

Penetracijska testiranja: iskustva iz prakse

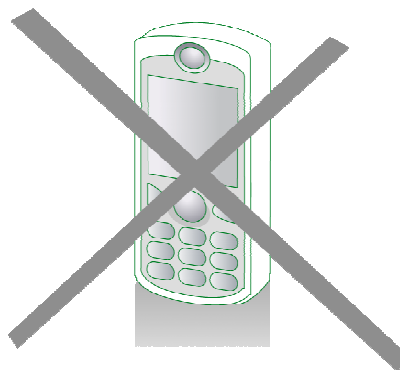
Saša Jušić, CISA, CISSP
<Sasa.Jusic@infigo.hr>
Leon Juranić
<Leon.Juranic@infigo.hr>



Sadržaj



10 godina
Prvi puštava polaznika
1998 - 2008



Sadržaj



10 godina
Prvi po izboru poslovnika
1998 • 2008



- INFIGO IS iskustva
- Što je penetracijski test?
- Ciljevi penetracijskog testiranja
- Ključni faktori uspjeha
- Postupak ispitivanja sigurnosti
- DEMO
 - Infigo Web Auditor
- Zaključak

INFIGO IS iskustva



10 godina
Prvi po izboru poslovnika
1998 • 2008



- Više od 30 različitih ispitivanja sigurnosti
 - javni i interni dijelovi informacijskih sustava
 - Web aplikacije
 - E-banking
 - CMS sustavi
 - Web trgovine...
 - baze podataka
 - specijalizirane poslovne aplikacije

INFIGO Security research - Infocus



10 godina
Prvi po izboru poslovnika
1998 • 2008



- Kontinuirano objavljivanje *security advisorya*
 - McAfee E-Business Server
 - Mdaemon
 - FTP serveri
- Razvoj specijaliziranih *security* alata
 - INFIGO FTP Fuzzer
 - Infigo Web Auditor
- Kontinuirano praćenje *underground* scene
- Kontakti s vodećim svjetskim *security* centrima
 - SANS ISC

Što je penetracijski test?



10 godina
Prvi po izboru poslovnika
1998 • 2008



- Sistematičan proces ispitivanja sigurnosti
- Simulacijom neovlaštenih aktivnosti:
 - vanjskih napadača (hakera)
 - internih korisnika (zaposlenici, konzultanti, vanjski partneri...)
- U kontroliranim i precizno definiranim uvjetima
- Bez ugrožavanja poslovnih procesa klijenta

Ciljevi penetracijskog testiranja



- Zaštita poslovanja od neovlaštenih aktivnosti
 - procjena i unaprjeđenje razine sigurnosti informacijskog sustava
 - preventivno otkrivanje i uklanjanje sigurnosnih propusta
- Podizanje svijesti o informacijskoj sigurnosti
- Usklađivanje s normama/regulativama

10 godina
Prvi po izboru poslovnika
1998 • 2008



Ključni faktori uspjeha



- Jasna vizija Naručitelja
 - koji će precizno definirati zahtjeve projekta
- Odabir kvalitetnog Izvršitelja
 - koji će moći ispuniti definirane zahtjeve
- Metodologija provođenja ispitivanja
 - način provođenja ispitivanja
- Predanost projektu
 - kako bi se ispravili svi uočeni sigurnosni propusti i spriječila njihova ponovna pojava

10 godina
Prvi po izboru poslovnika
1998 • 2008



Definiranje zahtjeva naručitelja



- Bitni parametri:
 - opseg i vrsta ispitivanja
 - razumijevanje sigurnosnih rizika i prijetnji poslovanju
 - scenariji obuhvaćeni ispitivanjem
- Mogući problemi:
 - zahtjev za “potpunim” security testom:
 - u produkcijskom okruženju
 - bez ikakvog rizika na raspoloživost sustava
 - nerealno kratki rokovi

10 godina
Prvi po izboru poslovnika
1998 • 2008



Odabir izvršitelja



- Temeljni kriteriji:
 - povjerenje
 - strogo poštivanje pravila definiranih ugovorom
 - čuvanje poslovne tajne (NDA)
 - *professional code of ethics*
 - stručnost
 - “background” tvrtke
 - reference
 - security research
 - nepristranost
 - objektivno izvješćivanje i prikaz rezultata

10 godina
Prvi po izboru poslovnika
1998 • 2008



Metodologija ispitivanja



10 godina
Prvi po izboru polaznika
1998 • 2008



- Obuhvaća:
 - provođenje samih testova
 - tehnike i alati
 - nadzor i bilježenje aktivnosti
 - generiranje i pohrana zapisa o svim aktivnostima
 - mogućnost naknadne analize svih testova
 - razmjenu informacija i komunikaciju na projektu
 - izvješćivanje
 - jasno i pregledno
 - s min. brojem "false-positive" rezultata

Penetracijski test u praksi



10 godina
Prvi po izboru polaznika
1998 • 2008



- Prikupljanje informacija o predmetu ispitivanja
- Identifikacija aktivnih komponenti
 - poslužitelji / mrežna oprema
 - mrežni servisi
 - aplikacije
- Detaljna analiza i prikupljanje informacija o aktivnim komponentama
 - identifikacija OS-ava, aplikacija i servisa
 - analiza sigurnosnih postavki

Penetracijski test u praksi



10 godina
Prvi po izboru posmatnika
1998 • 2008



- Provjera ranjivosti
 - korištenje specijaliziranih alata
 - podloga za detaljniju analizu ranjivosti
- Ručno ispitivanje ranjivosti
 - najzahtjevniji dio ispitivanja
 - otkrivanje “skrivenih” i kompleksnih ranjivosti
 - samostalni razvoj potrebnih alata/skripti
- Izrada završnih izvještaja
 - tehnički izvještaj
 - izvještaj za rukovoditelje

Najčešći sigurnosni propusti



10 godina
Prvi po izboru posmatnika
1998 • 2008

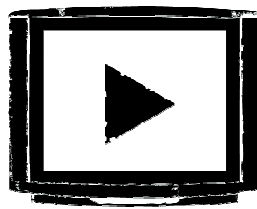


- Ranjivosti u Web aplikacijama
 - SQL Inject, XSS, RFI/LFI, ...
- Pogreške u konfiguraciji mrežnih servisa
 - WWW, SMTP, DNS,...
- “*Information leakage*” ranjivosti
 - informacije o arhitekturi sustava
 - korištenim tehnologijama
 - ugrađenim sigurnosnim kontrolama

DEMO



- INFIGO IS Web Auditor
 - demonstracija otkrivanja i iskorištavanja sigurnosnih propusta u Web aplikacijama



10 godina
Prvi po izboru posmatnika
1998 • 2008



Savjet za kraj...



- “The Shellcoder’s Handbook” citat:

“...hacking and learning is a way to live your life, not a day job or semi-ordered list of instructions found in a thick book.”

10 godina
Prvi po izboru posmatnika
1998 • 2008



Hvala na pažnji

Infigo IS d.o.o.
Horvatovac 20
10000 Zagreb

tel. +385 1 4662 700
fax. +385 1 4662 701
info@infigo.hr
www.infigo.hr

