



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών,

Τομέας Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής

Ροή Δ, Μάθημα: *Ασφάλεια Δικτύων Υπολογιστών* (Εξάμηνο 8<sup>ο</sup>)

Τρίτη Εργαστηριακή Άσκηση : Φύλλο Απαντήσεων

**Συγκέντρωση πληροφοριών και ανίχνευση  
αδυναμιών σε δίκτυα υπολογιστών**

Όνοματεπώνυμο: ΜΙΧΑΛΗΣ ΠΑΠΑΔΟΠΟΥΛΛΟΣ
Αριθμός Μητρώου: 031 14702
Εξάμηνο: 8

```
C:\WINDOWS\system32\cmd.exe
Windows IP Configuration

    Host Name . . . . . : pc-b21
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : pclab.ece.ntua.gr

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix . : pclab.ece.ntua.gr
    Description . . . . . : Realtek PCIe GBE Family Controller
    Physical Address. . . . . : 78-45-C4-25-EB-25
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 147.102.38.121
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 147.102.38.200
    DHCP Server . . . . . : 147.102.38.11
    DNS Servers . . . . . : 147.102.222.210
    Lease Obtained. . . . . : Δευτέρα, 16 Απριλίου 2018 10:32:15 πμ
    Lease Expires . . . . . : Δευτέρα, 16 Απριλίου 2018 10:42:15 πμ
```

### Ερώτηση 3.1

[www.ethz.ch](http://www.ethz.ch)

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\labuser>nslookup www.ethz.ch
Server: achilles.noc.ntua.gr
Address: 147.102.222.210

Non-authoritative answer:
Name: www.ethz.ch
Address: 129.132.19.216

C:\Documents and Settings\labuser>
```

set type=A

IP Address: 129.132.19.216

DNS: dummy-ns.ethz.ch

Our DNS: [achilles.noc.ntua.gr] 147.102.222.210

```
C:\WINDOWS\system32\cmd.exe - nslookup

C:\Documents and Settings\labuser>nslookup
Default Server: achilles.noc.ntua.gr
Address: 147.102.222.210

> type=PTR
Server: achilles.noc.ntua.gr
Address: 147.102.222.210

*** achilles.noc.ntua.gr can't find type=PTR: Non-existent domain
> set type=PTR
> www.ethz.ch
Server: achilles.noc.ntua.gr
Address: 147.102.222.210

ethz.ch
      primary name server = dummy-ns.ethz.ch
      responsible mail addr = hostmaster.ethz.ch
      serial = 2010079554
      refresh = 10800 <3 hours>
      retry = 3600 <1 hour>
      expire = 1814400 <21 days>
      default TTL = 600 <10 mins>
>
```

MX:

set type=MX

### Ερώτηση 3.2

[www.mit.edu](http://www.mit.edu)

echo request type = 8, code =0

payload = 32bytes

61:62:63:64:65:66:67:68:69:6a:6b:6c:6d:6e:6f:70:71:72:73:74:75:76:77:61:62:63:64:  
65:66:67:68:69

### Ερώτηση 3.3

[www.princeton.edu](http://www.princeton.edu)

echo request type = 8, code =0

protocol = icmp

payload = 64 bytes όλα μηδενικά

απαντήσεις : echo reply type = 0, code =0

Ναι μπορεί να υλοποιηθεί μέσω TCP όπως και σε /Σ GNU/Linux

### Ερώτηση 3.4

[www.upatras.gr](http://www.upatras.gr)

Εργαλείο IP whois του RIPE: <https://apps.db.ripe.net/search/query.html>

Subnet: 150.140.128.0 – 150.140.255.255

Address: 26504 Campus Rio, Patras, Greece

organisation: [ORG-UOP8-RIPE](#)

AS: 5408

https://apps.db.ripe.net/db-web-ui/#/query?bflag&searchtext=150.140.129.201&source=RIPE#resultsSection	
NO abuse contact found	
<input checked="" type="checkbox"/> Highlight RIPE NCC managed values	
inetnum:	150.140.128.0 - 150.140.255.255
netname:	UPnet
descr:	Patras, Greece
country:	GR
org:	ORG-UOP8-RIPE
admin-c:	UPS-RIPE
tech-c:	UPS-RIPE
status:	LEGACY
mnt-by:	RIPE-NCC-LEGACY-MNT
mnt-by:	UPnet-MNT1
mnt-routes:	UPnet-MNT1
created:	2006-08-02T11:32:40Z
last-modified:	2016-04-14T09:39:51Z
source:	RIPE
sponsoring-org:	ORG-GRaT1-RIPE

<input checked="" type="checkbox"/> Highlight RIPE NCC managed values	
organisation:	ORG-UOP8-RIPE
org-name:	University of Patras
org-type:	OTHER
address:	Campus Rio
address:	26504
address:	Greece
e-mail:	noc@upatras.gr
admin-c:	UPS-RIPE
mnt-by:	GRNET-NOC
mnt-ref:	GRNET-NOC
mnt-ref:	UPnet-MNT1
mnt-by:	UPnet-MNT1
created:	2015-09-24T09:38:02Z
last-modified:	2017-10-30T16:42:50Z
source:	RIPE

### Ερώτηση 3.5

nic.grnet.gr

Εργαλείο looking glass της Hurricane Electric: <https://lg.he.net/>

### Ερώτηση 3.6

Εργαλείο Visual Traceroute: <http://en.dnstools.ch/visual-traceroute.html>

### Ερώτηση 3.7

[www.ntua.gr](http://www.ntua.gr)

### Ερώτηση 3.8

```

11:06:49.097467 ARP, Request who-has 10.10.10.3 tell 10.10.10.4, length 28
0x0000: 0001 0800 0604 0001 0800 2710 d751 0a0a .....Q..
0x0010: 0a04 0000 0000 0000 0a0a 0a03 .....
11:06:49.100620 ARP, Request who-has 10.10.10.3 tell 10.10.10.3, length 46
0x0000: 0001 0800 0604 0001 0800 27d4 163c 0a0a .....<..
0x0010: 0a03 0000 0000 0000 0a0a 0a03 0000 0000 .....
0x0020: 0000 0000 0000 0000 0000 0000 0000 .....
11:06:49.100620 IP 10.10.10.4.32912 > 10.10.10.3.33447: UDP, length 32
0x0000: 4500 003c 9061 0000 0511 fd35 0a0a 0a04 E..<.a.....5....
0x0010: 0a0a 0a03 8090 82a7 0028 2854 4041 4243 .....((T@ABC
0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS
0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^_
11:06:49.100620 IP 10.10.10.4.60616 > 10.10.10.3.33448: UDP, length 32
0x0000: 4500 003c 9062 0000 0511 fd34 0a0a 0a04 E..<.b.....4....
0x0010: 0a0a 0a03 ecc8 82a8 0028 2854 4041 4243 .....((T@ABC
0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS
0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^_
11:06:49.100620 IP 10.10.10.4.57737 > 10.10.10.3.33449: UDP, length 32
0x0000: 4500 003c 9063 0000 0611 fc33 0a0a 0a04 E..<.c.....3....
0x0010: 0a0a 0a03 e189 82a9 0028 2854 4041 4243 .....((T@ABC
0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS
0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^_
11:06:49.100620 ARP, Reply 10.10.10.3 is-at 08:00:27:d4:16:3c (oui Unknown), length 46
"PAPADOPOULLOS_MICHALIS.txt" 62 lines, 4327 characters

```

Παρατηρούμε ότι χρησιμοποιεί UDP για την αποστολή των πακέτων.

32 byte payload

A..Z

Διαφορά με Windows: Χρήση UDP και το περιεχόμενο του payload στα Windows είναι σε HEX το ακόλουθο:

61:62:63:64:65:66:67:68:69:6a:6b:6c:6d:6e:6f:70:71:72:73:74:75:76:77:61:62:63:64:65:66:67:68:69

### Ερώτηση 3.9

Unable to connect to remote host : connection refused

ότι η υπηρεσία είναι κλειστή.

Γνωρίζουμε ότι τρέχει server Lighthttp v1.4.35

connection close

Bad request 400.

```

GET / HTTP/1.1

HTTP/1.1 400 Bad Request
Content-Type: text/html
Content-Length: 349
Connection: close
Date: Mon, 16 Apr 2018 08:11:03 GMT
Server: lighthttpd/1.4.35

<?xml version="1.0" encoding="iso-8859-1"?>
<!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" xml:lang="en" lang="en">
  <head>
    <title>400 - Bad Request</title>
  </head>
  <body>
    <h1>400 - Bad Request</h1>
  </body>
</html>
Connection closed by foreign host.
root@debian:~# telnet 10.10.10.2
Trying 10.10.10.2...
telnet: Unable to connect to remote host: Connection refused
root@debian:~# U_

```

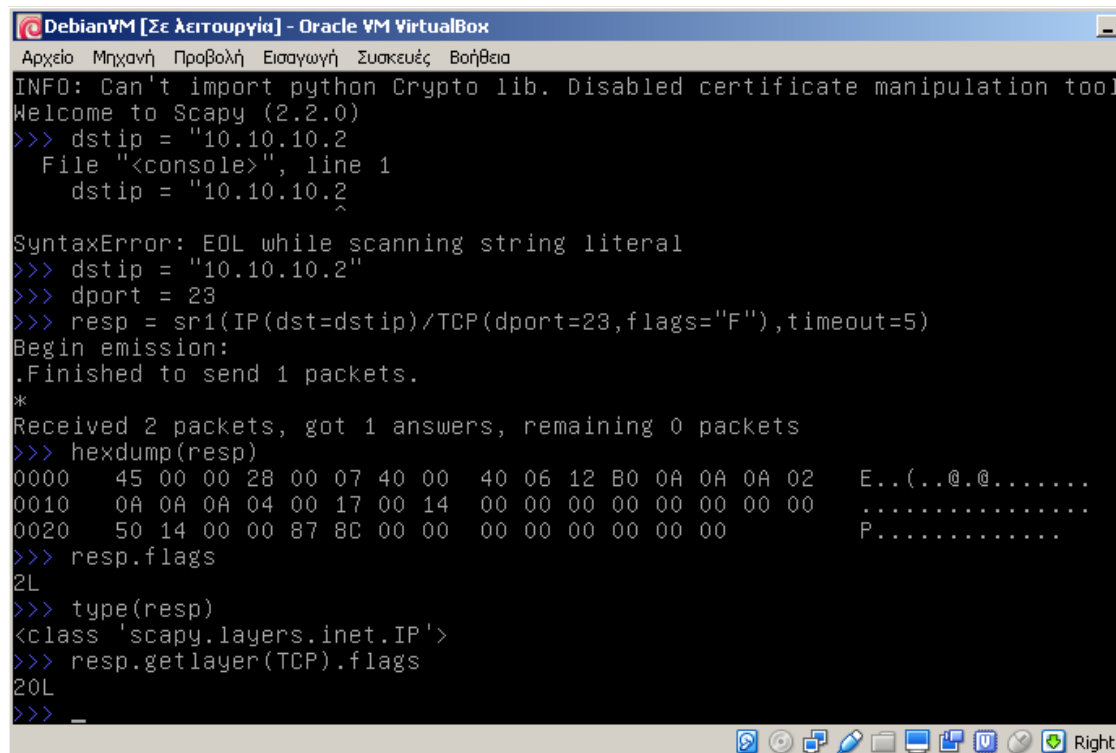
### Ερώτηση 3.10

### Ερώτηση 3.11

10.10.10.2

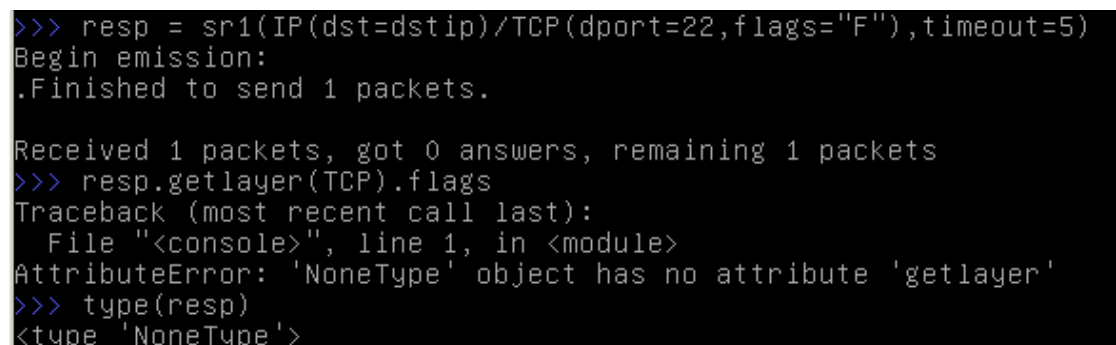
### Ερώτηση 3.12

Ζητούμενη τεχνική scan: FIN



```
DebianVM [Σε λειτουργία] - Oracle VM VirtualBox
Αρχείο Μηχανή Προβολή Εισαγωγή Συσκευές Βοήθεια
INFO: Can't import python Crypto lib. Disabled certificate manipulation tool
Welcome to Scapy (2.2.0)
>>> dstip = "10.10.10.2"
      File "<console>", line 1
        dstip = "10.10.10.2"
                                     ^
SyntaxError: EOL while scanning string literal
>>> dstip = "10.10.10.2"
>>> dport = 23
>>> resp = sr1(IP(dst=dstip)/TCP(dport=23,flags="F"),timeout=5)
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
>>> hexdump(resp)
0000  45 00 00 28 00 07 40 00  40 06 12 B0 0A 0A 0A 02  E..(..@.@.....
0010  0A 0A 0A 04 00 17 00 14  00 00 00 00 00 00 00 00  .....
0020  50 14 00 00 87 8C 00 00  00 00 00 00 00 00 00 00  P.....
>>> resp.flags
2L
>>> type(resp)
<class 'scapy.layers.inet.IP'>
>>> resp.getlayer(TCP).flags
20L
>>> _
```

TCP PORT 23 IS CLOSED



```
>>> resp = sr1(IP(dst=dstip)/TCP(dport=22,flags="F"),timeout=5)
Begin emission:
.Finished to send 1 packets.

Received 1 packets, got 0 answers, remaining 1 packets
>>> resp.getlayer(TCP).flags
Traceback (most recent call last):
  File "<console>", line 1, in <module>
AttributeError: 'NoneType' object has no attribute 'getlayer'
>>> type(resp)
<type 'NoneType'>
```

TCP PORT 22 IS OPEN|FILTERED

### Ερώτηση 3.13

52000 – 53999

### Ερώτηση 3.14

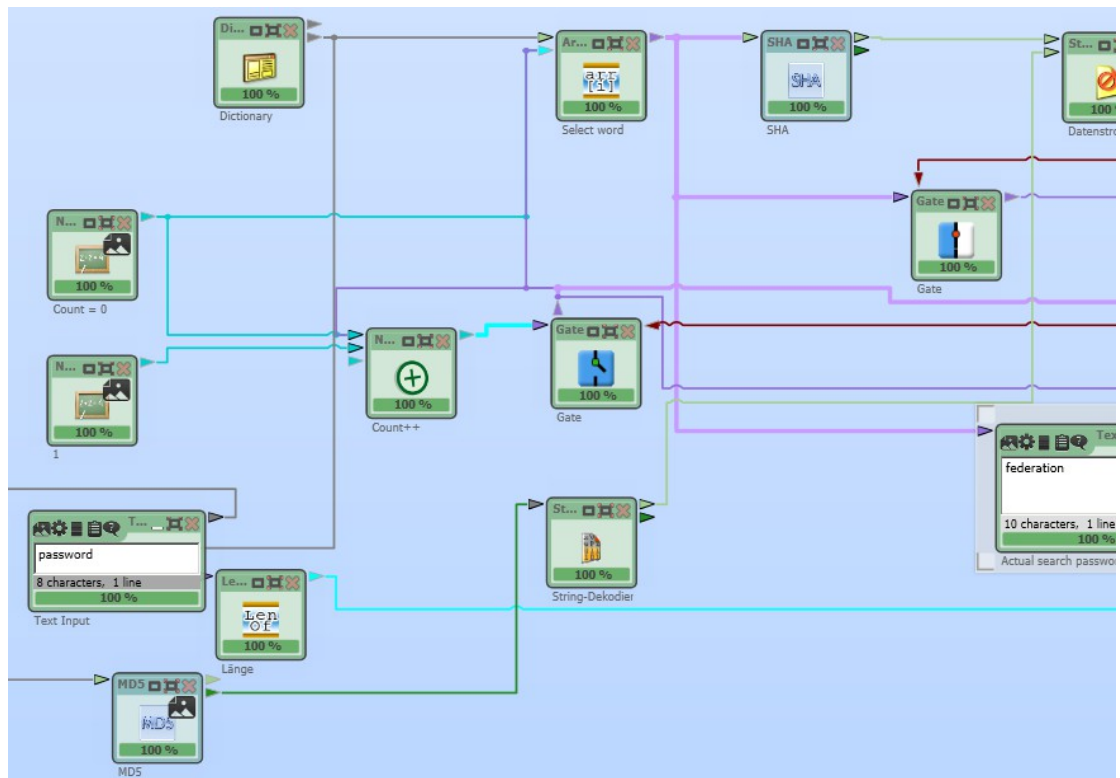
10.10.10.3

### Ερώτηση 3.15

Username: user

Password Hash: 5F 4D CC 3B 5A A7 65 D6 1D 83 27 DE B8 82 CF 99

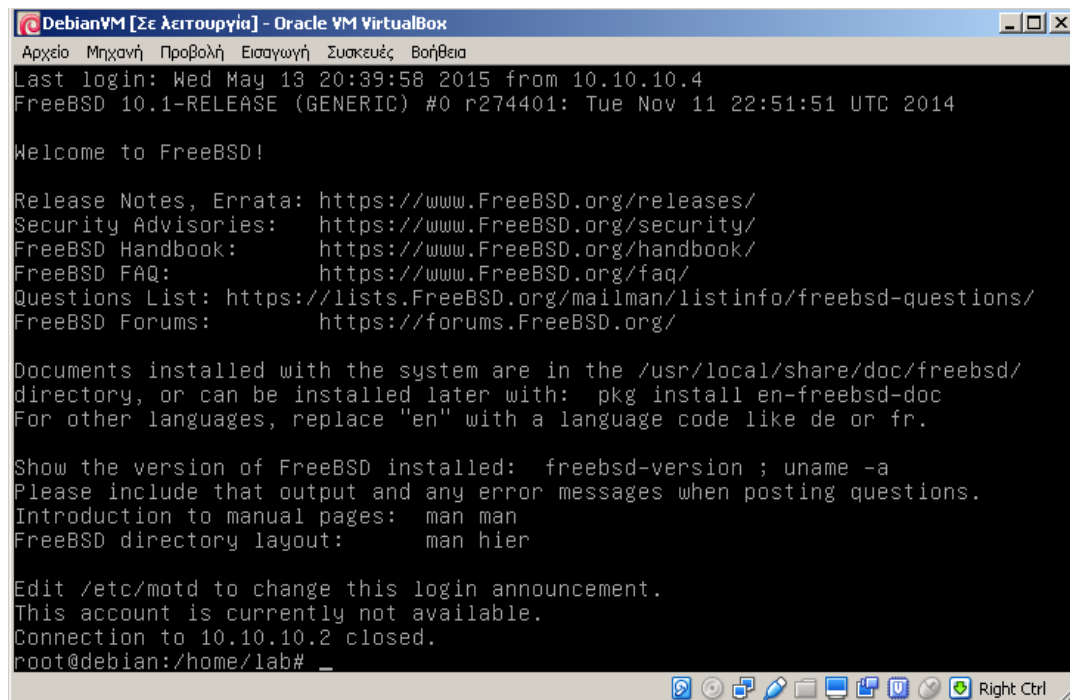
Dictionary Attack (CrypTool - Running)



Cracked Hash: **password**

### Ερώτηση 3.16

ssh user@10.10.10.2



```
DebianVM [Σε λειτουργία] - Oracle VM VirtualBox
Αρχείο Μηχανή Προβολή Εισαγωγή Συσκευές Βοήθεια
Last login: Wed May 13 20:39:58 2015 from 10.10.10.4
FreeBSD 10.1-RELEASE (GENERIC) #0 r274401: Tue Nov 11 22:51:51 UTC 2014

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:  https://www.FreeBSD.org/security/
FreeBSD Handbook:    https://www.FreeBSD.org/handbook/
FreeBSD FAQ:         https://www.FreeBSD.org/faq/
Questions List: https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums:      https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

Edit /etc/motd to change this login announcement.
This account is currently not available.
Connection to 10.10.10.2 closed.
root@debian:/home/lab# _
```

### FTP:

```
root@debian:/home/lab# ftp user@10.10.10.2
ftp: user@10.10.10.2: Name or service not known
ftp> root@debian:/home/lab# ^C
root@debian:/home/lab# ftp 10.10.10.2
Connected to 10.10.10.2.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 15 allowed.
220-Local time is now 12:15. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 15 minutes of inactivity.
Name (10.10.10.2:root): user
331 User user OK. Password required
Password:
230 OK. Current directory is /
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

### HTTP/HTTPS:

```
root@debian:/home/lab# telnet 10.10.10.2 80
Trying 10.10.10.2...
Connected to 10.10.10.2.
Escape character is '^]'.
^]
telnet> Connection closed.
root@debian:/home/lab# telnet 10.10.10.2 443
Trying 10.10.10.2...
Connected to 10.10.10.2.
Escape character is '^]'.
^]
```



### NMAP PORTSCAN:

```
root@debian:/home/lab# nmap -Pn 10.10.10.2

Starting Nmap 6.47 ( http://nmap.org ) at 2018-04-16 12:16 EEST
Nmap scan report for 10.10.10.2
Host is up (0.0015s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: 08:00:27:0F:36:25 (Cadmus Computer Systems)
```

### Ερώτηση 3.17

greg

### Ερώτηση 3.18

### Ερώτηση 3.19

### Ερώτηση 3.20

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,AAFE3EABF8514113

YY8iBtaW0RT407NoG0hKiZpccuc7MvA2/I4SpRQjgN6w+F9Rm0SJcLbobqndjI/H
p36W0IfXck5hT4VZqkcIn2iiuUCZbm1UnRGw4QS9T1tmqno4AJeXaDf4CIUEFXpP
Gid8QEhAqNLPWuIQG02UmGQM4lTXZHpPA4jsuj1vScbD/pM99TEPDHfhJ2BuMASu
tYT8x0WaxRafS+zD/GD6FLmDUoh7zo0nuC9Fw8v11ddqV/g2A0y0RYsxsSMjjvG+i
hmLgqGxWWUKYIDM2i/jtCmNs6CQK8vg1ne1A1J2hYMUUpFnKYvFMvb9v0E8C0ih70
b1PF2NR6T2hhSbWDIKdkMeCHdzA3XP/iYeww3J1qzjEdX3z0d7GKXj11XqSR50jQ
Nuiiv4D33FN9Kk7p8WvN8PCPrVbTJI2vXY8tJuvZm8AhLCYyCMzKehezdvQJsfo/a
P40Y0IJsnnHLuJM1KMAZsIIkAJFU7b8kYhJbJDh9St1TM0L7dtNQiJro1rr9Xuts
YKn65qrTKoocN5NGeY4+KXNJc7q6ZbGvda/FVsU8JCp0y47Po14cs48znCZdNXT
73+BD0bDdG+QioN/YQss+HsIOJ0xD7ftswiDGu+trGB36Ayhd/Ocd+EiMzo3dKWb
4X2L3KM4+3Jc2uJDtwpz3mE5ejH3/GXfkrMdoqI4pai8+Fw3PcgjEGAYSrT5LKwF
pLKuPivSx/F0cA42IHAioHirn7g92OG719IjDagDV0Vd5SN+C57/jZ3rL55HDSya
FfmLmkt/4LuIs4uC1VvisaaH8hoaSvkU3o0URdPGdKg+vUjRpgt7XzAERxhGfXl1
PXXdMYRqR8prbDWzCsESLD2fCcZCHdhsUYt3Wb2G8jjVLH0NGTnoT9g6h0hi5idl
/6XuXhXT43pU59jhp8mlQtC09S0BdBCCYdIhbmWCf5ATH1JG2Sroer9pnt6/9D9E
FKq0qzF6njgI+R0nbew+x74faFlnEW+Gatc9Z88u6Jm8Jb9PQVzPviZPRzLsCPKj
kDRZBEtZt+Cm/dxcZlD3xQCSxZ2bAl17eJC/LVUcpEFw7JNEUCQCDDAKI4kkXvwg
WcVRnqLMYF0uT3x2I7NevB2xXjy0mBN5knMfwYaRjU7ycbeSdQAPIVjYL9kgDeBq
yt1S6G0gDGBsr3fqA2mPjs+nm1n2asb64afqeS5oM0Bxetk/TADxv/JAA36QUvom
iWPFgpmh/CMgdmH2grPCU7kSGG700+i05uoz+fIs64fDCRqQ4Vd1YRIwHn1/PJUC
keuset_03114702.pem_
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAOzj1Nk6rqo8KPSHM00kvkLmjKFyWF/rYPTZ/1s8an9N5/6XE
CkQG3e5n1BqW3+ZT+mamcBSPFz6S41YGe4xkusZHq0NBmmuCnf9wIrzCsGF6U6gY
C2CPhy2y6wWhqfwYABL+ykk9CLOxsFhEdLbJFZYA14h92uK4Veh1KRTexBickHib
dnLxz9qffHCuMz4QEoo6p3MAuc300cDndUnP+ImNN1NmwipiLWB+cXdtPzfTxEvG
5WwkuW75HrpKftI1Kp158frr2Fr2bPcKYfm9pPP1oWqK8eWbd0GMSxR+R13MB+2a
VG/Q7V5wq46Xe0IxZXBuBr3hDRz22e+ChnsSqwIDAQABAoIBABJyuxgPLvcqnX5P
wWKKHG1xsmliVfZaCljhidi/wzsZ+1fz6IXE0F9VyaSchW2Qa3eLU7FyFrym8kV+r
W82WqYWXNS1EKoquMS5TjRu7mNWG7gQ4fkEgIekQmLvmNgR+vCn1ftN0KhyFBqn8
S55WCKIWA984UKW5f5ghQBSiegJuaxhRhjL1mxfuSQLLqFF3h6iaw7gMEWptkM9h
zBtZvMhSoNgG/E7KHK/H/rJ8wmrQZv2oZ0d8yy5kLoTd3Isu2uJXY3C7j2v2aTvJ
QXiADuinoqs9J8noD0XkYUFhGVhptDHLGjajSAJtGwwR4be7nNXJoMJfT1G12WYP
RJzg9uECgYEA/aFiIw6Y1o7vmEt142Ho80Hr7n/8xRMSfNxV2BsKRvWds50u9G4m
1TiSsNP9K0VXAv6z2nstlpQuPbEhc+XJaeZsQod32j+yfpNR2vpt4U/7Br411JAS
rCwX0gCSIrMIFhMs0NluwPnvttvfNZCM2LpkgNyhGfEiPEnUFVXMrZcCgYEA1TI1
Yo8J9XAVvfM9msCx4Zhr45WJS18h2xULyUIIm7Qn95MxCzRrgzYSB9L94nb6rLi+
HFIrXV8QkYUD7w9PuSTydXzN1qpjyMSxvhI1BZ/+oCU58aN8S9/XS3nPsqFUygPQ
aGEtI2XR8nf8DIDqBVw44ENfvf9RfJ4VTYoDg0CgYEAmc6HU9kjSGIP3BxFInoa
qBFpYQ30fLiPKpb3nADx34w9n0X/YA14kS8ojgFQczAuJwtkQc6LG9iqnhDPx5fe
59CrcED0pq6gEPBhmhpeDhfR1Ao/XLMuD6kBnQFpnY9S2Qi1ldagt60roux1dPc+
4qN0FXM2YyP+7e6bpYCNiesCgYEAxIigvBW+iXrVIDcwrnwBu0thPDSzpzwiYzjy
9i7+m4LdoTYYbQra3a93uazAjQc/mQAJiVQas60q0evUL4n+5V9w/+uYWX7j0823
SM+zP1c5xGns25vpVoy4DQTy+eoNntkbQ03p698QFqSTPvct50I0uhVa2qRD4Dpg
wbTWAfUCgYEAstncAtc/AWqPBkYYowTUZeJgGJrfMiKAQaP6XuzkxBsLtQc27IML
-----
```

Συμμετρική κρυπτογράφηση 3DES χρησιμοποιείται για κρυπτογραφία ζευγούς κλειδιών ασυμμετρης κρυπτογράφησης επειδη είναι ασφαλεις για ιδανικα keylength και λογω ταχυτητας αποκρυπτογράφησης

The `-des3` option [specifies how the private key is encrypted](#) with a password. Without a cipher option, the private key is not encrypted, and no password is required.

Password encryption can protect the private key even when file-system-based access control is circumvented.

## Ερώτηση 3.21

```
DebianVM [Σε λειτουργία] - Oracle VM VirtualBox
Αρχείο Μηχανή Προβολή Εισαγωγή Συσκευές Βοήθεια
Private-Key: (2048 bit)
modulus:
  00:d3:38:f5:36:4e:ab:aa:8f:0a:3d:21:cc:38:e9:
  2f:90:b9:a3:90:5c:96:17:fa:d8:3d:36:7f:d6:cf:
  1a:9f:d3:79:ff:a5:c4:0a:44:06:dd:ee:67:d4:1a:
  96:df:e6:53:fa:66:a6:70:14:8f:17:3e:92:e2:56:
  06:7b:8c:64:ba:cc:c7:ab:43:41:9a:6b:82:9d:ff:
  70:22:bc:c2:b0:61:7a:53:a8:18:0b:60:8f:87:2d:
  b2:eb:05:a1:a9:fc:18:00:12:fe:ca:49:3d:08:ba:
  31:b0:58:44:74:b6:c9:15:96:00:97:88:7d:da:e2:
  b8:55:e8:65:29:14:de:c4:18:9c:90:78:9b:76:72:
  f1:cf:da:9f:7c:70:ae:33:3e:10:12:8a:3a:a7:73:
  00:b9:cd:f4:39:c0:e7:75:49:cf:f8:89:8d:37:53:
  66:c2:2a:62:2d:60:7e:71:77:6d:3f:37:d3:c4:4b:
  e0:e5:65:a4:b9:6e:f9:1e:ba:4a:7e:d2:35:2a:99:
  79:f1:fa:eb:64:5a:d9:6c:f7:0a:61:f9:bd:a4:f3:
  e5:a1:6a:8a:f1:e5:9b:77:41:8c:4b:14:7e:46:5d:
  cc:07:ed:9a:54:6f:d0:ed:5e:70:ab:8e:97:78:e2:
  31:cd:70:6e:06:bd:e1:0d:1c:f6:d9:ef:82:86:7b:
  12:ab
publicExponent: 65537 (0x10001)
privateExponent:
  12:72:bb:18:0f:2e:f7:2a:9f:1e:4f:c1:62:87:1b:
  5c:6c:9a:58:95:7d:96:82:96:38:62:76:2f:f0:ce:
  :_

c6:7e:d5:fc:fa:21:71:34:17:d5:72:69:27:21:5b:
64:1a:dd:e2:d4:ec:5c:85:af:29:bc:91:5f:ab:5b:
cd:96:a9:85:97:35:29:44:2a:8a:ae:31:2e:53:8d:
1b:bb:98:d5:86:ee:04:38:7e:41:20:21:e9:10:98:
bb:e6:36:04:7e:bc:29:e5:7e:d3:74:2a:1c:85:06:
a9:fc:4b:9e:56:08:a2:16:03:df:38:50:a5:b9:7f:
98:21:40:14:a2:7a:02:6e:6b:18:51:86:32:f5:9b:
17:ee:49:02:cb:a8:51:77:87:a8:9a:c3:b8:0c:11:
6a:6d:90:cf:61:cc:1b:59:bc:c8:52:a0:d8:06:fc:
4e:ca:1c:af:c7:fe:b2:7c:c2:6a:d0:66:fd:a8:64:
e7:7c:cb:2e:64:2e:84:dd:dc:8b:2e:da:e2:57:63:
70:bb:8f:6b:f6:69:3b:e3:41:78:80:0e:e8:a7:a2:
ab:3d:27:c9:e8:0f:45:e4:61:41:61:19:58:69:b4:
31:cb:1a:36:a3:48:02:6d:1b:0c:11:e1:b7:bb:9c:
d5:c9:a0:c2:5f:4f:51:b5:65:66:0f:44:9c:e0:f6:
e1
prime1:
  00:fd:a1:62:23:0e:98:d6:8e:ef:98:4b:65:e3:61:
  e8:f0:e1:eb:ee:7f:fc:c5:13:12:7c:dc:55:d8:1b:
  0a:46:f5:83:b3:93:ae:f4:6e:26:d5:38:92:b0:d3:
  fd:2b:45:57:02:fe:b3:66:7b:2d:96:94:2e:3d:b1:
  21:73:e5:c9:69:e6:6c:42:87:77:da:3f:b2:7e:93:
  51:66:fa:6d:e1:4f:fb:06:be:35:d4:90:12:ac:2c:
  17:d2:00:92:22:b3:08:16:13:2c:38:d9:6e:c0:f9:
  :_
```

```

ef:b6:db:df:35:90:8c:d8:ba:64:80:dc:a1:19:f1:
22:3c:49:d4:15:55:cc:ad:97
prime2:
00:d5:32:25:62:8f:09:f5:70:15:bd:f9:8d:f6:6b:
02:c7:86:61:47:8e:56:25:2d:7c:87:6c:54:2f:25:
08:9b:b4:27:f7:93:31:0b:34:6b:83:36:12:07:d2:
fd:e2:76:fa:ac:b8:be:1c:52:2b:c5:5f:10:91:85:
03:ef:0f:4f:b9:24:f2:75:7c:cd:d6:aa:63:c8:c4:
b1:be:12:25:05:9f:fe:a0:25:39:f1:a3:7c:4b:df:
d7:4b:79:cf:b2:a1:54:ca:03:d0:68:61:2d:21:95:
d1:f2:77:fc:0c:80:83:a8:15:70:e3:81:0d:7e:f7:
fd:45:f2:78:55:36:28:0e:0d
exponent1:
00:99:ce:87:53:d9:23:48:62:0f:dc:1c:45:22:7a:
1a:a8:11:69:61:0d:ce:7c:b8:8f:2a:96:f7:9c:00:
f1:df:8c:3d:9c:e5:ff:60:0d:78:91:2f:28:8e:01:
50:73:30:2e:8f:0b:64:41:ce:8b:1b:d8:aa:9e:10:
cf:c7:97:de:e7:d0:ab:70:40:f4:a6:ae:a0:10:f0:
47:9a:1a:5e:0e:17:d1:94:0a:3f:5c:b3:2e:0f:a9:
01:9d:01:69:9d:8f:52:65:08:a5:75:a8:2d:e8:ea:
e8:ba:cc:65:74:f7:3e:e2:a3:4e:15:73:36:63:23:
fe:ed:ee:9b:a5:80:8d:89:eb
exponent2:
00:c4:88:a0:bc:15:be:89:7a:d5:20:37:30:ae:6c:
:

```

```

47:9a:1a:5e:0e:17:d1:94:0a:3f:5c:b3:2e:0f:a9:
01:9d:01:69:9d:8f:52:65:08:a5:75:a8:2d:e8:ea:
e8:ba:cc:65:74:f7:3e:e2:a3:4e:15:73:36:63:23:
fe:ed:ee:9b:a5:80:8d:89:eb
exponent2:
00:c4:88:a0:bc:15:be:89:7a:d5:20:37:30:ae:6c:
01:b8:eb:61:3c:34:b3:a7:3c:22:63:38:f2:f6:2e:
fe:9b:82:dd:a1:36:18:6d:0a:da:dd:af:77:b9:ac:
c0:8d:07:3f:99:00:09:89:54:1a:b3:ad:2a:39:eb:
d4:2f:89:fe:e5:5f:70:ff:eb:98:59:7e:e3:d3:cd:
b7:48:cf:b3:3f:57:39:c4:69:ec:db:9b:e9:56:8c:
b8:0d:04:f2:f9:ea:0d:9e:d9:1b:43:4d:e9:eb:df:
10:16:a4:93:3e:f7:2d:e7:42:34:ba:15:5a:da:a4:
43:e0:3a:60:c1:b4:d6:01:f5
coefficient:
00:b2:d9:dc:02:d7:3f:01:6a:8f:06:46:18:a3:04:
d4:65:e8:e0:18:9a:df:32:22:80:41:a3:fa:5e:ec:
e4:c4:1b:0b:b5:07:36:ec:83:0b:9b:cd:51:b1:29:
ee:7c:b0:48:6c:ef:49:10:7e:e2:95:30:10:b1:3d:
67:91:79:dd:2b:07:0e:6c:2b:28:43:0a:98:68:74:
5d:fc:df:44:d3:b8:d2:6d:ff:31:16:e6:bc:c6:6d:
6f:1a:9e:75:94:5c:d0:53:ff:77:52:42:26:ac:96:
07:f6:7d:48:77:b2:9e:b6:8f:04:2d:d0:a4:50:2e:
0a:d3:94:80:44:9a:53:fe:ce
(END)

```

```

root@debian:/home/lab# openssl rsa -in keyset_03114702.pem -pubout
Enter pass phrase for keyset_03114702.pem:
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0zj1Nk6rqo8KPSHM00kv
kLmjKfYwF/rYPTZ/1s8an9N5/6XEckQG3e5n1BqW3+ZT+mamcBSPFz6S41YGe4xk
uszHq0NBmmuCnf9wIrzCsGF6U6gYC2CPhy2y6wWhqfwYABL+ykk9CLoxsFhEdLbJ
FZYA14h92uK4Veh1KRtExBickHibdnLxz9qffHCuMz4QEoo6p3MAuc300cDndUnP
+ImNN1NmwiPiLWB+cXdtPzfTxEv95WwKuW75HrpKftI1Kp158frr2Fr2bPcKYfm9
pPPloWqK8eWbd0GMSxR+R13MB+2aVG/Q7V5wq46Xe0IxzXBuBr3hDRz22e+ChnsS
qwIDAQAB
-----END PUBLIC KEY-----

```

n	
e	
d	
p	
q	

(Εάν στον παραπάνω πίνακα δεν μπορείτε εύκολα να κάνετε copy-paste τα ζητούμενα, παραθέστε το σχετικό screenshot.)

### Ερώτηση 3.22

### Ερώτηση 3.23