

Όνοματεπώνυμο: Περόγαμβρος Γεώργιος	Όνομα PC:
Ομάδα: 2	Ημερομηνία: 08/06/2022

Εργαστηριακή Άσκηση 12

Υπηρεσίες στο Διαδίκτυο

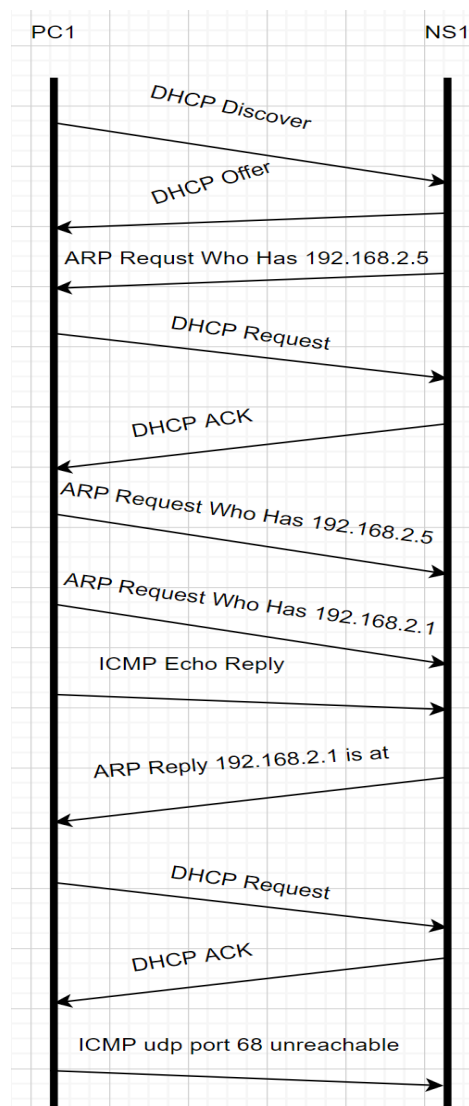
Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 Χρησιμοποίησα την εντολή `tcpdump -i em0 -vvn -e -n`.

1.2 Χρησιμοποίησα την εντολή `dhclient em0`.

1.3



1.4 Ανταλλάσσονται τα εξής μηνύματα:

```
root@PC:~ # dhclient em0
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 8
Jun  2 20:27:05 PC dhclient[7631]: send_packet: Network is down
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 21
DHCPOFFER from 192.168.2.1
DHCPREQUEST on em0 to 255.255.255.255 port 67
DHCPACK from 192.168.2.1
bound to 192.168.2.5 -- renewal in 60 seconds.
```

Στην καταγραφή φαίνεται μόνο ένα DHCP Discover μήνυμα.

1.5 Η διεύθυνση που αποδόθηκε στο PC1 είναι η 192.168.2.5 και η IPv4 του εξυπηρετητή είναι η 192.168.2.1

1.6 Μετά από 60 δευτερόλεπτα.

1.7 Το UDP.

1.8 Η 67 για το NS1 και η 68 για το PC1.

1.9 DHCP Discover:

Αποστολέας 0.0.0.0 – Παραλήπτης 255.255.255.255

DHCP Offer:

Αποστολέας 192.168.2.1 – Παραλήπτης 192.168.2.5

DHCP Request:

Αποστολέας 0.0.0.0 – Παραλήπτης 255.255.255.255

DHCP ACK:

Αποστολέας 192.168.2.1 – Παραλήπτης 192.168.2.5

1.10 DHCP Discover:

Αποστολέας 08:00:27:4f:64:6a (em0 PC1) – Παραλήπτης ff:ff:ff:ff:ff:ff (broadcast)

DHCP Offer:

Αποστολέας 08:00:27:69:b3:ab (em0 NS1) – Παραλήπτης 08:00:27:4f:64:6a (em0 PC1)

DHCP Request:

Αποστολέας 08:00:27:4f:64:6a (em0 PC1) – Παραλήπτης ff:ff:ff:ff:ff:ff (broadcast)

DHCP ACK:

Αποστολέας 08:00:27:69:b3:ab (em0 NS1) – Παραλήπτης 08:00:27:4f:64:6a (em0 PC1)

1.11 Κατά την αποστολή ο PC1 στέλνει τα πακέτα χρησιμοποιώντας την απροσδιόριστη IP (0.0.0.0), ενώ κατά την λήψη καταλαβαίνει πως τα πακέτα απευθύνονται λόγω της MAC.

1.12 Ναι. Το πλαίσιο ARP παράχθηκε από τον NS1 προκειμένου να μάθει αν η 192.168.2.5 χρησιμοποιείται ήδη από κάποιο μηχάνημα πριν την προσφέρει στο PC1.

1.13 Όχι, δεν παρατηρείται μήνυμα ICMP πριν την απάντηση DHCP Offer.

1.14 Το ARP αυτό στέλνεται για να βεβαιωθεί πως κανείς άλλος δεν χρησιμοποιεί αυτήν την IP και

για να ενημερωθούν οι arp πίνακες των γειτόνων του.

1.15 Ναι, παρατηρούνται μηνύματα ICMP μετά την απόδοση διεύθυνσης στο PC1. Το PC1 στέλνει αυτά τα μηνύματα προκειμένου να επιβεβαιώσει πως μπορεί να επικοινωνεί μέσω της νέας IP.

1.16 Διαρκεί για 120 δευτερόλεπτα.

1.17 Υπάρχει το Option 54 (Server-ID) και το Option 50 (Requested-IP).

1.18 Η MAC και η IP δεν είναι broadcast, αλλά είναι αυτές του NS1 και επίσης δεν υπάρχουν τα options Server-ID και Requested-IP.

1.19 Για να ενημερώσει τον NS1 πως έλαβε το DHCP Ack.

1.20 Στο αρχείο /var/db/dhcpd/dhcpd.leases.

1.21 Κάθε 1 λεπτό.

1.22 Πότε ξεκίνησε το δάνειο, πότε λήγει, πότε υπήρξε τελευταία φορά επικοινωνία σχετικά με αυτό το δάνειο, το τρέχον και το επόμενο binding state, rewinding binding state, τη mac το uid και το hostname του μηχανήματος στο οποίο έχει δοθεί αυτό το δάνειο,

1.23 Στο αρχείο /var/db/dhclient.leases.em0.

1.24 Την διεπαφή την οποία αφορά το δάνειο, την ip, τη μάσκα υποδικτύου, την ip του δρομολογητή, την διεύθυνση broadcast, την διάρκεια του δανείου, dhcp message type 5, dhcp server-id, renew, rebind και expire time.

1.25 Πρέπει να περάσουν 45 δευτερόλεπτα.

1.26 Ζήτησε 9 παραμέτρους.

1.27 Προσδιορίζει τις Subnet-Mask, BR, Default-Gateway.

1.28 Χρησιμοποίησα την εντολή tcpdump -i em0 -n.

1.29 Χρησιμοποίησα την εντολή service isc-dhcpd stop.

1.30 Ο έλεγχος έγινε με την εντολή ifconfig em0 και η επανεκκίνηση με την εντολή service isc-dhcpd restart.

1.31 Με την εντολή ifconfig em0 βλέπουμε πως μετά από λίγο αποδίδεται διεύθυνση στον PC1.

1.32 Στέλνει 6 μηνύματα DHCP Request πριν χάσει την IP του ανά ~10-15 δευτερόλεπτα.

1.33 Λαμβάνει απάντηση ICMP udp port 67 unreachable που σημαίνει πως ο εξυπηρετητής δεν είναι διαθέσιμος.

1.34 Η διεύθυνση εκπομπής.

1.35 Χρησιμοποιήθηκε η διεύθυνση εκπομπής προκειμένου το PC1 να αναζητήσει διεύθυνση IP από κάποιον άλλο dhcp server.

1.36 Είναι οι ff:ff:ff:ff:ff:ff και η 255.255.255.255. Καταλαβαίνουμε πως έχει απολεσθεί η διεύθυνση IP από το πεδίο Requested-IP.

1.37 Για να δει αν η διεύθυνση χρησιμοποιείται.

1.38 Τα προηγούμενα δάνεια διαγράφηκαν.

1.39 Επειδή ο εξυπηρετητής χρειάζεται να επικοινωνήσει με τον πελάτη χωρίς να γνωρίζει την IP

του. Έτσι, μπορεί να χρειαστεί ο εξυπηρετητής να στείλει broadcast μήνυμα. Αν χρησιμοποιούσαμε μια τυχαία θύρα για τον πελάτη, μπορεί άλλα μηχανήματα στο δίκτυο να χρησιμοποιούσαν αυτήν την τυχαία θύρα για κάποια άλλη υπηρεσία και έτσι να δημιουργούνταν προβλήματα, τα οποία αποτρέπονται με την ύπαρξη της θύρας 67 ως θύρα πελάτη dhcp.

2

2.1 Άνοιξα το αρχείο με vi. Έτρεξα την εντολή `%s/my.domain/ntua.lab/g`. Πρόσθεσα τις εγγραφές 192.168.2.5 PC1.ntua.lab PC1 και 192.168.2.6 PC2.ntua.lab PC2.

2.2 Σε όλες τις περιπτώσεις απαντάει το PC2. Άρα η χρήση μικρών ή κεφαλαίων δεν παίζει ρόλο.

2.3 Πράγματι, απαντά το PC1.

2.4 Παίρνουμε την απάντηση ping: cannot resolve PC1: Host name lookup failure.

2.5 Πρόσθεσα τις εγγραφές local-data:"pc1.ntua.lab. IN A 192.168.2.5" και local-data:"pc2.ntua.lab. IN A 192.168.2.6"

2.6 Πρόσθεσα τις εγγραφές local-data-ptr:"192.168.2.5 pc1.ntua.lab.192.168.2.5" και local-data-ptr:"192.168.2.6 pc2.ntua.lab."

2.7 Χρησιμοποίησα τις εντολές unbound-checkconf, cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf και service unbound restart.

2.8 Χρησιμοποίησα την εντολή tcpdump -i em0 -vvv -n.

2.9 Χρησιμοποίησα τις εντολές ifconfig em0 192.168.2.5/28 delete και dhclient em0.

2.10 Έλαβε την 192.168.2.5.

2.11 Οι επιπλέον παράμετροι που υπάρχουν στο DHCP Offer σε σύγκριση με την 1.27 είναι οι Domain-Name Option 15 "ntua.lab", Domain-Name-Server Option 6 192.168.2.1.

2.12 Έχει δημιουργηθεί. Το περιεχόμενό του είναι :

```
# Generated by resolvconf
```

```
search.ntua.lab
```

```
nameserver 192.168.2.1
```

2.13 Χρησιμοποίησα την εντολή host 192.168.2.5. Το όνομα του 192.168.2.5 είναι pc1.ntua.lab.

2.14 Χρησιμοποίησα την εντολή host ns1. Η διεύθυνση του μηχανήματος NS1 είναι η 192.168.2.1.

2.15 Ναι, μπορώ.

2.16 Χρησιμοποίησα τις εντολές ifconfig em0 192.168.2.6/28 delete και dhclient em0.

2.17 Έλαβε την 192.168.2.6.

2.18 Ναι, μπορώ.

2.19 Από τον εξυπηρετητή DNS, αφού έχουμε διαγράψει την αντίστοιχη εγγραφή στο αρχείο /etc/hosts.

2.20 Όχι, καθώς προσπαθεί να κάνει ping την 192.168.2.7.

2.21 Πρώτα αναζητείται η πληροφορία στο /etc/hosts και έπειτα, αν δεν βρεθεί, ρωτάται ο DNS.

- 2.22 Το σχετικό περιεχόμενο είναι hosts: files dns, που συμφωνεί με αυτό που παρατηρήσαμε.
- 2.23 Είναι η 192.168.2.6. Χρησιμοποίησα την εντολή host PC2.
- 2.24 Η εντολή host λειτουργεί πραγματοποιώντας queries στους dns servers του αρχείου /etc/resolv.conf
- 2.25 Χρησιμοποίησα τις εντολές rm /etc/resolv.conf, resolvconf -u. Το περιεχόμενο του αρχείου είναι ακριβώς το ίδιο με πριν.
- 2.26 Χρησιμοποίησα την εντολή tcpdump -i em0 -n -vvv "not port 67 && not port 68".
- 2.27 Χρησιμοποίησα την εντολή host ntua.lab. Η ζητούμενη IP είναι η 192.168.2.1.
- 2.28 Ναι, υπάρχει.
- 2.29 Χρησιμοποιείται το UDP.
- 2.30 Χρησιμοποιούνται οι θύρες 53, 52326, 59844, 42208.
- 2.31 Η 53.
- 2.32 Χρησιμοποίησα την εντολή tcpdump -i em0 -n -vvv port 53.
- 2.33 Χρησιμοποίησα την εντολή host ns1. Είναι η 192.168.2.1.
- 2.34 Παράχθηκαν 6 μηνύματα DNS.
- 2.35 Αντιστοιχούσαν σε ερωτήματα για την IPv4 (A?), για την IPv6(AAAA?) και για τον mailserver(MX?). Όλες αφορούσαν το όνομα ns1.ntua.lab.
- 2.36 Σε αυτήν για την IPv4 και σε αυτήν για τον mailserver.
- 2.37 Χρησιμοποίησα την εντολή drill ns1 και drill ns1.ntua.lab.
- 2.38 Έγιναν ερωτήσεις για το όνομα ns1 και για το ns1.ntua.lab αντίστοιχα. Απάντηση λάβαμε μόνο στο δεύτερο (ποια είναι η IP του).
- 2.39 Η drill αναζητά μόνο για το όνομα το οποίο ζητήσαμε. Η host το προσθέτει (από το αρχείο /etc/resolv.conf) αν δεν υπάρχει ήδη.
- 2.40 Δεν παράγονται σε καμία από τις δύο περιπτώσεις.
- 2.41 Χρησιμοποίησα την εντολή ping ns1.
- 2.42 Ανταλλάχθηκαν 2 μηνύματα DNS που αφορούσαν την IPv4 του ns1.
- 2.43 Κάθε φορά που εκτελούμε την εντολή ping παράγονται δύο DNS μηνύματα (ερώτηση και απάντηση).
- 2.44 Οι απαντήσεις του εξυπηρετητή δεν φαίνεται να αποθηκεύονται στο PC1 μετά το πέρας της εκτέλεσης της εντολής.

3

- 3.1 Χρησιμοποίησα την εντολή sysrc hostname="SRV" και sysrc lighttpd_enable="YES".
- 3.2 Χρησιμοποίησα την εντολή mkdir /usr/local/www/data.
- 3.3 Χρησιμοποίησα την εντολή touch /usr/local/www/data/index.html και επεξεργάστηκα το αρχείο με vi.

- 3.4 Χρησιμοποίησα την εντολή `reboot`.
- 3.5 Χρησιμοποιώντας την εντολή `service lighttpd status`.
- 3.6 Με την εντολή `netstat -a |grep http` βλέπουμε πως η υπηρεσία `http` είναι σε state `LISTEN`.
- 3.7 Χρησιμοποίησα την εντολή `ifconfig em0 192.168.2.3/28`.
- 3.8 Πρόσθεσα την εγγραφή `local-data: "srv.ntua.lab IN A 192.168.2.3"`.
- 3.9 Πρόσθεσα την εγγραφή `local-data-ptr: "192.168.2.3 srv.ntua.lab"`.
- 3.10 Χρησιμοποίησα τις εντολές `unbound-checkconf`, `cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf` και `service unbound restart`.
- 3.11 Χρησιμοποίησα την εντολή `tcpdump -i em0 -n`.
- 3.12 Χρησιμοποίησα την εντολή `fetch http://srv.ntua.lab/index.html`.
- 3.13 Χρησιμοποιήθηκε το πρωτόκολλο μεταφοράς `tcp` και η θύρα `80`.
- 3.14 Στο `index.html` που δημιουργήθηκε.

4

- 4.1 Χρησιμοποίησα την εντολή `sysrc gateway_enable="YES"`.
- 4.2 Χρησιμοποίησα την εντολή `sysrc firewall_enable="YES"`.
- 4.3 Χρησιμοποίησα την εντολή `sysrc firewall_type="open"`.
- 4.4 Χρησιμοποίησα την εντολή `sysrc firewall_type="open"`.
- 4.5 Χρησιμοποίησα την εντολή `sysrc firewall_nat_enable="YES"`.
- 4.6 Χρησιμοποίησα την εντολή `cat /etc/rc.conf`.
- 4.7 Με `netstat -rn` βλέπουμε πως είναι ορισμένη η σωστή `default gateway`.
- 4.8 Το επιβεβαίωσα με `host pc2`.
- 4.9 Χρησιμοποίησα τις εντολές `sysrc ifconfig_em0="DHCP"` και `service netif restart`.
- 4.10 Χρησιμοποίησα τις εντολές `sysrc ifconfig_em0="inet 192.168.2.4 netmask 255.255.255.240"` και `sysrc defaultrouter="192.168.2.1"`.
- 4.11 Χρησιμοποίησα τις εντολές `service netif restart` και `service routing restart`. Αφού έφτιαξα το `/etc/resolv.conf` βεβαιώθηκε πως η επίλυση ονομάτων λειτουργεί χρησιμοποιώντας την εντολή `host pc1`.
- 4.12 Χρησιμοποίησα τις εντολές `sysrc ifconfig_em0="inet 192.168.2.18 netmask 255.255.255.240"` και `sysrc defaultrouter="192.168.2.17"`, `service netif restart` και `service routing restart`.
- 4.13 Αφού άλλαξα στις κατάλληλες εγγραφές την διεύθυνση του `pc2` σε `192.168.2.3` και του `srv` σε `192.168.2.18`, χρησιμοποίησα τις εντολές `unbound-checkconf`, `cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf` και `service unbound restart`.
- 4.14 Ναι, μπορώ.
- 4.15 Χρησιμοποίησα την εντολή `ipfw add 2000 deny all from any to 192.168.2.0/28 in recv em2`.
- 4.16 Όχι, δεν μπορώ.

- 4.17 Χρησιμοποίησα την εντολή `ipfw add 1900 allow all from 192.168.2.0/28 to 192.168.2.16/28 in recv em0 keep-state`.
- 4.18 Ναι, μπορώ.
- 4.19 Ναι, μπορώ.
- 4.20 Όχι, δεν μπορώ.
- 4.21 Χρησιμοποίησα την εντολή `ipfw nat 111 config if em1 unreg_only reset`.
- 4.22 Χρησιμοποίησα την εντολή `ipfw add 3000 nat 111 ip4 from any to any via em1`.
- 4.23 Ναι, μπορώ.
- 4.24 Χρησιμοποιώντας την εντολή `host 147.102.1.1` βλέπουμε πως το όνομα που αντιστοιχεί στην συγκεκριμένη διεύθυνση είναι το `theseas.softlab.ece.ntua.gr`.
- 4.25 Χρησιμοποίησα την εντολή `tcpdump -i em1 -n`.
- 4.26 Με τη διεύθυνση 10.0.3.15.
- 4.27 Η διεύθυνση προορισμού των `icmp echo requests` είναι η 147.102.224.101.
- 4.28 Προς τον 1.1.1.1
- 4.29 Χρησιμοποίησα την εντολή `tcpdump -i em1 -n port 53`.
- 4.30 Όλα αρχικά απευθύνονται στον 8.8.8.8. Επίσης στα περισσότερα ο εξυπηρετητής απαντάει με το CName του ονόματος για το οποίο γίνεται η ερώτηση και γίνεται επιπλέον ερώτηση για να μάθουμε τη διεύθυνσή του παρόλο που αυτή έχει δοθεί από το πρώτο μήνυμα (μαζί με το CName).
- 4.31 Χρησιμοποίησα την εντολή `tcpdump -i em0 -n port 53`.
- 4.32 Το κανονικό όνομα είναι `courses.cn.ece.ntua.gr`.
- 4.33 Ο PC1 ζήτησε να μάθει την IPv4 του `courses.cn.ntua.gr` και ο NS1 του απάντησε με τη ζητούμενη ip και το αντίστοιχο cname. Ο NS1 κάνει ερώτηση για την IPv4 και των κανονικών ονομάτων που βρίσκονται στις απαντήσεις που λαμβάνει. Επίσης, τα δικά του ερωτήματα είναι μεγαλύτερα από του PC1 και έχουν τη σημαία 1au.
- 4.34 Χρησιμοποίησα την εντολή `tcpdump -i em1 -n -vvv port 53`.
- 4.35 Παρατηρούμε μόνο 1 ερώτημα. Η απάντηση έχει διάρκεια 20 λεπτά.
- 4.36 Παράγονται μηνύματα DNS με τη χρονική διάρκεια να μειώνεται σε κάθε απάντηση.
- 4.37 Ο τοπικός DNS στο NS1 διατηρεί τοπικά για ένα χρονικό διάστημα τις απαντήσεις που λαμβάνει από άλλους DNS.
- 4.38 Ναι, μπορούμε.
- 4.39 Δεν μπορούμε καθώς δεν έχουμε ορίσει DNS Server στον srv.
- 4.40 Έφτιαξα το αρχείο `/etc/resolv.conf` με περιεχόμενο `search ntua.lab nameserver 192.168.2.17`.
- 4.41 Τώρα μπορούμε.
- 4.42 Με την εντολή `host www.ntua.lab` λαμβάνουμε το αποτέλεσμα `www.ntua.lab is an alias for ntua.lab`. Αν κάνουμε `ping` λαμβάνουμε το error `ping: cannot resolve www.ntua.lab: Unknown server error`.

4.43 Πρόσθεσα την εγγραφή local-data: "www.ntua.lab. IN A 192.168.2.18".

4.44 Απαντά ο SRV.

5

5.1 Χρησιμοποίησα την εντολή sysrc hostname="ns2.ntua.lab".

5.2 Χρησιμοποίησα τις εντολές sysrc ifconfig_em0="inet 192.0.2.1 netmask 255.255.255.248" και sysrc ifconfig_em2="inet 192.0.2.9 netmask 255.255.255.248".

5.3 Χρησιμοποίησα την εντολή sysrc ifconfig_em1="DHCP".

5.4 Χρησιμοποίησα την εντολή sysrc gateway_enable="YES".

5.5 Χρησιμοποίησα την εντολή sysrc firewall_enable="YES".

5.6 Χρησιμοποίησα την εντολή sysrc firewall_type="open".

5.7 Χρησιμοποίησα την εντολή sysrc firewall_nat_enable="YES".

5.8 Χρησιμοποίησα τις εντολές sysrc -x dhcp_ifaces="em0" και sysrc -x dhcp_enable="YES").

5.9 Χρησιμοποίησα την εντολή sysrc -a | grep unbound. Υπάρχει.

5.10 Αφού έκανα τις ζητούμενες αλλαγές εκτέλεσα τις εντολές unbound-checkconf, cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf.

5.11 Χρησιμοποίησα την εντολή reboot και την εντολή netstat -rn. Υπάρχει προκαθορισμένη διαδρομή.

5.12 Χρησιμοποίησα την εντολή ipfw nat 222 config if em1 reset same_ports.

5.13 Χρησιμοποίησα την εντολή ipfw add 1100 nat 222 ip4 from any to any via em1.

5.14 Χρησιμοποίησα τις εντολές sysrc ifconfig_em0="inet 192.0.2.2 masknet 255.255.255.248" και sysrc defaultrouter="192.0.2.1".

5.15 Χρησιμοποίησα τις εντολές service netif restart, service routing restart. Έκανα τις απαραίτητες αλλαγές στο /etc/resolv.conf και επιβεβαίωσα πως λειτουργεί η επίλυση ονομάτων κάνοντας host google.com.

5.16 Ναι, μπορώ.

5.17 Χρησιμοποίησα τις εντολές sysrc ifconfig_em1="inet 192.0.2.10 netmask 255.255.255.248" και sysrc defaultrouter="192.0.2.9".

5.18 Αφού μετακίνησα την em1 έτρεξα τις εντολές service netif restart και service routing restart.

5.19 Ναι, μπορούμε. Η λειτουργία του nat 111 παραμένει.

5.20 Στο PC1 επιστρέφει την 192.168.2.18(SRV) και στο PC2 την 192.0.2.10(NS1). Χρησιμοποίησα την εντολή host www.ntua.lab.

5.21 Δεν μπορούμε, εμφανίζεται το λάθος fetch: <http://www.ntua.lab>: Connection refused.

5.22 Χρησιμοποίησα την εντολή ipfw nat 111 config if em1 unreg_only reset redirect_port tcp 192.168.2.18:80 80.

5.23 Ναι, μπορούμε τώρα.

5.24 Μπορούμε και απαντάει ο NS1.

5.25 Συνδεόμαστε στον SRV.

5.26 Τώρα συνδεόμαστε στον NS1 καθώς η ανακατεύθυνση που ορίσαμε προηγουμένως αφορούσε μόνο την θύρα 80, η οποία δεν χρησιμοποιείται από το ssh. Επομένως σύμφωνα με τον DNS του PC2 (NS2) το www.ntua.lab ανακατευθύνεται στον NS1. Ο PC1 συνδέθηκε στον SRV καθώς υπάρχει εγγραφή στον DNS του (NS1) που ταιριάζει το www.ntua.lab στον SRV.

5.27 Χρησιμοποίησα την εντολή `ipfw nat 111 config if em1 unreg_only reset redirect_port tcp 192.168.2.18:80 80 redirect_port tcp 192.168.2.18:22 22`.

5.28 Ναι, πλέον συνδεόμαστε με ssh στον SRV και το επιβεβαιώνουμε με την εντολή `who` στον SRV.