**Report by network security**

To fulfil our project, we have to install 3 virtual machines, which has a distributive called Ubuntu or another distributive Linux.

Our group chose Ubuntu as main operating system. Our task is to create a connection between a server and client using DNS tunnel.

As I wrote above, we will have 3 VMs, which will communicate each other. One of the VMs will performs a DNS server’s role. To do that, we have rented a server, which has a public IP address and, we have bought a domain name.

Text

Description automatically generated

As we can see our server has really public IP address, it means anybody can knock to its server from network, it simplifies to set up a DNS server since it doesn’t have to solve a problem with a private IP address, because every local computer has a private IP address. That’s why we have rented a server, it will be our DNS server. Our client will be created via Timofey’s local computer.

We have bought a domain name “timofeydankevich.com”, it can see settings of our domain name below.

Graphical user interface, text, application

Description automatically generated

We clarified the following lines, such as:

A is also known as a DNS host record, stores a hostname and its corresponding IPv4 address. We specified on our server that it has a hostname called “h.timofeydankevich.com”.

A picture containing shape

Description automatically generated

After that, we wrote that if someone refers to our name server or our hostname, then it must move on server’s IP address.

In order to deploy DNS server, which will translate our domain in IP address and back, primarily, we decided to install a tool called bind9.

We have the following parameters:

Our IP address: 109.228.58.81

Domain name: timofeydankevich.com

Primarily, we have created our zone in configuration file called named.conf.default-zones, this file contains information about zones, which are served by our DNS server.

Text

Description automatically generated

We have added our domain name “timofeydankevich.com”, also we defined our DNS server as master, that means it servers queries itself.

The next step is to configure a file called timofeydankevich.com.

Text

Description automatically generatedIt can see that this file contains the important settings for our domain name.

Text

Description automatically generated

The above file contains the common settings for our DNS server.

Text

Description automatically generated

This picture shows us our DNS server works successfully and it responds our clients. Now, we can start to install DNS tunneling using iodine. Primary, we have to stop bind9, which was used for deployment the DNS server and to install iodine on our DNS server and client.