5.b Ismertesse a Windows operációs rendszerek hitelesítési módjait, a címtárak és a fájlrendszer biztonságát támogató lehetőségeket!

Windows Operációs rendszerek hitelesítési módjai

NTLM

- Microsoft által fejlesztett hitelesítési protokoll, ami Windows operációs rendszerekben használatos.
- Hitelesítési token kerül használatra, ami az adott munkamenetre vonatkozik.
- Token elkészítéséhez szükség van egy hitelesítési szolgáltatóra, ami felhasználó jelszavával és más azonosító adatok alapján állítja elő.

Kerberos

- Nyílt hálózat esetén, jelszavas hitelesítés.
- Egyszeri regisztráció és a hálózati munkamenet teljes ideje alatt megbízhatóvá válik.
- Szimmetrikus vagy titkos kulcsú kriptográfián alapul.
- Egy adatbázisban tárolja a felhasználóit és a privát kulcsokat.
- **Igazolvány**
    - **Jegy (Tartalmazza) = Session key**
        - A kiszolgáló és a kliens nevét
        - Kliens internetes címét
        - Időbélyegét
        - Életciklusát
        - Egy véletlenszerűen generált kulcsot
    - **Hitelesítő (Tartalmazza) = Titkosítva a kapcsolati kulccsal**
        - A kliens nevét
        - IP-címét
        - A munka-állomás aktuális idejét
- **Alany (principal)**
    - Egy egyedi azonosító (felhasználó vagy szolgáltatás), amelyhez jegy rendelhető.
        - **primary:** Az alany első része, ami a felhasználó esetén megegyezhet a felhasználónévvel.
        - **instance:** Elhagyható, a primary mezőt jellemző adatok és ’/’ karakterrel kerül elválasztásra a primary mezőtől.
        - **realm:** Általában a domain neve, nagybetűs karakterekkel.

Kölcsönös hitelesítés

- A kliens és a kiszolgáló egyaránt megbizonyosodhat a másik azonosságáról.
- Közös kapcsolati kulcson osztoznak és ezt használják a titkosított kommunikációra.

Kapcsolati kulcs

- Ideiglenes privát kulcs.
- A kliens ismeri és ezekkel titkosítja a kiszolgáló és a munkaállomás közötti kommunikációt.

A címtár

- Hálózati objektumok (kiszolgálók, kötetek, nyomtatók, hálózat felhasználói, számítógépfiókjai) adatainak tárolására szolgáló hierarchikus struktúra.
    - Felhasználók azonosságának, jogosultságainak ellenőrzése.
    - Megkönnyíti a hálózati erőforrások elérését.
    - A címtár és így a hálózat is központi helyről felügyelhető.
    - A hálózat távfelügyelete automatizálható.

Címtár szükségessége

- **Igény**
    - Sok felhasználó és sok kiszolgálónál is maximális teljesítmény és biztonság.
- **Korábban**
    - Felhasználók nyilvántartása minden kiszolgálón külön-külön.
        - A jogokat mindenhol külön be kellett állítani.
- **Címtárral**
    - A kiszolgálókat és a szolgáltatásokat egy adminisztratív egységbe fogjuk össze.

AD biztonsági rései

- Szerver megrongálható.
- Jogosultsági rések kihasználása és megpróbálják növelni a feltört fiók jogait.
- Bejelentkezési hibák, jele annak, hogy akár egy támadó próbál belépni.
- Távoli bejelentkezésnél elérjük a rendszert, és ha azt látjuk, hogy más országból vagy IP címről jelentkeztek be, akkor a rendszert feltörték.

Minden felhasználónak joga van munkaállomásokat hozzáadni a tartományhoz

- Alapértelmezett beállítás.
- Kockázata, hogy a felhasználók csatlakozhatnak a gépekhez, hogy elérjék a vállalati tartományt is és lehet, hogy nem rendelkezik védelemmel.
- Rendszergazdai jogosultságot szerez, amikor rácsatlakozott a gépre.
- Megoldás, hogy limitáljuk a jogosultságokat.

Túl sok felhasználó egy csoportban

- Veszélyes, mert ha feltörik, akkor máris rendszergazdai jogosultságot szereznek.
- Megoldás, hogy a szükséges csoportoknak adjunk jogokat, akik elengedhetetlenek a rendszerben.

Gyenge jelszó házirend

- Könnyebben feltörhetőek, így a fiókok.
- Összetett jelszavak használata és a minimum jelszó hossz beállítása.

AD biztonságossá tétele

- Felhasználók és csoportok automatizálása.
- Felhasználói engedélyek elemzése.
- Sebezhetőségek, nem használt fiókok elemzése.
- AD naplózása.
- Biztonsági mentések készítése.
- Biztonsági kezelés és jelentéskészítés központosítása, tehát egy konkrét csapat foglalkozzon ezzel.

Fájlrendszer biztonsága

- **NTFS**
    - Alapból a rendszerkönyvtárak írása tiltva van.
        - Ha törlünk egy fájlt a rendszerkönyvtárból, abból nagy bajt is okozhatunk.
    - Deny jog
    - Tulajdon-átvétel
    - Jogosultság kimutatás
        - Kik is férhetnek hozzá.
- Fájl szintű titkosítás az NTFS köteteken
- **Tartományban**
    - Jobb ha egy CA (Certificate Authority) szervertől kapja a felhasználó.
    - Mindkét helyen tároljuk.

NTFS jogosultsági szintek

- **Full control:** Teljes hozzáférés és jogok módosítása.
- **Modify:** Írás, olvasás, törlés.
- **Read & execute:** Megtekintés és alkalmazások futtatása.
- **Read:** Megtekintés
- **Write:** Írás