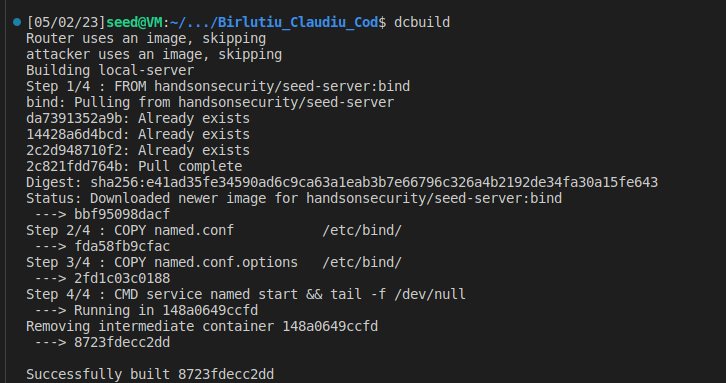
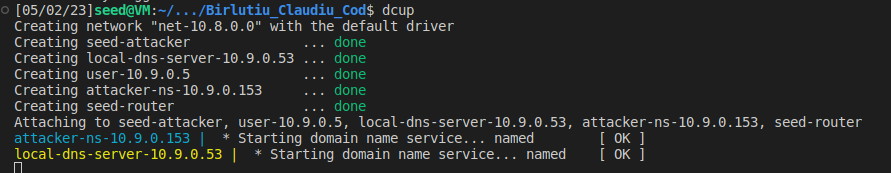
# Raport pentru lucrarea 8: Atacul asupra DNS local

# Autor: Birlutiu Claudiu-Andrei

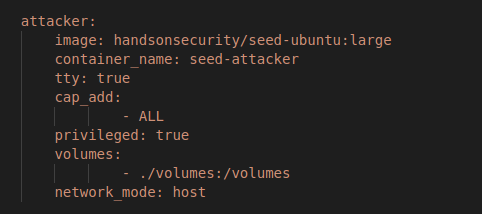
# Setarea mediului

* Pentru a crea mediul local de simulare a atacului DNS a fost nevoie de crearea celor 4 containere docker: unul pentru victima, unul pentru serverul DNS local și 2 pentru atactor
* am rulat comand dcbuild urmat de dcup pentru construirea containerelor necesare și pornirea lor





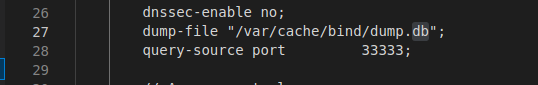
* de remarcat este ca la configurarea container-ului pentru atacator avem setat **network\_mode** la **host** pentru a putea vedea pachetele din alte containere



* în acest caz, containerul attacker este configurat astfel încât vede toate interfetele de retea ale gazdei si chiar areaceleasi adrese IP ca si gazda.

În ceea ce prveste containerul pentru DNS:

* observam ca în fișierul **name.conf.options** avem fixat portul sursa 33333



* de asemenea observam ca a fost dezactivat sistemul de protecția **dnssec**
* am observat de asemenea în fișierul **name.conf** configurarea domeniului attacker32.com, car în momentul în care este accesat se va face o redirectare spre serverul de domeniu din containerul atacatorului

ASPECTE CONTAINER USER

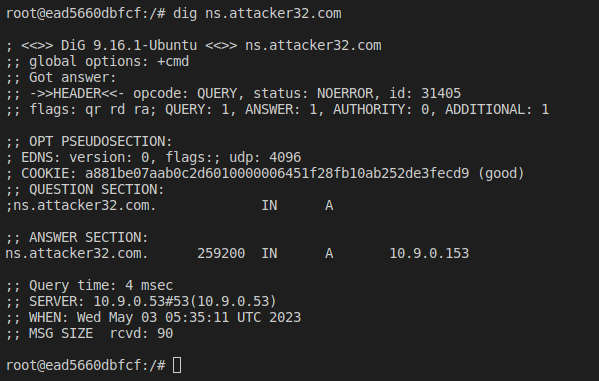
* în fișierul resolv.conf regasim faptul ca serverul 10.9.0.53 este adaugat primul ca server de nume și va juca rolul de dns -server

ASPECTE CONTAINER SERVER NUME ATACATOR

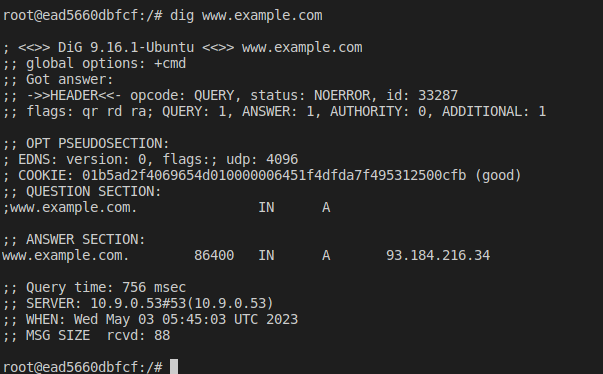
* în acesta în fișierul named.conf sunt declarate 2 zone:
  + - zona legitima a atacatorului **attacker32.com**
    - zona falsa **example.com**

TESTARE CONFIGURARI

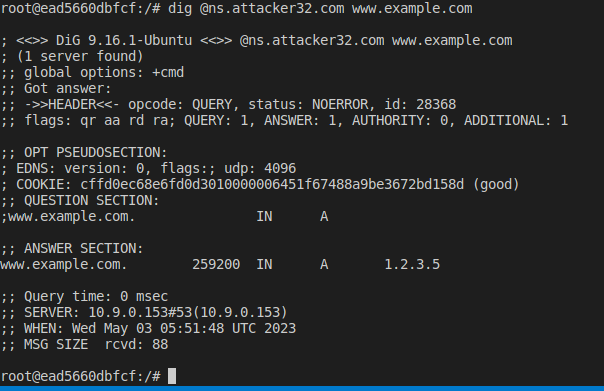
* m-am conectat la containerul user; am rulat comanda *dig ns.attacker32.com* și am obitnut rezultatele din
* comanda dig se folosește pentru a interoga serverele DNS și pentru a obține informații despre adresele IP, recordurile DNS și alte informații de rețea.
* Deoarece în serverul dns e configurat faptul să se facă o redirectionare spre dns server al atacatorului -> obținem informații din fiserul attacker32.com.zone



* în continuare am rulat comand *dig* [*www.example.com*](http://www.example.com/)și am observat faptul ca obținem un ip public, deci cererea a fost trimisa către serverul oficial de nume al domain name-ului example.com



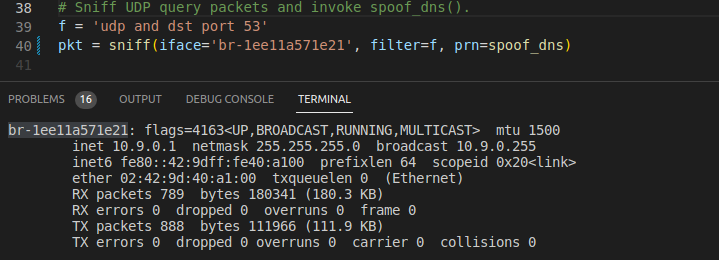
* dacă punem *dig @ns.attacker32.com* [*www.example.com*](http://www.example.com/)
  + interoghează serverul DNS specificat prin "ns.attacker32.com" pentru a obține informații despre adresa IP asociată cu domeniul "[www.example.com](http://www.example.com/)"
  + obținem ip-ul din zone\_example.com din serverul de nume al atacatorului



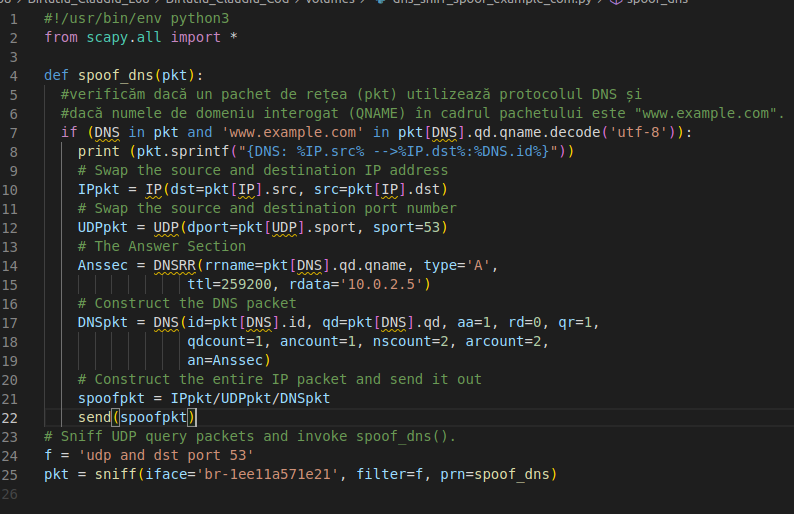
# Sarcini de atac

## Sarcina 1: Falsificarea directă a răspunsului dat utilizatorului

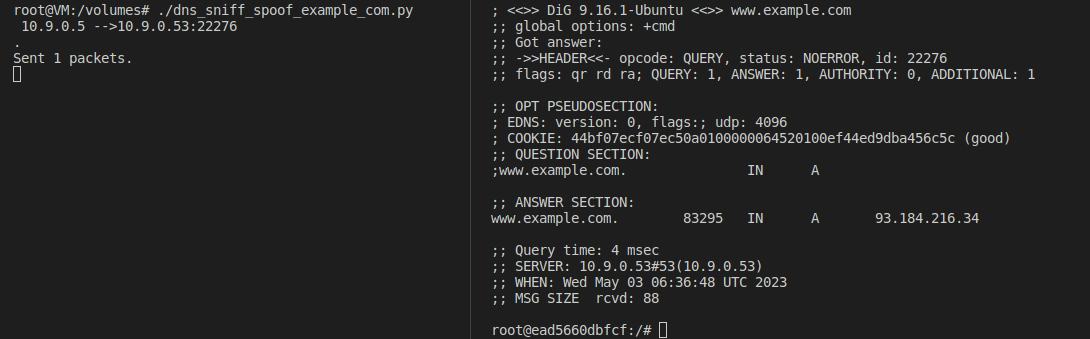
* In prima faza m-am conectat pe containerul atacatorului si am rulat ifconfig pentru a vedea interfata pentru 10.9.0.0 pentru a modifica fisierul dns\_sniff\_spoof.py



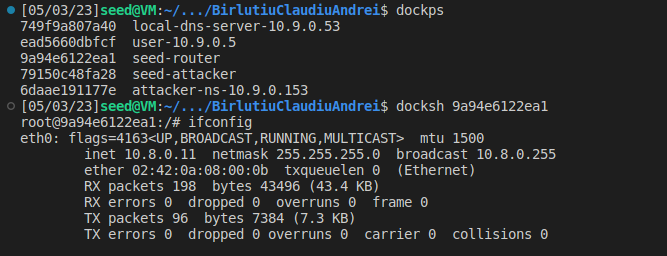
Fisierul de atac arata in felul urmator; am preluat informatia din fisierul dns\_sniff\_spoof.py pus la dispozitie in laborator si am facut pentru example.com



* rulam programul dns\_sniff\_spoof\_example\_com.py creat (cel de sus) din containerul atacatorului
* in prima faza observam ca atacatprul a interceptat cererea DNS si chiar daca a trimis un pachet ca raspuns, userul a primit raspuns mai rapid de la serverul de nume real al domeniul [www.example.com](http://www.example.com/)



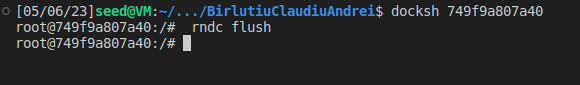
* pentru a remedia problema, am aplicat sugestiile din laborator prin care incetinesc traficul de internet
  + - gasim in prima faza interfata pentru 10.8.0.0 si aceasta e eth0

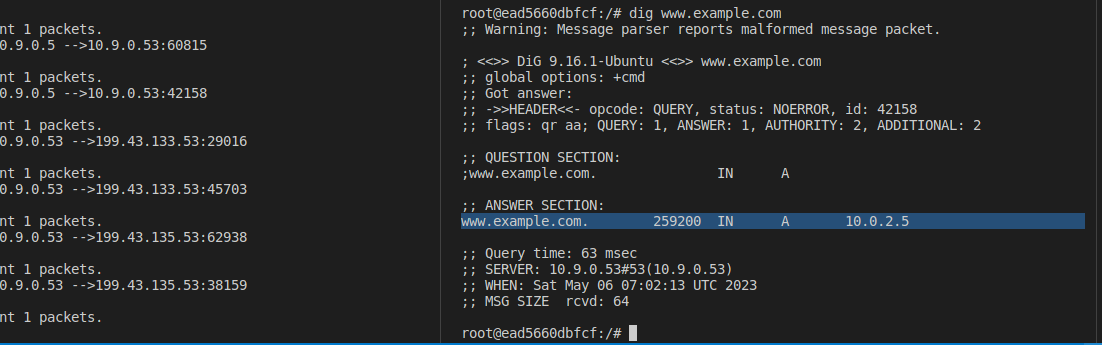


* + - al doilea pas este executia comenzii tc pe eth0: *tc qdisc add dev eth0 root netem delay 100ms*



* + - facem clear la dns-ul local



* + - executam comanda dq si observam ca nu se va mai ajunge la serverul de nume real al domeniului example.com ci la atacator

## Sarcina 2: Atacul cu otrăvirea cache DNS – falsificarea răspunsurilor

## Sarcina 3: Falsificarea înregistrărilor NS

## Sarcina 4: Falsificarea înregistrărilor NS pentru alt domeniu

## Sarcina 5: Falsificarea înregistrărilor din secțiunea Additional