDs de gr admin (deny-only) + suppression des priviléges admin : Groups S-1-5-32-544-DenyOnly → jeton avec les droits user : Groups-Mandatory Default Enabled Owner

2. par défaut, les processus se voient attribuer le jeton filtré. Si besoin des droits admin, utiliser jeton privilégié → POP UP.

3. élévation priviléges : tag requestedExecutionLevel dans le manifest du binaire (AsInvoker, HighestAvailable, RequireAdministrator)

4. contourner UAC → exploitation de la fonctionnalité anti-élévation (exécuteables corrompus comme virus par Windows → sans popup)

5. - Mandatory Integrity Control : mécanisme qui contrôle l'accès au niveau intégrité aux objets qui s'effectue avant le contrôle d'accès sur les DACL

6. les descripteurs de sécurité des objets ont aussi un niveau intégrité et les ACE définissent les règles d'accès vis à vis de l'intégrité

7. → objets sous niveau intégrité (medium) → objets n'ont pas niveau intégrité du jeton. Le jeton d'accès des processus des utilisateurs ont aussi un niveau d'intégrité et une mandatory policy détermine le comportement face aux niveaux d'intégrité. Les processus respectent le niveau d'intégrité le plus bas entre celui du jeton et celui du fichier exécuté.

8. S-1-16-0x000 contrôlent les processus avec gr Admin

9. S-1-16-0x1000 Low (1) : mode protégé Internet Explorer

10. S-1-16-0x2000 Med (2) : appli normale

11. S-1-16-0x3000 High (3) : utilisé par applics administratifs

12. S-1-16-0x4000 Syst (4) : appli sys (ex: winlogon)

13. les ACE de type SYSTEM-MANDATORY-LABEL ACE des SACL associent un SID de niveau intégrité avec un masque accès. Ce masque peut être : obj SYS-MANDAT-LABEL-NO-WRITE-UP = 1 (compte avec niveau intégrité + bits de masque obj)

14. NO-READ-UP : compte avec niveau intégrité + bits de masque obj

15. NO-EXEC-UP : → exéc obj, pour défaut objets NO-WRITE-UP

16. NO-WRITE-UP : → écrit obj, pour défaut objets NO-EXEC-UP

17. les jetons peuvent avoir mandatory policy qui définit quel jeton/niveau intégrité : TOKEN-MANDAT-POL-CFF(0) = 0 contre niveau intégrité jeton ; NO-WRITE-UP (le jeton jeton ne peut pas écrire sur l'obj) / niveau intégrité 1 / Windows Defender : analyse signature, heuristique, analyse comportement (par exemple, 1 fichier écrit avec 1 niveau intégrité Low décritre de l'obj avec 1 niveau intégrité Medium m si DACL de l'objet autorise cette opération)

18. Windows Firewall = filtre statique (IP, ports...) - Bitlocker = chiffre disque (TPM (génére crypte) et/ou PIN d'un USB) - AppLocker empêcher programmes non autorisés à s'exécuter.

- Active Directory (AD) annuaire : ① centraliser info relatives aux utilisateurs d'un réseau entre eux. ② fournit mécanismes identifiant et authentifiant ③ simplifier & centraliser administration ④ sécuriser accès données ⑤ centralisé si 1 compte privilégié compromis tout est compromis
- Domain Controller (DC) = serveur avec fonctionnalités d'AD et peut avoir plusieurs rôles (serveur DNS, Annuaire LDAP, service authent Kerberos, service gestion config (GPO)). GPO contient copie base domaine (base NTDS) et authent machines + users domaines.
- machine membre = période base locale comptes (SAM). Il est possible de faire des ouvertures de session de comptes locaux ou domaines
- stockage des données d'AD sont stockées ds C:\Windows\NTDS. Diff ou HKLM\SYSTEM\CurrentControlSet\services\NTDS parcoure et stockées dans une bdd ESE contenant des infos sur les objets (y compris users, gr, ordi, doma, Unité Orga, strat scén.). On y trouve empreintes de mdp des utilisateurs du domaine. Les GPO (strat scén) et scripts de connexion s'exécutant à l'ouverture de session des users sont stockés sous C:\Windows\SYSVOL \ annuaire LDAP (ldap) = ① une racine RootDSE qui contient info sur le domaine et le contrôleur (version et nom domaine, version LDAP) ② séparation en Naming Context (NC) : définition classes d'objets et attributs (notion hérédité), partition domaine (users, machines, gr, OU) ③ différences par AD Distinguished Name (DN) ex: CN=Computer, DC=usq, DC=fr | OU=Computers, DC=usq, DC=fr | struct logique: ① domaine = contient 1 ensemble d'unités d'organisation. est identifié par un nom DNS (ex: usq.fr) qui est le nomenclature ② unité d'organisation (OU) = contient généralement qui regroupe d'autres obj (users ou d'autres OU). analogie = dossier ds 1 ms fichier ③ arbre = regar hiérarchique de plusieurs domaines. Les domaines d'un même arbre partagent 1 espace de nom contigu ex: usq.fr - versailles.usq.fr + guyancourt.usq.fr ④ forêt = regar de plus. arbres. 1 ère espace nom. Les relations d'appartenance : permet de mutualiser l'authentification pour que des users d'une forêt A puisse accéder aux ressources de la forêt B avec leurs authent de la forêt A. → 2 aspects: ① direction unidirectionnelle (le domaine A apprend B (A→B) et B peut accéder res A) ou direct bidirectionnel (si A→B et B→C alors A→C) ou non transitivité.
- Group Policy (Strategies groupes) : permettent de gérer la config des machines, des appli et des utilisateurs sur l'ensemble d'un domaine sous la forme de GPO (Group Policy Objects) → long min mdp, bloq accès gest tâches, resto domain, install logiciel, motif politiq.
- stockés ds un obj de GPO appelé CPC (conteneur) → CN=<GroupPolicy>, CN=Policy, CN=System, DC=<domain>; ds C:\Windows\SYSVOL\domain\Policy dans l'autre GPO Link des objets où s'applique la GPO. s'appliquent de cet ordre: local-site-domaine-OU et actu. 90 min groupote
- Réplication (pull) : Knowledge Consistency Checker (KCC) - processus de réplication (intrazone=auto, interzone=manuel)
- authentification par défaut avec Kerberos (client et serveur (kerberos.dll), KDC (kdcsvc.dll)); protocole NTLM peut être utilisé
- contrôle accès : Les obj de l'annuaire possède un descripteur de sécurité. Les gr de sécurité permettent d'organiser les utilisateurs et les autres obj selon des permissions d'accès. Les groupes de distribution sont utilisés pr la distribution de emails uniquement. - privilégié droit d'un compte (user ou gr) d'effectuer des actions système sur la machine (ex: éteindre, ajouter machine domaine) - délegation privilégié: mécanisme pr séparer des privilégiés et permettre à un admin de déléguer contrôle sur objets à des utilisateurs en groupes - archi siile : éviter qu'un admin chasse ses credentials (mdp, secrets stockés) sur le pc
- segmentation du domaine en zones (zone DC sécurité, zone serveur, zone stations) - analyse de chemins de contrôle = succession de relation de contrôle direct entre obj (réalise info AD, générera relations, extraction chemin control graph)
- WSUS (Win Serv Update Service): service permettant de déployer maj (téléch + distib), paramétrable avec GPO.
- assume break = considérer systématiquement qu'un attaquant finira par trouver un point d'entrée.
- première exécution de code: → point d'entrée: menace externe (phishing, exploitation vuln, maladorene web), menace interne (employé, attaque de USB, téléphone, ordinateur, social engineering) ⇒ objectif: avoir une exécution de code au niveau utilisateur et si possible canal contrôlé-commande. → cartographie: fingerprint distant (avance de phase): user agent, entêtes... cartographie passive (après 1ère exec): étude config machines (users, processes, files system, périph, prog), plan adresse, proxy?, netstat, services en écoute, table ARP. → découverte de l'environnement: énumération users, groupes, mails, ping, scan, traceroute, scan réseau → identification des services d'intérêt (info qu'ils contiennent, vuln).
- → contremeasure détection intrusion: surveillance échanges extérieur, P2P anti-spam, flux internes, surveillance journal évén. collecte de logs, politiques de logs: détection par signature et comportementale; segmentation réseau, filtrage, fermeture accès anonymes
- élévation privilégié: → élévation de priviléges (privé); exploitation de vuln non corrigée + failles de configuration / exploit
- élévation de priviléges à distance: attaques sur les services ayant des possibilités d'exécution de code (ex: web, webservice)
- contremeasures: segmentation réseau: principe du mainline privilégié → minimiser les points d'entrée: ne pas laisser config par défaut, identifier les applicatifs à risques (vuln récurrentes) → auditifs scans périodique: audits (vuln), permissions / mmap + mems... ; filtrage réseau: parefeu, VLAN; filtrage applicatif: blocage USB, AppLocker, WER, Sysmon; AppLocker: whitelisted des emplacements où lancer executable → WER: permet de récupérer core dumps de crash d'applications
- mouvement lateral et pénétration: → recherche à infiltrer d'autres systèmes: dump de mdp (ng suite, samdump, mdsniff...), NT (alphabet simplifié, facilement crackable), NTLM (pas the hash) → hash → attaque 2. White hat Admin Domain: ① réutilisation de credentials sur d'autres machines accessibles à distance (mdp, john, pas the hash) ② vol d'autres identifiants (mimikatz, keylogger) ③ Scan réseau ④ réutilisation des identifiants sur plus de machines.
- pénétration de l'accès: → partageant la badgeuse virtuelle → récupération des empreintes de mdp → silver ticket Kerberos: si l'attaquant détient le hash NTLM d'un service, il peut forger un ticket de service (TS) sans passer par le KDC.
- golden ticket Kerberos: si l'attaquant détient le hash NTLM du domaine, il peut forger un TGT pour le TGS.
- Ainsi, le TGS fournit à l'attaquant un TS pour démarrer la communication avec le service.
- exfiltration de données: exfiltration DNS, partition cachée sur USB. - contremeasures: administration en silos + limiter authentification explicite et privilégiée l'authentification implicite (Kerberos).
 - 1) Alice demande à AS de contacter TGS + envoie timestamp chiffré avec Ka-1bis AS génère Ka-tas
 - 2) AS envoie Ka-tas (de session A-TGS) chiffrée avec Ka à Alice. AS envoie TGT (ticket) qui contient (Ka-TGS, Alice, expi) chiffrée avec K-TGS à Alice
 - 3) Alice demande à TGS de contacter service Bob + envoie TGT à TGS
 - 4) Alice envoie son timestamp chiffré avec Ka-TGS à TGS 3bis) TGS génère Ka-b (session a et b)
 - 5) TGS envoie (Ka-b, Bob) chiffré avec Ka-TGS à Alice + envoie TS (ticket service) contenant (Ka-b, Alice, expi) chiffrée avec Kb à Alice
 - 6) Alice envoie TS (Ka-b, Alice, expi) + timestamp chiffré avec Kb à Bob
 - 7) Bob s'authent en envoyant Timestamp + 1 chiffré avec Kb à Alice.
- Forensic: identifier info fiables + centraliser info (logs, process tracking) + dump RAM(volatility) + anturun (lister programmes configurés pr s'exécuter post lancement ou la connexion système), historique USB (setupapi), cache navigation.