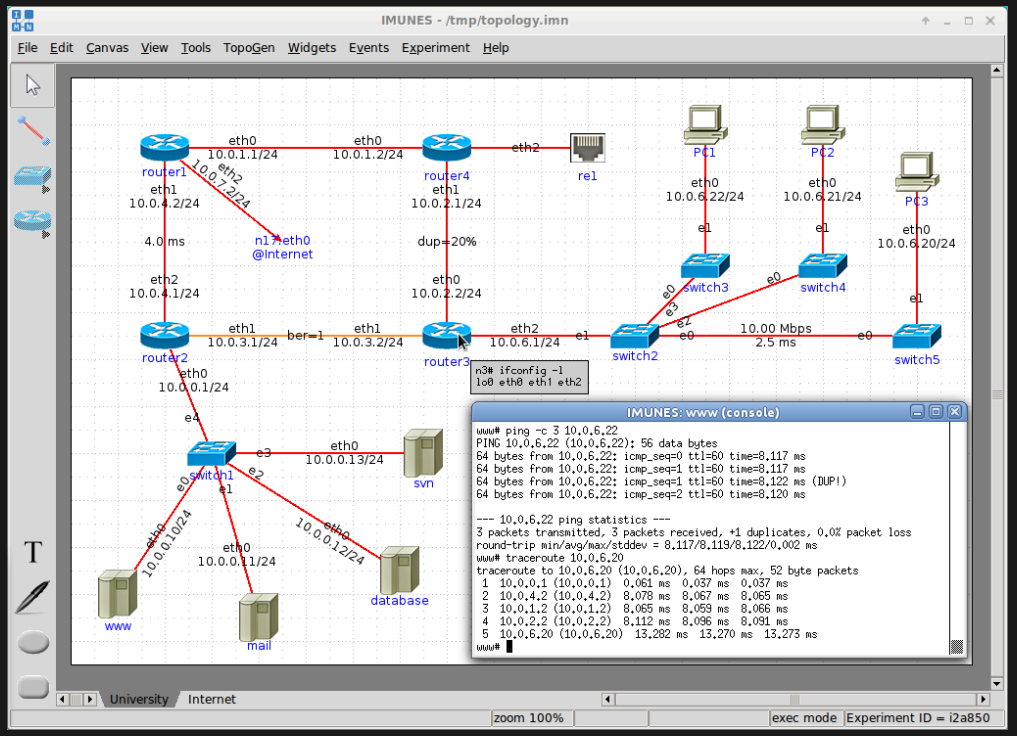
Kako učiti i testirati sigurnost koristeći IMUNES?



Povijest

```
$ whoami
dr. sc. Valter Vasić: https://github.com/oikuda
Završni i diplomski rad: IMUNES + prof. Mikuc + M. Zec
2010 - 2016: FER - razvoj IMUNES-a + Denis
2016 - 2017: Ericsson Nikola Tesla - razvoj softvera (IPsec)
2017 - 2021: ZSIS - sigurnost, pentest, DFIR, NTA
2021 - 20xx: Span - sigurnost, DFIR, docker
```

IMUNES + docker = IMUNES na Linuxu

*s *malo* sigurnosti

Motivacija

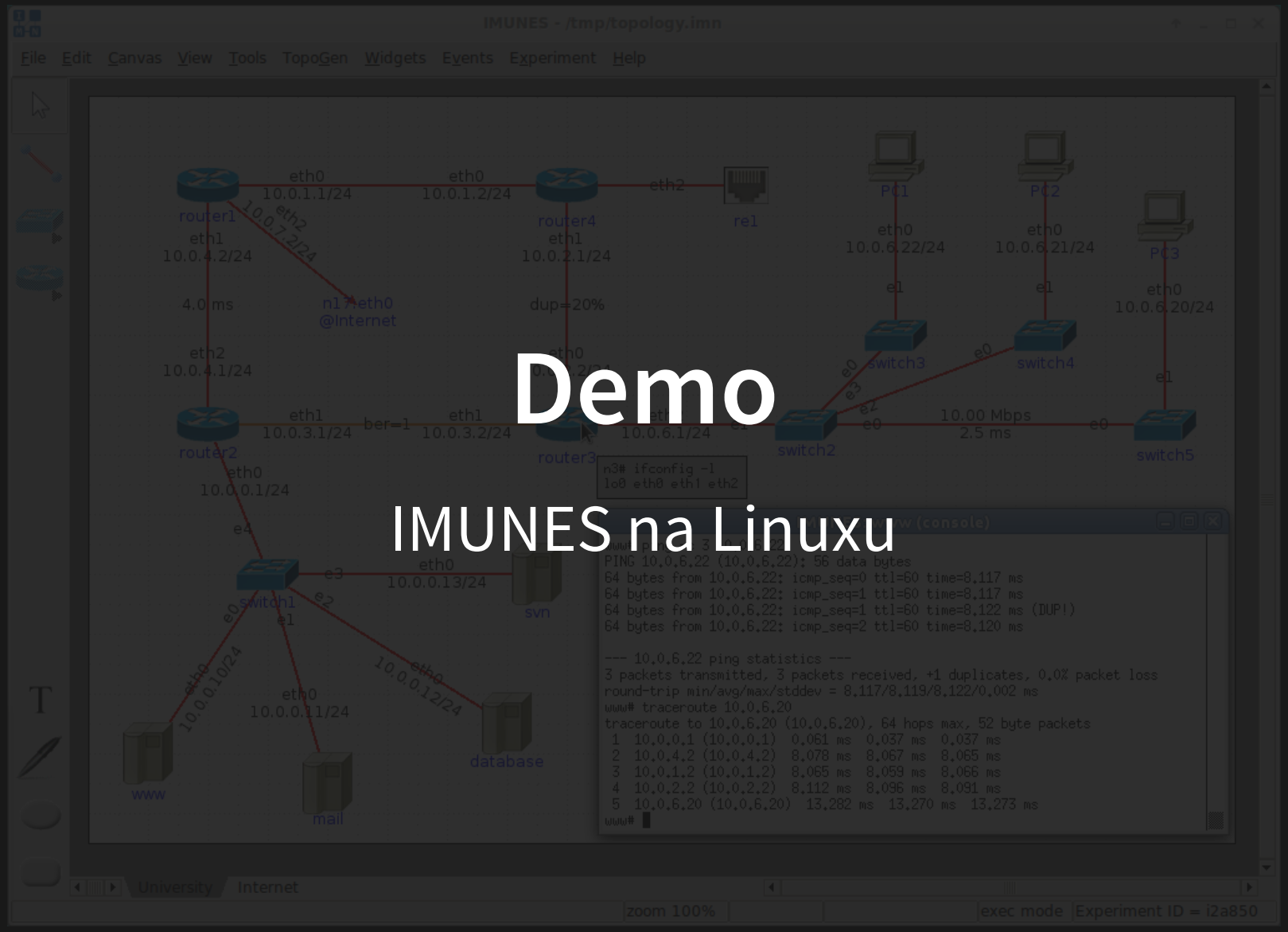
It's not DNS. There's no way it's DNS! It was DNS.

- Jel' ima više DNS *zone transfer* ranjivosti?
  - penetracijsko testiranje (enumeracija)
- Kako se radi DNS amplifikacijski napad?
  - prevencija, sudjelovanje u DDoS napadu
- Kako rekonstruirati ranjivost iz 2018. godine?
  - penetracijsko testiranje
  - odgovor na incidente

Motivacija

Zašto su takve stvari važne?

- Učenje postojećih koncepata značajno olakšava razumijevanje novih.
- Temeljni principi u pravilu ostaju isti, metode se mijenjaju.
- Igranje sa živim sustavom daje dublji uvid u tematiku.



Demo

IMUNES na Linuxu

Demo 1. - DNS *zone transfer*

- omogućuje *krađu* cjelokupne baze za pojedinu poddomenu
- metoda enumeracije, prikupljanja podataka
  - pronalaženje novih meta napada
- autoritativni DNS poslužitelji

Demo 2. - DNS amplifikacija

- omogućuje priliku sudjelovanja u DDoS napadu
  - Distributed Denial of Service
- metoda amplifikacije mrežnog prometa - *IP spoofing*
  - ISP egress filtering
- rekurzivni DNS poslužitelji

Demo 3. - ranjivost SSH servera

- neautentificirano izvođenje koda - RCE
  - kao `root` korisnik, CVE-2018-10933
- teško reproducirati bez specifične verzije softvera
  - https://github.com/vulhub/vulhub
- potrebno postaviti u izoliranoj okolini
  - *honeypot*?

Par sitnica

- *appliancei* su svuda oko nas, teško testirati i pohvatati mušice
- prelazak na *open-source* je težak i zahtijeva resurse
- možda bolje nego hrpa zastarjelog softvera koji se ne ažurira?
- ne postoji *silver bullet*, ali ključno je razumijeti kako stvari rade

https://twitter.com/wdormann/status/1754574402903998502

← Post

Will Dormann
@wdormann

Things on a currrent Ivanti VPN box:
curl 7.19.7 2009-11-04 (14 years)
openssl 1.0.2n-fips 2017-12-07 (6 years)
perl 5.6.1 2001-04-09 (23 years)
psql 9.6.14 2019-06-20 (5 years)
cabextract 0.5 2001-08-20 (22 years)
ssh 5.3p1 2009-10-01 (14 years)
unzip 6.00 2009-04-29 (15 years)

7:35 PM · Feb 5, 2024 · **132.6K** Views

XZ utils?

Zaključak

- Kad se jednom posloži, nema straha od mijenjanja
  - *ako radi, ne diraj* postaje prošlost
- Olakšava učenje mrežnih i sigurnosnih koncepata
  - svatko u timu može imati svoj *pješčanik*
  - ubrzava proces *ukrcavanja* novih ljudi
- Omogućava bezbolno testiranje promjena
  - čak i za kompleksna okruženja


Hvala na pažnji!