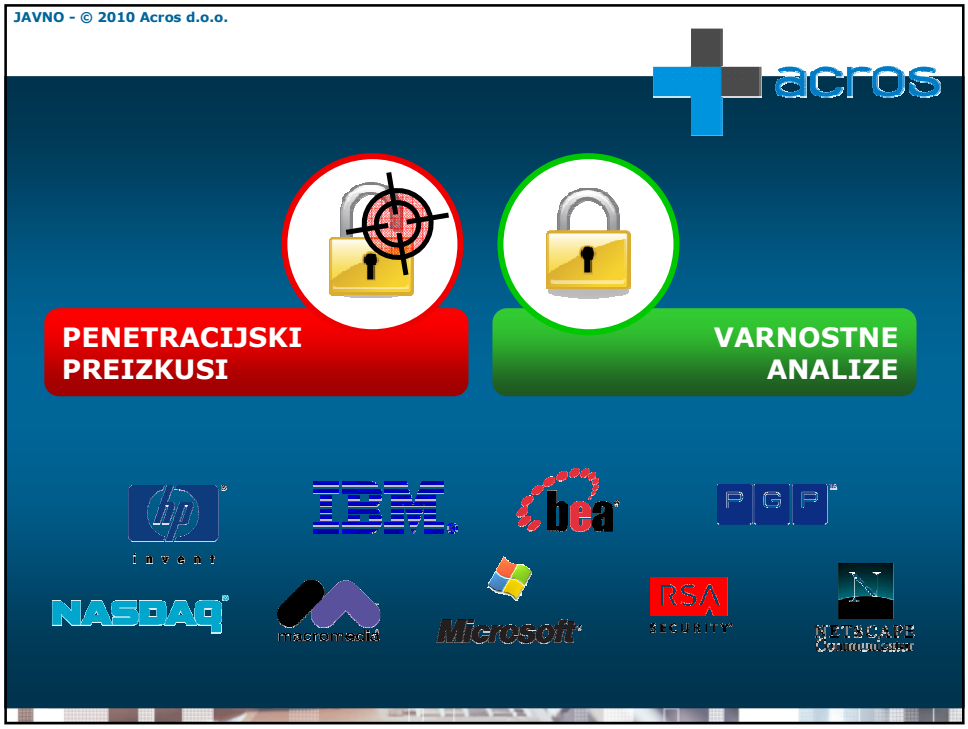
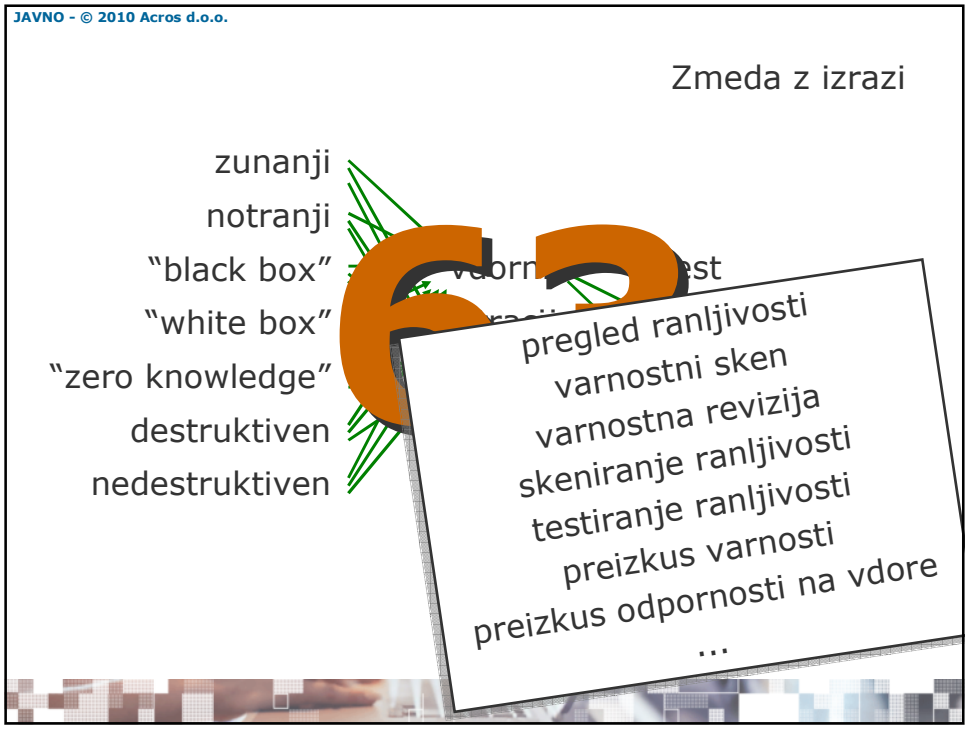
Penetracijski preizkusi: jabolke, hruške in kaviar

Mitja Kolšek
ACROS d.o.o.
www.acros.si
2.2.2010

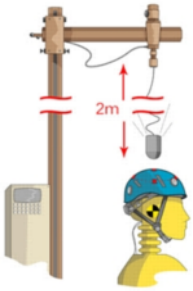
acros


JAVNO - © 2010 Acros d.o.o.
acros
PENETRACIJSKI PREIZKUSI
VARNOSTNE ANALIZE
hp invent
IBM
bea
PGP
NASDAQ
macromedia
Microsoft
RSA SECURITY
NETSCAPE Communications


JAVNO - © 2010 Acros d.o.o.
Zmeda z izrazi
zunanji
notranji
"black box"
"white box"
"zero knowledge"
destruktiven
nedestruktiven
pregled ranljivosti
varnostni sken
varnostna revizija
skeniranje ranljivosti
testiranje ranljivosti
preizkus varnosti
preizkus odpornosti na vdore
...

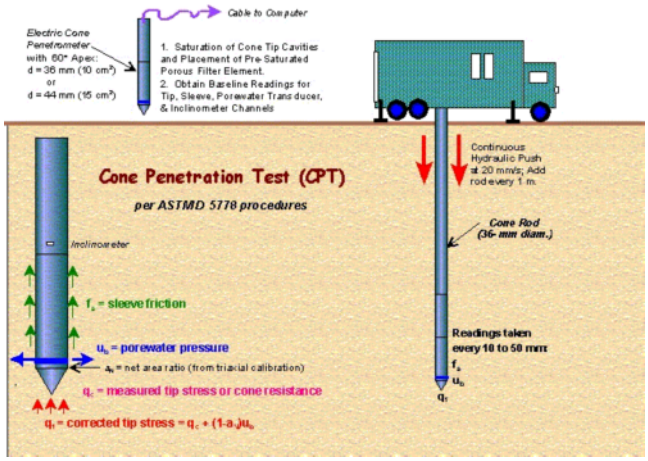
Penetracijsko preizkušanje čelad

(vir: bikechatter.co.uk)



(vir: wildcountry.co.uk)

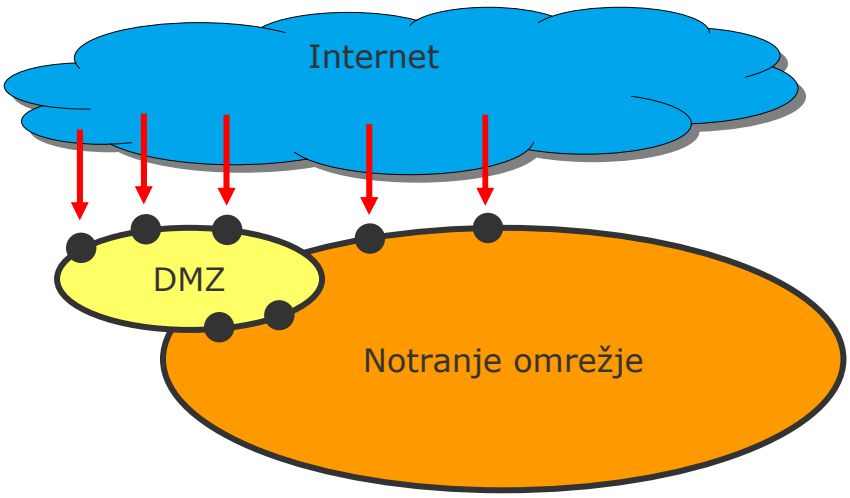
Geološko penetracijsko preizkušanje



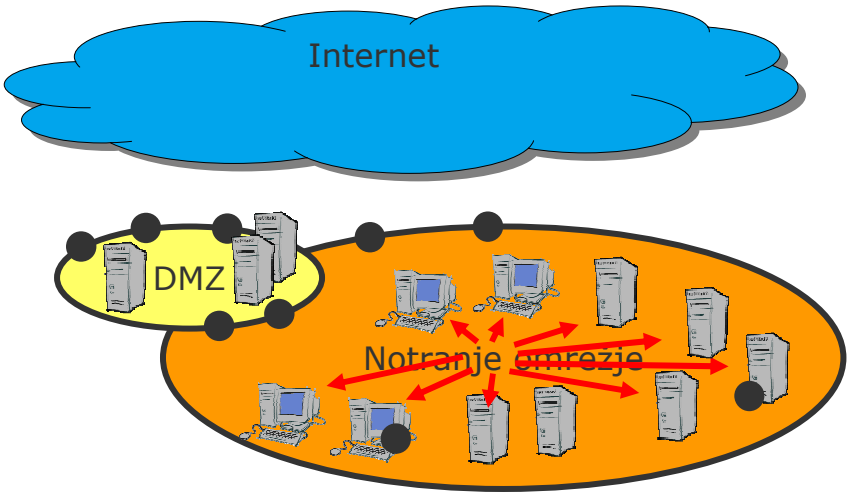
ISACA in penetracijski preizkusi

- **IS AUDITING PROCEDURE, Document P8: "Security Assessment–penetration Testing And Vulnerability Analysis" (2004)**
  - Zunanji penetracijski preizkus (Internet, modemi)
  - Notranji penetracijski preizkus (iskanje notranjih ranljivosti)
  - Fizični dostop (nezavarovani komunikacijski priključki)
  - Socialni inženiring (telefonski dostop, brskanje po smeteh)
  - Brezžična komunikacija
  - Spletne aplikacije
- **ISACA konferenca 2001: "Penetracijsko preizkušanje informacijskih sistemov"**

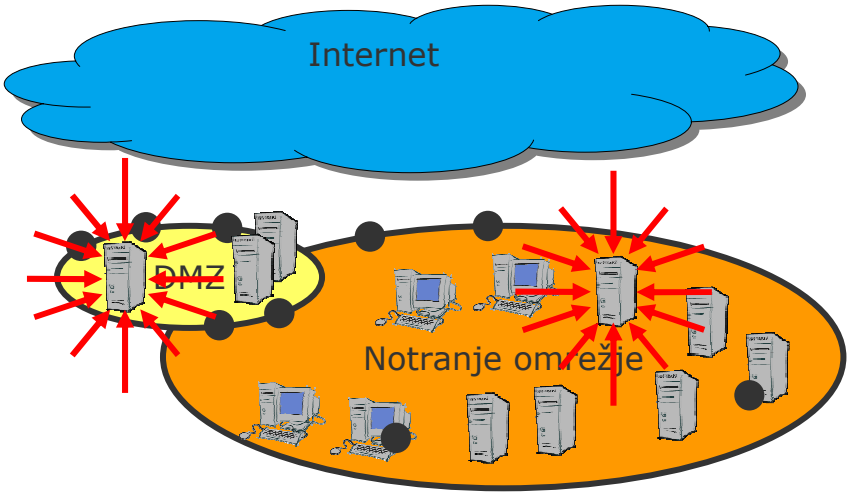
Internetni sken



Varnostni pregled notranjega omrežja



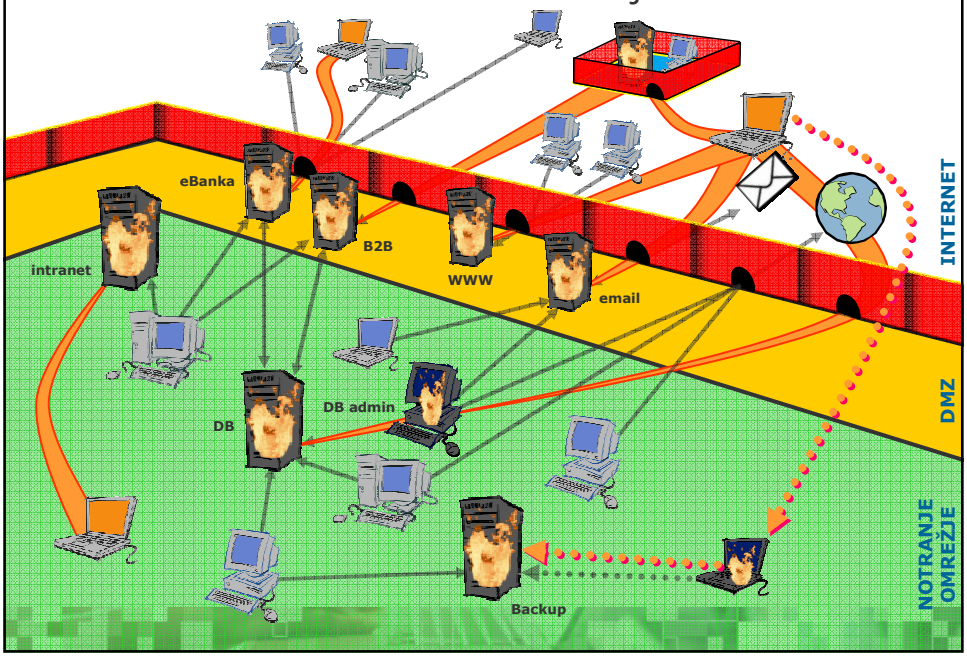
Varnostni pregled aplikacije



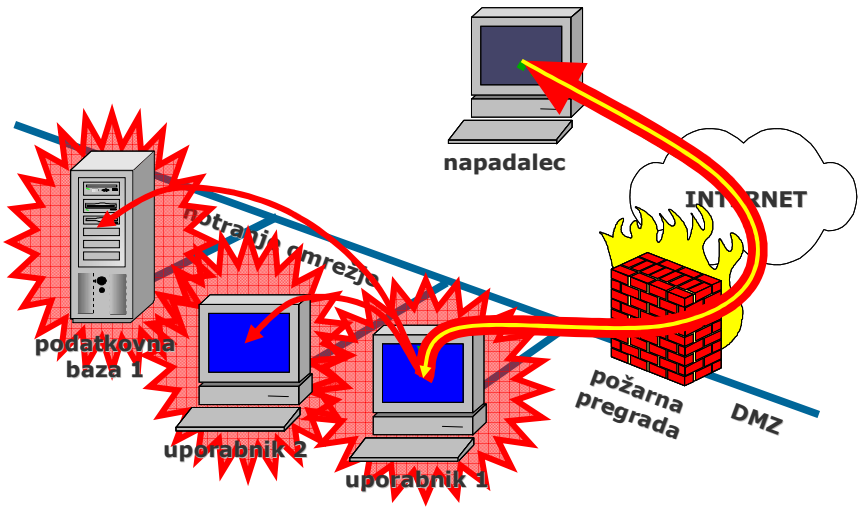
Simulacija vdora: Tipični varnostni cilji

1. Sprememba spletne predstavitve
2. Pridobitev dostopa do notranjega omrežja
3. Pridobitev administrativnega dostopa v Windows domeni
4. Pridobitev nadzora nad omrežjem
5. Pridobitev bralnega dostopa do ključnih podatkov v bazi
6. Pridobitev zaupnih dokumentov uprave
7. Pridobitev informacij iz kadrovske ali pravne službe
8. (banke) Prenos 1€ z izbranega računa na svoj račun
9. (banke) Pridobitev finančnih informacij izbranega komitenta (ali vseh)
10. (infrastruktura) Prevzem upravljanja s sistemom
11. Onesposobitev pomembne poslovne aplikacije
12. Onesposobitev osnovne dejavnosti

Simulacija vdora v banko



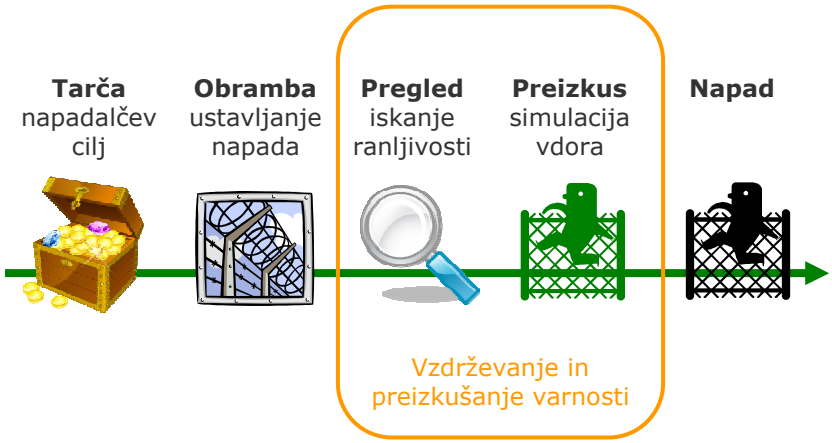
Sestavljanje ranljivosti v simulaciji vdora



Bistvene razlike med pregledom in preizkusom

Pregled (iskanje ranljivosti)	**Preizkus** (simulacija vdora)
najti čimveč ranljivosti	najti čim boljše ranljivosti za doseganje zastavljenih "napadalskih" ciljev
samo iskanje ranljivosti	iskanje in izraba ranljivosti
hipotetičen pristop	praktičen pristop
samo znane ranljivosti	tudi neznane ranljivosti
zapiranje varnostnih lukenj	dejanski preizkus varnosti
možna precejšnja avtomatizacija	predvsem ročno (možgansko) delo
	je edini način, da ugotovimo stanje varnosti

Zgodba o varnosti



Iskanje ranljivosti: Pasti

Naročnik

- Podcenjevanje notranjih napadov
- Omejevanje na avtomatizirane preglede
- Spregledane pomembne aplikacije

Izvajalec

- Dobimo dolg seznam vseh sumov ali prečesan seznam potrjenih ranljivosti?
- So odkrite ranljivosti ocenjene pavšalno ali glede na konkretni kontekst v našem okolju?
- So priporočila izvedljiva v našem okolju?
- So priporočila strokovno objektivna ali so reklamni material?
- Je cena sumljivo nizka?

Simulacija vdora: Pasti

Naročnik

- Večno odlašanje
- Omejevanje izvajalca

Izvajalec

- Ali izvajalec lovi natančno določene cilje, ki so za nas tudi najbolj kritični?
- Ali izvajalec dejansko doseže zastavljene (nedestruktivne) cilje in ne zgolj opisuje, kako bi jih lahko dosegel?
- Ali izvajalec uporablja tudi neznane ("0-day") ranljivosti?
- Je sposoben odkrivanja neznanih ranljivosti v našem sistemu?
- Kako blizu zastavljenim ciljem je izvajalec prišel?
- So priporočila izvedljiva v našem okolju?
- So priporočila strokovno objektivna ali so reklamni material?

~~Najprej: "Kakšna sploh je naša varnost?"~~

pregled ≠ preizkus

pregled ≠ pregled
preizkus ≠ preizkus

Mitja Kolšek
mitja.kolsek@acros.si

www.acros.si