

Personal Development Portfolio



Javier Duran

Student Number: 3567885

Infrastructure Engineering

Tutor: Mikaeil Shaghelani

Table of Contents

INTRODUCTION	5
PURPOSE	5
OBJECTIVES	5
1.0 PROGRAMMING FOR INFRASTRUCTURE	6
1.1 WRITING CODE	6
1.2 FUNCTIONS	6
1.3 CLASSES	7
1.3.1 EVIDENCE	8
1.4 OS MODULE	8
1.4.1 EVIDENCE	9
1.5 SQLITE	9
1.6 TKINTER	10
1.6.1 EVIDENCE	10
1.7 FLASK MICROFRAMEWORK	11
1.7.1 EVIDENCE	11
1.8 DBMS	12
1.9 HEROKU	12
1.10 REFLECTION & SELF EVALUATION	12
2.0 MANAGING INFRASTRUCTURE	13
2.1 AGILE PROJECT MANAGEMENT	13
2.1.1 EVIDENCE	14
2.2 ITIL	14
2.2.1 EVIDENCE	15
2.3 SECURITY MANAGEMENT	15
2.4 GDPR	16
2.5 REFLECTION & SELF EVALUATION	16
3.0 SECURING INFRASTRUCTURE	16

3.1	FIREWALL	17
3.1.1	EVIDENCE	18
3.2	SECURE NETWORK PROTOCOLS	18
3.3	BACKUPS	19
3.4	IDS/IPS	19
3.4.1	EVIDENCE	20
3.5	SNORT	20
3.6	FORENSICS	21
3.7	PEN-TESTING	21
3.7.1	EVIDENCE	22
3.8	REFLECTION & SELF EVALUATION	22
4.0	CONNECTING INFRASTRUCTURE	22
4.1	ACTIVE DIRECTORY	23
4.2	DHCP	23
4.2.1	EVIDENCE	24
4.3	BASH	24
4.3.1	EVIDENCE	25
4.4	HIGH AVAILABILITY	25
4.5	LDAP	26
4.5.1	EVIDENCE	26
4.6	REFLECTION & SELF EVALUATION	27
5.0	PROVISIONING INFRASTRUCTURE	27
5.1	HYPER-V	27
5.2	VPN	28
5.3	PROXY	28
5.4	RADIUS	29
5.4.1	EVIDENCE	29
5.5	DOCKER	29
5.5.1	EVIDENCE	30
5.6	REFLECTION & SELF EVALUATION	30
6.0	PERSONAL LEADERSHIP	31
7.0	PROBLEM SOLVING	31

8.0	FUTURE-ORIENTED ORGANIZATION	31
9.0	TARGETED INTERACTION	32
	CASE STUDY	32
	CASE STUDY 2	33
	CONCLUSION	34
	REFERENCES	35
	APPENDIX	36

Introduction

The Personal Development Portfolio (PDP) are all the activities that have helped me gain or improve certain skills during a certain project or time lapse. Through this PDP descriptions of assignments, skills learned and knowledge that assist with my personal and professional development.

My name is Javier Duran, I am an international student at Fontys University of Applied Sciences, in the Infrastructure Engineering BSc program. Very interested and motivated to keep learning about IT in general but more specifically cybersecurity. As risks keep in this area keep growing, I think it is very important to have a secure infrastructure to give companies the edge advantage. In addition, I want to be part of people who will help build a smarter and better future through technology.

Purpose

The purpose of this assignment is to create Development Portfolio through which skills, techniques, knowledge, and topics learned during lectures will be laid out. In addition, the case studies will help us develop these knowledge and skills learned by putting them into practice. Most importantly, my personal development in professional skills such as teamwork, communication skills, and leadership will be evaluated. Different forms of evidence will support all the above-mentioned characteristics. Critical reflection will be done on the work delivered. This facilitates the progress and gives an insight into my learning process.

Objectives

- Learn new technical and professional skills.
- Getting an insight into my learning process.
- Inform on the skills and knowledge learned during the semester.
- Reflecting on the assignments and case studies.
- Improve through self-evaluating what are my weak and strong areas and/or skills.

1.0 Programming for Infrastructure

In this semester, programming course will be covering Python language. Python is a powerful object-oriented programming language. Python has many features, one of its most recognizable is that it has clear and elegant syntax. In addition, Python comes with a large standard library that supports many of the most common and important programming tasks. Moreover, this programming language is an interpreted language, which saves considerable amount of time during program development.

All course exercises and tasks can be found in the following Git repository: <https://git.fhict.nl/I408431/3567885-javierduran-feb21-python101.git>

1.1 Writing Code

Writing clean and organized code is very important. Other developers and co-workers should be able to read and understand the code easily. This is very important because most likely, it will be a team project. In addition, people might need to fix bugs, add features, or change the code in the future and a clean code would save time, money, and resources.

During the first weeks of the course, writing code for the assignments seemed easy due to the knowledge I had about Python from before the course started. After a short time into the course tasks started to get a bit more complex, making me read more of other's people code and explanations which caused improvements in the way I wrote code. I think I write more clear code and comments to it.

1.2 Functions

A function is a block of organized, reusable code that is used to perform a single, related action. Functions provide better modularity for your application and a high degree of code reusing (TutorialsPoint). Python also provides built-in functions like `print()`, `type()`, `list()` and many more. A function is defined by using the keyword “def”, a given name for the function and finishes with parentheses and a colon. For example, to define a function with the name “example”, it would look something like this: *def example()*:

Functions can also pass parameters. A parameter is the variable listed inside the parentheses in the function definition. By default, parameters have a positional behavior, and you need to pass them in the same order that they were defined.

Functions in Python were easy to understand from my part due to the previous knowledge I had in Python and other programming languages such as C# and C++. Although the logic is basically the same compared to other programming languages, it is still different. The function is not declared in between brackets or parentheses like other programming languages, instead, Python uses spaces or indentation to declare the scope of the function. Functions are very useful as it allows us to re-use pieces of code. This helps the program be more efficient.

1.3 Classes

Classes provide a means of bundling data and functionality together. Creating a new class creates a new type of object, allowing new instances of that type to be made. Each class instance can have attributes attached to it for maintaining its state. Class instances can also have methods (defined by its class) for modifying its state (Python Software Corporation). Using classes is an easy way of keeping data and methods to change data in one place. This helps the program to run smoother and keeps the code organized. Classes are also very important for object-oriented programming, which is key for today's programming and development.

Learning classes in Python is important because it is key for object-oriented programming. Almost every Python code is based on objects, its properties, and methods. For these reasons, learning and understanding how to properly program with classes and object is key to today's programming and application development. In addition, using classes provides the ability to reuse certain chunks of code, making the program run smoother and more efficient.

Classes was new to me, which gave me trouble at the beginning. Retrieving objects and their characteristics was complicated at first. In conclusion, I learned a lot from the first assignment of classes to creating a complete 'To Do List' using and defining a class for 'Person' and a class for the 'To Do List' which turned out to function properly. Programming with classes is something that requires practice, and the time I put into this section of the course helped understand better how data in programs is structured.

1.3.1 Evidence

```
#Defining class ToDo
class ToDo():
    def __init__(self):
        self.taskList = [[100, 'Wake up!'], [101, 'Morning run'], [102, 'Study time']]

    #Add a task
    def addTask(self, key, task):
        self.taskList.append([key, task])

    #Give task a key starting from 100
    def addKey(self):
        last_index = len(self.taskList)
        key = last_index + 100
        return key

    #Print the objects in the list
    def __str__(self):
        s= "\n".join(map( str, self.taskList))
        return s

    #Check if an item exists by name
    def onList(self, task):
        if any(task in t for t in self.taskList):
            return True
        else:
            return False

    #Check to see if the list is empty or not
    def isEmpty(self):
        if not self.taskList:
            return True
        else:
            return False
```

Figure 1.3.1

- In the image Figure 1.3.1, the declaration of the class 'ToDo' from the To Do List assignment. Functions for this class can also be appreciated in this image.

1.4 OS Module

The OS module in Python provides functions for interacting with the operating system. OS comes under Python's standard utility modules. This module provides a portable way of using operating system-dependent functionality (GeeksForGeeks, 2021). The module allows us to perform many OS tasks such as getting current working directory, read, modify and copy files and directories. To make use of this module, first it should be called at the beginning of the script by typing: *import os* as appreciated in figure 1.4.1.

The OS module provides an easy way for the user to interact with several OS functions. This is very useful for OS automation or saving information from a script or function in a local file. It is

important to learn this module as it can be very powerful. It is possible to create files and directories, add data to them and even edit them.

In retrospect, the OS module in Python can become very useful as the assignments made it clear. Many functions in the module are possible to use such as *os.open()* and *os.close()* to open and close files. Helping with OS automation, such as creating files or folders or adding data into these files.

1.4.1 Evidence

```
import os

#define class Person
class Person:
    def __init__(self, name):
        self.name = name

    def getName(self):
        return self.name

names = open('names.txt', 'w')
x = 0

#Ask for names until empty string
while True:
    name = str(input("Enter new name to add: "))
    indiv = Person(name)
    new_name = indiv.getName()
    x += 1

#write names to file
with open('names.txt', 'a') as new:
    new.writelines(f'{x}. {new_name}\n')

    if name == '':
        break
```

Figure 1.4.1

- A script to record the class person being input into a newly created .txt file using the OS module is shown in figure 1.4.1

1.5 SQLite

SQLite is an in-process library that implements a self-contained, serverless, zero-configuration, transactional SQL database engine. Unlike other SQL databases, SQLite does not need a separate server process. It is a very popular database as it is used in lots of projects and applications. SQLite3 can be integrated with Python using sqlite3 module, which was written by Gerhard Haring. It provides an SQL interface compliant with the DB-API 2.0. To use sqlite3 module, you must first create a connection object that represents the database and then optionally you can create a cursor object, which will help you in executing all the SQL statements (TutorialsPoint).

In this section, a lot of time was being put into researching because I had never used databases inside an application. Understanding and learning on how to implement databases in applications and for management is very important as it is key for developing applications, automation, and management. Developing a CRUD application to handle events was very useful to learn about SQLite module.

1.6 Tkinter

Tkinter is the only framework that's built into the Python standard library. Visual elements are rendered using native operating system elements, so applications built with Tkinter look like they belong on the platform where they're run. Tkinter is lightweight and relatively painless to use compared to other frameworks. This makes it a compelling choice for building GUI applications in Python, especially for applications where a modern sheen is unnecessary, and the top priority is to build something that's functional and cross-platform quickly (Amos).

Tkinter is a cross platform library for developing GUI python applications. It is very useful as you can create simple GUI applications that require small amount of resources. For this section, several management tools were developed for the case study, in addition a calculator was also coded. The management tools that were developed with a UI were the CRUD application, a system KPI monitoring tool and a DHCP log parser that will allow the user to send copies from the log through email.

1.6.1 Evidence

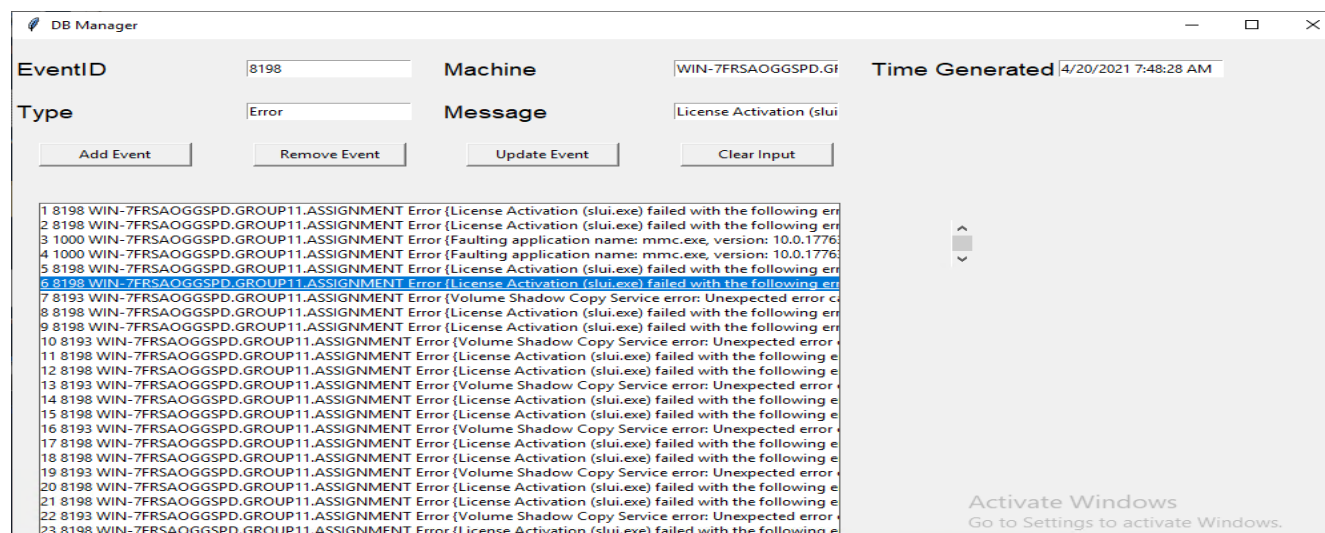


Figure 1.6.1

- In Figure 1.6.1 it is possible to see that Tkinter and SQLite were both used in developing the above application. It handles csv from event logs and puts them into a database.

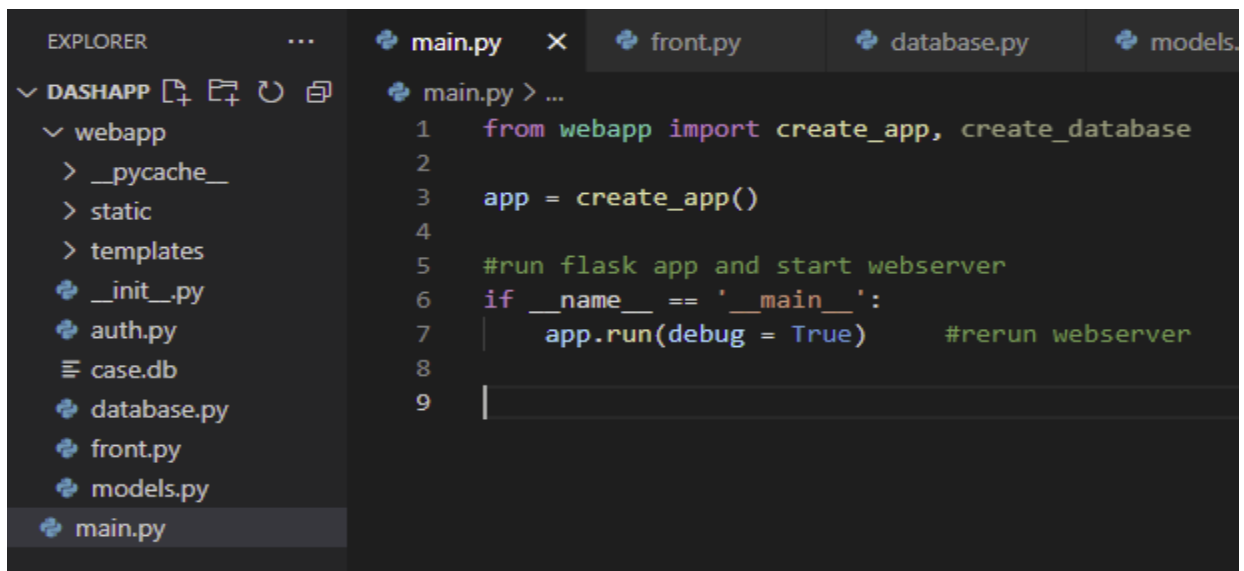
More applications making use of Tkinter can be found in the following git repository under the ManageTools folder: <https://git.fhict.nl/l408431/casestudy1-group11.git>

1.7 Flask Microframework

Flask is a micro web framework written in Python. It is classified as a microframework because it does not require tools or libraries. It has no database abstraction layer, form validation, or any other components where pre-existing third-party libraries provide common functions (Wikipedia, n.d.) .

The group is going to be using the Flask framework to develop and run an application for the second case study of the semester. Flask provides us with libraries and modules that will help us develop a social media clone that will allow users to create, edit and delete the posts. Flask is useful for this situation as it has libraries such as 'login manager' which allows us to check which users are active, also provides assistance in authentication. Another great feature is that you can run a development server that will help you see the changes made to the application in an easier way. After the development is done, Flask allows you to run a production server which will be hosted in a container. The application can be found in the git repository for the second case study: <https://git.fhict.nl/l408431/group11-casestudy2> .

1.7.1 Evidence



```
main.py > ...
1  from webapp import create_app, create_database
2
3  app = create_app()
4
5  #run flask app and start webserver
6  if __name__ == '__main__':
7      app.run(debug = True)      #rerun webserver
8
9
```

Figure 1.7.1

- In Figure 1.4 we can observe a Flask folder structure. It has a main.py that will create and run the application, on the left, all the folders that will provide the back and front end like 'static' and 'templates'.

1.8 DBMS

A database management system (DBMS) is a software package designed to define, manipulate, retrieve and manage data in a database. A DBMS generally manipulates the data itself, the data format, field names, record structure and file structure (Techopedia, n.d.). The groups will use a DBMS, in this case PgAdmin4, to make the management and maintenance of the database more efficient and time saving as it provides an interface to perform various operations like database creation, storing data in it, updating data, creating a table in the database and a lot more.

We will be using Postgresql for our case study as it is an open-source database SQL compatible. The database is using a hierarchy model of a database with the parent table of Users. We will be using it to manage, monitor and maintain tables in the database such as the users and the posts table. This can be used to check which user posted a post and what date this happen in a very efficient manner.

1.9 Heroku

Heroku is a container-based cloud Platform as a Service (PaaS). This service is used by developers to deploy their applications, this gives the developers more time to focus on developing applications or products without having to worry much on maintaining an infrastructure. To deploy applications in flask is very simple. Deploying an application in Heroku just requires downloading Heroku CLI. Once installed, you can connect your application to Heroku by connecting a Git repository. I had to add a 'Procfile' to declare what the callable object of the application for it to run on a uWSGI production server. In the following link you will be able to find the ToDo List application done in the programming course.

<https://todos2p.herokuapp.com/>

1.10 Reflection & Self Evaluation

Programming has been more involved than what I thought it was going to be for Infrastructure Engineering. Although I had some previous, self-thought Python knowledge I have learned a lot and has pushed me to keep learning by realizing how useful programming can be. The impact in the infrastructure a program can have can be large. Automation and management of such infrastructures can become a time saver, extra security or just the ability to manage the infrastructure and the clients in an effective and efficient way.

During the case studies I developed different types of applications with different uses and functionalities. I did some Tkinter applications and a full stack web application in Flask. Some of the Tkinter applications are a KPI monitoring application, an automated DHCP log parser and save it to a file. In the other hand, in Flask I made a full stack To Do List that is currently hosted on Heroku, and a product we named “Medit”. Medit is a posting site where several different topics related to ICT can be discussed.

2.0 Managing Infrastructure

During this course skills and knowledge for managing and securing network and infrastructure. Processes and systems will be used to realize support services to guarantee quality, reliability, and continuity. Moreover, measures and skills to secure all system components in the infrastructure, as well as testing its security.

2.1 Agile Project Management

Agile project management is an iterative approach to managing and delivering projects through its life cycle. This type of approaches is frequently used in software development projects to promote velocity and adaptability since the benefit of iteration is that you can adjust as you go along rather than following a linear path. One of the aims of an agile or iterative approach is to release benefits throughout the process rather than only at the end (Association for Project Management, 2007). During the course different methods to properly plan an agile project.

Learning about agile project management, in my opinion, was very important. Most of the applications and/or products aim to have a useful time for a long time, here is where agile project management is probably the best approach. This approach allows change and adding future features to the application or product. In addition, agile project management can save resources because a minimal viable product can be launched to the market and can be developed in the short future. During the first case study, agile project management was crucial because the project was essentially divided into two different parts. In the first part, an infrastructure was to set up and secure a proper IT infrastructure. After noticing managerial problems for the infrastructure, the group had to create a complete application to help the business manage their clients and network.

2.1.1 Evidence

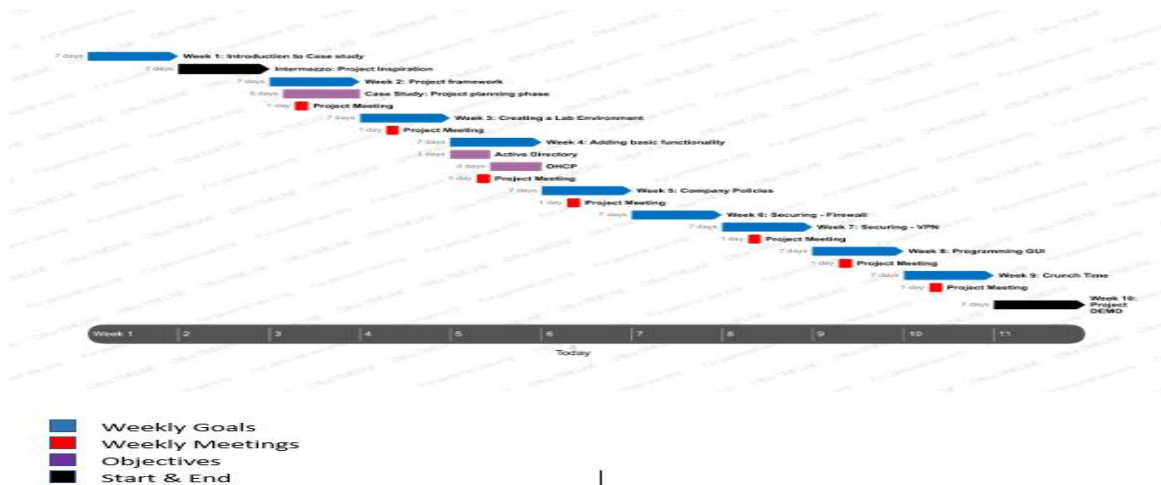


Figure 2.1.1

- In figure 2.1.1, you can observe a planning based on the agile methodology as we aim to complete certain goals every week during the time period, but changes and improvements are always possible.

2.2 ITIL

The IT Infrastructure Library (ITIL) is a library of volumes describing a framework of best practices for delivering IT services. ITIL has gone through several revisions in its history and currently comprises five books, each covering various processes and stages of the IT service lifecycle (CIO, 2019). ITIL's approach to IT services management will help business reduce and manage risks, strengthen customer relations, reduce costs in practice, and have a reliable and continuous service.

ITIL is a management method for IT services. An organization that can manage their risks and keep the infrastructure working efficiently and continuous. An IT company that can manage risks and use their IT resources efficiently will not only save money, but it will enhance the working environment and will allow people in the business to do their jobs more effectively. ITIL is also known to be the best practice for managing an IT service due to the following benefits:

- Reduce costs
- Improved productivity
- General standards and guidelines
- Efficient, effective and improves experience

The above-mentioned benefits are, in my opinion, the most essential benefits ITIL will bring to a company or service. In addition, the course also explained Configuration Management Database which is very helpful to plan and create relationships between 'sectors' of the project.

2.2.1 Evidence

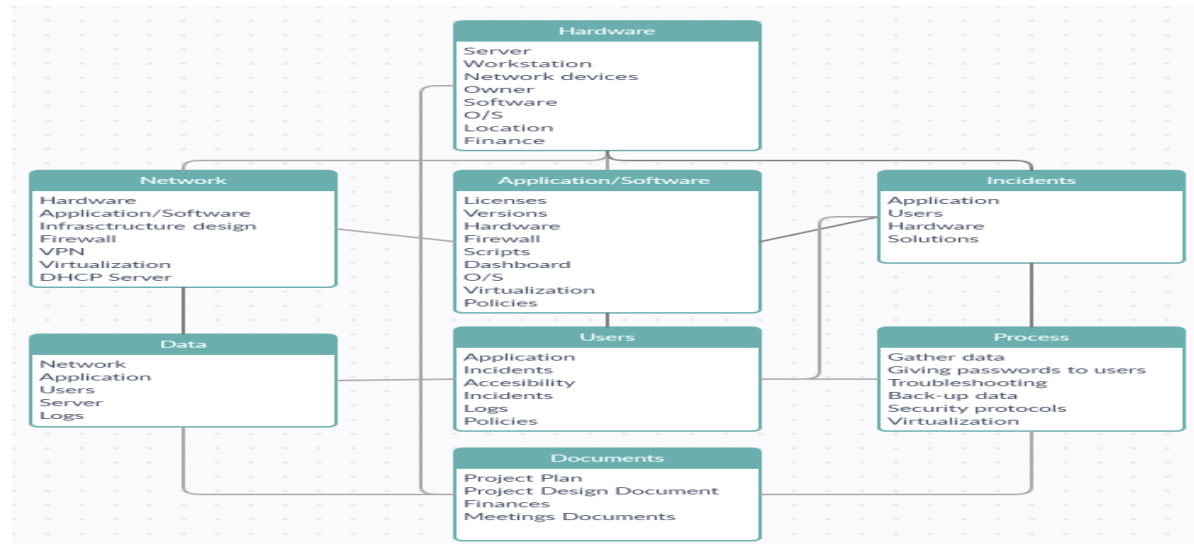


Figure 2.2.1

- In figure 2.2.1, the CMDB (Configuration Management Database) that was developed during week 4 of the semester.

2.3 Security Management

Security Management in IT is to put processes and tasks into action to protect the organizations assets and operations against possible threats and risks. These actions are enabled to ensure confidentiality, integrity and availability of IT systems, data and resources. Lots of aspects are to be considered when securing an infrastructure, for example user and group policies, security protocols and processes, and other rules and regulations to reduce risks, threats and actors to the minimum possible. Take into consideration what possible vulnerabilities can be found.

It is critical to set the correct processes for the company to work properly and not be affected by any external or internal threats that want to cause a financial or reputational damage to the organization. The IT security processes are essentially part of an organization's risk management processes and business continuity strategies. In a business environment marked by globalization, organizations must be aware of both national and international rules and regulations.

2.4 GDPR

GDPR is a set of data protection rules and conditions, that take into consideration how people can access their data and how a company uses a client's data. This set of rules also creates limits on what a company can do with the users' data. This framework of rules was created to guide companies on how people's data is used and handled. According to Article 5 of the GDPR, there are seven key principles. These principles are:

- Lawfulness
- Fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

We have taken into consideration these seven principles to proceed with the data handling of our users.

2.5 Reflection & Self Evaluation

It is very important to have good managerial skills, especially in the field of IT as many projects will be starting from scratch or will go through change constantly. Knowing which factors and variables such as, risks or threats or available resources, and properly planning a solution around those factors to satisfy the client's needs will save time and problems for the company and service being provided. I learned a lot about properly planning and managing in this semester. During both case studies I was 'leader' of the group and it was my responsibility to make sure that everyone in the team could finish their own responsibilities. Although our work division was not the best, we managed to complete the project and exceed our own expectations.

3.0 Securing Infrastructure

Securing infrastructure is part of the managing and securing course. In this section, students learn how to take proper and efficient measures to secure all system components of the infrastructure. Different skills, techniques and theory like penetration testing, physical organization, and technical measures will be achieved. Recent studies suggest that cybercrime and cyber threats are causing world economy around 445 billion USD annually.

The report from the Center for Strategic and International Studies (CSIS) said cybercrime was a growth industry that damaged trade, competitiveness, and innovation. A conservative estimate would be \$375 billion in losses, while the maximum could be as much as \$575 billion, said the study, sponsored by security software company McAfee (Sandle, 2016). It is very important for any company to take cyber threats seriously, making it critical to learn about these methods and skills during our educational and professional career.

3.1 Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and permits, or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) to block malicious traffic like viruses and hackers (ForcePoint, 2021). Depending on the type of firewall, they have different functionalities. In general, firewalls analyze incoming network traffic on established rules and policies to filter unsecured, malicious, or suspicious sources to prevent attacks. Firewalls can also be used as gateways or virtual routers.

Firewall servers as the “the first line of defense” to external threat, malware and cyber criminals trying to gain access to the system. It is important to learn how to configure and set up a firewall in a network as it will have many benefits regarding security. Some of these benefits are monitors network traffic, can detect and stop virus attacks, prevents unwanted people having access to data or systems.

For the case study, the team had to install a firewall in the internal network to help provide security. This firewall will block unauthorized people to have access to data or systems. We used Pfsense, which is an open-source firewall that was installed in a virtual machine to make it a dedicated firewall and gateway for our private network.

3.1.1 Evidence

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
Hyper-V Virtual Machine - Netgate Device ID: 72470b85ad655d83fbef
*** Welcome to pfSense 2.5.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> hn0      -> v4/DHCP4: 176.16.11.11/24
LAN (lan)      -> hn1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
Status: Running
```

Figure 3.1.1

- In figure 3.1.1 it is possible to observe the firewall installed and its interfaces in hn0 and hn1 and some routing configurations.

3.2 Secure Network Protocols

SFTP (SSH File Transfer Protocol) is a secure file protocol that is used to access, manage, and transfer files over an encrypted SSH transport. When compared with the traditional FTP protocol, SFTP offers all the functionality of FTP, but it is more secure and easier to configure (Linuxize, 2020).

The team made use of this secure network protocol to automate file sharing through a SFTP connection between the client and our main server. We installed OpenSSH and WinSCP to perform this task. OpenSSH allowed us to create a SFTP connection between both computers by authenticating the key given to the client. With an SFTP connection established we used WinSCP for file sharing through the SFTP connection. More information about this method and how we manage to implement it can be found in the Design Document for our project which describes the complete functionality that OpenSSH, WinSCP and the SFTP protocol. (Link can be found in appendix).

3.3 Backups

Backups are the process of storing copies of data or stages of a process that can be used to protect an organization's data in case of hardware failure, data breaches and other critical circumstances that can end in data loss. The purpose of backing up data is that it can be recovered in case of a critical event that can cause primary data failures. Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data.

The backup software the team decided to use for the case study was Windows Server Backup feature that can be installed using Server Manager. Since we were using Windows Server Essentials, we found this software to be the most reliable as it is provided directly by Microsoft. In experience, we had a problem that required for us to restore the whole state of a virtual machine due to the accidental deletion of a critical file. For evidence, please refer to the Design Document in the git repository for the case study (Link can be found in appendix).

3.4 IDS/IPS

The main difference between them is that IDS is a monitoring system, while IPS is a control system. An IDS will analyze and monitor network traffic for signs that indicate attackers are using a known cyberthreat to infiltrate or steal data from your network. IDS systems compare the current network activity to a known threat database to detect several kinds of behaviors like security policy violations, malware, and port scanners. On the other hand, IPS, is live in the same area of the network as a firewall, between the outside world and the internal network. IPS proactively *deny* network traffic based on a security profile if that packet represents a known security threat (Petters, IDS vs IPS, 2020).

Both systems were installed in our server environment to provide extra security in our system. The systems were configured with Pfsense firewall as it provides these amazing features to help system administrators prevent and detect possible attacks to our system.

3.4.1 Evidence

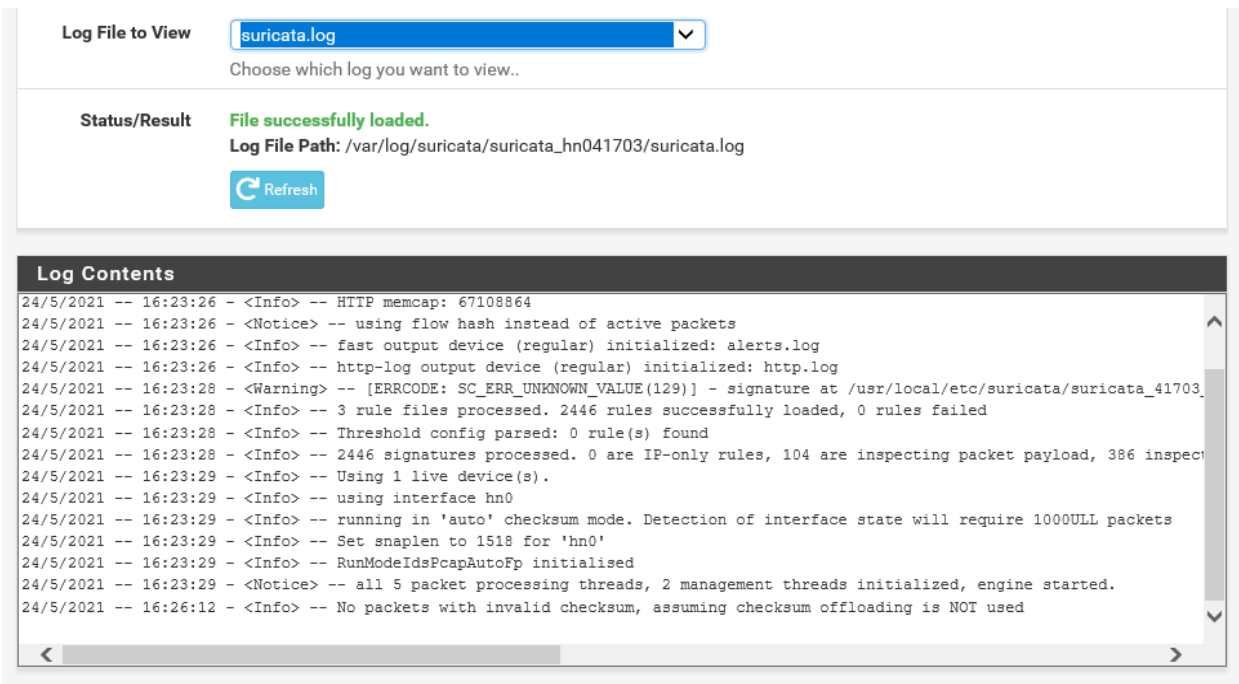


Figure 3.4.1

- In figure 3.4.1 we can observe that Suricata is recording logs on the interfaces configured.

3.5 Snort

Snort is an open-source Intrusion Prevention System (IPS) that uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users (Snort Team, n.d.). Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger, or it can be used as a full-blown network intrusion prevention system.

The team implemented some rules to help us monitor and prevent possible attacks in our network. Some of the rules implemented have the following purposes:

- Check if web server is visited.
- Check for failed SSH connections to the Ubuntu Server.
- Possible DoS attacks, like SYN flooding.

3.6 Forensics

To perform digital forensics investigations, we used an open-source tool called Autopsy. Autopsy runs background tasks in parallel using multiple cores and provides results to you as soon as they are found. It may take hours to fully search the drive, but you will know in minutes if your keywords were found in the user's home folder (SourceForge, n.d.). This tool will help us analyze files and directories, including some deleted files. Some other features include keyword search, hash matching, registry analysis and web analytics.

Performing digital forensics will help us detect malicious attacks and will allow us to develop or put in place software that will prevent cyber criminals from accessing our network or data. In addition, performing digital forensics can help us prevent these attacks before it even happens, as we can detect possible weaknesses or vulnerabilities in the network. Essentially, Autopsy will help maintain the network more secure.

3.7 Pen-Testing

During the penetration testing assignment, I performed reconnaissance and some malicious attacks on the case study's infrastructure to provide an insight of the possible security flaws in the infrastructure. The group found services running on the environment and researched about possible vulnerabilities in these services. Nmap was used to find what ports were hosting a service and from there we analyzed and explored the different options on the system. The discovery of the SSH service running on an Ubuntu server allowed us to perform a brute-force attack on the SSH connection using Hydra. The password list used had no success trying to gain brute-force access to the Ubuntu server.

The main objectives where:

- Identify possible access points to our network such as SSH or other communication protocols.
- Identify web application vulnerabilities or probable exploits.
- Perform controlled malicious attacks on the system.
- Report about the current security status of the infrastructure.

3.7.1 Evidence

```
(jads@kali)-[~]
$ hydra -l group11 -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou-75.txt -s 2222 10.0.2.111 -t 4 ssh -I
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** * ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-11 09:36:26
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 59185 login tries (l:1/p:59185), ~14797 tries per task
[DATA] attacking ssh://10.0.2.111:2222/
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 59149 to do in 27:24h, 4 active
```

Figure 3.7.1

- In figure 3.7.1 we can see an example of a brute-force attack using Hydra on an SSH connection on the IP of our network and port 2222.

3.8 Reflection & Self Evaluation

As threats constantly change, it is very important to be as secure as possible to avoid at least most of these threats and decrease the number of actors capable of penetrating and doing damage to the infrastructure. A lot of business nowadays, are looking to have some sort of online presence which makes them possible victims for some actors.

Keeping the business and customer data is important. Not only for the operations and management of the business but also in the image of it. Things that might seem obvious to do like backing up the important data is critical for a business as there could be a human or software mistake and delete data by accident. In addition, a data breach is always possible, so it is important to use secure protocols and have security measures and rules to reduce the possible vulnerabilities in the infrastructure.

4.0 Connecting Infrastructure

Connecting infrastructure refers to connecting system component so that data can be exchanged in a secure and effective environment. It is critical to have the infrastructure properly structured and its components properly connected so that quality, continuity, reliability, security, and performance are guaranteed for the clients and users.

4.1 Active Directory

Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information (Microsoft). In other words, Active Directory helps a company organize their users, computers and information.

Active Directory is a system that automates and therefore improves network management of resources, users, data and security. In addition, Active Directory helps organizations manage their computers or devices. Active Directory was installed in the server so that the group could manage the sales group of the company being mimicked.

According to Michael Ritter, an experienced pen-tester professional, explained that 95% percent of Fortune 1000 companies use Active Directory. It is important to learn how to properly manage users, domains, and resources and how to properly secure it as it contains important a crucial information about these companies and users.

Evidence can be found in the Case Study 1 git repository. (Link is declared in the appendix).

4.2 DHCP

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used in local area networks (LAN). DHCP server is present in the network. When a client connects to the network it requests an IP from the scope of IPs previously configured by the server administrator. The DHCP server will automatically assigned an IP to a newly connected client. This will make connectivity efficient and time saving for the clients, server and administrators.

DHCP automatically assigns an IP address to a new client in the network when they join the network, therefore this service brings key and important value and efficiency to ICT operations. First, tasks are reduced because an IP no longer must be assigned manually. In addition, addressing and availability is optimize because when an IP is no longer in use it is free for use for another client.

It is important to learn how to proper configure and use DHCP because it can bring great benefits like the ones mentioned before. In the study case, a DHCP server will be installed in the same VM containing active directory. It will help us mimic the company's infrastructure virtually. The DHCP will automatically provide an IP for every new virtual machine connected to the domain. The DHCP IP address pool scope was configured from 176.16.11.10 to 176.16.11.100.

4.2.1 Evidence

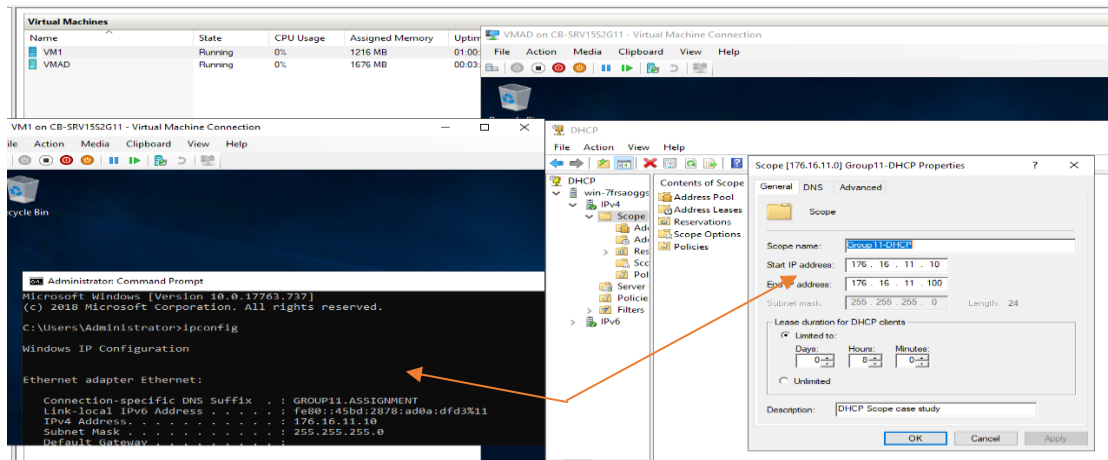


Figure 4.2.1

- In figure 4.2.1, you can see that the team set up a DHCP server in our domain controller and connected a client to the network to test. Successfully received IP, as indicated by the arrows.

4.3 Bash

Bash is the shell, or command language interpreter, for the GNU operating system. Bash scripting will help you automate routine tasks and save valuable time, whether you're a sys admin, Linux user or software developer.

In the future, it is very possible that I will end up working as a sys admin, Linux server manager or even a software developer, so it is very important that I am able to automate and create scripts that will help me save time while performing tasks in a GNU operating system. During the course we developed a few scripts that helped me learn the basics of BASH scripting such as variables, performing commands, loops and conditions and argument and user input. This tutorial helped me have a clear understanding of BASH. It was not really complicated as I had learned other programming languages before, and the logic was very similar.

4.3.1 Evidence

```
#!/bin/bash
DAY=$(date +%a)
if (($DAY = Mon));
then
    echo 'Monday boreday';
elif (($DAY = Tue));
then
    echo 'Trashed Tuesday';
elif (($DAY = Wed));
then
    echo 'Wasted Wednesday';
elif (($DAY = Thu));
then
    echo 'Thirsty Thursday';
elif (($DAY = Fri));
then
    echo 'Freaky Friday';
elif (($DAY = Sat));
then
    echo 'Salsaturday';
else (($DAY = Sun));
    echo 'Sunday Funday';
fi
```

Figure 4.2

- In Figure 4.2 a BASH scripts that, depending on the current day, will give the adequate message to the user.

4.4 High Availability

High Availability in PfSense comes down to hardware redundancy, essentially having a hot spare instantly taking over a router that becomes unavailable. Instantly in this case being one or two seconds, without firewall states being broken, so your file will just continue downloading and your video will continue streaming (Vorkbaard, 2017). The HA techniques used by Pfsense include CARP protocol, pfsync and XML-RPC.

CARP protocol is for configuring a virtual IP that will be used by the firewall as a secondary server if the primary server crashes or encounters errors. Second, pfsyncs is another protocol used to sync the status of connections of the two servers. Last, XML-RPC is a protocol that will replicate data from one server to another, Pfsense uses this protocol to replicate the firewall configuration on both the servers. Although, we didn't implement HA in our case study as it was optional and other groups were having connection issues, I made enough research to understand the main idea and purpose of HA. If we were to

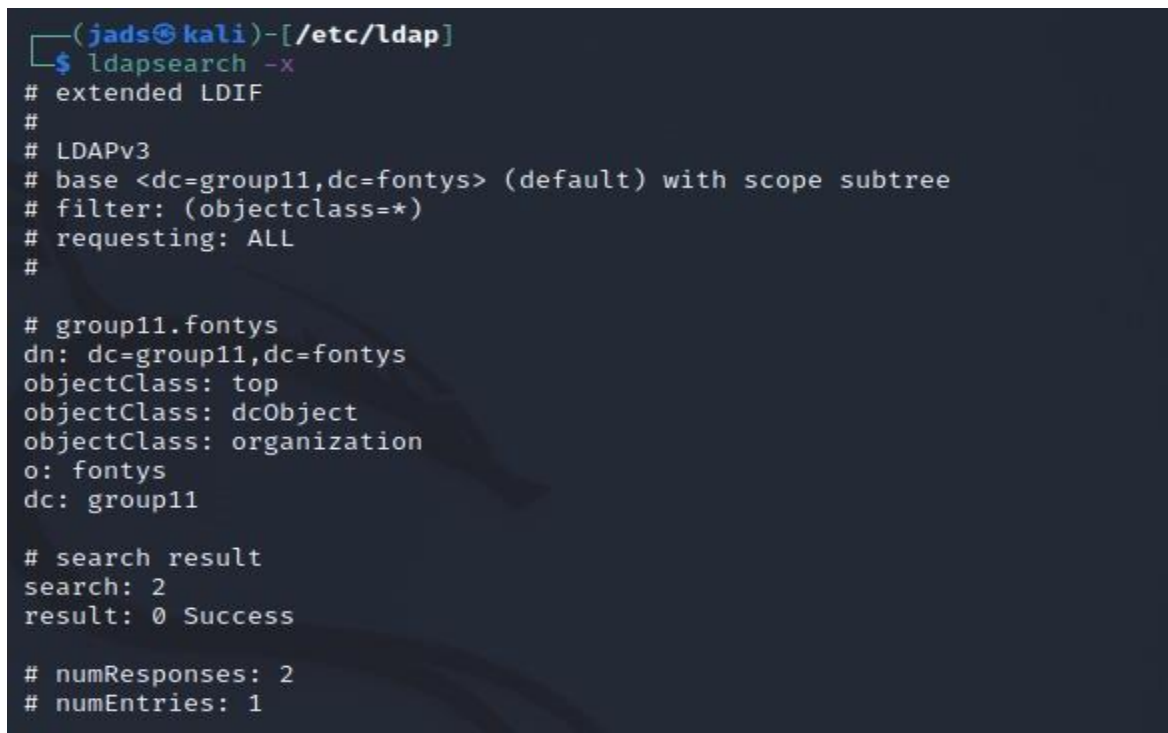
implement it in our infrastructure, then we would have a secondary server on IP 10.0.2.112 as our secondary server, in case of failure.

4.5 LDAP

LDAP provides the communication language that applications use to communicate with other directory services servers. Directory services store the users, passwords, and computer accounts, and share that information with other entities on the network (Sobers, 2020).

For the assignment I have created LDAP server in my own virtual machine. It was successfully installed and configured to be able to connect with clients. This LDAP server was given an DN of group11.fontys for testing purposes. Although we did not implement it in the case study infrastructure, we consider that this service would have helped the environment greatly, by removing certain bottlenecks on user authentication by avoiding interaction with the database often. In addition, if a client needs to locate a piece of data they can in a fast and efficient way. In Figure 4.5.1 we can observe that LDAP server was successfully built for DN group11.fontys. We know it is accepting clients because the result indicates '0 success'.

4.5.1 Evidence

A terminal window with a dark background and light-colored text. The prompt is '(jads@kali)-[/etc/ldap]'. The command 'ldapsearch -x' has been executed. The output shows LDAP search details: extended LDIF, LDAPv3, base <dc=group11,dc=fontys> (default) with scope subtree, filter: (objectclass=*), requesting: ALL. The search result for 'group11.fontys' is displayed, including dn: dc=group11,dc=fontys, objectClass: top, objectClass: dcObject, objectClass: organization, o: fontys, and dc: group11. The search result summary shows 'search: 2' and 'result: 0 Success'. At the bottom, it shows 'numResponses: 2' and 'numEntries: 1'.

```
(jads@kali)-[/etc/ldap]
$ ldapsearch -x
# extended LDIF
#
# LDAPv3
# base <dc=group11,dc=fontys> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# group11.fontys
dn: dc=group11,dc=fontys
objectClass: top
objectClass: dcObject
objectClass: organization
o: fontys
dc: group11

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Figure 4.5.1

4.6 Reflection & Self Evaluation

I have learned a lot about connecting and routing since most of the services and software the team used in the case studies required knowledge on properly connecting the infrastructure. For example, for VPN to work we had to give static IP's and remove them from the DHCP pool of IP's so there would not be a conflict. It is also very important to know how to use and connect Active Directory so that resources, services and data between groups, users and computers is always optimal for the company and its needs. I also learned how to write Bash scripts and how to automate certain tasks with Bash. In addition, learning from our mistakes, problems and struggles will help us in the future. Many useful skills and knowledge were gain from these topics because we will be able to connect an infrastructure properly and find the problems and errors in the system faster, as well as finding solutions for these problems and keeping protocols to avoid these errors repeat too frequently.

5.0 Provisioning Infrastructure

Provisioning is the process of setting up IT infrastructure. It can also refer to the steps required to manage access to data and resources and make them available to users and systems (Red Hat). It refers to the use platforms to make system resources available to applications. For example, properly provision hardware, virtualization, system resources, storage and make information and resources available for clients.

5.1 Hyper-V

Hyper-V is a platform that enables IT or server administrators to make better use of the hardware or provision and test different environments by virtualizing multiple operating systems running in the same physical server simultaneously. Hyper-V can run virtual machines with client and server operating systems. In addition, it can also mimic hardware devices such as switches. In this case study, Hyper-V will be used to create a virtual environment to be able to mimic a business infrastructure in our own hardware.

An IT professional may need to run different operating systems for many reasons such as services, development, or testing. It is important to learn how to manage virtual machines as it can be essential for testing or creating virtual solutions with limited hardware resources.

Hyper-V allowed the group to mimic the infrastructure of the company by creating a virtual server and other virtual machines to enable services for the network. In addition, a Windows client virtual machine was created to be able to test our environment. Services like the windows server, DHCP and firewall were enabled through virtualization.

Evidence can be found in the Case Study 1 git repository. (Link is declared in the appendix).

5.2 VPN

VPN stands for Virtual Private Network. This service is a technology that can transmit network data over another network. It lets users make use of the network resources in the connected network through VPN. OpenVPN is a virtual private network system that implements techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities (Yonan).

With OpenVPN server properly installed in our virtual environment we were able to connect through OpenVPN client service into the server. This was done as the case study suggested employees should be able to connect remotely to the previously installed infrastructure. By properly creating a connection through the gateway and correct port forwarding this purpose can be achieved. It is very important to know about VPN as many organizations are part of the international market, so connections from different locations may be crucial to the operations of a company.

Evidence can be found in the Case Study 1 git repository. (Link is declared in the appendix).

5.3 Proxy

A proxy server acts as a gateway between the LAN or client and the internet. IT separates direct connection between clients and the website. Therefore, proxy can filter traffic providing certain functionalities, security, and privacy.

Modern proxy servers do much more than forwarding web requests, all in the name of data security and network performance. Proxy servers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests. A good proxy server keeps users and the internal network protected from the bad stuff that lives out in the wild internet. Lastly, proxy servers can provide a high level of privacy (Petters, What is a Proxy Server?, 2020).

Although proxy server sound like a good idea to implement in your LAN, the team created a policy where proxy settings could not be changed. This was since firewall was already installed, and

proxy servers can change how the infrastructure operates by letting clients browse through websites that were previously ruled out by the firewall.

Evidence can be found in the Case Study 1 git repository. (Link is declared in the appendix).

5.4 RADIUS

A RADIUS server is a networking device that is used to authenticate users. A RADIUS Server is a background process that runs on a UNIX or Windows server. It lets you maintain user profiles in a central database. Hence, if you have a RADIUS Server, you have control over who can connect with your network (Bhatt, 2019).

We will install FreeRadius in Pfsense, which is the firewall previously set up. RADIUS will allow us to keep privacy and allow only authenticated users to connect to the network. This way we can manage and monitor who can connected or is connected to the domain, adding an extra security feature as well as a managerial feature.

5.4.1 Evidence

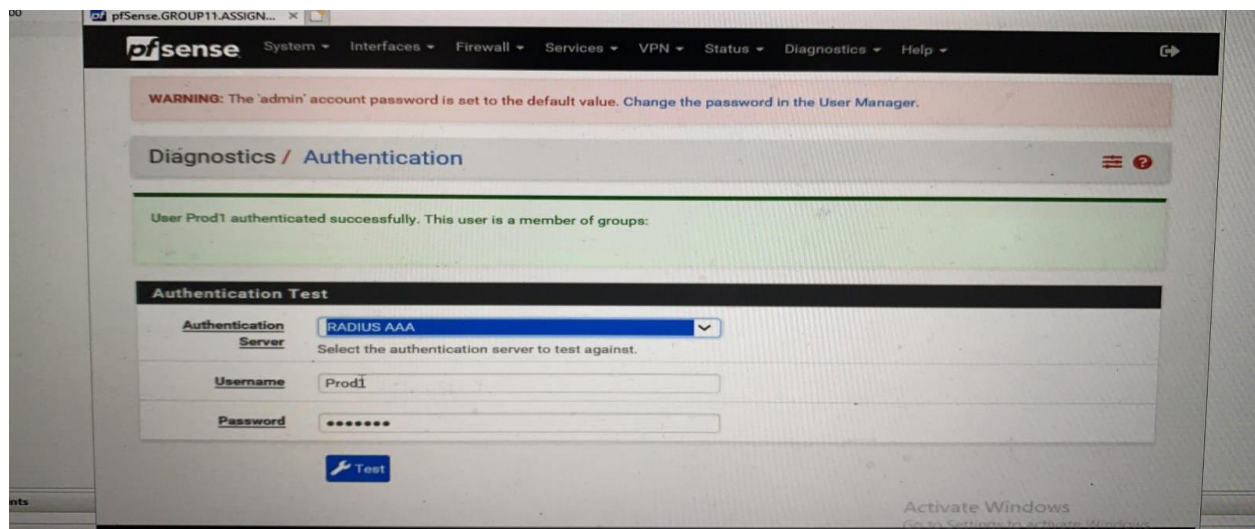


Figure 5.4.1

- In figure 5.4.1 we can observe RADIUS server connected to the Production group for testing.

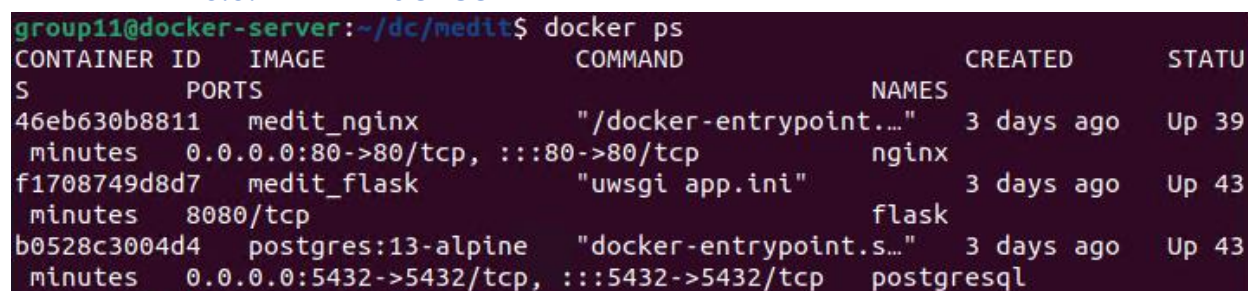
5.5 Docker

Docker is an open platform for developing, shipping, and running applications. Docker enables you to separate your applications from your infrastructure so you can deliver software

quickly. With Docker, you can manage your infrastructure in the same ways you manage your applications (Docker, n.d.).

The team will use docker to deploy the web application in an efficient and secure way. The application will be deployed in three different containers created through one “docker-compose” file. The containers will host different services that are required for the application to run properly, without using many resources. These containers will run the Flask application through a uWSGI server, Nginx and a Postgresql server.

5.5.1 Evidence



CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS
46eb630b8811	medit_nginx	"/docker-entrypoint..."	3 days ago	Up 39 minutes
f1708749d8d7	medit_flask	"uwsgi app.ini"	3 days ago	Up 43 minutes
b0528c3004d4	postgres:13-alpine	"docker-entrypoint.s..."	3 days ago	Up 43 minutes

Figure 5.5.1

- In figure 5.5.1 we can observe the Docker containers explained above. Nginx, flask and Postgresql containers.

5.6 Reflection & Self Evaluation

In times of uncertainty, like the current ones, it is very important to know how to provision and properly connect your infrastructure. Many people are currently working remotely from home, from other cities and in some instances even from other countries. IN these extreme situations, every member of the organization should be able to access the necessary resources in order to complete their tasks. In other, more “normal” situations, organizations are becoming global thanks to their online presence. We also learned how to deploy services on Docker containers which is essential for Dev Ops nowadays to deploy applications securely. This is also a very important reason why provisioning infrastructure for a business a learning outcome.

In my opinion, here is where most struggle was found personally and as a group because a lot of problems were met, and many troubleshooting attempts were made to have an efficient and working infrastructure. For example, VPN was quite time consuming as we needed to go through researching about the errors and troubleshooting possible solutions according to our research.

6.0 Personal Leadership

Being entrepreneurial regarding the ICT assignments and personal development, while being aware of own learning capacity and keeping in mind what ambitions that drive ICT professionals and/or which types of positions.

During the semester I have grown personally and professionally. Having a hard time with some case study problems, and delays made a more responsible and disciplined me. Since I was chosen “Group Leader” for both case studies, it also helped me organized and plan ahead which is a great managerial and ICT professional quality. I feel I have developed qualities such as self-discipline, communication and having a vision/plan for each task and project, and perseverance. Although, problems where met it is very important to always keep trying and troubleshooting because that is and ICT professional daily life.

7.0 Problem Solving

Critically consider ICT assignments from various perspectives, identify problems, finding an effective approach and coming up with appropriate solutions.

Problem solving is crucial in ICT. You will encounter problems almost daily, many which will be different each day. Planning and having certain protocols or procedures against some of the possible problems can be very helpful and time saving. It is important to know how to recognize certain problems, not only in the infrastructure, but in the team, you work with too. These problems will be met almost daily in any ICT area due to the continuous changes in software, hardware and techniques used and it is important to do proper research on the recognized problems to solve them the best way possible.

8.0 Future-oriented Organization

The organizational context of ICT assignments explores making corporate, sustainable, and ethical considerations and managing all aspects of carrying out the assignment.

It is important we consider ethical, corporate, and regulatory implications for every case study we tackle. As an infrastructure engineer, most likely, costumer data will be handled in many different scenarios. Some of this data can be critical which is why it is important to consider these

aspects. Considering the risks and problems to be faced regarding security or project development is also very important to consider regarding corporate and ethical considerations.

9.0 Targeted Interaction

Determine which partners play a role in the ICT assignment, constructively collaborate and fitting communication aimed at achieving the desired impact.

As a group we considered all our skills and knowledge to plan and divided tasks accordingly to our best area and/or skills. We also took into consideration the time available weekly for each group member (ex. People who work and study). This way we divided tasks accordingly so they would be completed in the time established. Some problems can be met, but these are mentioned in the risk assessment and solutions were defined if someone had problems completing their tasks. I also consider that it's recommended that all the members participate in at least most of the tasks to learn and understand about the infrastructure. This way there will be no misunderstandings on what it is being done.

Case Study

During the first phase of the project the company 'Make IT Work4U' is realizing improved infrastructure for its business clients. Current clients are small to medium businesses who need help adapting their infrastructure to satisfy the ever-rising needs of the end customer. The company provides a one-stop-solution that includes acquiring and installing hardware. Moreover, during the second phase, the company is having hard time to monitor the distribution of their resources and they lack a real time dashboard with server and client's statistics. The company has an urgent request to create an application for them to manage their infrastructure and clients.

The work was completed accordingly to the following chart:

Javier Duran	Svatoslav Pich	Ilia Baroff
<ul style="list-style-type: none"> • Active Directory • DHCP Server • Firewall • Management Tools: <ul style="list-style-type: none"> ➤ DHCP Log ➤ DB Manager ➤ Network Scanner ➤ KPI's • Automation (Task Scheduler) & WinSCP • Documentation 	<ul style="list-style-type: none"> • Active Directory • Virtualization • Firewall • Groups & Policies • Backups • OpenVPN • Automation (Task Scheduler) & WinSCP • Documentation 	<ul style="list-style-type: none"> • Network Architecture • OpenVPN • Automation (Task Scheduler) & WinSCP • Help troubleshooting dashboards

Case Study 2

This project is oriented on our own idea. In the group of three people the group must brainstorm the product according to their own ideas and relevance. In this project we shall create a reasonable and usable product, which will have a purpose for a more specific set of people, therefore making it more viable and specialized. We shall also use the knowledge from the previous semester and apply it in our project accordingly.

Javier Duran	Svatoslav Pich
<ul style="list-style-type: none"> • Full Stack Web Application • Bash Script • Documentation: <ul style="list-style-type: none"> ➤ Technical Manual ➤ User Manual ➤ Design Document ➤ URS Report • Docker Containers <ul style="list-style-type: none"> ➤ Nginx ➤ Postgresql ➤ Flask • OpenSSH 	<ul style="list-style-type: none"> • Documentation: <ul style="list-style-type: none"> ➤ Technical Manual ➤ Design Document ➤ Project Plan • Backend on web application. • RADIUS • Backups • OpenSSH

Conclusion

In conclusion, I have learned a lot related to all the learning outcomes regarding this personal development portfolio. Programming and provisioning were the most challenging as they were the subjects that required more time for troubleshooting and research. I realize the importance of all the learning outcomes and how they can affect my professional career in the future by knowing about these practices and skills. I believe that managing and programming skills being thought are going to be a key advantage for our professional life as it will give us an advantage against other IT professionals, although every subject adds to our professional life and to our general knowledge on our ICT area. I grew as a person, professional and learned a lot during the semester.

References

- Amos, D. (n.d.). *GUI with Tkinter*. Retrieved from Real Python: <https://realpython.com/python-gui-tkinter/>
- Association for Project Management. (2007). *What is Agile Project Management?*
- Bhatt, M. (2019, November 24). *RADIUS Server Authentication*. Retrieved from FOXPASS: [https://www.foxpass.com/blog/radius-server-and-how-it-works#:~:text=A%20RADIUS%20Client%20\(or%20Network,profiles%20in%20a%20central%20database.](https://www.foxpass.com/blog/radius-server-and-how-it-works#:~:text=A%20RADIUS%20Client%20(or%20Network,profiles%20in%20a%20central%20database.)
- CIO. (2019). *Your guide to the IT Infrastructure Library*. Retrieved from CIO Netherlands: <https://www.cio.com/article/2439501/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html>
- Docker. (n.d.). *dockerdocs*. Retrieved from Docker: <https://docs.docker.com/get-docker/>
- ForcePoint. (2021). *Firewall*. Retrieved from ForcePoint: <https://www.forcepoint.com/cyber-edu/firewall>
- GeeksForGeeks. (2021, February 19). *OS Module in Python with Examples*. Retrieved from GeeksForGeeks: <https://www.geeksforgeeks.org/os-module-python-examples/>
- Google. (2020). *Translate*. Retrieved from Google: [google.com](https://www.google.com)
- Linuxize. (2020, July 24). *How to Use SFTP to Transfer Files*. Retrieved from Linuxize: [https://linuxize.com/post/how-to-use-linux-sftp-command-to-transfer-files/#:~:text=SFTP%20\(SSH%20File%20Transfer%20Protocol,secure%20and%20easier%20to%20configure.](https://linuxize.com/post/how-to-use-linux-sftp-command-to-transfer-files/#:~:text=SFTP%20(SSH%20File%20Transfer%20Protocol,secure%20and%20easier%20to%20configure.)
- Microsoft. (n.d.). *AD DS Getting Started*. Retrieved from Microsoft: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/ad-ds-getting-started>
- Petters, J. (2020, 3 29). *IDS vs IPS*. Retrieved from Varonis: <https://www.varonis.com/blog/ids-vs-ips/#:~:text=The%20main%20difference%20between%20them,prevents%20traffic%20by%20IP%20address.>
- Petters, J. (2020, 6 10). *What is a Proxy Server? Data Security*.

Python Software Corporation. (n.d.). *Classes*. Retrieved from Python:
<https://docs.python.org/3/tutorial/classes.html>

Red Hat. (n.d.). *Provisioning*. Retrieved from Red Hat:
<https://www.redhat.com/en/topics/automation/what-is-provisioning#:~:text=Provisioning%20is%20the%20process%20of,steps%20in%20the%20deployment%20process.>

Sandle, P. (2016). Cyber Crime Costs Global Economy 444 Billion a Year. *Reuters*.

Snort Team. (n.d.). *Snort*. Retrieved from Snort: <https://www.snort.org/>

Sobers, R. (2020). *AD vs LDAP*. varonis.com.

SourceForge. (n.d.). *Autopsy*. Retrieved from Sourceforge:
<https://sourceforge.net/software/product/Autopsy/>

Techopedia. (n.d.). *techopedia*. Retrieved from DBMS:
[https://www.techopedia.com/definition/24361/database-management-systems-dbms#:~:text=A%20database%20management%20system%20\(DBMS\)%20is%20a%20software%20package%20designed,validate%20and%20manipulate%20this%20data.](https://www.techopedia.com/definition/24361/database-management-systems-dbms#:~:text=A%20database%20management%20system%20(DBMS)%20is%20a%20software%20package%20designed,validate%20and%20manipulate%20this%20data.)

TutorialsPoint. (n.d.). *Functions*. Retrieved from Learn Python:
https://www.tutorialspoint.com/python/python_functions.htm

TutorialsPoint. (n.d.). *SQLite*. Retrieved from TutorialsPoint:
https://www.tutorialspoint.com/sqlite/sqlite_python.htm

Vorkbaard, K. (2017). *High Availability in Pfsense*. TECH.

Wikipedia. (n.d.). *Flask*. Retrieved from Wikipedia:
[https://en.wikipedia.org/wiki/Flask_\(web_framework\)](https://en.wikipedia.org/wiki/Flask_(web_framework))

Yonan, J. (n.d.). *OpenVPN*.

Appendix

- Git repository for Case Study #1: <https://git.fhict.nl/I408431/casestudy1-group11.git>

Documentation and applications referred to the first case study can be found in the above git repository.

- Git repository for Programming assignments: <https://git.fhict.nl/I408431/3567885-javierduran-feb21-python101.git>

All the assignments for the programming course can be found in this git repository.

- Git repository for Case Study #2: <https://git.fhict.nl/I408431/group11-casestudy2>

Documentation and application for second case study can be found in this git repository.