

Навчально-науковий інститут інформаційних технологій
Харківський національний економічний університет
імені Семена Кузнеця

Звіт

З Виконання лабораторної роботи №4
за дисципліною: “Організація безпеки функціонування веб-серверів”

Виконав: студент кафедри
Кібербезпеки та інформаційних
технологій

4 курсу, спец. Кібербезпека,
групи 6.04.125.010.21.2

Бойко Вадим Віталійович

Перевірив:

Лимаренко Вячеслав Володимирович

ХНЕУ ім. С. Кузнеця

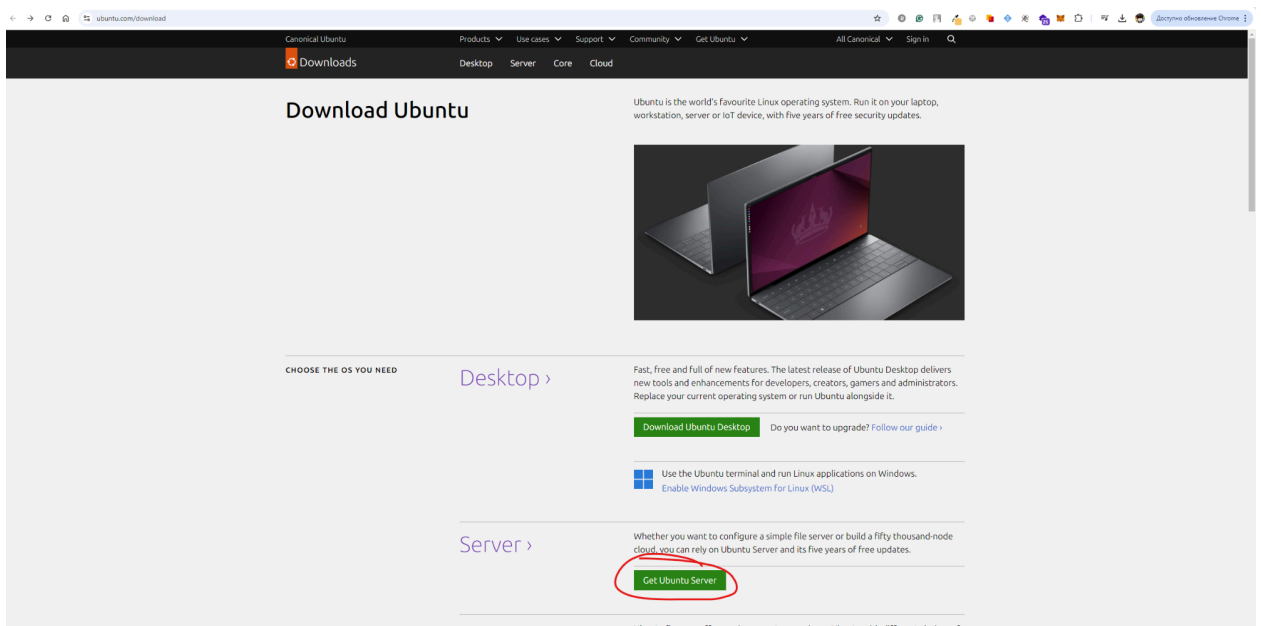
2024

Завдання:

1. Встановити у віртуальному середовищі на ОС Linux панель керування хостингом VestaCP <https://vestacp.com/> . Задля спрощення встановлення бажано мати "чисту" ОС Linux, без встановленого веб-серверу та його складових (MySQL, php).
2. Встановити панель моніторингу MUNIN <https://munin-monitoring.org/>.
3. Пройти курс Intro to Log Analysis на <https://tryhackme.com/r/room/introtologanalysis> за спробувати застосувати отримані знання на практиці.

Хід роботи:

Спочатку перейду на офіційний сайт та завантажу Ubuntu



Мені потрібна версія 18.04 оскільки вона підтримується ПЗ VestaCP

Ubuntu 18.04.6 LTS (Bionic Beaver)

Select an image

Ubuntu is distributed on three types of images described below.

Desktop image

The desktop image allows you to try Ubuntu without changing your computer at all, and at your option to install it permanently later. This type of image is what most people will want to use. You will need at least 1024MiB of RAM to install from this image.

64-bit PC (AMD64) desktop image

Choose this if you have a computer based on the AMD64 or EM64T architecture (e.g., Athlon64, Opteron, EM64T Xeon, Core 2). Choose this if you are at all unsure.

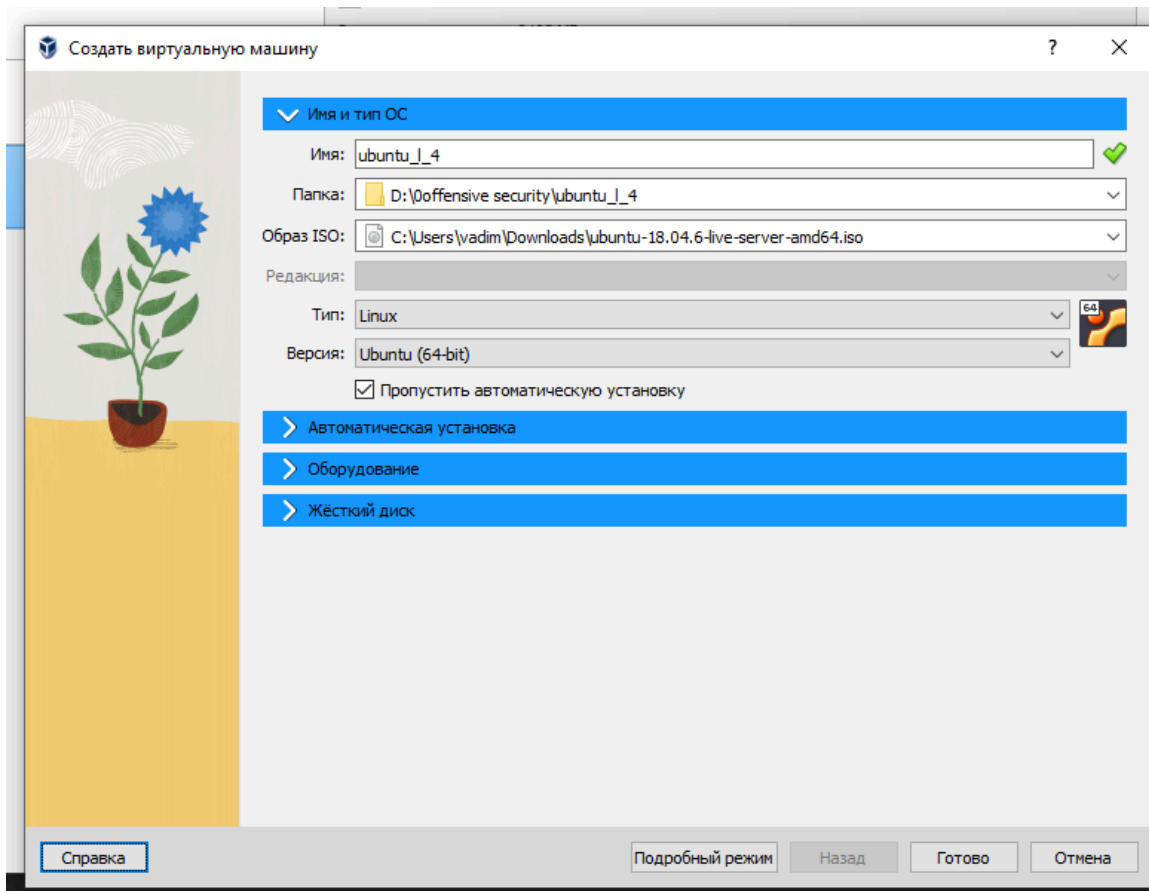
Server install image

The server install image allows you to install Ubuntu permanently on a computer for use as a server. It will not install a graphical user interface.

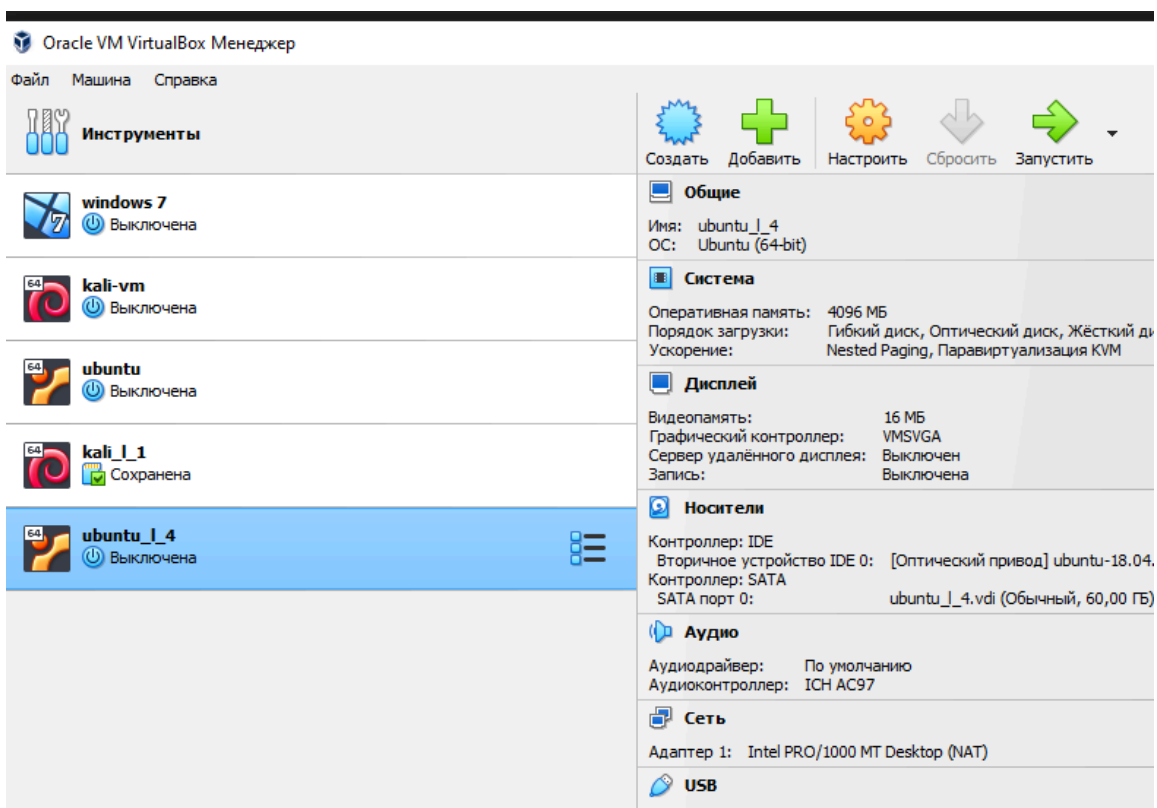
64-bit PC (AMD64) server install image

Choose this if you have a computer based on the AMD64 or EM64T architecture (e.g., Athlon64, Opteron, EM64T Xeon, Core 2). Choose this if you are at all unsure.

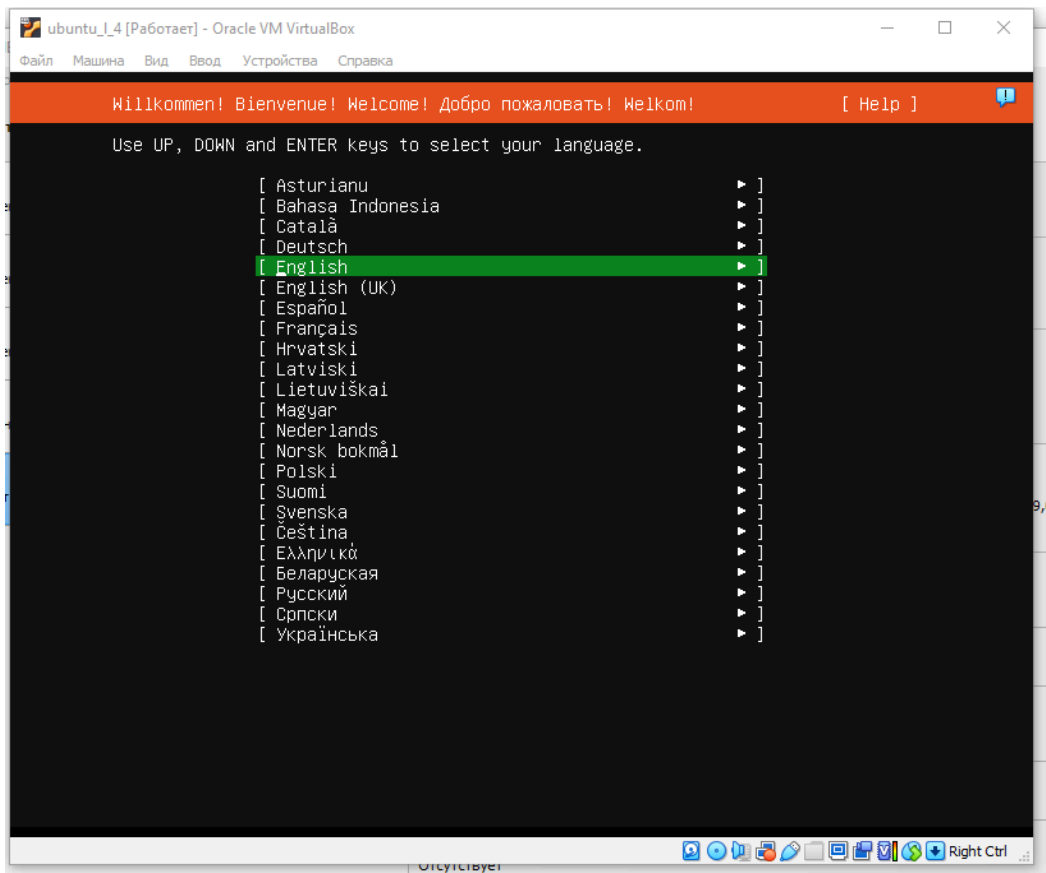
Наступним кроком відкриваю VirtualBox та створюю нову віртуальну машину, й образ встановлюю той, який щойно завантажив



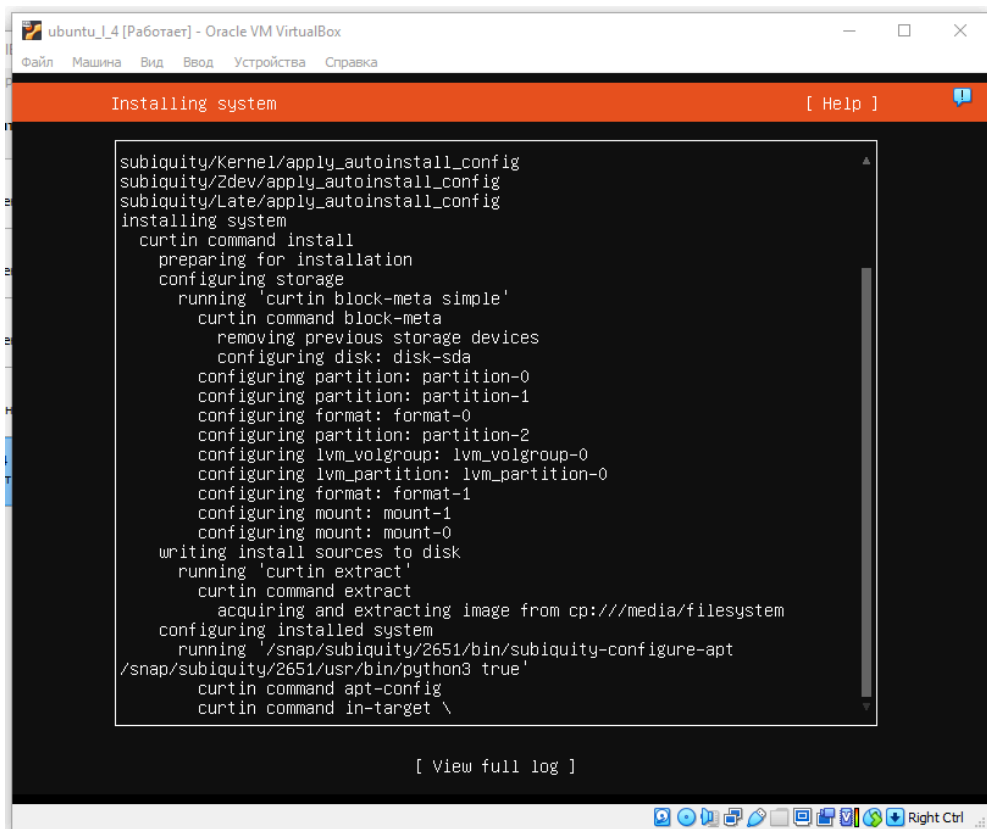
Й запуску нову віртуальну машину для встановлення ОС



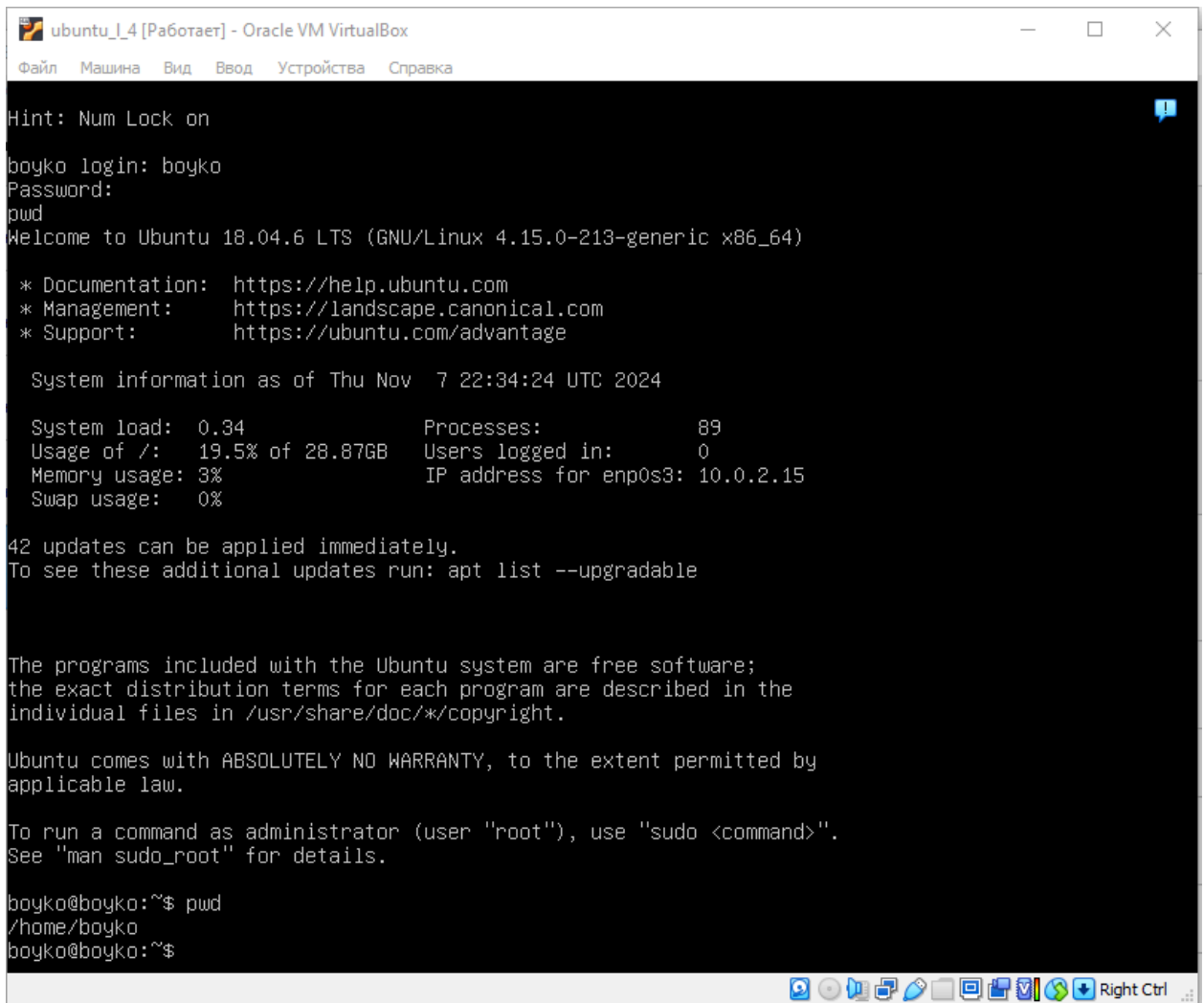
Наступним кроком проходжу через процес встановлення ОС та майже все залишу стандартне



Й почекаю, доки ОС буде встановлена



Після встановлення ОС входжу до системи



```
ubuntu_1_4 [Работаer] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Hint: Num Lock on

boyko login: boyko
Password:
pwd
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-213-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Thu Nov  7 22:34:24 UTC 2024

System load:  0.34               Processes:            89
Usage of /:   19.5% of 28.87GB   Users logged in:     0
Memory usage: 3%                IP address for enp0s3: 10.0.2.15
Swap usage:  0%

42 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

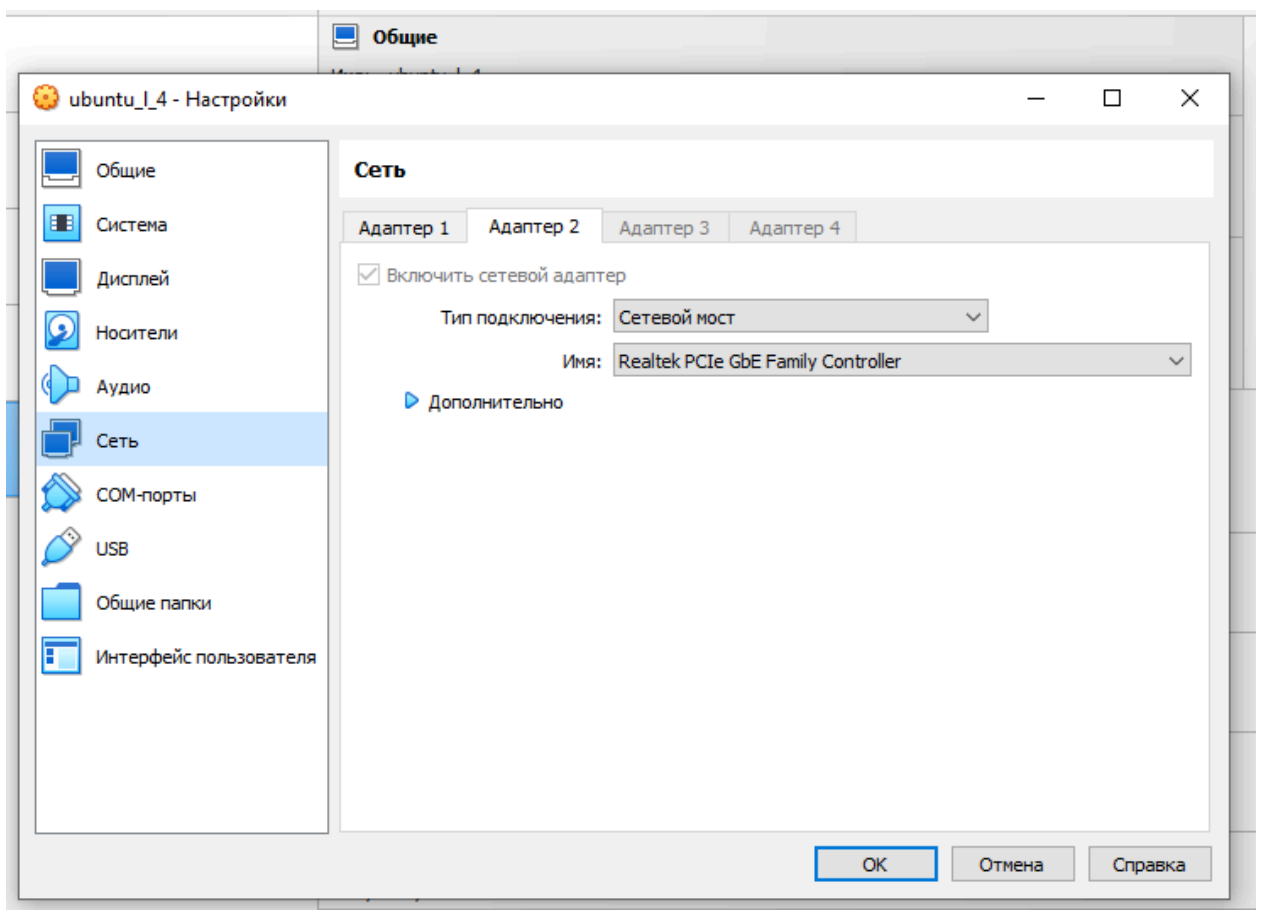
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

boyko@boyko:~$ pwd
/home/boyko
boyko@boyko:~$
```

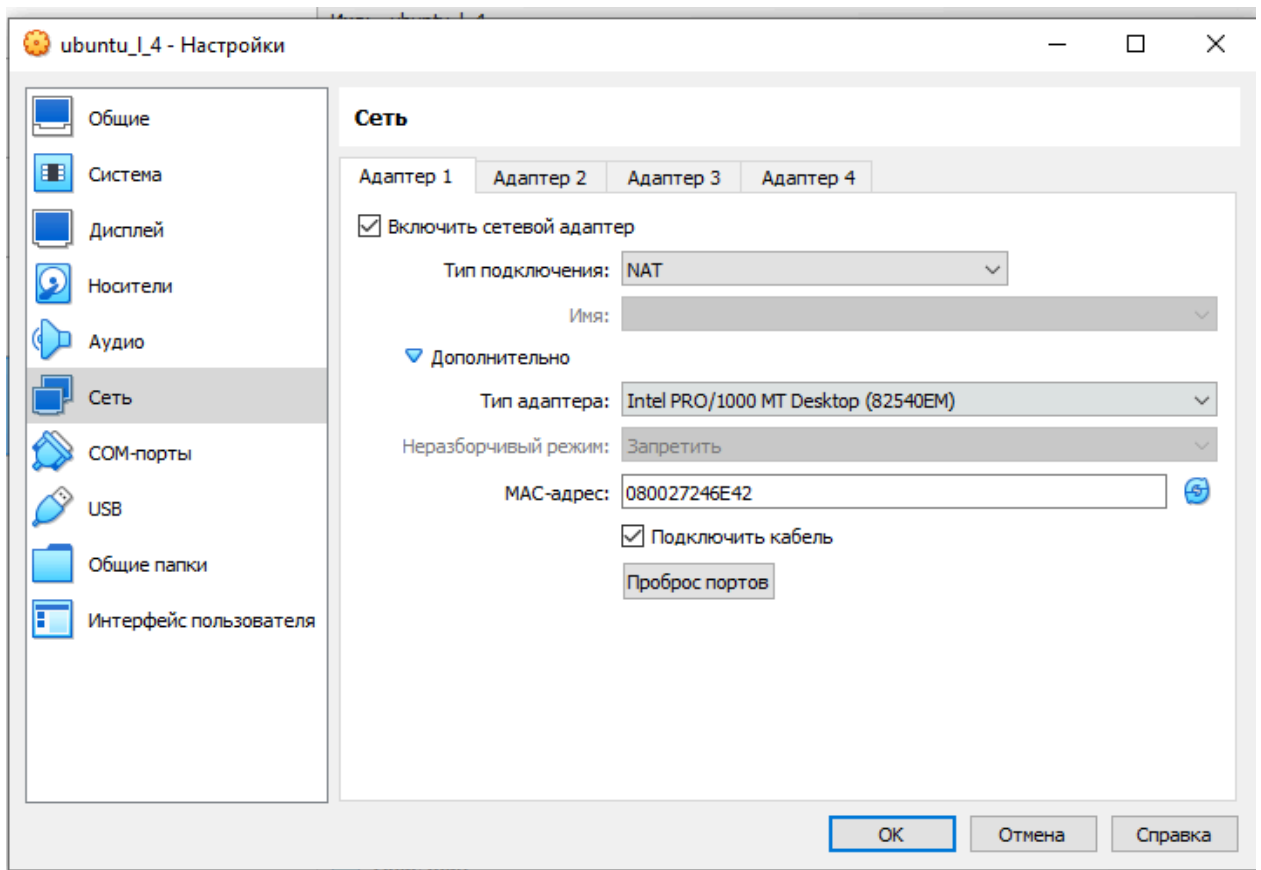
Та бачу, що система працює

Наступним кроком прокину порти на основну машину

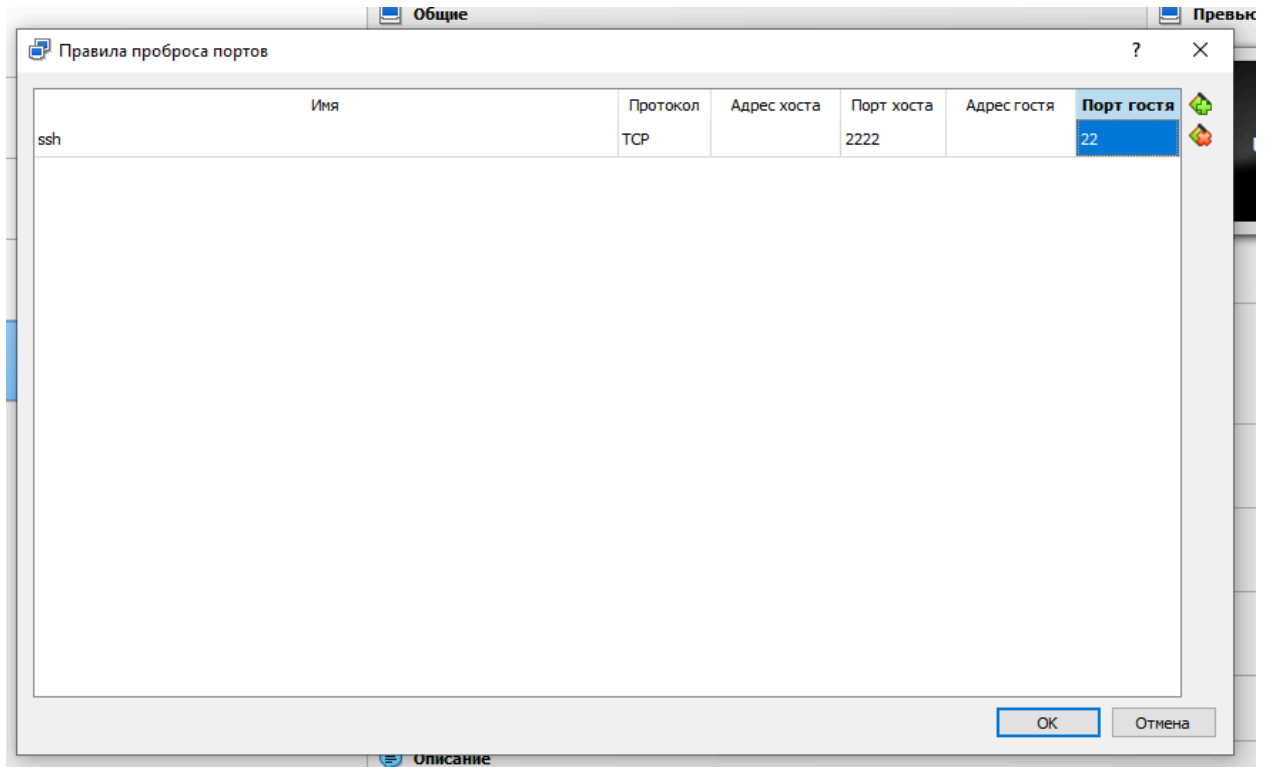
Для цього відкрию налаштування мережі та як другий адаптер оберу
“Сетевой мост”



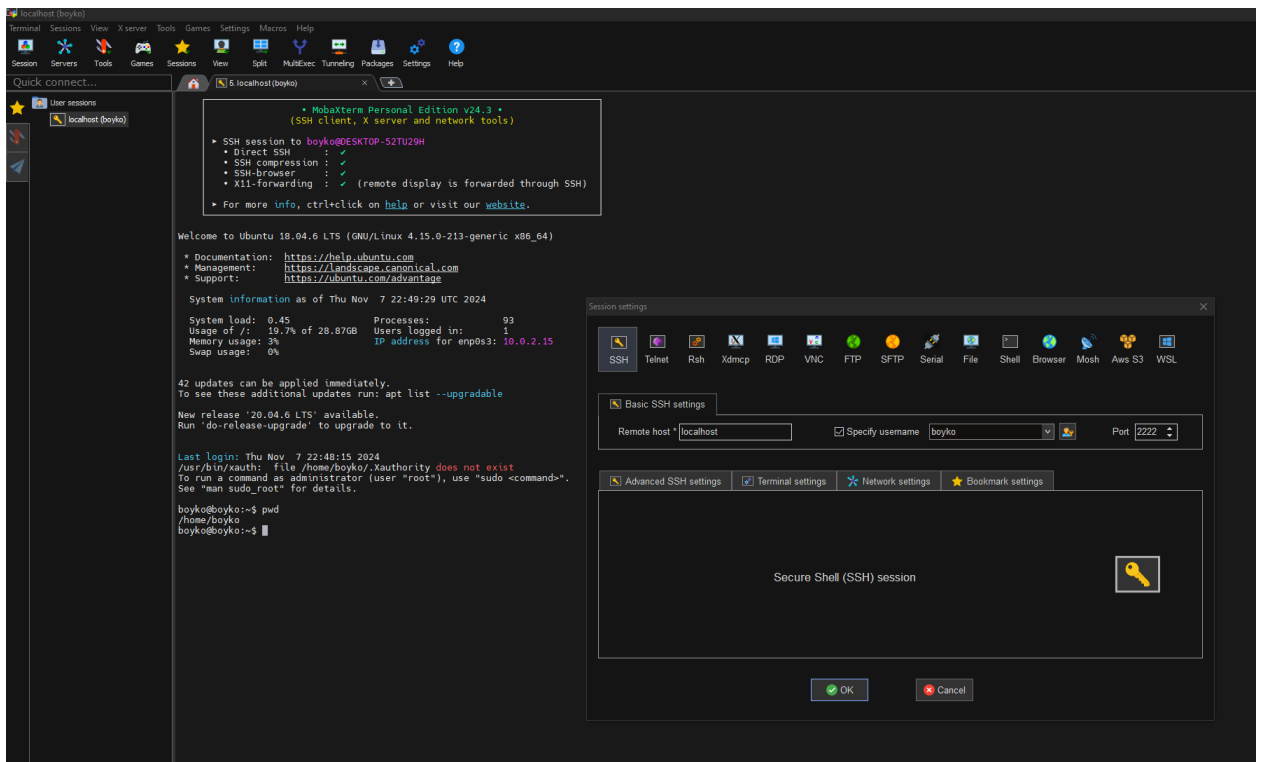
Та перейду до NAT адаптеру та натисну на “Проброс портов”



У відкритшомуся вікні додаю порти, спочатку для SSH



Оскільки при встановленні я додав SSH сервер, та порти прокинуті, то ж під'єднуюсь через застосунок MobaXTerm



Наступним кроком перейду до сайту VestaCP та оберу налаштування для завантаження

Advanced install settings

IMPORTANT! The current version of Vesta is deprecated! We are working on a full rebuild of Vesta. Learn more →

WEB
nginx + apache

FTP
vsftpd

MAIL
exim + dovecot + spamassassin + clamav

DNS
named

FIREWALL
iptables + fail2ban

SOFTACULOUS
no

ADDITIONAL REPOSITORY
yes

FILE SYSTEM QUOTA
no

DB
☐ MySql
☐ PostgreSQL

HOST NAME
HOST NAME

EMAIL
EMAIL

PORT
PORT

PASSWORD
Password

Generate Install Command

В результаті отримаю команди для встановлення

```
1 # Connect to your server as root via SSH
ssh root@your.server

2 # Download installation script
curl -O https://vestacp.com/pub/vst-install.sh

3 # Run it
bash vst-install.sh --nginx yes --apache yes --phpfpm no --vsftpd yes --proftpd no --exim yes --dovecot yes --spamassassin yes --clamav yes --named yes --iptables yes --fail2ban yes --softaculous no --remi yes --quota no --mysql no --postgresql no
```

Та запуску ці команди у терміналі

```
boyko@boyko:~$ pwd
/home/boyko
boyko@boyko:~$ curl -O https://vestacp.com/pub/vst-install.sh
% Total % Received % Xferd Average Speed Time Time Current
Dload Upload Total Spent Left Speed
100 1714 0 1714 0 0 7324 0 --:--:-- --:--:-- --:--:-- 7324
boyko@boyko:~$ bash vst-install.sh --nginx yes --apache yes --phpfpm no --vsftpd yes --proftpd no --exim yes --dovecot yes --spamassassin yes --clamav yes --named yes --iptables yes --fail2ban yes --softaculous no --remi yes --quota no --mysql no --postgresql no
Error: this script can only be executed by root
boyko@boyko:~$ sudo bash vst-install.sh --nginx yes --apache yes --phpfpm no --vsftpd yes --proftpd no --exim yes --dovecot yes --spamassassin yes --clamav yes --named yes --iptables yes --fail2ban yes --softaculous no --remi yes --quota no --mysql no --postgresql no
[sudo] password for boyko:
--2024-11-07 22:53:34-- https://vestacp.com/pub/vst-install-ubuntu.sh
Resolving vestacp.com (vestacp.com)... 188.114.97.11, 188.114.96.11, 2a06:98c1:3120::b, ...
Connecting to vestacp.com (vestacp.com)|188.114.97.11|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]
Saving to: 'vst-install-ubuntu.sh'

vst-install-ubuntu.sh [ <=> ] 48.87K --.-KB/s in 0.03s

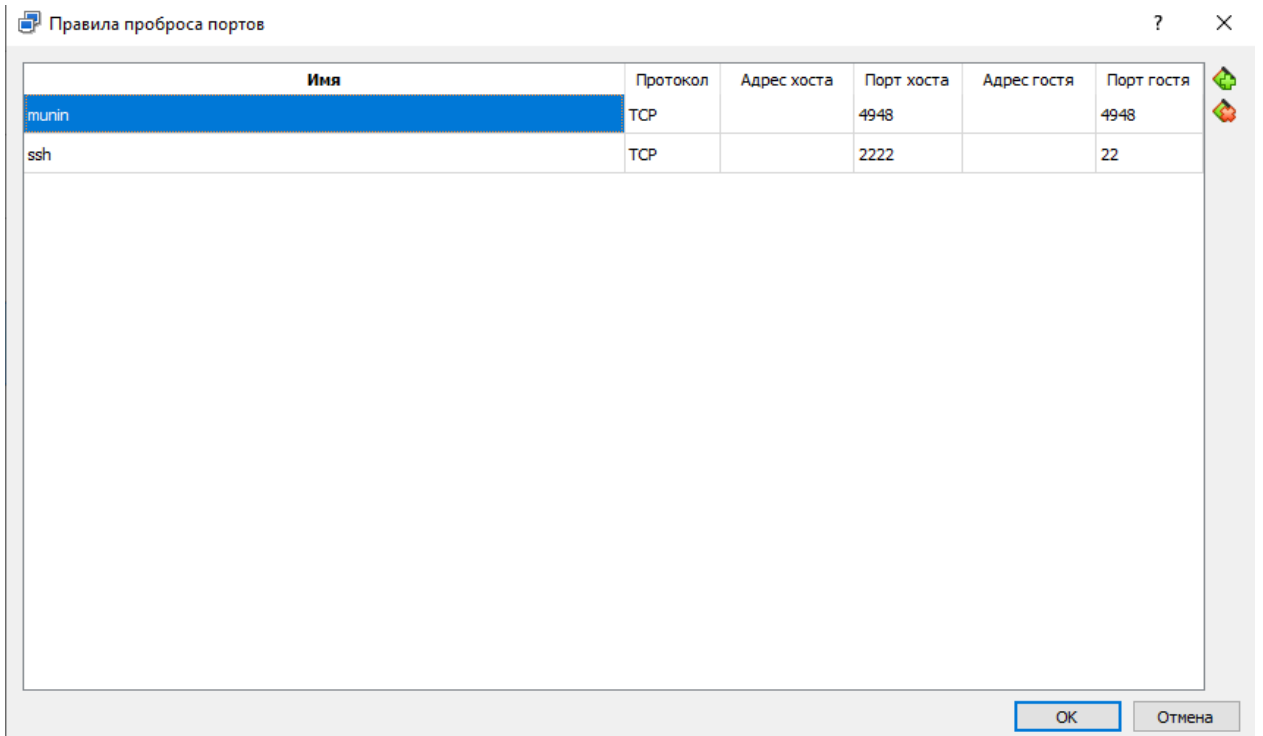
2024-11-07 22:53:35 (1.44 MB/s) - 'vst-install-ubuntu.sh' saved [50046]

Reading package lists... Done
Building dependency tree
Reading state information... Done
gnupg is already the newest version (2.2.4-1ubuntu1.6).
gnupg set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 45 not upgraded.
```

Та одразу встановлю мунін

```
boyko@boyko:~$ pwd
/home/boyko
boyko@boyko:~$ sudo apt-get install munin
[sudo] password for boyko:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
libalgorithm-c3-perl libb-hooks-endofscope-perl libb-hooks-op-check-perl libcgi-fast-perl libcgi-pm-perl libclass-c3-perl
libclass-c3-xs-perl libclass-data-inheritable-perl libclass-method-modifiers-perl libdata-optlist-perl libdate-manip-perl
libdevel-callchecker-perl libdevel-caller-perl libdevel-globaldestruction-perl libdevel-lexalias-perl
```

Також як у попередніх кроках прокину порт, для того, щоб можна було подивитись на панель через основну ОС



Панель була встановлена успішно, та в мене наступні дані для доступу до системи

```
Congratulations, you have just successfully installed Vesta Control Panel
https://109.87.23.215:8083
username: admin
password: RqTKdJs1Er
We hope that you enjoy your installation of Vesta. Please feel free to contact
```

В результаті в мене є доступ до панелі

The screenshot shows the Vesta control panel interface. The top navigation bar includes links for Packages, IP, Graphs, Statistics, Log, Updates, and Firewall. The main content area is divided into four tabs: USER, WEB, DNS, and MAIL. The 'USER' tab is active, displaying a table with user statistics. Below the table, there is a section for the 'admin' user, showing the date '8 Nov 2024', a status icon, and a bandwidth usage of '0 mb'. To the right, there are statistics for 'Web Domains' (1 / 100) and 'DNS Domains' (1 / 100).

USER		WEB		DNS		MAIL	
users:	1	domains:	1	domains:	1	domains:	1
suspended:	0	aliases:	1	records:	14	accounts:	0
		suspended:	0	suspended:	0	suspended:	0

Наступним кроком налаштую конфіг для моніторинг системи, змінені строки підкреслені червоним

The screenshot shows a terminal window with the nano text editor open, editing the file /etc/munin/munin.conf. The editor displays the following content:

```
GNU nano 2.9.3 /etc/munin/munin.conf

# Example configuration file for Munin, generated by 'make build'

# The next three variables specifies where the location of the RRD
# databases, the HTML output, logs and the lock/pid files. They all
```

The screenshot shows the same terminal window with the nano text editor open, editing the file /etc/munin/munin.conf. The editor displays the following content:

```
GNU nano 2.9.3 /etc/munin/munin.conf Modified

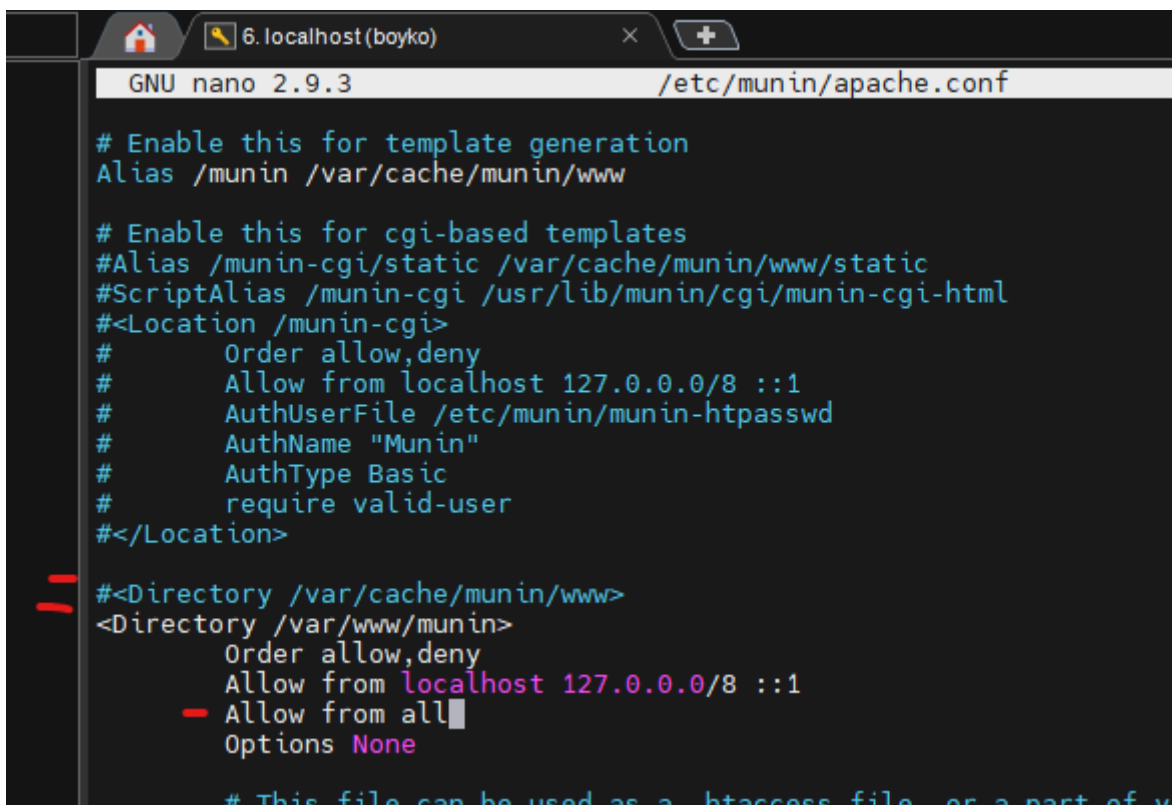
# Example configuration file for Munin, generated by 'make build'

# The next three variables specifies where the location of the RRD
# databases, the HTML output, logs and the lock/pid files. They all
# must be writable by the user running munin-cron. They are all
# defaulted to the values you see here.
#
dbdir /var/lib/munin
htmldir /var/cache/munin/www
logdir /var/log/munin
rundir /var/run/munin

# Where to look for the HTML templates
#
templdir /etc/munin/templates

# Where to look for the static www files
```

The lines for dbdir, htmldir, logdir, and rundir are highlighted with a red circle. The line for templdir is underlined with a red line.



```
GNU nano 2.9.3 /etc/munin/apache.conf

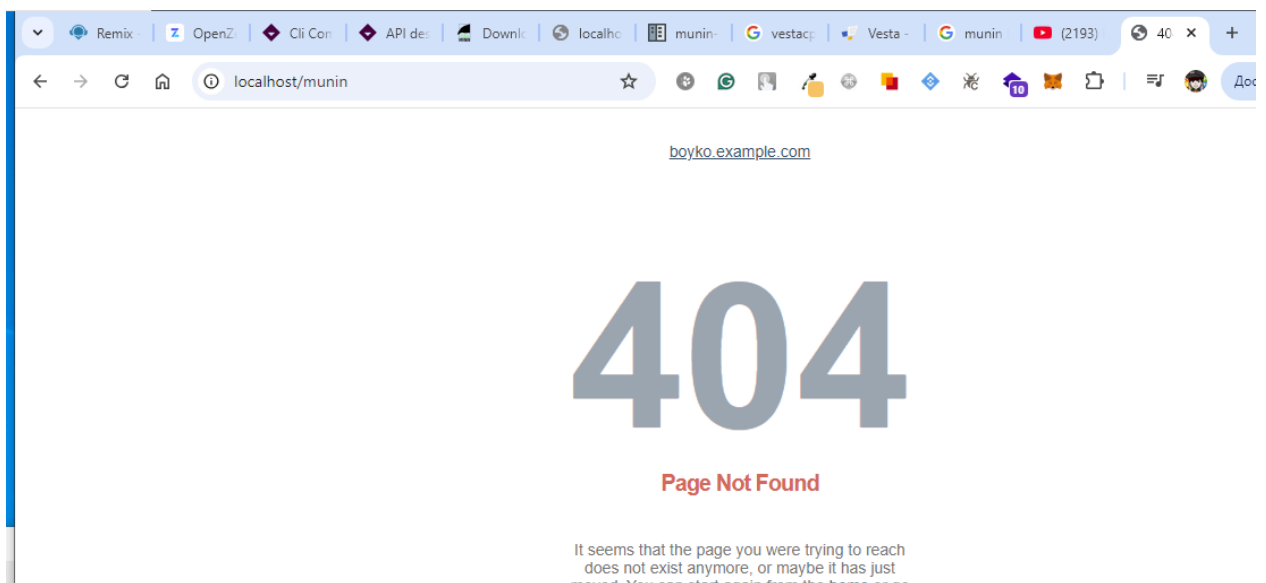
# Enable this for template generation
Alias /munin /var/cache/munin/www

# Enable this for cgi-based templates
#Alias /munin-cgi/static /var/cache/munin/www/static
#ScriptAlias /munin-cgi /usr/lib/munin/cgi/munin-cgi-html
#<Location /munin-cgi>
#     Order allow,deny
#     Allow from localhost 127.0.0.0/8 ::1
#     AuthUserFile /etc/munin/munin-htpasswd
#     AuthName "Munin"
#     AuthType Basic
#     require valid-user
#</Location>

#<Directory /var/cache/munin/www>
<Directory /var/www/munin>
    Order allow,deny
    Allow from localhost 127.0.0.0/8 ::1
    - Allow from all
    Options None

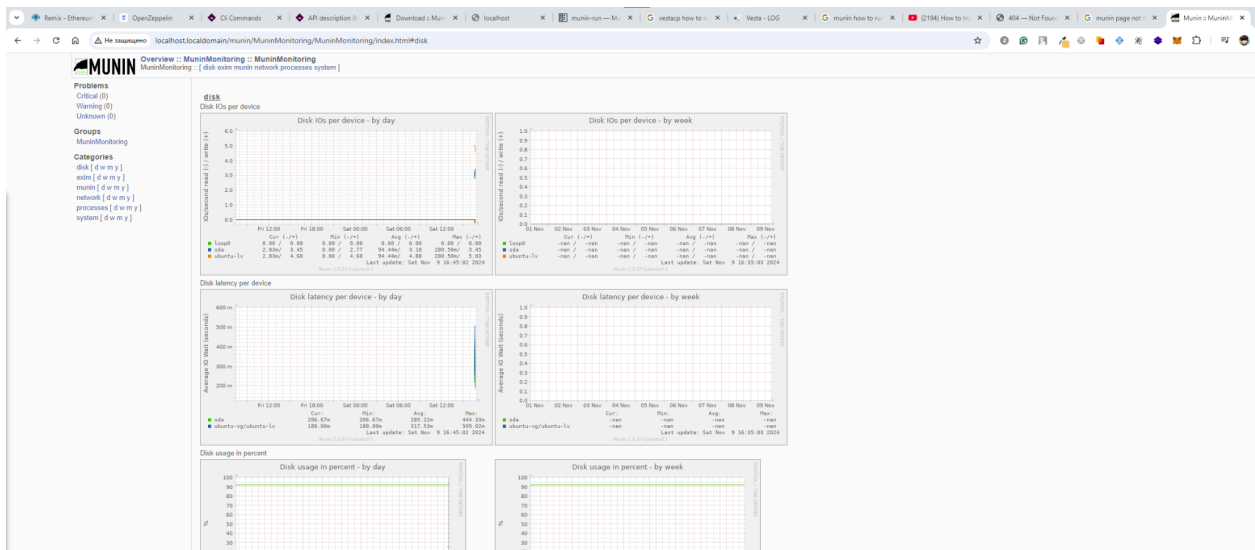
# This file can be used as a .htaccess file or a part of v
```

Якщо відкрити моніторинг систему, то бачу помилку 404



трохи змінив налаштування та тепер маю доступ до моніторингу,

Декілька разів походжу по системі VestaCP, та можна побачити, що вкладка мережі йде вгору, отже моніторинг працює вірно



Й пройду на платформі TryHackMe модуль стосовно логів

The screenshot shows the TryHackMe 'Intro to Log Analysis' room interface. The top navigation bar includes 'Dashboard', 'Learn', 'Compete', and 'Other'. The main header area features the room title 'Intro to Log Analysis' and a description: 'An intro to log analysis, best practices, and essential tools for effective detection and response.' Below the header, there is a 'Room completed (100%)' status bar. The main content area lists 10 tasks: 'Task 1 Introduction', 'Task 2 Log Analysis Basics', 'Task 3 Investigation Theory', 'Task 4 Detection Engineering', 'Task 5 Automated vs. Manual Analysis', 'Task 6 Log Analysis Tools: Command Line', 'Task 7 Log Analysis Tools: Regular Expressions', 'Task 8 Log Analysis Tools: CyberChef', 'Task 9 Log Analysis Tools: Yara and Sigma', and 'Task 10 Conclusion'. A modal window titled 'Logging Legend' is open, displaying a 3D puzzle icon and the text: 'Completed the Log Analysis room. Complete the room to earn this badge!'.

Як висновок - я встановив систему управління доменів, моніторинг та пройшов модуль про аналіз логів