|  |  |  |  |
| --- | --- | --- | --- |
|  | TO00BR92-3003  Network and Application Security |  | 1 (12) |
|  |  |
|  |  |
| Anup Nepal | 4.11.2023 |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |  |

Practice Lab work- Report-2

(Anup Nepal)

Table of Contents

[1 Introduction 3](#_Toc152796419)

[2 Methodology 3](#_Toc152796420)

[3 Practice Lab 3](#_Toc152796421)

[3.1 Lab work 6 3](#_Toc152796422)

[3.1.1 Introduction 3](#_Toc152796423)

[3.1.2 Learning outcomes 3](#_Toc152796424)

[3.1.3 Challenges 4](#_Toc152796425)

[3.1.4 Screenshots 4](#_Toc152796426)

[3.2 Lab work 7 6](#_Toc152796427)

[3.2.1 Introduction 6](#_Toc152796428)

[3.2.2 Learning outcomes 6](#_Toc152796429)

[3.2.3 Challenges . 6](#_Toc152796430)

[3.2.4 Screenshots 6](#_Toc152796431)

[3.3 Lab work 8 8](#_Toc152796432)

[3.3.1 Introduction 8](#_Toc152796433)

[3.3.2 Learning outcomes 8](#_Toc152796434)

[3.3.3 Challenges 8](#_Toc152796435)

[3.3.4 Screenshots 8](#_Toc152796436)

[3.4 Lab work 9 10](#_Toc152796437)

[3.4.1 Introduction 10](#_Toc152796438)

[3.4.2 Learning outcomes 10](#_Toc152796439)

[3.4.3 Challenges 10](#_Toc152796440)

[3.4.4 Screenshots 10](#_Toc152796441)

[3.5 Lab work 10 11](#_Toc152796442)

[3.5.1 Introduction 11](#_Toc152796443)

[3.5.2 Learning outcomes 11](#_Toc152796444)

[3.5.3 Challenges 11](#_Toc152796445)

[3.5.4 Screenshots 11](#_Toc152796446)

[4 Conclusion 12](#_Toc152796447)

# Introduction

This report is the first part of lab work which consists of fourteen different lab exercises grouped under 5 lab sessions, completed in a period of a month or so. This report summarizes the introduction of lab work, the process involved, learning reflections and challenges faced during the lab work and to validate the process, I have attached multiple screenshots for each lab session.

To provide a clear description of the lab work, I have divided the lab work into three sections under the lab work (section 3) title below and describe the learning outcomes and screenshots respectively. Since the focus of this report is mostly on the reflection of the lab work, I think it is a better way to describe them separately. Moreover, the methodology involved for all the tasks is the same, hence I have written general methodology.

# Methodology

Prior to commencing any laboratory work, my initial step was to thoroughly review the instructions for utilizing the Precipio lab environment as provided by the instructors on Canvas. After configuring the setup, I proceeded to tackle the lab assignments by thoroughly observing the Precipio lab environment's guidelines. Instead of immediately starting the tasks, I ensured that I began with a comprehensive understanding. I started by familiarizing myself with the introduction, objectives, examining the lab diagram, and gaining insights into the background of the topic. This approach allowed me to obtain a holistic perspective of the tasks I would be undertaking.

# Practice Lab

## Lab work 6

### Introduction

This lab work focuses on various techniques and attacks related to network sniffing, social engineering exploits, DOS, and session hijacking.

### Learning outcomes

I find this lab work particularly challenging and very technical. However, it was very interesting overall and I have learned about various tools to perform sniffing, poisoning, hijacking and other hacking concepts and techniques.

Even though I have finished the lab, I would have to revisit it once more as it was very difficult to follow some of the concepts.

### Challenges

There were some technical challenges regarding the lab machine boot up issues and lagging during the lab session mainly due to the need of long polling.

### Screenshots

|  |
| --- |
| Fig 1. Configuring burp suite to listen to proxy server.    Fig 2. Intercepting the http traffic to hijack the session Id using burp suite.    Fig 3. Using dnschef - A DNS proxy to allow to redirect all DNS queries to single IP.    Fig 4. Macflooding using yersinia GUI application.    Fig 5. DOS attack in process and the performance overload |

----------------

## Lab work 7

### Introduction

This lab work consists of lab compromising web server, web application exploitation concepts and attacks.

### Learning outcomes

During this lab session, I acquired substantial hands-on expertise in the field of web application security. As a dedicated enthusiast of web applications with prior development experience, the lab exercises were not only captivating but also enjoyable. Engaging in practical tasks not only deepened my comprehension but also familiarized me with diverse vulnerabilities and successful mitigation techniques. Moreover, I was able to learn more about the webservers and the vulnerabilities that could be exploited and prevented. The most important discovery of this lab module was the bWAPP application and the plethora of attacks available there to practice.

### Challenges There were some technical challenges regarding the lab machine boot up issues and lagging during the lab session mainly due to need of long polling.

### Screenshots

|  |
| --- |
| Fig 1. Cloned version of bWAPP web app, example of how hackers could fool us pretending to be legitimate web application. |
| Fig 2. Cracking the password using Brutespray application |
| Fig 3. Authorization attack using URI -bypassing the authorization and able to access the document without login using the URL path. |
|  |

----------------

## Lab work 8

### Introduction

This lab work was all about SQL Injection, techniques, and mitigation methods.

### Learning outcomes

The lab session was fascinating because it covered the most common types of attacks in the web application domain i.e. SQL injection. The lab exercises were straightforward and effectively taught how to inject code, locate injection points, understand syntax variations, and employ different techniques to exploit web applications for extracting valuable information. In addition to learning about attacking tools and techniques, I also gained insights into preventing SQL injection. For instance, using parameterized queries and implementing input validation and sanitation were highlighted as effective methods to prevent these types of attacks.

### Challenges

There were some technical challenges regarding the lab machine boot up issues and lagging during the lab session mainly due to need of long polling.

### Screenshots

|  |
| --- |
| Fig 3. Able to extract the user’s information using SQL injection     A screenshot of a search box  Description automatically generated  Fig 4. Verifying the possibilities of SQL injection |
| Fig 4. Bypassing the login using sql injection  A screenshot of a computer  Description automatically generated  Fig 5. Detecting SQL injection using webcruiser |

## Lab work 9

### Introduction

This set of lab work dealt with exploiting wireless vulnerabilities, compromising IoT and OT platforms and Compromising & Exploiting Mobile devices.

### Learning outcomes

During these lab sessions, I gained theoretical knowledge about a wide range of topics related to network and device security. I learned about Wireless Networks, including standards, encryption, authentication, and potential threats. The lab also covered the Internet of Things (IoT) and Operational Technology (OT), explaining their concepts, vulnerabilities, attacks, and countermeasures. Furthermore, I was able get insights into mobile platform attack vectors, hacking Android OS, securing iOS devices, mobile device management, and various security guidelines and tools.

The only drawback of this lab session was the absence of a practical exercise. Having a hands-on lab would have enhanced the learning experience and complemented the theoretical knowledge offered.

### Challenges

A lot of new terms and terminologies and technologies to follow was little overwhelming.

### Screenshots

|  |
| --- |
| No screenshot available for this lab. |

----------------

## Lab work 10

### Introduction

This set of lab work dealt with cloud computing vulnerabilities, Cryptographic concepts, implementation, and detection.

### Learning outcomes

The lab session had a combination of theory and practice. Most of it was theoretical, covering topics like cloud computing and cryptography concepts, which gave me a solid understanding. Fortunately, there was also a practical lab where we focused on hashing and encrypting files.

Personally, I wish there was more emphasis on the practical side, but I believe the theoretical knowledge gained will be beneficial when it comes to implementing cloud computing and encryption in real-world scenarios. I hope to apply what I've learned effectively in practical situations.

### Challenges

It was challenging to understand the concept of cryptography and related terminology.

### Screenshots

|  |
| --- |
| Fig 1. Comparing hash value when made changes to the original text  Fig 2. scan for spyware using superantispyware |

# Conclusion

# In general, my experience with the lab sessions has been positive and fruitful. The exercises are well-constructed, and the instructions are clear. However, there were occasional disconnects between hands-on practice and theoretical concepts. Despite this, the labs offered valuable insights into real-world practices, providing a practical perspective.

# While facing technical challenges like machine lag and reboots, I successfully completed all tasks. I appreciate the instructors for the opportunity to learn through these labs. The Precipio learning environment's accessibility and content quality have been crucial. This course has equipped me with significant cybersecurity knowledge and practical experience.