

1.a Ismertesse a határforgalomirányítók védelmének különböző területeit, majd mutassa be az egyes területeken alkalmazható megoldásokat!

Határforgalomirányító

- Hálózat külső és belső rendszerének határán található eszköz.
- **Célja**
 - o Adatintegritás és adatvédelem megvalósítása.
- **Védelme**
 - o Legelső szenzitív pont
 - o Hálózatnak az első védelme

Védekezés

Eszköz védelem - Router hardening

- Jelszavas védelem
- AAA – (Authentication, Authorization, Accounting)
- Privilege level

Fizikai védelem

- Zárt, jól szellőző terem
- Port védelem
 - o IDS/IPS

Szoftver védelem

- Nem használt szolgáltatások letiltása

AAA

Authentication

- Hitelesítés megvalósítható felhasználónév jelszó párokkal, kihívás és válasz üzenetekkel, token, smart cards

Authorization - Jogosultságkezelés

- Mely erőforrásokhoz férhetnek hozzá a felhasználók, milyen műveleteket végezhetnek

Accounting – Könyvelés

- Naplózza → mit csinált/változtatott a felhasználó, milyen erőforrást és mennyi ideig ért el

AAA Authentication

- Felhasználónevek és jelszavak tárolása
 - Local
 - lokálisan a Cisco forgalomirányítókban tárolja, ez alapján hitelesíti a felhasználókat.
 - Kis hálózatokban
 - Server-based
 - központi AAA szerveren
 - Több hálózati eszközt tartalmazó hálózat esetén

Szerver alapú AAA megvalósítására használható protokollok

	TACACS+	RADIUS
Funkcionalitás	AAA-t részekre osztja, modularitást lehetővé teszi	Kombinálja az hitelesítést és a jogosultságkezelést, külön könyvelés. Ezáltal nem olyan rugalmas, mint a TACACS+
Támogatottság	Cisco	Nyitott/RFC standard
Szállítási protokoll	TCP	UDP
CHAP	Kétirányú hívás és válasz, mint a Challenge Handshake Authentication Protocol (CHAP)	Egyirányú a RADIUS szerver és kliens között
Bizalmasság	Egész csomag titkosított	Csak a jelszó titkosított
Testreszabhatóság	biztosítja az útválasztó parancsok jogosultságkezelését felhasználónként vagy csoportonként	nem biztosítja
Könyvelés	Limitált	Széleskörű

IDS és IPS rendeltetése

- Behatolás érzékelő eszközöknek a hálózat kritikus forgalmat átbocsátó pontjaira helyezésével a nem kívánt vagy jogosulatlan forgalom érzékelése és valós idejű beavatkozás is elvégezhető.

IDS és IPS alapfunkciók

- **Érzékelik**
 - o Gyanús csomagokat
 - o Illegális tevékenységre utaló adattartalmakat
 - o Normálistól eltérő forgalom mintákat
 - o Küszöb értékeket meghaladó mennyiségű csomagokat
 - o IDS jelzi a behatolás tényét
 - o IPS valós időben ellenintézkedéseket tesz a támadás megelőzésére

Tervezési megfontolások

- **Védelem:** Biztonsági politika kialakítása és megvalósítása megfelelő technológia alkalmazásával.
- **Érzékelés:** Támadások észlelése
- **Elhárítás:** Válaszlépés megtétele
- **Értékelés:** Kockázatelemzés, ellenintézkedések és költség/haszon elemzés
- **Javítás:** Kiválasztott ellenintézkedések megvalósítása

Szolgáltatások és lehetőségek

IDS

- **Előnyei:** Nem érinti negatívan a hálózati forgalmat.
- **Hátrányai:** Nem skálázható és a rosszindulatú csomag célba juttatását nem akadályozza meg.

IPS

- **Előnyei:**
 - o Single-packet támadásokat megállítja
 - o Real-time figyel a forgalmat
 - o Harmadik és negyedik rétegben figyel
- **Hátrányai:**
 - o Negatívan érinti a hálózati teljesítményt (latency, jitter)
 - o Kieséskor megszakad a forgalom

1.b Mutassa be a kockázatkezelés szerepét az informatikai biztonság megteremtésében, valamint ismertesse a kockázatkezelési ciklus fő lépéseit!

Kockázat kezelésének módszerei

- A kockázatmenedzsment célja a kockázat hatékony csökkentése és a biztonság növelése.
- Kockázati tényező kezelésének eszközei
 - o A kockázat csökkentése megfelelő szintű védekezéssel
 - o Kockázat áthárítása
 - o Tudatos kockázatvállalás

Védekezés

- A bekövetkezési valószínűségek és az okozott károk csökkentésével valósulhat meg.
- **Kockázatcsökkentés alapszerei**
 - o Bekövetkezési valószínűség csökkentése.
 - o Veszélyforrás kiküszöbölése.
 - o Okozott kár nagyságának korlátozása, csökkentése.
- **PreDeCo**
 - o **Preventive:** Megelőző, kivédő kontrollok
 - o **Detective:** Felismerő kontrollok
 - o **Corrective:** Elhárító, helyreállító kontrollok
- Egy kontroll cél biztosítására tett védelmi intézkedések ebből a három védelmi mechanizmus ötvözéséből tevődnek össze.
- Bekövetkezési valószínűség csökkenthető erősebb védelmi mechanizmus alkalmazásával.

Kockázatáthárítás

- Ha a kár bekövetkezését megakadályozását már nem tudjuk, akkor a kockázat és ezzel a károk áthárítása orvosolhatja a problémát.
- Áthárítás másik módja biztosítás kötése.

Tudatos kockázatvállalás

- Célszerűtlenül nagy költségekkel lehet védekezni.
 - o Veszélyforrás által jelentett kockázat vállalható, de tisztában kell lennie ezekkel a kockázatokkal.
- Felső vezetésnek kell a döntést meghoznia és jóváhagynia.

Kockázatkezelési ciklus fő lépései

Kockázatkezelés lépései

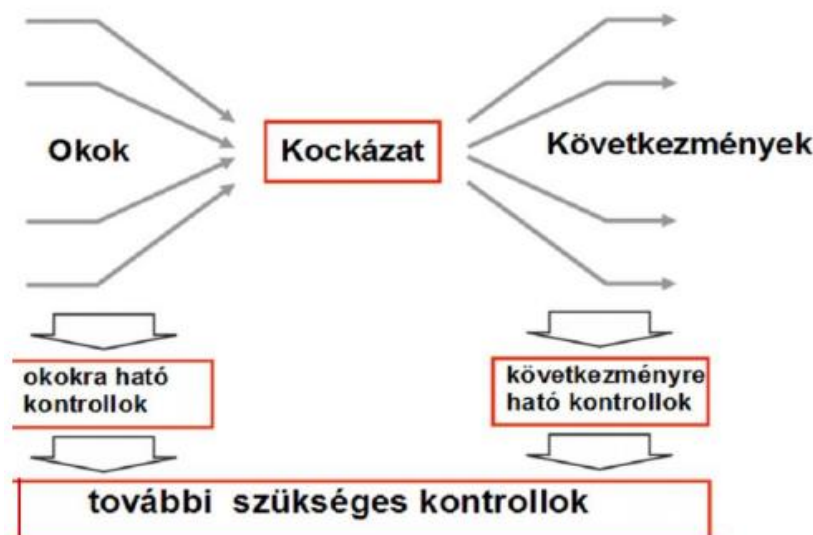
1. Kezelési opciók azonosítása
2. Opciók értékelése
3. Alkalmazni kívánt eszközök, intézkedések kiválasztása
4. Kezelési terv kidolgozása

Kockázatkezelés célja

- Célja az értékelt, rangsorolt kockázatok kockázati tényezőinek kezelésére alkalmas kontrollok meghatározása vagy a már meglévők módosítása.
- Kulcsfontosságú kockázatok kezelésére kell koncentrálni, a kontrollok meghatározása mellett a kockázathordozó munkatársakkal és vezetőikkel kommunikálni a lehetséges megoldásokról.
- A kezelhetőségi vizsgálat és a hatásvalószínűség alapján lehet dönteni arról, hogy mely kockázatok kerüljenek az ellenőrzési nyomvonalba.
- A kockázatok kezelésének módját minden egyes kockázatnál külön meg kell határozni.

Kockázatok mérlegelése

- A kockázat sajátosságainak mérlegelése alapján vagy a kockázati tényezőket, okokat vagy a következményeket célszerű kezelni.



Felülvizsgálás

- A szervezet kockázatprofilját és az ahhoz illeszkedő kontrollokat rendszeresen felül kell vizsgálni és újra értékelni, hogy a kockázatprofil továbbra is érvényes legyen.

Kockázatkezelési terv készítése, kezelési folyamat dokumentálása

- Célja a kockázatkezelési lehetőségek közül kiválasztott intézkedések megvalósítási módjának rögzítése, mely alapul szolgál mind a módszerek és eszközök, mind pedig a teljes folyamat javításához.
- A kockázatkezelés érdekében kialakított intézkedéseket, azok felelőseit, határidőit, a monitoring eljárásokat szintén a kockázatkezelési tervbe kell foglalni.
- Az intézkedési terveket irányítási folyamatba kell integrálni, és egyeztetni kell az érdekelttekkel.

2.a Mire szolgál a lokális és a központosított AAA (Authentication, Authorization Accounting)? Ismertesse a szerver-alapú megvalósítás lehetőségeit és a beállítás menetét!

AAA – **A**uthentication **A**uthorization **A**ccounting

Hogyan volt eddig?

- Legegyszerűbb hitelesítési módszer: login és password
 - console, vty és aux line-on
- Könnyű implementáció, nem biztonságos
- Telnet, SSH
 - Biztonságosabb, van accounting
 - Lokális adatbázishoz felhasználónév kell
 - Naplózza a rendszer
 - Minden eszközön helyileg kell konfigurálni

Jobb megoldás

- Tartalék megoldásokat is konfiguráljunk (ha valami meghibásodik)
- Minden eszköz egy központi szerver adatbázisára épít
 - Egyszerre kezeli a hitelesítést, jogosultságkezelést

AAA felügyeli

- Hálózatot
 - Ki érheti el (authentication)
 - Mit tehet (authorization)
 - Mit csinált (accounting)

AAA komponensek - keret a hozzáférés felügyeletére

Authentication

- Hitelesítés megvalósítható felhasználónév jelszó párokkal, kihívás és válasz üzenetekkel, token, smart cards

Authorization - Jogosultságkezelés

- Mely erőforrásokhoz férhetnek hozzá a felhasználók, milyen műveleteket végezhetnek

Accounting – Könyvelés

- Naplózza → mit csinált/változtatott a felhasználó, milyen erőforrást és mennyi ideig ért el

AAA Authentication

- Felhasználónevek és jelszavak tárolása
 - Local
 - lokálisan a Cisco forgalomirányítókban tárolja, ez alapján hitelesíti a felhasználókat.
 - Kis hálózatokban
 - Server-based
 - központi AAA szerveren
 - Több hálózati eszközt tartalmazó hálózat esetén

Local AAA Authentication működése

1. kliens kapcsolatot létesít a forgalomirányítóval
2. Az AAA router felhasználónevet és jelszót kér
3. Router hitelesíti a felhasználót és a jelszavát a lokális adatbázis alapján
4. Adatbázisban tárolt információ alapján a felhasználó jogosult a hálózat használatára

Server-Based AAA Authentication működése

1. kliens kapcsolatot létesít a forgalomirányítóval
2. AAA router felhasználónevet, jelszót kér
3. router hitelesíti a felhasználót és a jelszavát a távoli szerver alapján
4. szerveren tárolt információ alapján a felhasználó jogosult a hálózat használatára

Jogosultság-kezelés (szerver alapú)

- Hitelesítés után automatikusan: felhasználó által kért szolgáltatásokra engedélyt kér a forgalomirányító a szervertől.
 - Milyen erőforrásokat érhet el/műveleteket hajthat végre?
 - AAA authorization egy nevesített listával konfigurálható, interfészhez kell rendelni
 - Privilege level, role-based CLI-hez hasonlóan jogokat biztosít
1. hitelesítése után egy viszony alakul ki a router, szerver között
 2. felhasználó megpróbál privilegizált EXEC módba lépni, a router visszaigazolást kér az AAA szervertől, rendelkezik-e a jogokkal?
 3. AAA szerver visszaküld egy "PASS/FAIL" választ

AAA Accounting

Jegyzőkönyvezi a használt adatokat: kezdés, végzés időpontja, parancsok, küldött/fogadott csomagok száma

1. felhasználó hitelesítése után egy start üzenetet generál, a könyvelés megkezdődik
2. kijelentkezést stop üzenet követi, lezárul a könyvelés

AAA előnyei

- Skálázhatóság, rugalmasság
 - Központi konfiguráció (lokális adatbázist routerenként kellene)
- Több backup rendszer használata → hiba esetén más hitelesítési módszerek
 - Szabványos hitelesítési módszerek
 - RADIUS - Remote Authentication Dial-In User Service
 - TACACS+ - Terminal Access Controller Access Control System Plus
 - Diameter

Local Authentication konfigurálása

1. Lokális adatbázis konfigurálása: *Username ADMIN algorithm-type scrypt secret Password*
2. AAA engedélyezése: *aaa new-model*
3. Hitelesítési lista: *aaa authentication login*
 - milyen hitelesítési módszert vegyen figyelembe és hogy milyen sorrendben
 - Megfelelő interfészhez rendelése

Felhasználói fiókok kizárása

- Ha a sikertelen belépési kísérletek száma meghalad egy értéket
 - *aaa local authentication attempts max-fail number-of-unsuccessful-attempts*
- sikertelen belépések közt eltelt idő beállítása
 - *login delay*

Szerver alapú AAA megvalósítására használható protokollok

	TACACS+	RADIUS
Funkcionalitás	AAA-t részekre osztja, modularitást lehetővé teszi	Kombinálja az hitelesítést és a jogosultságkezelést, külön könyvelés. Ezáltal nem olyan rugalmas, mint a TACACS+
Támogatottság	Cisco	Nyitott/RFC standard
Szállítási protokoll	TCP	UDP
CHAP	Kétirányú hívás és válasz, mint a Challenge Handshake Authentication Protocol (CHAP)	Egyirányú a RADIUS szerver és kliens között
Bizalmasság	Egész csomag titkosított	Csak a jelszó titkosított
Testreszabhatóság	biztosítja az útválasztó parancsok jogosultságkezelését felhasználónként vagy csoportonként	nem biztosítja
Könyvelés	Limitált	Széleskörű

Diameter – a RADIUS továbbfejlesztése

- Kapcsolatorientált, TCP vagy SCTP – port 3868, megbízható
- Ugrástól ugrásig, Végpont-Végpont biztonság
- Alkalmazási és biztonsági szint egyeztetése
- Szerver által kezdeményezett üzenetet használ
- Statikus, dinamikus konfiguráció
- Gyártó specifikus tulajdonságok és üzenetek

Szerver alapú AAA konfigurációs lépései

1. AAA engedélyezése globális konfigurációs módban: *aaa new-model*
2. Security paraméterek konfigurálása: Server IP, kulcs (az adatok titkosításához)
3. Hitelesítési lista konfigurálása: *aaa authentication*
4. Megfelelő interfészhez rendelés

Globális konfigurációs módban opcionális

- Jogosultságkezelés: *aaa authorization*
- Könyvelés: *aaa accounting*

2.b Ismertesse a felhasználó- és hozzáférés kezelés problémáit, gyengeségeit, integrált, központosított megoldási lehetőségeit!

Felhasználó és hozzáférés kezelés

- Identity and Access Management (IAM)
- Segítségével azonosítják, hitelesítik és engedélyezik a felhasználók hozzáférését az adatokhoz, alkalmazásokhoz és szolgáltatásokhoz.
- **Négy A-ből tevődik össze:**
 - o Admisztráció
 - **Felhasználó/Identitás kezelés**
 - o Autentikáció – Ki vagy?
 - **Hozzáférés kezelés**
 - o Autorizáció – Mit akarsz csinálni?
 - **Hozzáférés kezelés**
 - o Audit
 - Azt a célt szolgálja, hogy megbizonyosodjunk arról, hogy biztosan jól csináltuk az **Adminisztráció-t**, **Autentikáció-t**, **Autorizáció-t**.

IAM rendszer problémák, megoldások

Megfelelő hozzáférés a megfelelő személyek számára

- **Probléma**
 - o A felhasználók rendelkeznek nem szükséges jogokkal.
- **Megoldás**
 - o Biztosítja, hogy a felhasználók a számukra nem szükséges bizalmas információk elérésének lehetővé tétele nélkül hozzáférjenek azokhoz az erőforrásokhoz, amikre szükségük van.

Akadálytalan munkavégzés

- Fontos a felhasználói élmény.
- **Problémák**
 - o Többszöri bejelentkezések és jelszavak bekérése.
- **Megoldás**
 - o Single-Sign-On (SSO) bevezetése, amivel csak egyszer kell bejelentkezni a felhasználóknak.

Adatbiztonsági incidensek elleni védelem

- **Probléma**
 - o Adatbiztonsági incidensek kockázata
 - o Feltörések
- **Megoldás**
 - o További biztonsági réteget ad hozzá a bejelentkezési folyamathoz.

Adattitkosítás

- **Probléma**
 - o Bizalmas adatok nincsenek védve.
- **Megoldás**
 - o Titkosítás használata, például AES, RSA vagy SHA megoldásokkal.
 - o Használhatunk titkosítást az adatok tárolására, adatátvitelkor vagy a hitelesítő adatokhoz.

Kevesebb manuális munka az informatikai részlegen

- **Probléma**
 - o Olyan funkciók automatizálása, amik elengedhetetlenek, mint például a jelszó alaphelyzetbe állítása, fiók zárolásának feloldása, anomáliák érzékelése.
- **Megoldás**
 - o Naplózás
 - o Funkciók automatizálása
 - o Ezáltal az informatikai részlegen dolgozók idejét és energiáját megspórolja, így tud foglalkozni a magasabb prioritású feladatával.

IAM és megfelelőségi szabályozások

- Lehetővé teszik az identitások ellenőrzését és kezelését, illetve a gyanús tevékenységek észlelését és az incidensek jelentését, amik mind szükségesek a megfelelőségi követelmények teljesítéséhez.
- A megfelelő IAM-rendszer használata megkönnyíti a követelmények teljesítését.
 - o GDPR (Európai általános adatvédelmi rendelet)
 - o HIPAA (Egészségbiztosítási hordozhatósági és elszámoltathatósági törvény)
 - o Egyéb adatvédelmi szabványok (Pl.: amerikai Sarbanes-Oxley törvény)

IAM technológiák és eszközök

- **SAML:** Egyszeri bejelentkezést teszi lehetővé.
- **OpenID Connect (OIDC):** OIDC identitási aspektust ad hozzá a OAuth 2.0-hoz, ami egy engedélyezési rendszer.
 - o **OAuth 2.0:** Például bejelentkezhetünk egy másik szolgáltatás segítségével a saját alkalmazásunkba. (Gmail, Facebook segítségével mondjuk)
 - **Ezáltal nem kell regisztrálnunk manuálisan fiókot.**
- **SCIM:** A szervezetek szabványosított módon kezelhetik a felhasználói identitásokat, ami több alkalmazáson és megoldáson (szolgáltatón) működik.

IAM megvalósítása

- Az IAM-rendszerek minden részlegre és felhasználóra kiterjednek.
- Emiatt az IAM-megoldás sikeres üzembe helyezéséhez az implementáció előtti alapos tervezés kell.
- **Lépések**
 1. Ki kell számolni, hogy hány felhasználónak kell hozzáférnie és összeállítani a szervezet által használt megoldások, eszközök, alkalmazások és szolgáltatások listáját.
 - a. **Ezek a listák segítenek az IAM-megoldások összehasonlításában annak érdekében, hogy kompatibilisek legyenek a szervezet meglévő informatikai beállításával.**
 2. Fontos feltérképezni azokat a különböző szerepköröket és helyzeteket, amikhez az IAM-rendszernek alkalmazkodnia kell.
 - a. **Ez a keretrendszer lesz az IAM-rendszer architektúrája és képezi az IAM dokumentációjának alapját.**
 3. Hosszú távú ütemterv készítése, mivel a szervezet növekedésével és terjeszkedésével az IAM-rendszer igényei változni fognak.
 - a. **A növekedés előre megtervezése biztosítja, hogy az IAM-megoldás megfeleljen az üzleti céloknak és lehetővé tegye a hosszú távú sikerességét.**

3.a Ismertesse az ISR (Integrated Services Router) forgalomirányítókön megvalósítható hitelesítési és jogosultságkezelési megoldásokat!

Integrated Services Router (ISR)

- Sokkal megbízhatóbb és biztonságosabb az általános routerknél.
- A Cisco ISR lehetővé teszi a biztonságos **felhőalapú computing**-ot a **Group Encrypted Transport Virtual Private Network** segítségével.
 - o **Emiatt biztonságosabb a kommunikáció**
- Sokkal drágább, mint egy általános router, mert extra licenszt vagy modulokat kell vásárolni.

AAA

- Felügyeli a hálózatot
 - o Ki érheti el (authentication)
 - o Mit tehet (authorization)
 - o Mit csinált (accounting)

AAA komponensek - keret a hozzáférés felügyeletére

Authentication

- Hitelesítés megvalósítható felhasználónév jelszó párokkal, kihívás és válasz üzenetekkel, token, smart cards

Authorization - Jogosultságkezelés

- Mely erőforrásokhoz férhetnek hozzá a felhasználók, milyen műveleteket végezhetnek

Accounting – Könyvelés

- Naplózza → mit csinált/változtatott a felhasználó, milyen erőforrást és mennyi ideig ért el

AAA Authentication

- Felhasználónevek és jelszavak tárolása
 - o **Local**
 - lokálisan a Cisco forgalomirányítókön tárolja, ez alapján hitelesíti a felhasználókat.
 - Kis hálózatokban
 - o **Server-based**
 - központi AAA szerveren
 - Több hálózati eszközt tartalmazó hálózat esetén

AAA előnyei

- Skálázhatóság, rugalmasság
 - Központi konfiguráció (lokális adatbázist routerenként kellene)
- Több backup rendszer használata → hiba esetén más hitelesítési módszerek
 - Szabványos hitelesítési módszerek
 - RADIUS - Remote Authentication Dial-In User Service
 - **Hálózati hozzáférésre használják inkább**
 - TACACS+ - Terminal Access Controller Access Control System Plus
 - **Eszközkezelésre (device management) tervezték**
 - Diameter (RADIUS továbbfejlesztése)

Szerver alapú AAA megvalósítására használható protokollok

	TACACS+	RADIUS
Funkcionalitás	AAA-t részekre osztja, modularitást lehetővé teszi	Kombinálja az hitelesítést és a jogosultságkezelést, külön könyvelés. Ezáltal nem olyan rugalmas, mint a TACACS+
Támogatottság	Cisco	Nyitott/RFC standard
Szállítási protokoll	TCP	UDP
CHAP	Kétirányú hívás és válasz, mint a Challenge Handshake Authentication Protocol (CHAP)	Egyirányú a RADIUS szerver éskliens között
Bizalmasság	Egész csomag titkosított	Csak a jelszó titkosított
Testreszabhatóság	biztosítja az útválasztó parancsok jogosultságkezelését felhasználónként vagy csoportonként	nem biztosítja
Könyvelés	Limitált	Széleskörű

Az IOS különböző privilegizált szintjei által kínált lehetőségek kihasználása, beállítása

0. Szint

- Előre definiált felhasználói szintű hozzáférés
- Ritkán használt
- Parancsok: **disable**, **enable**, **exit**, **help**, **logout**

1. Szint – User Exec Mode

- Router CLI-vel történő bejelentkezés alapértelmezett szintje.
- Felhasználó nem hajthat végre változtatásokat és nem tekintheti meg a futó konfigurációs fájlt.

2. Szint – 2-14 Szint

- Testreszabható a felhasználói szintű jogosultságokhoz.
- Alacsonyabb szintek parancsai magasabb szintre hozhatóak.
- Magasabb szintek parancsai lejjebb vihetőek alacsonyabb szintre.

3. Szint – 15 Szint – Privileged Exec Mode

- Engedélyezési mód jogosultságainak fenntartva.
- Felhasználók megtekinthetik és módosíthatják a konfigurációt.

Hátrányok

- **Hierarchikus**
 - o Egy szinten definiált parancsok a magasabb szinten mind elérhetők.
 - o A magasabb szinten definiált parancsok az alacsonyabb szinten nem elérhetők.
- **Több parancsszóból álló parancs**
 - o Ha több parancsszóból álló parancsot definiálunk egy szinthez, minden parancs alkalmazható lesz az adott szinten, amiben az adott parancsszavak valamelyike megtalálható.
- **Nem lehet korlátozni**
 - o Nem lehet korlátozni az egyes felhasználók meghatározott porthoz vagy interfészhez történő hozzáférést.

```
R1# conf t
R1(config)# username USER privilege 1 secret cisco
R1(config)#
R1(config)# privilege exec level 5 ping
R1(config)# enable secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 secret cisco5
R1(config)#
R1(config)# privilege exec level 10 reload
R1(config)# enable secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 secret cisco10
R1(config)#
R1(config)# username ADMIN privilege 15 secret cisco123
R1(config)#
```

A szerep-alapú elérést korlátozó megoldás lényege, előnyei és konfigurálása

Lényege

- **Parser view**
- VIEW-kat, vagyis nézeteket hoz létre.
- A VIEW-k nem hierarchikusan szerveződnek.
- A parancsok specifikusabban rendelhetők a VIEW-hoz.
- **Root View** szükséges a **View** és **SuperViews** meghatározásához (Parancsokat tartalmaznak)
- Egy parancs több VIEW-ban is megjelenhet

Előnye

- VIEW és SuperViews létrehozása és módosítása csak gyökérnézetből lehetséges.
- Különbség a szerep-alapú menedzsment és a jogosultság alapú 15. szintje között az, hogy csak a Root View felhasználó hozhat létre vagy módosíthat View és SuperViewt.

Konfigurálása

Step 1

Router#

```
enable [view [view-name]]
```

Step 2

Router(config)#

```
parser view view-name
```

Step 3

Router(config-view)#

```
secret encrypted-password
```

Step 4

Router(config-view)#

```
commands parser mode {include | include-exclusive | exclude} [all]  
[interface interface-name | command]
```

3.b Ismertesse a behatolás érzékelő és megelőző rendszerek (IDS/IPS) célját, típusait, működési elveit!

IDS és IPS rendeltetés, alapfunkciók, tervezési megfontolások, lehetőségek, szolgáltatások

IPS és IPS rendeltetése

- Behatolás érzékelő eszközöknek a hálózat kritikus forgalmat átbocsátó pontjaira helyezésével a nem kívánt vagy jogosulatlan forgalom érzékelése és valós idejű beavatkozás is elvégezhető.

IDS és IPS alapfunkciók

- **Érzékelik**
 - o Gyanús csomagokat
 - o Illegális tevékenységre utaló adattartalmakat
 - o Normálistól eltérő forgalom mintákat
 - o Küszöb értékeket meghaladó mennyiségű csomagokat
 - o IDS jelzi a behatolás tényét
 - o IPS valós időben ellenintézkedéseket tesz a támadás megelőzésére

Tervezési megfontolások

- **Védelem:** Biztonsági politika kialakítása és megvalósítása megfelelő technológia alkalmazásával.
- **Érzékelés:** Támadások észlelése
- **Elhárítás:** Válaszlépés megtétele
- **Értékelés:** Kockázatelemzés, ellenintézkedések és költség/haszon elemzés
- **Javítás:** Kiválasztott ellenintézkedések megvalósítása

Szolgáltatások és lehetőségek

IDS

- **Előnyei:** Nem érinti negatívan a hálózati forgalmat.
- **Hátrányai:** Nem skálázható és a rosszindulatú csomag célba juttatását nem akadályozza meg.

IPS

- **Előnyei:**
 - o Single-packet támadásokat megállítja
 - o Real-time figyeli a forgalmat
 - o Harmadik és negyedik rétegben figyel
- **Hátrányai:**
 - o Negatívan érinti a hálózati teljesítményt (latency, jitter)
 - o Kieséskor megszakad a forgalom

Host alapú IPS megoldások jellemzői, alkalmazása, előnyök és hátrányok

Host alapú IPS megoldás lényege

- Lényege, hogy a kliensre egy szoftvert telepítenek, ami monitorozza a gépen végzett tevékenységeket.
- **Előnyei:**
 - o Oprendszerre tipikus támadásokat figyeli
 - o Szokásostól eltérő műveleteket is detektálja
- **Hátrányai:**
 - o Csak lokális
 - o Minden gépen implementálni kell
 - o Nem ismeri az egész hálózatot, mivel a hálózat legvégén van

A hálózat alapú IPS megoldások jellemzői, alkalmazása, eszközei, előnyök és hátrányok

Hálózat alapú IPS megoldás lényege

- Host-based szenzorok nem tudják megvédeni a hálózatot, ezért fontos a hálózati szenzorok alkalmazása.
 - o Ezeket a szenzorokat a hálózat megfelelő pontjaira kell telepíteni a maximális biztonság elérése céljából.
- **Előnyei:**
 - o Költséghatékony
 - o Hálózaton transzparens
 - o Alacsony szintű hálózati eseményeket is látja
- **Hátrányok**
 - o Titkosított forgalmat nem látja
 - o Nem tudja a támadás sikerességét

Hálózati alapú IPS megoldások eszközei

- **Port mirroring:** A bejövő csomagokat tovább küldi a cél felé és le is másolja és elküldi egy meghatározott portján az analizáló eszköz felé.
 - o CISCO SPAN (switched port analyzer) egy cisco implementációja

A „signature” alapú IPS rendszerek működése, jellemzői, alkalmazása

- Olyan biztonsági megoldások, amik a hálózati forgalom ellenőrzésére használnak aláírásokat.
- Ezek az aláírások egyedi azonosítók, amik a hálózati támadásokra jellemző mintákat és jellemzőket tartalmazzák.
- Figyelik a hálózati forgalmat és ha találnak egy aláírást, akkor riaszt. (Rendszergazdának szól)
- Gyors reakcióideje van
- Magas fokú pontosság és könnyű kezelhetőség.
- Javasolt olyan környezetekben használni, ahol a hálózati forgalom ellenőrzése és szabályozása fontos szempont.

A minta-, az anomália-, a policy es a „Honeypot” alapú érzékelés sajátosságai

Minta alapú

- Előre definiált mintákat keres a forgalomban.
- Atomi és összetett mintákat is felismer.
- **Előnye:** Könnyen konfigurálható és kevesebb hibás pozitív eredmény.
- **Hátrányai:**
 - o Eddig nem ismert hibákat nem tudja felismerni.
 - o Kezdetben sok a hibás pozitív eredmény.
 - o Mintákat folyamatosan frissíteni kell.

Anomaly/Anomália

- Normál profilt létre kell hozni, ahol meg kell határozni mi a normális működés és minden ami attól eltér, az negatív.
- **Előnyei:**
 - o Ismeretlen támadási fajta detektálható
 - o Elég normális mintát meghatározni, nem kell minden támadási fajtra mintát írni.
- **Hátrányai:**
 - o Nem mondja meg pontosan milyen támadás történik.
 - o Meg kell határozni a normál működést.
 - o Tanulási időszakban biztosan támadásmentesnek kell lenni a hálózatnak, különben az lesz a normális.

Policy alapú

- Nem mintákat határoz meg, hanem viselkedéseket.
- Riaszt, ha x csinál y-t.
- Mindenre alkalmazkodik.
- **Előnye:** Ismeretlen támadások detektálása
- **Hátrányai:**
 - o Nehéz nagy profilokba kategorizálni a hálózati forgalmat nagy hálózaton
 - o Nem változhat a hálózati forgalom profilja

HoneyPot

- Álszervereket állít a hálózatba, hogy azt támadják.
- Adatokat gyűjt a különböző támadásokról, így finom hangolva az IDS, IPS szenzorait.
- Biztonsági cégek alkalmazzák kutatás céljából.
- **Előnyei:**
 - o Megtéveszti, lelassítja a támadókat
 - o Információkat gyűjt a támadásról
- **Hátrányai:** Dedikált szerver, eszközt igényel

A riasztások veszélyességi fokozatai, a riasztások kezelése, téves riasztás típusok

Riasztások típusai

- **False positive:** Elvárt, de nem kívánt riasztás.
- **False negative:** Rendszer nem ismeri fel a támadást.
- **True positive:** Helyesen ismeri fel a támadást.
- **True negative:** Helyes működésnél nem riaszt.

Riasztások kezelése

- Figyelmeztetés
- Logolás
- Aktivitás megszakítása
- TCP kapcsolat reset
- Jövőbeli kapcsolat blokkolása
- Engedélyezés

4.a Milyen feladat elvégzésére alkalmasak a tűzfalak? Ismertesse a különböző tűzfal architektúrákat és típusokat!

Tűzfalak feladata és rendeltetése

- Szoftveres vagy hardveres hálózatzbiztonsági eszköz.
- A tűzfalak a hálózatba be és kimenő kapcsolatokat figyelik, és csak azokat engedélyezik, amik megfelelnek a beállított szabályoknak.
- **Előnyei:**
 - o Nem befolyásolják negatívan a hálózat működését és biztonságot nyújt
- **Hátrány:**
 - o Általános szabályok alapján működnek.
 - o Letilt olyan kapcsolatokat, amik nem is veszélyesek.
 - o Lehet, hogy lassítja a hálózat működését, így a szolgáltatások minősége romolhat.
 - o Nem megfelelő konfiguráció esetén, nem lesz jó a védelem.
 - o Nem véd olyan kapcsolatokról, amik nem mennek rajta keresztül

Tűzfalak generációi és fejlődésük

Első generáció – Packet Filtering Firewall

- **Döntését ezekre alapozza:**
 - o Forrás / Cél MAC címe, ip címe és port száma
 - o IP csomagba beágyazott protokoll

Működése

- A csomag fejlécében lévő információt **összeveti a tűzfalban megadott szabályokkal.**
- A hálózati és szállítási rétegben működik, adattartalmat nem figyel.
- Alacsony szintű biztonságot nyújt, mert nem vizsgálja a csomag tartalmát.
- Nem kezeli a kapcsolatállapotot
- Kétirányú forgalmat külön szabályokkal kell megadni
- Egész port tartományt engedélyezni kell, mert sok protokoll dinamikus választ portot kliens oldalon.

Második generáció – Stateful Firewalls (OSI 5. rétegben dolgozik)

- Tartalmakat vizsgál és figyelembe veszi a felépített kapcsolatokat.
- Figyeli az összes áthaladó hálózati csomagot és megállapítja, hogy:
 - o melyik már egy meglévő kapcsolat része
 - o melyik kezdeményez új kapcsolatot
 - o melyik csomag nem része egyik kapcsolatnak sem
- A felépített kapcsolat információt gyorsítótárban tárolja.
- A kapcsolat csomagjait a gyorsítótárban lévő bejegyzésekkel hasonlítja össze (hatékony)

Előnyei

- Jobban le lehet írni a hálózati szabályokat (állapotokat).
- Nagyobb biztonságot nyújt, mint a csomagszűrő tűzfalak (sorszámokat folyamatosan követi)

Hátrányai

- Állapotok kezelése miatt erőforrás igényes és nem mindig képesek megkülönböztetni a biztonságos és a veszélyes adatokat a csomagokban.

Harmadik generáció – Application Level Firewall

- **Két kategóriája van:** Proxy tűzfalak – Proxy Firewalls, Mély csomag ellenőrző – Deep Packet Inspection

Előnyei

- Biztonságos, és a puffer túlsordulás típusú támadásoknak ellenáll, mert figyeli a protokoll fejléc mezőinek hosszát.

Hátrányai

- Erőforrás igényes, nem megfelelő megvalósításnál gyenge teljesítmény
- Transzparencia hiánya

Proxy firewalls

- A közvetlen kapcsolat megszakad, a továbbítandó csomagot újraelőállítják, átmásolják az összes protokollréteg szükséges mezőit.
- Alkalmazás szinten képes a parancsok szűrésére.

Deep Packet Inspection Firewalls

- Transzparensten működik, nem épít fel külön kapcsolatot a két kommunikáló fél között.
- Egyszerre szűri az OSI modell mind a 7 rétegét.
- Figyeli a protokollnak nem megfelelő csomagokat és szűri azokat.
- Csomagokat az alkalmazásoknak megfelelően osztályozza.

Next Generation Firewalls

- Több hálózatzbiztonsági technológia együttes integrációja.
- Olyan megoldás, ami DPI tűzfalat, IDS/IPS eszközöket, antivirus átjárót, proxy megoldást, VPN kiszolgálót, QoS és sáv szélesség menedzsmentet biztosít, hogy a lehető legjobban kielégítse a mai kor igényeit.

Lehetséges Tűzfal topológiák

Dual-Homed

- Két interfésszel rendelkezik, amik külön hálózatba csatlakoznak és közöttük szűri a hálózati forgalmat.
- Speciális esete, amikor a router a tűzfal (screening router)

Single-Homed - Screened host

- A szolgáltatást nyújtó (bástya) gép csak a belső hálózatra csatlakozik.
- Elsődleges biztonságot a csomagszűrő forgalomirányító adja, ami megakadályozza, hogy a felhasználói gépek közvetlenül hozzáférjenek az internethez.
- Csomagszűrő forgalomirányítót úgy konfigurálják, hogy az internet gépei csak a bástya géppel léphetnek érintkezésbe.
- Bástya gép biztonsága fontos és proxy-ként működik.
- **Előnyei:**
 - o A screened host architektúra nagyobb biztonságot nyújt, mint a dual-homed host architektúra és nincs Single Point Of Failure
- **Hátránya**
 - o Screened subnet architektúra biztonságosabb
 - o Ha a támadó betört a bástya gépre, onnan már a többi gépet is eléri a LAN hálózaton.

Single-Homed - Screened subnet

- Screened subnet architektúra újabb biztonsági réteget helyez el az internet és a belső hálózat felé, ez a határ (perimeter) hálózat.
- **Bástya gép sebezhető**
 - o Ha a támadó bejut a bástya gépre, még mindig útját állja a belső forgalomirányító.
- **Perimeter hálózat**
 - o Ha a támadó bejut a bástya gépre, csak a perimeter hálózat forgalmát lehallgatja, a belső hálózat forgalmát nem láthatja.
 - o A perimeter hálózaton megy keresztül a bástya gép és az internetre irányuló forgalom, de két belső gép egymás közötti forgalma nem.
- **Bástya gép**
 - o A bejövő forgalom kezelésének helye
 - o **A kifelé irányuló szolgáltatások két módon kezelhetők:**
 - Belső és a külső forgalomirányítók csomagszűrő szabályainak beállításával.
 - Proxy szerverek futtatásával a bástya gépen.
- **Belső router (Choke router)**
 - o Szabályozza, hogy a belső hálózatról melyik szolgáltatások érhetőek el közvetlenül.
 - o Szabályozza a belső hálózat és a bástya gép közötti forgalmat.
- **Külső router (Access router)**
 - o Védi a perimeter és a belső hálózatot az internet felől.
 - o Minden forgalmat kienged a perimeter hálózatról.

Multi-Homed

- Három vagy több interfésszel rendelkezik, amik külön hálózatban csatlakoznak és közöttük szűri a hálózat forgalmát.

Routereken megvalósítható tűzfalak

CBAC – Context-based access control

- **Állapottartó szűrés – Stateful Packet Filtering**
 - o Nem csak hálózati és szállítási réteg információk alapján vizsgálja a viszonyok állapotát, hanem alkalmazási réteg információkat is.
- **Forgalom figyelés – Traffic Inspection**
 - o SYN flood támadások, TCP sorszámozást figyel és gyanúsakat eldobja.
- **Behatolás érzékelés – Intrusion Detection**
 - o A syslog üzenetek átvizsgálásával ki lehet szűrni az smtp támadások és SYN flood támadások sajátosságait, ezeket a kapcsolatokat eldobja és riasztást, értesítést küld a rendszernek.

CBAC működése

- TCP, UDP és ICMP kapcsolatokról információt tárol az állapot táblában. (state table)
- Állapot tábla alapján dinamikusan ACL-t hoz létre a visszajövő csomagok számára.
- CBAC ideiglenes nyílásokat hoz létre megadott kapcsolathoz, amik beengedik a blokkolt forgalmat.
- Az állapottábla automatikusan frissül a forgalom áramlásának megfelelően.

ZPF

- ACL-től független
- Mindent tiltunk, amíg külön nem engedjük
- Könnyen értelmezhető
- Házirend minden forgalom hatással van, így nem kell több ACL/ellenőrzési művelet.

ZPF funkciói

- **Inspect**
 - o Automatikusan beengedi a válasz forgalmat.
 - o Támogatja azokat a protollokat, amik több párhuzamos kapcsolat felépítését igénylik.
- **Pass**
 - o Hasonló az ACL permit-hez.
 - o Nem követi a kapcsolat állapotát
 - o Csak egy irányban engedi át a forgalmat
 - o Megfelelő szabványt kell alkalmazni a válaszforgalom beengedésére
- **Drop**
 - o Hasonló egy ACL deny-hoz
 - o Blokkolt csomagok naplózása

ZPF, ZBF szabályok

- Egy zónát először konfigurálni kell.
- Egy interfész egy biztonsági zónához rendelhető.
- Egy zónához tartozó interfészek közötti forgalom engedélyezett.
- Különböző zónák közötti forgalom engedélyezéséhez policy-t kell konfigurálni.
- Egy zónabeli és egy nem zónabeli interfész közötti forgalom nem engedélyezett.
- Zónák között: **pass, inspect, drop** események definiálhatóak.
- Nem zónához tartozó interfészen CBAC-ot lehet konfigurálni.

Zónák

- Self zone
- DMZ
- Privát
- Publikus/Internet

4.b Ismertesse az informatikai rendszerek főbb elemeit és azok sérülékenységeit, valamint a tipikus védelmi megoldási formákat!

Informatikai rendszer

- Az adatok kezelésére használt elektronikus eszközök, eljárások és az ezeket kiszolgáló és a felhasználó személyek együttese.
- Egymással szervesen együttműködő és kölcsönhatásban lévő elemek összessége.

Adatkezelés

- Adatok gyűjtése, felvétele, tárolása, feldolgozása, továbbítása, törlése, hasznostása és a felhasználásuk megakadályozása.

Informatikai rendszer elemei

- A környezet infrastruktúra elemei
- A rendszerelemekkel kapcsolatba kerülő személyek
- Hardver elemek
- Szoftver elemek
- Adathordozók, adatok, dokumentumok
- A kommunikáció elemei

Sérülékenységek

A környezet infrastruktúra

- Nem védett, helytelenül tervezett átviteli vezetékek.
- Cégen kívüli személyek bent tartózkodása.
- Nem felügyelt munkálatok az épületekben vagy azokon kívül (ablak tisztítás, építési munkálatok)
- Informatikai berendezések nem védett helyezete
- Gyenge belépési biztonság

Hardver elemek

- A készülékek kismértékű súlya, így könnyen lopható
- Ütésérzékeny

Szoftverek

- Specifikációs hiba, helytene program-előállítás
- Nincs hitelesítés, implementálási hibák
- Bonyolult felhasználói felület
- Hiányos dokumentáció
- Titkosító algoritmus ismerete
- Gyenge jelszavak, változtatás hiánya
- Vírusfertőzés
- Távolról való adminisztráció

Adathordozók

- Nem védett tárolás
- Kapcsolható írásvédelem
- Érzékenység
- Ellenőrizetlen használat
- Újrafelhasználhatóság elégtelen kezelése

Dokumentumok

- Hiányos dokumentálás
- Nem védett tárolás
- Ellenőrizetlen sokszorosítási lehetőségek
- Nincs felhasználói dokumentáció

Adatok

- Adatvesztések, károsodások
- Hibás manuális adatbeadás/változtatás
- Hibás utasítás, rendszermegszakítás
- Adatok jogosulatlan másolása

Informatikai biztonság

- Az informatikai rendszer, az érintett számára kielégítő mértékű állapota, aminek védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása és a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Hogyan védhetjük informatikai rendszereinket?

- OS biztonsági szolgáltatással, például naplózás, házirend kialakítása, felhasználó kezelés, hozzáférés-vezérlés.
- Titkosítás
- Tűzfalak, IDS/IPS alkalmazása
- Jelszókezelés jelentősége
- Vírusvédelem jelentősége
- Például oktatással, ha mondjuk van egy új gyakornok, akkor annak megtanítjuk, hogy hogyan használja az előírtaknak megfelelően, biztonságosan a rendszert.

5.a Ismertesse a tűzfalak különböző generációit és hasonlítsa össze őket!

Tűzfalak feladata és rendeltetése

- Szoftveres vagy hardveres hálózatzbiztonsági eszköz.
- A tűzfalak a hálózatra be és kimenő kapcsolatokat figyelik, és csak azokat engedélyezik, amelyek megfelelnek a beállított szabályoknak.
- **Előnyei:**
 - o Nem befolyásolják negatívan a hálózat működését és biztonságot nyújt
- **Hátrány:**
 - o Általános szabályok alapján működnek.
 - o Letilt olyan kapcsolatokat, amelyek nem is veszélyesek.
 - o Lehet, hogy lassítja a hálózat működését, így a szolgáltatások minősége romolhat.
 - o Nem megfelelő konfiguráció esetén, nem lesz jó a védelem.
 - o Nem véd olyan kapcsolatokról, amelyek nem mennek rajta keresztül

Tűzfalak generációi és fejlődésük

Első generáció – Packet Filtering Firewall

- **Döntését ezekre alapozza:**
 - o Forrás / Cél MAC cím, IP cím és port száma
 - o IP csomagba beágyazott protokoll

Működése

- A csomag fejlécében lévő információt **összeveti a tűzfalban megadott szabályokkal**.
- A hálózati és szállítási rétegben működik, adattartalmat nem figyel.
- Alacsony szintű biztonságot nyújt, mert nem vizsgálja a csomag tartalmát.
- Nem kezeli a kapcsolatállapotot
- Kétirányú forgalmat külön szabályokkal kell megadni.
- Egész port tartományt engedélyezni kell, mert sok protokoll dinamikusan választ portot kliens oldalon.

Második generáció – Stateful Firewalls (OSI 5. rétegben dolgozik)

- Tartalmakat vizsgál és figyelembe veszi a felépített kapcsolatokat.
- Figyeli az összes áthaladó hálózati csomagot és megállapítja, hogy:
 - o melyik már egy meglévő kapcsolat része
 - o melyik kezdeményez új kapcsolatot
 - o melyik csomag nem része egyik kapcsolatnak sem
- A felépített kapcsolat információt gyorsítótárban tárolja.
- A kapcsolat csomagjait a gyorsítótárban lévő bejegyzésekkel hasonlítja össze (hatékony)
- Figyeli a dinamikus protokollok állapotát.

Előnyei

- Jobban le lehet írni a hálózati szabályokat (állapotokat).
- Nagyobb biztonságot nyújt, mint a csomagszűrő tűzfalak (sorszámokat folyamatosan követi)

Hátrányai

- Állapotok kezelése miatt erőforrás igényes és nem mindig képesek megkülönböztetni a biztonságos és a veszélyes adatokat a csomagokban.

Harmadik generáció – Application Level Firewall

- **Két kategóriája van:** Proxy tűzfalak – Proxy Firewalls, Mély csomag ellenőrző – Deep Packet Inspection

Előnyei

- Biztonságos, és a puffer túlcsordulás típusú támadásoknak ellenáll, mert figyeli a protokoll fejléc mezőinek hosszát.

Hátrányai

- Erőforrás igényes, nem megfelelő megvalósításnál gyenge teljesítmény
- Transzparencia hiánya

Proxy firewalls

- A közvetlen kapcsolat megszakad, a továbbítandó csomagot újraelőállítják, átmásolják az összes protokollréteg szükséges mezőit.
- Alkalmazás szinten képes a parancsok szűrésére.

Deep Packet Inspection Firewalls

- Transzparensen működik, nem épít fel külön kapcsolatot a két kommunikáló fél között.
- Egyszerre szűri az OSI modell mind a 7 rétegét.
- Figyeli a protokollnak nem megfelelő csomagokat és szűri azokat.
- Csomagokat az alkalmazásoknak megfelelően osztályozza.

Next Generation Firewalls

- Több hálózatzbiztonsági technológia együttes integrációja.
- Olyan megoldás, ami DPI tűzfalat, IDS/IPS eszközöket, antivirus átjárót, proxy megoldást, VPN kiszolgálót, QoS és sávszélesség menedzsmentet biztosít, hogy a lehető legjobban kielégítse a mai kor igényeit.

Lehetséges Tűzfal topológiák

Dual-Homed

- Két interfésszel rendelkezik, amik külön hálózatba csatlakoznak és közöttük szűri a hálózati forgalmat.
- Speciális esete, amikor a router a tűzfal (screening router)

Single-Homed - Screened host

- A szolgáltatást nyújtó (bástya) gép csak a belső hálózatra csatlakozik.
- Elsődleges biztonságot a csomagszűrő forgalomirányító adja, ami megakadályozza, hogy a felhasználói gépek közvetlenül hozzáférjenek az internethez.
- Csomagszűrő forgalomirányítót úgy konfigurálják, hogy az internet gépei csak a bástya géppel léphetnek érintkezésbe.
- Bástya gép biztonsága fontos és proxy-ként működik.
- **Előnyei:**
 - o A screened host architektúra nagyobb biztonságot nyújt, mint a dual-homed host architektúra és nincs Single Point Of Failure
- **Hátránya**
 - o Screened subnet architektúra biztonságosabb
 - o Ha a támadó betört a bástya gépre, onnan már a többi gépet is eléri a LAN hálózaton.

Single-Homed - Screened subnet

- Screened subnet architektúra újabb biztonsági réteget helyez el az internet és a belső hálózat felé, ez a határ (perimeter) hálózat.
- **Bástya gép sebezhető**
 - o Ha a támadó bejut a bástya gépre, még mindig útját állja a belső forgalomirányító.
- **Perimeter hálózat**
 - o Ha a támadó bejut a bástya gépre, csak a perimeter hálózat forgalmát lehallgatja, a belső hálózat forgalmát nem láthatja.
 - o A perimeter hálózaton megy keresztül a bástya gép és az internetre irányuló forgalom, de két belső gép egymás közötti forgalma nem.
- **Bástya gép**
 - o A bejövő forgalom kezelésének helye
 - o **A kifelé irányuló szolgáltatások két módon kezelhetők:**
 - Belső és a külső forgalomirányítók csomagszűrő szabályainak beállításával.
 - Proxy szerverek futtatásával a bástya gépen.
- **Belső router (Choke router)**
 - o Szabályozza, hogy a belső hálózatról melyik szolgáltatások érhetőek el közvetlenül.
 - o Szabályozza a belső hálózat és a bástya gép közötti forgalmat.
- **Külső router (Access router)**
 - o Védi a perimeter és a belső hálózatot az internet felől.
 - o Minden forgalmat kienged a perimeter hálózatról.

Multi-Homed

- Három vagy több interfésszel rendelkezik, amik külön hálózatban csatlakoznak és közöttük szűri a hálózat forgalmát.

ASA tűzfal bemutatása, alapvető működése

- **Feladata**
 - o Megvédi a hálózatot a külső támadásoktól és az engedély nélküli hozzáférésektől.
 - o Ellenőrizzé és szabályozza az összes kommunikációt, ami a hálózatba és onnan kifelé történik.
- **Két féle forgalmat kezel**
 - o Kezdeményező forgalom, amit a hálózatban lévő eszközök indítanak.
 - o Elfogadott forgalom, ami a külső hálózatokról érkező kérésre válaszolnak.

Működése

1. Ellenőrzi a forgalmat, hogy megfelel-e a szabályoknak.
2. Ha megfelel, akkor engedélyezi és továbbítja azt.
3. Ha nem felel meg, akkor blokkolja azt.

Biztonsági szintek szerepe és jelentősége ASA tűzfal esetén

- 0 és 100 közötti értékek, amik növekvő biztonsági szintet jelentenek.
- Szerepe, hogy meghatározzák milyen forgalom engedélyezett vagy tiltott.
- Alacsonyabb biztonsági szinten lévő számítógépek csak olyan forgalmat küldhetnek, és fogadhatnak, ami megfelel a szabályoknak.
- A magasabb szinten lévők szélesebb körű forgalmat küldhetnek és fogadhatnak.

Alapkonfigurációs megoldások ASA tűzfal esetén, ACL, NAT, PAT, AAA konfigurálása

5505

- Switch modul, vlan interfészeket kell létrehozni, de alap licensszel csak 2-t lehet.

IP cím lehet

- Kézzel beállított, DHCP vagy PPPoE

Minden port alapértelmezésben VLAN1 tag

- Vlan beállítása ugyanúgy, mint switcheken és utána be kell kapcsolni az interfészt.

ACL

- Hozzáférés szabályozás vagy hálózati forgalom szűrésére szolgál.
- Permit és deny állításokból épül fel.
- Forgalomirányító csomagszűrőként viselkedik, amikor továbbítja vagy eldobja a csomagokat.

NAT, PAT

- Belső, külső irány vagyis kétirányú
- **Dinamikus NAT:** Címcsoportok között fordít.
- **Dinamikus PAT:** Egy külső címhez fordít belső címet, portok alapján.
- **Statikus NAT:** Kézzel beállított 1:1 fordítás.
- **Szabály alapú NAT:** Szabály alapú címfordítás.

AAA

- Hálózatot felügyel, aminek három komponense van:
 - o Authentication, Authorization, Accounting

Object, object group és a Modulár Policy Framework célja, jelentősége, működése és konfigurálása

Objects and Object Groups

- IP címeket, cím tartományokat, protokollokat, port számokat/tartományokat **Object**-ként definiálhatunk és ezután erre a névre hivatkozva konfigurálhatunk.
- **Előnye**, hogy az **Object** tartalma változik, akkor az **Object**-et használó konfigurációkat nem kell változtatni.

Network Object

- Egy elemet tartalmazhat: **IP** és **Maszk** páros, ami lehet host, subnet vagy range.

Service Object

- Tartalmazhat protokollt, port számot vagy intervallumot és csak egy elemet tartalmazhat.

Object Group

- Több **Object**-et csoportba lehet szervezni és a beállításai minden **Object**-re vonatkozik.

Modular Policy Framework

- **Class maps:** Forgalom figyelése
- **Policy maps:** Több **Class map**-et felvehetünk, amiket feladatokat rendelhetünk.
- **Service policy:** Alkalmazásra interfészre vagy a teljes rendszerre.

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**
 - o **Jegy (Tartalmazza) = Session key**
 - A kiszolgáló és a kliens nevét
 - Kliens internetes címét
 - Időbélyegét
 - Életciklusát
 - Egy véletlenszerűen generált kulcsot
 - o **Hitelesítő (Tartalmazza) = Titkosítva a kapcsolati kulccsal**
 - A kliens nevét
 - IP-címét
 - A munka-állomás aktuális idejét
- **Alany (principal)**
 - o 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

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

Kapcsolati kulcs

- o Ideiglenes privát kulcs.
- o 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.
 - o Felhasználók azonosságának, jogosultságainak ellenőrzése.
 - o Megkönnyíti a hálózati erőforrások elérését.
 - o A címtár és így a hálózat is központi helyről felügyelhető.
 - o A hálózat távfelügyelete automatizálható.

Címtár szükségessége

- **Igény**
 - o Sok felhasználó és sok kiszolgálónál is maximális teljesítmény és biztonság.
- **Korábban**
 - o Felhasználók nyilvántartása minden kiszolgálón külön-külön.
 - A jogokat mindenhol külön be kellett állítani.
- **Címtárral**
 - o 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**
 - o Alapból a rendszerkönyvtárak írása tiltva van.
 - Ha törölünk egy fájlt a rendszerkönyvtárból, abból nagy bajt is okozhatunk.
 - o Deny jog
 - o Tulajdon-átvétel
 - o Jogosultság kimutatás
 - Kik is férhetnek hozzá.
- Fájl szintű titkosítás az NTFS köteteken
- **Tartományban**
 - o Jobb ha egy CA (Certificate Authority) szervertől kapja a felhasználó.
 - o 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

6.b Mi indokolja a kockázatelemzés szükségességét? Adjon példát a kockázatelemzés gyakorlati megvalósítási lehetőségére (pl. táblázatos módszer)!

Kockázatelemzés hasznossága

- Segítséget nyújt a rendszer leggyengébb pontjainak.
- Legnagyobb kockázatot jelentő fenyegető tényezők azonosítása.
- Ezek ismeretében költséghatékony, kockázatarányos védekezést lehet kialakítani.

Egyenszilárdságú védelem

- Kockázatok meghatározása alapvető szerepet játszik.
- Értelmetlen túlzottan védekezni, amíg más területeken sokkal nagyobb kockázatú veszélyek is vannak a rendszerben. **(pl.: Erős ajtó, de az ablakon be lehet mászni.)**

Kockázatmenedzsment

- Kockázatok, károk.
- Kockázatbecslés problémáit a kockázatmenedzsment módszerével szokás kezelni a gyakorlatban, ami a kockázatok értékeit nem határozza meg konkrét érték formájában.
 - o Olyan összehasonlításra lehetőséget adó elemzést alkalmaz, ami alapján legcélszerűbb védelmi intézkedések meghatározhatóak.
- Egyes kockázati tényezőket egymáshoz hasonlítva határozzuk meg a gyenge láncszemeket, ahol a legcélszerűbb védekezni.

Problémák

- Veszélyforrások bekövetkezésének gyakoriságára nincsenek jó statisztikák.
- Okozott károk anyagilag sem határozhatóak meg.

Kockázati paraméterek becslése

- Veszélyforrások támadási folyamatának hatásmechanizmusa
 - o Informatikai rendszerek konkrét rendszerelemeinek támadása.
 - o Egyes rendszerelemek sérülése hat a velük kapcsolatban lévő alkalmazásokra.
 - o Nem sikerül jól kezelni a károkat, akkor az ügyfeleknél is érzékelhető lesz.

Károk

- Hatás továbbterjedése = elsődleges, másodlagos, harmadlagos, stb. károk
- Veszélyforrás elbírálása meddig terjedhet ki, mivel a másodlagos, harmadlagos károk nagyobbak az elsődleges károknál.
- Elsődleges kár = Merevlemez meghibásodás
- Másodlagos kár = Nagy mennyiségű adat visszaállíthatatlanul megsemmisül.
- Harmadlagos kár = Üzleti haszon elmaradása a károk miatt

Kockázatelemzés módszerei

- Egyetlen módszertan sem vállalkozik arra, hogy informatikai rendszerek esetén a kockázat pénzügyi nagyságát közvetlenül megbecsülje.

Kockázatelemzés táblázatos módszere

- Alapja a veszélyforrások számbavétele és részletes elemzése, egy kockázatelemzési tábla szisztematikus, oszlopról-oszlopra haladó kitöltésével.

Kockázatelemzés lépései

1. Kategóriák felállítása:

Bekövetkezési valószínűség, Kár, Kockázati, Kockázati szorzótábla meghatározása

2. Veszélyforrások meghatározása
3. Bekövetkezési valószínűségek nagyságrendi meghatározása
4. Kárérték nagyságrendi meghatározása
5. Kockázati tényezők származtatása
6. Elviselhetetlen kockázatok kezelése
7. Védelmi intézkedések számbavétele és a megfelelő alternatívák kiválasztása

Kategóriák felállítása

- A bekövetkezés valószínűségének, a támadási potenciálnak leírása.
- A bekövetkező kár becslése.
- A kockázat veszélyforrásonkénti nagyságának meghatározása.
- Meghatározzuk a közöttük lévő kapcsolatot a kockázati szorzótáblával.

Veszélyforrások listájának összeállítása

- **Veszélyforrások:** A rendszer helyes működését fenyegető események.
- A kockázatelemzési tábla sorait alkotják.
- Egyértelmű azonosítóval látjuk el.
- **Helyzetfelmérés:** Dokumentumok elemzésével, Interjúkkal, Szemlével
- **Veszélyforrások feltárása**
 - o Tapasztalatok felhasználásával és a rendszer elemzéséből felderített hiányosságok számbavételével történhet.
- A lista soha nem lehet teljes, de lehet részletes.
- Kimaradó veszélyforrásokat kockázatként kezelhetjük.

Veszélyforrások csoportjai

- Szervezési gyengeségek
- Természeti veszélyforrások (tűz, villám), Fizikai veszélyek (betörés, lopás)
- Logikai fenyegetések (hálózati betörés, lehallgatás)
- Humán veszélyforrások (visszaélések, munkatársak gondatlansága)

Bekövetkezési valószínűségek nagyságrendi becslése

- **Probability oszlop**
- Tapasztalatok alapján történik.
- A támadási potenciál meghatározásánál figyelembe kell venni a gyengeség kihasználásához szükséges felkészültségi szintet és, hogy mennyire érdemes támadást végrehajtani az adott rendszer ellen.
- **Felkészülési szintek alapján:**
 - o Automatizált eszközökkel végrehajtható
 - o Átlagos felhasználó által kihasználható
 - o Profi támadót igénylő gyengeség

Kárérték nagyságrendi meghatározása

- Komplex feladat
- Hatás megfigyelése egy adott rendszerelem sérülése esetén.
- **Okozott kár természete:** Érintett rendszerelem milyen tulajdonsága sérült.
- Károk meghatározásának szempontjai
 - o Bizalmasság (Confidentiality) megsértése, jogtalan információ szerzés.
 - o Sértetlenség (Integrity) elvesztése, a tárolt adatok manipulálása.
 - o Rendelkezésre állás (Availability) elvesztése.

Kockázati tényezők származtatása

- Risk oszlop kitöltése a kockázati szorzótábla segítségével.
- A szorzótábla sorát a veszélyforrás előfordulási gyakorisága
 - o Oszlopát általában a CIA szempontok közül a legnagyobb kárral járó kár-kategóriája határozza meg. Sor és oszlopnak megfelelő cella tartalmazza a kockázatot.

Elviselhetetlen kockázatok

- Helyrehozhatatlan, hosszabb távon is kiható tényezők által jelentett veszély.
- Védelmi intézkedések kiválasztásakor a cél:
 - o Olyan védelmi intézkedések alkalmazása, amik költsége kevesebb, mint az általuk kiküszöbölt kockázat.
 - o Hosszú távon, és egyéb üzletpolitikai szempontok figyelembe vétele.
- A szorzótáblában és a kockázatelemzési táblában általában külön (pl.: *-gal) jelölhetők.
- Az elviselhetetlen kockázatú veszélyforrás kockázatát legalább elviselhető mértékűvé csökkentése.

Lehetséges védelmi intézkedések számbavétele

- Felírjuk az összes elképzelhető védelmi intézkedést.
- Mindegyiknél megadjuk, hogy milyen hatása van.
- Majd az összes lehetséges kombináció értékelésével megkaphatjuk, hogy miket kell kiválasztani.
 - o Választás legfontosabb szempontja az ár és az elért hatás.
 - o Költségeknél célszerű megkülönböztetni az egyszeri beruházási költségeket az éves fenntartási költségektől.
 - o Rövid és hosszú távú pénzügyi célok jól elkülöníthetők.
- Védelmi intézkedések egymásra hatással vannak, ezért a veszélyforrásokra gyakorolt hatásaikat már nem szokás kategorikusan meghatározni.
- A veszélyforrásokra gyakorolt hatást a valószínűség és a hatás csökkentésének mértékével adhatjuk meg.
- A hatás leírásában meg kell adni az intézkedés által befolyásolt veszélyforrás azonosítóját és a befolyásolás módját.

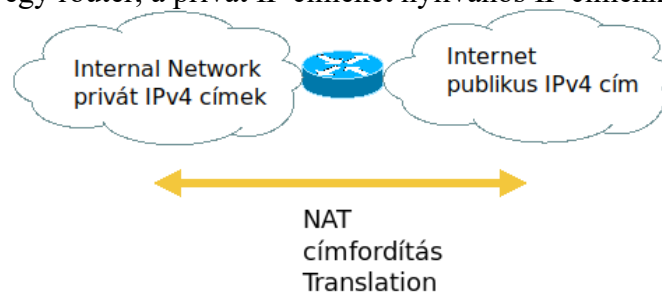
Hatásmegjelölés magyarázat

- E: (eliminates) a veszélyforrás teljes kiküszöbölés.
- D: (decreases damage) az okozott kár egy kategóriával csökken.
- DD: (decreases damage) az okozott kár két kategóriával csökken.
- P: (decrease probability) a bekövetkezési valószínűség egy kategóriával csökken.
- PP: (decrease probability) a bekövetkezési valószínűség két kategóriával csökken.

7.a Magyarázza el hogyan működik a hálózati címfordítás és portfordítás! Hol és miért van rá szükség?

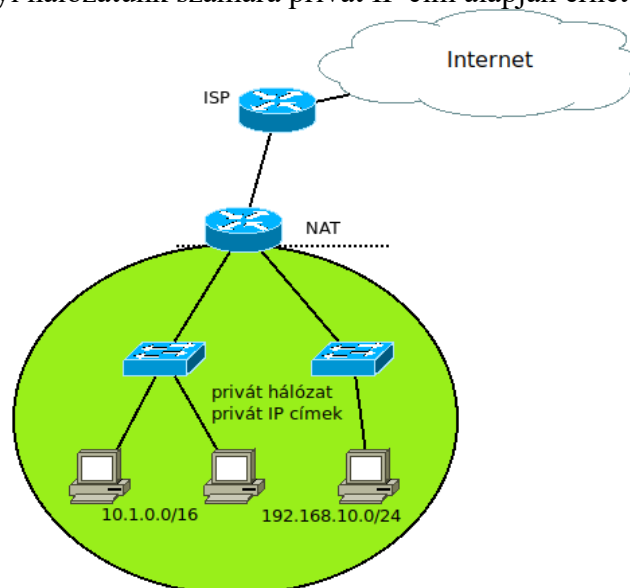
NAT

- Network Addresss Translations, vagyis hálózati címfordítás.
- Általában arra használjuk, hogy privát IP cím tartomány és az Internet között egy szerver vagy egy router, a privát IP címeket nyilvános IP címekké alakítsa és vissza.



NAT példa

- Amikor egy ISP-től kapunk Internet hozzáférést.
- Az ISP routere ad egy nyilvános IP címet a saját routerünknek.
- A routerünk a helyi hálózatunk számára privát IP cím alapján érhető el.



- Ha a helyi hálózatunk egyik gépe csomagot akar küldeni az Internetre, akkor saját routerünk a belső IP címet átírja külső IP címre és így továbbítja az ISP router felé. **Ezt nevezzük címfordításnak.**

IP cím elnevezése

- Belső vagy külső hálózaton vannak
- Bejövő vagy kimenő a forgalom
- **Belső:** A cím amit fordítunk és amire fordítjuk
- **Külső:** A céleszköz címe

NAT címtípusok

- Belső helyi cím
- Belső globális cím
- Külső helyi cím
- Külső globális cím

NAT típusok

1. Statikus NAT:

- Kézzel beállított 1:1 fordítás, állandó leképezést biztosít
- Akkor hasznos, ha külső hálózatról kell elérni a belső hálózat egy gépét
- **Beállítása:**

```
ip nat inside source static <belső helyi cím> <belső globális cím>  
interface <interfész>  
ip address <IP cím> <Maszk>  
ip nat inside VAGY outside
```

- **Ellenőrzése:**

```
clear ip nat statistics  
show ip nat statistics (Kapcsolódás után)
```

2. Dinamikus NAT

- Címcsoportok között fordít, automatikus leképezés
- **Beállítása:**

```
ip nat pool <POOL NEVE> <IP kezdő> <IP vég> <Wildcard maszk>  
access-list 1 permit VAGY deny <Hálózat IP címe> <Wildcard maszk>  
ip nat inside VAGY outside source list 1 pool <POOL NEVE>  
interface <interfész>  
ip nat inside VAGY outside
```

3. PAT

- Port Address Translation
- Egy külső címhez fordít belső címet, portok alapján
- NAT túlterhelés
- Belső globális cím használat sok belső helyi címhez.
- **Egy vagy több címet is tudunk használni.**
- Az **overload** parancsot kell hozzáírunk, hogy érvénybe léphessen a PAT.

Portfordítás

- Például a 80-as portot 8080-as portra szeretnénk fordítani.
- **Beállítása:**

```
ip nat inside VAGY outside source static <Szolgáltatás, pl.: tcp> <IP cím>  
<ERRŐL A PORTRÓL> <KÜLSŐ IP CÍM> <ERRE A PORTRA>
```

- **Ellenőrzés:**

```
show ip nat translations
```

NAT előnyök és hátrányok

- **Előnyök**
 - o IPv4-es címek megtakarításávan segít.
 - o Skálázhatóságot vihetünk a hálózatba, ha egyszerre többféle globális címtartományt, tartalék címtartományokat implementálunk.
 - o A belső hálózatbeli gépek teljesen elrejtethetővé válnak a külvilág elől, emiatt biztonság.
- **Hátrányok**
 - o Minimális naplózási szolgáltatásokat nyújt.
 - o NAT megszakíthat alkalmazásokat és megnehezítheti futtatásukat.

7.b Vesse össze a Microsoft és az IBM által nyújtott eszközöket felhasználó- és hozzáférés menedzsment szemszögből!

Problémák

- Jelszórendszer megkerülhető (Nincs bejelentkezés azonosítás)
- Üres jelszó
- Gyenge jelszavak, ezek feltörhetőek.
- Nem megfelelően kezelt jelszavak
- Jelszókezelés nincs szabályozva
- Nem biztonságos alkalmazások (Nincs titkosítás beépítve)
- Szoftver hibák
- Konfigurálási hibák (szoftverfrissítések, emberi tévedések)
 - o Megoldás: Integrált jogosultság kezelés

Identity

- Öntudat, identitás
- Hitelesítési információk olyan csoportja, amik a rendszer egy adott egyedét egyértelműen meghatározzák.

User provisioning

- Felkészülés, szolgáltatás
- Felhasználói fiókok létrehozása és jogosultságaik beállítása cél erőforrásokon.

IBM központ felhasználó menedzsment = IBM Tivoli

- A felhasználók a rendszerrel kapcsolatos jogosultságainak kezelése.
- A szervezetbe történő belépéstől a kilépésig.
- Előnyei:
 - o A felhasználók csak olyan alkalmazásokat, adatokat érhetnek el, amikhez joguk van.
 - o A jogosultságok menedzselése folyamatosan és centralizált.
 - o A jogosultságot központilag azonnal le lehet tiltani, ha szükséges.

Integrált jogosultság kezelés

- A felhasználók a jogosultságuk szerint különböző felhasználói azonosítókkal és jelszavakkal elérhető más rendszereket, alkalmazásokat, adatokat egy központi jelszóval elérik.
- Képes a más rendszerek, alkalmazások, adatok eléréséhez szükséges jelszavak automatikus generálására, a bejelentkezési és azonosítási folyamatok elvégzésére.
- Előnyei:
 - o Csak egy jelszóval tud belépni a felhasználó.
 - o Könnyű kezelhetőség, automatizálhatóság.
 - o Minimalizálja a problémák, tévedések lehetőségét.

Identity Manager működési modellje „Role Based”

- A felhasználó felelősségi körnek megfelelő szerepkörhöz rendelés.
- A szerepkör tagjainak erőforráshoz rendelése.
- Provisioning Policy attribútumokat is meghatározhat.
 - o Felhasználó lemezterület kvóta
 - o Csoport-tagság

Microsoft

- Active Directory és csoportházirendek.
- Felhasználók központi menedzselése
 - o Jelszó jogosultságok
 - o Csoportok
 - o Szervezetek
- A csoportházirendekkel az AD csoportjaihoz rendelhetünk jogosultság-gyűjteményeket, amik az adott csoport tagjaira lesznek érvényesek.
 - o Adott felhasználónál egy adott jogosultság felüldefiniálható.

8.a Milyen állapotartó tűzfal konfigurálható a forgalomirányítókön? Mutassa be a működés elvét, jellemzőit és a beállítás lépéseit!

Tűzfalak feladata és rendeltetése

- Szoftveres vagy hardveres hálózatzbiztonsági eszköz.
- A tűzfalak a hálózatba be és kimenő kapcsolatokat figyelik, és csak azokat engedélyezik, amik megfelelnek a beállított szabályoknak.
- **Előnyei:**
 - o Nem befolyásolják negatívan a hálózat működését és biztonságot nyújt
- **Hátrány:**
 - o Általános szabályok alapján működnek.
 - o Letilt olyan kapcsolatokat, amik nem is veszélyesek.
 - o Lehet, hogy lassítja a hálózat működését, így a szolgáltatások minősége romolhat.
 - o Nem megfelelő konfiguráció esetén, nem lesz jó a védelem.
 - o Nem véd olyan kapcsolatokról, amik nem mennek rajta keresztül

Access Control List – ACL

- Legegyszerűbb, első generációs tűzfal
- Állapotmentes, 3. és 4. rétegben működik

Context-Based Access Control – CBAC

- 1997-ben vezették be
- CBAC csak azokat a protokollokat szűri, amiket az adminisztrátor konfigurált
- Csak azokat a csomagokat szűri, amik áthaladnak a routeren.

Fő funkciói

- **Állapotartó szűrés (Stateful packet filtering)**
 - o Nem csak hálózati réteg, szállítási réteg információk alapján, hanem alkalmazási réteg információt is vizsgál, hogy megállapítsa a viszonyok állapotát.
- **Forgalom figyelés (Traffic inspection)**
 - o SYN flood támadások, TCP sorszámozást figyel és gyanúsakat eldobja.
- **Behatolás érzékelés (Intrusion detection)**
 - o Syslog üzenetek átvizsgálásával bizonyos SMTP támadások, SYN Flood támadások, sajátosságait ki lehet szűrni, ezeket a kapcsolatokat eldobja és riasztást, értesítést küld a rendszernek.
 - o CISCO IOS tűzfal 3 küszöbértéket is figyel a TCP DoS támadások kivédésére:
 - Félig megnyitott TCP kapcsolatok száma.
 - Félig megnyitott TCP kapcsolatok száma adott intervallumban.
 - Félig megnyitott TCP kapcsolatok száma egy adott host-tól.

CBAC működése

- **TCP, UDP és ICMP kapcsolatokról információt tárol az állapot táblában (state table).**
- Amikor a hálózaton belüli eszköz munkamenetet kezdeményez, egy dinamikus bejegyzés kerül az állapottáblába és a kimenő forgalom áthaladhat a routeren.
- Ennek a bejegyzésnek a segítségével a kimenő forgalom válasza áthaladhat a routeren, mivel a hálózaton belül kezdeményezett forgalomra is van bejegyzése.
- Ideiglenes lyukakat nyit a bejövő forgalomra alkalmazott hozzáférési listán, hogy engedélyezze a reply csomagokat.

CBAC konfigurálása

- 1. Interfész kiválasztása**
 - a. Belső interfész ahonnan indulhat egy viszony felépítés.
- 2. ACL konfigurálás az interfészen**
 - a. Milyen típusú forgalmat engedélyezünk az interfészen
 - i. Alap konfiguráció, hogy a belső hálózattól a külső hálózatig mindent, de a külső hálózattól a belső hálózating semmit.
 - ii. Engedélyezzük azt a forgalmat, amit meg kell vizsgálni a CBAC-nak.
 - iii. Implicit deny-t tegyük explicitté a naplózás miatt.
- 3. Inspection rule megfogalmazása a vizsgált forgalomra**
- 4. Alkalmazás a megfelelő interfészen**

8.b Ismertesse egy általános célú, több belső és külső szolgáltatást nyújtó Windows hálózati kiszolgáló biztonsági konfigurációs (hardening) lehetőségeit intézményi környezetben!

Fizikai védelem

- **Szerverterem**
 - o Zárt helyiség, ellenőrzött bejutás
 - o Folyamatos áramellátás biztosítása
 - PDU, UPS
 - o Megfelelő hőmérséklet biztosítása, monitorozása
- **Erős BIOS jelszó beállítása**

Hálózati védelem

- Tűzfal megfelelő beállítása
- Távoli eléréshez VPN kiépítése
 - o Tanúsítványok megkövetelése

Vírusvédelem

- Vírusirtó szoftver telepítése
 - o Szoftver adatbázisnak frissítése

Active Directory Védelem

- Telepítésnél a helyreállítási jelszó tárolva legyen
- Csak arra a jogosult személy léphet be a kiszolgálókra
 - o Erős jelszó megkövetelése, havonta csere
 - Group Policy-val jelszóháziparancs megkövetelése
 - o Tanúsítványok érvényessége
- A user szerepkörök szabályozása
 - o Belső tevékenység szabályozása, ki-mihez férhet hozzá
 - o Állomány hozzáférés szabályozás
 - Organization Unit
 - Group
 - Group Policy

Frissítések kezelése

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

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

Mentések

Biztonsági mentés fontossága

- A mentés célja a helyreállíthatóság biztosítása, adatvesztések elkerülése, minimalizálása másolati adatpéldányok készítésével.

Mentés célja

- Üzletfolytonosság biztosítása
- **Törlés**
 - o A felhasználó véletlenül vagy szándékosan
- **Meghibásodás**
 - o Egy tároló eszköz vagy elromlott a rendszer

Mentési stratégia kialakítását befolyásoló tényezők

- **Adattípusok**
 - o Adatok jellege
 - o Mennyire kritikus adat
 - o Meddig kell tárolni
- **Adatmennyiség**
 - o Mentési időt befolyásolja
- **Adatok helye**
 - o Honnan/hova szeretnénk menteni
- **Mentési gyakoriság**
 - o Adatok fontossága, mennyisége
- **Mentési típusok**
 - o Teljes
 - o Differenciális
 - o Inkrementális

Differenciális mentés

- Ciklus első napján teljes mentés
- Utána minden nap csak az előző teljes mentés óta történt változások
 - o Nagyobb, egyre növekvő napi adatmennyiség
- Gyorsabb és hatékonyabb, mint a teljes mentés
- Maximum 2 helyreállítási folyamatot igényel az adat visszaállítása

Inkrementális mentés

- Ciklus első napján teljes mentés
- Utána minden nap csak az előző óta történt változások
 - o Kis adatmennyiség, emiatt gyors és kisebb követelményei vannak, mint a differenciális mentésnél.
- Hosszú visszaállítási idő
 - o Az adatok visszaállítása, több egymást követő mentésekből álló folyamatot igényel.

Központi loggyűjtés a tevékenységekről

- Kategorizáció

Monitoring rendszer kialakítása

- CPU, RAM, DISK terheltség
- Service-k állapota
- Riasztási küszöb beállítása

9.a Ismertesse a VPN-ek (Virtual Private Network) célját, feladatát és fajtáit! Milyen megvalósításait ismeri? Miben különböznek a különböző rétegekben megvalósított VPN-ek?

A VPN fogalma, rendeltetése, alaptípusai, funkciói, szolgáltatásai, topológiák

VPN – Virtual Private Network

- **Virtuális:** A magánhálózat forgalma nyilvános hálózaton halad keresztül egy virtuális alagúton.
- **Védett:** Átmenő forgalom titkossága biztosított.

Rendeltetése

- Biztonság növelése
- Anonimitás
- Nem elérhető tartalomhoz jutás (adott országon belül például tiltva van)
- Adatvédelem

Alaptípusai

- IPSec – Internet Protocol Security
- L2TP - Layer 2 Tunneling Protocol
- PPTP – Point-to-Point Tunneling Protocol
- SSL és TLS
- OpenVPN
- SSH – Secure Shell

Topológiák

- **Site-to-Site VPN**
 - o Két vagy több LAN kapcsolható össze.
 - o Az állomások normál IP csomagokat küldenek, ami egy VPN gateway-en megy keresztül.
- **Client-to-Site VPN:**
 - o Kliens-szerver kapcsolat, ahol kliens alkalmazás szükséges.
- **Client-to-Client VPN:**
 - o Közvetlen kommunikáció két számítógép között, központi szerver nélkül.

A különböző OSI modell szerinti rétegekben széles körben elterjedt VPN megvalósítások jellemzői, előnyei és hátrányai

L2 VPN

- Független a felső protokolltól
- Egy-egy kapcsolatot véd, így minden összeköttetésre külön alkalmazni kell.
- MITM támadás lehetséges

L3 VPN

- Média és alkalmazás független
- IPSec, GRE, MPLS védelem

L4 VPN

- SSL-lel biztosítja a titkosságot, a felhasználók hitelességét és az adatok sértetlenségét a TCP alkalmazások számára.
- Nem rugalmas, nehéz megvalósítani
- Nem alkalmazás független

L7 VPN

- Az alkalmazás rétegbeli VPN-t minden alkalmazásban külön-külön meg kell valósítani.

GRE kapcsolat szolgáltatásai, alkalmazási kör, jellemzők, „site-to-site” GRE konfigurálása

GRE kapcsolat szolgáltatásai

- Hálózati protokollok közötti átjárás
- Többszintű hálózatok összekapcsolása
- Hálózatok közötti tűzfalak átjárásának lehetősége
- Hálózatok közötti VPN-ek létrehozása

Jellemzők

- Nem alkalmaz titkosítást, így IPSec-et kell alkalmazni.
- Támogatja a routing protokollokat
- Több protokollal alagutakat is támogat
- Multicast csomagokat is kezel
- Alkalmas irányító protokollok irányítási információinak szállítására és cseréjére.

Az SSL protokoll célja és feladata, szerkezeti felépítése, alprotokolljai és feladataik

SSL célja

- Titkosított kommunikációt biztosító protokoll, ami nyílt hálózatokban, kapcsolatorientált kommunikációban nyújt védelmet.
- Csak egy-egy kommunikációs csatornát biztosít.
- Gyakran használják a weboldalak biztonságos titkosítására is.

SSL szerkezeti felépítése

- Minden egyes kapcsolat egyedi kulccsal titkosít.
- Tanúsítvány igazolja a szerveret.
- Biztosítja az adatintegritást. (MD5, SHA-1)

SSL működése

1. Kliens csatlakozik a kiszolgálóhoz.
2. Kiszolgáló elküldi a hitelesítési tanúsítványt a kliensnek.
3. Kliens ellenőrzi a tanúsítvány hitelességét, majd létrehozza a titkosított kapcsolatot a kiszolgálóval.
4. Kliens és kiszolgáló között így már biztonságosan lehet adatokat cserélni.
5. Ha az SSL kapcsolat megszakad, akkor a kliens és a kiszolgáló kapcsolata is megszakad.

SSL alprotokolljai

Rekord protokoll

- Feladata a kliens és a szerver és a felsőbb SSL protokoll entitások védelme:
 - Titkosítás, integritásvédelem, üzenet-visszajátszás elleni védelem

Handshake protokoll

- Rekord protokollban használt kriptográfiai algoritmusok és paramétereik egyeztetése.
- Kulcscsere és hitelesítés

Change-Cipher-Spec protokoll

- Egyetlen üzenetből áll, ami a Handshake protokoll kulcscsere részének végét jelzi.
- Ezt az üzenetet elküldi, utána az adott fél az új algoritmusokat és kulcsokat kezdi használni a küldése.
 - A vétel még mindig a Handshake előtti állapot szerint történik.

Alert protokoll

- Figyelmeztető és hibaüzenetek továbbítása.

A handshake, valamint a record alprotokoll feladata, működése és üzenetei

Rekord protokoll működése

- A felsőbb protokoll rétegektől érkező üzeneteket:
 - o Fragmentálja, ha szükséges.
 - o Fragmenseket tömöríti
 - o Tömörített fragmenseket fejléccel látja el
 - o Fejléccel ellátott, tömörített fragmensre üzenethitelesítő kódot/MAC-et számol és azt a fragmenshez csatolja.
 - o Az üzenethitelesítő kóddal ellátott fragmenst rejtjelezi.

Rekord üzenetei

- **type:** Rekord üzenetben melyik felsőbb protokoll található.
- **version:** SSL verzió
- **length:** Fragmens hosszát tartalmazza bájtban mérve.
- **MAC:** Üzenethitelesítő kód generálása

Handshake protokoll működése

1. **fázis:** Kliens és szerver elküldi a tulajdonságait, megállapodnak
2. **fázis:**
 - a. Kulcscseremódszertől függ
 - b. Szerver elküldi a tanúsítványát és kéri a kliens tanúsítványát.
3. **fázis:** Tanúsítvány ellenőrzés és kulcscsere folytatása
4. **fázis:** Kulcscsere életbelépése, befejezése

Handshake üzenetei

- **KliensHello:**
 - o Kliens küldi ezt az üzenetet az SSL Handshake kezdeményezésére.
 - o Kliens verzió, véletlenszám, viszonyazonosító, biztonsági algoritmusok, tömörítő algoritmusok
- **SzerverHello:**
 - o Kiszolgáló küldi a **KliensHello** üzenetre válaszul.
 - o Szerver verzió, véletlenszám, viszonyazonosító, biztonsági algoritmusok, tömörítő algoritmusok
- **Szerver kulcscsere üzenet**
- **Tanúsítvány kérés**
 - o Előfordulhat olyan eset is, amikor a tanúsító hatóságok listája üres.
 - Ilyenkor a kliens eldöntheti, hogy elküldi-e az ügyféltanúsítványt vagy sem.
- **Kliens tanúsítvány**
 - o A kliens bemutatja a tanúsítványláncát a kiszolgálónak.
- **Kliens kulcscsere üzenet**
 - o Lényege, hogy létrehozza a közös kulcsot a kliens és a kiszolgáló között anélkül, hogy azt egy kívülálló számára felfedné.
- **Kész üzenet**
 - o Első olyan üzenet, ami már az új algoritmusokat használva, az új kulcsokkal van kódolva.

9.b Ismertesse az informatikai ellenőrzés feladatához és az ellátásához kapcsolódó alapfogalmakat (rendelkezésre állás, bizalmasság, sértetlenség), valamint a két kiegészítő követelményt (funkcionalitás, dokumentáció), mondjon példát a teljesítésük mérésére!

Kockázatelemzés hasznossága

- Segítséget nyújt a rendszer leggyengébb pontjainak.
- Legnagyobb kockázatot jelentő fenyegető tényezők azonosítása.
- Ezek ismeretében költséghatékony, kockázatarányos védekezést lehet kialakítani.

Kockázatmenedzsment

- Kockázatok, károk.
- Kockázatbecslés problémáit a kockázatmenedzsment módszerével szokás kezelni a gyakorlatban, ami a kockázatok értékeit nem határozza meg konkrét érték formájában.
 - o Olyan összehasonlításra lehetőséget adó elemzést alkalmaz, ami alapján legcélszerűbb védelmi intézkedések meghatározhatóak.
- Egyes kockázati tényezőket egymáshoz hasonlítva határozzuk meg a gyenge láncszemeket, ahol a legcélszerűbb védekezni.

Károk

- Hatás továbbterjedése = elsődleges, másodlagos, harmadlagos, stb. károk
- Veszélyforrás elbírálása meddig terjedhet ki, mivel a másodlagos, harmadlagos károk nagyobbak az elsődleges károknál.
- Elsődleges kár = Merevlemez meghibásodás
- Másodlagos kár = Nagy mennyiségű adat visszaállíthatatlanul megsemmisül.
- Harmadlagos kár = Üzleti haszon elmaradása a károk miatt

Kockázatelemzés táblázatos módszere

- Alapja a veszélyforrások számbavétele és részletes elemzése, egy kockázatelemzési tábla szisztematikus, oszlopról-oszlopra haladó kitöltésével.

Kockázatelemzés lépései

1. Kategóriák felállítása:

Bekövetkezési valószínűség, Kár, Kockázati, Kockázati szorzótábla meghatározása

2. Veszélyforrások meghatározása

3. Bekövetkezési valószínűségek nagyságrendi meghatározása

4. Kárérték nagyságrendi meghatározása

5. Kockázati tényezők származtatása

6. Elviselhetetlen kockázatok kezelése

7. Védelmi intézkedések számbavétele és a megfelelő alternatívák kiválasztása

CIA

Confidentiality

- Adatok kiszivárgásának megakadályozása, vagyis titkosítás

Integrity

- Sértetlenség, vagyis integritást védő algoritmusok

Availability

- Rendelkezésre állás, vagyis hálózati eszközök és adatok elérhetősége

Példa

- Az áramszünet nem okozza a bizalmasság sérülését, de hatással van a rendelkezésre állásra és akár a tárolt adatok is sérülhetnek.
 - o Ezt a hatásmechanizmust az **I** és **A** oszlopok megfelelő kitöltésével, a **C** oszlopban kihúzással jelölhetjük.

Informatikai ellenőrzés

- Standardok, irányelvek alapján járnak el az ellenőrök.

Funkcionalitás

- Azt vizsgáljuk, hogy a szoftver vagy rendszer megfelel-e a felhasználói igényeknek és elvárásoknak.
- Teszteket és vizsgálatokat végzünk a rendszer különböző részein.

Dokumentáció

- Ellenőrizzük, hogy a rendszerhez vagy a szoftverhez készült dokumentáció megfelel-e és teljes.
- A dokumentáció magába foglalja a használati útmutatót, az implementációs dokumentációt, a tesztelési tervet és a működési dokumentációt is.
- Tehát ellenőrizzük, hogy a dokumentáció tartalmazza-e a szükséges információkat, például azokat a folyamatokat, amik segítségével a rendszer működik, a szükséges eszközöket, a szükséges konfigurációkat és azokat a paramétereket, amik befolyásolhatják a rendszer működését.

10.a Ismertesse az IPSec protokoll célját, felépítését, működését, üzemmódjait és beállításának lépéseit!

A VPN fogalma, rendeltetése, alaptípusai, funkciói, szolgáltatásai, topológiák

VPN – Virtual Private Network

- **Virtuális:** A magánhálózat forgalma nyilvános hálózaton halad keresztül egy virtuális alagúton.
- **Védett:** Átmenő forgalom titkossága biztosított.

Rendeltetése

- Biztonság növelése, Anonimitás
- Nem elérhető tartalomhoz jutás (adott országon belül például tiltva van)
- Adatvédelem

Alaptípusai

- IPSec – Internet Protocol Security
- L2TP - Layer 2 Tunneling Protocol
- PPTP – Point-to-Point Tunneling Protocol
- SSL és TLS, OpenVPN, SSH – Secure Shell

Topológiák

- **Site-to-Site VPN**
 - o Két vagy több LAN kapcsolható össze.
 - o Az állomások normál IP csomagokat küldenek, ami egy VPN gateway-en megy keresztül.
- **Client-to-Site VPN:**
 - o Kliens-szerver kapcsolat, ahol kliens alkalmazás szükséges.
- **Client-to-Client VPN:**
 - o Közvetlen kommunikáció két számítógép között, központi szerver nélkül.

IPsec VPN komponensek (protokollok), alprotokollok, működés, előnyök, korlátok

AH – Authentication Header

- Sértetlenséget, hitelesítést és visszajátszás elleni védelmet biztosít.
- Beszúr egy AH fejléct, ami egy MAC-et tartalmaz.
- A visszajátszás detektálásának érdekében, az IP csomagokat sorszámozza.
- Az AH fejlécben található MAC érték a sorszámot is védi.

ESP – Encapsulated Security Payload

- Feladata az IP csomag tartalmának rejtése és opcionálisan a tartalom integritásának védelme.
- IP csomag tartalmának rejtését rejtjelezéssel oldja meg.
- **Tartalom integritásának védelme:** ESP fejlécre és a csomag tartalmára számít MAC kódot és azt a csomaghoz csatolja.
- ESP MAC nem védi az IP fejléc mezőit.

ISAKMP – Internet Security Association and Key Management Protocol

- Általános célú keretprotokoll, ami bármilyen konkrét kulcscsere protokoll üzeneteit képes szállítani.

IKE – Internet Key Exchange

- IPSec hivatalos kulcscsere protokollja.
- A host-ok ebben a fázisban hitelesítik egymást shared secret vagy RSA kulcs segítségével.
- Felépítenek egy kétirányú ISAKMP SA-t.
- Az ISAKMP SA-t alkalmazva megvitatják az egyirányú IPSec SA-kat.

Az IPsec protokollok paramétereinek konfigurálási megfontolásai és lépései

Megfontolások

- **Titkosítási módszer:** DES, 3DES, AES, stb
- **Autentikációs módszer:** Például SHA, MD5, stb
- **Kulcsrotációs periódus:** Mennyi ideig használhatjuk ugyanazt a titkosítási és autentikációs kulcsot.
- **Pre-shared key:** Összes hálózati eszköz ismeri a kulcsot.
- **Perfect Forward Secrecy:** A régi kulcsok már nem használhatóak.

IPsec üzemmódok jellemzői, működése, konfigurálása, tesztelése

Üzemmódok

- **Szállítási (transport) mód**
 - o Az AH vagy az ESP fejléc a csomag eredeti IP fejléce és a felsőbb szintű protokoll fejléce közé kerül.
- **Alagút (tunnel) mód**
 - o Az eredeti IP csomagot teljesen beágyazzuk egy másik IP csomagba.
 - o Az AH vagy az ESP fejléc az új és az eredeti IP fejléc közé kerül.
 - o Az AH fejléc vagy az ESP trailer következő fejléc mezője IP-re utal.

IPsec működése

- Adatgyűjtés
- Titkosítás
- Autentikáció
- Csomagolás
- Továbbítás
- Titkosítás feloldása
- Adatok fogadása

Konfigurálása

- ISAKMP policy
- Pre-shared key
- Érdemleges forgalom definiálása ACL segítségével
- IPSec policy
- Alagút paraméterek
- Interfészek kiválasztása

10.b Mutassa be a biztonság tervezési elveit! Határozza meg az információbiztonsági célok elérésére használható intézkedés típusokat, adjon példát ezekre intézményi környezetben!

Tervezés

1. A rendszerterv és a használt biztonsági protokoll legyen nyilvános.
2. Alapértelmezés legyen az, hogy valaki valamihez nem férhet hozzá.
3. A security-vel kapcsolatos kérdéseket a rendszer tervezésének korai fázisában tisztázni kell és a security csomagot a rendszer magjába integrálni kell.
4. Legyen a rendszer felhasználóbarát.
5. Ha lehet, akkor kerüljük az egész rendszer felett „teljes hatalommal bíró” (superuser, supervisor) rendszergazda koncepciót.
 - a. A rendszert bontsuk moduljaira, például egy-egy modul egy-egy fontosabb erőforrás kezelését végezze és az egyes moduloknak legyenek külön-külön felügyelői.

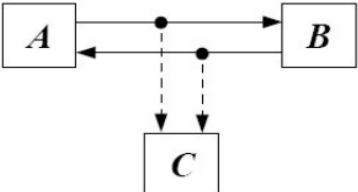
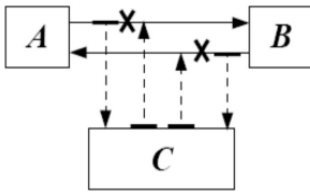
Legfontosabb nézőpontok

- Központi vírusvédelem
- Virtuális magánhálózatok (VPN) konfigurálása
- Jogosultságkezelés (hitelesítés, azonosítás)
- Tartalomszűrés (dokumentálás, logolás)
- Tűzfalak
- Behatolás detektáló rendszerek (intrusion-detection)
- Felhasználó és hozzáférés menedzsment
- Adatmentés

Hálózat védelme

- Támadó célja
 - o Információs szerzés
 - o Illetéktelen hozzáférés
 - o Szolgáltatások megbénítása
 - o Rendszer feltörése
 - o Rosszindulatú programok bejuttatása

Aktív és passzív támadások

Passzív	Aktív
A lehallgatás (evesdropping, wire-tapping), az érzékeny információ megszerzésére irányul, a támadó nem módosítja az átviteli csatorna tartalmát.	A támadó maga is forgalmaz a csatornán <ul style="list-style-type: none"> • üzenetmódosítás • megszemélyesítés • visszajátszás • szolgáltatás megtagadás (DoS – denial of service) típusú támadások
	

Csomag szintű támadások

IP spoofing

- IP cím hamisítása
- **Védekezés:** A tűzfalak bizonyos forrás IP címeket csak bizonyos irányból fogadnak el.

Smurf

- DoS típusú támadás, ami a megtámadott gép nevében ICMP echo request üzenetet küld egy irányított IP broadcast címre.
- **Védekezés:** A routerek IP broadcast-ot ne engedje át, IP broadcast címre ICMP echo request-re a gépeink ne válaszoljanak.

SYN flood

- DoS támadás
- Ha a rosszindulatú **C** támadó az **A** nevében nagy mennyiségű SYN csomagot küld **B**-nek (**C** nem kapja meg a válaszokat), akkor ezzel kimeríti **B** erőforrásait és az nem lesz képes fogadni a valódi kéréseket.
- **Védekezés:**
 - o Mikro blokkok használatával:
 - A szabványos adatstruktúráknál lényegesen kisebb helyet foglalunk le, és ha a kapcsolat kérés valódinak bizonyul, csak akkor foglaljuk le a szükséges erőforrásokat (10x annyi támadó csomagot bírunk el).
 - SYN cookie használatával.

Xmas, Ymas

- A TCP fejrészben az URG bittől balra levő két bitet 2003 májusában az IANA (Internet Assigned Numbers Authority) az ECN (Explicit Congestion Notification) mechanizmus céljára osztotta ki.
- A korábbi TCP implementációk azt várják el, hogy ez a 2 bit 0 értékű legyen.
- A bitek 0-tólkülönböző értékre állításával és a TCP implementáció viselkedésének megfigyelésével a támadó információt szerezhet a TCP/IP protocol stack implementációjáról.

Hálózati szintű támadások

Switchek elleni támadás

- **Switch normál működése:** Keretek továbbítása csak arra a portra, ahol a címzett található.
- **Portokhoz MAC címek beállítása:**
 - o Statikusan, munkaigényes konfiguráció változásánál át kell vezetni (hálókártya csere)
 - o Öntanuló módban, megjegyzi, hogy az egyes MAC címekkel forráscímként melyik portján találkozott.
- Ha a támadó sok különböző MAC címmel való forgalmazással, megtelíti a switch táblázatát, akkor a működés fenntartása érdekében minden keretet minden portjára kiküld (fail open). Ezzel a forgalom lehallgathatóvá válik.

ARP poisoning

- A támadó kéretlen és hamis ARP válaszokat küld, amiben a kérdéses IP címhez a saját MAC címét tünteti fel.
- **ARP (Address Resolution Protocol):** Címlekérdező protokoll. Üzenetszórásos hálózatokon broadcast (minden gépnek szóló) üzenettel megszerzi az információt (IP cím – fizikai cím összerendelés) és elraktározza (cache).

ICMP redirect

- Az ICMP redirect üzenettel egy router egy számítógép számára egy jobb útvonalat tud megadni. A támadó ezzel maga felé tudja irányítani a megtámadott gép forgalmát.
- Használhatja pl:
 - o Lehallgatásra: A csomagokat tovább küldi a címzettnek, hogy a támadás észrevétlen maradjon.
 - o IP spoofing támogatásra: A redirecttel elérte, hogy az A válaszai őhozzá érkezzenek, a TCP kapcsolat ténylegesen felépül.
- **Védekezés: accept_redirects** kikapcsolása.

RIP (Routing Information Protocol) távolságvektor hamisítása

- RIP: Distance-vector protokoll, ami egy célponthoz (hálózatok, subnetek, állomások vagy a default router) táblázatában tárolja:
- A célpont IP címét.
- Az odavezető út költségét (egy csomagnak az adott linken való átküldésének költsége alapján).
- Az odavezető út első routerét.
- Időzítőket
- Mivel a RIP nem használ autentikációt, a támadó számítógépe hamis távolságvektorral becsaphatja a routereket azt állítva, hogy rajta keresztül rövidebb út vezet a cél felé.

Source route IP opció

- A forrás megadhatja, hogy adott IP című állomás felé mely routereken keresztül haladjon a csomag.
- Támadó: privát IP című hálózatok elérésére.
- A **C** támadó az **R1** routernek megmondja, hogy **R2**-n keresztül kell a csomagot küldenie. **R2** privát IP címmel rendelkező hálózat gateway-e, a datagrammot már a cél IP cím alapján küldi a címzettnek.
- A visszaút: A támadó publikus IP címmel rendelkezik.
- **Védekezés: accept_source_router** kikapcsolása.

DNS (cache) ellen való támadás

- Kihasználja, hogy lejár az ns.myisp.com által tárol www.mybank.com TTL (Time To Live) ideje.

Felhasználók védelme

- Legnagyobb probléma a jelszavak.
- Erős jelszó megkötése:
 - o Több karakter
 - o Kis-nagybetű
 - o Számok
 - o Speciális karakterek
- Kerberos, LDAP, NIS
- Jelszavakat védett fájlban tároljuk
- Jelszavak titkos kezelése, például nem írjuk fel publikus cetlire.

Szerverek védelme

- Folyamatos vizsgálat
 - o Rajta futó programok
 - o Hozzáférések naplózása
- Tűzfalak használata
 - o Alapértelmezetten portok tiltása
- Naplózás
 - o Külön partícióra
- Fájlrendszer megfelelő kialakítása
 - o Jogosultságok kezelése
 - o Írás jogokat nem adunk mindenkinek
- Külön szerverek a szolgáltatásoknak
 - o FTP, DNS, WEB
- Virtualizáció
- Biztonsági frissítések és adatmentések

11.a Milyen forgalom védelmét látja el az SSL (Secure Socket Layer) protokoll és miben befolyásolhatja ez a tervezést? Mutassa be az SSL protokoll felépítését és működését!

Az SSL protokoll célja és feladata, szerkezeti felépítése, alprotokolljai és feladatai

SSL célja

- Titkosított kommunikációt biztosító protokoll, ami nyílt hálózatokban, kapcsolatorientált kommunikációban nyújt védelmet.
- Csak egy-egy kommunikációs csatornát biztosít.
- Gyakran használják a weboldalak biztonságos titkosítására is.

SSL szerkezeti felépítése

- Minden egyes kapcsolat egyedi kulccsal titkosít.
- Tanúsítvány igazolja a szerveret.
- Biztosítja az adatintegritást. (MD5, SHA-1)

SSL működése

1. Kliens csatlakozik a kiszolgálóhoz.
2. Kiszolgáló elküldi a hitelesítési tanúsítványt a kliensnek.
3. Kliens ellenőrzi a tanúsítvány hitelességét, majd létrehozza a titkosított kapcsolatot a kiszolgálóval.
4. Kliens és kiszolgáló között így már biztonságosan lehet adatokat cserélni.
5. Ha az SSL kapcsolat megszakad, akkor a kliens és a kiszolgáló kapcsolata is megszakad.

SSL alprotokolljai

Rekord protokoll

- Feladata a kliens és a szerver és a felsőbb SSL protokoll entitások védelme:
 - Titkosítás, integritásvédelem, üzenet-visszajátszás elleni védelem

Handshake protokoll

- Rekord protokollban használt kriptográfiai algoritmusok és paramétereik egyeztetése.
- Kulcscsere és hitelesítés

Change-Cipher-Spec protokoll

- Egyetlen üzenetből áll, ami a Handshake protokoll kulcscsere részének végét jelzi.
- Ezt az üzenetet elküldi, utána az adott fél az új algoritmusokat és kulcsokat kezdi használni a küldése.
 - A vétel még mindig a Handshake előtti állapot szerint történik.

Alert protokoll

- Figyelmeztető és hibaüzenetek továbbítása.

A handshake, valamint a record alprotokoll feladata, működése és üzenetei

Rekord protokoll működése

- A felsőbb protokoll rétegektől érkező üzeneteket:
 - o Fragmentálja, ha szükséges.
 - o Fragmenseket tömöríti
 - o Tömörített fragmenseket fejléccel látja el
 - o Fejléccel ellátott, tömörített fragmensre üzenethitelesítő kódot/MAC-et számol és azt a fragmenshez csatolja.
 - o Az üzenethitelesítő kóddal ellátott fragmenst rejtjelezi.

Rekord üzenetei

- **type:** Rekord üzenetben melyik felsőbb protokoll található.
- **version:** SSL verzió
- **length:** Fragmens hosszát tartalmazza bájtban mérve.
- **MAC:** Üzenethitelesítő kód generálása

Handshake protokoll működése

1. **fázis:** Kliens és szerver elküldi a tulajdonságait, megállapodnak
2. **fázis:**
 - a. Kulcscseremódszertől függ
 - b. Szerver elküldi a tanúsítványát és kéri a kliens tanúsítványát.
3. **fázis:** Tanúsítvány ellenőrzés és kulcscsere folytatása
4. **fázis:** Kulcscsere életbelépése, befejezése

Handshake üzenetei

- **KliensHello:**
 - o Kliens küldi ezt az üzenetet az SSL Handshake kezdeményezésére.
 - o Kliens verzió, véletlenszám, viszonyazonosító, biztonsági algoritmusok, tömörítő algoritmusok
- **SzerverHello:**
 - o Kiszolgáló küldi a **KliensHello** üzenetre válaszul.
 - o Szerver verzió, véletlenszám, viszonyazonosító, biztonsági algoritmusok, tömörítő algoritmusok
- **Szerver kulcscsere üzenet**
- **Tanúsítvány kérés**
 - o Előfordulhat olyan eset is, amikor a tanúsító hatóságok listája üres.
 - Ilyenkor a kliens eldöntheti, hogy elküldi-e az ügyféltanúsítványt vagy sem.
- **Kliens tanúsítvány**
 - o A kliens bemutatja a tanúsítványláncát a kiszolgálónak.
- **Kliens kulcscsere üzenet**
 - o Lényege, hogy létrehozza a közös kulcsot a kliens és a kiszolgáló között anélkül, hogy azt egy kívülálló számára felfedné.
- **Kész üzenet**
 - o Első olyan üzenet, ami már az új algoritmusokat használva, az új kulcsokkal van kódolva.

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!

Security Management eszközök

- **Elemzés**
 - o Microsoft Baseline Security Analyzer
 - o Systems Management Server
 - o Microsoft Software Update Services
 - o Security Configuration and Analysis snap-in
 - o RSoP
- **Management**
 - o Group Policy Management Console
 - o Microsoft Operations Manager
 - o Systems Management Server
 - o Microsoft Software Update Services
 - o ISA Server

Frissítés szükségessége

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

WSUS üzemeltetés

- Windows Server Update Services
- Kiszolgáló előfeltételek megteremtése
- Adatbázis kezelő telepítése
- WSUS kiszolgáló telepítése és konfigurálása
- Tűzfal konfigurálása
- Kliens telepítés megtervezése, beállítása
- Csoportos házirend, Gépek csoportosítása, teszt kijelölése
- Üzemeltetés

WSUS követelmények

- **Szerver**
 - o x64 alapú, legalább 2GHz
 - o RAM 2 GB felett, Tárhely 10GB felett
 - o Internet sebessége legalább 100Mbps
- **Kliens**
 - o Minimum Windows 2000 Server

WSUS konfigurálása

1. Be kell állítani, hogy a kiszolgáló honnan töltsen le a frissítéseket. **Upstream Server**, ahol két opció közül lehet választani:
 - **Microsoft Update-ből való szinkronizálás:**
 - 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.

12.a Ismertesse a hálózati kommunikáció védelmére alkalmazott kriptográfiai algoritmusokat! Magyarázza el működésüket!

Kriptográfia

- A kriptográfia lényege, hogy az adatokat biztonságban tárolhassuk az illetéktelen hozzáférések ellen és adatküldésnél a CIA elvek alapján biztonságban áramoljon az információ.
- **Elvárások**
 - o Gyors encryptelés és a megfelelő decrypt kulcs esetén visszafejthetőség vagy egyirányú legyen.

Adatkapcsolati titkosítások

- **AES – Advanced Encryption Standard:**
 - o Alacsony memóriaigény, gyors, leváltotta a **DES**-t.
 - o Szimmetrikus blokk-kódolás
 - o Támogatja a 128, 256 bit hosszú kulcsokat
- **RSA - Manapság leggyakrabban használt**
 - o Titkosításhoz egy nyílt és egy titkos kulcs tartozik.
 - o Nyílt kulcs bárki számára elérhető, és ezzel lehet kódolni a másoknak szánt üzenetet.
 - o Titkos kulccsal lehet megfejteni a nyílt kulccsal kódolt üzenetet.
- **MD5**
 - o Egyirányú
 - o 128 bites
- **SHA**
 - o Bármilyen hosszú karakterláncból adott hosszúságú hash-t állít elő.
 - o Több fajtája létezik
 - o SHA-256 elterjedt

Szimmetrikus titkosítás

- Lényege, hogy a küldő és a fogadó is ugyanazzal a kulccsal végzi a titkosítást és a visszafejtést.
- Használata olyankor célszerű, amikor a kulcsokat nem kell folyton küldözgetni.
- Leggyakrabban használt algoritmusok: DES, 3DES, AES

Asszimmetrikus titkosítás

- Az algoritmus kulcspárral dolgozik, nyilvános és privát kulcsot használ.
- A nyilvános kulcs szabadon továbbítható, a privát kulcsot biztonságban kell tartani.
- A kulcs egyik párjából nem következtethető a másik fele.
- Diffie-Hellman módszerén alapszik a működése, RSA módszer során használják.

IPSec

AH – Authentication Header

- Sértetlenséget, hitelesítést és visszajátszás elleni védelmet biztosít.
- Beszúr egy AH fejléctet, ami egy MAC-et tartalmaz.
- A visszajátszás detektálásának érdekében, az IP csomagokat sorszámozza.
- Az AH fejlécben található MAC érték a sorszámot is védi.

ESP – Encapsulated Security Payload

- Feladata az IP csomag tartalmának rejtése és opcionálisan a tartalom integritásának védelme.
- IP csomag tartalmának rejtését rejtjelezéssel oldja meg.
- **Tartalom integritásának védelme:** ESP fejlécre és a csomag tartalmára számít MAC kódot és azt a csomaghoz csatolja.
- ESP MAC nem védi az IP fejléc mezőit.

ISAKMP – Internet Security Association and Key Management Protocol

- Általános célú keretprotokoll, ami bármilyen konkrét kulcscsere protokoll üzeneteit képes szállítani.

IKE – Internet Key Exchange

- IPSec hivatalos kulcscsere protokollja.
- A host-ok ebben a fázisban hitelesítik egymást shared secret vagy RSA kulcs segítségével.
- Felépítenek egy kétirányú ISAKMP SA-t.
- Az ISAKMP SA-t alkalmazva megvitatják az egyirányú IPSec SA-kat.

SSL célja

- Titkosított kommunikációt biztosító protokoll, ami nyílt hálózatokban, kapcsolatorientált kommunikációban nyújt védelmet.
- Csak egy-egy kommunikációs csatornát biztosít.
- Gyakran használják a weboldalak biztonságos titkosítására is.

SSL szerkezeti felépítése

- Minden egyes kapcsolat egyedi kulccsal titkosít.
- Tanúsítvány igazolja a szervert.
- Biztosítja az adatintegritást. (MD5, SHA-1)

SSL működése

1. Kliens csatlakozik a kiszolgálóhoz.
2. Kiszolgáló elküldi a hitelesítési tanúsítványt a kliensnek.
3. Kliens ellenőrzi a tanúsítvány hitelességét, majd létrehozza a titkosított kapcsolatot a kiszolgálóval.
4. Kliens és kiszolgáló között így már biztonságosan lehet adatokat cserélni.
5. Ha az SSL kapcsolat megszakad, akkor a kliens és a kiszolgáló kapcsolata is megszakad.

SSL alprotokolljai

Rekord protokoll

- Feladata a kliens és a szerver és a felsőbb SSL protokoll entitások védelme:
 - Titkosítás, integritásvédelem, üzenet-visszajátszás elleni védelem

Handshake protokoll

- Rekord protokollban használt kriptográfiai algoritmusok és paramétereik egyeztetése.
- Kulcscsere és hitelesítés

Change-Cipher-Spec protokoll

- Egyetlen üzenetből áll, ami a Handshake protokoll kulcscsere részének végét jelzi.
- Ezt az üzenetet elküldi, utána az adott fél az új algoritmusokat és kulcsokat kezdi használni a küldése.
 - A vétel még mindig a Handshake előtti állapot szerint történik.

Alert protokoll

- Figyelmeztető és hibaüzenetek továbbítása.

12.b Határozza meg az informatikai biztonság szabályzási és dokumentációs rendszerét, adjon példát az egyes dokumentumok tartalmára intézményi környezetben!

Mi a szabályozási rendszer?

- Fontos szerepet játszik az intézmények biztonságos és hatékony működésében, mivel biztosítja a szabályok és előírások betartását, megelőzve az esetleges jogi, biztonsági vagy reputációs kockázatokat.
- Az informatikai biztonság szabályzási és dokumentációs rendszere egy olyan strukturált módszer, ami segíti az intézményeket abban, hogy az információik biztonságosan legyenek kezelve és védelmezve legyenek.
 - o A rendszer magában foglalja azokat a szabályokat, folyamatokat, dokumentumokat és eljárásokat, amik az intézmény informatikai rendszerének biztonságához szükségesek.

Felhasználói kézikönyv

- Ez a dokumentum az informatikai eszközök használatára vonatkozó legfontosabb irányelveket tartalmazza, beleértve a felhasználói fiókok kezelését, az adatok tárolását és a biztonsági szabályokat.

Rendszerdokumentáció

- Ez a dokumentum az informatikai rendszerek és szolgáltatások részletes leírását tartalmazza, beleértve a rendszer felépítését, a telepített szoftvereket és azok konfigurációját.

Rendszerfelügyeleti dokumentáció

- Ez a dokumentum az informatikai rendszerek és szolgáltatások működésének felügyeletére vonatkozó részletes eljárásokat tartalmazza, beleértve a rendszeres karbantartást, a mentéseket és a hibaelhárítást.

Jogi dokumentumok

- Ezek a dokumentumok az adatvédelmre és az információvédelemre vonatkozó jogszabályokat és rendeleteket tartalmazzák.
 - o Például az adatvédelmi szabályzat, a felhasználói szerződés vagy az adatvédelmi tájékoztató.

Mentési dokumentáció

- Ez a dokumentum az adatmentési folyamatokat és eljárásokat írja le, beleértve a mentési tervet, a mentési protokollokat és az adatok helyreállítását.

Információbiztonsági kézikönyv

- Az információbiztonsági kézikönyv a szervezet informatikai biztonsági folyamatait és eljárásait részletesen tartalmazza, ideértve a hozzáférést-kezelést, az adatvédelmi eljárásokat és az incidenskezelést is.

Felhasználói szabályzat

- A felhasználói szabályzat részletesen meghatározza azokat a szabályokat és eljárásokat, amiket az intézmény dolgozói kötelesek betartani, beleértve a jelszóhasználatot, az internetes és az email használatot is.

Biztonsági audit jelentések

- A biztonsági audit jelentések dokumentálják az intézmény informatikai rendszerének ellenőrzését és értékelését.
- A jelentésekben szerepelnek azonosított hibák és javaslatok a rendszer javítására.

Rendszerbevezetési dokumentáció

- A rendszerbevezetési dokumentáció leírja az informatikai rendszer telepítését és konfigurálását és az alkalmazott biztonsági beállításokat és teszteket.

Rendszerfelügyeleti naplók

- A rendszerfelügyeleti naplók azok a naplóbejegyzések, amiket a számítógépes rendszer felügyelete alatt gyűjtenek és tárolnak.

13.a Ismertesse a 2. (adatkapcsolati) rétegbeli hálózati támadások fajtáit! Milyen protokollok biztonsági réseit használják ki ezek a támadások?

Támadás fajtái

CAM Table Attack

- Hamis MAC címek áradatát küldi a switch-nek.
- Ez az adatáradat arra készteti a switch-et, hogy a CAM- adatbázis tábláiban lévő érvényes címeket kidobja, hogy helyet csináljon a hamis információknak.

VLAN Attack

- **VLAN Hopping**
 - o A VLAN hálózati erőforrásainak támadására szolgáló módszer, ami csomagok küldésével történik egy olyan portra, ami általában nem érhető el egy végrendszerből.
 - o Fő célja, hogy hozzáférést szerezzen más VLAN-okhoz ugyanabban a hálózatban.

STP Attack

- Az STP támadásakor a támadó meghamisítja a root bridge-t a topológiában.
 - o A támadó egy STP konfiguráció/topológiaváltás BPDU-t sugároz ki, hogy megpróbálja kikényszeríteni az STP újraszámítását.
 - o A kiküldött BPDU azt jelenti, hogy a támadó rendszere lower bridge prioritással rendelkezik.

DHCP Attack

- **DHCP starvation**
 - o A DHCP starvation támadás egy olyan támadás, ami a DHCP kiszolgálókat célozza és aminek során a támadó hamisított DHCP kérelmeket készít azzal a céllal, hogy kimerítse a DHCP kiszolgáló által kiosztható összes rendelkezésre álló IP címet.
- **DHCP snooping**
 - o A DHCP snooping egy olyan biztonsági funkció, ami tűzfalként működik a nem megbízható állomás és a megbízható DHCP kiszolgálók között.
 - o A DHCP snooping érvényesíti a nem megbízható forrásokból érkező DHCP üzeneteket és kiszűri az érvénytelen üzeneteket.

ARP Attack

- **ARP spoofing**
 - o A támadó hamis ARP csomagokat küld, amik összekapcsolják a támadó MAC címét a LAN-on lévő számítógép IP címével.
- **ARP poisoning**
 - o A sikeres ARP spoofing után a támadó megváltoztatja a vállalat ARP táblát, így a hamisított MAC térképeket tartalmaz és a fertőzés elterjed.

Address Spoofing Attack

- **Mac address spoofing**

- A Mac address spoofing egy olyan technika, ami egy hálózati eszköz hálózati interfészének gyárilag kiosztott MAC címét változtatja meg.
 - A hálózat interfészvezérlő (NIC) keményen kódolt MAC-cím nem módosítható.
 - Sok illesztőprogram lehetővé teszi a MAC cím megváltoztatását.

13.b Ismertesse az adatok biztonsági mentési stratégiájának kialakítását befolyásoló kritériumokat, ismertesse az adatok teljes, differenciális és inkrementális mentésének jellemzőit!

Biztonsági mentés fontossága

- A mentés célja a helyreállíthatóság biztosítása, adatvesztések elkerülése, minimalizálása másolati adatpéldányok készítésével.

Mentés célja

- Üzletfolytonosság biztosítása
- **Törlés**
 - o A felhasználó véletlenül vagy szándékosan
- **Meghibásodás**
 - o Egy tároló eszköz vagy elromlott a rendszer

Mentési stratégia kialakítását befolyásoló tényezők

- **Adattípusok**
 - o Adatok jellege
 - o Mennyire kritikus adat
 - o Meddig kell tárolni
- **Adatmennyiség**
 - o Mentési időt befolyásolja
- **Adatok helye**
 - o Honnan/hova szeretnénk menteni
- **Mentési gyakoriság**
 - o Adatok fontossága, mennyisége
- **Mentési típusok**
 - o Teljes
 - o Differenciális
 - o Inkrementális

Differenciális mentés

- Ciklus első napján teljes mentés
- Utána minden nap csak az előző teljes mentés óta történt változások
 - o Nagyobb, egyre növekvő napi adatmennyiség
- Gyorsabb és hatékonyabb, mint a teljes mentés
- Maximum 2 helyreállítási folyamatot igényel az adat visszaállítása

Inkrementális mentés

- Ciklus első napján teljes mentés
- Utána minden nap csak az előző óta történt változások
 - o Kis adatmennyiség, emiatt gyors és kisebb követelményei vannak, mint a differenciális mentésnél.
- Hosszú visszaállítási idő
 - o Az adatok visszaállítása, több egymást követő mentésekből álló folyamatot igényel.

14.a Ismertesse a 2. (adatkapcsolati) rétegbeli hálózati támadások kivédésének módjait!

Támadás fajtái

CAM Table Attack

- Hamis MAC címek áradatát küldi a switch-nek.
- Ez az adatáradat arra készíti a switch-et, hogy a CAM- adatbázis tábláiban lévő érvényes címeket kidobja, hogy helyet csináljon a hamis információknak.
- **Kivédése**
 - o Port security, vagyis a port nem továbbít olyan csomagot, amik forráscímei nem tartoznak a meghatározott címek csoportjába.

VLAN Attack

- **VLAN Hopping**
 - o A VLAN hálózati erőforrásainak támadására szolgáló módszer, ami csomagok küldésével történik egy olyan portra, ami általában nem érhető el egy végrendszerből.
 - o Fő célja, hogy hozzáférést szerezzen más VLAN-okhoz ugyanabban a hálózatban.
 - o **Kivédése**
 - DTP (automatikus trunk) negotiation letiltása a nem trunk (switchport mode access) és trunk portokon (switchport non-negotiate).
 - Nem használt portok letiltása és külön VLAN-ba helyezése
 - Trunk port engedélyezése manuálisan (switchport mode trunk)
 - VLAN 1 ne legyen natív, használaton kívüli VLAN-ra állítsa be.

STP Attack

- Az STP támadásakor a támadó meghamisítja a root bridge-t a topológiában.
 - o A támadó egy STP konfiguráció/topológiaváltás BPDU-t sugároz ki, hogy megpróbálja kikényszeríteni az STP újraszámítását.
 - o A kiküldött BPDU azt jelenti, hogy a támadó rendszere lower bridge prioritással rendelkezik.
- **Kivédése:**
 - o BPDU Guard
 - o Root Guard
 - o Loop Guard

Address Spoofing Attack

- **Mac address spoofing**
 - o A Mac address spoofing egy olyan technika, ami egy hálózati eszköz hálózati interfészének gyárilag kiosztott MAC címét változtatja meg.
 - A hálózat interfészvezérlő (NIC) keményen kódolt MAC-cím nem módosítható.
 - Sok illesztőprogram lehetővé teszi a MAC cím megváltoztatását.
 - o **Kivédése**
 - Port security
 - Megengedett MAC-címek számának korlátozása egy porton.

DHCP Attack

- **DHCP starvation**
 - A DHCP starvation támadás egy olyan támadás, ami a DHCP kiszolgálókat célozza és aminek során a támadó hamisított DHCP kérelmeket készít azzal a céllal, hogy kimerítse a DHCP kiszolgáló által kiosztható összes rendelkezésre álló IP címet.
- **DHCP snooping**
 - A DHCP snooping egy olyan biztonsági funkció, ami tűzfalként működik a nem megbízható állomás és a megbízható DHCP kiszolgálók között.
 - A DHCP snooping érvényesíti a nem megbízható forrásokból érkező DHCP üzeneteket és kiszűri az érvénytelen üzeneteket.
- **Kivédése**
 - DHCP snooping megbízható port beállítása
 - DOT1x autentikáció
 - Port security
 - Nem használt portok lekapcsolása

ARP Attack

- **ARP spoofing**
 - A támadó hamis ARP csomagokat küld, amik összekapcsolják a támadó MAC címét a LAN-on lévő számítógép IP címével.
- **ARP poisoning**
 - A sikeres ARP spoofing után a támadó megváltoztatja a vállalat ARP táblát, így a hamisított MAC térképeket tartalmaz és a fertőzés elterjed.
- **Kivédése:**
 - Dynamic ARP Inspection használata
 - DHCP snooping validálja

14.b Elemezze a távoli munkavégzést a biztonság szemszögéből!
Relevancia. Problémák az elérendő célok szerint. Kivitelezési lehetőségek.

Igény

- Manapság egyre nagyobb az igény a távoli munkavégzésre, amit manapság „Home Office”-nak is nevezünk.
 - o Tehát távmunka vezeték nélkül azon a gépen, ami a céges környezeten belül helyezkedik, ahol a hálózathoz is hozzá lehet férni.
- Általában ehhez szükséges:
 - o RDP
 - o HTTPS
 - o VPN
 - o SSH

Problémák

- **Távoli elérés sosem biztonságos, mert:**
 - o Más is használhatja a távoli gépet.
 - o Nincs felügyelet, nincs központi figyelés.
 - o Nincs Group Policy, központi antivirus szoftver
- Adatlopás
- Identitáslopás

Példák

„Scam”, vagyis csaló email-ek

- Viszonylag ez a legtöbbet használt „támadási” fajta, amivel elhitetjük a potenciális áldozattal, hogy például nyert x összeget a lottón és azt átutalják, ha megadja a bankszámla adatait az illető.
- A támadók általában valamilyen programot, bot-ot használnak, hogy automatizálják a „támadást”.
- Ezt úgy tudjuk elkerülni, hogy vagy szűrőt használunk, ami alapján blokkoljuk a csaló email-eket vagy megbizonyosodunk a küldőről, hogy tényleg az, akinek ő hiteti magát.

Gyenge jelszavak

- Single Sign On, vagyis mindenhol ugyanaz a jelszó van használatban.
- Kódolatlan HTTP weboldalak.
- Plain-text-ben való jelszó megosztás.
- **Megoldás:**
 - o Ne használjuk a vállalati jelszavunkat, ha a weboldal kódolatlan HTTP oldal.
 - o Ne használjuk ugyanazt a jelszót, használjunk jelszó generátort komplexebb mintákkal.

Gyenge biztonsági ellenőrzések

- A vállalaton belül tűzfal szabályokat kell bevezetnie.
 - o Csak a tényleges szolgáltatásokat engedjük át, amit nem használunk vagy nem is tudunk róla, hogy mi célt szolgál, azt kapcsoljuk le.
- Fontos a monitorozás is, de előfordulhat olyan is, hogy például a vállalat ad egy laptopot a dolgozónak, így technikailag nem a vállalat környezetén belül dolgozik, hanem fizikailag azon a laptopon.
 - o Ezzel az a probléma, hogy így már nem tudja a vállalat feltétlenül monitorozni például a hálózati forgalmat.

Hálózati támadások

- Tegyük fel, hogy miután az áldozat rákattintott egy linkre, amit az áldozat küldött email-ben, az adatokat gyűjtött az áldozatról.
 - o Megszerzett olyan adatokat, mint az IP, lokáció, név.
 - o Ez alapján végrehajthat egy port szkenneléses támadást.
 - o Majd rájön, hogy az RDP port nyitva van, így brute force, vagyis nyers erő módszerével megpróbálja feltörni az áldozat gépét.
- Meg is tudja bénítani az áldozatot DDoS támadással vagy elérheti, hogy a teljes vállalat hálózata ne legyen elérhető.

Nyilvános helyen történő munkavégzés

- Például egy dolgozó egy kávézóban dolgozik épp a laptopján és rácsatlakozik a nyilvános, ingyenes Wi-Fi-re, akkor azt könnyedén le lehet hallgatni.
- Előfordulhat az is, hogy érzékeny adatok vannak a kijelzőn és azt valaki meglátja és hasznot húz belőle vagy ott hagyja a laptopot felügyelet nélkül.

Titkosítatlan fájlmegosztás

- Mai napig sokan használják az FTP szolgáltatást fájlmegosztásra, ami nem túl biztonságos.
 - o Plain-text felhasználónév és jelszó és az adatátvitel nincs titkosítva.
 - o Emiatt használhatóak a packet sniffing, spoofing és brute force támadások.
- Sokkal biztonságosabb az SFTP, ami Secure Shell kriptográfián alapszik adatátvitelkor.
 - o Mivel az információt csomagokban továbbítják, nem pedig plain-text-ben, ami gyorsabb átviteli időt eredményez az FTP-hez képest.

Rossz konfigurációk környezetben belül

- Jogosultság kezelést be kell vezetni a környezetben belül, viszont előfordulhat, hogy a vállalat nem fordít rá elég figyelmet, hogy kinek mihez is van joga.
 - o Például egy asszisztens ne férhessen hozzá a fejlesztők fájljaihoz.

Webkamerás támadás

- A támadó ezzel személyiségi jogok megsértését hajtja végre.
- Előfordulhat, hogy például egy dokumentum olyan látószögben van, ami alapján láthatóak a privát vállalati adatok, ami a támadó számára értékes lehet.

Megoldások

- Többlépcsős autentikáció használata.
- Jelszó kezelő szoftverek használata.
- Vállalaton belüli VPN
- Tűzfal alkalmazása szigorú szabályokkal
- Jogosultságkezelés
- Végponti biztonság fokozása