Jegyzőkönyv

Biztonság és védelem az informatikában c. tárgy

5. feladat

Készítette:

Csomor Bence, TVIK4I

2021.03.17.

**Windows, Linux Hardening**

A legtöbb cég egy új szolgáltatás bevezetése vagy éppen egy új operációs rendszer, hálózati eszköz telepítése során a kiépítés, illetve installálás végeztével teljesen befejezettnek tekinti a fejlesztést.

Ahhoz, hogy a rendszerünket a megfelelő biztonsági szinten tartsuk, nem elégedhetünk meg az egyszeri felülvizsgálattal, hiszen ahogyan egy ház is folyamatos karbantartást és javítást igényel, a már megvizsgált beállítások időszakonkénti ellenőrzése, módosítása is elengedhetetlen.

A számítás során a Hardening általában a rendszer biztonságossá tételének folyamata a sérülékenységi felület csökkentésével, amely nagyobb, ha a rendszer több funkciót lát el. Elvileg az egyfunkciós rendszer biztonságosabb, mint a többcélú. A rendelkezésre álló támadási módok csökkentése általában magában foglalja az alapértelmezett jelszavak megváltoztatását, a felesleges szoftverek, a felesleges felhasználónevek vagy bejelentkezések eltávolítását, valamint a felesleges szolgáltatások letiltását vagy eltávolítását.

Sok weboldal tartalmaz részletesebbnél részletesebb útmutatót Hardeningre. Van olyan amely a Windows Serveréhez ad részletes Hardening útmutatót, mint például a ” <https://www.upguard.com/blog/the-windows-server-hardening-checklist> „ oldalon található. Ezen az oldalon minden lépést megtalálhatunk Windows Serverünk védelmének ellenőrzésére és annak fenntartására.

Egy másik hasznos oldalon egy régebbi Windows rendszerhez találunk egy igen terjedelmes Hardening útmutatót. Ez a weboldal itt található:

„ <https://docplayer.hu/24406663-Sep2-kiberbiztonsagi-muveleti-kozpont.html> „

Itt a részletes útmutató mellett rengeteg letölthető fájl, szoftver (pl.: antivírus szoftver) linkje is megtalálható, amik hasznosak és egyszerűen elérhetőek innen.

A „ <http://www.itsecure.hu/biztonsagi_utmutatok/virtualizacio> „ oldalon szinte minden, a témával kapcsolatos Hardening útmutató elérhető. Különböző pdf tartalmakat tölthetünk le a kívánt útmutatóval.

**Windows Server 2016 Hardening lépések:**

*1. Hálózati biztonság*

* Statikus IP-k beállítása a szerverekhez. Ez biztosítja, hogy a megfelelő szervert érje el a kapcsolatok létrehozásakor.
* Szegmentálja hálózatát. Azok az állomások, amelyek ugyanazon az alhálózaton / Vlan-on vannak, könnyebben maszkírozhatók, mint a kiszolgáló. A szegmentálás segít ennek kezelésében.
* Hálózati tűzfal hozzáadása.
  + Ügyeljen arra, hogy tiltson le minden olyan szolgáltatást, amelyet nem használ, például az IPv6-ot.
  + A nem használt portokon tiltsa le a bejövő forgalmat is.
* Használjon másodlagos DNS-kiszolgálókat a terheléselosztáshoz és a redundanciához.
  + Több DNS-kiszolgálóval rendelkezzen a visszalépés engedélyezéséhez.
* Minden szervernek rendelkeznie kell (DNS-ben):
  + Rekord
  + PTR rekord

*2. Konfigurálja az idő szinkronizálását*

* A tartományvezérlőkön lévő idő szinkronizálása egy-egy réteg külső időszerverrel.
  + Szintén szinkronizálja az időt a nem tartományi kiszolgálókon egy külső NTP-kiszolgálóval.
  + Külső NTP-kiszolgálóra támaszkodva véd az NTP-alapú DDoS támadások ellen.
* Ezenkívül ellenőrizze, hogy a szerverek megfelelő időzónára vannak-e állítva (naplózáshoz stb.)

*3. Győződjön meg arról, hogy a Windows Server naprakész az összes telepített javítással*

* Ha lehetséges, frissítse az összes meglévő kiszolgálót a legújabb Windows Server rendszerre.
  + A kritikus frissítéseket a lehető leghamarabb alkalmazni kell. Ezeket a frissítéseket először tesztkörnyezetekben alkalmazza a megfelelő működés megerősítéséhez, majd a gyártás során, ha nincsenek kompatibilitási problémák.
* Ügyeljen arra, hogy frissítse az összes többi használatban lévő Microsoft-terméket, mint például az Exchange Server és az SQL Server.
* Frissítsen más, harmadik féltől származó alkalmazásokat is egy szokásos ütemben.

*4. Konfigurálja a Windows tűzfalat*

* A forgalmat csak azokra a kikötőkre korlátozza, amelyeknek nyitva kell lenniük a szolgáltatások számára. Például a webkiszolgálóknak hozzáférést kell biztosítaniuk a 80 és 443 TCP portokhoz a legtöbb felhasználó számára, de nincs szükség RDP hozzáférésre minden forrásból.
* A felügyeleti hozzáférést (pl. RDP, WMI stb.) Csak azokra az IP-kre és hálózatokra korlátozza, amelyek a rendszergazdákhoz tartoznak.

*5. Biztonságos és titkosítsa a távoli hozzáférést*

* Az RDP-hez csak az arra jogosult rendszergazdák férhetnek hozzá.
  + A Távoli asztali felhasználók csoport metszése.
* A Telnet és más titkosítatlan felügyeleti protokollokat le kell tiltani az egész környezetben.
* Csak titkosított távoli hozzáférést használjon:
  + SFTP
  + SSH (VPN hozzáférésből)

*6. A szükségtelen szolgáltatások korlátozása*

* Tiltsa le a felesleges szolgáltatásokat.
* Speciális szolgáltatásfiókok beállítása, lokálisan vagy az Active Directoryban, az alkalmazás- és felhasználói szolgáltatásokhoz.
  + Ily módon az alkalmazások sérülése esetén a támadónak korlátozott felhasználói jogai vannak, nem teljes rendszerű vagy privilegizált felhasználói jogokkal.

*7. Tiltsa le a helyi rendszergazdákat, és biztosítsa a rendszergazdai jogokat*

* Legalább készítsen biztonságos jelszót a helyi rendszergazdák számára.
* Ne használja újra az adminisztrátori jelszavakat az egész környezetben.
  + Rendszeresen változtassa meg a rendszergazdai jelszavakat, hogy megakadályozza a jelszavak szivárgását új megsértésekhez.
  + Erős jelszószabályzat érvényesítése az alábbi szempontok felhasználásával:
  + Összetettség és hosszúság
  + Lejárat
  + Újrafelhasználási irányelv
* Engedélyezze a fiók zárolását ismételt sikertelen próbálkozások esetén.
* Hozzon létre egy új fiókot (az Active Directory-ban, vagy lokálisan, ha a környezet nem használja az AD-t), és adja hozzá a Rendszergazdák csoporthoz.
  + Használjon nem rendszergazdai felhasználói fiókot a normál üzleti tevékenységhez.
  + Használja a „Futtatás másként” funkciót adott alkalmazások futtatásához rendszergazdai jogosultságokkal, ha szükséges.
* Tiltsa le a helyi vendégfiókokat.

*8. Konfigurálja a felhasználói hozzáférés-vezérlést (UAC)*

* Ezek a házirend-beállítások a Helyi házirendek biztonsági beállításai részben találhatók a Helyi biztonsági házirend beépülő modulban.

*9. Távolítsa el a felesleges keretrendszereket és csomagokat a Windows szolgáltatásain keresztül*

* Alapértelmezés szerint távolítsa el a Windows Server alkalmazásban található alkalmazásokat, de a környezetben nem használható.

*10. Végezze el a tevékenységnaplózást*

* Szilárdítsa a naplókat gyűjtési naplók segítségével egy központi helyre.
* Készítsen biztonsági másolatot a naplókról az adatvesztés megelőzése érdekében.
* Figyelje és elemezze a naplókat a támadók, a szélhámos eszközök és a gyanús használati minták azonosításához.

**10 biztonsági lépés a számítógéped „megerősítéséhez” és az üzleted megvédéséhez:**

1. Tiltsa le a Windows 10 automatikus bejelentkezését.

2. Állítson be egy jelszót a képernyővédővel.

3. Kapcsolja be a tűzfalat.

4. Tiltsa le a távoli hozzáférést.

5. Engedélyezze vagy telepítse a víruskereső eszközöket.

6. Engedélyezze az automatikus frissítéseket az operációs rendszeréhez.

7. Állítsa be a fájlmentéseket.

8. Kapcsolja be a titkosítást.

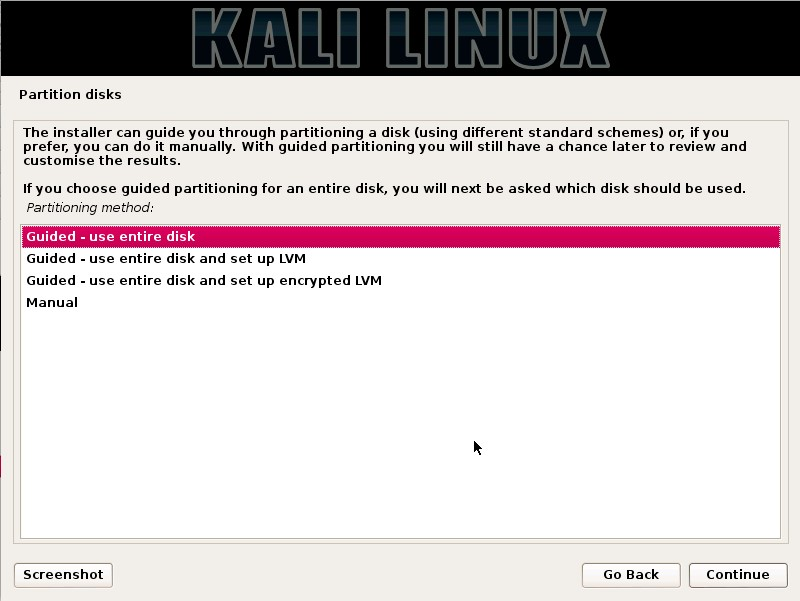
9. Állítsa be felhasználói fiókjait.

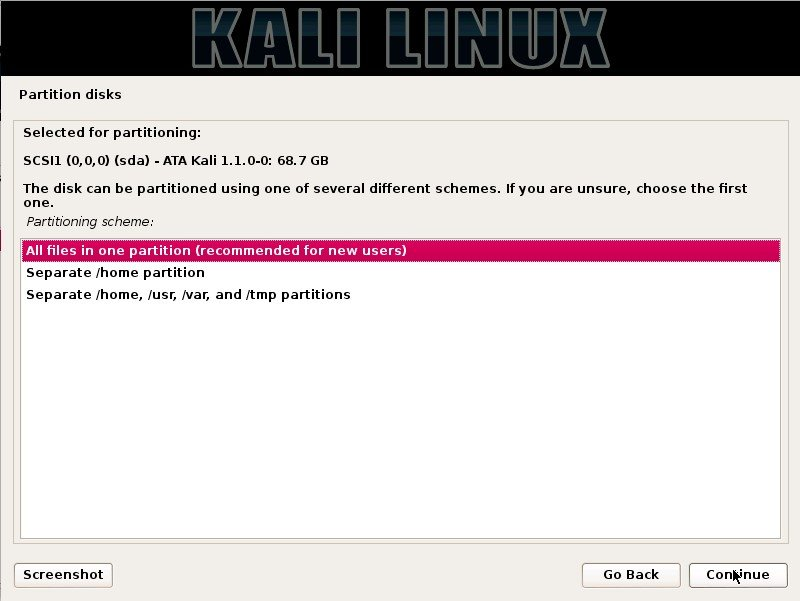
10. Állítson be egy jelszókezelőt.

**Linux Hardening lépések:**

1. Dokumentálja a gazdagép adatait

2. BIOS védelem

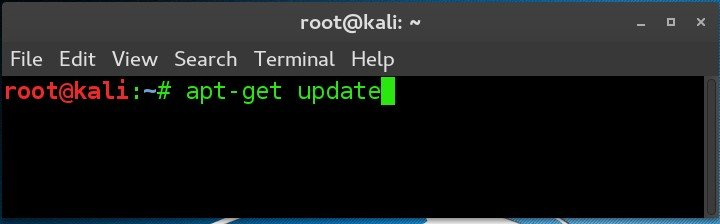
3. Merevlemez-titkosítás (titoktartás) 

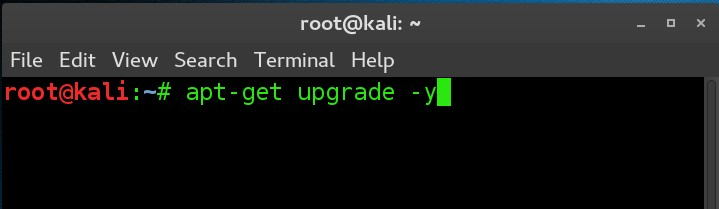
4. Lemezvédelem (elérhetőség) 

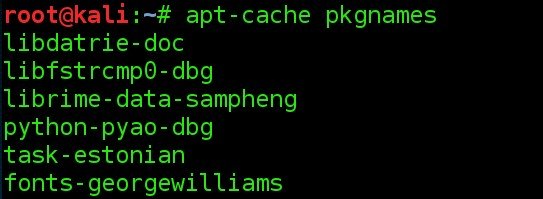
5. Zárolja a rendszerindító könyvtárat

6. Tiltsa le az USB használatát

7. Rendszerfrissítés





8. Ellenőrizze a telepített csomagokat

9. Ellenőrizze a nyitott portokat



10. Biztonságos SSH



11. Engedélyezze a SELinuxot

12. Hálózati paraméterek

13. Jelszópolitikák

14. Engedélyek és ellenőrzések

15. További folyamatkeményedés

A Windows és a Linux operációs rendszere is elég erős a legtöbb „támadás„ ellen, viszont egyik sem képes minden kártevőt és biztonsági rést detektálni és megszűntetni. Erre egy jó megoldás a Hardening, melynek segítségével szinte minden téren biztonságban tudhatjuk eszközünket.

A Windows alapvetően egy elég biztonságos rendszer, de nem árt időnként vagy legalább közvetlen a telepítés után elvégezni a Hardening lépéseket.

A Linux is egy alapjáraton meglehetősen biztonságos OS, de mint mindegyiket, így ezt is sok veszély fenyegetheti. Linux esetén a rendszeres Hardening ajánlott, így képes biztosítani a kifogástalan védelmet és biztonságot adataink és rendszerünk számára.

források: <https://nador.hu/hu/biztonsagi-hardening-es-monitoring>

<https://en.wikipedia.org/wiki/Hardening_(computing)>

<https://www.tevora.com/10-essential-baseline-security-hardening-considerations-windows-server-2016/>

<https://www.linkedin.com/pulse/hardening-windows-10-rafael-hart>

<https://www.securicy.com/blog/security-best-practices-hardening-windows-10/#auto-login>

<https://www.pluralsight.com/blog/it-ops/linux-hardening-secure-server-checklist>