Fogalomtár

Etikus hackelés tárgyban

Azonosító: S2_Fogalomtar_v1

Silent Signal Kft.
Email: info@silentsignal.hu
Web: www.silentsignal.hu

SILENT SIGNAL
VÉSZJELZÉS HELYETT...

Tartalom

1. BEVEZETŐ

A fogalomtár célja, hogy az etikus hackelési projektek során tapasztalható definíciós zavarokat csökkentse, valamint elősegítse egy jól meghatározott, az ügyfél számára megfelelő vizsgálat elvégzését.

1.1 Architektúra (terv) felülvizsgálat

A kialakításra váró vagy kialakított architektúra terv felülvizsgálata biztonsági szempontból, amely során a támadási felületek minimalizálása és az adott környezet maximális biztonsági szintjének elérése a cél.

1.2 Automatikus vizsgálat

A szakértők egy sérülékenység azonosításra alkalmas szoftver segítségével megvizsgálják az adott rendszert, alkalmazást. A vizsgálat nem teljes körű, összetettebb hibákat nem képes detektálni, hamis pozitív, hamis negatív találatokat ki kell szűrni az eredményből. A vizsgálat alkalmazása speciális esetekben javasolt, és ilyenkor legyen része a találatok manuális ellenőrzése és az eredmények különálló, érthető dokumentálása.

1.3 Behatolás tesztelés (penetration testing)

Írásos megbízás során a megbízó saját üzemeltetési hatáskörébe tartozó rendszerelemek (szerver, hálózat, alkalmazás, szolgáltatás stb.) biztonsági felülvizsgálatára ad engedélyt, felhatalmazást. A vizsgálat(ok) során a tesztelők feladata meghatározni, hogy a vizsgálat tárgyát képező rendszerbe be lehet-e hatolni az adott vizsgálati körülmények között, vagy nem. A vizsgálatok végén az elvégzett feladatok dokumentálása szükséges.

1.4 Belső vizsgálat

A vizsgálat elvégzéséhez a megbízó egy belső hálózati hozzáférést biztosít a szakértőknek a munkavégzéshez. A vizsgálat szimulálhat akár egy munkavállalót, belső hálózatba jutott külső támadót is.

1.5 Black-box vizsgálat

A vizsgálatok megkezdéséhez a megbízó csak minimális információkat szolgáltat (pl. IP cím, cégnév, weboldal, stb.) a tesztelő szakértők számára. Ilyen vizsgálatokat a nyilvános elérésű rendszerek esetén javasolt elvégezni (Internetes megjelenés (nem csak web!), Wi-Fi hálózat, stb.).

1.6 Etikus hackelés (ethical hacking)

Írásos megbízás során a megbízó saját üzemeltetési hatáskörébe tartozó rendszerelemek (szerver, hálózat, alkalmazás, szolgáltatás stb.) biztonsági felülvizsgálatára ad engedélyt, felhatalmazást. A vizsgálat(ok) során a tesztelők feladata a lehető legtöbb hiba meghatározása, majd részletes dokumentálása az elvégzett feladatoknak. A humán és fizikai védelmi megoldások tesztelése - social engineering - is ebbe a fogalomkörbe tartozik.

1.7 Forráskód analízis

A szakértők az alkalmazás forráskódjának birtokában azon biztonsági felülvizsgálatot végeznek. A teszt célja a legtöbb biztonsági szempontból kifogásolható megvalósítás azonosítása, kiszűrése. Javasolt, hogy az automatikus ellenőrzések mellett a vizsgálatoknak intuitív ellenőrzés is legyen része. Annak érdekében, hogy a feltárt problémák kihasználhatósága is ellenőrzésre kerüljön, javasolt tesztrendszert biztosítani a vizsgálathoz.

1.8 Gray-box vizsgálat

A vizsgálatok megkezdéséhez a megbízó az adott rendszer elérésén túl még plusz információkat szolgáltat a tesztelést végző szakértők számára. A plusz információk lehetnek:

- hozzáférés a tesztelt rendszerhez, alkalmazáshoz;
- forráskód a könnyebb hibaazonosítás érdekében (nem kódaudit, csak plusz információ).

Az ilyen típusú vizsgálatokat olyan rendszerelemeken javasolt elvégezni, ahol korlátozott, regisztrációval létrehozható felhasználói hozzáféréssel lehetséges műveleteket végezni (pl. Netbank).

1.9 Hálózati teszt

A vizsgálat elvégzéséhez a megbízó egy belső hálózati hozzáférést biztosít a szakértőknek a munkavégzéshez. A szakértők feladata a hálózati eszközök és az alkalmazott hálózati protokollok biztonsági hiányosságainak meghatározása.

1.10 Hardening

A vizsgálat során a szakértőknek a támadási felület csökkentése érdekében javaslatokat kell tenni a vizsgált rendszer biztonsági beállításaival kapcsolatosan. Általában konfiguráció elemzés és egyéb tesztek képezhetik részét a vizsgálatnak. Javasolt elvégezni kritikus rendszerek vagy üzletileg kritikus információkat kezelő rendszerek esetén.

1.11 Kliens oldali biztonsági teszt

A megbízó által használt munkaállomások biztonsági felülvizsgálata. A teszt kiterjedhet konfiguráció vizsgálatra, kliens oldali alkalmazások biztonsági ellenőrzésére (böngészők, dokumentum olvasók, stb.). Javasolt elvégezni, amennyiben a vállalat egységes szoftverkörnyezetet használ. Egyéb esetekben az üzletileg kritikus információkat kezelő személyek munkaállomásának vizsgálata javasolt.

1.12 Konfiguráció vizsgálat

A kijelölt rendszerelem konfigurációs beállításainak birtokában határozzák meg a szakértők a lehető legtöbb biztonsági problémát. Tipikusan hálózati eszközök, alkalmazás szerverek, operációs rendszerek beállításainak felülvizsgálatára szolgáló vizsgálat típus.

1.13 Környezet vizsgálat (alkalmazás tesztnél)

Alkalmazás tesztelésnél architekturálisan szorosan összefüggő rendszerkomponensek biztonsági vizsgálata (pl. webalkalmazásnál a kiszolgáló szerver teljes körű vizsgálata).

1.14 Külső vizsgálat

A vizsgálat elvégzése internet, DMZ, külső partner, wireless hálózat, egyéb hálózat irányából történik. A vizsgálat szimulálhat egy külső támadót.

1.15 Sérülékenység vizsgálat

A vizsgálat során a lehető legtöbb biztonsági hiányosság meghatározása. A vizsgálatokat akkor is el kell végezni, ha az első vizsgálati pontnál teljes hozzáférést sikerült szerezni a vizsgálat tárgyát képező rendszer felett.

1.16 Social engineering

Írásos megbízás során a megbízó saját munkavállalóinak biztonságtudatos viselkedésének felülvizsgálatára ad engedélyt, felhatalmazást. A vizsgálat(ok) során a tesztelők feladata meghatározni, hogy a vizsgált munkavállalókkal a szerződésben meghatározott módon (e-mail, telefon, stb.) felvéve a kapcsolatot rávehetők-e arra, hogy a szervezet IT rendszereinek biztonságát megsértsék, akár információ (jelszavak és egyéb érzékeny adat) átadásával, akár ehhez hozzásegítő műveletek elvégzésével.

1.17 Szerver vizsgálat

A vizsgálat során a megbízó által kijelölt szervereken elérhető összes szolgáltatás biztonsági hiányosságainak meghatározása. Egyéb vizsgálati elemeket is magában foglalhat pl. webalkalmazás teszt.

1.18 Teszt felhasználó

A vizsgálatok végrehajtásához szükséges jogosultsággal rendelkező felhasználó, amely üzletileg káros műveleteket nem tud elvégezni (nagy értékű utalás, vásárlás, egyebek...).

1.19 Teszt rendszer/Éles rendszer

Élesnek nevezünk minden, a felhasználók számára elérhető, üzleti logikát megvalósító alkalmazást. Tesztnek nevezzük az olyan rendszereket, melyek a felhasználók számára nem elérhetők, de a felhasználás céljától (integrációs, fejlesztői, stb.) függő mértékben az élessel megegyező módon valósítanak meg üzleti logikát.

1.20 Tesztelési módszertan

A biztonsági vizsgálat fázisait, az ezek során elvégzendő vizsgálati lépéseket, valamint a lépések megvalósításához ajánlott módszereket és eszközöket nemzetközi ajánlások alapján meghatározó útmutató.

1.21 Túlterheléses teszt

A vizsgálat során hálózati vagy alkalmazás szinten a cél rendszer erőforrásainak felhasználása, amely mellett a normális kérések kiszolgálása nem válik lehetővé. A

tesztelésnél megkülönböztetünk egy vonalról végzett (alacsony sávszélességű) és több vonalról végzett (elosztott, nagy sávszélességű) tesztelési eljárást.

1.22 Visszaellenőrzés

Az elvégzett vizsgálatok során feltárt hiányosságok megfelelő javításának ellenőrzése. Nem új, teljes körű vizsgálat, csak a korábban feltárt hibák ellenőrzése a cél.

1.23 Webalkalmazás teszt

A teszt során csak a kijelölt webalkalmazás biztonsági vizsgálatát kell elvégezni. Javasolt elvégezni minden dinamikus tartalommal, szenzitív információval rendelkező webalkalmazás estén. Bizonyos esetekben a környezet vizsgálata is javasolt. A leggyakoribb vizsgálatok közé tartozik.

1.24 White-box vizsgálat

A vizsgálatok megkezdéséhez a megbízó teljes hozzáférést (privilegizált) biztosít a tesztelendő rendszerhez. A szakértők egy teljes körű auditot végeznek az adott környezeten (operációs rendszer és szolgáltatások biztonsági vizsgálata, hardening javaslatok, alkalmazás vizsgálatok, konfiguráció elemzés, stb.). Az ilyen típusú vizsgálatokat kritikus infrastruktúra elemeken javasolt elvégezni.

1.25 Wi-Fi teszt

A vezeték nélküli hálózat biztonsági hiányosságait meghatározó vizsgálati típus.