|  |  |  |  |
| --- | --- | --- | --- |
|  | TO00BR92-3003  Network and Application Security |  | 1 (14) |
|  |  |
|  |  |
| Anup Nepal | 3.11.2023 |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |  |

Practice Lab work- Report-1

(Anup Nepal)

Table of Contents

[1 Introduction 3](#_Toc150002147)

[2 Methodology 3](#_Toc150002148)

[3 Practice Lab 3](#_Toc150002149)

[3.1 Lab work 1 3](#_Toc150002150)

[3.1.1 Introduction 3](#_Toc150002151)

[3.1.2 Learning outcomes 3](#_Toc150002152)

[3.1.3 Challenges 3](#_Toc150002153)

[3.1.4 Screenshots 4](#_Toc150002154)

[3.2 Lab work 2 4](#_Toc150002155)

[3.2.1 Introduction 4](#_Toc150002156)

[3.2.2 Learning outcomes 4](#_Toc150002157)

[3.2.3 Challenges . 4](#_Toc150002158)

[3.2.4 Screenshots 5](#_Toc150002159)

[3.3 Lab work 3 7](#_Toc150002160)

[3.3.1 Introduction 7](#_Toc150002161)

[3.3.2 Learning outcomes 7](#_Toc150002162)

[3.3.3 Challenges 7](#_Toc150002163)

[3.3.4 Screenshots 8](#_Toc150002164)

[3.4 Lab work 4 10](#_Toc150002165)

[3.4.1 Introduction 10](#_Toc150002166)

[3.4.2 Learning outcomes 10](#_Toc150002167)

[3.4.3 Challenges 10](#_Toc150002168)

[3.4.4 Screenshots 10](#_Toc150002169)

[3.5 Lab work 5 12](#_Toc150002170)

[3.5.1 Introduction 12](#_Toc150002171)

[3.5.2 Learning outcomes 12](#_Toc150002172)

[3.5.3 Challenges 12](#_Toc150002173)

[3.5.4 Screenshots 12](#_Toc150002174)

[4 Conclusion 14](#_Toc150002175)

# Introduction

This report is the first part of lab work which consists of ten 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 1

### Introduction

This lab work focuses on ethical hacking concepts.

### Learning outcomes

I learned about the fundamentals of information security, the Cyber Kill Chain, hacking concepts, ethical hacking, information security controls, and the laws and standards that govern this field. Overall good module for building my foundational knowledge regarding ethical hacking and somewhat prepare myself for the upcoming technical assignments.

### Challenges

The lab work had no challenges whatsoever.

### Screenshots

|  |
| --- |
| There are no screenshots for this module. |

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

## Lab work 2

### Introduction

This lab work consists of lab regarding techniques foot printing and reconnaissance, tools, and techniques for vulnerability scanning.

### Learning outcomes

During this lab work, I was able to explore various techniques for foot printing, which is essentially the process of gathering information about a target for security assessment. I learned to use Google Advanced Search Operators to search for information, leverage web services like Opencorporates, and inspect source code to uncover details about the target. I also used Archive.org to access historical data, created a wordlist using CeWL for potential password attacks, and performed banner grabbing with Nmap to identify vulnerabilities. Additionally, I utilized Whois to obtain domain ownership information and conducted DNS footprinting using Nslookup and Dnsenum to reveal valuable DNS records. To understand network infrastructure better, I employed Network Topology Mapper and Advanced IP Scanner.

In conclusion, this lab work has equipped me with a strong foundation in footprinting techniques. I have gained a deeper understanding of how to gather and analyze information about a target, which is crucial for strengthening the security posture of organizations and enhancing my capabilities as a cybersecurity practitioner. These skills are not only valuable for assessments but also for safeguarding digital assets and systems from potential threats and vulnerabilities.

### Challenges No significant challenges during this lab works other than overwhelming number of resources to implement and understand them.

### Screenshots

|  |
| --- |
| Fig 1. Recon using google dorks: resulting in pdf file with the title cybersecurity |
| Fig 2. footprint using webservice\_example\_opencorporates |
| Fig 3. snapshot of Microsoft web page from 25 Jan 2002 using archive.org |
| Fig 4. Scanning the network using advanced ip scanner  Fig 5. DNS enumeration using dnsenum command in linux |

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

## Lab work 3

### Introduction

This set of lab work dealt with Network resource discovery methods, different kind of network enumeration techniques and countermeasures.

### Learning outcomes

During this phase of my learning journey, I explored a wide range of network scanning and enumeration techniques, using tools like SuperScan, Nbtstat, Nmap, IP Network Browser, Snmp-check, and Softerra LDAP Administrator. These methods allowed me to uncover valuable information about network resources, services, and devices. Additionally, I learned about strategies to prevent DNS, Windows, FTP, and SMTP enumeration, which are essential for safeguarding network security. This learning experience has equipped me with valuable skills and knowledge to enhance network defense and protect against potential threats and vulnerabilities.

### Challenges

Not many technical issues, however, the volume of exercise and amount of information was incredibly overwhelming.

### Screenshots

|  |
| --- |
| Fig 1. Using hping3 to determine open ports on target using syn flag Fig 2. Discovering the network and drawing the network topology with the Dude app  Fig 3. Using nbtstat with flag c \_ result display the cache name table which display name and IP address of the remote system    Fig 4. SMB NetBIOS enumeration  Fig 5. Performing DNS Enumeration using ‘host’ command in kali  Fig 6. Service policy change to allow SNMP packets from any host |

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

## Lab work 4

### Introduction

This set of lab work dealt with vulnerability scanning and assessment and system hacking and manipulation.

### Learning outcomes

In this lab on, I gained a comprehensive understanding of the process and its significance in cybersecurity. I learned to use tools like Nikto and Lynis for web server and system vulnerability scanning, as well as creating formatted reports to communicate findings effectively. The lab work has broadened my knowledge on various aspects, including vulnerability classification, assessment types, specialized assessments, and the importance of standardized systems like CVE and CVSS. I also acquired practical skills, such as disabling the Windows 10 Firewall and using tools like wordlists and Hydra for username and password guessing. This knowledge has equipped me to identify and mitigate vulnerabilities effectively, emphasizing the importance of continuous assessment to enhance security measures.

### Challenges

There were not so many challenges other than occasional lagging with the devices in virtual environment.

### Screenshots

|  |
| --- |
| Fig 1. Nikto Scan result  Fig 2. Password cracking using hyda with previously created wordlist  Fig 3. Using lynis for system vulnerability scanning to perform security auditing. |

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

## Lab work 5

### Introduction

This set of lab work dealt with implementing malware concepts and the task related to malware analysis.

### Learning outcomes

In this lab work, I had an opportunity to explore the world of malware, its analysis, and countermeasures. I learned to create a basic virus (fork bomb) and employ various tools, including Windows Defender, online anti-malware scanners, and SUPERAntiSpyware for malware detection and removal. Additionally, I expanded my knowledge of advanced topics like Advanced Persistent Threats (APTs), malware analysis methods, detection techniques, and countermeasures. This module equipped me with valuable skills and insights to identify, combat, and protect against malware threats, contributing to the security of digital assets and systems.

### Challenges

There were not so many challenges other than occasional lagging with the devices in virtual environment.

### Screenshots

|  |
| --- |
| Fig 1. Created a filebomb virus to observe the CPU process  Fig 2. scan for spyware using superantispyware  Fig 3. Scanning for malware using Microsoft online tool. |

# Conclusion

My experience with the lab sessions has been quite positive overall. The lab exercises are of high quality, and the instructions provided are clear and effective. However, there have been occasional gaps between the practical hands-on experience and the underlying concepts being taught. Nevertheless, these labs have provided valuable insights into real-world practices, offering a practical perspective on how things are executed.

Along the way, I did encounter some technical challenges such as machine lag, booting issues, and mid-exercise reboots. Despite these challenges, I am pleased to report that I was able to complete all the tasks.

I want to express my gratitude to the instructors for giving me the opportunity to engage in and learn from these lab exercises. The Precipio learning environment, with its accessibility and content quality, has been a significant asset. Through this course, I have gained substantial knowledge, and the hands-on lab work has allowed me to gain practical experience in the field of cybersecurity.