

Internship Program - Cyber Security - Group 2

Name : Karthik N P

USN : 4MT19CS067

1) Exploiting DVWA

This report describes how to access the Damn Vulnerable Web Application (DVWA) on Kali Linux and demonstrate some of its vulnerabilities. The user enables superuser privileges, scans the network to find the IP address of the Metasploitable machine running DVWA, and logs in. The user sets the security level to "low" and demonstrates SQL injection vulnerabilities, reflected and stored cross-site scripting (XSS) vulnerabilities, and an insecure file upload vulnerability that allows accessing uploaded files.

Provide the super user privilege using the command

\$sudo su and enter the password of kali

start the metasploitable machine

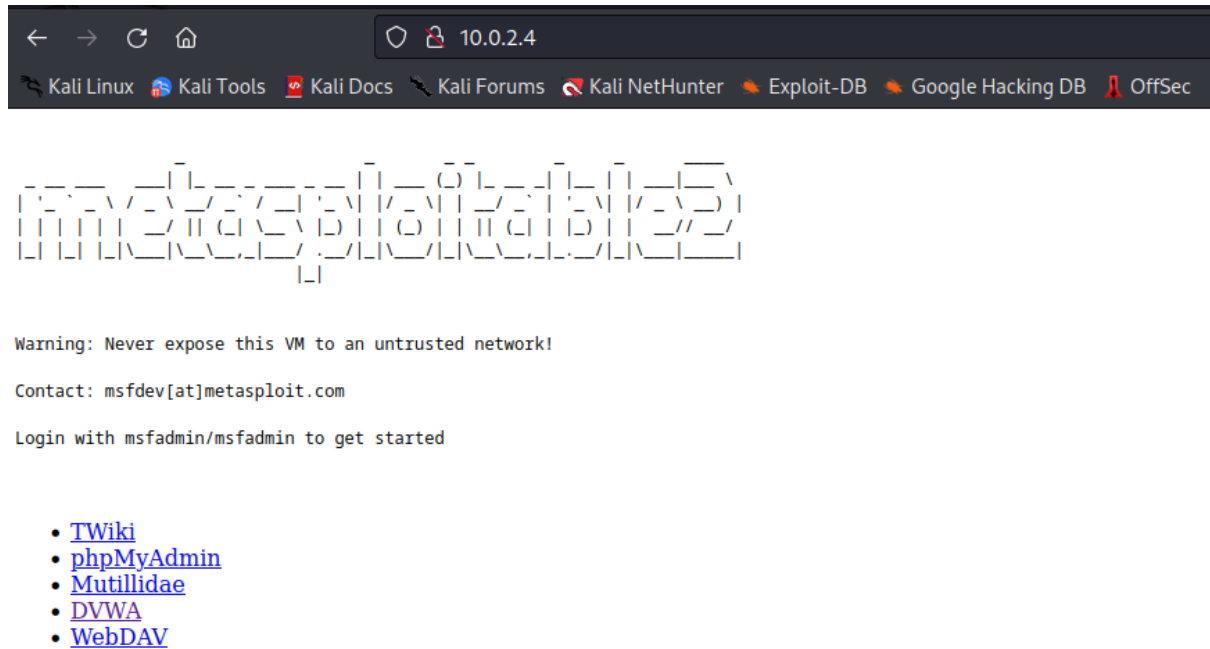
scan for the available network using the command **#nbtscan** and provide the ip address range

```
(kali㉿kali)-[~/Desktop]
$ sudo su
[sudo] password for kali:
(kali㉿kali)-[~/Desktop]
# nbtscan 10.0.2.0/24
Doing NBT name scan for addresses from 10.0.2.0/24
```

IP address	NetBIOS Name	Server	User	MAC address
10.0.2.4	METASPLOITABLE	<server>	METASPLOITABLE	00:00:00:00:00:00
10.0.2.255	Sendto failed: Permission denied			

```
(kali㉿kali)-[~/Desktop]
#
```

now you have the ip address of the metasploitable search that ip address in the browser.



Then select the **DVWA** option which will be there in the window. Then login to DVWA by providing username as **admin** and password as **password**.



Username

admin

Password

••••••••

Login

After login then make sure that **DVWA Security** is set to **low**.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

▼

Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.


You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)


1a) SQL injection on DVWA

We can use SQL Injection option then we enter a query **1"or"1="1** in the provided field after that we can see the information provided in that field.



The screenshot shows the DVWA web application interface. At the top is the DVWA logo. On the left is a sidebar menu with various options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted in green), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: SQL Injection". It contains a "User ID:" label, a text input field, and a "Submit" button. Below the input field, the output is displayed in red text: "ID: 1\"or\"1=\"1", "First name: admin", and "Surname: admin". Underneath this is a "More info" section with three links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>. At the bottom left, it shows "Username: admin", "Security Level: low", and "PHPIDS: disabled". At the bottom right, there are "View Source" and "View Help" buttons. The footer at the very bottom says "Damn Vulnerable Web Application (DVWA) v1.0.7".

Similarly we can use the SQL Injection (Blind) for the same purpose.



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection (Blind)

User ID:

Submit

ID: 1"or"1="1
First name: admin
Surname: admin

More info

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

Username: admin
Security Level: low
PHPIDS: disabled


View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

1b) Perform Cross-site scripting on DVWA

XSS reflected option is used to display the message on the screen whatever is entered in the field provided here we use the `<script>alert("karthik n p")</script>` command to display the text.



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello

More info

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

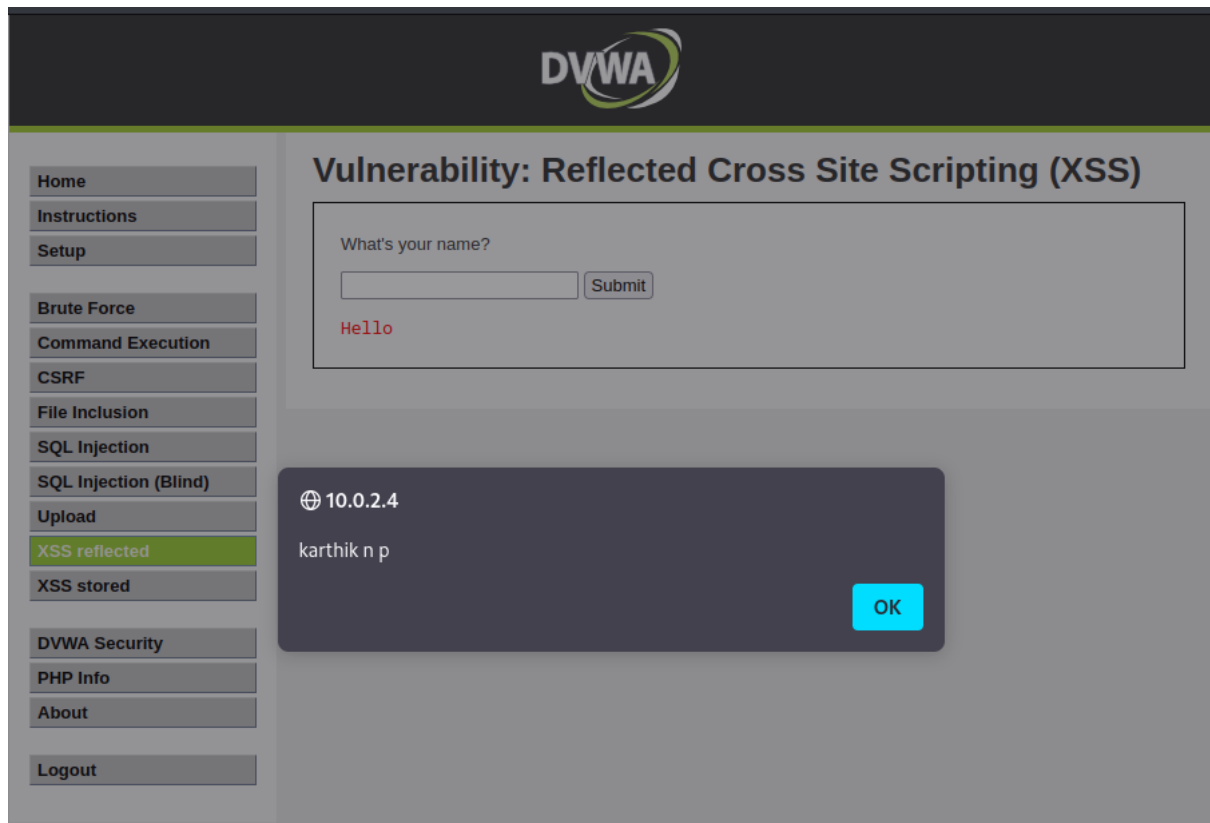
Username: admin
Security Level: low
PHPIDS: disabled

View Source


View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

So it pop up a alert message by displaying the message provided in the alert command.



The difference between **XSS reflected** and **XSS stored** is that in XSS stored method we can store the procedure and can use afterwards also which is not possible in XSS reflect method.



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

karthik np

Message *

<script> prompt("Hi there")</script>

Sign Guestbook

Name: test

Message: This is a test comment.

Name: abhishek

Message: <script>alert("hacked")</script>

Name: abhishek

Message: <script>alert("hacked")</script>

Name: k

Message:

More info

<http://hackers.org/xss.html>

http://en.wikipedia.org/wiki/Cross-site_scripting

<http://www.cgisecurity.com/xss-faq.html>


Username: admin

Security Level: low

PHPIDS: disabled

View Source

View Help



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Sign Guestbook

10.0.2.4

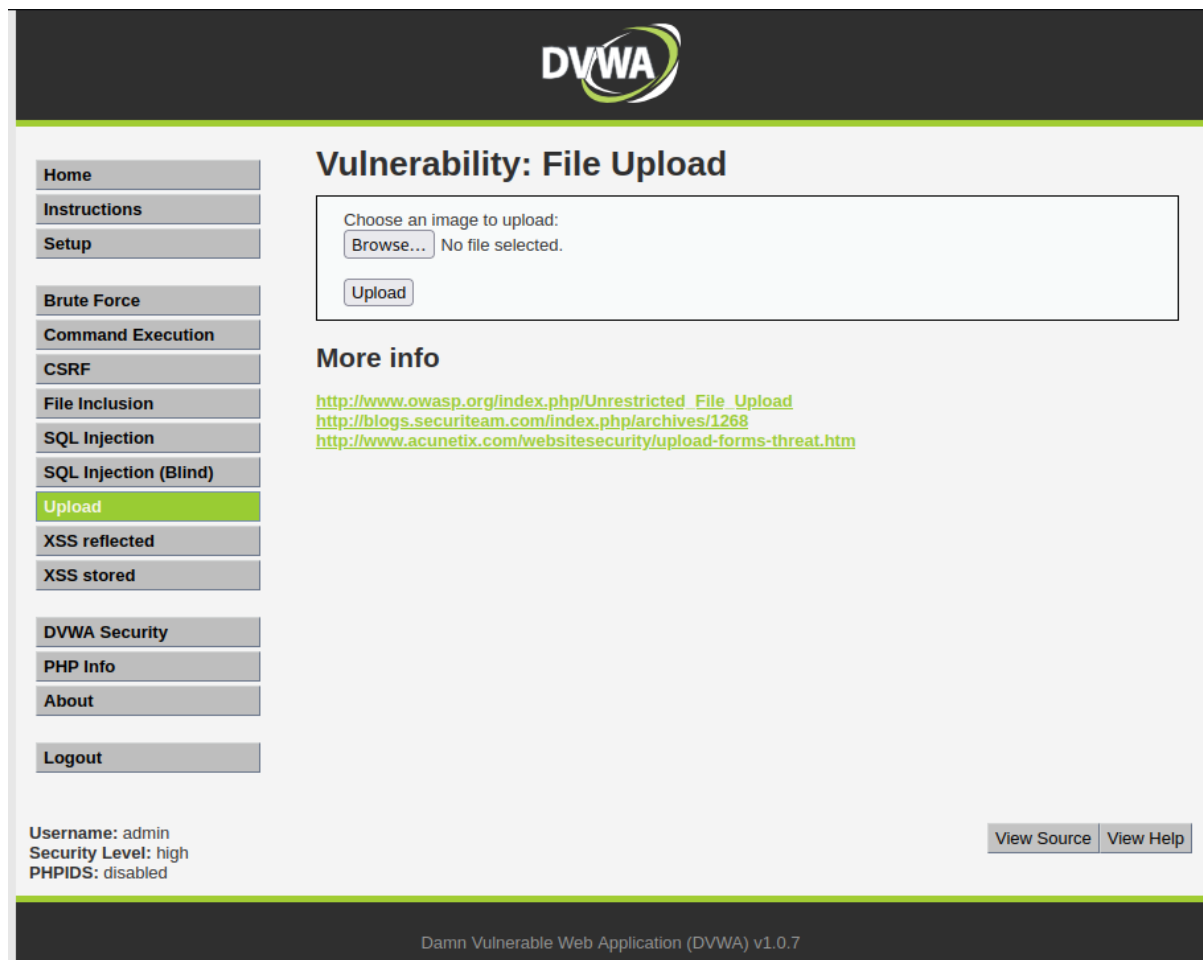
k

Cancel

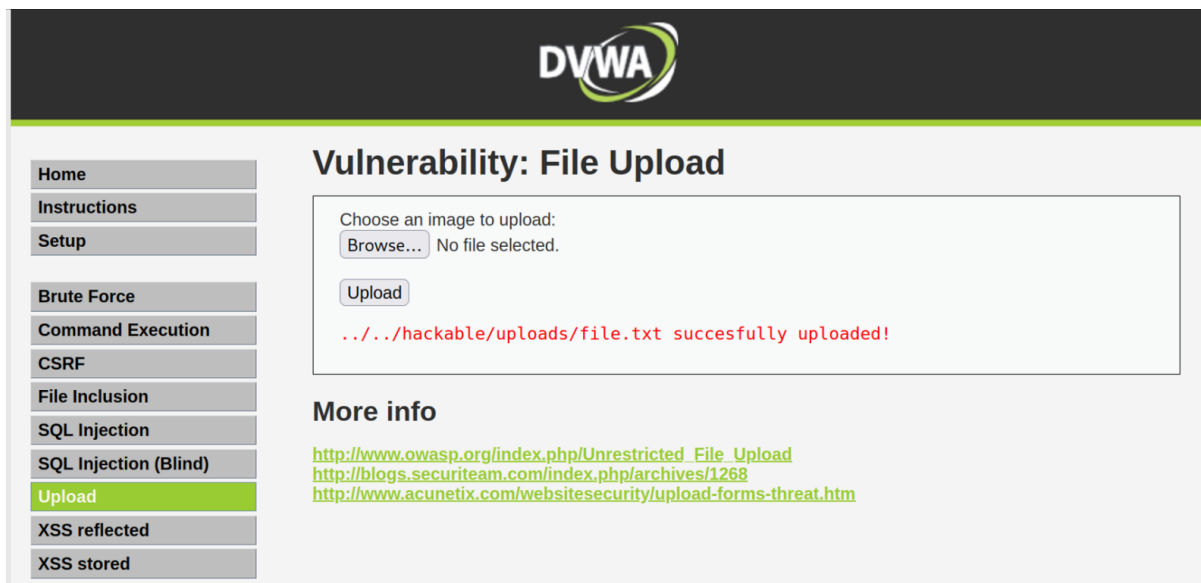
OK

1c) Perform File upload DVWA




Upload option is used to upload a file which resides in the user machine.



The screenshot displays the DVWA web application interface. At the top, there is a dark header with the DVWA logo. Below the header, a left sidebar contains a list of navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload (highlighted in green), XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: File Upload". It features a form with the text "Choose an image to upload:" followed by a "Browse..." button and the text "No file selected.". Below this is an "Upload" button. Under the "More info" section, there are three links: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websecurity/upload-forms-threat.htm>. At the bottom left, the user status is shown: "Username: admin", "Security Level: high", and "PHPIDS: disabled". At the bottom right, there are "View Source" and "View Help" buttons. The footer of the page states "Damn Vulnerable Web Application (DVWA) v1.0.7".



After uploading the file if we change the url to **/dvwa/hackable/uploads** then we can view the contents of the uploaded file.

Index of /dvwa/hackable/uploads				
	Name	Last modified	Size	Description
	Parent Directory		-	
	dvwa_email.png	16-Mar-2010 01:56	667	
	file.txt	20-Feb-2023 18:39	51	

2a) Sniffing with wire shark in kali linux

The text describes how to use Wireshark, a network packet analyzer tool, to sniff HTTP traffic and capture login credentials. It instructs the reader to log into a test website called [testfire.net](#), then use Wireshark to analyze the HTTP traffic from logging in. By examining the HTTP POST request, the username and password used to log into the website can be discovered.

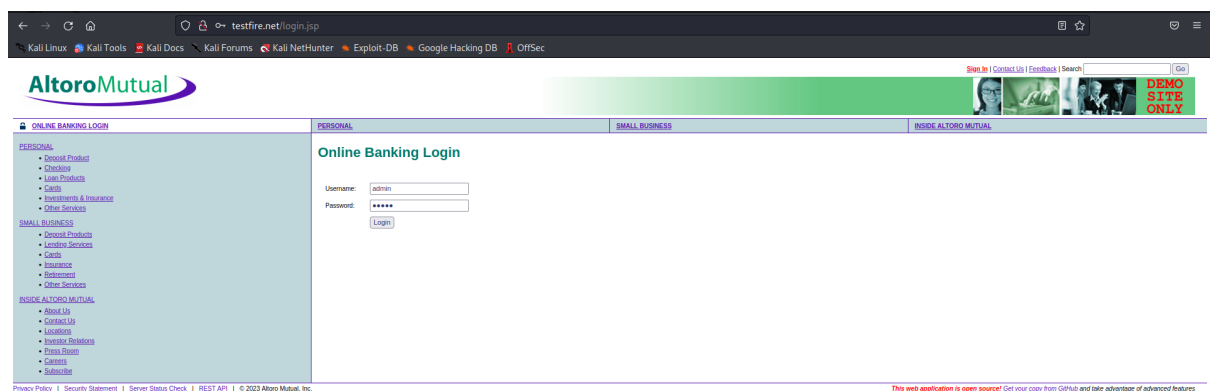
Getting super user privilage using the command

\$ sudo su

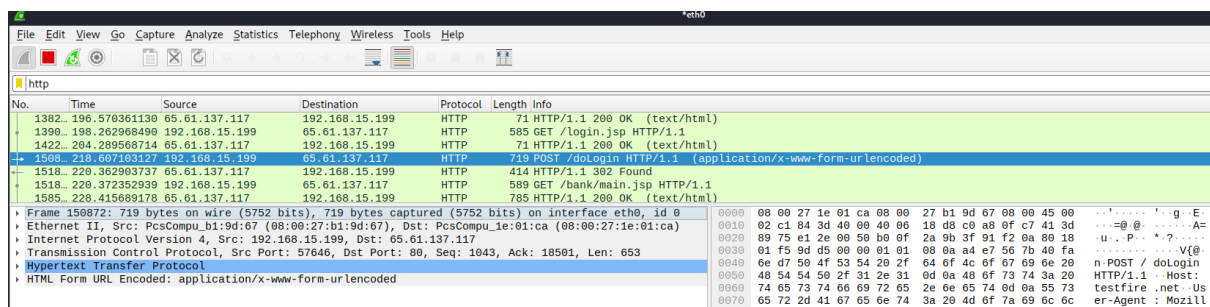
Then we have to search **wireshark** in the terminal to use it

```
(kali㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for kali:
(kali㉿kali)-[/home/kali/Desktop]
└─# wireshark
** (wireshark:16784) 00:21:03.724910 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

After that we have to search **testfire.net** in the browser inside the kali linux then we should login to the website by providing username as **admin** and password as **admin**

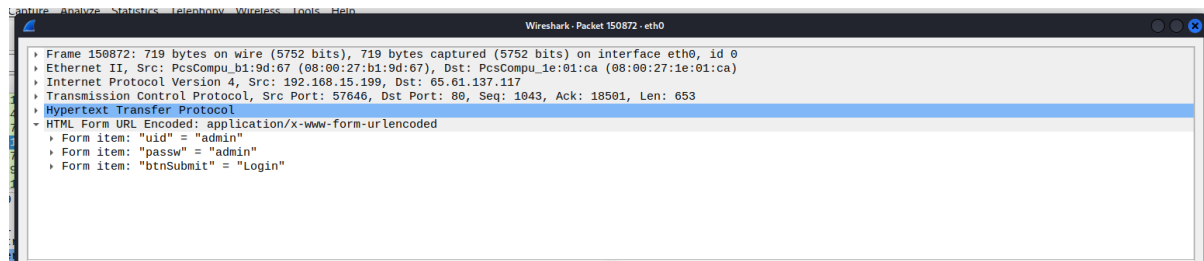


Then we come back to the **wireshark** tool which was opened previously then we search **http** in the search bar in order to get information about http connection, we should search for **http post methods** then we should double click on that connection.



After double clicking that connection we should search for **Hypertext Transfer Protocol** in the dropdown we can see the username and password we entered in

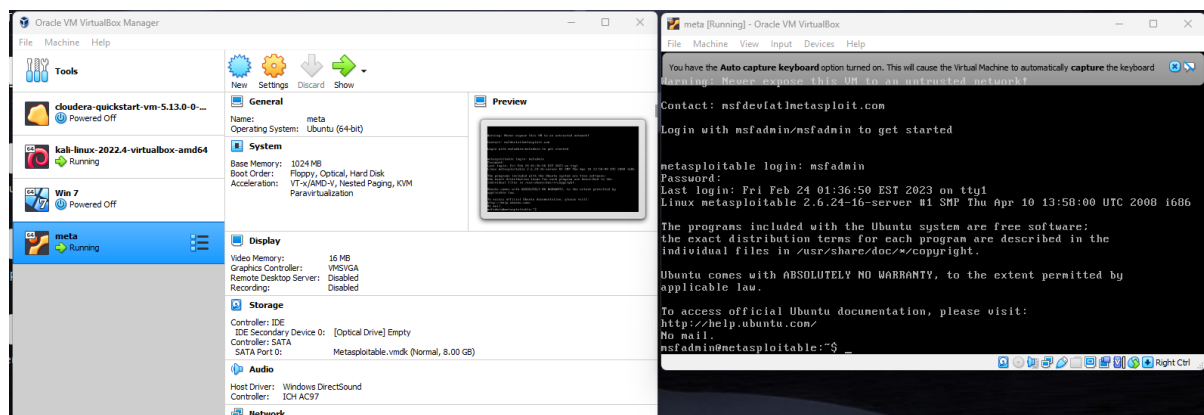
the testfire.net.

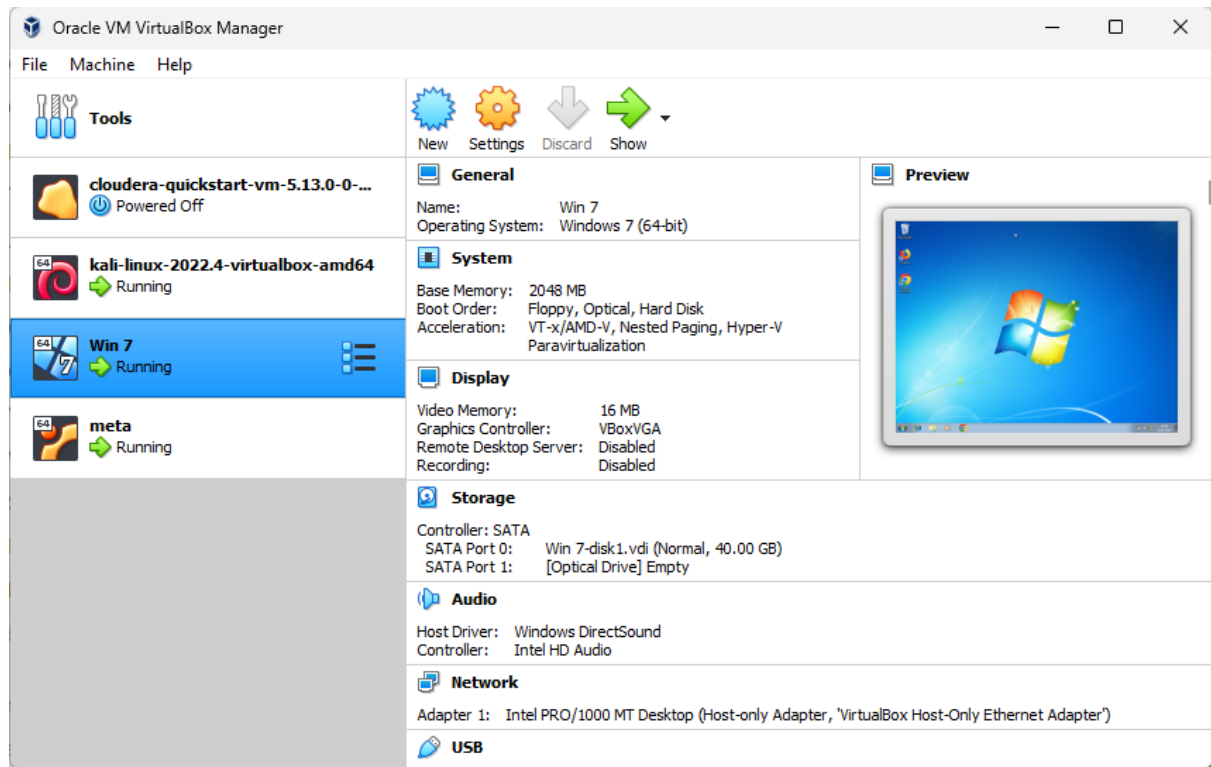


2b) Sniffing with Ettercap in kali linux

The text describes how to perform a man-in-the-middle attack using Kali Linux, Metasploitable, and Windows 7 virtual machines. The attacker scans the network to find the IP addresses of the Windows 7 and Metasploitable machines. They then use ettercap to intercept traffic between the two machines. When the user on Windows 7 logs into the DVWA website on Metasploitable, the attacker is able to see the username and password that was entered.

We set all three machine that is kali, Metasploitable and Windows 7 to **Host only adapter** and start them.





Getting super user privilage using the command

\$ sudo su

then we search for the available ip addresses using the command **#nbtscan 192.168.56.0/24**.when we run that commnad we see the ip addresses of **Windows 7** and **Metasploitable** machine.

```
(kali㉿kali)-[~/Desktop]
$ sudo su
[sudo] password for kali:
(kali㉿kali)-[~/Desktop]
# ifconfig
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::f041:29be:71b0:a9c5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
    RX packets 1934 bytes 510575 (498.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1948 bytes 169963 (165.9 KiB)
    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 1000 (Local Loopback)
    RX packets 126 bytes 12024 (11.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 126 bytes 12024 (11.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

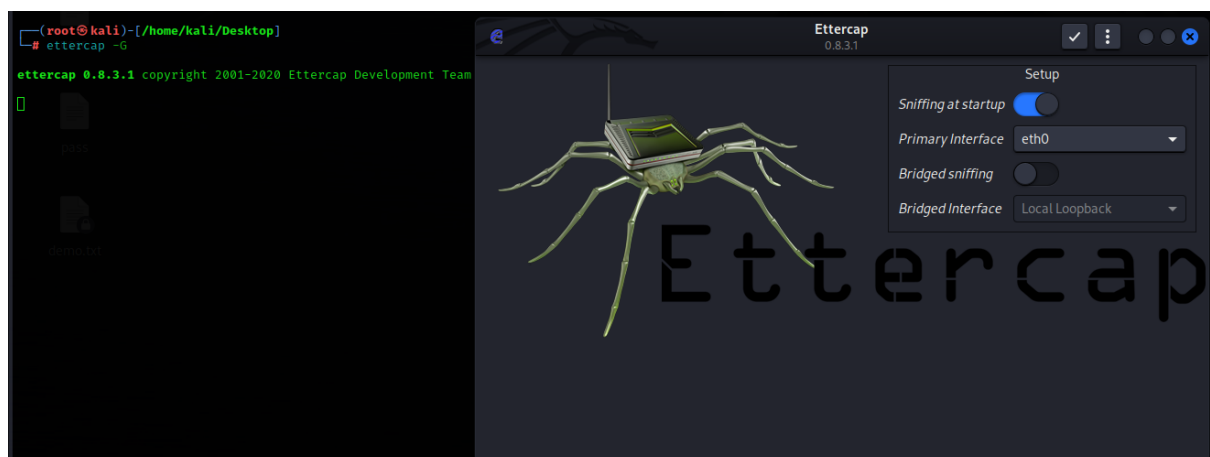
(kali㉿kali)-[~/Desktop]
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address      NetBIOS Name    Server    User          MAC address
-----
192.168.56.1    KARTHIKNP       <server>  <unknown>    0a:00:27:00:00:14
192.168.56.103  WINDOWS7-PC     <server>  <unknown>    08:00:27:9e:37:29
192.168.56.101  METASPLOITABLE  <server>  METASPLOITABLE 00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

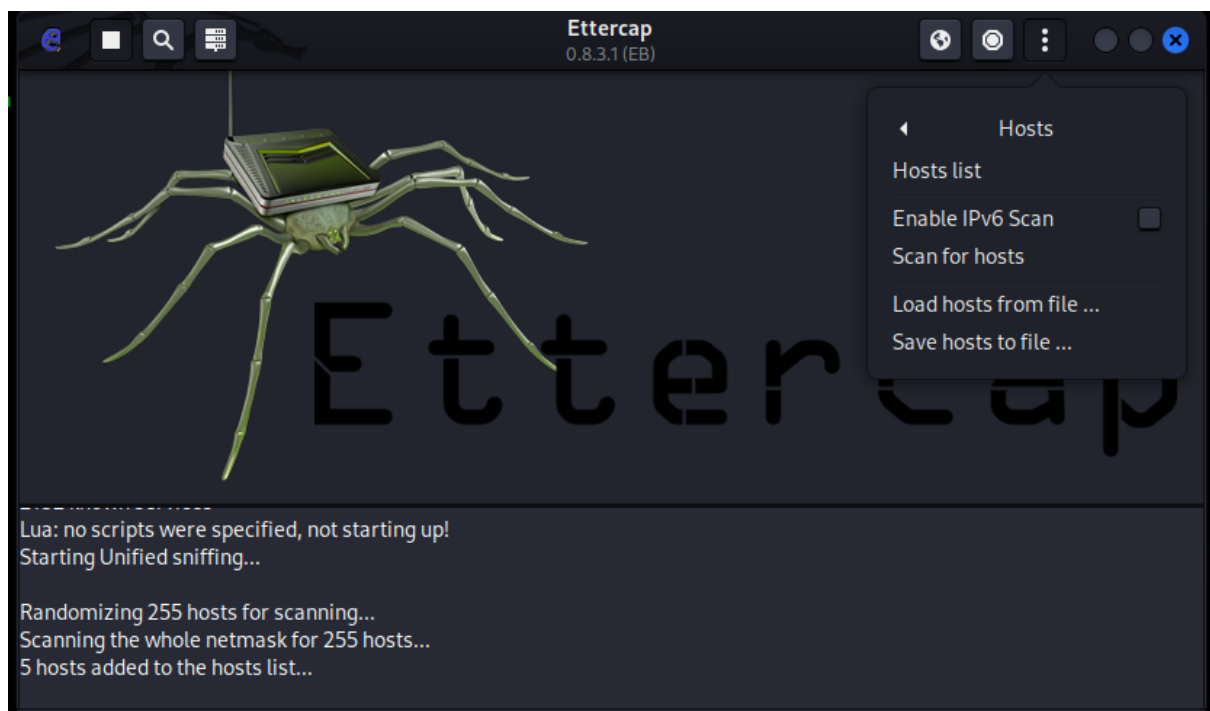
(kali㉿kali)-[~/Desktop]
# ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

Then we open the tool called ettercap using the command **ettercap -G**.



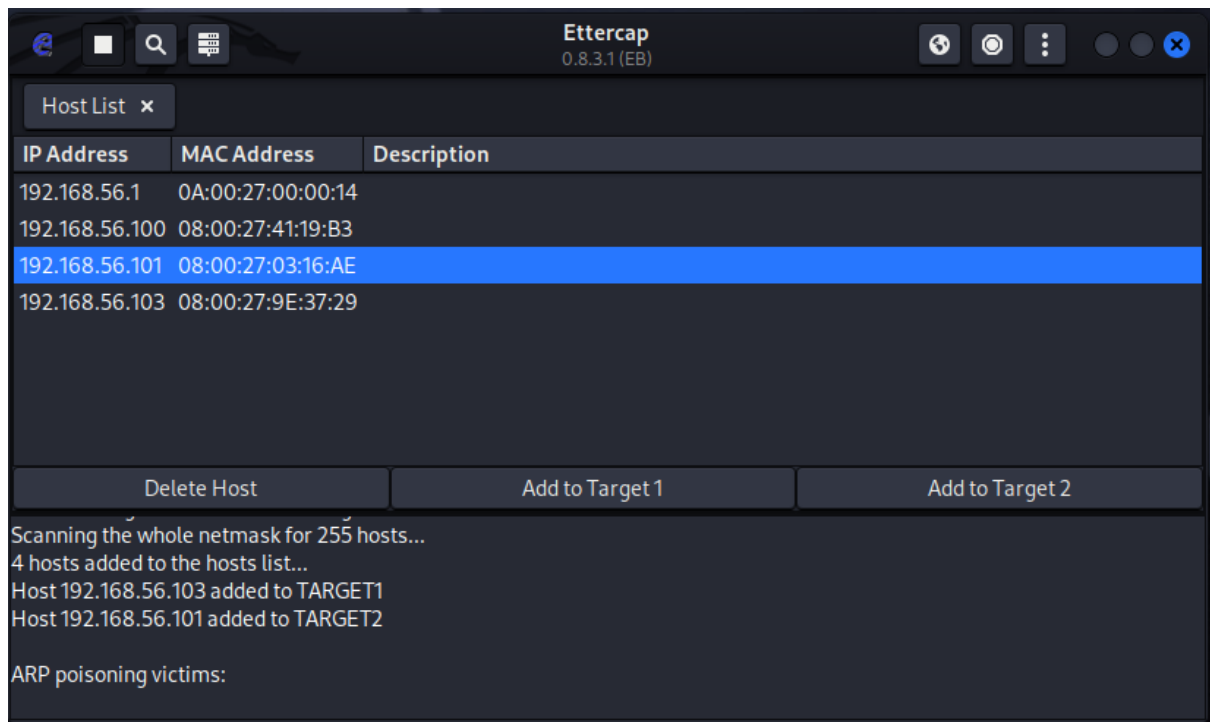
Then we scan for hosts using the option **Scan for hosts** which will be present under the **Hosts** option.

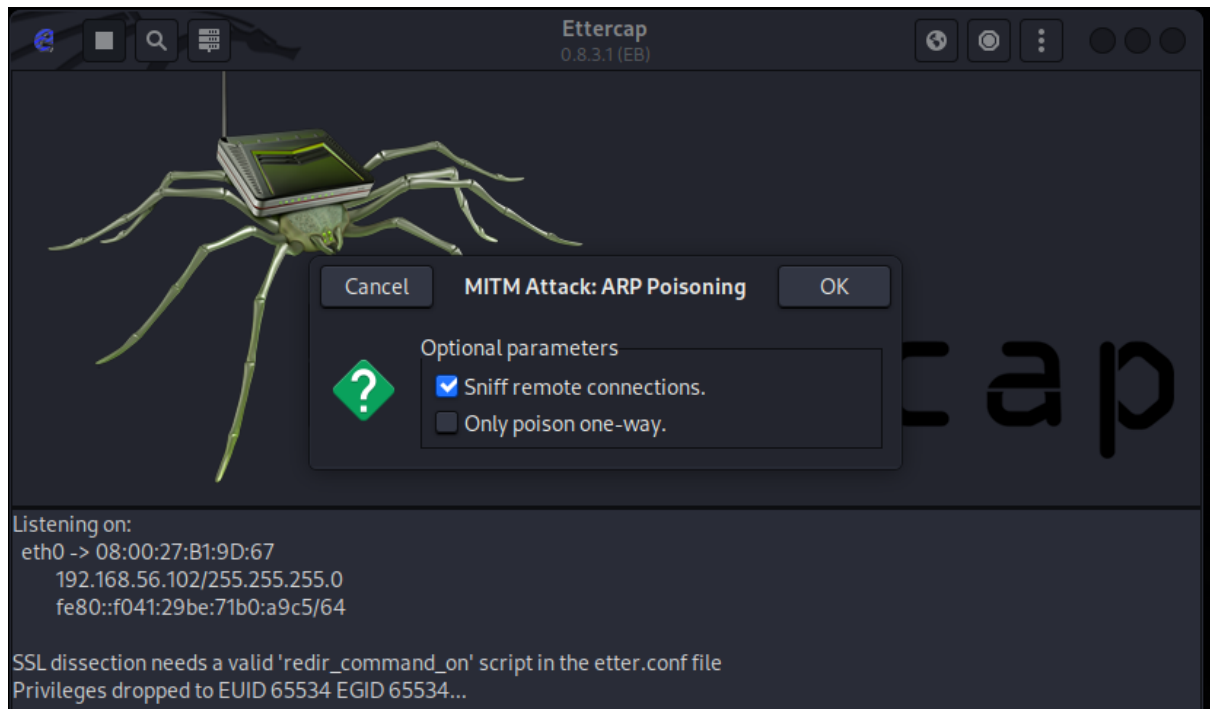


After that we have to set Targets using the option **Add to Target 1** and **Add to Target 2**.

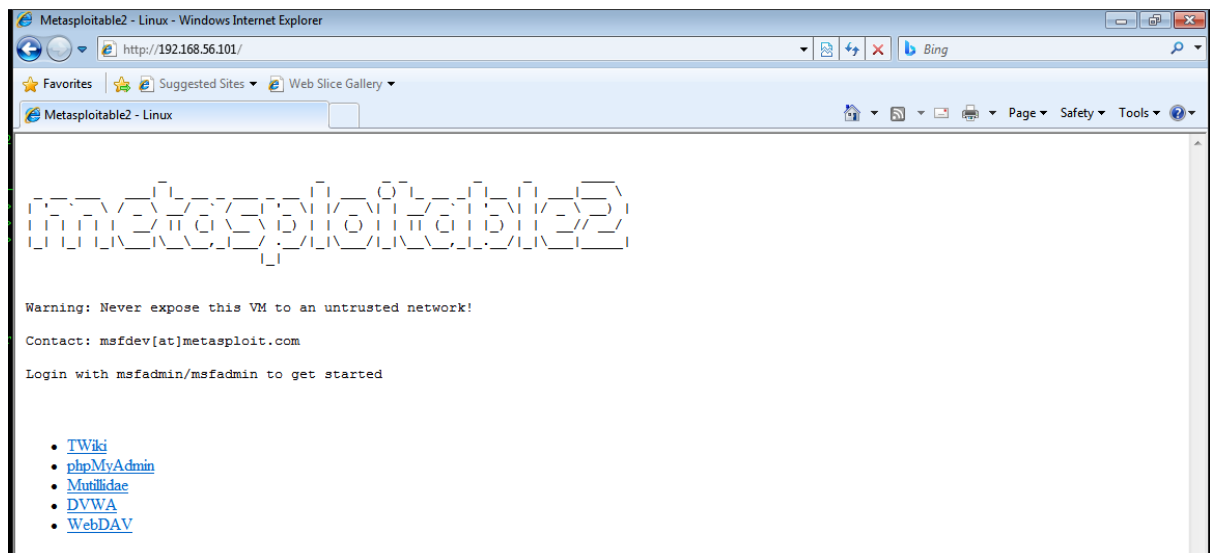
Target 1 → Windows 7

Target 2 → Metasploitable

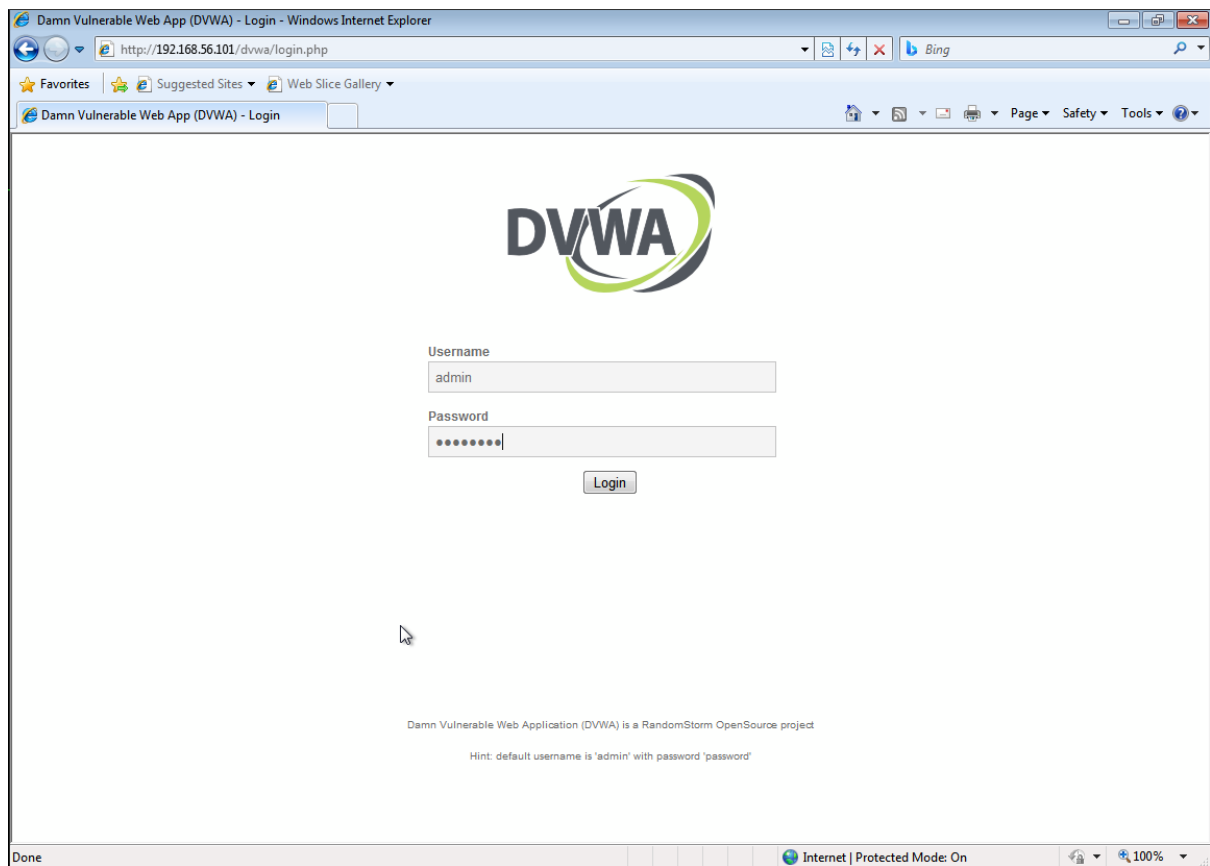




Then we have to note down the ip address of the **Metasploitable** and search it in the URL of the browser inside the **Windows 7**.



Login to the DVWA by providing Username as **admin** and Password as **password**.



In the ettercap [Kali] we can see the username and password we entered in the DVWA [Windows 7]

as **username=admin&password=password&Login=Login.**

