|  |  |  |  |
| --- | --- | --- | --- |
|  | TO00BR92-3003  Cybersecurity Analyst |  | 1 (12) |
|  |  |
|  |  |
| Anup Nepal | 22.11.2023 |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |  |

Practice Lab work- Report-2

(Anup Nepal)

Table of Contents

[1 Introduction 3](#_Toc151680267)

[2 Methodology 3](#_Toc151680268)

[3 Practice Lab 3](#_Toc151680269)

[3.1 Lab work 1 3](#_Toc151680270)

[3.1.1 Introduction 3](#_Toc151680271)

[3.1.2 Learning outcomes 3](#_Toc151680272)

[3.1.3 Challenges 4](#_Toc151680273)

[3.1.4 Screenshots 4](#_Toc151680274)

[3.2 Lab work 2 6](#_Toc151680275)

[3.2.1 Introduction 6](#_Toc151680276)

[3.2.2 Learning outcomes 6](#_Toc151680277)

[3.2.3 Challenges 6](#_Toc151680278)

[3.2.4 Screenshots 6](#_Toc151680279)

[3.3 Lab work 3 8](#_Toc151680280)

[3.3.1 Introduction 8](#_Toc151680281)

[3.3.2 Learning outcomes 8](#_Toc151680282)

[3.3.3 Challenges 8](#_Toc151680283)

[3.3.4 Screenshots 8](#_Toc151680284)

[3.4 Lab work 4 10](#_Toc151680285)

[3.4.1 Introduction 10](#_Toc151680286)

[3.4.2 Learning outcomes 10](#_Toc151680287)

[3.4.3 Challenges 10](#_Toc151680288)

[3.4.4 Screenshots 10](#_Toc151680289)

[4 Conclusion 12](#_Toc151680290)

# Introduction

This report is the first part of lab work which consists of six different lab exercises grouped under 4 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 attack methodology frameworks and vulnerability data analysis and prioritization.

### Learning outcomes

In this module, I learned to navigate the MITRE ATT&CK Framework, gaining insights into the Cyber Kill Chain and the Diamond Model of Intrusion Analysis. Engaging with the OWASP Testing Framework honed my skills in detecting web server vulnerabilities, emphasizing the importance of proactive cybersecurity measures. The Common Vulnerability Scoring System (CVSS) Calculator exercise provided hands-on experience in assessing vulnerability severity and making informed decisions on issue prioritization. Lastly, the exercise on detecting web application vulnerabilities improved my ability to systematically address security issues in real-world scenarios. Overall, this module significantly enhanced my understanding of attack methodology frameworks and practical skills in vulnerability detection, contributing to my overall competence in the field of cybersecurity.

### Challenges

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

### Screenshots

|  |
| --- |
| Fig 1. Using MITRE attack navigator to determine which type of attacks a specific threat actor conduct. In this example, the APT19 threat group was selected. |
| Fig 2. Searching for vulnerabilities for the apache server implemented in the target system & turns out the mentioned version has known vulnerabilities    Fig 3. Web application scan result showing different severity level using Nessus    Fig 4. Simulating a vulnerability to measure the CVSs score with the set of matrices |

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

## Lab work 2

### Introduction

This lab work consists of lab regarding incident response management techniques and incident response communication and reporting.

### Learning outcomes

During this lab session, I learned to implement structured incident response strategies by exploring the NIST Incident Handling Guide, CISA Cybersecurity Incident & Vulnerability Response Playbook, and Microsoft Incident Response Playbooks. Through practical exercises, I was able to navigate Splunk for real-time threat detection, install the necessary components, and identify port scanning incidents effectively. Additionally, I acquired hands-on experience in forensic investigation, understanding the creation and analysis of forensic images using the OS Forensics Application.

Furthermore, I expanded my knowledge of coordination and information sharing, as well as reporting protocols, by reviewing guidelines from NIST, CISA, and federal incident notification standards. This lab enhanced my ability to generate required reports and understand the implications of the security cost, emphasizing the critical role accurate reporting plays in mitigating the impact of cybersecurity incidents.

Overall, I've significantly advanced my skills in incident response, threat detection, and reporting, contributing to a more robust cybersecurity skill set.

### Challenges Not so technically challenging other than overwhelming amount of information to absorb.

### Screenshots

|  |
| --- |
| Fig 1. CISA - report a cyber issue (picture showing one of the type) |
| Fig 2. Information security incident report template for Enterprise. |
| Fig 3. Splunk log report.  Fig 4. Setting up a new case for forensic image for investigation |

## Lab work 3

### Introduction

This set of lab work dealt with vulnerability reporting concepts.

### Learning outcomes

In this lab, I strengthened my skills in log collection and vulnerability reporting using Splunk. The hands-on experience began with installing and configuring the Splunk Enterprise Application, followed by setting up a Splunk Client for seamless communication. I learned to effectively use Splunk Enterprise to gather and analyze logs, providing valuable insights into system and application activities.

Furthermore, the lab work extended my capabilities to vulnerability reporting, demonstrating how to generate comprehensive reports with Splunk. This not only enhanced my technical proficiency but also emphasized the proactive role Splunk plays in identifying and addressing potential security vulnerabilities within IT infrastructures. Overall, the module deepened my understanding of Splunk's capabilities, making it a powerful tool for robust log management and insightful vulnerability reporting.

### Challenges

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

### Screenshots

|  |
| --- |
| Fig 1. Splunk enterprise capturing the log events from remote computer  Fig 2. Created a dashboard from the logs containing the errors occured in past 24 hours    Fig 3. Setting up firewall rules to ensure the traffic can be received on the port |

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

## Lab work 4

### Introduction

This set of lab work dealt with vulnerability patching and attack surface management.

### Learning outcomes

In this final lab, I learned to implement Windows and Linux patch management techniques. The emphasis was on creating a production workstation, providing valuable insights into the fundamental elements of an effective update environment. As I progressed, configuring a windows workstation update group policy deepened my understanding of customizing and managing update policies within a Windows environment. The exploration of Linux patch management techniques expanded my skills, particularly in creating an update Script and implementing a scheduled update task. Through these exercises, I learned how to orchestrate systematic and efficient patch management processes for both Windows and Linux systems. This lab session highlighted the importance of maintaining up-to-date systems for optimal performance and security in diverse production environments, enriching my understanding of effective patch management strategies.

### Challenges

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

### Screenshots

|  |
| --- |
| Fig 1. Writing an update script  Fig 2. Create an organizational unit and added a win11 workstation into it from Active directory Users and computers    Fig 3. A Group Policy has been created to ensure the Production Workstations will check and install Windows Updates every Friday at 16 |

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

# Conclusion

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

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

I extend my sincere gratitude to the instructors 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 proven to be a significant asset. Through this course, I've acquired substantial knowledge, and the lab work has allowed me to gain practical, hands-on experience in the cybersecurity domain.