

OS sérülékenység

• Frissítés szükségessége

- Sérülékenység kihasználásával fontos adatokhoz lehet jutni
- Rosszinducatív bejuttatása
- Belső/külső feltörések
- Megoldás
 - Javítások ellenőrzött és gyors telepítése véd a felsoroltak ellen.
 - Központosított frissítés kezelése
 - Frissítés kezelése automatizálása

• WSUS konfigurálása (Windows Server Update Services)

1. Be kell állítani, hogy a kiszolgáló onnan töltse le a frissítéseket. Upstream Server, ahol két opció közül lehet választani
 - Microsoft Update-ből való szinkronizálás → Microsoft Update-ről tölti le a frissítéseket.
 - Szinkronizálás egy másik WSUS kiszolgálóról
 - Ha már van egy meglévő WSUS kiszolgáló, akkor innen tölti le a frissítéseket.
 - Meg kell adni a kiszolgáló nevét és portját.
2. Proxy szerver megadása → Kiszolgáló, port megadása és opcionálisan a szükséges hitelesítő adatok megadása.
3. Nyelv és Productok beállítása, amit frissíteni szeretnénk.
4. Update Classifications → Frissítési besorolások
 - Kritikus, Biztonsági, Rollup, Driverok, Toolok, stb.:
5. Szinkronizálási ütemterv megadása
 - Manuálisan vagy automatikusan egy adott időpontban és hogy napi hányzor.

• WSUS működése

• Szerver

1. WSUS időzített letöltés
2. Tört?
- A frissítésre tesszük, ha **igen**.
- A csomagok engedélyezése, ha **nem**.

• Kliens

- WSUS frissítés figyelése
- Admin van belépve?
 - Figyelmén kívül hagyhatja a telepítést, ha **igen**.
 - Időzített letöltés és telepítés, ha **nem**.
 - Szükséges a restart?
 - Restart, ha **igen**.
 - Következő ellenőrzésre várakozás, ha **nem**.

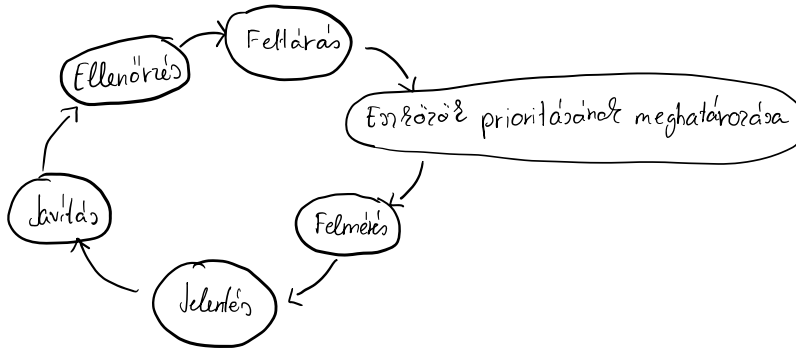
• Biztonsági javítások típusai

- Service pack → Ritkábban kiadott, de nagyobb mértű javítás, ami új elemeket is tartalmazhat.
- Security rollup package → Csak biztonsági javító csomag.
- Hotfix/patch → Kisebbs hibat javít




• Microsoft Baseline Security Analyzer → Szűrőrendszer vizsgálat

- Helyi és távoli szűrőgátló biztonsági hiányosságait igyekszik felderíteni.
- Kiszolgáló fájljait hasonlítja össze egy internetről letöltött XML adatbázissal.
- Megmutatja, hogy milyen javítások hiányozhatnak.
- Ellenőrzi a beállításokat és ha azokat nem találja biztonságosnak, akkor jelzi az észlelt jelentősben
- Egy tapasztalt szakértőt szimulál, aki ellenőrzi a gépen futó szoftvereket és beállításokat, hogy azok mennyire biztonságosak.

• Szűrőrendszer vizsgálat életciklusa



• Szűrőrendszer vizsgálat módjai

- Black box → A vizsgálat az infrastruktúra előzetes ismerete nélkül. 
- Gray box → A vizsgálat feltételezi a vizsgált infrastruktúra részleges ismeretét. 
- White box → A vizsgálat előtt a tesztelő megismeri a teljes infrastruktúrát, a hálózati diagramokat, forráskódot, az IP cím információkat. 

• Web alkalmazások elleni támadások

- Oka → Hagyományos támadások a hálózati / OS rétegből indulnak, ma már az alkalmazás réteg.
- Kód tartalmazhat kritikus biztonsági hibákat → Sok idő megjavítani.
- OWASP → Open Web Application Security Project
 - Nyitott figyelési rendszer
 - Web alapú biztonsági rendszert vizsgálja és optimalizálja.

• Hibás fejlesztői szemlélet

- Minden működik, nem fog elromlani.
- Feltehetően

• Alapvető fejlesztési hibák

- Hibaérzékelés hiánya → Tartalmaz fontos információkat, amivel vissza lehet élni.
- Brute force belépés → Captcha használata!
- SQL Injection input mezőből → input mező szabályozása
- Nincs tesztelés → DE KELL = Unit, TDD

• Felderítés

- Hacsak nem meg kell ismernie a célba vett rendszert.
- Információk szerezhetőek:
 - Utadói táblázatból
 - Internetes keresőktől → például google dorking
 - DNS szerverektől
 - Közvetlen vizsgálati technikák → nmap

• Leggyakoribb támadási formák

- XSS → Cross-site Scripting
 - Idegen parancsok végrehajtása
 - Káros javascript kód
- Információszivárgás
- SQL Injection
- Váratlan kód kombináció
- Szolgáltatás megsemmisítés
 - Denial of Service (DoS)
 - Egyetlen gépről indított támadás szolgáltatás megtagadásnak nevezzük → DoS
 - Több gépről indított támadás elosztott szolgáltatás megtagadásnak nevezzük → DDoS

• Bűntetteléség

- Számítógépes bűncselekmény
- Jogszulatlan hozzáférés géphez → Betörés
- Jogszulatlan hozzáférés adatbázishoz → Lopás
- Adatok másolása, módosítása, hamisítása, törlése vándalizmusnak számít.

• Lehetőséges biztonsági intézkedések

- Böngésző oldalon
 - Nem engedélyezzük a scriptek automatikus letöltését.
 - Hivatkozások ellenőrzése
- Webserver oldalon
 - Leért adatok korlátjainak beállítása
 - script, object, embed beágyazott elemek törlése.
 - Adatbevitel csak HTTP POST-tól fogadjunk el.
 - Sütiik ellenőrzése
 - Speciális karakterek szűrése