

Министерство образования и науки Республики Казахстан

Astana IT University, 2023 г.

## ОТЧЕТ

О выполнении программы производственной практики

База практики: РГП “КазСтандарт”

Студент: Ергазин Адиль Берикович

Образовательная программа: “6B06301-Cybersecurity”

Группа: CS-2115N

Руководитель практики: Аймагамбетова Раушан Жанатулы

## Contents

Calendar Plan.....	3
Charachteristic.....	5
Introduction.....	6
1. Network architecture of Organization.....	6
2. Information security of Organization.....	7
3. First stage assignments.....	10
a. Set Up a Private network.....	11
b. LDAP addition.....	14
4. Second stage assignments.....	15
a. Deployment of information security platforms.....	16
b. Graylog deployment and connecting with Active Directory.....	17
c. OpenDLP deployment and agent connections.....	19
5. IT specialists duties.....	21
Conclusion.....	22
References.....	23

## КАЛЕНДАРНЫЙ ПЛАН-ГРАФИК ПРОХОЖДЕНИЯ ПРАКТИКИ ОТ ПРЕДПРИЯТИЯ

Ергазин Адиль Берикович студента, студента 3 курса, образовательной программы «БВ06301 Cybersecurity», период практики с «18» марта 2024 г. по «11» мая 2024 г.

№ нед.	Наименование работ	Сроки исполнени я	Название подразделения или рабочего места	Отметка об исполнении
1	2	3	4	5
1 нед.	Ознакомление с ИТ-инфраструктурой здания	1 неделя	Служба ИТ, РГП «КазСтандарт»	Выполнено
2 нед.	Ознакомление с сетевыми и конечными устройствами (Switch, hub, router, Physical Server, Virtual Server)	1 неделя	Служба ИТ, РГП «КазСтандарт»	Выполнено
3 нед.	Подробное изучение основных платформ и инструментов поддержания ИБ компании (LDAP, Active Directory, Kaspersky Endpoint Security)	1 неделя	Служба ИТ, РГП «КазСтандарт»	Выполнено
4 нед.	Имитация ИТ инфраструктуры в Windows Server 2022  1. Создать внутреннюю сеть 2. Подключить LDAP-server	1 неделя	Служба ИТ, РГП «КазСтандарт»	Выполнено
5 нед.	Развертка дополнительных платформ и инструментов для поддержания ИБ компании  1. Graylog - поднять сервер, добавить	1 неделя	Служба ИТ, РГП «КазСтандарт»	Выполнено

	<p>агента для малого мониторинга</p> <p>2. OpenDLP - поднять сервер и подключить к пользователю</p>			
6 нед.	Практический анализ действия с Active Directory при поддержании ИТ-инфраструктуры компании	1 неделя	Служба ИТ, РГП «КазСтандарт»	Выполнено
7 нед.	Практический анализ и моментальное реагирование на появление любых инцидентов ИТ-инфраструктуры здания	1 неделя	Служба ИТ, РГП «КазСтандарт»	Выполнено
8 нед.	Практический анализ и взаимодействие с сетевыми и конечными устройствами (IP Phone, Network Printer Router и т.д)	1 неделя	Служба ИТ, РГП «КазСтандарт»	Выполнено

*Руководитель практики от предприятия: Аймагамбетова Раушан Жанатова*

*Руководитель практики от АИТУ: Накипова Саяжан*

### Характеристика с места прохождения практики

Студент Ергазин Адиль Берикович за время прохождения практики проявил себя с положительной стороны. Место проведения практики посещал регулярно в соответствии с планом прохождения практики. К должностным обязанностям и поставленным задачам относился с особым вниманием, проявляя интерес к работе. Опозданий не допускал. Порученные задания выполнял аккуратно и в срок. Обладает достаточными теоретическими знаниями, необходимыми для формирования профессиональных качеств.

В коллективе вежлив и дружелюбен. Претензий и замечаний во время прохождения практики не получал. Получил устную благодарность от руководства организации за добросовестное и качественное выполнение поставленных при прохождении практики задач.

Программу прохождения практики выполнил в полном объеме. Замечаний в ходе прохождения практики не получал. По результатам практики рекомендована положительная оценка.

Поднял платформы для поддержания ИБ, такие как Graylog, OpenDLP. Заданную задачу с сетью полностью выполнил создав под организационную архитектуру сети внутреннюю сеть в Windows Server 2022 с LDAP сервером и подключил к Graylog. Дополнительно добавил пользователей к OpenDLP для сохранения данных от кражи. В любой ситуации решал проблемы более уверенно и отличился аналитическим мышлением.

Рекомендуемая оценка: **100**

Руководитель практики от организации: Аймагамбетова Раушан Жанатова

## **Introduction**

In this report will be unfolded about the collected experiences and learnings in field of Cybersecurity and its fundamental begins. And passed practice place was the Kazakhstan Institute of Standardization and Metrology company which is the governmental organization that dealing with the standardization, metrology and technical regulation issues in Kazakhstan. For instance, when we are dealing with business there it comes for standardizations and other things to be legal. Furthermore, they acquired with internet shop of standards as GOST international standard, GOST "Conformity assessment. Study of product design", GOST Small arms terms and definitions and other type of standards.

By coming to my industrial practice, I went to IT specialists duties and obtained magnificiently more experiences from discovering a physical layer of widely known OSI 7 layers. The practice duration was 8 hours of work as beginning from 09:00 am until 06:30 pm at 5/2 works with 2 weekends.

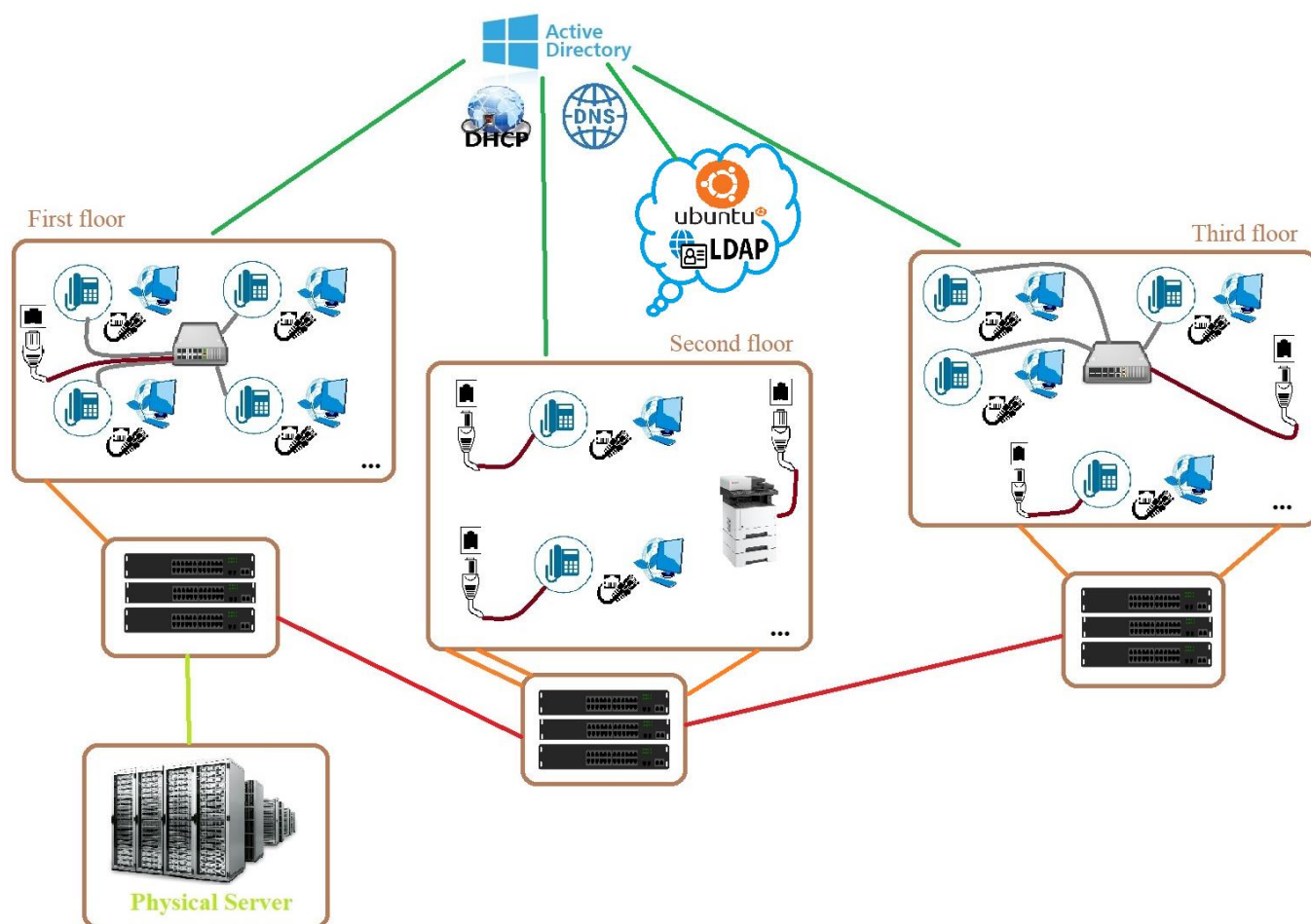
The objective of industrial practice was to explore government building information technology infrastructure and collect main pieces of knowledge to Information Security and in it to Cybersecurity profession.

The next step of exploration subject was to use physical and network layer basement knowledge and by considering their functions being able to connect and secure them from gain access by considering their vulnerabilities and other kind of external attacks and furthermore on account of it to acquire knowledge of Penetration Tester and Information Security Specialist. They are useful for learning their vulnerabilities, for instance, port, cable, and radio wave vulnerabilities to be aware of data leaks.

The practice results relied on the objectives and plan of works to do. The auditor of practice was chief of IT Specialists Abylai Imanberdinov and discovered practice procedures supporting with advice and giving experiments to be more advanced in my profession sphere. But also, there was a full-time scheduled practice with 8 hours of standard work hours.

## **1. Network architecture of Organization**

Everywhere we are able to see internet routers and other kind of simple network architecture and their segments as network device, for instance, in University, in Cafe and other locations. But in organizations where a security is the significant thing and their intranets might be much more difficult or in other side, simple and even secure. Furthermore, for my astonishments in KazStandard was a lightweight network architecture, because when I was in other government buildings, in Ministry of Industry and Infrastructure Development of Kazakhstan, there was a little complex network architecture with one more domains and other things. By coming to KazStandard's networks they had one domain with less restrictions on user's sides and was understandable for eyes but covering with satisfactory protection to be comfortable to users. But they was equipped with three or more servers as for website and for users as Active Directory in Windows Server. Next we can see the KazStandard net builds on Picture 1.



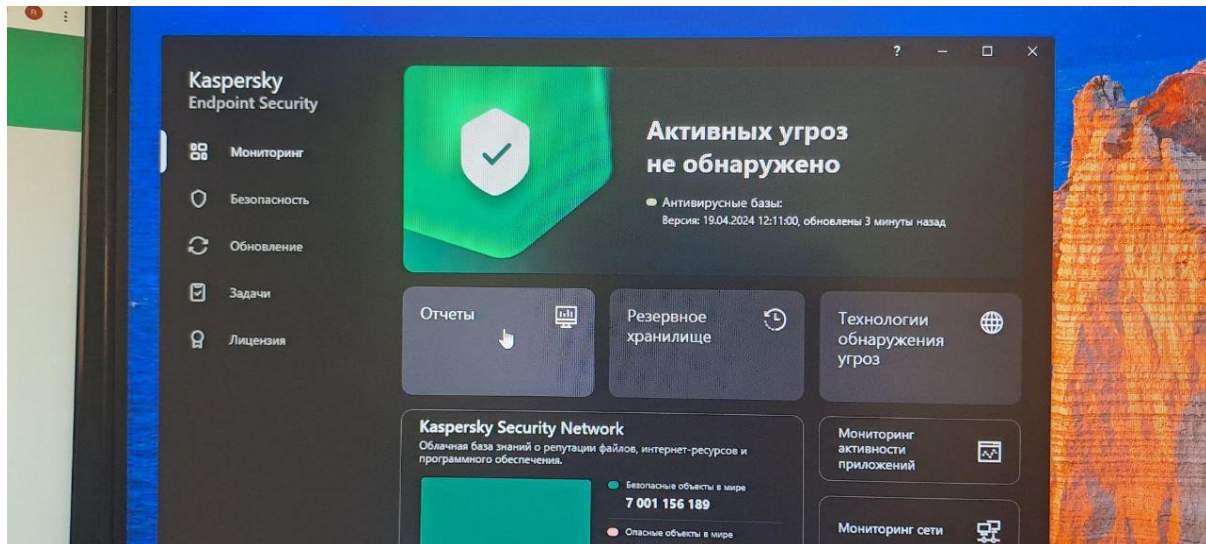
**Picture 1.** KazStandard Intranet Network Architecture

The Intranet architecture is essential to know, and it was a pre-assignment to me by a curator. They have only one domain, and as I said before about servers, they've covered one physical server and one Ubuntu server with an LDAP server on it for using one or two network printers for the floor. To provide private internet, they possessed IP phones, and internet access was provided through them to computers by Ethernet cables. After that, it goes to switches and to other switches. In KazStandard, there were 3 floors with workers, and if in one cabinet sat two more workers, there would be a hub to share the internet. Therefore, on each floor, there was one room with switches that connected to each other and, in the end, went to one physical server on the first floor.

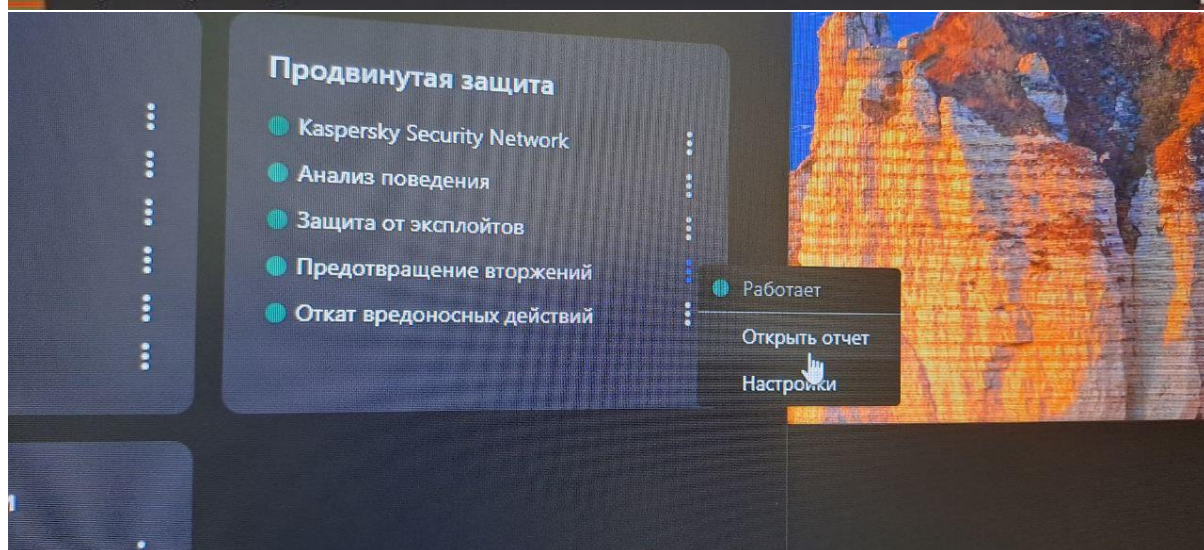
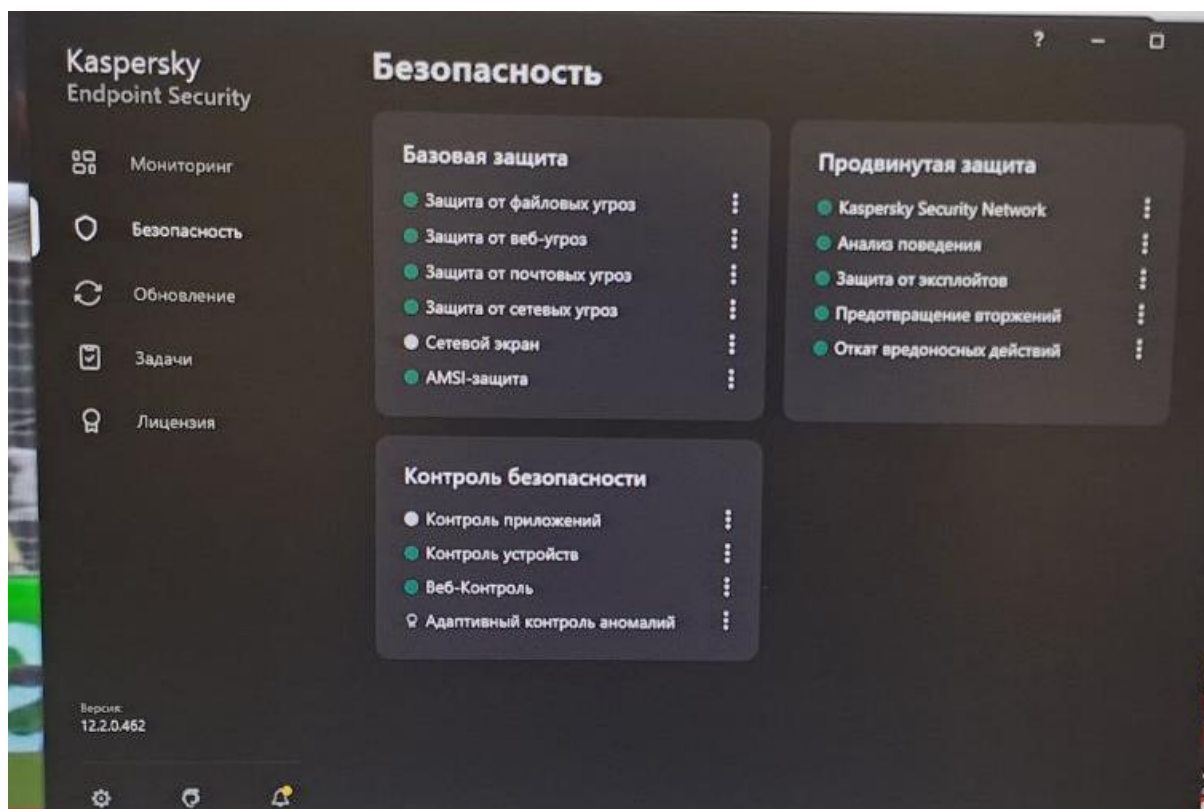
## 2. Information Security of Organization

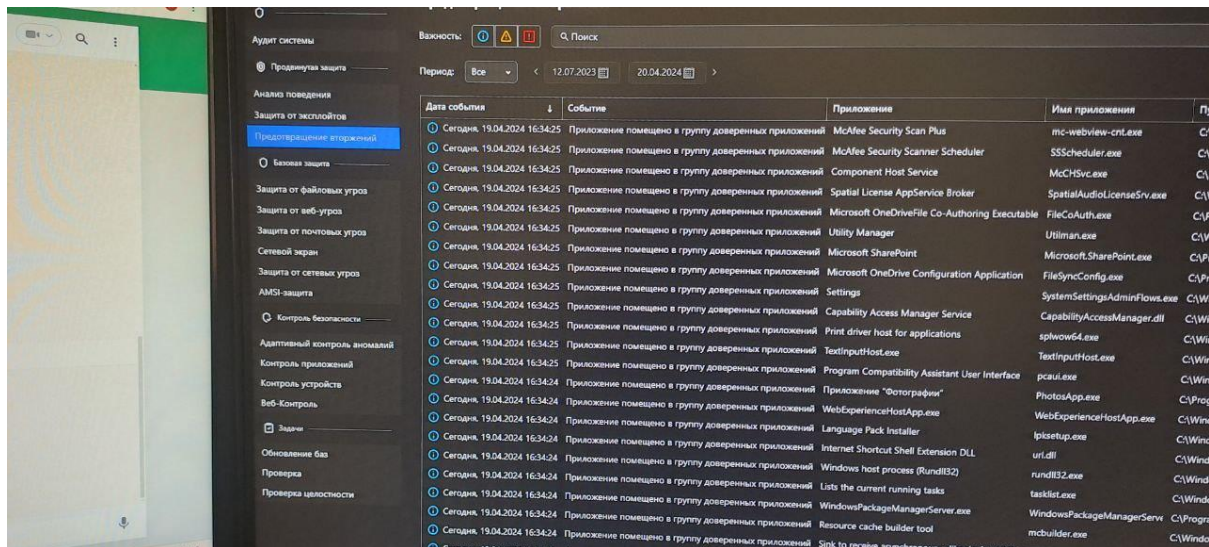
In the process of practice, I have had occasions to check the information security of organizations. To be more professional in my sphere, some questions bothered me, and other IT specialists helped me gain knowledge about company information technology infrastructure security. They had not so complex security in their company and in endpoint devices usages. Briefly touching their security side, they had a settled Group Policy Object (GPO) of Active Directory and Kaspersky Endpoint Security with its antivirus. If I say about the group policy

they had, in every user's computer, nobody is able to change any option of computer settings except the system administrator of Active Directory or of domain. It is needed to be protected from any external changes from the user side or hackers. The next level of protection is about DLP (data loss prevention) and, in addition, virus monitoring to be aware of computer malware. For DLP system a company possessed with an Endpoint Security relied on defending by managing the system at the endpoint side. Kaspersky Endpoint Security owned with basic antiviruses functions, IPS (Intrusion Prevention Systems), and reporting of each action, that antivirus segments made or activities users made around of whole computer consuming, which we are able to see on the Picture 2-5.









Picture 2-5. Kaspersky Endpoint Security features

### 3. First stage assignments

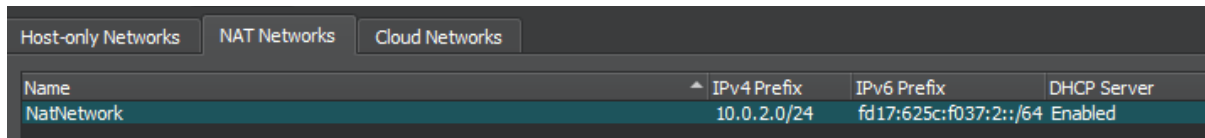
By coming to the first assignments part, I had to execute some activities with networking as the duties of System Administrator. The aim of the first task focused on acquisition of insights around security issues and information security of organization globally. For receiving some practice skills, I should create an intranet of company in my virtual machine. As a virtual machine platform Virtual Box was consumed with Windows Server 2022 virtualization and Active Directory in it. Furthermore, Active Directory is needed in the LDAP configuration in order to connect with the internet printer and its website on the Ubuntu Server. But for lightness of task and knowledge gains, the curator indicated that I should just configure LDAP by adding it in Role and Features of Active Directory.

Windows Server 2022 is a platform that is necessary for organizations, and it might work as the creation of infrastructure for websites, applications, and workgroups just in our case. It is the widespread, convenient server for system administrators demonstrating its sufficient features, roles and other functionalities. Additionally, it facilitates with any roles and features as well as LDAP, which I've done completely.

If briefly touch to LDAP (Lightweight directory access protocol), it is a protocol which requires license management, authorization of users merging with their emails as the email services, and user accounts with managing, for information discovers about users, organizations defined as infrastructure. It has two insights in storing data and directory authentication to users. And this protocol is used by the LDAP server of the company to store user data and authenticate them to gain access to the network printer.

## a. Set up a Private Network

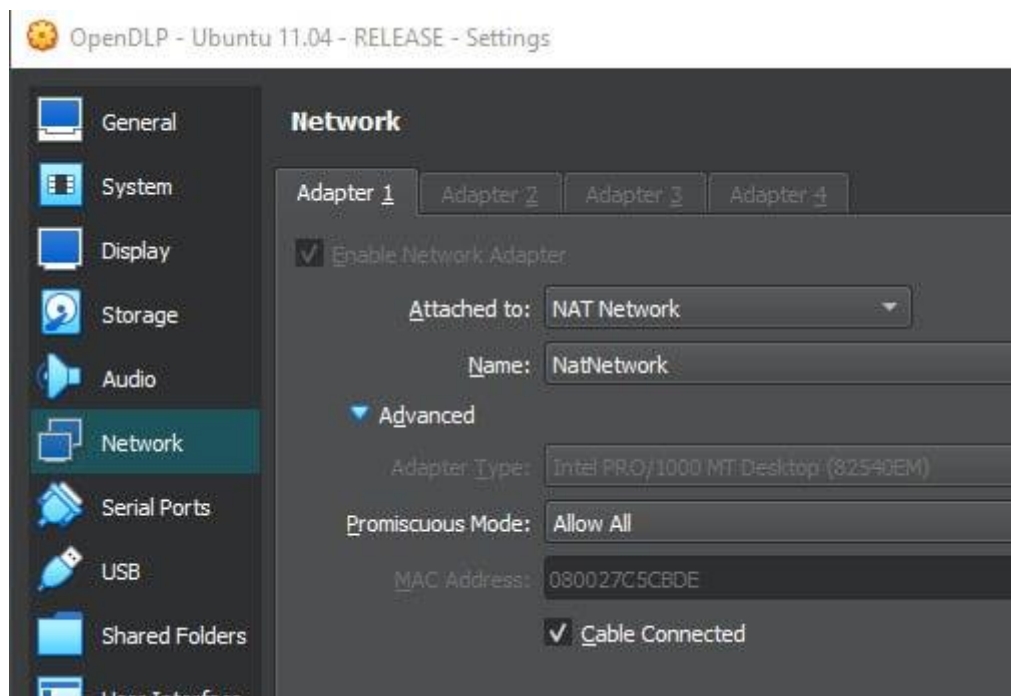
The creation of private network required for DHCP Server and for this realization Virtual Box covered with DHCP server over NAT Networking with 10.0.2.0/24 net mask which we are able to see in Picture 6.

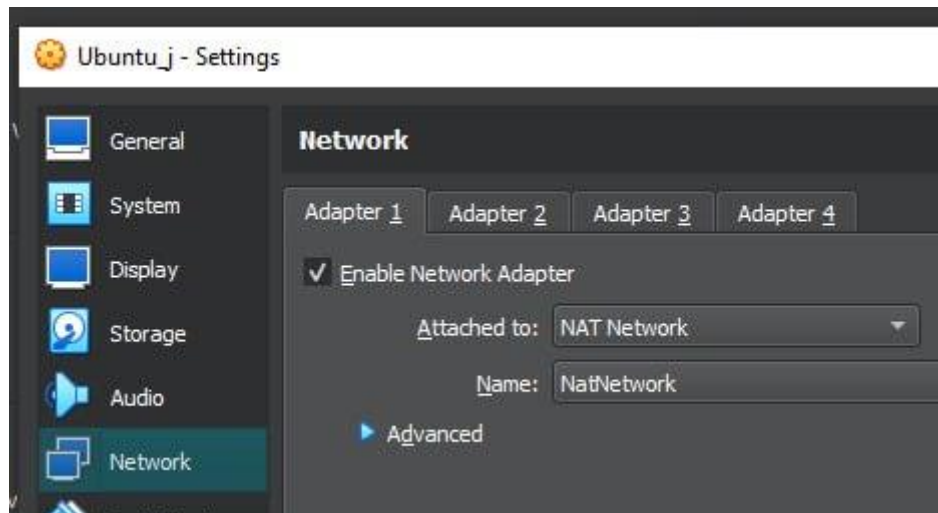


Host-only Networks   NAT Networks   Cloud Networks			
Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	10.0.2.0/24	fd17:625c:f037:2::/64	Enabled

**Picture 6.** NAT Networks

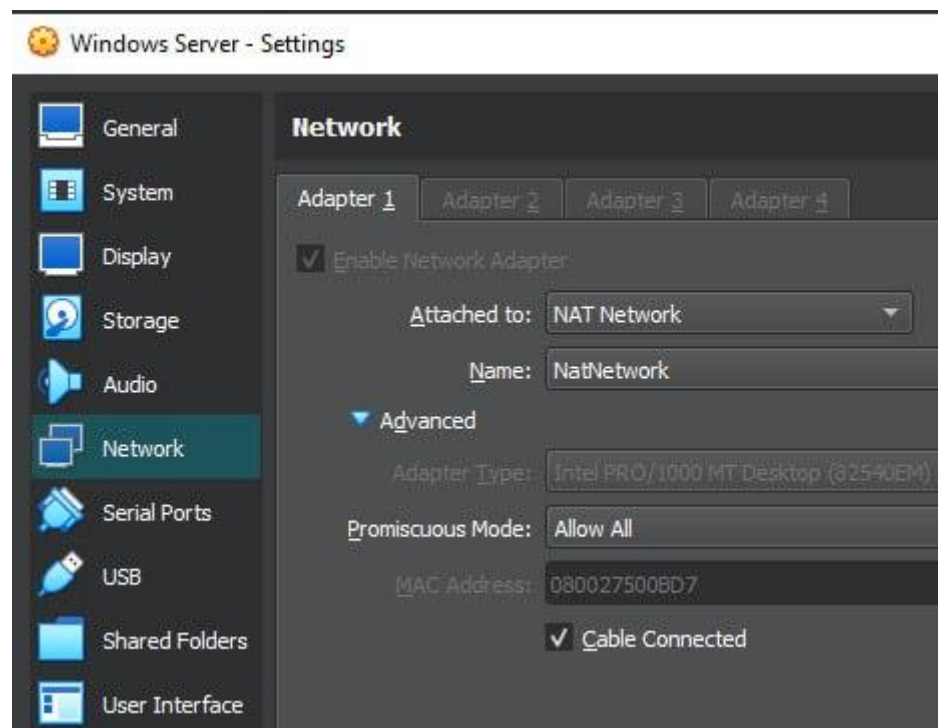
NAT Networks (Network Address Translation) it is a network that is navigating private addressed devices in the local network to a global network with public addresses. But likely this we possessed with NAT that is widely used in the most of organizations which is similar to NAT Networks, but NAT Networks providing local network to internet in the VirtualBox ensuring internal communication between virtual machines but they might not speak with external internet equipments which is needed in adding some configuration to be able to intercommunicate with external network devices. The NAT Networks necessity relied on the intercommunication of the three virtual machines and they are Ubuntu 11.04 with 512MB RAM, Ubuntu 22.04 with 4GB RAM and final one Windows Server 2022 with 6GB RAM which are shown with NAT Networks changement in Picture 7-8.





**Picture 7-8.** Ubuntu 11.04 and Ubuntu net preconfiguration

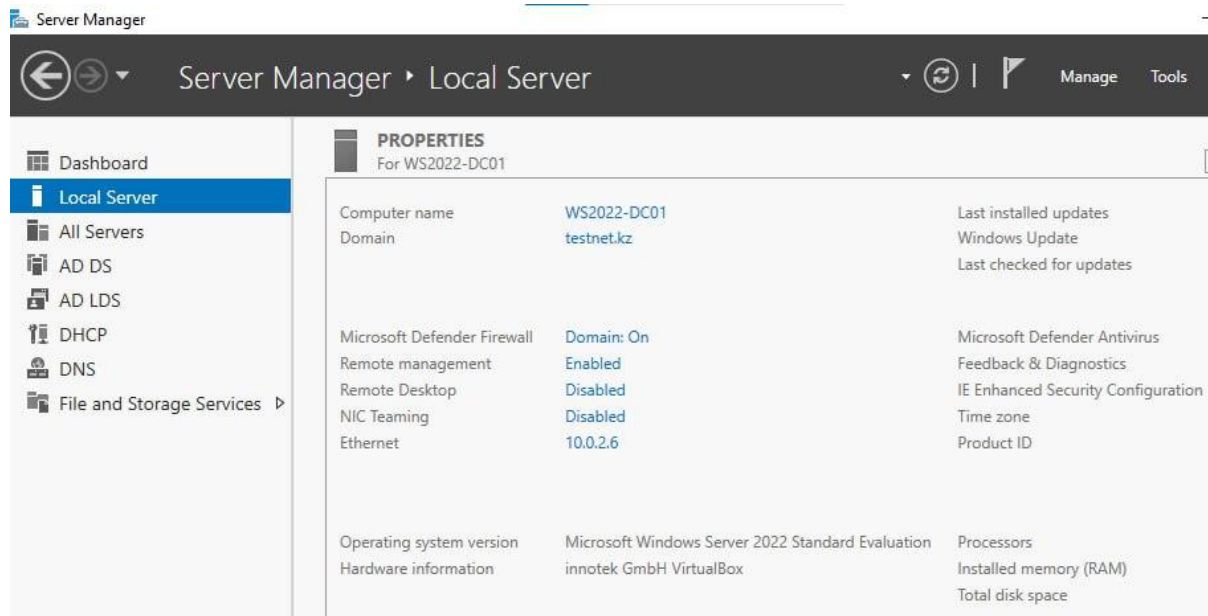
By coming to Windows Server part, first we should configure its network issues and change it to NAT Networks which we can see in Picture 9.



**Picture 9.** Windows Server 2022 net preconfiguration

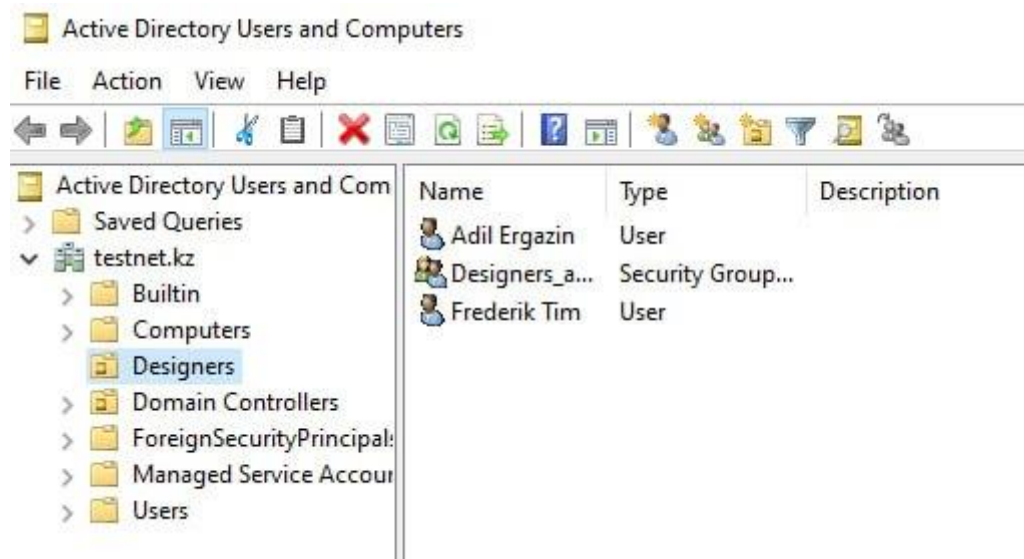
In the next step we are configuring Windows Server to static IP with 10.0.2.6 and executing DNS and DHCP server installations to be able to provide internet by obtaining DNS requests from client side (DNS Server) and assign IP addresses to active directory users (DHCP Server) in Role and Features. And they are already displayed in Picture 8.

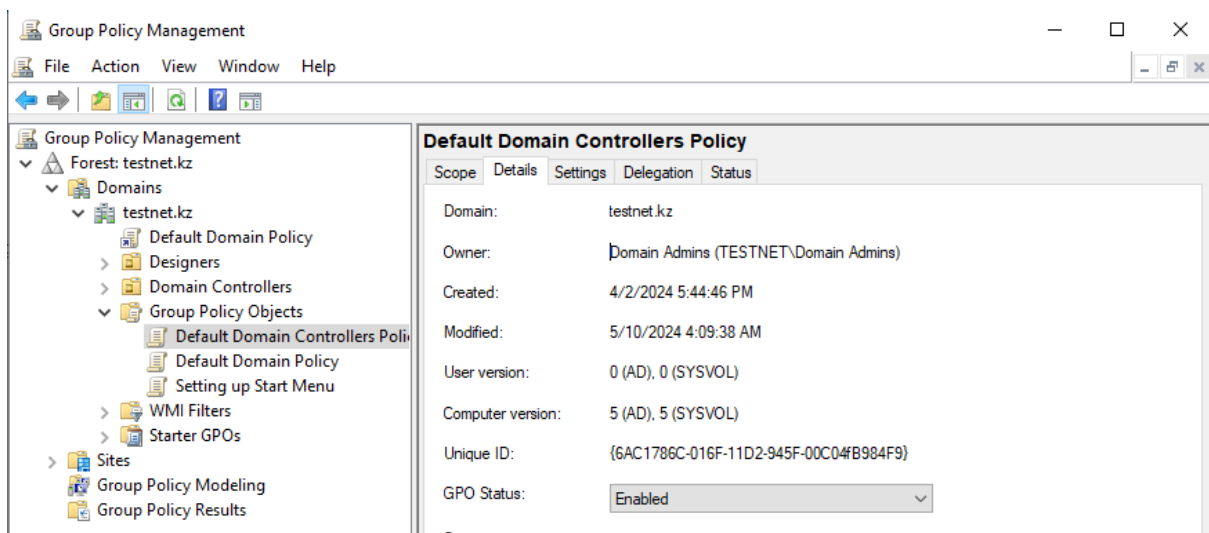
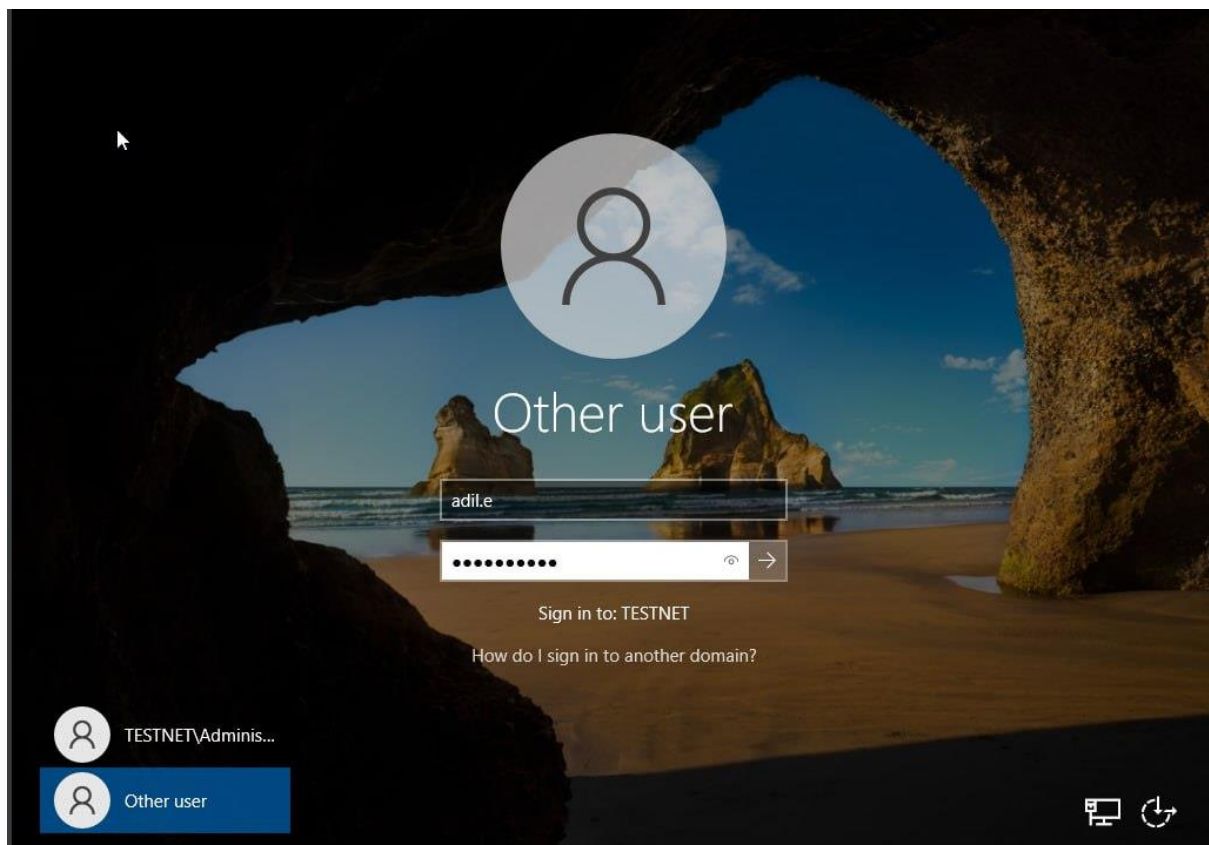




**Picture 10.** Windows Server 2022 configurations

As displayed on Picture 8, I had created one domain to my internal network defined with a name testnet. In the next step, two users were created: adile and frederik, who joined the designers admin group and configured with some changes in the GPO (Group Policy Object) of Active Directory for complete safety. And they are indicated in Picture 11-13.



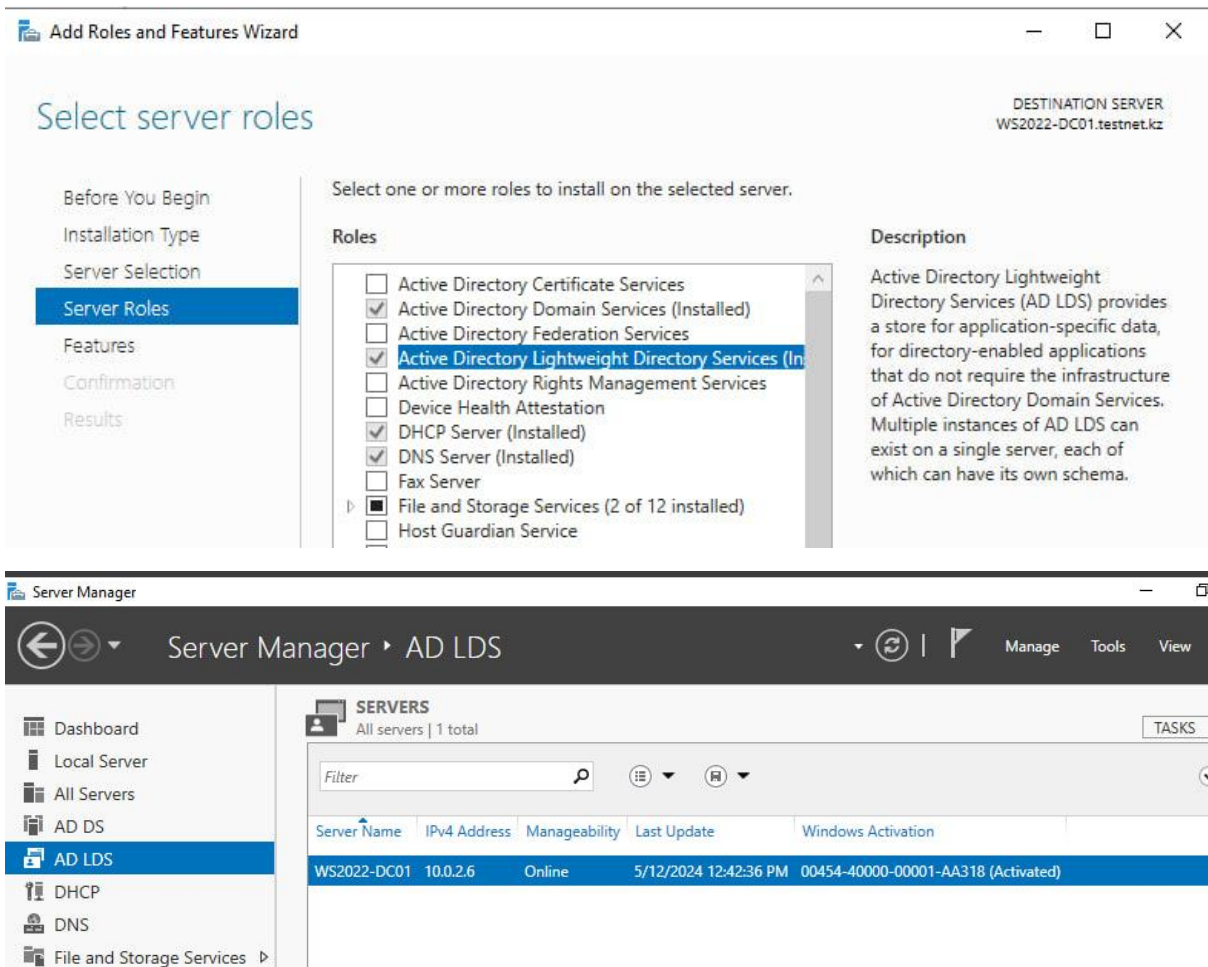


**Picture 11-13.** Active Directory security procedures

## b. LDAP addition

In the part of LDAP addition was needed just install the AD LDS (Active Directory Lightweight Directory Services) in the roles and features tab and configure it with creating network service account where we should name the DC (Domain Controller) with its DNS

(Domain Name Service) which was kz and OU (Organizational Unit) which was designers admin where adil.e user is located. And the installation process we might see in Picture 14-15.



Picture 14-15. LDAP installation

#### 4. Second stage assignments

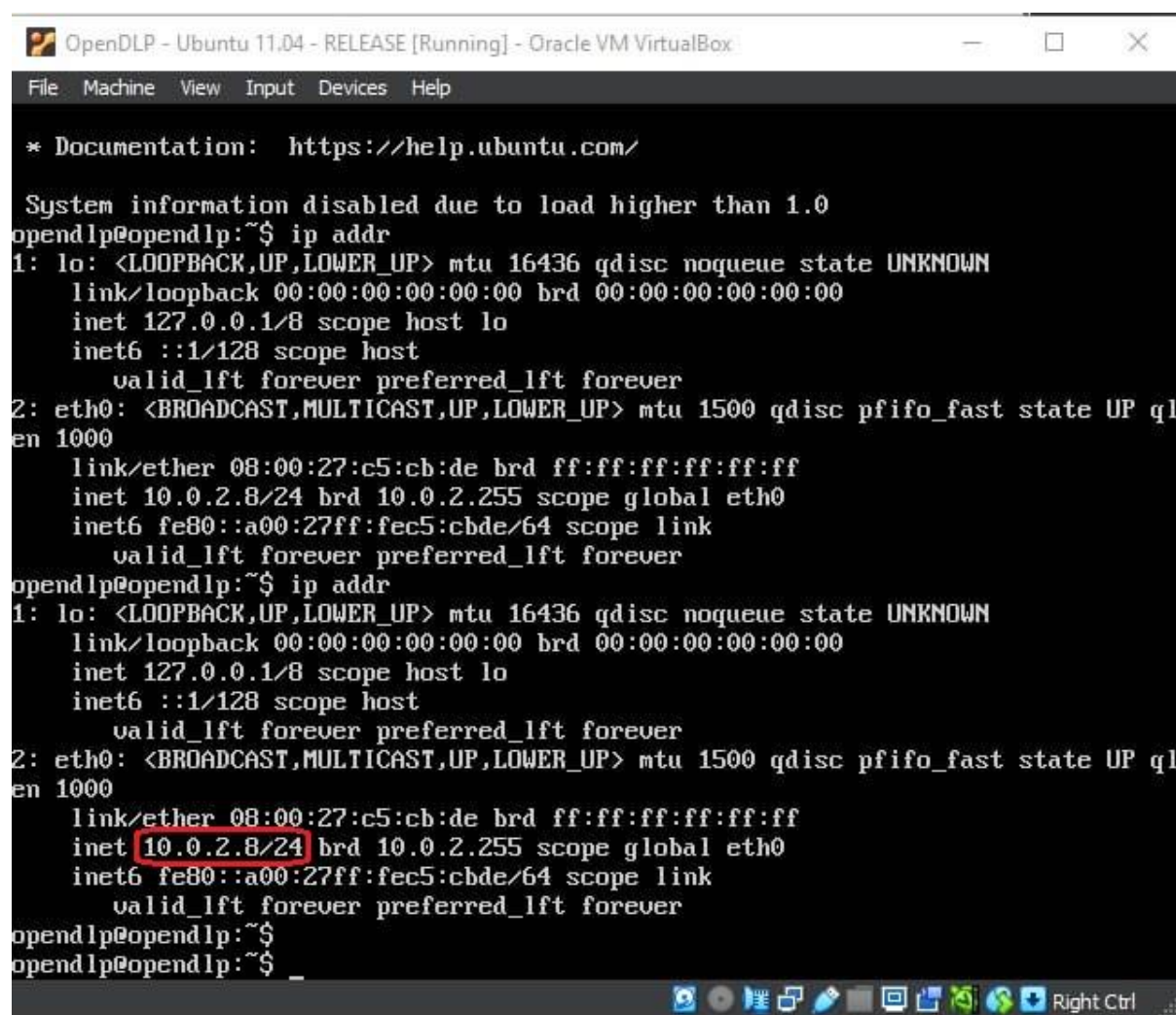
In the second part of assignments the obtained tasks from the curator were to deployment of information security platforms called as Graylog on Ubuntu and OpenDLP on Ubuntu 11.04. Also they should be communicated with each other. The purpose of the second tasks was in deeply discovering the information security issues of information technology infrastructure and being able to install, deploy and utilize its protection tools.

The deployment of cybersecurity tools were successfully done with complete understanding. The tools such as the Graylog is a prevalent in most of companies, open source tool needed for log management and partially working as SIEM system. And if say about the second tool called as OpenDLP it is an open source, mostly Ubuntu 11.04-based d at a loss prevention centralized and agent extensible, agentless tool released by GPL. The OpenDLP is a crucial for not so large, small businesses to be able to save sensitive data from external

accesses. But Graylog on the other side, is needed for monitoring logs of company what kind of incidents will be and what type of incidents occurred to sit in a safe position. For instance, in this company, Graylog is usable and in such as the Ministry of Industry and Infrastructure Development of Kazakhstan additionally meaning they are government buildings.

## a. Deployment of information security platforms

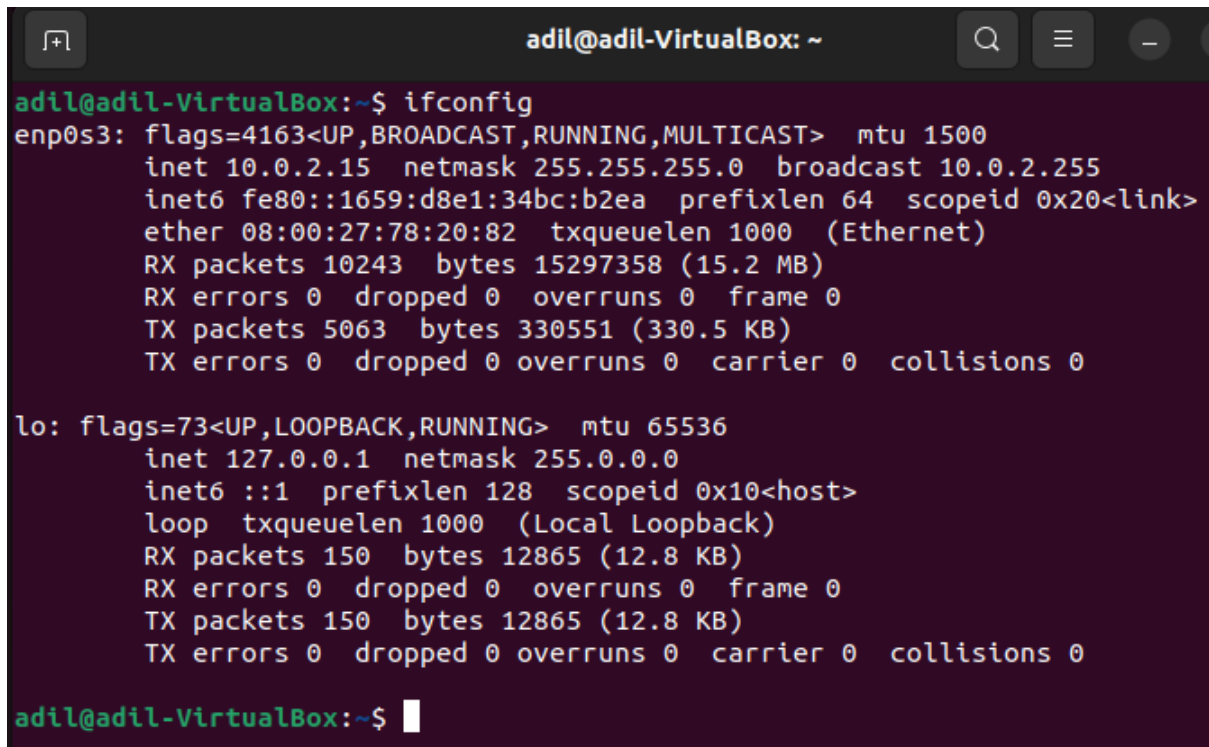
For a deployment of information security platforms was needed interconnected virtual machines, therefore Ubuntu and Ubuntu 11.04 were installed in VirtualBox and net preconfiguration was made for intercommunication abilities which are we might see in Picture 7-8. But also over the VBox DHCP Server with IP address 10.0.2.3 was obtained 10.0.2.8 to OpenDLP Ubuntu 11.04 virtual machine. Furthermore, Ubuntu was declared over the 10.0.2.5 IP address. And they are shown in Picture 16-17.



```
* Documentation:  https://help.ubuntu.com/

System information disabled due to load higher than 1.0
opendlp@opendlp:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:c5:cb:de brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.8/24 brd 10.0.2.255 scope global eth0
        inet6 fe80::a00:27ff:fec5:cbde/64 scope link
            valid_lft forever preferred_lft forever
opendlp@opendlp:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:c5:cb:de brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.8/24 brd 10.0.2.255 scope global eth0
        inet6 fe80::a00:27ff:fec5:cbde/64 scope link
            valid_lft forever preferred_lft forever
opendlp@opendlp:~$
opendlp@opendlp:~$ _
```



A terminal window titled 'adil@adil-VirtualBox: ~' with search, menu, and window control icons in the title bar. The terminal shows the output of the 'ifconfig' command. It displays details for the 'enp0s3' interface, including its flags, MTU, IP address (10.0.2.15), netmask, broadcast address, MAC address, and statistics. It also shows details for the 'lo' loopback interface, including its flags, MTU, IP address (127.0.0.1), netmask, and statistics. The prompt 'adil@adil-VirtualBox:~\$' is visible at the bottom.

```
adil@adil-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::1659:d8e1:34bc:b2ea prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:78:20:82 txqueuelen 1000 (Ethernet)
    RX packets 10243 bytes 15297358 (15.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5063 bytes 330551 (330.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

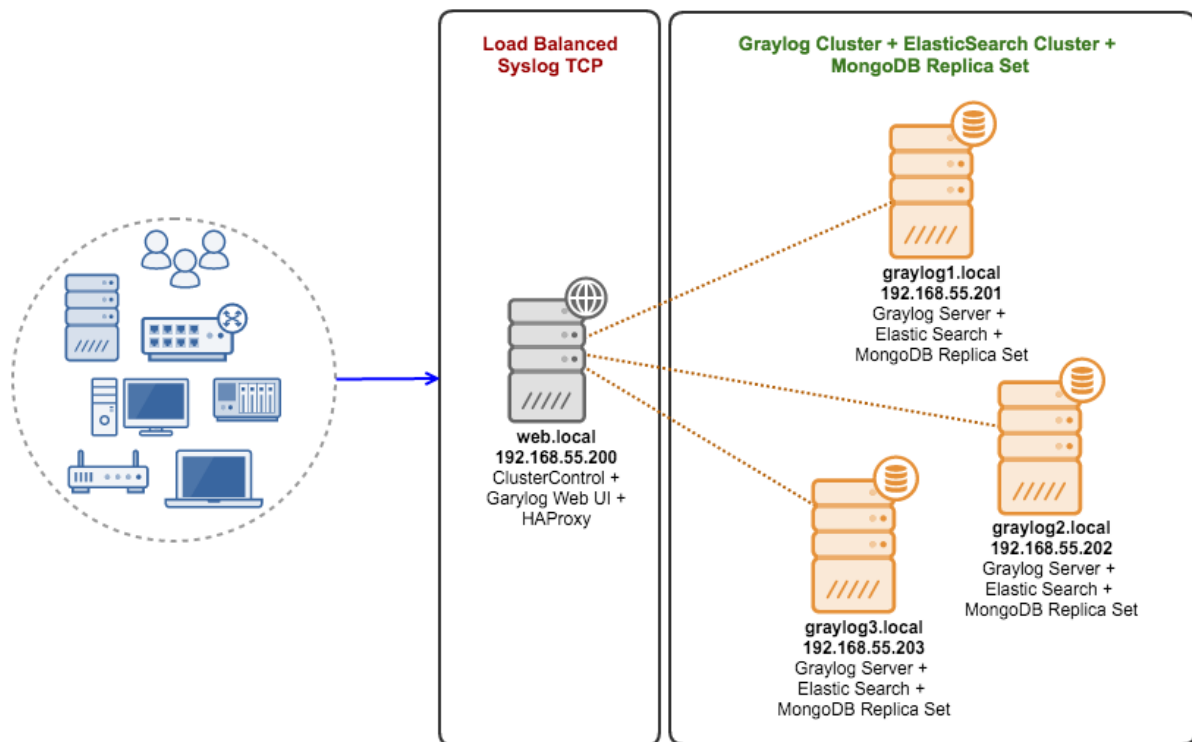
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 150 bytes 12865 (12.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 150 bytes 12865 (12.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

adil@adil-VirtualBox:~$
```

**Picture 16-17.** OpenDLP and Ubuntu configurations

## **b. Graylog deployment and connecting with Active Directory**

In the deployment of Graylog on the Ubuntu virtual machine we should needed to install part by part with tools such as ElasticSearch or OpenSearch, MongoDB, and the Graylog in the final step. But nowadays one of the part is elder and it is ElasticSearch, so OpenSearch is more required. In order to understand the structure of Graylog and its workflow we might see its structure on Picture 18.



**Picture 18.** Graylog structure

In the Picture 18, we might see the devices which are deployable or possessed with the ability of connection and in our case it is a Windows Server 2022 with Active Directory. But for connecting Graylog to Windows Server it is not mandatory to be in internal network, therefore it was deployed on Ubuntu Server. Additionally, Ubuntu utilized for web interface of OpenDLP. And Graylog's IP address was 91.108.121.237 over the port 9000 as a standard port for Graylog configurations which we might see in Picture 19.

```

GNU nano 6.2 /etc/graylog/server/server.conf
#####
# HTTP settings
#####

#### HTTP bind address
#
# The network interface used by the Graylog HTTP interface.
#
# This network interface must be accessible by all Graylog nodes in the cluster and by all cli
# using the Graylog web interface.
#
# If the port is omitted, Graylog will use port 9000 by default.
#
# Default: 127.0.0.1:9000
http_bind_address = 91.108.121.237:9000
#http_bind_address = [2001:db8::1]:9000

```

**Picture 19.** Graylog server configuration

Next we should create an user in Users and Teams Active Directory and we can see the monitoring section after the connection of Active Directory in Picture 20-21.

graylog Search Streams Alerts Dashboards Enterprise Security System / Users 0 in 0 out

Users Overview

### Create New User

Use this page to create new Graylog users. The users and their permissions created here are not limited to the web interface but valid and required for the REST APIs of your Graylog server nodes, too. [Permissions documentation](#)

[Create user](#)

**Profile**

**First Name**   
The user's first name.

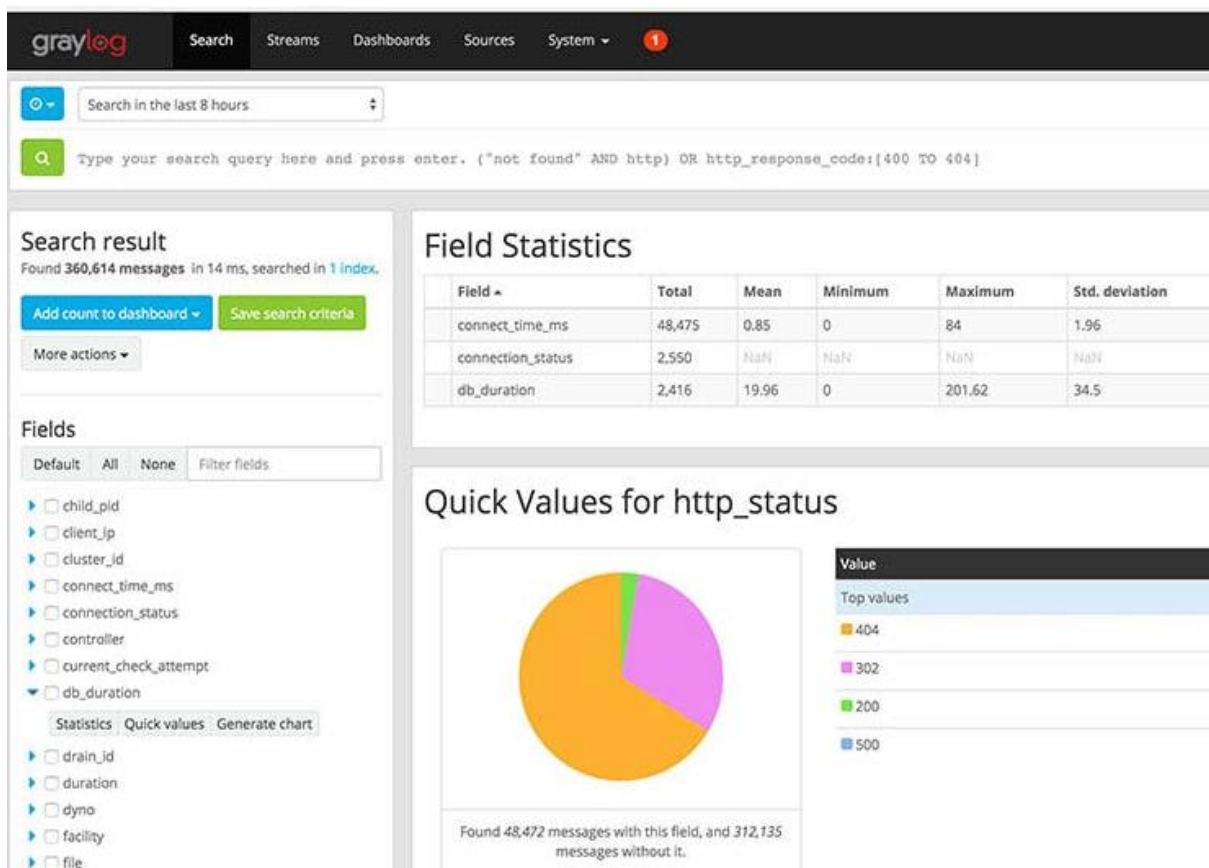
**Last Name**   
The user's last name.

**Username**   
Select a unique user name used to log in with.

**E-Mail Address**   
The user's email address.

**Settings**

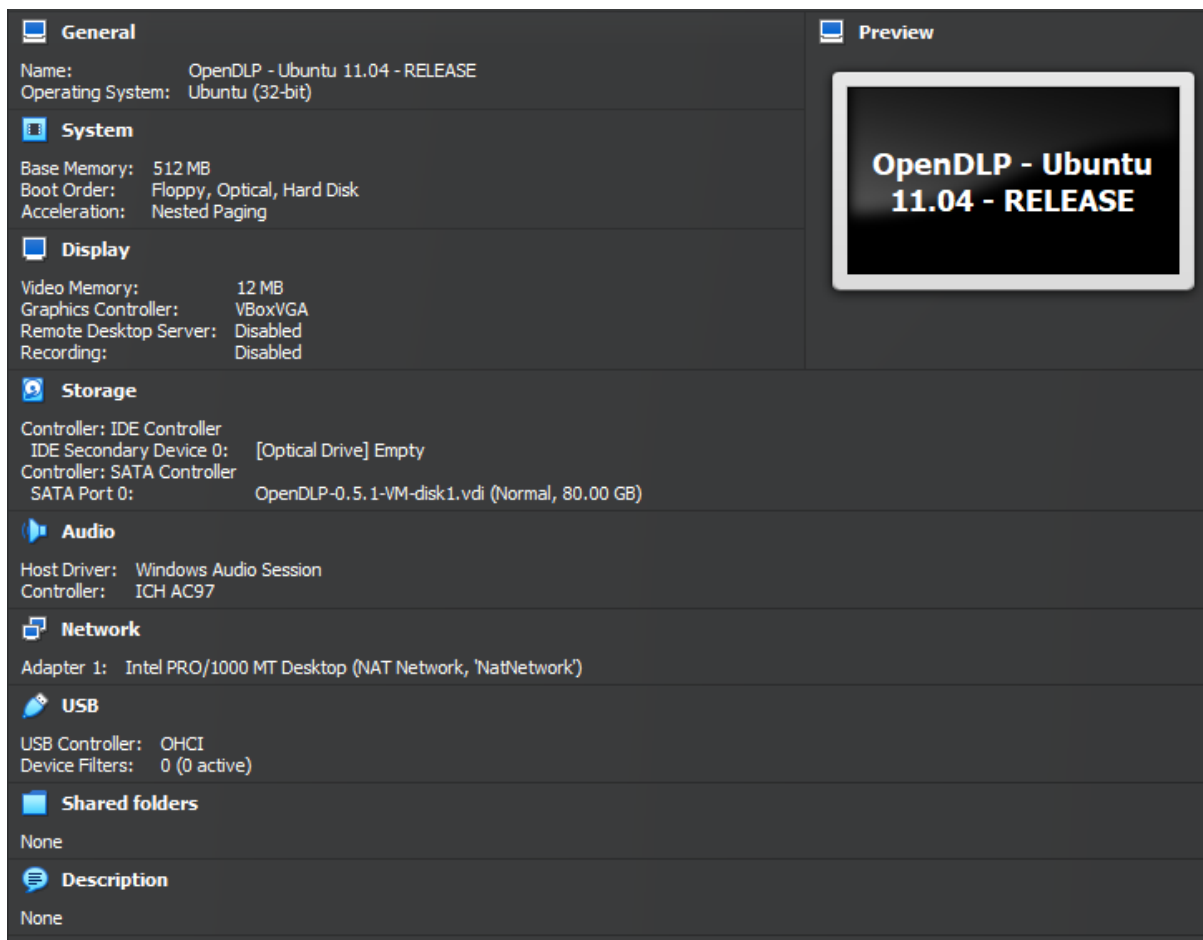
**Sessions Timeout** ☐ Sessions do not time out  
When checked, sessions never time out due to inactivity.



Picture 20-21. Graylog connection with Active Directory

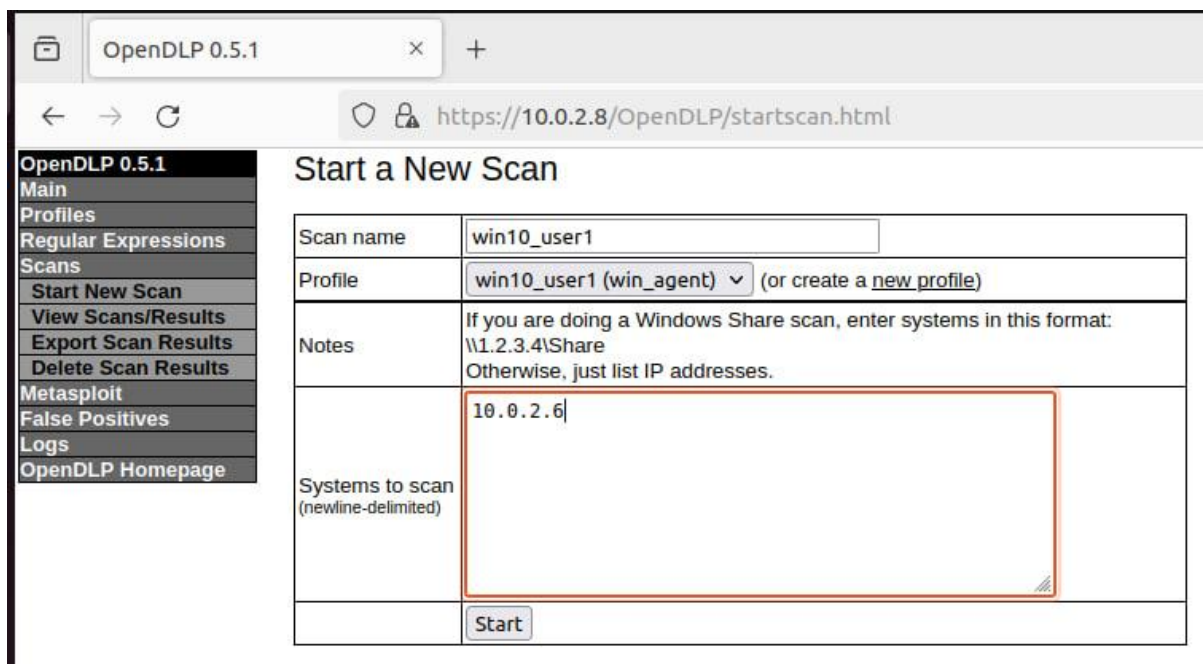
## c. OpenDLP deployment and agent connections

In the deployment of OpenDLP as I have told about Ubuntu in Graylog deployment section the Ubuntu was utilized to DLP web interface. If we concrete the deployment of OpenDLP, it is pretty simple for anyone with just its installation on Ubuntu 11.04 with its iso file. And it is showed a lightness of its configuration parts obtained with 512MB RAM and 10GB as the minimum memory of virtual disk image which is shown in Picture 22.



**Picture 22.** OpenDLP configurations

By navigating to agent connections, it was about to connect the user to OpenDLP in order to control it and defend the sensitive data. For the relationship with OpenDLP and Windows 10, the user acquired an adile account for checking sensitive data, as shown in Picture 23-24.



OpenDLP 0.5.1

https://10.0.2.8/OpenDLP/profiles-new.html

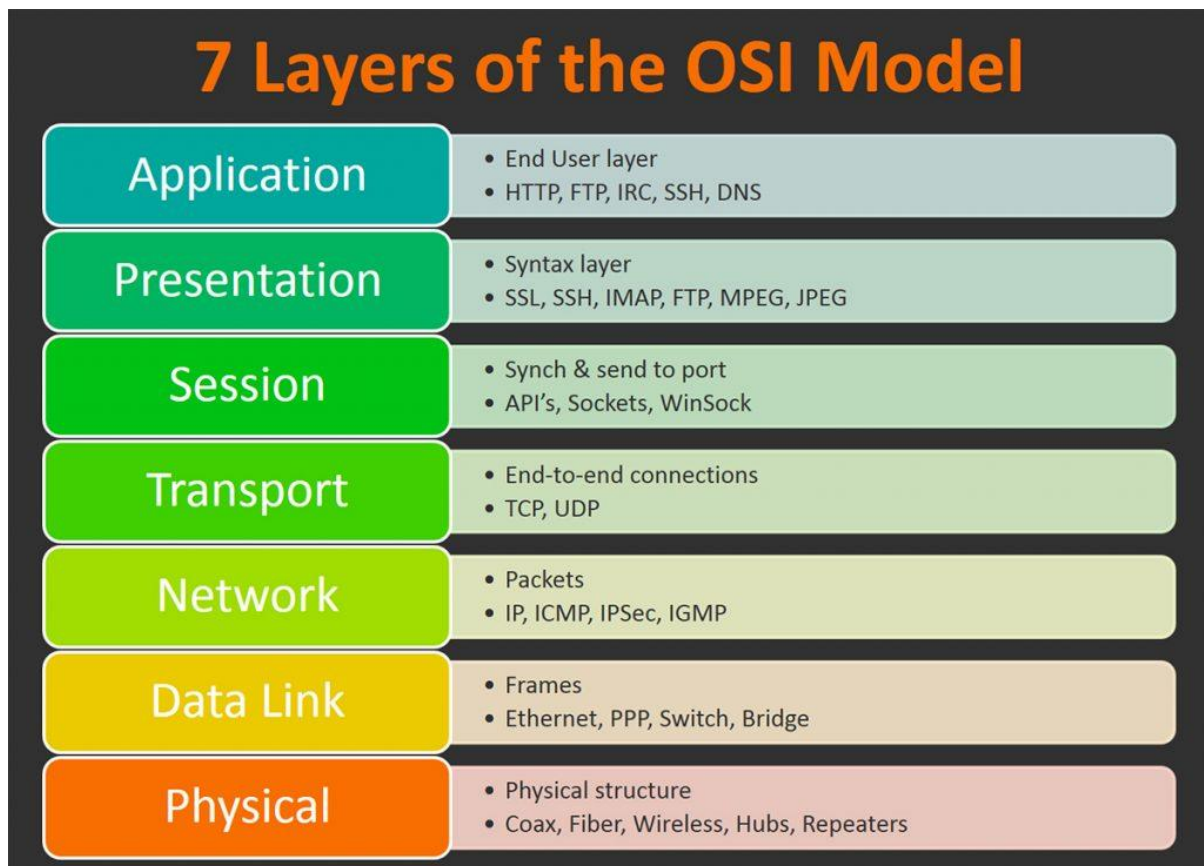
**New Profile Submission:**

Profile Name	win10_user1
Scan type	win_agent
Username	adil.e
SMBHash	
Password	*****
Domain Name	testnet.kz
Installation Path	c:\Program Files\OpenDLP
Memory Limit	10%
Mask Sensitive Data	Yes
Scan directories	everything
Directories	
Scan file extensions	ignore
Extensions	323 386 3g2 3gp 3gp2 3gpp 7z aac aca cmf cnv cod com ctx datasource del de j idl inf ink inl ism iso jfif jpe jpeg jpg ldf le mpegmpv2maw mpg mpq msi msp ncb pywqpa qt qti qtif qtl rar rb rbw rc rc2 rcc wma wmf wmv wpc wpl
Regular Expressions	AMEX, Credit_Card_Track_1, Credit_C Mastercard, Social_Security_Number_d
Credit Cards	Mastercard Visa AMEX Diners_Club_1
Zip File Extensions	zip jar xlsx docx pptx odt odp ods odg
Phone home URL username	dlpuser
Phone home URL password	*****
Phone home delay	300
Concurrent deployments	59
Windows Service description	deployed
Log Verbosity	0

**Picture 23-24.** OpenDLP agent connection

## 5. IT specialists duites

As an IT specialist we should know basics of information technologies and its equipments. For instance, in whatever situation we should be able to fix the problems that came from nowhere. In order to be able to fix problems in information technologies infrastructure we should know the OSI (Open Systems Interconnection) Model 7 layers which is shown in Picture 25.



**Picture 25.** OSI Model 7 layers

Furthermore, this knowledge helped me to analyze every problems in fixing them, beginning from physical layer ending with application layer.

## Conclusion

In the conclusion of whole two months practice, I have got completed knowledge around information technology infrastructure and its security issues. But actually, for being IT specialist might be a stepping origin ladder of information security and cybersecurity profession. And it might help to gain full experiences for being advanced, confident and prudent in cybersecurity sphere. By collecting insights from deployment issues, network configuration, creation of an internal network, connecting security platforms to internal network and users, analyzing activities in fixing problems completed in getting more experienced in the way of information security specialist.



## Reference

Lennart, K. (2024). Graylog documentation. [https://go2docs.graylog.org/5-2/home.htm?\\_ga=2.230691546.471004981.1713673429-697855700.1710865149&\\_gl=1\\*1s88db7\\*\\_ga\\*Njk3ODU1NzAwLjE3MTA4NjUxNDk.\\*\\_ga\\_4053DBR6X5\\*MTcxMzY3NTIzMy4yMTkuMC4xNzEzNjc1MjMzLjAuMC4w\\*\\_ga\\_NCQ7VMMZNQ\\*MTcxMzY3NTIzNC42MC4wLjE3MTM2NzUyMzQuMC4wLjA.\\*\\_gcl\\_au\\*N Dk0NDY3NDg5LjE3MTE5ODYyMDY](https://go2docs.graylog.org/5-2/home.htm?_ga=2.230691546.471004981.1713673429-697855700.1710865149&_gl=1*1s88db7*_ga*Njk3ODU1NzAwLjE3MTA4NjUxNDk.*_ga_4053DBR6X5*MTcxMzY3NTIzMy4yMTkuMC4xNzEzNjc1MjMzLjAuMC4w*_ga_NCQ7VMMZNQ*MTcxMzY3NTIzNC42MC4wLjE3MTM2NzUyMzQuMC4wLjA.*_gcl_au*N Dk0NDY3NDg5LjE3MTE5ODYyMDY)

Andrew, G. (2009). OpenDLP Google Archive.  
<https://code.google.com/archive/p/opendlp/>

Kazakhstan Institute of Standardization and Metrology, (2024). KazStandard.  
<https://ksm.kz/en/>

Justin, E. (2015, May 25). Understanding the LDAP Protocol, Data Hierarchy, and Entry Components. DigitalOcean.  
<https://www.digitalocean.com/community/tutorials/understanding-the-ldap-protocol-data-hierarchy-and-entry-components>

Ilya (2021, October 13). NAT (Network Address Translation) for beginners.  
<https://habr.com/ru/articles/583172/>