Ethical Hacking

“Give Me Shell or Give Me Death”

Pánczél Zoltán, CISSP,OSCP,OSCE

panczel.zoltan@silentsignal.hu

Tartalomjegyzék

Meghatározások

Vizsgálati lehetőségek

Vizsgálati eredmények

Problémák

Nemzetközi módszertanok

Esettanulmányok

Eszközök

SILENT SIGNAL

Meghatározások

- **Ethical hacking**

  Írásos megbízás, hacker technikák, bizt. szint növelése
- **Penetration testing**

  Hozzáférés szerzése, védelmi megoldások kikerülése
- **Biztonsági felmérés**

  Sérülékenység azonosítása, papír hack :)

Vizsgálati lehetőségek

- Információ mennyisége alapján
  - BlackBox
  - GreyBox
  - WhiteBox
- Vizsgálat iránya alapján
  - Külső, internet irányából
  - Belső, intranet felől

SILENT SIGNAL

Vizsgálat tárgya szerint

- Hálózati teszt
- Webes alkalmazás teszt
- Vezeték nélküli hálózat
- Social Engineering
- Kliens oldali biztonsági teszt
- Alkalmazás audit
- Forráskód analízis

SILENT SIGNAL

Egyéb lehetőségek

- Konfiguráció felülvizsgálata
- Architektúra vizsgálat
- Interjúztatás

SILENT SIGNAL

Vizsgálati eredmények

- Legtöbb sérülékenység feltárása
- Külső támadó mihez férhet hozzá?
- Kliens oldali támadások

SILENT SIGNAL

Problémák, kritikák

- Kevés a rendelkezésre álló idő
- Nem megfelelő hozzáférés biztosítása
- Minimalizált eszköz készlet
- Vizsgálatot végző személyek:
  - Szakmai hozzáértése, kompetenciája
  - Helyzetfelismerő képessége

SILENT SIGNAL

Módszertan szerinti vizsgálati lehetőségek

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

SILENT SIGNAL

Esettanulmány
Levelező rendszer

- Iskolapélda kezdőknek
- Perzisztens XSS
- SQL injection (szinte mindenhol)
- Plain text jelszavak (millió)
- Végső csapás, SQL rootként

SILENT SIGNAL

Esettanulmány Pénzintézet

- Feltöltés funkció hibája
- Kliens oldali ellenőrzés ☺
- Jogosultsági problémák miatt adminisztrátori hozzáférés

Esettanulmány
Tartalom szolgáltató

- Feltöltési hiba
- Fejlesztői hibák
- Hozzáférés vezérlési problémák
- Gyenge jelszó policy, algoritmus

SILENT SIGNAL

Hálózati érdekesség

- Eltérítés, lehallgatás?
- ARP spoofing (Cain, Ettercap)
- Routing protokollok hibái
- Videó

SILENT SIGNAL

Kliens oldali támadás

- Egyre gyakoribb
- Szinte minden szoftver érintett
- Felhasználói beavatkozás szükséges(SE)
- Szinte észrevehetetlen
- Video

SILENT SIGNAL

Exploit írás

- Miért szükséges? (POC)
- Stack overflow
- Alapok a megértéshez (memória, regiszterek, assembly)
- Debugger a hiba azonosítására

Köszönöm megtisztelő figyelmüket!

SILENT SIGNAL

VÉSZJELZÉS HELYETT...

Pánczél Zoltán, CISSP,OSCP,OSCE

panczel.zoltan@silentsignal.hu

http://www.silentsignal.hu