|  |  |  |  |
| --- | --- | --- | --- |
|  | TO00BR92-3003  Cybersecurity Analyst |  | 1 (14) |
|  |  |
|  |  |
| Anup Nepal | 10.10.2023 |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |  |

Practice Lab work- Report-1

(Anup Nepal)

Table of Contents

[1 Introduction 3](#_Toc148038888)

[2 Methodology 3](#_Toc148038889)

[3 Practice Lab 3](#_Toc148038890)

[3.1 Lab work 1 3](#_Toc148038891)

[3.1.1 Introduction 3](#_Toc148038892)

[3.1.2 Learning outcomes 3](#_Toc148038893)

[3.1.3 Challenges 4](#_Toc148038894)

[3.1.4 Screenshots 4](#_Toc148038895)

[3.2 Lab work 2 8](#_Toc148038896)

[3.2.1 Introduction 8](#_Toc148038897)

[3.2.2 Learning outcomes 8](#_Toc148038898)

[3.2.3 Challenges 8](#_Toc148038899)

[3.2.4 Screenshots 8](#_Toc148038900)

[3.3 Lab work 3 11](#_Toc148038901)

[3.3.1 Introduction 11](#_Toc148038902)

[3.3.2 Learning outcomes 11](#_Toc148038903)

[3.3.3 Challenges 11](#_Toc148038904)

[3.3.4 Screenshots 11](#_Toc148038905)

[4 Conclusion 14](#_Toc148038906)

# Introduction

This report is the first part of lab work which consists of six different lab exercises grouped under 3 lab sessions, completed in a period of a month or so. This report summarizes the introduction of lab work, 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 system and network security implementation concepts, threat intelligence and threat gathering concepts.

### Learning outcomes

This lab work had many intriguing elements, and it was great to practice them. First, I had to learn and get comfortable with Splunk, a data analysis tools aiding SIEM system. It was also interesting to see and practice encrypting disks with BitLocker and using multifactor authentication. During the lab work, I also got to learn various ways to gather information from the internet, such as using OSINT tools and frameworks. I learned about MITRE frameworks and got a basic understanding of honeypots and how they are set up. Additionally, this was my first time using the Windows Event Viewer, and the knowledge I gained can be applied to everyday computing.

### Challenges

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

### Screenshots

|  |
| --- |
| Fig 1. Installation of Splunk with password. |
| Fig 2. Setting up firewall rules to allow splunk to listen to port 9997    Fig 3. Events logs successfully imported to the Splunk enterprise application.  Fig 4. Installing BitLocker from server manager  Fig 5. The D: volume drive has been encrypted using BitLocker.    Fig 6. Security log from Event viewer.  Fig 7. A popular internet registry which resolves the domain name    Fig 8. Honeypot setup diagram |

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

## Lab work 2

### Introduction

This lab work consists of lab regarding techniques to determine malicious activity, tools, and techniques for vulnerability scanning.

### Learning outcomes

Building on my previous lab work, where I discovered the Event Viewer and explored the analysis of different system logs, this set of lab exercises offered a comprehensive overview. I gained valuable insights into auditing login events, log generation for subsequent assessment, and the creation of scripts to monitor failed logins on both my own computer and remote machines. Furthermore, it was crucial to understand how to prevent brute force attacks, which this exercise skillfully demonstrated by enabling account locking after a certain number of attempts.  
The second lab exercise shifted the focus to active vulnerability scanning tools like Nmap, Nessus, and Metasploit. It was fascinating to realize the scope of capabilities these tools offer and the various reconnaissance tasks they can accomplish. Lastly, revisiting the use of Wireshark for network activity analysis provided a solid review of this essential skill.

### Challenges Although not overly challenging, there were instances where I faced difficulties understanding the sequence of exercises and dealing with technical issues in this set of lab work. I had to make several attempts to get the machine to start up, and there were frequent occasions when the machine became unresponsive, forcing a restart.

### Screenshots

|  |
| --- |
| Fig 1. Applying the prevention measure to stop brute force attack. |
| Fig 2. Script to monitor failed logon on remote commuter. |
| Fig 3. Monitoring the failed attempts having code 4625 using PowerShell script. |
| Fig 4. Nmap scanning using different flags: in this case flag -A.  Fig 5. Scan report from Nessus showing different severity of vulnerabilities. |

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

## Lab work 3

### Introduction

This set of lab work dealt with identifying and analyzing malicious activity and different tools used for the identification and analysis.

### Learning outcomes

The primary takeaway from this lab exercise was realizing the extensive monitoring capabilities provided by the built-in Task Manager. I had used it previously for basic tasks like observing processes, enabling, or disabling database servers, and ending unresponsive tasks. However, upon completing the lab work, I discovered its potential to effectively monitor system anomalies. This was equally enlightening when applied in a Linux environment using command-line tools, which was a new experience for me. Additionally, detecting unauthorized user privilege escalation through the Event Viewer was a valuable addition to my skillset.

The second part of the lab centered on network monitoring, and once again, it was intriguing to explore the multitude of tasks achievable through Wireshark. This included modifying headers, filtering results, and more. Lastly, practicing the monitoring of malicious files within a sandbox environment was a beneficial exercise.

The only limitation I encountered in this lab exercise, especially when monitoring malicious files on a computer, was the inability to pinpoint which specific file was causing the issue. While system monitoring can alert me to potential problems, perhaps, identifying the root cause might require more intensive research and observation, potentially using OSINT tools.

### Challenges

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

### Screenshots

|  |
| --- |
| Fig 1. Using sandbox to explore malicious files.  Fig 2. Customizing the Wireshark.    Fig 3. Monitoring the process activity using Sysinternal.  Fig 4. Observing the event and it shows that administrator account has created another user with administrative privilege — privilege escalation  Fig 5. Monitoring Linux system using htop application. |

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

# Conclusion

I've had a highly positive experience with the lab sessions. The quality of these lab exercises is commendable, and the instructions provided are clear and effective. However, there are occasional gaps between the practical hands-on experience and the underlying concepts being conveyed. Nonetheless, these labs have given me valuable insights into real-world practices, offering a perspective on how things are executed in practical scenarios.

Along the way, I encountered some technical challenges such as machine lag, booting issues, and mid-exercise reboots. Despite these hurdles, I'm pleased to report that I managed to complete most of the tasks, with a few exceptions.

I extend my sincere gratitude to the teachers for granting 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've gained substantial knowledge, and the lab work has allowed me to gain hands-on experience in the cybersecurity domain.