

# Ασφάλεια συστημάτων υπολογιστών

## Εργασία εργαστηρίου 5

### Σάββας Λιάπης 57403

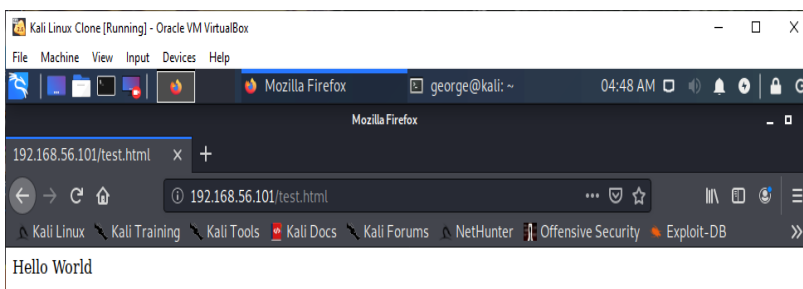
#### Άσκηση 1

Σε ένα web directory πολλές φορές μπορεί να έχουμε αρχεία τα οποία δεν πρέπει να είναι προσπελάσιμα από το κοινό. Ένας τρόπος για να το καταφέρουμε αυτό είναι να ρυθμίσουμε κατάλληλα τα permissions των αρχείων αυτών. Για παράδειγμα μπορούμε να αφαιρέσουμε το δικαίωμα της ανάγνωσης ενός αρχείου. Η εντολή για να το κάνουμε αυτό είναι η εξής:

**sudo chmod -r foo.txt** (όπου foo.txt το όνομα του αρχείου)

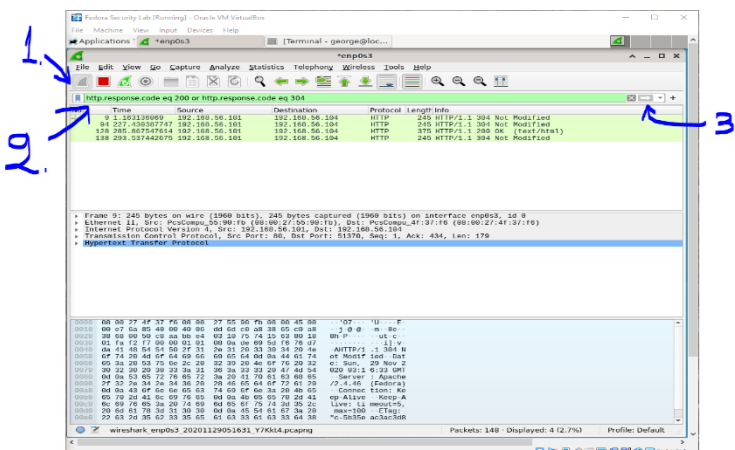
Αν κάποιος επιχειρήσει να προσπελάσει ένα τέτοιο αρχείο π.χ. μέσω ενός web browser, ποιο HTTP status code θα λάβει; (συμβουλευτείτε το link με τα response codes της προηγούμενης εργαστηριακής άσκησης)

Στο default web directory του web server που έχουμε εγκαταστήσει στο Fedora να δημιουργήσετε μια απλή html σελίδα, έστω την test.html που να περιέχει ένα οποιοδήποτε περιεχόμενο, έστω το μήνυμα Hello World. Δοκιμάστε να προσπελάσετε την σελίδα αυτή από τον web browser του Kali Linux. Το αποτέλεσμα θα πρέπει να είναι κάπως έτσι:



Στη συνέχεια να αφαιρέσετε το δικαίωμα ανάγνωσης του παραπάνω αρχείου και να δοκιμάσετε να το προσπελάσετε από το τον web browser του Kali Linux. Να επισυνάψετε ένα screenshot με το αποτέλεσμα.

Εάν στα logs ενός web server δούμε πολύ μεγάλο αριθμό προσπαθειών για πρόσβαση σε ένα αρχείο στο οποίο η πρόσβαση δεν επιτρέπεται θα μπορούσαμε να υποθέσουμε ότι οι προσπάθειες αυτές είναι κακόβουλες (πχ brute force attack ή DoS attack). Πέρα από την παρακολούθηση των logs του web server, θα μπορούσαμε να παρακολουθήσουμε τέτοιες κινήσεις με τη βοήθεια του λογισμικού Wireshark.



Στο λογισμικό Wireshark με τη βοήθεια των φίλτρων μπορούμε να φιλτράρουμε μόνο την κίνηση που μας ενδιαφέρει. Για παράδειγμα αν θέλουμε να παρακολουθήσουμε την κίνηση μόνο σε σελίδες που απαντούν με τον κωδικό επιτυχίας (200) τότε ένα φίλτρο που θα μπορούσαμε να εφαρμόσουμε είναι το εξής:

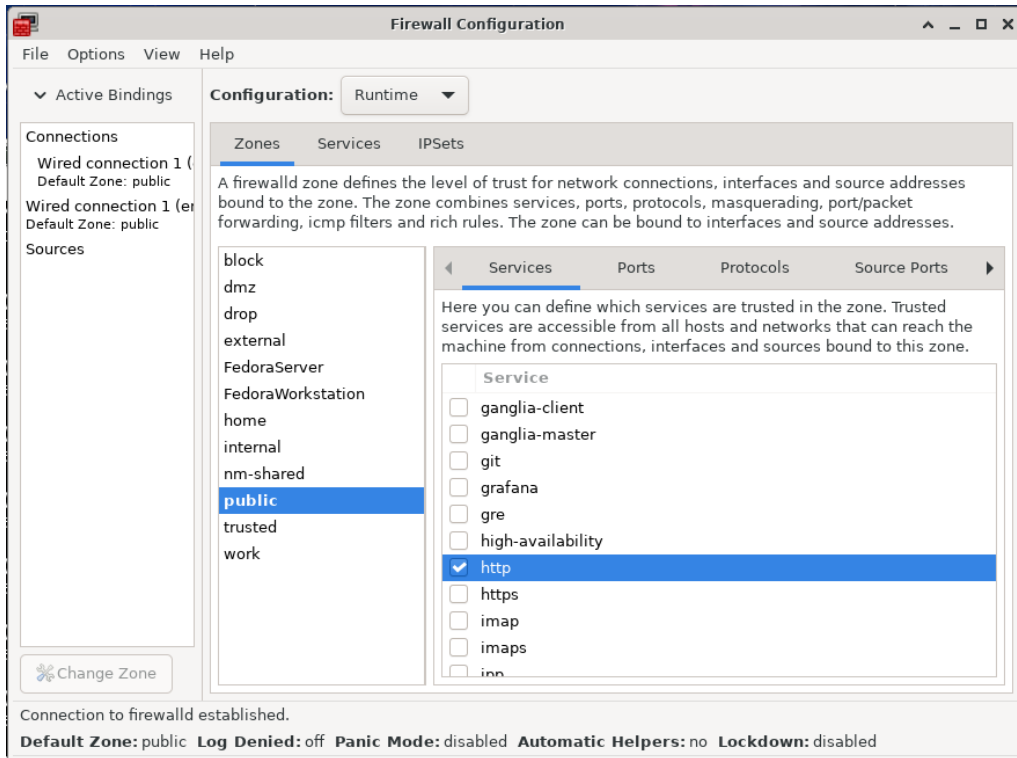
http.response.code eq 200 or http.response.code eq 304

Τα βήματα που χρειάζεται να κάνουμε είναι τα εξής (αφού πρώτα τρέξουμε το πρόγραμμα με την εντολή “sudo wireshark”):

Να εφαρμόσετε ένα φίλτρο που να «πιάνει» τις προσπάθειες προσπέλασης σε σελίδες που δεν επιτρέπεται η προσπέλασή τους και να το δοκιμάσετε προσπαθώντας να προσπελάσετε την σελίδα που δημιουργήσατε προηγουμένως. Να επισυνάψετε ένα screenshot με το αποτέλεσμα.

### Απάντηση 1 :

- πηγαίνουμε στον φάκελο html με την εντολή : **cd /var/www/html**
- δημιουργώ το αρχείο **nano test.html** και γράφω μέσα savvas (και το σώζω με ctrl+o ctrl+x)
- τρέχω την εντολή **sudo firewall-config** και μαρκάρω το http



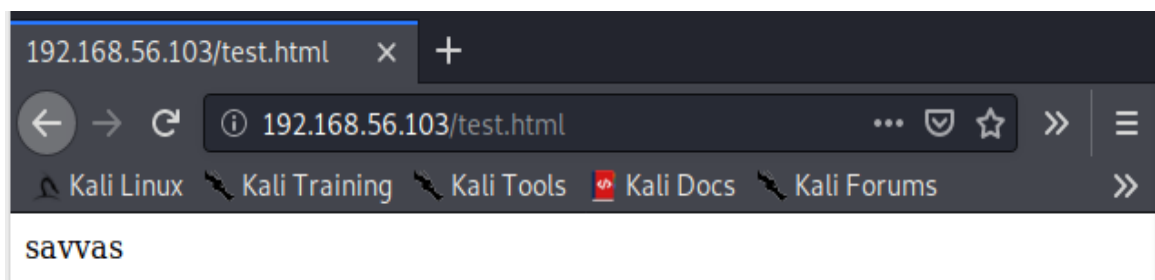
- βλέπω το ip με την εντολή **ip addr show** (επέλεξα το 192.168.56.103 γτ αυτό δουλεύει στην συνέχεια)

```
[savvas@localhost html]$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN gr
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel s
oup default qlen 1000
    link/ether 08:00:27:7a:68:8b brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic nop
enp0s3
        valid_lft 1067sec preferred_lft 1067sec
    inet6 fe80::30b4:dc2b:402c:60bc/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[savvas@localhost html]$
```

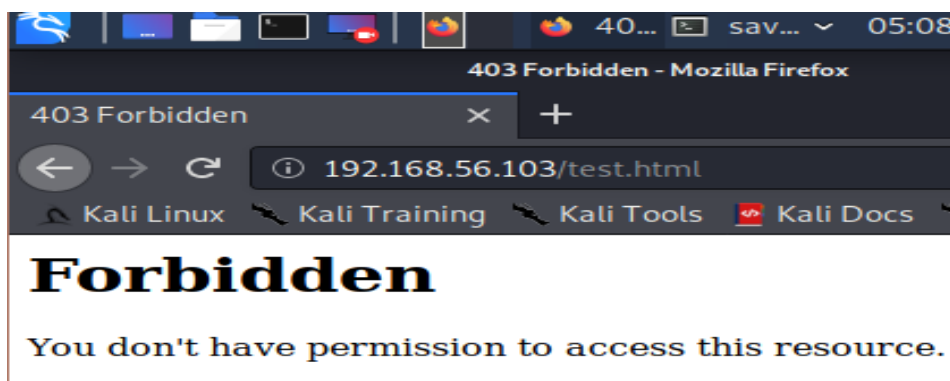
- ανοίγω το kali linux και στο command window και τρέχω την εντολή : **ping 192.168.56.103**

```
savvas@kali:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data:
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=1.20 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=1.56 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=1.50 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.907 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=1.17 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=1.16 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=64 time=1.15 ms
^C
--- 192.168.56.103 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6013ms
rtt min/avg/max/mdev = 0.907/1.235/1.562/0.208 ms
savvas@kali:~$
```

- ανοίγω το web browser και τρέχω **192.168.56.103/test.html** και μου εμφανίζεται :



- αφού το τρέξω πάω στο terminal του fedora και για να αφαιρέσω το δικαίωμα ανάγνωσης του αρχείου τρέχω την εντολή : **sudo chmod -r test.html**



Βλέπω ότι πλέον δεν μπορώ να δω από τον browser του kali το περιεχόμενο του αρχείου test.html

- τώρα ανοίγω το wireshark με την εντολή **sudo wireshark** και αφού τρέξω τα βήματα που περιγράφει η εκφώνηση της άσκησης παίρνω το παρακάτω αποτέλεσμα . Εδώ για να εντοπίσουμε αυτό που θέλουμε ξέρουμε ότι το αντίστοιχο response code είναι 403 οπότε πληκτρολογούμε στην αναζήτηση: **http.response.code eq 403**

The image shows a Wireshark capture on the interface `enp0s3`. The filter bar at the top is set to `http.response.code eq 403`. The packet list shows five filtered packets, all of which are HTTP 403 Forbidden responses from `192.168.56.103` to `192.168.56.102`. The details pane for packet 11 is expanded, showing the following structure:

- Frame 11: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface `enp0s3`, id 0
- Ethernet II, Src: PcsCompu\_7a:68:8b (08:00:27:7a:68:8b), Dst: PcsCompu\_72:55:ab (08:00:27:72:55:ab)
- Internet Protocol Version 4, Src: `192.168.56.103`, Dst: `192.168.56.102`
- Transmission Control Protocol, Src Port: 80, Dst Port: 38186, Seq: 1, Ack: 350, Len: 416
- Hypertext Transfer Protocol**
- Line-based text data: text/html (7 lines)

The raw data pane at the bottom shows the hex and ASCII representation of the packet data, including the HTTP status line:

```

0000 08 00 27 72 55 ab 08 00 27 7a 68 8b 08 00 45 00  ..rU... 'zh...E...
0010 01 d4 4d 5b 40 00 40 06 f9 aa c0 a8 38 67 c0 a8  ..M[...@...8g...
0020 38 66 00 50 95 2a d2 9c f8 e9 9d c9 c1 b5 80 18  8fP*... ..80 18
0030 01 fb f3 e4 00 00 01 01 08 0a 33 48 92 2d c9 12  .. ....3H....
0040 09 02 48 54 54 50 2f 31 2e 31 20 34 30 33 20 06  ..HTTP/1.1 403 ..
0050 5f 72 62 60 64 64 65 66 0d 0a 44 61 74 65 3a 20  forbidden ..Date:
0060 54 75 65 2c 20 30 31 20 44 65 63 20 32 30 32 30  Tue, 01 Dec 2020
0070 20 30 35 3a 31 38 3a 32 32 20 47 4d 54 0d 0a 53  05:18:22 GMT...S
0080 65 72 76 65 72 3a 20 41 70 61 63 68 65 2f 32 2e  erver: Apache/2.
0090 34 2e 34 30 20 28 46 65 64 6f 72 61 29 0d 0a 43  4.46 (Fedora); C
00a0 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31  ontent-Length: 1
00b0 39 39 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a 20  99-Keep-Alive:
00c0 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61 78 3d 31  timeout=5, max=1
00d0 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20  00-Connection:
00e0 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6e 74  Keep-Alive...Cont
  
```

The status bar at the bottom indicates that 97 packets were captured and 5 (5.2%) are displayed, matching the filter.

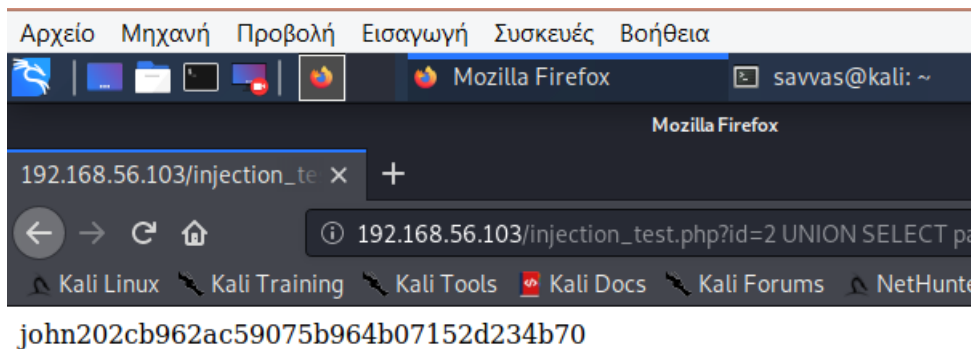
## Άσκηση 2

Χρησιμοποιώντας το php script που δημιουργήσαμε στην Εργαστηριακή Άσκηση 3 να κάνετε κάποιες προσπάθειες sql injection. Με τη βοήθεια του Wireshark να προσπαθήσετε να εντοπίσετε τις προσπάθειες αυτές χρησιμοποιώντας το φίλτρο: `http.request.uri matches "xxxx"` , όπου xxxx ένα κατάλληλο regular expression. Να επισυνάψετε screenshot με το αποτέλεσμα.

## Απάντηση 2:

Από την εργαστηριακή άσκηση 3 θυμάμαι ότι χρησιμοποίησα τις εντολές :

- `localhost/injection_test.php?id=1`
- `localhost/injection_test.php?id=1 OR 1=1`
- `localhost/injection_test.php? id=1 UNION SELECT password FROM users where id=1 AND 1=1`
- `localhost/injection_test.php? id=1 UNION SELECT password FROM users where id=2 AND 1=1`
- παρομοίως και τώρα πάω στο kali και τρέχω τις παραπάνω εντολές αλλά αντί για localhost βάζω **192.168.56.103** ( για παράδειγμα : **192.168.56.103/injection\_test.php?id=1** )



- αν τσεκάρω στο wireshark μπορώ να βάλω την εντολή αναζήτησης : `http.request.uri matches "(select|union|id)"`

