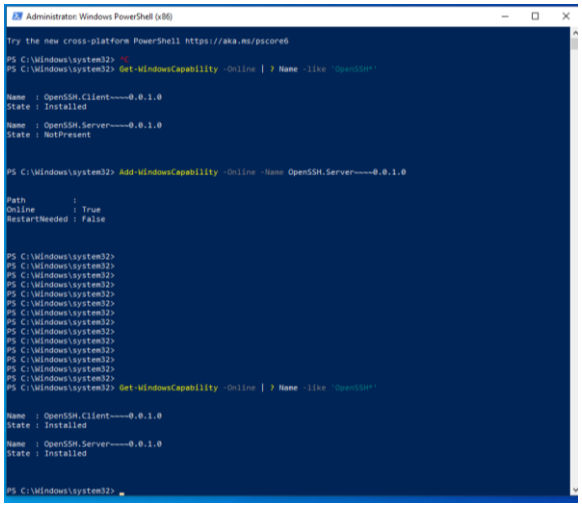
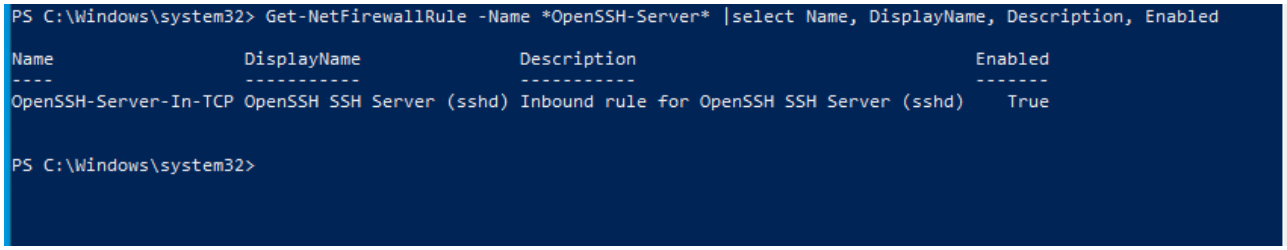
1. Check the implementability of the most frequently used OPENSSH commands in the MS Windows operating system. (Description of the expected result of the commands + screenshots: command – result should be presented)

Settings OPENSSH:





2. Implement basic SSH settings to increase the security of the client-server connection (at least

$ vi /etc/ssh/sshd_config

Ubuntu [Запущено] - Oracle VM VirtualBox

Файл Машина Перегляд Введення Пристрої Довідка

```
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protoc
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin without-password
StrictModes yes
"/etc/ssh/sshd_config" 88 lines, 2541 characters
```

Mouse integration ...

Auto capture keyboard ...

Right Ctrl

```
# What ports, IPs and protocols we listen for
Port 33654
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
```

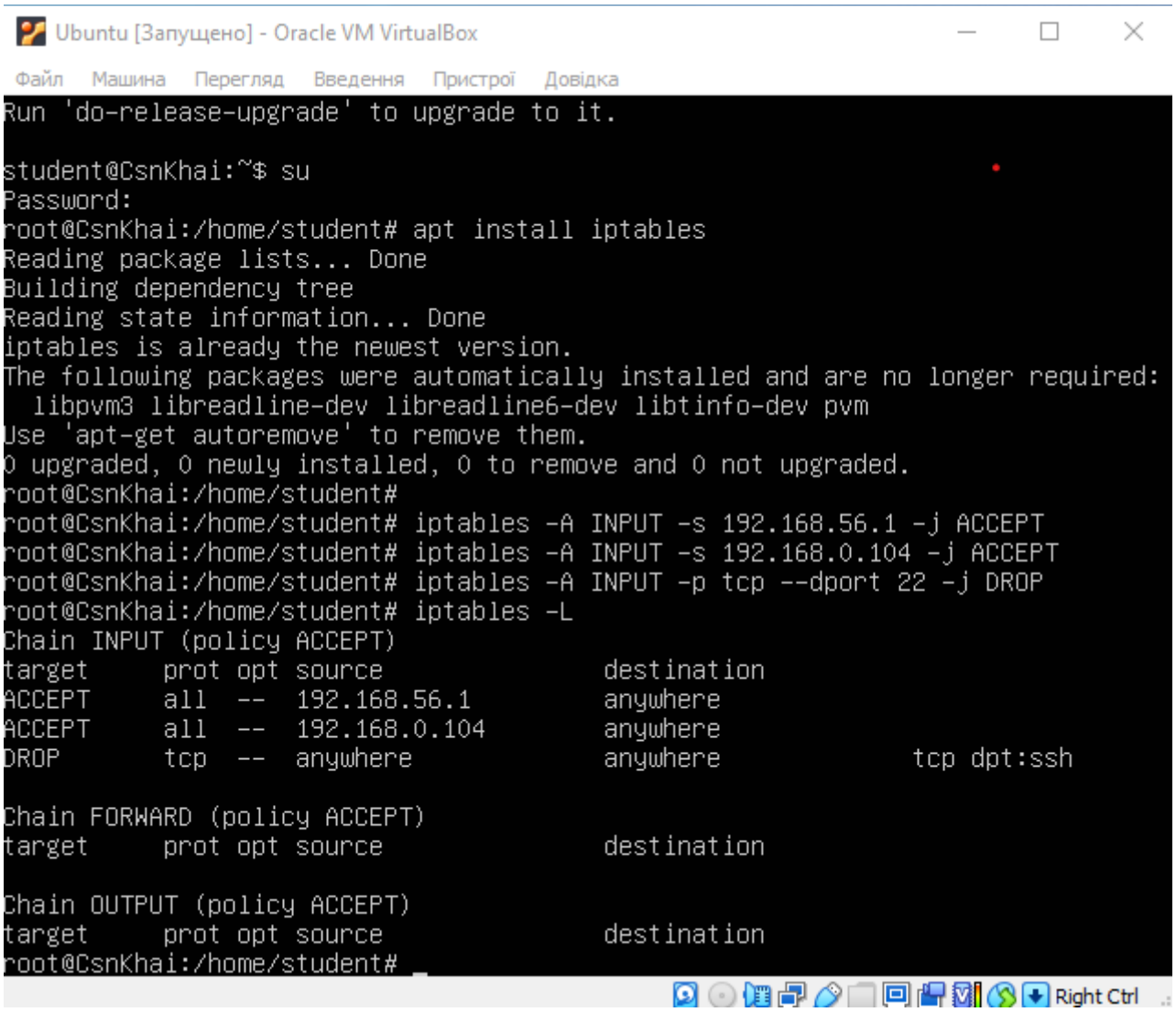
```
# Authentication:
LoginGraceTime 120
PermitRootLogin no
AllowUsers student
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile     %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

```
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
PasswordAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
```

These commands allow access for two IP addresses:

$ iptables -A INPUT -s 192.168.56.1 -j ACCEPT
$ iptables -A INPUT –s 192.168.0.104 -j ACCEPT

This command **will block port** 22**:**
$ iptables -A INPUT -p tcp --dport 22 -j DROP



3. List the options for choosing keys for encryption in SSH. Implement 3 of them.

The ssh-keygen program can generate four types of keys: **dsa, rsa, ecdsa, ed25519**

Implement dsa:

Ubuntu клон2 [Запущено] - Oracle VM VirtualBox

Файл Машина Перегляд Введення Пристрої Довідка

```
Ubuntu 14.04.3 LTS CsnKhai tty1

CsnKhai login: student
Password:
Last login: Tue Aug 15 14:20:31 UTC 2023 from 192.168.0.104 on pts/0
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.13.0-63-generic i686)

 * Documentation:  https://help.ubuntu.com/
student@CsnKhai:~$ ssh student@192.168.0.105
The authenticity of host '192.168.0.105 (192.168.0.105)' can't be established.
ECDSA key fingerprint is d6:eb:2b:a9:bd:63:86:af:31:2f:bb:01:b5:14:63:ab.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.105' (ECDSA) to the list of known hosts.
student@192.168.0.105's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.13.0-63-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Aug 21 01:20:52 2023 from 192.168.0.105
student@CsnKhai:~$ _
```

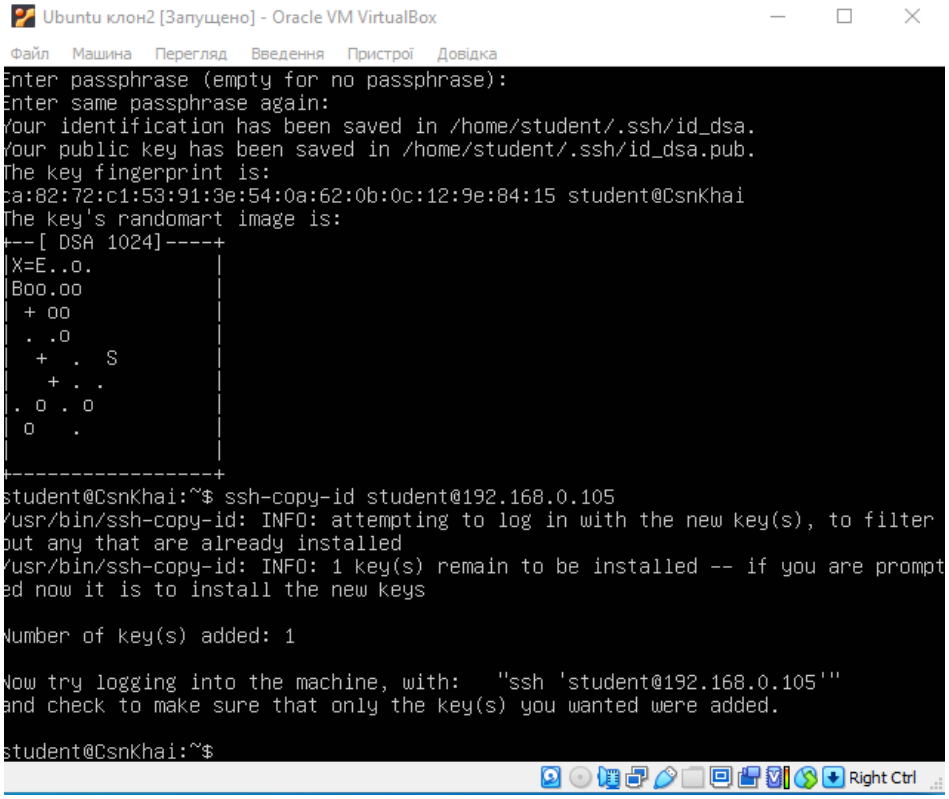
Right Ctrl

Ubuntu клон2 [Запущено] - Oracle VM VirtualBox

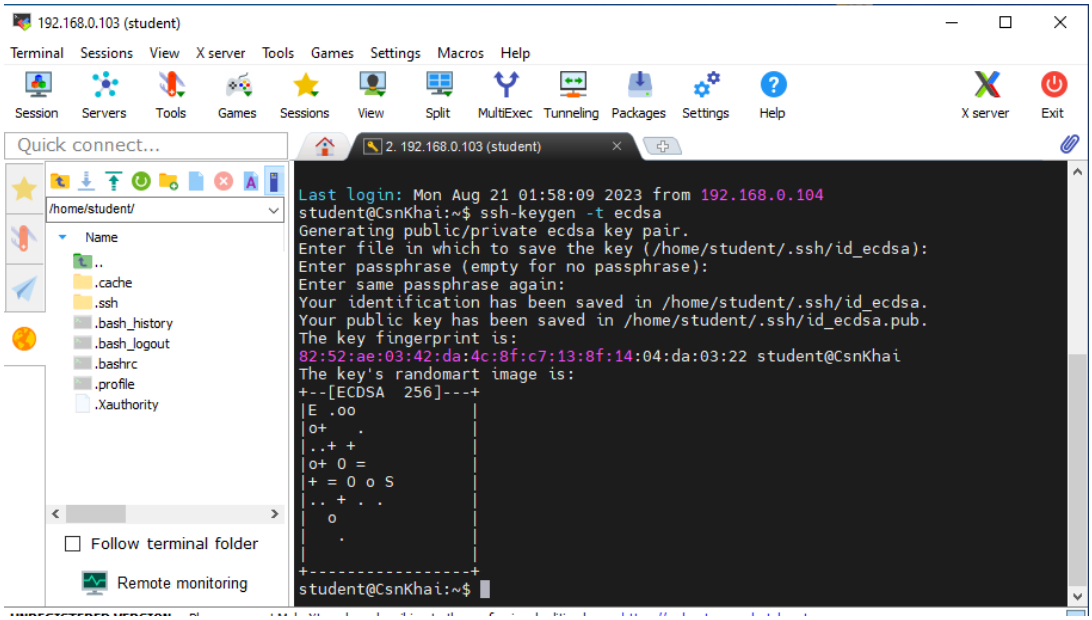
Файл Машина Перегляд Введення Пристрої Довідка

```
student@192.168.0.105's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.13.0-63-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Aug 21 01:20:52 2023 from 192.168.0.105
student@CsnKhai:~$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/student/.ssh/id_dsa.
Your public key has been saved in /home/student/.ssh/id_dsa.pub.
The key fingerprint is:
ca:82:72:c1:53:91:3e:54:0a:62:0b:0c:12:9e:84:15 student@CsnKhai
The key's randomart image is:
+--[ DSA 1024]----+
|X=E..o.          |
|Boo.oo           |
| + oo            |
| . .o            |
|  +  .  S        |
|   + . .         |
|. o . o          |
| o   .           |
|                 |
+-----------------+
student@CsnKhai:~$
```

Right Ctrl



Implement ecdsa:



Implement rsa:

192.168.0.105 (student)

```
Last login: Mon Aug 21 01:01:42 2023
student@CsnKhai:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa):
Created directory '/home/student/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/student/.ssh/id_rsa.
Your public key has been saved in /home/student/.ssh/id_rsa.pub.
The key fingerprint is:
7d:b3:61:73:c7:3e:16:77:59:47:5b:d0:ab:b6:9f:98 student@CsnKhai
The key's randomart image is:
+--[ RSA 2048]----+
|              .oo|
|               .+|
|               .+|
|         .     o+|
|        S . * oo=|
|           o 0 o+|
|            o .o.|
|             .+ o|
|             E.o |
+-----------------+
student@CsnKhai:~$
```

192.168.0.105 (student)

```
|               .+|
|               .+|
|         .     o+|
|        S . * oo=|
|           o 0 o+|
|            o .o.|
|             .+ o|
|             E.o |
+-----------------+
student@CsnKhai:~$ sudo ssh student@192.168.0.105
[sudo] password for student:
The authenticity of host '192.168.0.105 (192.168.0.105)' can't be established.
ECDSA key fingerprint is d6:eb:2b:a9:bd:63:86:af:31:2f:bb:01:b5:14:63:ab.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.105' (ECDSA) to the list of known hosts.
student@192.168.0.105's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.13.0-63-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Aug 21 01:04:02 2023 from 192.168.0.104
student@CsnKhai:~$
```

```
student@CsnKhai:~$ ssh-copy-id student@192.168.0.105
The authenticity of host '192.168.0.105 (192.168.0.105)' can't be established.
ECDSA key fingerprint is d6:eb:2b:a9:bd:63:86:af:31:2f:bb:01:b5:14:63:ab.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
student@192.168.0.105's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'student@192.168.0.105'"
and check to make sure that only the key(s) you wanted were added.

student@CsnKhai:~$
```

4. Implement port forwarding for the SSH client from the host machine to the guest Linux virtual machine behind NAT.