|  |  |  |  |
| --- | --- | --- | --- |
|  | TO00BR94-3003 System Security |  | 1 (21) |
|  |  |
|  |  |
| Anup Nepal | 5.3.2023 |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |  |

Practice Lab work

(Anup Nepal)

Table of Contents

[1 Introduction 3](#_Toc129032799)

[2 Methodology 3](#_Toc129032800)

[3 Practice Labs 3](#_Toc129032801)

[3.1 Lab work 1 3](#_Toc129032802)

[3.1.1 Introduction 3](#_Toc129032803)

[3.1.2 Learning outcomes 3](#_Toc129032804)

[3.1.3 Challenges 4](#_Toc129032805)

[3.1.4 Screenshots 4](#_Toc129032806)

[3.2 Lab work 2 6](#_Toc129032807)

[3.2.1 Introdcution 6](#_Toc129032808)

[3.2.2 Learning outcomes 6](#_Toc129032809)

[3.2.3 Challenges 7](#_Toc129032810)

[3.2.4 Screenshots 8](#_Toc129032811)

[3.3 Lab work 3 13](#_Toc129032812)

[3.3.1 Introdcution 13](#_Toc129032813)

[3.3.2 Learning outcomes 13](#_Toc129032814)

[3.3.3 Challenges 13](#_Toc129032815)

[3.3.4 Screenshots 13](#_Toc129032816)

[3.4 Lab work 4 17](#_Toc129032817)

[3.4.1 Introdcution 17](#_Toc129032818)

[3.4.2 Learning outcomes 17](#_Toc129032819)

[3.4.3 Challenges 18](#_Toc129032820)

[3.4.4 Screenshots 18](#_Toc129032821)

[4 Conclusion 21](#_Toc129032822)

# Introduction

This report is an outcome of twelves lab works 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 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 task 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 1

### Introduction

This was the first ever lab work for me and I was very excited to proceed with them. This lab work which focused on introduction to CISSP explaining different domains of CISSP, security and risk management and the lab work related to encryption and hashing. 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 takeaway from this first set of labs was to get the feel of how security professionals work and get familiar with the kinds of task the professionals must perform. The first provided me with good theoretical insights into the eight domains of CISSP, the second lab was a good revision of conceptual security and risk management concepts such as CIA, frameworks, governance, policies and so on. The last one was the actual practical lab where I had to work with remote machines, servers, installation of cryptography tool and learn to perform encryption/decryption and hashing. I had studied about cryptography, but this was good to observe how encryption/decryption and hashing is done and comparing different hashing algorithms using tools such as cryptoDemo and Hashcalc.

### Challenges

The first two labs were pretty straightforward as it was mostly reading about the concepts. However in the third lab where I had to connect to remote virtual machines, there were times that it was loading very slowly and a lot of lagging while trying to work on those machines.

### Screenshots

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

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

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

Graphical user interface, text, application, email

Description automatically generated

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

## Lab work 2

### Introdcution

This lab work that I had completed within this sets were related to SCCM configuration items and baselines, implementing two factor authentication, implementation of OpenPGP for email encryption.

### Learning outcomes

Among many other things that I have learned during this lab work, getting to know how the server computer works and how we can configure, set policy rules and getting to observe and use configuration manager tool for managing all the settings were the key learning for me from the first lab work.

The second lab work was to implement openPGP by using windows PowerShell and Gpg4win tool. The exercise taught me little bit of PowerShell, how I can access the application from one machine to another machine and perform the installation. Moreover, I learned how to create the certificate, digital signature in order to encrypt the email.

The third lab was to implement two factor authentication using google authenticator. I know about the two-factor authentication and have been using it in my day-to-day life, so I was very excited to see how this lab turns out to be. However, I was unable to complete the lab work as I was not able to install the libpam-google-authenticator using kali Linux. There was an issue with some dependencies and it did not allow to install, as a result I could not complete this lab.

### Challenges

As mentioned earlier, I had issue with downloading the required application to complete the task. Apart from this issue, I also had an issue with a virtual machine (PLABCAS01), the task required me to download the Gpg4win application using the PLABCAS01, however, it was not possible for me to connect in my lab environment. I then decided to perform the same task in another machine, and it worked, and I was able to complete the lab.

Other than technical issues, these lab works were a bit advanced for my level of understanding and I was having some difficulties to follow and understand what is happening behind the scenes. As I am following the instructions rigorously, at time it felt like what am I doing and what is happening with whatever I am doing.

### Screenshots

|  |
| --- |
| Graphical user interface, text  Description automatically generated |
| Graphical user interface, text  Description automatically generated |
| A screenshot of a computer  Description automatically generated  Graphical user interface, text, application, Word  Description automatically generated |
| Graphical user interface  Description automatically generated Graphical user interface, text, application, email  Description automatically generated |
| Graphical user interface, text  Description automatically generated |

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

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

## Lab work 3

### Introdcution

This set of lab work dealt with SSL VPN using ASA device manager, configuring access lists in both ipv4 and ipv6, configuring Ip tables. I was only able to complete the first two labs, in the last lab I was not able to download the application. I will explain more in challenges section about this.

### Learning outcomes

The key learning for me from the first lab work was that I was able to gain understanding on how VPN works, how to configure it based on policies such as clientless and AnyConnect. I believe these are very fundamentals skills required to be in the security profession and I was very happy to have learned something new.

In the second lab, I had to configure a router with both standard and extended numbered access-lists for ipv4 and configure also the ipv6 access lists. I had previously done some lab work related to this in cisco packet tracer, so I find this lab work relatively easy to follow and a good revision and addition to my previous knowledge of access lists.

I went through the instructions and tasks details for the third lab; however, I was not able to complete. I would have learned about the iptables in Kali Linux in this lab. Even though I was not able to download putty in Kali Linux, I learned that there are other better ways to do ssh connections then using putty.

### Challenges

I had to go through both technical and theoretical knowledge challenges during this lab work. The technical challenges were with the third lab where I had to install putty in Kali Linux, which failed multiple times.

As mentioned earlier, I was very excited about the VPN connection lab, and I have apparently learned something regarding to VPN connections. The instructions were very lengthy, and I was blindly following the instructions without knowing much about what is happening. Since this is advanced course, and I genuinely want to gain hand on skills, but it felt that I am just doing as instructed without understanding much.

### Screenshots

|  |
| --- |
| Text  Description automatically generated |

|  |
| --- |
| A screenshot of a computer  Description automatically generated  Graphical user interface, text, application, email  Description automatically generated  Graphical user interface, text, application  Description automatically generatedGraphical user interface, text, application  Description automatically generated  Graphical user interface, application  Description automatically generated |

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

## Lab work 4

### Introdcution

The set of labs involved working with windows command line, administering and deploying endpoint protection and implementing bit locker on portable media.

### Learning outcomes

The first lab work was quite straightforward and something I knew already. I had to use various networking command line tool to observe the networking activities and configuration. I have had used many tools earlier, however there were few commands which were new to me and it was good that I learned about them as well.

The second lab was challenging, interesting and something new for me. I learned what endpoint is, I had an opportunity to learn to use configuration manager to configure endpoint protection site system role. Also I kind of learned the ways to configure and deploy policies for endpoint protection such as antimalware policies. In short, I was able to get an insight into the job of an administrator or security practitioner and how one can implement different rules and policies for client computer.

The third lab was also very interesting for me as it dealt with the partition of hard disk and encrypting a hard drive using bit locker. I believe I have learned how it is done and I might perhaps try to do it in my virtual machine to gain more practice.

### Challenges

Not much of technical issues with this part but again, too many new concepts and so many steps to follow to accomplish some tasks, which was difficult to understand without knowing any context on what and why we need to do something.

### Screenshots

|  |
| --- |
| Graphical user interface, text, application, chat or text message  Description automatically generated |

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

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

# Conclusion

Overall experience is good for me so far. These lab works are of very high quality and the instructions are very good too. It just that there is a knowledge gap between the practical hand-on and concepts it is trying to imply. I am sure these lab work will not make me an expert, however it has shown me a way forward, provided me a perspective on how things are done in real life. It is well known to everyone about the technical glitches, I have kind of adapted to that one now. Looking forward to completing more labs in coming weeks.