SÉRÜLÉKENYSÉGVIZSGÁLATI METODIKÁK

Vezeték nélküli hálózatok vizsgálata

v 1.0

Hatályos:



Digitálisan aláírta: Kiss Tamás László
Dátum: 2026.10.12 07:35:48 +02'00'

Kiss Tamás László
Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Sérülékenységvizsgálati Főosztály

Figyelem! A dokumentum érzékeny információkat tartalmazhat!

1. Vizsgálatok összefoglaló leírása

A **vezeték nélküli hálózati** irányultság keretében az informatikai rendszerek ellenőrzése egyedi módszertan szerint történik. A vizsgálatok alapját automatizált sérülékenység-felderítő eszközök eredményei képezik, amelyeket a vizsgált rendszer technológiai sajátosságainak megfelelő, célzott manuális biztonsági tesztelés egészít ki.

A vizsgálat az egyedi módszertannak megfelelően az alábbi fő tesztelési területekre terjed ki:

- Információgyűjtés;
- Konfiguráció- és üzemeltetésbiztonság vizsgálata;
- Hálózati infrastruktúra vizsgálata;
- Hitelesítés vizsgálata;
- Hozzáféréskezelés vizsgálata;
- Hibakezelés vizsgálata.

2. Vizsgálatok részletes műszaki leírása

2.1 Vezeték nélküli eszközök fizikai felderítése - (WLAN-INFO-001)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek fizikai elhelyzése jelent-e kockázatot.

2.2 Vezeték nélküli eszközök hálózati felderítése - (WLAN-INFO-002)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközei milyen típusúak, illetve ezek publikus vagy jelszavazott hálózatból érhetők-e el.

2.3 Vezeték nélküli eszközök IP cím kiosztásának vizsgálata - (WLAN-INFO-003)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközei milyen struktúra alapján kezelik a hálózati IP címeket.

2.4 Vezeték nélküli eszköz keretrendszer információk felderítése - (WLAN-INFO-004)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközei milyen típusú operációs rendszerrel rendelkeznek.

2.5 Vezeték nélküli eszköz keretrendszer-módosításának vizsgálata - (WLAN-INFO-005)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek konfigurációja megfelelően védett-e módosítás ellen.

2.6 Megtévesztő hozzáférési pontok detektálása - (WLAN-INFO-006)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközei között megtalálható-e megtévesztő, adatgyűjtésre alkalmas rendszer.

2.7 Hálózati eszközök konfigurációjának vizsgálata - (WLAN-CONF-001)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközei megfelelően kerültek-e beállításra.

2.8 Infrastruktúra és alkalmazás adminisztrátori interfészek vizsgálata - (WLAN-CONF-002)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek működése szempontjából kritikus felületek szabadon hozzáférhetők-e.

2.9 Naplózás vizsgálata - (WLAN-CONF-003)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközein végzett műveletek megfelelően kerülnek-e naplózásra.

2.10 Szegmentáció vizsgálata - (WLAN-CONF-004)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeit összekötő alhálózatok megfelelően elkülönítettek-e.

2.11 Fizikai hozzáférés vizsgálata - (WLAN-CONF-005)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközei megfelelően védettek-e a fizikai hozzácsatlakozás ellen.

2.12 Hálózati eszközök feltérképezhetőségének vizsgálata - (WLAN-CONF-006)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek forgalma lehallgatható-e, valamint ezen forgalomból a vezetéknélküli rendszerek feltérképezhetők-e.

2.13 Védett hálózatok átjárhatóságának vizsgálata - (WLAN-CONF-007)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeihez mobilkapcsolatra képes rendszert lehet-e csatlakoztatni.

2.14 Szerepkör definíciók vizsgálata - (WLAN-IDNT-001)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközein milyen szerepkörök vannak definiálva, ezek hogyan működnek, valamint megfelelő hozzáférést biztosítanak-e a rendszer funkcionalitásához és információihoz.

2.15 Felhasználói regisztráció vizsgálata - (WLAN-IDNT-002)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeit használni kívánók miként juthatnak felhasználói jogosultságokhoz.

2.16 Felhasználói hozzáférés létrehozásának vizsgálata - (WLAN-IDNT-003)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeit használók képesek-e új felhasználót hozzáadni a rendszerhez.

2.17 Felhasználói hozzáférés felfüggesztésének vizsgálata - (WLAN-IDNT-004)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeit használók hozzáférésének felfüggesztése esetén a rendszer megfelelően kizárja-e a felhasználókat a rendszerből.

2.18 Felhasználókezelés vizsgálata - (WLAN-IDNT-005)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek adminisztrátori felületein megfelelően lehet-e azok felhasználóit kezelni.

2.19 Felsoroltatható és könnyen kitalálható felhasználói hozzáférések vizsgálata - (WLAN-IDNT-006)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek funkcióit felhasználva felderíthetők-e a rendszerekbe regisztrált felhasználók belépési azonosítói.

2.20 Felhasználónév házirend vizsgálata - (WLAN-IDNT-007)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek felhasználónév követelményeit szabályzó házirend kellően biztonságos-e.

2.21 Bejelentkezési információk titkosított átvitelének vizsgálata - (WLAN-AUTN-001)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközei megfelelően konfigurált és titkosított hálózati csatornát használnak-e az adataik továbbítására.

2.22 Alapértelmezett hitelesítési adatok vizsgálata - (WLAN-AUTN-002)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek telepítésekor használatos fiókok léteznek-e a rendszerekben.

2.23 Kizárási házirend vizsgálata - (WLAN-AUTN-003)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközei szankcionálják-e a helytelen bejelentkezési kísérleteket.

2.24 Hitelesítési séma megkerülésének vizsgálata - (WLAN-AUTN-004)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek felhasználóit beléptető felület tervezési vagy megvalósítási hibáin keresztül lehetséges-e a rendszerekbe jogosulatlanul belépni.

2.25 Jelszómegjegyző funkció vizsgálata - (WLAN-AUTN-005)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközein található-e olyan jelszómegjegyző funkció, ami nem megfelelően tárolja el a bejelentkezési adatokat.

2.26 Jelszó házirend vizsgálata - (WLAN-AUTN-006)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek jelszó követelményeit szabályzó házirend kellően biztonságos-e.

2.27 Jelszóváltoztató és visszaállító funkciók vizsgálata - (WLAN-AUTN-007)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek felhasználói visszaélhetnek-e a jelszóváltoztató és visszaállító funkciók gyengeségeivel.

2.28 Többfaktoros hitelesítés vizsgálata - (WLAN-AUTN-008)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek többfaktoros autentikációja megfelelően van-e konfigurálva.

2.29 Jogosultságkezelési séma megkerülésének vizsgálata - (WLAN-AUTZ-001)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek bizonyos jogosultsági szint birtokában elérhető funkciói hozzáférhetők-e az elvártnak nem megfelelő jogosultsági szint birtokában.

2.30 Jogosultság kiterjesztés vizsgálata - (WLAN-AUTZ-002)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek felhasználói hozzájuthatnak-e a számukra kiosztottnál bővebb jogosultságokhoz.

2.31 Kijelentkezés vizsgálata - (WLAN-AUTZ-003)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközein megfelelően működik-e a befejezett munkamenetek érvénytelenítése.

2.32 Munkamenet lejárat vizsgálata - (WLAN-AUTZ-004)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközeinek aktuális (bejelentkeztetett) munkamenetei érvénytelenítésre kerülnek-e észszerű időn belül.

2.33 Hibaüzenetek és hibaállapotok kezelésének vizsgálata - (WLAN-ERRH-001)

Annak vizsgálata, hogy a hálózat vezetéknélküli eszközei miként kezelik a munkamenetek során felmerülő hibaüzeneteket és hibaállapotokat.