

Tartalomjegyzék

Bevezetés

1. fejezet. Itt gépkalózzok élnék!

- 1.1. A célpont kiválasztása
- 1.2. Ártalmatlan információk megszerzése
- 1.3. Alkalom szülte célok
 - 1.3.1. Alkalom szülte cél a hálózatom?
- 1.4. Kiválasztott célpontok
 - 1.4.1. Kiválasztott célponttá váltunk-e?
- 1.5. A támadás folyamata
 - 1.5.1. Felderítés és nyomkeresés (a helyszíni szemle)
 - 1.5.2. Letapogató
 - 1.5.3. Kiértékelés
 - 1.5.4. Hozzáférés megszerzése
 - 1.5.5. A jogosultságok kiterjesztése
 - 1.5.6. A nyomok elfedése
- 1.6. Hálózatbiztonsági szervezetek
 - 1.6.1. CERT Koordinációs Központ
 - 1.6.2. SANS
 - 1.6.3. Internetbiztonsági Központ (CIS)
 - 1.6.4. SCORE
 - 1.6.5. Internet Viharközpont
 - 1.6.6. ICAT Metabase
 - 1.6.7. Security Focus
 - 1.6.8. Mit tanulhatunk ezektől a szervezetektől?
- 1.7. Gyakori támadások áttekintése
- 1.8. Összefoglalás
- 1.9. Összefoglaló kérdések

2. fejezet. A biztonsági házirend és a felelősség

- 2.1. A bizalmi viszonyok meghatározása
- 2.2. Indokolható használati házirend
 - 2.2.1. Áttekintés

- 2.2.2. Célkitűzés
- 2.2.3. Hatályosság
- 2.2.4. Általános használat és tulajdonjog
- 2.2.5. Biztonsági és tulajdonjogi információk
- 2.2.6. Visszaélések
- 2.2.7. Büntetések
- 2.2.8. Következtetések
- 2.3. A jelszavak szabályozása
 - 2.3.1. Áttekintés
 - 2.3.2. Célkitűzés
 - 2.3.3. Hatályosság
 - 2.3.4. Általános szabályok
 - 2.3.5. A jelszókészítés általános alapelvei
 - 2.3.6. Jelszóvédelmi szabályok
 - 2.3.7. Büntetések
 - 2.3.8. Következtetések
- 2.4. A virtuális magánhálózat (VPN) biztonsági szabályzata
 - 2.4.1. Célkitűzés
 - 2.4.2. Hatályosság
 - 2.4.3. Általános szabályok
 - 2.4.4. Következtetések
- 2.5. Az extranet-csatlakozás házirendje
 - 2.5.1. Célkitűzés
 - 2.5.2. hatályosság
 - 2.5.3. Biztonsági átvizsgálás
 - 2.5.4. A másik fél csatlakozási szerződése
 - 2.5.5. Üzleti érdek
 - 2.5.6. Kapcsolattartási pont
 - 2.5.7. A csatlakozás létrehozása
 - 2.5.8. A hozzáférés és a csatlakozás módosítása
 - 2.5.9. A hozzáférés visszavonása
 - 2.5.10. Következtetések
- 2.6. Az ISO-minősítés és a biztonság
- 2.7. Példák biztonsági szabályzatokra az interneten
- 2.8. Összefoglalás

2.9. Összefoglaló kérdések

3. fejezet. A biztonsági technológiák áttekintése

- 3.1. A biztonság fő tervezési elvei
- 3.2. Csomagszűrés a hozzáférés-vezérlő lista segítségével
 - 3.2.1. A bevásárló lista analógiája
 - 3.2.2. A csomagszűrés korlátai
- 3.3. Állapotteljes csomagvizsgálat
 - 3.3.1. Az SPI használatával kezelt bővített csomagfolyam
 - 3.3.2. Az állapotteljes csomagvizsgálat korlátai
- 3.4. A hálózati címfordítás
 - 3.4.1. A hálózatbiztonság növelése
 - 3.4.2. A címfordítás korlátai
- 3.5. A közvetítők és az alkalmazásszintű védelem
 - 3.5.1. A közvetítő korlátai
- 3.6. Tartalomszűrés
 - 3.6.1. A tartalomszűrés hátrányai
- 3.7. Nyilvános kulcsú infrastruktúra
 - 3.7.1. A PKI hátrányai
- 3.8. AAA technológiák
 - 3.8.1. Hitelesítés (azonosítás)
 - 3.8.2. Feljogosítás
 - 3.8.3. Könyvelés
 - 3.8.4. RADIUS
 - 3.8.5. TACACS
 - 3.8.6. A TACACS+ és a RADIUS összehasonlítása
- 3.9. Összefoglalás
- 3.10. Összefoglaló kérdések

4. fejezet. Biztonsági protokollok

- 4.1. A DES titkosítás
 - 4.1.1. A titkosítás erőssége
 - 4.1.2. A DES korlátai
- 4.2. A tripla DES (3DES) titkosítás
 - 4.2.1. A titkosítás erőssége

- 4.2.2. A 3DES korlátai
- 4.3. Az MD5 algoritmus
 - 4.3.1. Az MD5 algoritmus működése
- 4.4. A pont-pont közti alagútprotokoll (PPTP)
 - 4.4.1. A PPTP működése
 - 4.4.2. A PPTP korlátai
- 4.5. A második rétegbeli alagútprotokoll (L2TP)
 - 4.5.1. Az L2TP és a PPTP összehasonlítása
 - 4.5.2. Az L2TP előnyei
 - 4.5.3. Az L2TP működése
- 4.6. A biztonságos távelérés
 - 4.6.1. Az SSH és a telnet összehasonlítása
 - 4.6.2. Az SSH működése
 - 4.6.3. Alagút kiépítése és végpont áthelyezése
 - 4.6.4. Az SSH korlátai
- 4.7. Összefoglalás
- 4.8. Összefoglaló kérdések

5. fejezet. Tűzfalak

- 5.1. Gyakran ismételt kérdések a tűzfalakkal kapcsolatban
 - 5.1.1. Kinek van szüksége tűzfalakra?
 - 5.1.2. Miért van szükségem tűzfalakra?
 - 5.1.3. Vannak-e megvédendő értékeim?
 - 5.1.4. Hogyan működik a tűzfal?
- 5.2. A tűzfal maga a biztonsági házirend
- 5.3. A tűzfal működésének áttekintése
 - 5.3.1. A tűzfal működése
 - 5.3.2. A tűzfal alkalmazása
 - 5.3.3. A bejövő forgalomra vonatkozó szabályzat meghatározása
 - 5.3.4. A kimenő forgalomra vonatkozó szabályzat meghatározása
- 5.4. Elsőként az alapelvek: élet a DMZ-ben
- 5.5. Esettanulmányok
 - 5.5.1. Esettanulmány: demilitarizálni vagy nem demilitarizálni?
 - 5.5.2. Esettanulmány: levelezőszerver a tűzfalal védett belső hálózatban
 - 5.5.3. Esettanulmány: a tűzfal beállítása (levelezőszerver a DMZ-ben)

5.6. A tűzfalak korlátai

5.7. Összefoglalás

5.8. Összefoglaló kérdések

6. fejezet. Az útválasztók biztonsága

6.1. A peremi útválasztó mint ellenőrzőpont

6.1.1. Az ellenőrzőpontként működő útválasztók korlátai

6.2. Csomagvizsgáló útválasztó

6.2.1. A tűzfalkészlet előnyei

6.2.2. Tartalomalapú csomagvizsgálat

6.2.3. A behatolás érzékelése a Cisco IOS segítségével

6.2.4. Mikor használjuk a tűzfalkészlet IDS-modulját?

6.2.5. A tűzfalkészlet IDS-moduljának működése

6.2.6. A tűzfalkészlet korlátai

6.3. Biztonságos IOS-sablon

6.4. Összefoglalás

6.5. Összefoglaló kérdések

7. fejezet. A virtuális magánhálózat biztonsága

7.1. A VPN a biztonságos összeköttetés

7.2. A VPN áttekintése

7.2.1. A VPN előnyei és célja

7.2.2. A VPN implementációs stratégiái

7.2.3. Megosztott alagút

7.3. Az IPSec VPN áttekintése

7.3.1. Az adatok hitelesítése és sértetlensége

7.3.2. Alagúttechnika

7.3.3. Titkosító módszerek

7.3.4. IPSec protokollok

7.3.5. Az IPSec működése

7.4. Az útválasztó beállítása VPN-végpontként

7.4.1. Az ISAKAMP beállítása

7.4.2. Az IPSec beállítása

7.5. A tűzfal VPN-beállítása a kliens-hozzáférés számára

7.6. Összefoglalás

7.7. Összefoglaló kérdések

8. fejezet. Drótnélküli biztonság

8.1. Kezdjük az alapokkal: a vezeték nélküli helyi hálózatok

8.1.1. Mi az a WI-Fi?

8.1.2. A vezeték nélküli hálózatok előnyei

8.1.3. A vezeték nélküli egyenlő a rádióhullámokkal

8.2. A vezeték nélküli hálózat

8.2.1. Működési módok

8.2.2. Hatósugár

8.2.3. Elérhető sáv szélesség

8.3. Drótnélküli háborús játékok

8.4. A drótnélküliség veszélyei

8.4.1. Lehallgatás

8.4.2. Szolgáltatásmegtagadási támadások

8.4.3. Szélhámos/jogosulatlan elérési pontok

8.4.4. Hibásan beállított elérési pontok

8.4.5. Hálózati visszaélések

8.5. Drótnélküli biztonság

8.5.1. Szolgáltatáskészlet-azonosító (SSID)

8.5.2. Az eszközök és az AP csatlakozása

8.5.3. A vezetékkel egyenértékű titkosság (WEP)

8.5.4. MAC címszűrés

8.5.5. Bővíthető hitelesítőprotokoll

8.5.6. A drótnélküli biztonság növelése

8.6. A drótnélküli támadók eszközei

8.6.1. NetStumbler

8.6.2. Vezeték nélküli csomagszaglászók

8.6.3. AirSNORT

8.7. Összefoglalás

8.8. Összefoglaló kérdések

9. fejezet. A behatolás érzékelése és a mézesbödön

9.1. A behatolás érzékelése

9.1.1. Az IDS működése

- 9.2. Hogyan lehet észrevenni a behatolást?
 - 9.2.1. A kommunikációfolyam újbóli összeállítása
 - 9.2.2. Protokollanalízis
 - 9.2.3. Az eltérés felismerése
 - 9.2.4. A minta egyezősége
 - 9.2.5. Naplóanalízis
 - 9.2.6. A módszerek kombinálása
 - 9.2.7. A behatolás megakadályozása
 - 9.2.8. Az IPS reakciója
 - 9.2.9. IDS-termékek
 - 9.2.10. Az IDS korlátai
- 9.3. A mézesbödön
 - 9.3.1. A mézesbödön tervezésének stratégiái
 - 9.3.2. A mézesbödön korlátai
- 9.4. Összefoglalás
- 9.5. Összefoglaló kérdések

10. fejezet. Kereskedelmi eszközök

- 10.1. A sebezhetőség elemzése
 - 10.1.1. Alapvető támadások
- 10.2. A biztonság kiértékelése és az áttörhetőség ellenőrzése
 - 10.2.1. A belső sérülékenységi és áttörhetőség ellenőrzése
 - 10.2.2. A külső sérülékenységi és áttörhetőség ellenőrzése
 - 10.2.3. Fizikai biztonsági kiértékelés
 - 10.2.4. Különböző kiértékelések
- 10.3. Sérülékenységi-ellenőrzők
 - 10.3.1. A sérülékenységi-ellenőrzők jellemzői és előnyei
 - 10.3.2. Nessus
 - 10.3.3. Retina
- 10.4. A védelem áttörhetőségét vizsgáló termékek
 - 10.4.1. Core Impact
- 10.5. Összefoglalás
- 10.6. Összefoglaló kérdések

A) függelék. Válaszok az összefoglaló kérdésekre

B) függelék. Fogalomtár

A szerzőről

Tárgymutató