Lab 01: Initial Setup

Network Infrastructure Security (CSP)  
 2024-2025

© Henk Brouckxon, Nico Declerck, Chris Roets

# Introduction

## Lab concept

During this lab, we will get acquainted with the NIS lab environment, and its systems. We’ll also look into some best-practice configurations w.r.t. remote management of servers.

## Learning goals

* Network discovery with nmap
* Getting acquainted with the NIS lab platform
* Getting acquainted with a new Linux distro for servers 😊
* SSH private key authentication

## Practicalities and prerequisites

You will need the following:

* A laptop/desktop 😊

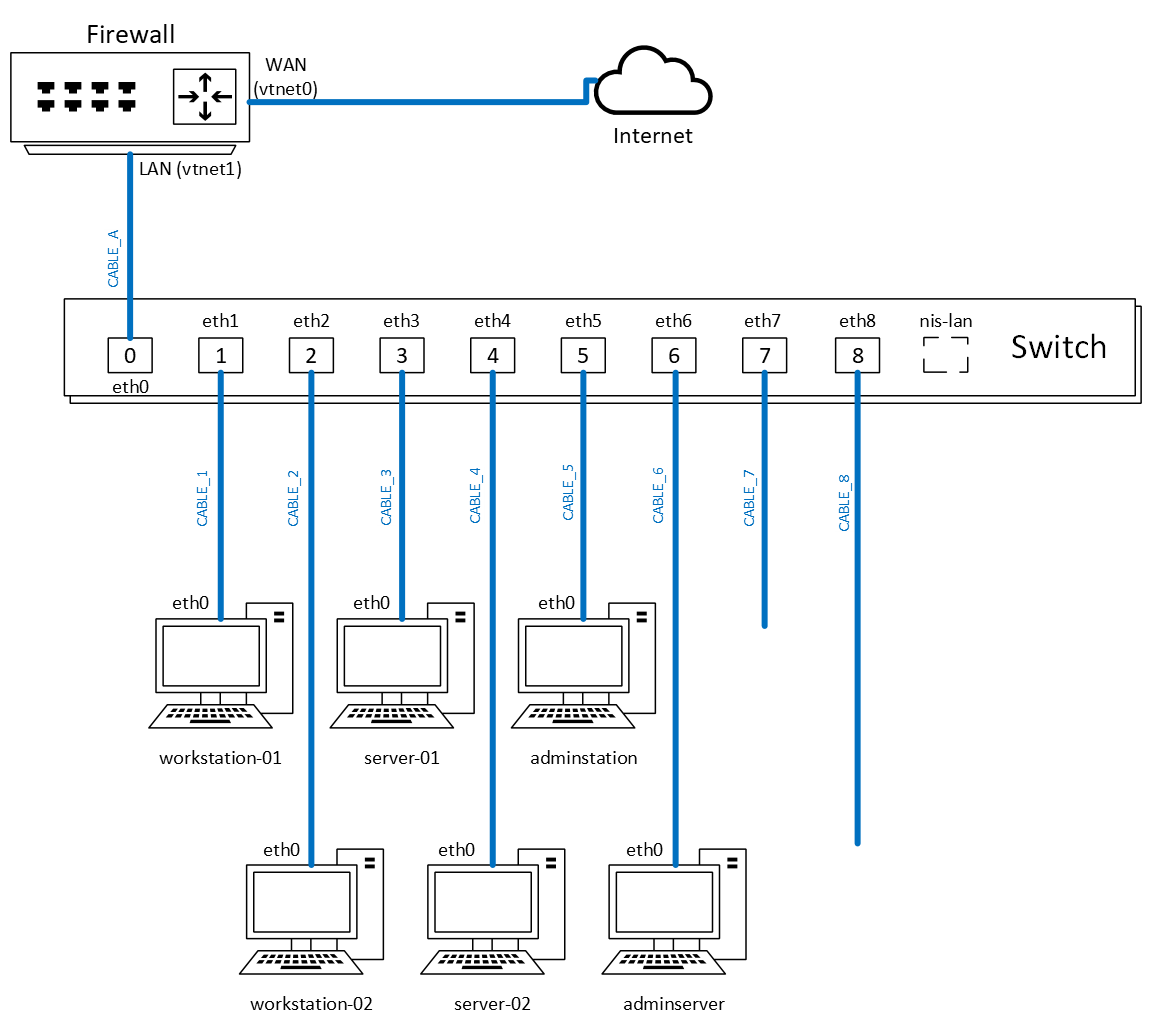


Figure 1 Equivalent physical layout for the NIS network

A computer icons on a black background

Description automatically generated

Figure 2 Equivalent logical layout for the NIS network

# A first exploration of the NIS environment

BEFORE THAT:

ACCESSING THE ENVIRONMENT:

* Connect to Howest-CIT-Hub (with howest credentials like eduroam)
* Go to https://10.30.6.11:8006
* Start the environment
* Then go to <http://serafim-ciobanu.co.edu.technet.howest.be:8006>
* Login with the credentials (in this student-student)
* CHANGE PASSWORD (CHECK THE PASSWORD MANAGER)

1. Connect to your assigned lab environment and start up the following virtual machines (VMs):

* 100 (firewall.nis.net)
* 101 (network.nis.net)
* 110 (workstation-01.nis.net)
* 111 (workstation-02.nis.net)
* 120 (server-01.nis.net)
* 121 (server-02.nis.net)
* 130 (adminserver.nis.net)
* 131 (adminstation.nis.net)

Do not start VM 102 (switch.nis.net), since this will for now cause problems and may crash your environment.   
These VMs were pre-configured to

1. Log in to the **adminstation** VM (131) as the “mickey” user, with the credentials that are given in the VM notes (VM “summary” tab).

Current user – mickey / rootroot

1. In general it is a good practice to always use personalized accounts, even for admin users. This allows logging who changed certain settings, and allows for easier management of who has access to what systems when the person’s role in the organization changes. Now create your own administrator user account for **adminstation**, with your first name (e.g. “henk”) as the username. From now on, you should use this personalized user whenever possible, and not the mickey user.   
   **Important remark**: in scored submissions of screenshots, we will require you to always use this account to prove that you performed the labs on your own environment.

sudo adduser serafim (set password – ciobanu)

sudo usermod -aG sudo serafim

su – serafim

groups (to check the groups)

A close up of a logo

Description automatically generated

1. Use nmap from the **adminstation** VM to scan all active hosts in the current subnet. The output of the nmap command should be limited to the lines containing hostnames and IP addresses of the machines. Insert a screenshot of the command and its output here.

ip -a (to find the eth0 network)

A computer screen shot of a computer code

Description automatically generated

sudo nmap -sn 10.0.0.0/24

A screenshot of a computer

Description automatically generated

1. Use nmap on the **adminstation** VM to determine which machines are hosting a website on the default HTTP port

sudo nmap -p 80 --open 10.0.0.0/24

A screenshot of a computer

Description automatically generated

10.0.0.5 - OPNsense.nis.net

10.0.0.20 - server-01.nis.net

10.0.0.21 - server-02.nis.net

1. What operating systems can you detect with nmap for the different hosts? For some of the hosts, this information may be relatively generic/incomplete, potentially because some of our VMs run as containers. Fill out the following documentation table as much as possible for the systems you’ve detected, without directly logging in to the different systems (not all information will be available yet)

sudo nmap -O 10.0.0.0/24 (to try and guess the OS)

cat /etc/resolv.conf (to get the DNS server)

A close up of a computer screen

Description automatically generated

ip r (to get the default route, and also the subnet mask)



subnet mask is /24 so 255.255.255.0 or 10.0.0.0/24

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| hostname | IP address | Subnet mask | Default Gateway | DNS | Operating System |
| OPNsense.nis.net | 10.0.0.5 | 10.0.0.5/24 | 10.0.0.5 | 10.0.0.5 | FreeBSD 11.X |
| network.nis.net | 10.0.0.6 | 10.0.0.6/24 | 10.0.0.5 | 10.0.0.5 | ??? |
| workstation-01.nis.net | 10.0.0.10 | 10.0.0.10/24 | 10.0.0.5 | 10.0.0.5 | Linux 4.X|5.X |
| workstation-02.nis.net | 10.0.0.11 | 10.0.0.11/24 | 10.0.0.5 | 10.0.0.5 | Linux 4.X|5.X |
| server-01.nis.net | 10.0.0.20 | 10.0.0.20/24 | 10.0.0.5 | 10.0.0.5 | Linux 4.X|5.Xs |
| server-02.nis.net | 10.0.0.21 | 10.0.0.21/24 | 10.0.0.5 | 10.0.0.5 | Linux 4.X|5.X |
| adminserver.nis.net | 10.0.0.30 | 10.0.0.30/24 | 10.0.0.5 | 10.0.0.5 | Linux 4.X|5.X |
| adminstation.nis.net | 10.0.0.31 | 10.0.0.31/24 | 10.0.0.5 | 10.0.0.5 | Kali Linux |

Table 1 Host documentation (initial nmap info)

1. Log in directly to the terminal of the individual hosts to gain more information. Here you can use the local root user account, as documented in the VM notes. Now fill out the complete table below (and add more details w.r.t. the OS):

uname -sr (to find the version of Linux and the release) / uname -a

traceroute google.com (to check the hops it does to find default gateway)

cat /etc/os-release (to find the version of linux used, and not Kernel)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| hostname | IP address | Subnet mask | Default Gateway | DNS | Operating System |
| OPNsense.nis.net | 10.0.0.5 | 10.0.0.5/24 | 192.168.16.1 | 127.0.0.1 + 192.168.16.5 | FreeBSD 14.1-RELEASE-p3 |
| network.nis.nit | 10.0.0.6 | 10.0.0.6/24 | 10.0.0.5 | 10.0.0.5 | Linux 6.8.12-1-pve  Alpine Linux 3.19 |
| workstation-01.nis.net | 10.0.0.10 | 10.0.0.10/24 | 10.0.0.5 | 10.0.0.5 | Alpine Linux 3.19  Linux 6.8.12-1-pve |
| workstation-02.nis.net | 10.0.0.11 | 10.0.0.11/24 | 10.0.0.5 | 10.0.0.5 | Alpine Linux 3.19  Linux 6.8.12-1-pve |
| server-01.nis.net | 10.0.0.20 | 10.0.0.20/24 | 10.0.0.5 | 10.0.0.5 | Alpine Linux 3.19  Linux 6.8.12-1-pve |
| server-02.nis.net | 10.0.0.21 | 10.0.0.21/24 | 10.0.0.5 | 10.0.0.5 | Alpine Linux 3.19  Linux 6.8.12-1-pve |
| adminserver.nis.net | 10.0.0.30 | 10.0.0.30/24 | 10.0.0.5 | 10.0.0.5 | Ubuntu 22.04.4 LTS  Linux 6.8.12-1-pve |
| adminstation.nis.net | 10.0.0.31 | 10.0.0.31/24 | 10.0.0.5 | 10.0.0.5 | Linux 6.8.11-amd64  Kali GNU/Linux 2024.2 |

Table 2 Host documentation (initial complete information)

# Accessing the VMs over SSH

1. Create a local personal user account (again based on your first name) with administrator rights on all hosts.   
   **Hint:** You may need to look up how administrator rights work on each of the Operating Systems of the different hosts.

for the network.nis.net it needs to start the service of ssh. (service sshd start)

for Alpine Linux, to add a user to the administrator privileges, do:

* adduser serafim (type password - ciobanu), and also for Alpine you can technically do everything via using doas instead of sudo

for Ubuntu:

* adduser serafim
* usermod -aG sudo serafim
* groups serafim

for FreeBSD:

* adduser (and provide all the information)
* pw usermod serafim -G wheel
* id serafim

Checklist:

* network.nis.net DONE (ssh [serafim@network.nis.net](mailto:serafim@network.nis.net) | THE SERVICE NEEDS TO BE MANUALLY STARTED EVERY TIME)
* workstation-01.nis.net DONE
* workstation-02.nis.net DONE
* server-01.nis.net DONE
* server-02.nis.net DONE
* adminserver.nis.net DONE
* firewall.nis.net (OPNsense.nis.net) DONE

1. Now go back to the adminstation host, and ensure that you can remotely log in to the other hosts over SSH from this machine.

Every SSH connection works, except for the network.nis.net it is always needed to start the service again (if shutdown). doas service sshd start

Even though it is possible to log in over SSH using classic username-password authentication (as you probably did in question 9), current best practices recommend using public key authentication. This authentication method is preferred over simple passwords for multiple reasons, but mainly security is an important factor. Public key authentication provides cryptographic strength that even extremely long passwords can not offer, and it frees the users from remembering complicated passwords (or worse yet, writing them down). In addition to security, public key authentication also offers usability benefits because it allows implementing single sign-on across multiple servers, and automated, passwordless login to simplify executing scripts.

1. On the adminstation host, create an SSH keypair for your personal user account. Use the ecdsa algorithm with a keylength of 521 bits to generate the keypair.

ssh-keygen -t ecdsa -b 521  
A screenshot of a computer

Description automatically generated  
Where are the keypair files located on the host?

in ~/.ssh

A screenshot of a computer

Description automatically generated

1. Now set up the other hosts, so you can use your newly generated keypair to log in with SSH from the adminstation using public key authentication. Also test whether SSH login in this way (i.e. without password) works.  
   hint: open-ssh includes a tool which will simplify copying the relevant key from adminstation to the remote servers.

Magic command is ssh-copy-id serafim@host

ssh-copy-id serafim@server-02.nis.net , then it prompts you for the password of the user, and then adds it.

CHECKLIST:

* server-02 DONE
* server-01 DONE
* workstation-01 DONE
* workstation-02 DONE
* network DONE
* adminserver DONE
* OPNsense DONE

Which key(s) is/are copied to the remote host? Only the public/private key, both or none?

Only the public key is being transferred to the remote host, as then you leave the private key on the host, and can verify yourself when logging in.

# Personalizing the VM hostnames

1. Personalize the hostname of all the VMs so they include your own first name. For example the hostname of server-01 would become server-01-chris (for a user called Chris). Remember that this hostname should also be updated in an important local file to avoid problems!

23.09 - Kali seems to be the only one that persists the values set for /etc/hosts and /hostname.

A screenshot of a computer program

Description automatically generated

Alpine of server01 and 02 just do not want to save and apply the changes.

UPD 25: Seems like it is a problem of Proxmox and it is getting fixed. But OPNsense can be changed.

To change the hostname on OPNsense (FreeBSD) - go to 10.0.0.5 via http firefox from Kali, then login with root or other admin, then System > Settings > General and look for Hostname field and change it. Give a reboot and done. It only changes the /etc/hosts though.

A computer screen with white text

Description automatically generated

The whole issue was regarding the Proxmox being the problem with hosts. After that, it appeared that the -sP flag did not work afterwards, because the hostnames were getting overwritten due to another service, which comes from the DNS server on our network. In this case it is the 10.0.0.5 server, overwriting the hostnames.

1. Now repeat the nmap scan from question 4 which should give the hostnames and IP addresses of the different hosts. Why have the hostnames not been updated? (hint: look at the man page of nmap). Change the configuration of the relevant server process to update the detected hostnames.

A computer screen shot of a computer

Description automatically generated

Could not even think to do a service scan on the OPNsense machine and see that

1. Run the nmap scan from question 4 one last time to verify that the shown hostnames are now correct, and insert a screenshot below (command + output). Finally update this information in your host documentation table in Table 3 below.

Had to manually check every possible hosts file and hostname, and also Unbound DNS service overrides, so that it does look properly.

A screenshot of a computer

Description automatically generated

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| hostname | IP address | Subnet mask | Default Gateway | DNS | Operating System |
| OPNsense-serafim-ciobanu.nis.net  / firewall.nis.net | 10.0.0.5 | 10.0.0.5/24  255.255.255.0 | 192.168.16.1 | 127.0.0.1  192.168.16.5 | FreeBSD 14.1-RELEASE-p3 |
| network-serafim-ciobanu.nis.net | 10.0.0.6 | 10.0.0.6/24  255.255.255.0 | 10.0.0.5 | 10.0.0.5 | Alpine Linux v3.19 |
| workstation01-serafim-ciobanu.nis.net | 10.0.0.10 | 10.0.0.10/24  255.255.255.0 | 10.0.0.5 | 10.0.0.5 | Alpine Linux v3.19 |
| workstation02-serafim-ciobanu.nis.net | 10.0.0.11 | 10.0.0.11/24  255.255.255.0 | 10.0.0.5 | 10.0.0.5 | Alpine Linux v3.19 |
| server01-serafim-ciobanu.nis.net | 10.0.0.20 | 10.0.0.20/24  255.255.255.0 | 10.0.0.5 | 10.0.0.5 | Alpine Linux v3.19 |
| server02-serafim-ciobanu.nis.net | 10.0.0.21 | 10.0.0.21/24  255.255.255.0 | 10.0.0.5 | 10.0.0.5 | Alpine Linux v3.19 |
| adminserver-serafim-ciobanu.nis.net | 10.0.0.30 | 10.0.0.30/24  255.255.255.0 | 10.0.0.5 | 10.0.0.5 | Ubuntu 22.04.4 LTS |
| adminstation-serafim-ciobanu.nis.net | 10.0.0.31 | 10.0.0.31/24  255.255.255.0 | 10.0.0.5 | 10.0.0.5 | Kali GNU/Linux Rolling 2024.2 |

Table 3 Host documentation (final complete information)