Penetrační testy

Postřehy z pilotního provozu

Martin Kunc • martin.kunc@nic.cz • 14. 11. 2019

CZ.NIC | SPRÁVCE DOMÉNY CZ

Zadání

- Cílem testu je simulace přiměřeně finančně motivovaného útočníka
- Otestovat možnosti zneužití slabin zadaného síťového rozsahu
- Testovaný rozsah /23

Přehled testů

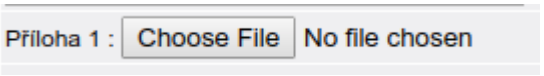
- Pasivní
  - Analýza veřejných zdrojů
  - Vyhledávání domén
- Aktivní
  - Sken portů
  - Analýza detekovaných služeb

Co se nepovedlo

- Převzít kontrolu nad doménovým řadičem
  - Ale našli jsme ho
- Vytvoření reverse shellu

Co se povedlo

- Webshell
  - neošetřený file upload
    - nejprve na „fóru“
    - později i v administračním rozhraní
  - vícero webů
  - celkem 5 strojů

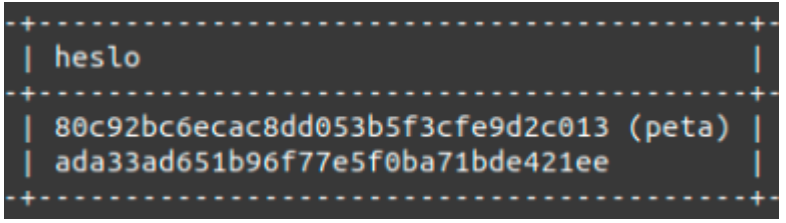


Co se povedlo

- Tunel pro laterální pohyb
  - Grafana – defaultní instalace
- SYSTEM
  - systémová oprávnění
  - plaintext heslo k jednomu z lokálních administrátorů
    - elevace oprávnění na dalších strojích

Co se povedlo

- Blind SQL injection
  - více zranitelných webů → více získaných databází
  - hesla k administračnímu rozhraní



Podmínky služby

- Basic
  - Malá/střední společnost
  - 4-5 serverových služeb
  - cca 90 000 Kč

Podmínky služby

- Standard
  - Malá až střední společnost silně závislá na IT
  - 10-20 serverových služeb
  - cca 336 000 Kč

Podmínky služby

- Premium
  - Střední až velká společnost silně závislá na IT
  - 20-30 serverových služeb
  - cca 784 000 Kč

Děkuji za pozornost

Martin Kunc • martin.kunc@nic.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ