Lyukvadászok szabálykönyve

Mit várhatunk egy behatolás teszteléstől?

Pánczél Zoltán

panczel.zoltan@silentsignal.hu

SILENT SIGNAL

Tartalomjegyzék

Értékeink

Alapfogalmak meghatározása

Vizsgálatok információs bázis szerint

Vizsgálatok kiindulási pont szerint

Vizsgálatok lehetséges fajtái

Vizsgálati módszertanok

Vizsgálatok lépései

Kérdések, tévhitek, problémák, kritikák

Értékeink

> 5 év szakmai tapasztalat minden szakterületen

Hacktivity 2004,2005,2007 wargame győztes

Goldenblog 2009. IT kategóriagyőztes

Hacktivity 2009. Hack the Vendor győztes

Offensive-Security nemzetközi hackerverseny 3. és 5. hely (> 1000 induló)

Hacktivity 2010 Wargame és CtF készítője

Sebezhetőségek jelentése a Zero Day Initiative program keretében

CISSP, CCNA, CCNP, HCSE, ITIL, OSCP, OSCE

SILENT SIGNAL

Meghatározások

Ethical hacking

Írásos megbízás, hacker technikák, biztonsági szint növelése (SE)

Penetration testing

Hozzáférés megszerzése, védelmi megoldások kikerülése

Biztonsági felmérés

Sérülékenység azonosítása, „papír hack”

Információs bázis

Blackbox

Minimális információk birtokában történő vizsgálat.

Greybox

Általában felhasználói hozzáférés birtokában végrehajtott ellenőrzés.

Whitebox

A rendelkezésre álló összes információ átadása(audit).

Kiindulási pont

Külső vizsgálat, internet irányából

Külső támadók megszemélyesítése.

Belső vizsgálat, intranet irányából

Rosszindulatú belső dolgozó vagy látogató lehetőségeinek vizsgálata.

Vizsgálat tárgya szerint

- **Hálózati teszt**

  A leggyakoribb vizsgálati típus, amely során a hálózatban található eszközök és szerverekben található sérülékenységek feltárása és kihasználása a cél.

- **Webalkalmazás teszt**

  Egyre több cég jelenik meg webes tartalommal – interneten, valamint intraneten egyaránt – a támadások jelentős része is erre a szegmensre koncentrálódik.

- **Vezeték nélküli hálózat**

  Illegálisan üzemeltetett vezeték nélküli hozzáférési pontok felderítése, valamint az engedéllyel használt eszközök biztonsági hiányosságainak feltárása

Vizsgálat tárgya szerint

- **Social Engineering**

  Emberi tényezőkre alapozott biztonsági vizsgálat.

- **Kliens oldali biztonsági teszt**

  Lehetséges-e a felhasználókat egy kártékony oldalra irányítani és ott egy böngésző alapú hiba segítségével átvenni az irányítást a számítógépük felett vagy hozzáférést szerezni a belső hálózathoz.

- **Alkalmazás vizsgálatok, forráskód analízis**

  Saját fejlesztésű vagy forráskód szinten hozzáférhető szoftverek esetében a teszt segítségével összetett hiányosságokat is sikeresen detektálni lehet.

Vizsgálat tárgya szerint

- **Konfiguráció felülvizsgálata**

  A konfiguráció vizsgálat során hálózati eszközök, alkalmazások és operációs rendszerek konfigurációs beállításainak felülvizsgálatával újabb biztonsági hiányosságokat lehetséges feltárni.

- **Architektúra kialakítás felülvizsgálata**

  A rendszerek kialakításának valamint kapcsolatának felülvizsgálatával lényeges biztonsági hiányosságokat lehetséges meghatározni.

- **Hardening**

  A hardening során olyan környezetfüggő konfigurációs módosításokat kell meghatározni, amely segítségével a rendszer biztonsági szintje növekszik.

Vizsgálati módszertanok

- Open Web Application Security Project (OWASP) Testing Guide
- Open Source Security Testing Methodology Manual (OSSTMM)
- NIST Special Publication 800-42: Guideline to Network Security Testing
- Penetration Testing Framework
- Open Information Systems Security Group - Information Systems SecurityAuditing Framework

SILENT SIGNAL

Vizsgálat lépései

Ajánlatkérés

Fontos, hogy a megrendelőnek legyen elképzelése arról, hogy mit szeretne megvizsgáltatni, mi ellen akar védekezni. (1 db Ethical hacking vizsgálatot kérek – nem működik)

Ajánlat

Pontosan leírja, hogy mi és hogyan (módszertan) lesz vizsgálva, az adott árért, így a teljesítés ellenőrizhető. (1 db black-box vizsgálat = X Ft – nem működik)

Vizsgálat lépései

Szerződés

Mit, mikor, hogyan, ki…

Minden projekt paramétert tisztázni kell a felek között. (A vizsgálatot végző csapat semmi „váratlant” nem tehet.)

Jelentés

Vizsgálat lépései és eredményei

Feltárt hibák kategórizálása és javaslat a hibák javítására

Visszaellenőrzés

Ügyfél igény szerint, a hibák kijavítása után.

Tipikus kérdések, tévhitek

A vizsgálat az első kritikus hibáig tart?

Mennyivel lesz jobb a rendszer a vizsgálat után?

Miért kell külsős vizsgálat, hiszen rendszeresen scanneljük a rendszereinket?

Mikor érdemes sérülékenységi vizsgálatot csináltatni?

Mennyi időnként érdemes a vizsgálatot megismételni?

Problémák, kritikák

Kevés a rendelkezésre álló idő

Nem megfelelő hozzáférés biztosítása

Minimalizált eszköz készlet

Vizsgálatot végző személyek:

- Szakmai hozzáértése, kompetenciája
- Helyzetfelismerő képessége

SILENT SIGNAL

Összefoglalás

Miről is volt szó?

- **Meghatározások, fogalmak tisztázása**
- **Vizsgálathoz szükséges információk csoportja**
- **Vizsgálati irányok**
- **Vizsgálati lehetőségek, ígények**
- **Főbb módszertanok**
- **Ajánlatkérés, ajánlat, szerződés, jelentés, visszaellenőrzés**
- **Tévhitek, tipikus kérdések**
- **Kritikák, problémák az etikus hackeléssel kapcsolatban**

Köszönöm megtisztelő figyelmüket!

SILENT SIGNAL

VÉSZJELZÉS HELYETT...

Pánczél Zoltán, CISSP,OSCP, OSCE

panczel.zoltan@silentsignal.hu