Basic knowledge assignment

**Made by** Tim Chermin

**Version:** 1.0

**Date:** 13/02/2020

Table of Contents

[Version 3](#_Toc32483469)

[Introduction 4](#_Toc32483470)

[Demo and Test Environment 4](#_Toc32483471)

[Test and Analysis results (Screenshots and explanation of all working solutions, like): 4](#_Toc32483472)

[Overall Conclusion 5](#_Toc32483473)

[Reflection 5](#_Toc32483474)

# Version

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Autor** | **Date** | **Changes** | **Time spend** |
| 1.0 | Tim Chermin | 13/02/2020 | * Basic setup | 10 min |
| 1.1 | Tim Chermin |  |  |  |
| 1.2 | Tim Chermin |  |  |  |

# Introduction

Before this semester I had some prior knowledge and experience on security, Linux and networking. Since I already did the CSA course. But I didn’t know a lot about defending and because of this my preferred learning style was the style for beginners (style 1) since I liked this a lot when I did CSA. In this document I have written down everything I learned and how I learned it. This was mostly done by following the instructions of the subjects and a lot of trial and error when trying things out myself.

My goal was to learn the basics of defending and try to use the knowledge I gained from the CSA course.

# Demo and Test Environment

Build (Implementation details and essential configurations for each basic knowledge theme):

* Threat Analysis
* IP-address plan and network drawing reflecting your own demo network
* Firewall settings and rules necessary
* Secure Network Connections needed
* Secure Remote Access and Management (VPN settings)
* Intrusion Detection rules
* IT monitoring configuration
* User and management accounts for role based access (System security)

# Test and Analysis results (Screenshots and explanation of all working solutions, like):

* Basic functioning of internal and public functionality/services (securely)
* Inbound and outbound firewall filtering (examples of both access and blocking of communication).
* VPN access and secure remote management of DMZ and LAN servers
* IDS functioning: show/prove for detections of intrusions, attempts, scans, attacks, abuse, malware that you wanted to detect.
* How should Incident Management (concepts) be set up if this was a real company
* Monitoring: Show that good and bad statuses of your IT environment can be monitored in a SOC-like environment
* What are the results of your IT Risk Analysis (qualitative)
* Is user management (System Defence) correctly implemented?

# Overall Conclusion

* Conclusions on the accomplished level of security for the company, and an advice for remaining improvements of the security for the company.

# Reflection

* Critical reflection on the results of your own learning process thus far.
* How was your Pro-active attitude (being present, taking initiative) towards the basic knowledge and the project activities
* How did you communicate with teachers, fellow students, experts (presenting, advising, inquiring and eventual reporting)