Ofenzivna sigurnost

Modeli penetracijskog testiranja

Andrija Krklec, 18.12.2025.

Pregled predavanja

- Definicija pojma pen test
- Metodologije
- Faze
- Primjer procesa
- Primjena u praksi

Motivacija

- Kompleksnost sustava
  - veći rizik nenamjernih sigurnosnih propusta
- Automatizirani alati ne otkrivaju sve ranjivosti
- Organizacije trebaju realnu procjenu iz perspektive napadača
- Pen test omogućuje provjeru učinkovitosti postojećih sigurnosnih mehanizama

Pitanja za ispite

- Što je penetracijsko testiranje (pen test) i koja je njegova primarna svrha?
- Objasnite razliku između Black-box, White-box i Grey-box modela penetracijskog testiranja.
- Navedite i ukratko opišite pet osnovnih faza penetracijskog testiranja.
- Nabrojite minimalno četiri metodologije ili okvira (frameworks).
- Objasnite na što je primarno fokusirana metodologija OWASP.

Definicija

- Autorizirani simulirani napad na računalni sustav
- Cilj – provjera sigurnosnog stanja
- Identifikacija ranjivosti u OS-u, aplikacijama, mrežama, procesima
- CIA (povjerljivost, integritet, dostupnost)

Podjela na temelju znanja o sustavu[1]

- Black-box
  - tester nema nikakvih prethodnih informacija o sustavu
- White-box
  - tester ima potpune informacije o infrastrukturi
- Grey-box
  - tester ima djelomične informacije

Metodologije[1]

- Različiti okviri (frameworks)
- Kako izvesti testiranje?
- Što mora biti zadovoljeno?
- OSSTMM, NIST, PTES, OWASP
- Moraju zadovoljavati standarde kibernetičke sigurnosti
- ISO 27000, PCI DSS, BSI

OSSTMM

- znanstveni pristup
  - bez pretpostavki i anegdotalnih dokaza
- fokus na operativnu razinu sigurnosti (OpSec)
- širok spektar
  - fizička, virtualna infrastruktura, oblak, ljudski faktor
- mjerljivi rezultati i vizualizacija površine napada
- nedostatak – složenost i vrijeme prilagodbe

NIST

- fleksibilan i fokusiran na procjenu i upravljanje rizikom
- jezgra - pet kontinuiranih funkcija
  - identifikacija, zaštita, detekcija, odgovor i oporavak
- sustav razine implementacije (1 do 4)
  - opisuje stupanj zrelosti kibernetičkih praksi organizacije
  - pomoć pri procjeni ishoda napada, sukladno poslovnim ciljevima
- potrebno visoko razumijevanje sig. zahtjeva

PTES

- definira 7 koraka izvršenja testa
  - od početne komunikacije i prikupljanja informacija, preko modeliranja prijetnji i analize ranjivosti, do iskorištavanja propusta i izvještavanja
- pruža smjernice za alate, tehnike i domene
- nedostatak – relativno nov i u fazi razvoja

OWASP

- izrazito orijentiran na sigurnost aplikacija i smanjenje pogrešaka (bugova) u softveru
- sastoji se od 3 glavna vodiča
  - **Web Security Testing Guide** - testiranje web aplikacija i osiguravanje kvalitete koda
  - **Mobile Application Security** - fokus na iOS i Android platforme
  - **Firmware Security Testing Methodology** - namijenjen testiranju ugrađenog softvera, IoT uređaja i analizi binarnih datoteka

PCI DSS[3]

- sigurnosni standard dizajniran za zaštitu podataka o bankovnim karticama
- odnosi se na svaku organizaciju koja rukuje podacima o vlasnicima kartica
  - Cardholder Data Environment - CDE
- cilj - smanjiti prijevare s karticama i osigurati sigurnu obradu plaćanja

Faze pen testa[1]

- Prikupljanje informacija
  - definiranje ciljeva i opsega testa
- Skeniranje
  - identifikacija potencijalnih ranjivosti i vektora napada
- Dobivanje pristupa
  - eksploatacija ranjivosti, izvođenje ciljanih napada
- Analiza i čišćenje
  - analiza rizika, kategorizacija nalaza i „čišćenje” artefakata napada
- Izvještavanje
  - izrada formalnog izvještaja, dokazi ranjivosti, preporuke za sanaciju

Primjer procesa[3] (1)

- Napad na trgovinu s POS mrežom
- Profil tvrtke
  - 6 fizičkih trgovina i jedan središnji ured (Corporate)
- Tok podataka
  - kartica se provlači na POS uređaju u trgovini
  - podaci idu na lokalni server u trgovini, šalju se procesoru plaćanja i nakon potvrde se brišu
  - **podaci o karticama se ne šalju u središnji ured**

Primjer procesa[3] (2)

- Mreža u trgovini
  - POS mreža (**CDE**)
  - opća mreža trgovine (Non-CDE)
- Središnji ured – VPN pristup trgovini
- Planiranje napada
  - opseg - dovoljno testirati dvije jer su sve identične
  - vanjsko testiranje - vanjska IP adresa
  - unutarnje - iz središnje mreže; iz opće mreže trgovine

Primjer procesa[3] (3)

- Izvedba napada i rezultati
  - vanjski – nema ranjivosti
  - unutarnji
    - ranjivost 1 – vatrozid POS mreže pogrešno konfiguriran
    - moguć pristup svim portovima i servisima iz opće mreže trgovine
    - ranjivost 2 – zadane (default) vjerodajnice na POS serveru
- Zaključak i rješenje
  - popraviti pravila na vatrozidu
  - promijeniti zadane lozinke
  - naručiti ponovno testiranje za potvrdu

Primjena modela testiranja u praksi[2] (1)

- Javne metodologije ne postižu svoje ciljeve
  - u praksi implementirane samo djelomično ili nikako
- Pristup „mix and match”
  - pružatelji usluga rijetko slijede jedan standard u potpunosti
  - stvaraju interne metodologije – dijelovi iz više različitih izvora koji im odgovaraju
- OSSTMM – smatra se prekompliciranim
- OWASP – najkorišteniji

Primjena modela testiranja u praksi[2] (2)

- Opća kvaliteta testova ocijenjena je **niskom do prosječnom**
  - prodaja jeftinih automatiziranih skeniranja ranjivosti
  - lažna sigurnost
- Moguća rješenja
  - pojednostaviti OSSTMM
  - educirati tržište o razlici između skeniranja i testiranja
  - razmotriti uvođenje industrijske certifikacije (poput modela CREST)

Zaključak

- Sigurnost sustava iznimno važna danas
  - uslijed digitalizacije svi podaci prolaze kroz aplikacije i mrežu
- Pen test predstavlja pouzdanu metodu provjere
  - formalni proces testiranja
  - važno se pridržavati specifične metodologije
  - pad kvalitete zbog automatskih skeniranja („pen test”)
  - detaljno proučiti sigurnosne zahtjeve i izvještaj pen testa

Literatura

1. Sarker, Kamal Uddin, Farizah Yunus, and Aziz Deraman. "Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods." Sustainability 15.13 (2023): 10471 [link, 10.12.2025.]
2. van den Hout, Niek Jan. "Standardised Penetration Testing? Examining the Usefulness of Current Penetration Testing Methodologies." no. August (2019): 70 [link, 10.12.2025.]
3. PCI Penetration Testing Guide [link, 10.12.2025.]
4. Cloudflare – What is pen testing? [link, 10.12.2025.]
5. IBM - What is penetration testing? [link, 10.12.2025.]

Dodatna literatura

- P. Herzog: "The Open Source Security Testing Methodology Manual (OSSTMM) [link, 10.12.2025.]
- OWASP Web Security Testing Guide [link, 10.12.2025.]
- NIST, Framework for Improving Critical Infrastructure Cybersecurity [link, 10.12.2025.]
- The Penetration Testing Execution Standard [link, 10.12.2025.]

Hvala!