

**SCHOOL OF COMPUTER SCIENCE**  
**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**  
**DEHRADUN, UTTARAKHAND**



**IT DATA SECURITY LAB**  
**LABORATORY FILE**  
**(2024-2025)**

**For**  
**V<sup>th</sup> Semester**

**Submitted To:**

Prof. Abhishek Yadav  
Assistant Professor S.S.  
[V<sup>th</sup> Semester]  
School of Computer Sciences

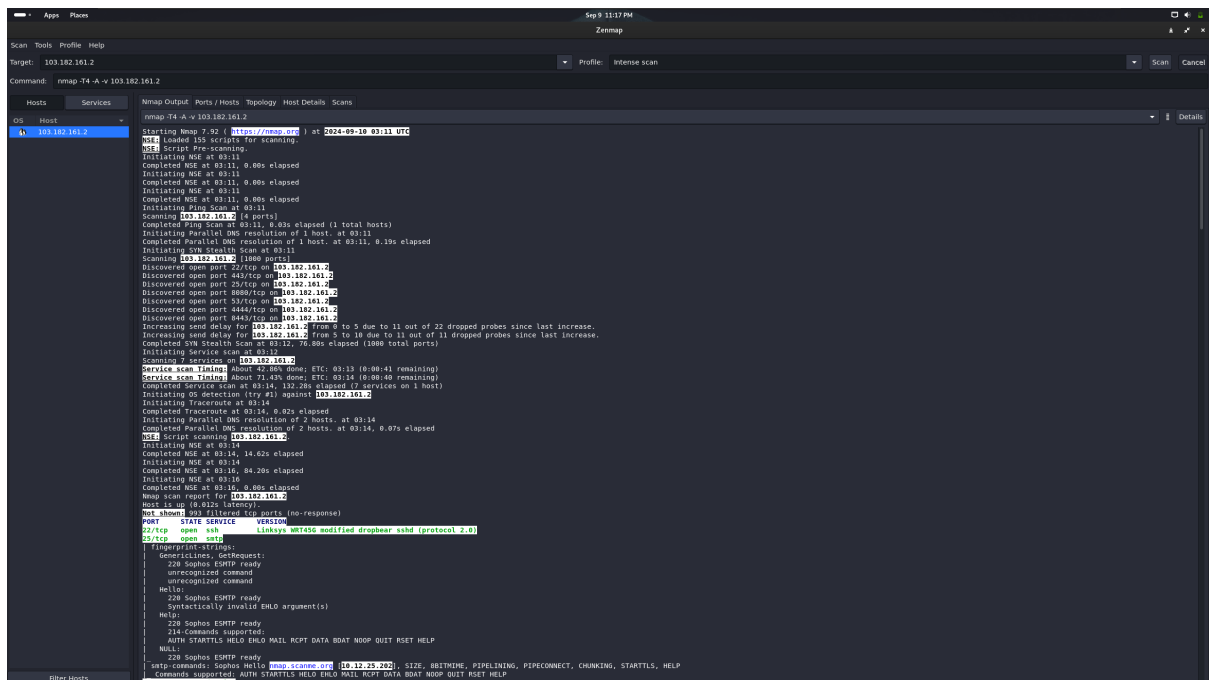
**Submitted By:**

Mr. Akshat Negi  
500106533(SAP ID)  
R2142220414(Roll No.)  
B.Tech. CSF (Batch-1)

**Nmap (Network Mapper)** is a huge tool and has many uses. Nmap is used to gather information about any device. Using the Nmap, we can gather information about any client that is within our network or outside our network, and we can gather information about clients just by knowing their IP. Nmap can be used to bypass firewalls, as well as all kinds of protection and security measures. In this section, we're going to learn some of the basic Nmap commands that can be used to discover clients that are connected to our network, and also discover the open ports on these clients.

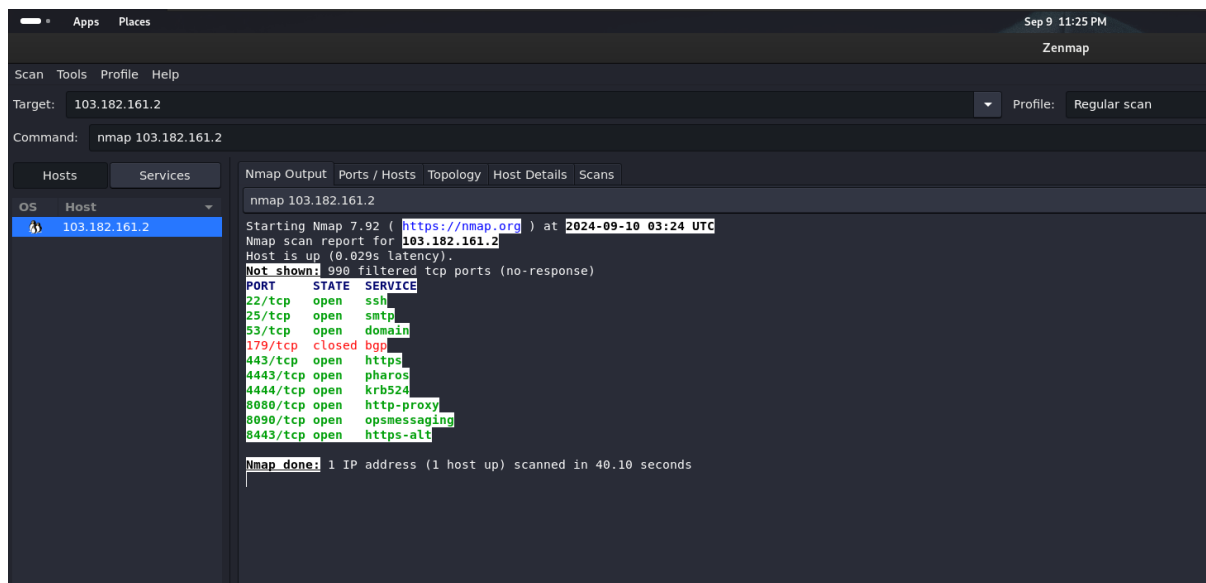
**Zenmap** is the official **Nmap Security Scanner GUI**. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open-source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

### Performing Intense scan:





## Performing Regular scan:



## DATABASE SCANNING WITH SCUBA

**Scuba** is a powerful database vulnerability scanner designed to identify and assess potential security risks within various database systems. By automating the process of vulnerability detection, Scuba helps organizations proactively protect their valuable data and prevent unauthorized access.

### Benefits of Using Scuba

- **Improved Data Security:** Scuba helps organizations protect their sensitive data from unauthorized access and exploitation.
- **Reduced Risk of Data Breaches:** By identifying and addressing vulnerabilities proactively, Scuba helps mitigate the risk of data breaches and their associated costs.
- **Enhanced Compliance:** Scuba can assist organizations in meeting compliance requirements such as GDPR, HIPAA, and PCI DSS.
- **Time and Cost Savings:** Automated scanning and vulnerability assessment can save time and resources compared to manual methods.

### With this tool you can:

- Scan enterprise databases for vulnerabilities and misconfiguration
- Know the risks to your databases
- Get recommendations on how to mitigate identified issues

Enter password: \*\*\*\*

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 15

Server version: 8.0.39 MySQL Community Server - GPL

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;

Database
information_schema
lab1
lab2
lab3
lab4
lab6
mysql
performance_schema
sakila
sys
world

11 rows in set (0.00 sec)

mysql> |


Scuba

Help

# IMPERVA®

Scuba is a free tool that scans leading enterprise databases for security vulnerabilities and configuration flaws, including patch levels. It includes more than 2,300 assessment tests for Oracle, Microsoft SQL Server, SAP Sybase, IBM DB2, MySQL, PostgreSQL and Informix.

With Scuba, you can uncover potential security risks undermining your database security.




**\*NEW\*** Scuba now supports scanning of the supported databases when installed in AWS, Azure and GCP!

[Click to learn more](#)

Note: Scuba does not support scanning database as a service. To scan RDS databases please use [Imperva Snapshot](#)

**Please fill in your database details and click "Go!"**



[Sales@imperva.com](mailto:Sales@imperva.com)

[www.imperva.com](http://www.imperva.com)

1-866-926-4678

☒ Local Network

☐ Cloud (SSH Tunnel)

SSH Host

SSH Username

SSH Private Key

MYSQL

127.0.0.1

3306

root

Password

lab1

Go!


Scuba

Help

# IMPERVA®

Scuba is a free tool that scans leading enterprise databases for security vulnerabilities and configuration flaws, including patch levels. It includes more than 2,300 assessment tests for Oracle, Microsoft SQL Server, SAP Sybase, IBM DB2, MySQL, PostgreSQL and Informix.


With Scuba, you can uncover potential security risks undermining your database security.



**\*NEW\*** Scuba now supports scanning of the supported databases when installed in AWS, Azure and GCP!  
[Click to learn more](#)

Note: Scuba does not support scanning database as a service. To scan RDS databases please use [Imperva Snapshot](#)

**Please fill in your database details and click "Go!"**



Sales@imperva.com

www.imperva.com

1-866-926-4678

☒ Local Network

☐ Cloud (SSH Tunnel)

SSH Host

SSH Username

SSH Private Key

MYSQL


127.0.0.1

3306

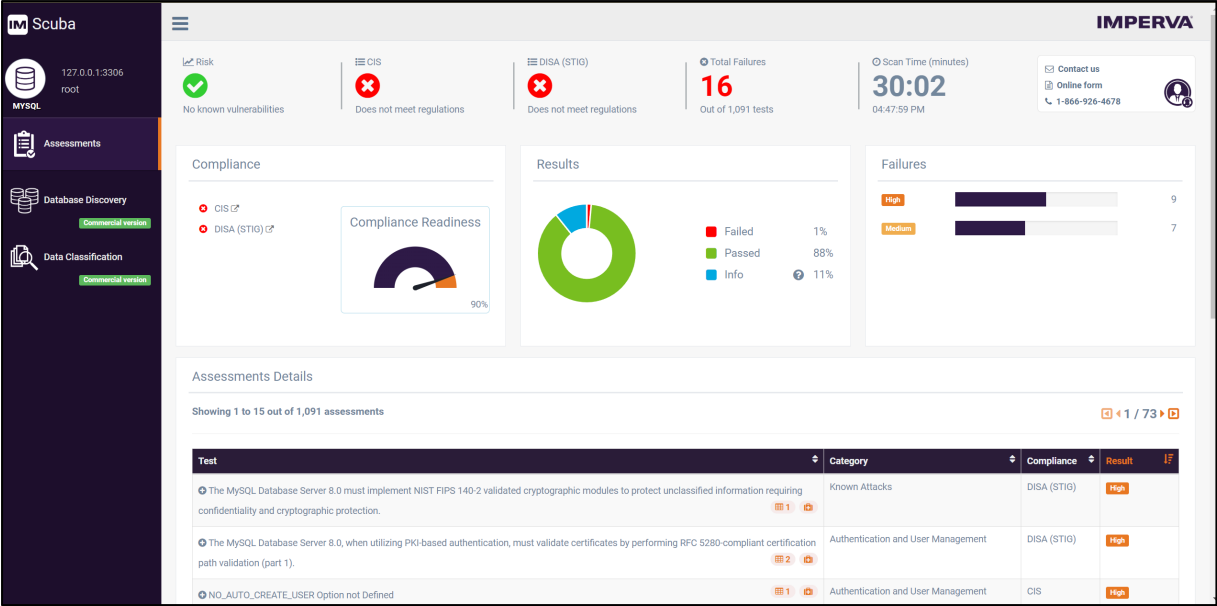
root

....

lab1



Initializing ...





Assessments Details

Showing 1 to 15 out of 1,091 assessments

1 / 73

Test	Category	Compliance	Result				
<div><div>The MySQL Database Server 8.0 must implement NIST FIPS 140-2 validated cryptographic modules to protect unclassified information requiring confidentiality and cryptographic protection.</div><div><div>1</div><div></div></div></div>	Known Attacks	DISA (STIG)	High				
<div>DETAILS</div> <div>It is the responsibility of the data owner to assess the cryptography requirements in light of applicable federal laws, Executive Orders, directives, policies, regulations, and standards.</div> <div>For detailed information, refer to NIST FIPS Publication 140-2, Security Requirements For Cryptographic Modules. Note that the product's cryptographic modules must be validated and certified by NIST as FIPS-compliant.</div>							
<div>DESCRIPTION</div> <div>se of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The application must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.</div>							
<div>DATA</div> <table><tr><th>VARIABLE_NAME</th><th>VARIABLE_VALUE</th></tr><tr><td>ssl_fips_mode</td><td>OFF</td></tr></table>				VARIABLE_NAME	VARIABLE_VALUE	ssl_fips_mode	OFF
VARIABLE_NAME	VARIABLE_VALUE						
ssl_fips_mode	OFF						

The provided Scuba scan summary indicates the following:

**Database:** MySQL

**Server:** 127.0.0.1:3306

**Scan Time:** 30 minutes and 1 second

**Total Failures:** 16

**Total Assessments:** 1,091

**Compliance Readiness:**

- Failed: 1% (11 out of 1,091 assessments)
- Passed: 88% (963 out of 1,091 assessments)
- Info: 11% (117 out of 1,091 assessments)

**Assessments Details:**

- The first two failed assessments are related to security best practices for the MySQL database server, such as implementing NIST FIPS 140-2 validated cryptographic modules and validating certificates using RFC 5280-compliant certification path validation.

**Overall, the scan identified 16 failures, indicating areas where the database system may be vulnerable.** It is important to address these issues to improve the security posture of the MySQL database.

**Additional Analysis:**

- Failed Assessments:** A more detailed analysis of the failed assessments would be necessary to understand the specific vulnerabilities and their potential impact.

- **Compliance Readiness:** The high percentage of passed assessments (88%) suggests that the database is generally compliant with security standards. However, the 1% of failed assessments should be addressed to ensure full compliance.
- **Info Assessments:** These assessments may provide additional recommendations or information that can be used to improve the database's security.

**Recommendations:**

- **Address Failed Assessments:** Prioritize the remediation of the failed assessments to mitigate potential security risks.
- **Review Info Assessments:** Consider the recommendations and information provided in the info assessments to further enhance the database's security.
- **Regular Scanning:** Conduct regular Scuba scans to identify and address new vulnerabilities as they emerge.
- **Security Best Practices:** Implement and maintain security best practices for MySQL databases, such as strong authentication, encryption, and regular patching.

By following these recommendations, organizations can improve the security of their MySQL databases and protect their valuable data.