



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής



Εργασία Μαθήματος **Ασφάλεια Πληροφοριακών Συστημάτων**

| | |
|---|-------------------------------|
| Άσκηση <<αριθμός άσκησης>> | 3- ipsec |
| Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας) | Κουσουνής Κωνσταντίνος p14086 |
| | |
| | |
| | |
| Ημερομηνία παράδοσης | 27-03-2019 |



Με βάση το αντίστοιχο εργαστηριακό μάθημα [1], να εγκαταστήσετε και να παραμετροποιήσετε IPSec συνδέσεις σε linux περιβάλλον, χρησιμοποιώντας το λογισμικό strongswan. Σημείωση: Πριν την υλοποίηση της άσκησης εκτελέστε την εντολή `apt-get install strongswan strongswan-pki` σε περίπτωση που παρατηρήσετε ότι η υπηρεσία αυτή δεν λειτουργεί.

(II) Δημιουργία και εγκατάσταση κλειδιών.

- a. Δημιουργήστε μία Αρχή Πιστοποίησης (ΑΠ - CA) η οποία θα χρησιμοποιήσει τον αλγόριθμο Elliptic Curve DSA (ecdsa-256) για τη δημιουργία του ιδιωτικού κλειδιού της μήκους 256 bit. Η ΑΠ μπορεί να δημιουργηθεί στον έναν από τους δύο κόμβους που θα χρησιμοποιήσετε στην άσκηση.
- b. Δημιουργήστε ένα self-signed πιστοποιητικό για την ΑΠ.
- c. Μέσω της ΑΠ να δημιουργήσετε, για κάθε άκρο της σύνδεσης τα ιδιωτικά κλειδιά και τα αντίστοιχα πιστοποιητικά. Για τα δύο άκρα της σύνδεσης τα κλειδιά να είναι κλειδιά RSA μήκους 2048 bit.
- d. Αντιγράψτε σε κάθε άκρο της σύνδεσης, στους αντίστοιχους φακέλους του ipsec τα εξής: το ιδιωτικό κλειδί του κόμβου, το πιστοποιητικό του και τέλος το πιστοποιητικό της ΑΠ. Τέλος διαμορφώστε ανάλογα το αρχείο `ipsec.secrets` ώστε να μπορεί κάθε κόμβος να χρησιμοποιεί το ιδιωτικό κλειδί του.

(II) Δημιουργία και δοκιμή συνδέσεων

Δημιουργήστε και δοκιμάστε διαδοχικά τις παρακάτω συνδέσεις (connections) που περιγράφονται στα βήματα (Α)-(Β). Κάθε μία από τις παρακάτω συνδέσεις εκκινήστε την και επαληθεύστε με τη βοήθεια ενός packet snifer (πχ wireshark) τις αντίστοιχες συνδέσεις. Στο τελικό σας παραδοτέο να περιλαμβάνονται τα αρχεία `ipsec.conf` από τα δύο άκρα, με όλες τις παραπάνω συνδέσεις και οποιοδήποτε άλλο αρχείο πιθανώς απαιτείται. Χρήσιμα παραδείγματα μπορείτε να βρείτε στα [2], [3].

(Α) Σύνδεση host-to-host (κόμβος-με-κόμβο) με IKE2 και με τη χρήση των παραπάνω πιστοποιητικών (όπως και το παράδειγμα του εργαστηρίου)

(Β) Παραλλαγή του προηγούμενου παραδείγματος με χρήση AH και αλγόριθμο hash SHA256.

Πηγές

[1] <https://pithos.oceanos.grnet.gr/public/KFTegMmilW2yk2AisrlsI4>

[2] <https://wiki.strongswan.org/projects/strongswan/wiki/UserDocumentation>

[3] <https://www.strongswan.org/testresults.html>



Εγκατάσταση IPsec (Strongswan) και στα δύο μηχανήματα μου.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# apt-get install strongswan  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  libstrongswan libstrongswan-standard-plugins strongswan-charon  
  strongswan-libcharon strongswan-starter  
Suggested packages:  
  libstrongswan-extra-plugins libcharon-extra-plugins  
The following NEW packages will be installed:  
  libstrongswan libstrongswan-standard-plugins strongswan strongswan-charon  
  strongswan-libcharon strongswan-starter  
0 upgraded, 6 newly installed, 0 to remove and 925 not upgraded.  
Need to get 1,359 kB of archives.  
After this operation, 3,877 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y
```

Με την εντολή `apt-get install strongswan`. Τρέχω την εντολή και στα δύο μηχανήματα μου.



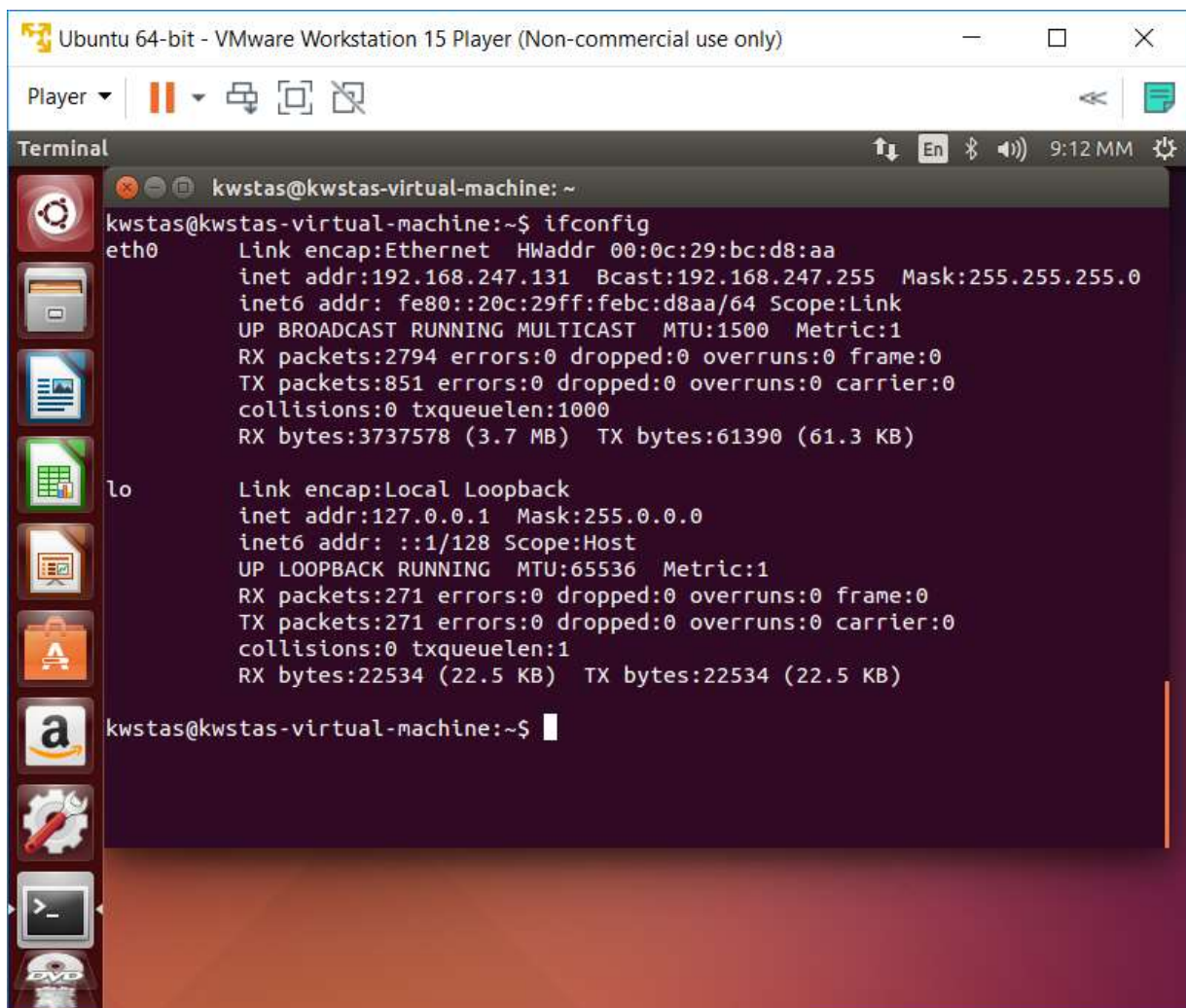
```
Ubuntu 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player ▾ | [Icons] | [Progress Bar]
Terminal [Icons] 9:10 MM
kwstas@kwstas-virtual-machine: ~
kwstas@kwstas-virtual-machine:~$ sudo apt-get install strongswan
[sudo] password for kwstas:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libstrongswan strongswan-ike strongswan-plugin-openssl strongswan-starter
Suggested packages:
  strongswan-tnc-imcvs network-manager-strongswan strongswan-plugin-agent
  strongswan-plugin-certexpire strongswan-plugin-coupling
  strongswan-plugin-curl strongswan-plugin-dnscert strongswan-plugin-dnskey
  strongswan-plugin-duplicheck strongswan-plugin-error-notify
  strongswan-plugin-ipseckey strongswan-plugin-ldap strongswan-plugin-led
  strongswan-plugin-lookip strongswan-plugin-ntru strongswan-plugin-pkcs11
  strongswan-plugin-radattr strongswan-plugin-sql strongswan-plugin-soup
  strongswan-plugin-unity strongswan-plugin-whitelist strongswan-tnc-client
  strongswan-tnc-server
The following NEW packages will be installed:
  libstrongswan strongswan strongswan-ike strongswan-plugin-openssl
  strongswan-starter
0 upgraded, 5 newly installed, 0 to remove and 451 not upgraded.
Need to get 3576 kB of archives.
After this operation, 15,5 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Θα χρησιμοποιήσω το ubuntu μηχανημα μου για την έκδοση του testCa

```
connect to socket failed: Permission denied
kwstas@kwstas-virtual-machine:~$ sudo ipsec status
RX bytes:22534 (22.5 KB)  TX bytes:22534 (22.5 KB)
kwstas@kwstas-virtual-machine:~$ ipsec status
Connect to socket failed: Permission denied
kwstas@kwstas-virtual-machine:~$ sudo ipsec status
Security Associations (0 up, 0 connecting):
  none
kwstas@kwstas-virtual-machine:~$
```



```
root@kali:~# sudo ipsec status
root@kali:~# ipsec start
Starting strongSwan 5.7.2 IPsec [starter]...
root@kali:~# ipsec status
Security Associations (0 up, 0 connecting):
    none
root@kali:~# ipsec stop
Stopping strongSwan IPsec...
root@kali:~#
```

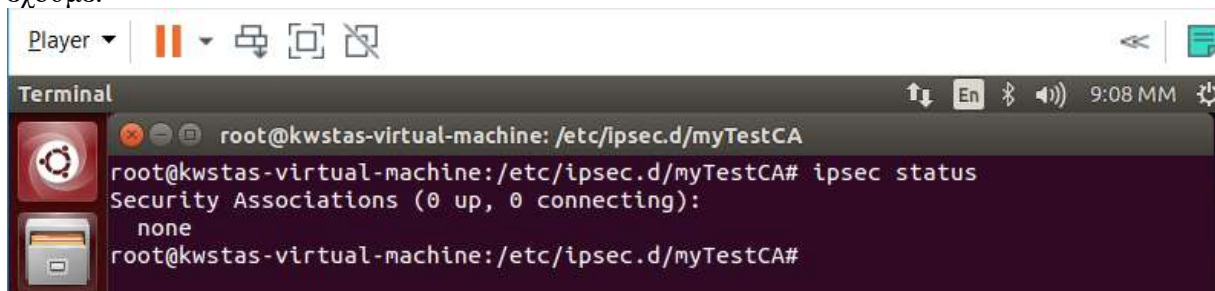




Με ip 192.168.247.131

Δημιουργήστε μία Αρχή Πιστοποίησης (ΑΠ - CA) η οποία θα χρησιμοποιήσει τον αλγόριθμο Elliptic Curve DSA (ecdsa-256) για τη δημιουργία του ιδιωτικού κλειδιού της μήκους 256 bit. Η ΑΠ μπορεί να δημιουργηθεί στον έναν από τους δύο κόμβους που θα χρησιμοποιήσετε στην άσκηση.

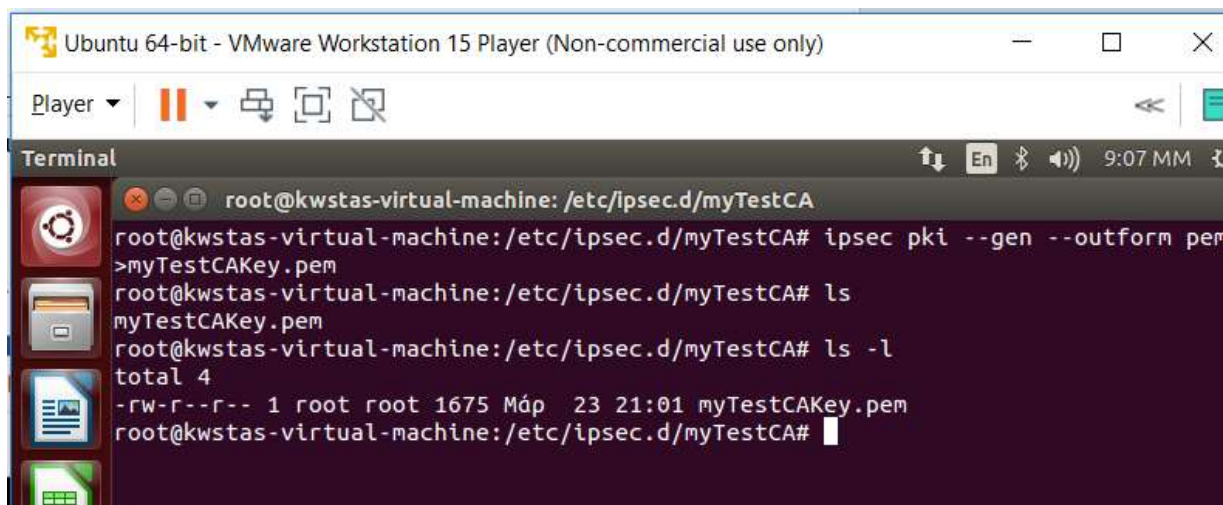
Για το παράδειγμα μας θα δημιουργήσουμε μια αρχή πιστοποίησης στο Μηχάνημα Ubuntu που έχουμε.



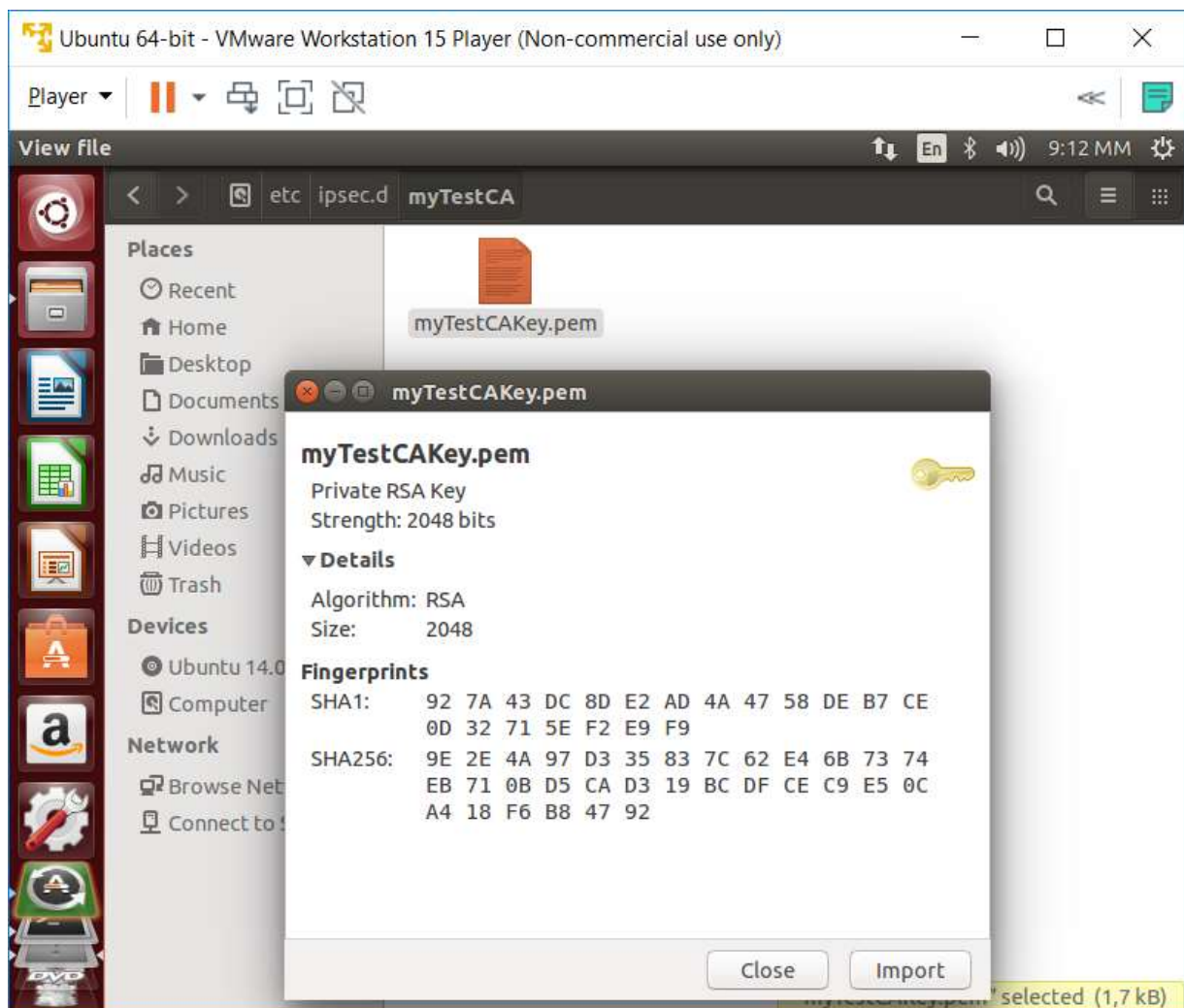
```
Player | [Icons] | 9:08 MM
Terminal
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA# ipsec status
Security Associations (0 up, 0 connecting):
    none
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA#
```

Δημιουργία πιστοποιητικού μέσα στο φάκελο /etc/ipsec.d.

Δημιουργία φακέλου **myTestCA**



```
Ubuntu 64-bit - VMware Workstation 15 Player (Non-commercial use only)
Player | [Icons] | 9:07 MM
Terminal
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA# ipsec pki --gen --outform pem
>myTestCAKey.pem
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA# ls
myTestCAKey.pem
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA# ls -l
total 4
-rw-r--r-- 1 root root 1675 Μάρ 23 21:01 myTestCAKey.pem
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA#
```



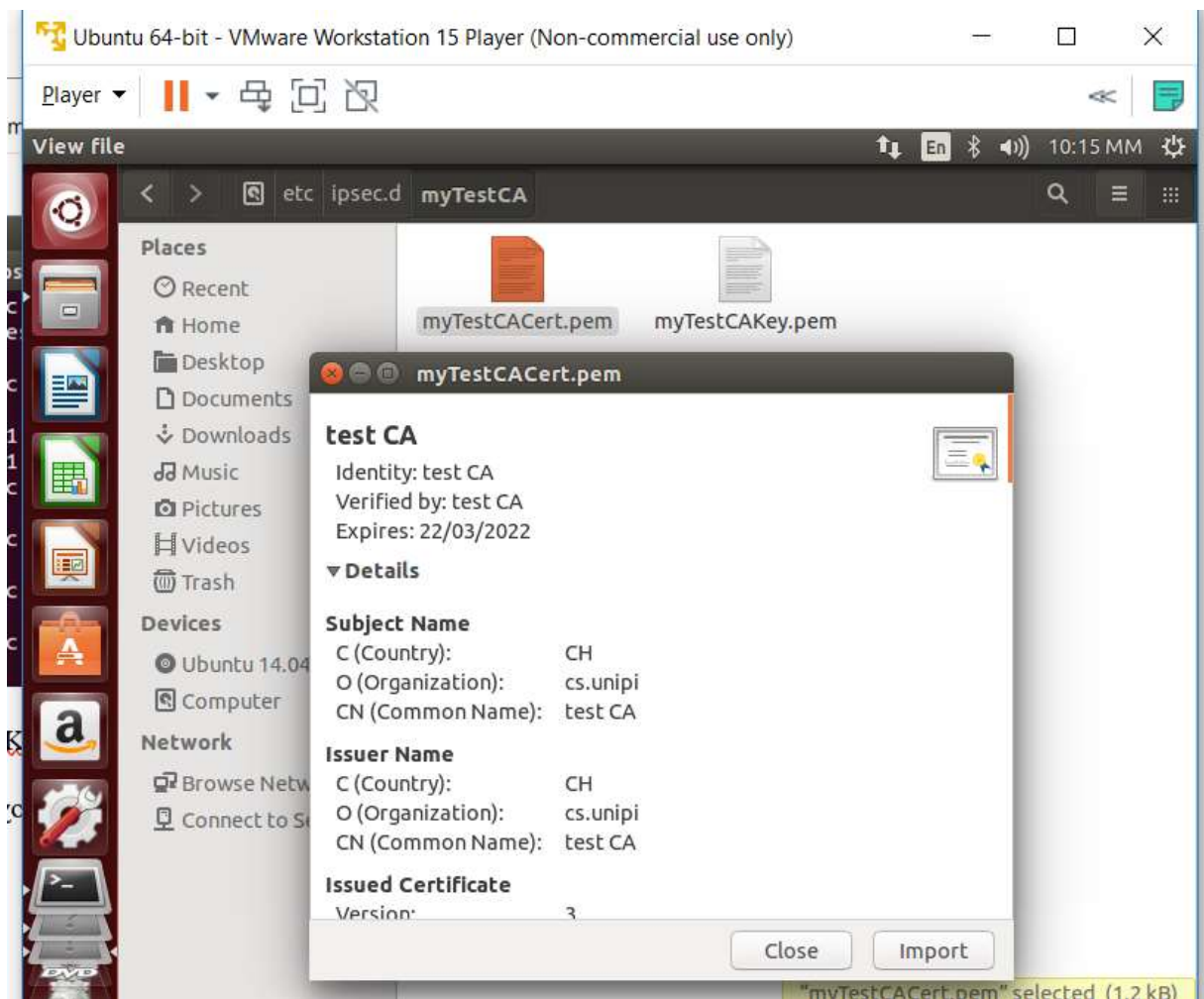
Μπαίνουμε και ελέγχουμε το πιστοποιητικό μας.

Στην συνέχεια θα μπούμε να δημιουργήσουμε ένα αυτό υπογεγραμμένο πιστοποιητικό

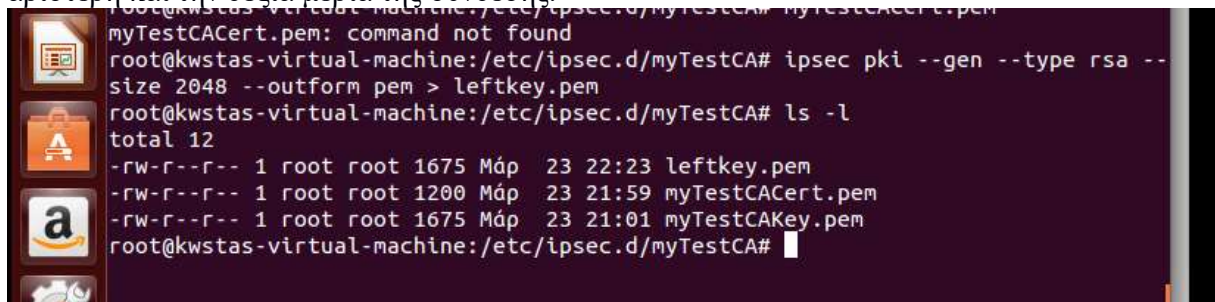


```
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA# ipsec pki --self --in myTestCAKey.pem --dn "C=CH, O=cs.unipi, CN=test CA" --ca --outform pem > myTestCACert.pem
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA# ls -l
total 8
-rw-r--r-- 1 root root 1200 Μάρ 23 21:59 myTestCACert.pem
-rw-r--r-- 1 root root 1675 Μάρ 23 21:01 myTestCAKey.pem
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA# ls
myTestCACert.pem myTestCAKey.pem
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA# ls
myTestCACert.pem myTestCAKey.pem
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA# myTestCACert.pem
myTestCACert.pem: command not found
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA#
```

Τρέχω την εντολή `ipsec pki --self --in myTestCAKey.pem --dn "C=CH, O=cs.unipi, CN=test CA" --CA --outform pem > myTestCACert.pem`
Στην συνέχεια μπαίνουμε να κάνουμε έναν έλεγχο.

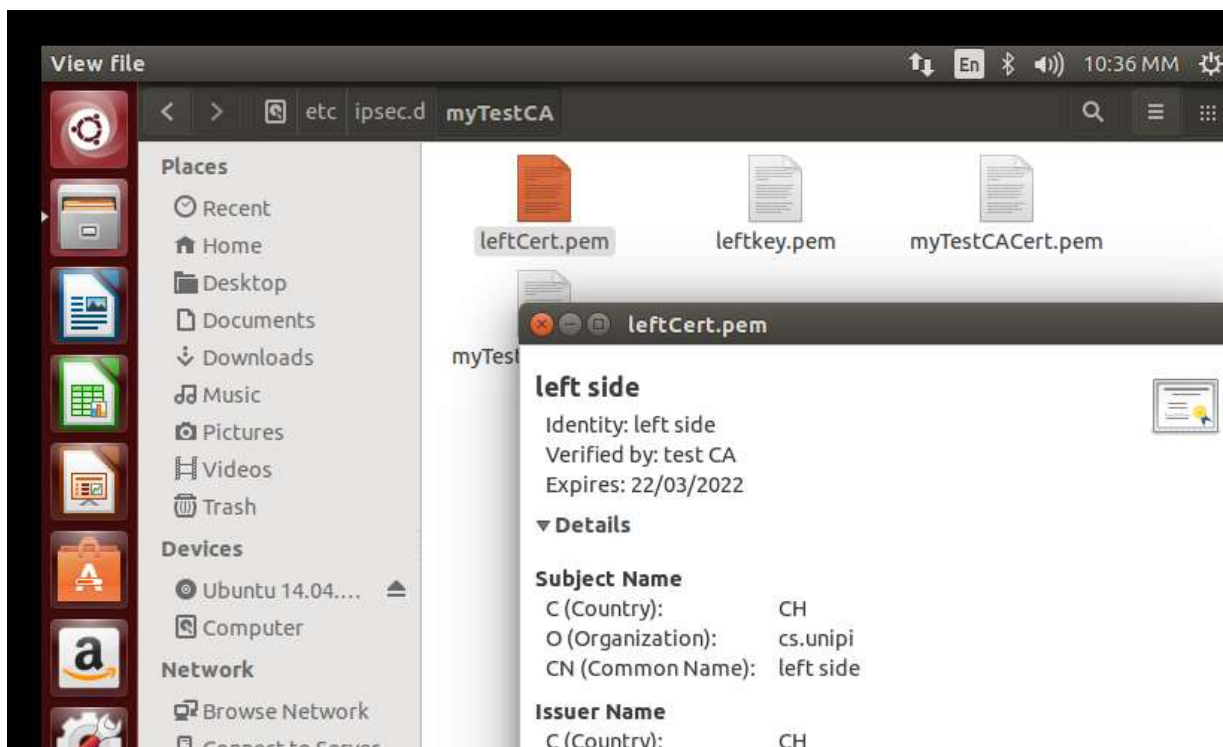


Δημιουργία με το test CA υπογραφής και εξαγωγής κλειδιά που θα δοκιμάσουμε για την αριστερή και την δεξιά μεριά της σύνδεσης.





```
root@kwstas-virtual-machine:/etc/ipsec.d/myTestCA# ipsec pki --pub --in leftkey.
pem | ipsec pki --issue --cacert myTestCACert.pem --cakey myTestCAKey.pem --dn "
C=CH, O=cs.unipi, CN=left side" --flag ikeIntermediate --flag serverAuth --outfo
rm pem >leftCert.pem
root@kwstas-virtual-machine:/etc/ipsec.d/myTestCA# ls -l
total 16
-rw-r--r-- 1 root root 1143 Μάρ  23 22:34 leftCert.pem
-rw-r--r-- 1 root root 1675 Μάρ  23 22:23 leftkey.pem
-rw-r--r-- 1 root root 1200 Μάρ  23 21:59 myTestCACert.pem
-rw-r--r-- 1 root root 1675 Μάρ  23 21:01 myTestCAKey.pem
root@kwstas-virtual-machine:/etc/ipsec.d/myTestCA#
```



Ομοίως για την άλλη πλευρά.

```
root@kwstas-virtual-machine:/etc/ipsec.d/myTestCA# ipsec pki --pub --in rightkey.
.pem | ipsec pki --issue --cacert myTestCACert.pem --cakey myTestCAKey.pem --dn
"C=CH, O=cs.unipi, CN=right side" --flag ikeIntermediate --flag serverAuth --outf
orm pem >rightCert.pem
root@kwstas-virtual-machine:/etc/ipsec.d/myTestCA# ls -l
total 24
-rw-r--r-- 1 root root 1143 Μάρ  23 22:34 leftCert.pem
-rw-r--r-- 1 root root 1675 Μάρ  23 22:23 leftkey.pem
-rw-r--r-- 1 root root 1200 Μάρ  23 21:59 myTestCACert.pem
-rw-r--r-- 1 root root 1675 Μάρ  23 21:01 myTestCAKey.pem
-rw-r--r-- 1 root root 1143 Μάρ  25 21:48 rightCert.pem
-rw-r--r-- 1 root root 1675 Μάρ  25 21:46 rightKey.pem
root@kwstas-virtual-machine:/etc/ipsec.d/myTestCA#
```



```
Terminal
root@kwstas-virtual-machine: /etc/ipsec.d/myTestCA
root@kwstas-virtual-machine:/etc/ipsec.d/myTestCA# ls ../cacerts/
myTestCACert.pem
root@kwstas-virtual-machine:/etc/ipsec.d/myTestCA# ls ../private/
leftkey.pem
root@kwstas-virtual-machine:/etc/ipsec.d/myTestCA# ls ../certs/
leftCert.pem
root@kwstas-virtual-machine:/etc/ipsec.d/myTestCA#
```

Κάνω αντιγραφή των αρχείων που δημιούργησα στα αντίστοιχα path.

```
KaliLinux32bit - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications Places Terminal Mon 16:30
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.247.132 netmask 255.255.255.0 broadcast 192.168.247.255
    inet6 fe80::20c:29ff:fe81:1d31 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:81:1d:31 txqueuelen 1000 (Ethernet)
    RX packets 12129 bytes 17646102 (16.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4014 bytes 243190 (237.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 18 bytes 1038 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 1038 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

Η IP της δεξιάς μεριάς.



```
root@kali: /etc/ipsec.d
File Edit View Search Terminal Help
root@kali:/etc/ipsec.d# ls
aacerts  cacerts  crls      ocspcerts  private
aacerts  certs    myTestCA  policies    reqs
root@kali:/etc/ipsec.d# ls certs/
rightCert.pem
root@kali:/etc/ipsec.d# ls private/
rightKey.pem
root@kali:/etc/ipsec.d# ls cacerts/
myTestCACert.pem
root@kali:/etc/ipsec.d#
```

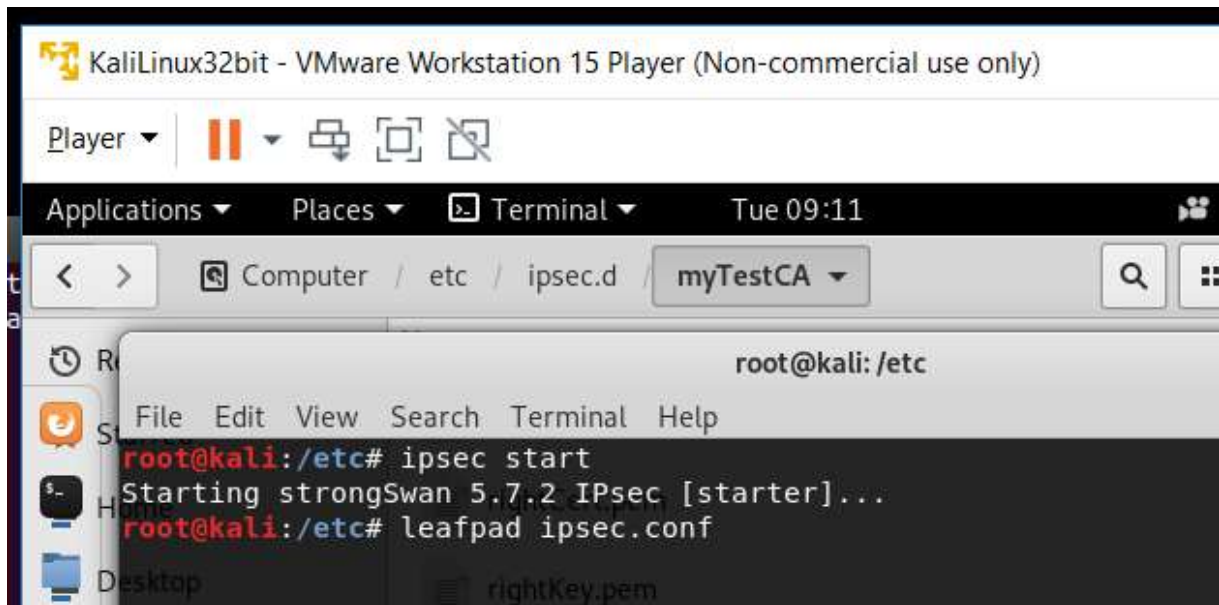
Με τον ίδιο τρόπο περνάμε τα αρχεία στην δεξιά μεριά.
Δημιουργία σύνδεσης και στις δύο πλευρές.

```
#con ifplugd -with-ca-cert profile
# ImageMagick-6t=10.1.0.0/16 profile.d
# root@kali:/etc# leafpad ipsec.conf
# right=192.168.0.2
```

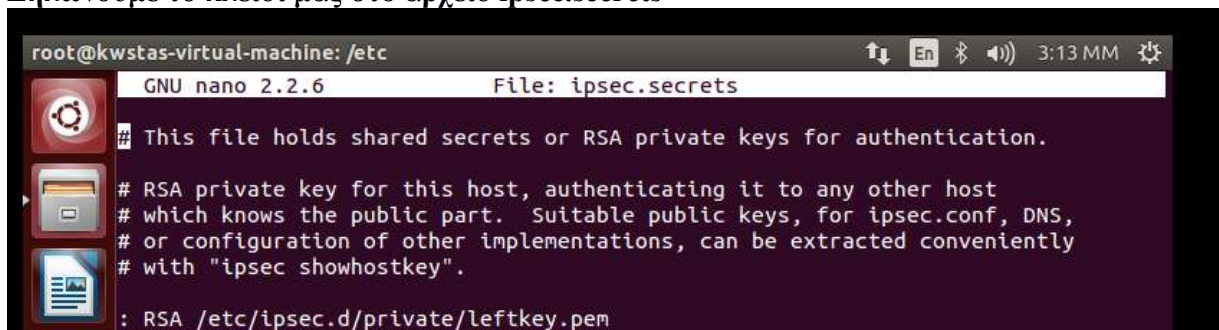
```
# auto=start

conn ipsec-con-right
    left=192.168.247.131
    leftid="0=cs.unipi, CN=left side"
    right=192.168.247.132
    rightcert=rightCert.pem
    keyexchange=ikev2
    auto=add
include /var/lib/strongswan/ipsec.conf.inc
```

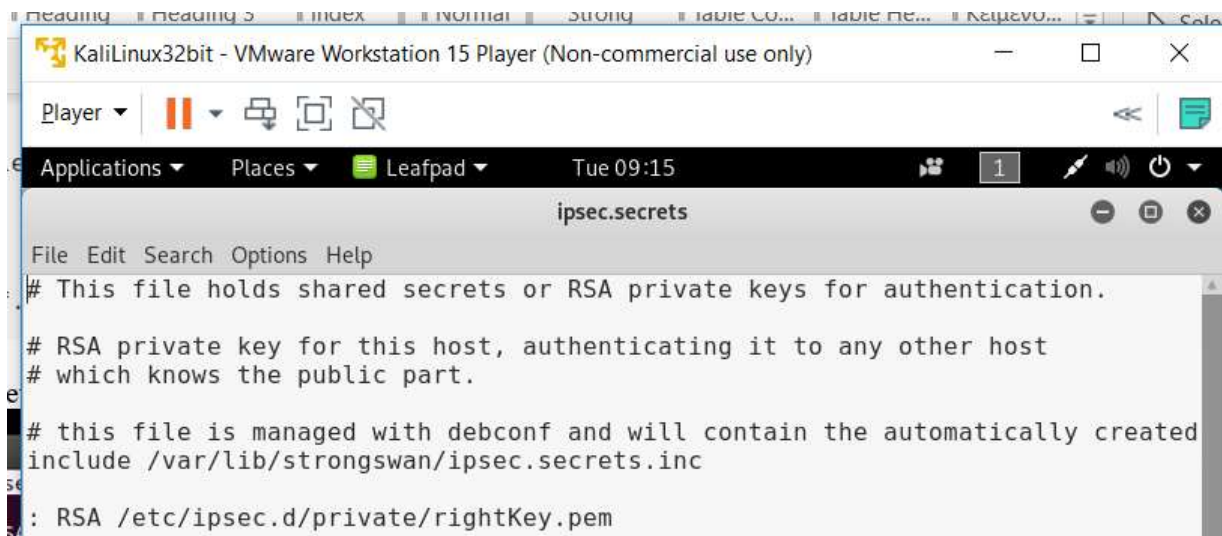
Στην συνέχεια πάμε στο άλλο μηχάνημα.



Δηλώνουμε το κλειδί μας στο αρχείο ipsec.secrets

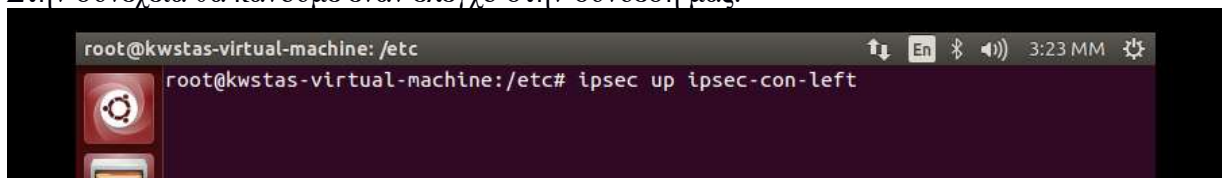


Με την ίδια διαδικασία και στην δεξιά μεριά.



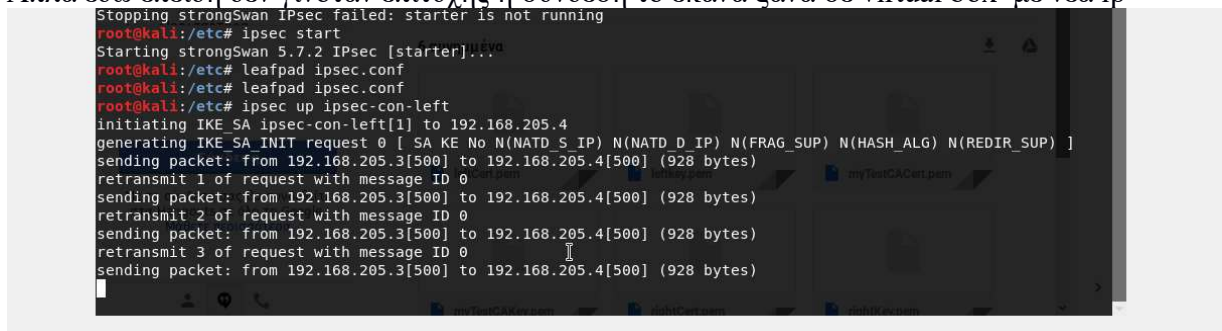
```
ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.
#
# RSA private key for this host, authenticating it to any other host
# which knows the public part.
#
# this file is managed with debconf and will contain the automatically created
include /var/lib/strongswan/ipsec.secrets.inc
: RSA /etc/ipsec.d/private/rightKey.pem
```

Στην συνέχεια θα κάνουμε έναν έλεγχο στην σύνδεση μας.



```
root@kwstas-virtual-machine: /etc
root@kwstas-virtual-machine: /etc# ipsec up ipsec-con-left
```

Αλλά εδώ επειδή δεν γινόταν επιτυχής η σύνδεση το έκανα ξάνα σε virtual box με νέα ip



```
Stopping strongSwan IPsec failed: starter is not running
root@kali: /etc# ipsec start
Starting strongSwan 5.7.2 IPsec [starter]...
root@kali: /etc# leafpad ipsec.conf
root@kali: /etc# leafpad ipsec.conf
root@kali: /etc# ipsec up ipsec-con-left
initiating IKE SA ipsec-con-left[1] to 192.168.205.4
generating IKE SA INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
sending packet: from 192.168.205.3[500] to 192.168.205.4[500] (928 bytes)
retransmit 1 of request with message ID 0
sending packet: from 192.168.205.3[500] to 192.168.205.4[500] (928 bytes)
retransmit 2 of request with message ID 0
sending packet: from 192.168.205.3[500] to 192.168.205.4[500] (928 bytes)
retransmit 3 of request with message ID 0
sending packet: from 192.168.205.3[500] to 192.168.205.4[500] (928 bytes)
```

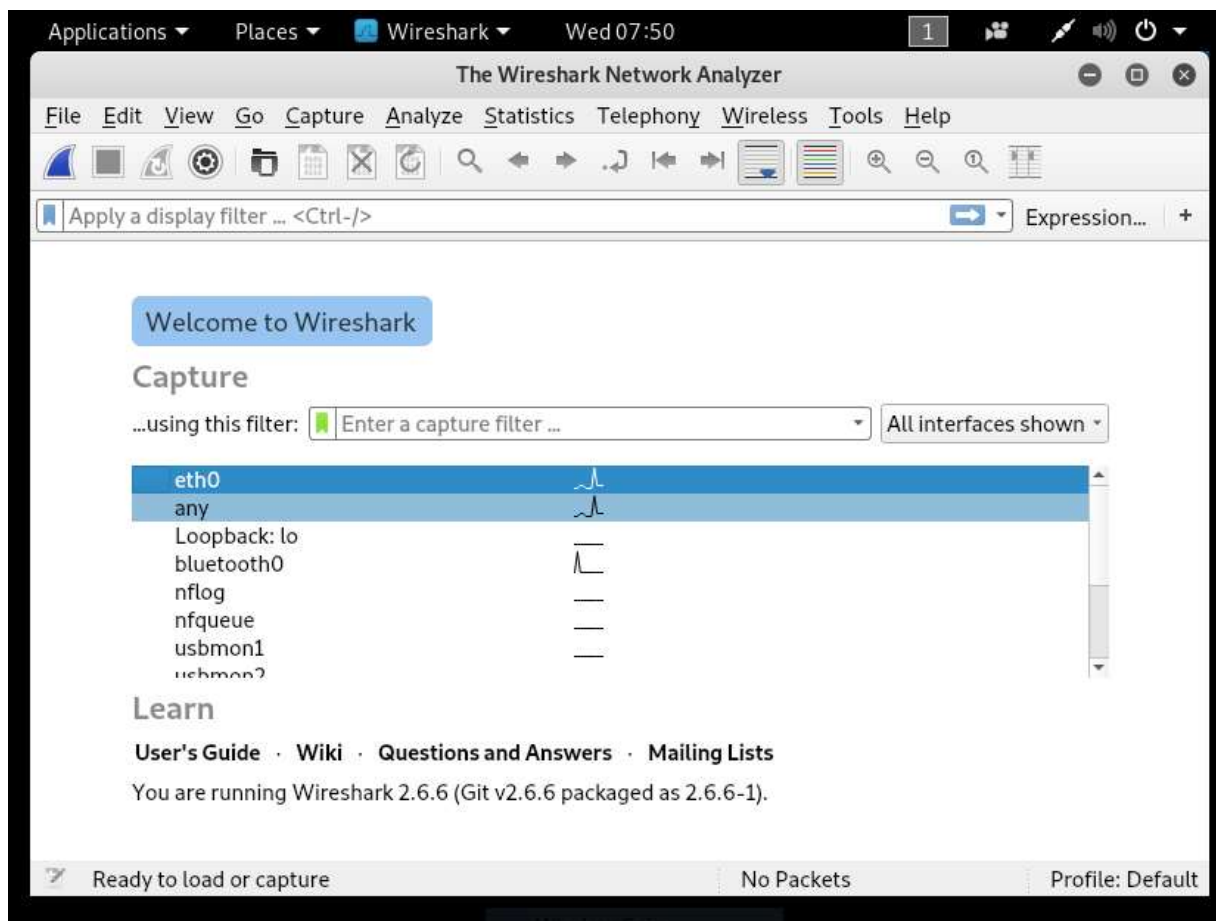
Ελέγχουμε αν έχει γίνει η σύνδεση μας με την εντολή **ipsec up ipsec-con-left**



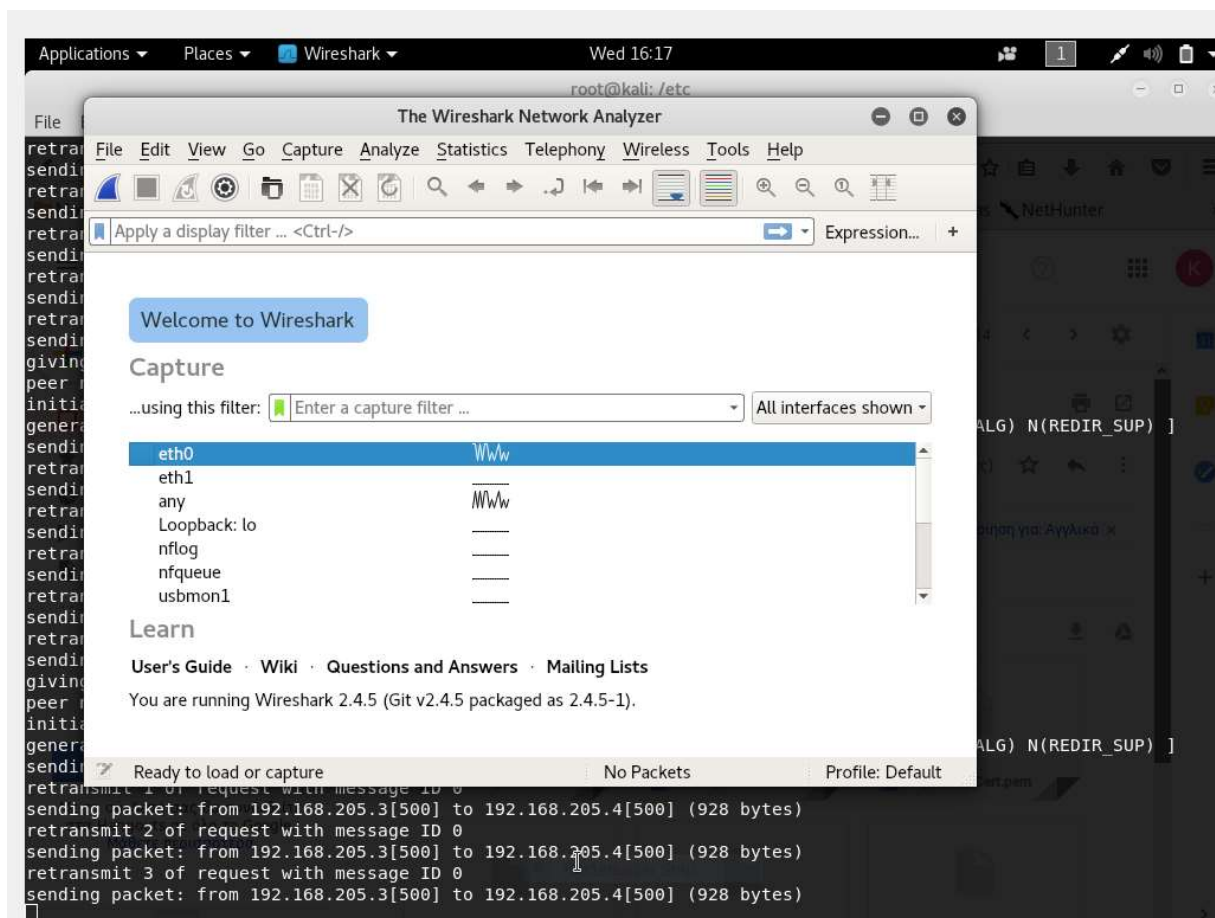
(II) Δημιουργία και δοκιμή συνδέσεων

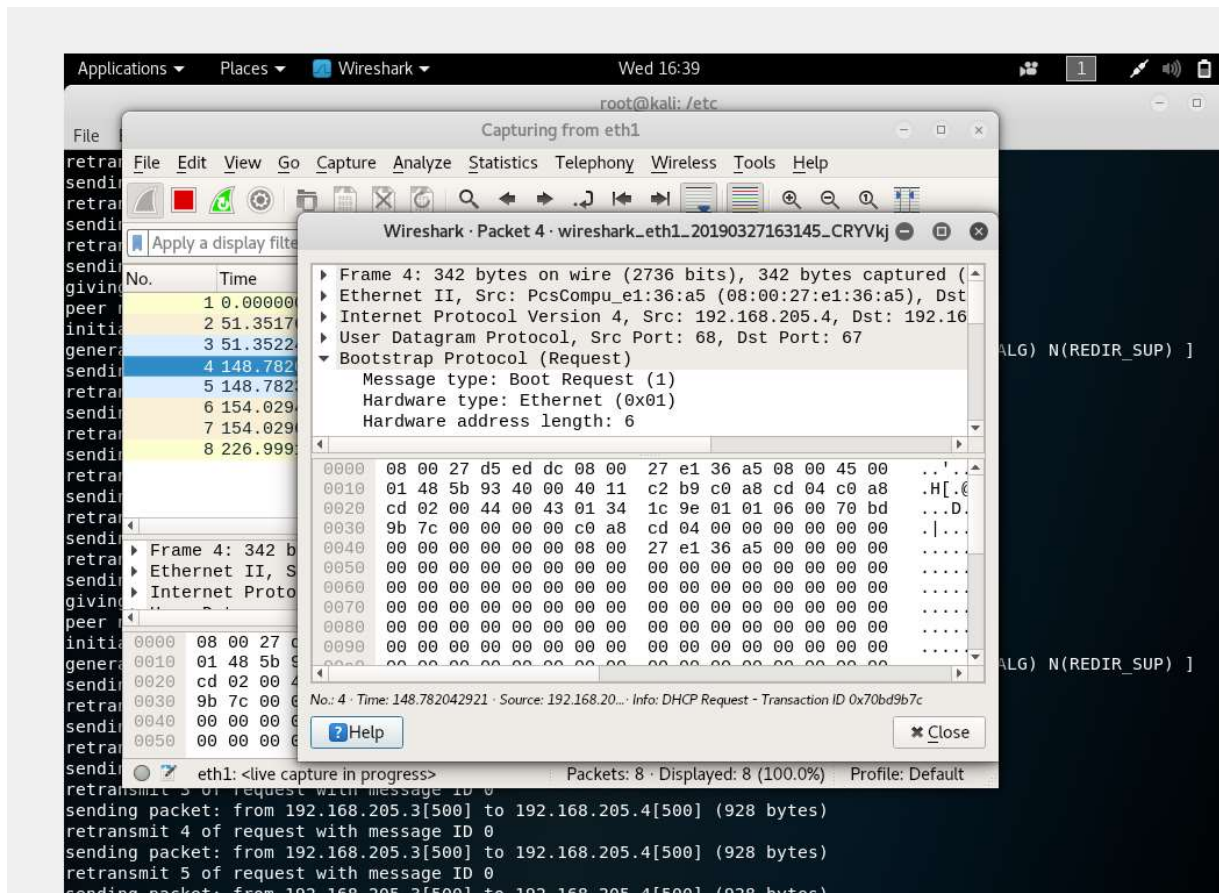
Δημιουργήστε και δοκιμάστε διαδοχικά τις παρακάτω συνδέσεις (connections) που περιγράφονται στα βήματα (Α)-(Β). Κάθε μία από τις παρακάτω συνδέσεις εκκινήστε την και επαληθεύστε με τη βοήθεια ενός packet snifer (πχ wireshark) τις αντίστοιχες συνδέσεις. Στο τελικό σας παραδοτέο να περιλαμβάνονται τα αρχεία `ipsec.conf` από τα δύο άκρα, με όλες τις παραπάνω συνδέσεις και οποιοδήποτε άλλο αρχείο πιθανώς απαιτείται.

Χρήσιμα παραδείγματα μπορείτε να βρείτε στα [2], [3]. (Α) Σύνδεση host-to-host (κόμβος-με-κόμβο) με IKE2 και με τη χρήση των παραπάνω πιστοποιητικών (όπως και το παράδειγμα του εργαστηρίου) (Β) Παραλλαγή του προηγούμενου παραδείγματος με χρήση AH και αλγόριθμο hash SHA256.



Ανοίγουμε το Wireshark.





Βλέπουμε την σύνδεση μας ότι είναι επιτυχημένη.