|  |  |  |  |
| --- | --- | --- | --- |
|  | TO00BR94-3003 System Security |  | 1 (17) |
|  |  |
|  |  |
| Anup Nepal | 16.4.2023 |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |  |

Practice Lab work- Part 2

(Anup Nepal)

Table of Contents

[1 Introduction 3](#_Toc132745972)

[2 Methodology 3](#_Toc132745973)

[3 Practice Labs 3](#_Toc132745974)

[3.1 Lab work 5 3](#_Toc132745975)

[3.1.1 Introduction 3](#_Toc132745976)

[3.1.2 Learning outcomes 3](#_Toc132745977)

[3.1.3 Challenges 4](#_Toc132745978)

[3.1.4 Screenshots 4](#_Toc132745979)

[3.2 Lab work 6 6](#_Toc132745980)

[3.2.1 Introdcution 6](#_Toc132745981)

[3.2.2 Learning outcomes 6](#_Toc132745982)

[3.2.3 Challenges 6](#_Toc132745983)

[3.2.4 Screenshots 6](#_Toc132745984)

[3.3 Lab work 7 9](#_Toc132745985)

[3.3.1 Introduction 9](#_Toc132745986)

[3.3.2 Learning outcomes 9](#_Toc132745987)

[3.3.3 Challenges 10](#_Toc132745988)

[3.3.4 Screenshots 10](#_Toc132745989)

[3.4 Lab work 8 12](#_Toc132745990)

[3.4.1 Introdcution 12](#_Toc132745991)

[3.4.2 Learning outcomes 12](#_Toc132745992)

[3.4.3 Challenges 13](#_Toc132745993)

[3.4.4 Screenshots 13](#_Toc132745994)

[4 Conclusion 17](#_Toc132745995)

# Introduction

This report is the second part of lab work which consists of twelve different lab work performed over a period of a month. This report summarizes the introduction of lab work, process involved, learning reflections and challenges faced during the lab works and to validate the process, there are multiple screenshots attached.

In order to provide a clear description of the lab work, I have divided the lab works into four 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

The first thing I did before starting any lab work was to read through the instructions on how to use precipio lab environment provided by the teachers in canvas. After the initial setup, all lab assignments were completed by following the instructions of Precipio lab environment. Before jumping directly into the tasks, I have gone through the introduction, objectives, observe the lab diagram and the background of the topic so that I get an overview of the kind of tasks that I will be carrying out.

# Practice Labs

## Lab work 5

### Introduction

This lab work focuses on managing remote desktop, role-based security and configuring MBSA Scanner. Since it was the first time, I had to spend some additional time to observe and understand the precipio lab environment.

### Learning outcomes

The key learning outcome of this lab was to explore different tools used to establish remote connections between two devices both using remote desktop and PowerShell. Furthermore, I learned how to do the quick config for allowing a firewall exception in order to establish a communication to the other remote computer. Moreover, I learned to create a custom security role and scope, learned to create a user with administrative rights using configuration manager console. The last lab in this set of lab work has broadened my understanding of MBSA Scanner to configure, scan and analyze the results using Microsoft baseline security analyzer. This lab work helps to visualize what we I have been studying about vulnerabilities, as there were exercises in this lab where I had to analyze and implement some remedies to nullify the found vulnerability.

### Challenges

There were not so many challenges other than trying to figure out what is happening and why some things are happening the way they are. The lab, as I have mentioned in earlier report as well, lacks the explanation of things, we mostly follow the instructions, at times it is difficult to figure out why something is happening.

### Screenshots

|  |
| --- |
| Graphical user interface, application  Description automatically generated |
| Graphical user interface, text, application  Description automatically generated |

|  |
| --- |
| Graphical user interface, application  Description automatically generated |
| A picture containing text, screenshot, monitor  Description automatically generated |

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

## Lab work 6

### Introdcution

This lab work consists of lab regarding compliance patching, passive topology discovery, scanning and remediating vulnerabilities with OpenVAS.

### Learning outcomes

I must admit that this set of labs was difficult for me to understand both theoretically and practically. I have completed the compliance patching; however, the other two labs had some issues, and I could not complete it. It is difficult for me to write about this part, reason being difficult to understand and unable to complete whole lab. However, having gone through the exercise, I was able to observe how patching is done using WSUS, configure disk storage for WSUS and some general understanding of windows server manager. The other exercise related to passive topology discovery was relatively easier to follow as I had to use Wireshark which I was somewhat familiar with. It was interesting to observe how the device communicates behind the scenes in a network. The last lab, I follow the instructions until the point the system stopped working, honestly, I don’t have anything that I can write except that the tool used in the lab did some vulnerabilities scanning and I was able to see the severity of them.

### Challenges

As mentioned earlier, I had issue with understanding the flow of the exercises and technical issues throughout this set of lab work. I had to try multiple times so that the machine starts up and there were many times the machine stops responding and I had to start over again. For Wireshark, the packet capture never stopped in my case, it kept on capturing and I could not move forward as per the instructions. In the OpenVAS exercise, I was following the instructions until the point I got and error while trying to download some file from windows server 2012 (picture attached). As a result, I could not complete this lab work till the end.

### Screenshots

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |
| Graphical user interface, application  Description automatically generated |
| Graphical user interface, text, application  Description automatically generated  Text  Description automatically generated |
| Graphical user interface, text, application  Description automatically generated |

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

## Lab work 7

### Introduction

This set of lab work dealt with installing Kali Linux, implementing backup and recovery and installation and verification of snort. The first two labs are completed and the third I was not able to complete, I will explain the reason in the following section.

### Learning outcomes

The first lab work to install kali was quite straightforward and I was able to do it easily. I have done this previously on several occasions, only difference was this time the installation was done on Hyper-V as opposed to virtual box. From the second lab exercise, I learned to allocate the disk for data protection manager and create protection group and adding members to the group. The third lab about configuring the snort provided me with an opportunity to observe how different rules are configured for the purpose of network intrusion detection and prevention.

### Challenges

There was hardly any challenge for the first and second lab, it went smoothly. However, in the third lab, I had to face technical issues, the machine kept misfunctioning after I reached a certain point in the exercise. In any case, I was following the instruction and completing the exercises as much as possible. Als, the third lab was a bit difficult to follow conceptually, there were many commands and rulesets that were provided in the instructions I was following them blindly.

### Screenshots

|  |
| --- |
| Graphical user interface, text  Description automatically generated  Graphical user interface, text, application, email  Description automatically generated  Graphical user interface, text, application, email  Description automatically generated |

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

## Lab work 8

### Introdcution

The last set of labs involved working with configuring and securing IIS, upgrading and securing SSH connection and Manual SQL Injection and password cracking.

### Learning outcomes

Finally, here comes the lab work, that was interesting, and I felt that I have learned something important. To start with, I learned about web server hosting and managing with IIS and how to configure them, manage permissions and so on for example allowed/denied IP addresses and allowed/deny keywords. The second lab about SSH helped to learn more about the SSH for example, how to install SSH, learned about running the SSH on services, adding sudo users and try to connect using SSH. Furthermore, I learned about the SSH key generation and changing the SSH port from 22 to some random port. The third lab allows me to practice my first ever SQL injection attack, I was very interested and excited to while doing this lab work.

### Challenges

Not many technical issues with this part but there were some minor issues with terminal and understanding CLI, but I overcame it quickly.

### Screenshots

|  |
| --- |
| Graphical user interface, application  Description automatically generated |

|  |
| --- |
| Table  Description automatically generated  Graphical user interface, text, application, email  Description automatically generated  Text  Description automatically generated |
| Graphical user interface  Description automatically generated  Graphical user interface, text  Description automatically generated  Text  Description automatically generated  Text  Description automatically generated |

# Conclusion

The overall experience of the lab has been very good for me. These lab works are of very high quality and the instructions are very good too. It is just that there is a knowledge gap between the practical hand-on and concepts it is trying to imply. It has shown me a way forward, provided me a perspective on how things are done in real life. There were some technical challenges on the way such as machine lagging, not booting up, rebooting in the middle of exercise and so on, I am happy that with all the struggle, I have managed to complete the task barring few.

My sincere thanks to the teachers for providing me with this opportunity to practice and learn these lab works. The precipio learning environment is good both with accessibility and quality of the contents. I feel that I have learned a lot during this course and the lab work helped me to get the feel of how it is to work in security domain. My only regret is, and it is because of personal reasons, I would have liked to spend more time and resources on this course as this course is of a very advanced level.