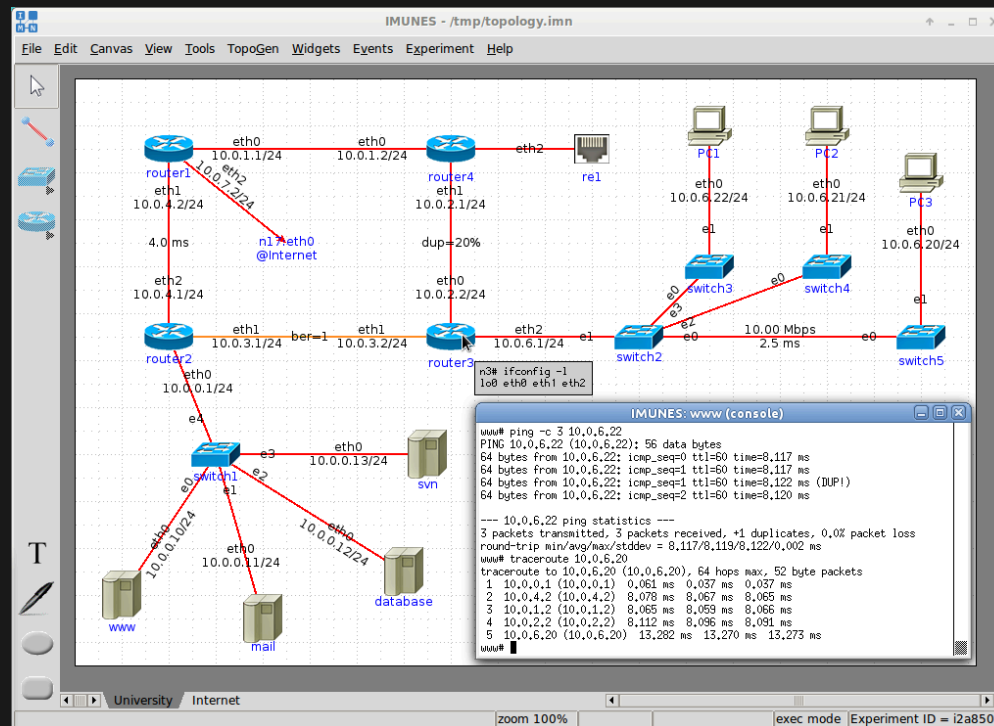


Kako učiti i testirati sigurnost koristeći IMUNES?



Povijest

```
1 $ whoami
2 dr. sc. Valter Vasić: https://github.com/oikuda
3 Završni i diplomski rad: IMUNES + prof. Mikuc + M. Zec
4 2010 - 2016: FER - razvoj IMUNES-a + Denis
5 2016 - 2017: Ericsson Nikola Tesla - razvoj softvera (IPsec)
6 2017 - 2021: ZSIS - sigurnost, pentest, DFIR, NTA
7 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.

IMUNES - /tmp/topology.imn

File Edit Canvas View Tools TopoGen Widgets Events Experiment Help

The screenshot displays a network simulation environment. The main canvas shows a network topology with several routers (router1, router2, router3, router4), switches (switch1, switch2, switch3, switch4, switch5), and servers (www, mail, database, svn). Connections are labeled with interface names and IP addresses. A console window in the bottom right shows the following output:

```

n3# ifconfig -l
lo# eth0 eth1 eth2

PING 10.0.6.22 (10.0.6.22): 56 data bytes
64 bytes from 10.0.6.22: icmp_seq=0 ttl=60 time=8.117 ms
64 bytes from 10.0.6.22: icmp_seq=1 ttl=60 time=8.117 ms
64 bytes from 10.0.6.22: icmp_seq=1 ttl=60 time=8.122 ms (DUP!)
64 bytes from 10.0.6.22: icmp_seq=2 ttl=60 time=8.120 ms

--- 10.0.6.22 ping statistics ---
3 packets transmitted, 3 packets received, +1 duplicates, 0.0% packet loss
round-trip min/avg/max/stddev = 8.117/8.119/8.122/0.002 ms

www# traceroute 10.0.6.20
traceroute to 10.0.6.20 (10.0.6.20), 64 hops max, 52 byte packets
 1 10.0.0.1 (10.0.0.1)  0.061 ms  0.037 ms  0.037 ms
 2 10.0.4.2 (10.0.4.2)  8.078 ms  8.067 ms  8.065 ms
 3 10.0.1.2 (10.0.1.2)  8.065 ms  8.059 ms  8.066 ms
 4 10.0.2.2 (10.0.2.2)  8.112 ms  8.096 ms  8.091 ms
 5 10.0.6.20 (10.0.6.20) 13.282 ms 13.270 ms 13.273 ms
www#

```

University Internet

zoom 100% exec mode Experiment ID = i2a850

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

- neautenticirano 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 current 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!