11.b Mutasson rá a szerverek és munkaállomások operációs rendszereinek sérülékenységeire! Mutasson példát az Operációs rendszerek szabályozásoknak való megfelelésének vizsgálati lehetőségeire (pl. MS MBSA). Ismertesse a szoftverjavítások, szoftverfrissítések fontosabb típusait, valamint vázolja a szoftverfrissítéseket támogató infrastruktúra kialakítási lehetőségét!

Frissítés szükségessége

- Sérülékenység kihasználásával fontos adatokhoz lehet jutni.
- Rosszindulatú kód bejuttatása.
- Belső/külső feltörések
- **Megoldás:**
    - Javítások ellenőrzött és gyors telepítése véd a felsoroltak ellen.
    - Központosított frissítéskezelés.
    - Frissítéskezelés automatizálása.

WSUS konfigurálása

1. Be kell állítani, hogy a kiszolgáló honnan töltse le a frissítéseket. **Upstream Server,** ahol két opció közül lehet választani:
    - **Microsoft Update-ből való szinkrinozálás:**
        - A 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**
    a. Kiszolgáló, port megadása és opcionálisan a szükséges hitelesítő adatok megadása.
3. **Nyelv és Productok kiválasztása, amit frissíteni szeretnénk.**
4. **Update Classifications**
    a. Frissítési „besorolásokat” lehet kiválasztani:
        i. Kritikus
        ii. Biztonsági
        iii. Rollup
        iv. Driverek
        v. Toolok
        vi. stb
5. **Szinkronizálási ütemterv megadása**
    a. Manuálisan vagy automatikusan egy adott időpontban és hogy napi hányszor.

WSUS működése

- **Szerver**
    1. WSUS időzített letöltés
    2. Teszt?
        a. A frissítések tesztelése, ha igen.
        b. A csomagok engedélyezése, ha nem.
- **Kliens**
    1. WSUS frissítés figyelése.
    2. Admin van belépve?
        a. Figyelmben kívül hagyhatja a telepítést, ha igen.
        b. Időzített letöltés és telepítése.
            i. Szükséges a restart?
                1. Restart, ha igen.
                2. Következő ellenőrzésre várakozás, ha nem.

Biztonsági javítások – Patch Management

- **Típusai**
    - **Service Pack**
        - Ritkábban kiadott, de nagyobb méretű javítás, ami új elemeket is tartalmazhat.
    - **Security Rollup Package**
        - Csak biztonsági javító csomag.
    - **Hotfix/Patch**
        - Kisebb hibákat megjavít.

Microsoft Baseline Security Analyzer

- Sérülékenysége vizsgálat
- Helyi és távoli kiszolgálók biztonsági hiányosságait igyekszik felderíteni.
- Kiszolgáló fájljait hasonlítja össze egy internetről letöltött XML állománnyal.
- Megmutatja, hogy milyen javítások hiányoznak.
- Ellenőrzi a beállításokat, és ha azokat nem találja biztonságosnak, akkor jelzi az elkészült jelentésben.
- Egy tapasztalt szakértőt szimulál, aki ellenőrzi a gépen futó szoftverek és beállítások mennyire biztonságosak.

Sérülékenység vizsgálat életciklusa

- Feltárás
- Eszközök prioritásának meghatározása
- Felmérés
- Jelentés
- Javítás
- Ellenőrzés

Sérülékenysége vizsgálat módjai

- **Black box:** A vizsgálat az infrastruktúra előzetes ismerete nélkül történik.
- **Gray box:** A vizsgálat feltételezi a vizsgált infrastruktúra részleges ismeretét.
- **White box:** A vizsgálat előtt a tesztelők megismerik a teljes infrastruktúrát, a hálózati diagramokat, forráskódot, az IP cím információkat.

Web alkalmazások elleni támadások

- **Oka**
  - Hagyományos támadások a hálózati/operációs rendszer rétegből indultak, ma már az alkalmazás réteg.
- **Kód tartalmazhat kritikus biztonsági hibákat**
  - Sok idő megjavítani.
- **OWASP = Open Web Application Security Project**
  - Nyitott fejlesztési rendszer
  - Web alapú biztonsági rendszereket vizsgálják és optimalizálják.

Hibás fejlesztői szemlélet

- A fejlesztett webalkalmazás működőképes, azt csinálja. amit kell.
- Munkamenet-azonosító felhasználóként.
- Munkamenet megszakítás.
- Autentikáció, autorizáció
- Adatok védelme, adatbázis
  - Illetéktelenek nem férhetnek hozzá, így megfelelően biztonságos.

Alapvető fejlesztési hibák

- Hibakezelés hiánya
  - Tartalmaz fontos információkat, amivel a támadó vissza tud élni!
- Sérülékenységek felhasználhatóak arra, hogy állományokat lehessen letölteni.
  - Kiderül az OS típusa.
- Bruteforce belépés
- A felhasználó névnél nem csak felhasználónevet fogad el egy alkalmazás, hanem egy SQL lekérdezést is végrehajthat.
- Tesztelésre nem marad idő.

Fejlesztési hibák megoldása

- Felhasználónév és jelszó külön-külön ellenőrzése.
- Adminisztrátor ne az első bejegyzés legyen a felhasználókat tartalmazó táblában.
- SQL Injection-höz használt karakterek letiltása.

Felderítés

- Hackernek meg kell ismernie a célba vett rendszert.
- Információk szerezhetőek
  - Útadó táblázatokból
  - Internetes keresőktől (Google dorking)
  - DNS szerverektől
  - Közvetlen vizsgálati technikák

Szoftver sérülékenység

- Programozási hibák, amiket a hacker kihasznál.
- Szoftverek kiadásával nem szoktak várni addig, amíg tökéletesen nem működik.
- Patchek, javítások

Védelem

- Szoftver sérülékenységek ellen a patchek és upgrade csomagok használata a legjobb és legegyszerűbb.
    - Kevesen frissítik az operációs rendszert és az alkalmazásokat.

Leggyakoribb támadási formák

- Cross-Site Scripting
    - Idegen parancsok végrehajtása.
    - Káros javascript kód.
- Információszivárgás
- SQL Injection
    - Ne jelenítsük meg az SQL hibaüzenetet.
- Beviteli korlátozások megkerülése
    - Nem a szerver végzi el az ellenőrzéseket, hanem a kliens.
- Váratlan kód kombináció
    - Ártalmatlannak tűnő paranccsal más programok befolyásolása.
- Szolgáltatás megbénítás
    - Denial of Service (DoS)
        - Egyetlen számítógépről indított támadás szolgáltatásmegtagadásnak nevezzük. (DoS)
        - Több számítógépről indított támadás elosztott szolgáltatás megtagadásnak nevezzük. (DDoS)
    - Büntethető
        - Számítógépes bűncselekmény
        - Számítógéphez való jogosulatlan hozzáférés = Betörés
        - Adathoz való jogosulatlan hozzáférés = Lopás
        - Adatok másolása, módosítása/hamisítása, tönkretétele/vandalizmusnak számít.

Lehetséges biztonsági intézkedések

- Böngésző oldalán
    - Ne engedélyezzük a scriptek automatikus lefuttatását.
    - Hivatkozások ellenőrzése.
- Webszerver oldaláról
    - Lekért adatok korlátjainak beállítása.
    - script, object, embed beágyazott elemek törlése.
    - Adatbevitel csak http POST-tól fogadjunk el.
    - Sütik ellenőrzése.
    - Speciális karakterek szűrése.