Gyakorlat #6.

1. A Windows NT alapú operációs rendszerek biztonsági alrendszere

   A Windows NT alapú operációs rendszerek olyan átfogó és konfigurálható biztonsági szolgáltatásokat nyújtanak, amelyek együttesen kielégítik az USA Védelmi Minisztériuma által a megbízható operációs rendszerekre előírt C2-es TCSEC (Trusted Computer System Evaluation Criteria) szintű biztonsági követelményeket.

   A Windows NT Server és a Windows NT Workstation 3.51 1996. októberben, a Windows NT 4.0 1999. márciusban, a Windows 7 és a Windows server 2008 pedig 2011. márciusában kapta meg a C2-es biztonsági jóváhagyást. A Windows XP, a Windows 2000 és a Windows Vista az EAL4+ (Evaluation Assurance Levels) minősítéssel rendelkezik, ami gyakorlatilag a C2-vel egyenértékű minősítési szint.

   Microsoft Windows Security (Microsoft, angol nyelvű)

   A biztonsági szolgáltatások és a szükséges alapvető tulajdonságaik a következők:

   - A biztonságos logon (bejelentkezés, hitelesítés, autentikálás) lehetősége megköveteli, hogy a felhasználó egyedi logon azonosítóval és jelszóval azonosítsa magát bejelentkezéskor.
   - A tetszőlegesen konfigurálható (discretionary) elérési ellenőrzés lehetővé teszi, hogy egy erőforrás tulajdonosa meghatározza, hogy ki érheti el az erőforrást, és mit tehet vele. A jogosultságok alapvetően csoportoknak adhatók, melyekhez csatlakozhatnak a felhasználók, hogy a csoport hozzáférési jogait átverhessék. (pl. biztonsági házirend, ACL - Access Controll List)
   - A biztonsági auditálás azt a képességet jelenti, amivel a biztonságot érintő események felismerése és feljegyzése történik, beleértve a rendszererőforrások létrehozására, elérésére vagy törlésére irányuló lépéseket. Mindez megkönnyíti az illetéktelen akciót végrehajtó személy kinyomozását.
   - A memóriavédelem megakadályozza, hogy egy jogosulatlan folyamat egy másik folyamat privát virtuális memóriáját elérhesse. Ezen túlmenően a Windows NT garantálja, hogy amikor egy memóriaoldal hozzárendelődik egy felhasználói folyamathoz, ebbe az oldalba soha nem kerülhetnek bele adatok másik folyamattól.

A fenti követelmények teljesítése a Windows NT alapú operációs rendszerek biztonsági alrendszerén és az ahhoz kapcsolódó komponenseken keresztül valósul meg.

2. A biztonsági alrendszer komponensei

   A Windows NT alapú operációs rendszerek biztonságát megvalósító legfontosabb komponensek a következők:

   - Biztonsági referencia monitor (SRM: Security Reference Monitor). Ez a komponens az executive-ban van, tehát kernel módú folyamat (NTOSKRNL.EXE).

     Funkciói: az objektumok biztonsági elérésének ellenőrzése, privilégiumok (felhasználói jogok) kezelése, biztonsági auditálási üzenek előállítása.
   - Helyi biztonsági jogosultság ellenőrző (LSA: Local Security Authority) szolgáltatása. Ez egy felhasználói módú folyamat, az LSASS.EXE image-et futtatja, ami a felhasználók bejelentkezési jogait és jelszavát ellenőrzi, a felhasználóknak és csoportoknak adott privilégiumokat, továbbá a biztonsággal kapcsolatos auditálás üzeneteit küldi az események naplójába.
   - LSA adatbázis. Ez az adatbázis tartalmazza a rendszer biztonságos működésére vonatkozó beállításokat.
   - Biztonsági témaszám kezelő (SAM: Security Accounts Manager) szerver. Ez egy szubrutinok halmazából álló szolgáltató. A szubrutinok a felhasználói neveket és a csoportokat tartalmazó adatbázist kezelik. Ezek a nevek és csoportok vagy a helyi gépre vannak definiálva, vagy – ha a gép egyben tartomány (domain) vezérlő – az adott domainre. Utóbbi esetben a rendszer tartományvezérlő. A SAM az LSASS folyamat környezetében fut.
   - SAM adatbázis. Adatbázis, ami tartalmazza a definiált felhasználókat és csoportjaikat, jelszavukkal és egyéb attribútumaikkal együtt.
   - Logon folyamat. Felhasználói módú folyamat, amely a WINLOGON.EXE-t futtatja. A folyamat a felhasználói nevet és jelszót veszi át, majd elküldi őket az LSA-hoz ellenőrzés céljából, ezután pedig a kezdeti folyamatot hozza létre.
   - Hálózati logon szolgáltatás. Felhasználói módú szolgáltatás a SERVICES.EXE folyamaton belül, amely a hálózati logon kérésekre válaszol. A jogosultságot úgy kezeli, mint a helyi logonokat, azáltal, hogy ellenőrzés végett ezeket is az LSA processzhez küldi el.

Az SRM, ami kernel módban fut, és az LSA, ami felhasználói módban fut, egymás között a helyi eljáráshívás (LPC) révén kommunikálnak.
Az engedélyek fajtáit, az engedélyezés csoportosítását a legalapvetőbb szempontok szerint így ábrázolhatjuk (természetesen más logikus rendezési szempontok is léteznek).
Az engedélyek csoportosítása:

- Kötelezőség szerint
    - Kötelező (mandatory)
    - Belátás szerint / Tetszés szerint (discretionaly)
- Szintek szerint
    - Rendszer szintű
    - Erőforrás szintű
- Típus szerint
    - Cimkézés alapú
    - Hozzáférési lista alapú

Az engedélyek konténer típusú objektumok (pl. könyvtárak) esetében öröklődnek.

A biztonsági rendszer által kezelt alábbi entitások összefoglaló neve a Principal.

- A SID - Security Identifier elemei:
    - user
    - group
    - machine

A SID alapú azonosítás azért szerencsésebb, mint a login név alapú, mert a login név egyszerűen megváltoztatható, míg a SID gépfüggő (gép specifikus). Azaz így meg lehet különböztetni két ugyanolyan nevű, de két különböző gépen létrehozott felhasználót.
A SID tehát a gépet és a felhasználót is azonosítja.

Az adatok a rendszerleíró adatbázisban tárolódnak, és még a rendszergazda sem érheti el azokat.
A gép SID-je itt található:

- HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account

A felhasználók jelszavai pedig itt találhatóak:

- HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users

...de sajna semmi sem látszik egyikből sem a pusztán csak a regedit segítségével...
(...megtekintésükhöz ismerünk egy-két trükköt!)

De, amennyiben rendelkezünk a PsExec programcsomaggal, és elindítunk egy rendszergazda cmd ablakot, majd a megfelelő elérési útba beírjuk ezt:

- psexec -i -s regedit.exe
  akkor megláthatjuk a tárolt jelszavak hash-ét, azaz kódolt adatszerkezetét
- psexec -i -s powershell.exe majd az új ablakban .\psgetsid.exe
  akkor megláthatjuk a gép SID azonosítóját
- psexec -i -s powershell.exe majd az új ablakban .\psgetsid.exe username
  akkor megláthatjuk az adott user SID azonosítóját

Látszik, hogy pl. az én notebook-om SID-je a következő:

- S-1-5-21-4057270313-3181039115-4176737963

és az én user accountom (dave) SID azonosítója a következő:

- S-1-5-21-4057270313-3181039115-4176737963-1006

(az utolsó rész a "1006" a RID - Relative Identifier) Ebből az is látszik, hogy ez a user ezen a gépen lett létrehozva.

A SID értelmezése elemenként (a fenti példa alapján):

- "S": azt jelzi hogy ez az érték (string) egy SID
- "1": a SID verziószáma
- "5": hozzáférési szint (authority level)
- "21-4057270313-3181039115-4176737963": tartomány (domain) vagy gép azonosító
- "1006": felhasználó vagy csoport azonosító (RID - Relative Identifier)

Ismert legfontosabb SID-ek:

- Everyone (mindenki): S-1-1-0
- Administrator (rendszergazda): S-1-5-domain-500

További hasznos információk a témában:
A regisztrált SID-ek a Windows alatt (Microsoft, angol nyelvű)

3. Trükk a hosszú ping idő csökkentésére

   A következő módszer azon online játékosoknak nyújt segítséget, akik néhány játék esetében bosszantóan magas ping időkkel (akár 200-300ms) találkoznak, miközben a hálózat (internet) sebessége elfogadható. A rendszerleíró adatbázis mélyebb bugyrainak ismerete ez esetben is segít.

   Nyissuk meg a HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/services/Tcpip/Parameters/Interfaces nevű kulcsot. Itt általában legalább két olyan kulcsot találunk, melyeknek a neve kapcsos zárójelekben szereplő hexadecimális érték. Ezek közül válasszuk ki azt, amelyikben a gépünk IP címét is megtaláljuk. (DHCP kiosztás esetében a DhcpIPAddress kulcs tartalmazza a gépünk IP címét.)

   A kiválasztott kulcsban létre kell hoznunk két új duplaszót:

   - az elsőt TcpAckFrequency névvel, majd az értékének adjunk 1-et
   - a másodikat TCPNoDelay névvel, majd az értékének adjunk 1-et

   Ez után a beállítás után mindenképpen újra kell indítani a Windowst, hogy a beállítások érvényre jussanak. A ping értéke (amennyiben a hálózat fizikailag nem korlátozza,) biztos, hogy ez után alacsonyabb lesz (a játékunk pedig játszható ☺).

4. További gyorsítások

   A következő három beállítás némi lélektani előnyt jelent, hiszen minden kétséget kizáróan gyorsabb lesz tőle az adott munkafázisok végrehajtása, de azt azért ne reméljük, hogy ettől a gépünk meg fog táltosodni.

   Továbbra is a rendszerleíró adatbázist fogjuk manipulálni.

   - Gyorsítsuk fel a menük megjelenési sebességét
     HKEY_CURRENT_USER/Control Panel/Desktop/MenuShowDelay
     Az ehhez a kulcshoz tartozó 400 milliszekundumos értéket állítsuk kisebbre, akár nullára is. Nulla milliszekundum esetében már egyáltalán nem fog kivárni az operációs rendszer a menük megjelenítésével.
   - Gyorsítsuk fel a betekintő ablakok megjelenési sebességét
     HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/Advanced
     Hozzunk létre egy új duplaszót ThumbnailLivePreviewHoverTime névvel, majd az értékének adjunk 200-at (ez is milliszekundumban értendő). Ezt az értéket nem célszerű nullára csökkenteni. A késleltetés egyébként csak az első betekintő ablakra vonatkozik, például az egymás melletti ablakok esetében.

- Csökkentsük a Windows 7 leállási idejét
  A teljes leállási időnek csak egy részét tudjuk így csökkenteni, azt az időt, amíg az operációs rendszer kivár egy még futó folyamat kényszerített lezárásáig. HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/ WaitToKillServiceTimeOut
  Az ehhez a kulcshoz tartozó 12000 milliszekundumos értékét csökkentsük le például 5000-re, azaz 5 másodpercre (Windows 10 esetében már ez a default érték), vagy esetleg még ennél is rövidebb időre, de semmiképpen sem 1000 milliszekundum alá. (Az 1000 nem kőbe vésett, csak tapasztalati minimum.)

Ezeket követően indítsuk újra a gépet, ami így akár érzékelhetően gyorsabb is lehet. A lényeg nyilván az érezhetőség, mert amit matematikailag megtehettük, azt megtettük ☺. Biztos, hogy gyorsabb a fentiektől tőle az adott munkafázisok végrehajtása, de azt azért ne reméljük, hogy ettől a gépünk meg fog táltosodni.