

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:

```
Administrator Windows PowerShell [x64] -
```

```
try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Windows\system32> .\c
PS C:\Windows\system32> Get-WindowCapability -Online | ? Name -like '*OpenSSH*'

Name       : OpenSSH.Client-----0.0.1.0
State      : Installed

Name       : OpenSSH.Server-----0.0.1.0
State      : NotPresent

PS C:\Windows\system32> Add-WindowCapability -Online -Name OpenSSH.Server----0.0.1.0

Path              :
Online             : True
RestartNeeded     : False


PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> Get-WindowCapability -Online | ? Name -like '*OpenSSH*'

Name       : OpenSSH.Client-----0.0.1.0
State      : Installed

Name       : OpenSSH.Server-----0.0.1.0
State      : Installed

PS C:\Windows\system32>
```

```
PS C:\Windows\system32> Get-NetFirewallRule -Name *OpenSSH-Server* |select Name, DisplayName, Description, Enabled
```

Name	DisplayName	Description	Enabled
OpenSSH-Server-In-TCP	OpenSSH SSH Server (sshd)	Inbound rule for OpenSSH SSH Server (sshd)	True

```
PS C:\Windows\system32>
```

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

```
$ vi /etc/ssh/sshd_config
```

```
# 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/protocols
#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
```

```
# 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
```

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

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin_no
StrictModes yes
```

```
# Logging
SyslogFacility AUTH
LogLevel INFO

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

These commands allow access to 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
```

```
Run 'do-release-upgrade' to upgrade to it.

student@CsnKhai:~$ su
Password:
root@CsnKhai:/home/student# apt install iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables is already the newest version.
The following packages were automatically installed and are no longer required:
  libpvm3 libreadline-dev libreadline6-dev libtinfo-dev pvm
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@CsnKhai:/home/student#
root@CsnKhai:/home/student# iptables -A INPUT -s 192.168.56.1 -j ACCEPT
root@CsnKhai:/home/student# iptables -A INPUT -s 192.168.0.104 -j ACCEPT
root@CsnKhai:/home/student# iptables -A INPUT -p tcp --dport 22 -j DROP
root@CsnKhai:/home/student# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    all  --  192.168.56.1           anywhere
ACCEPT    all  --  192.168.0.104         anywhere
DROP      tcp  --  anywhere              anywhere            tcp dpt:ssh

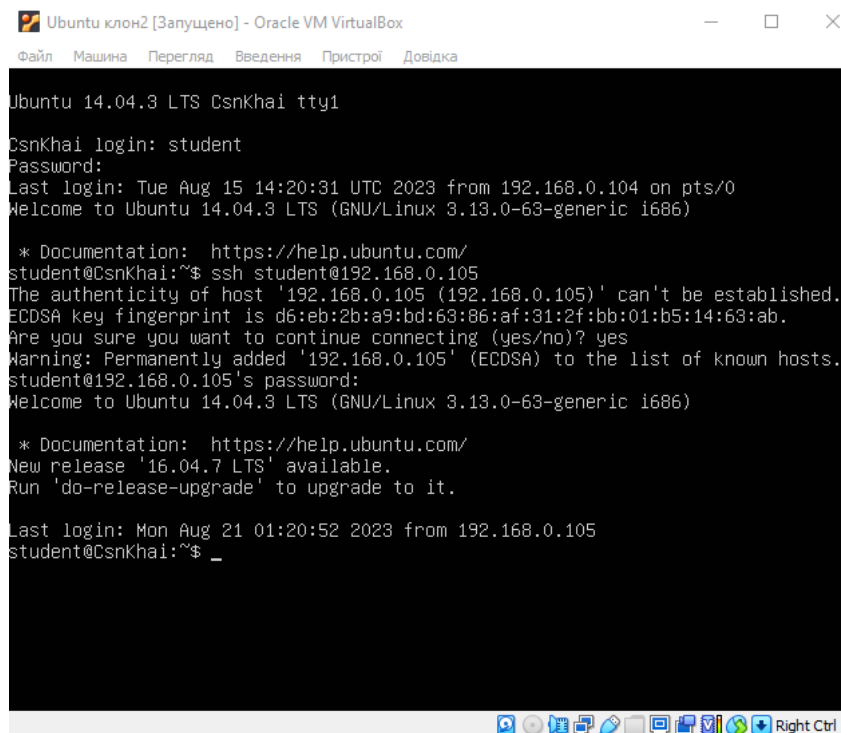
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@CsnKhai:/home/student#
```

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:



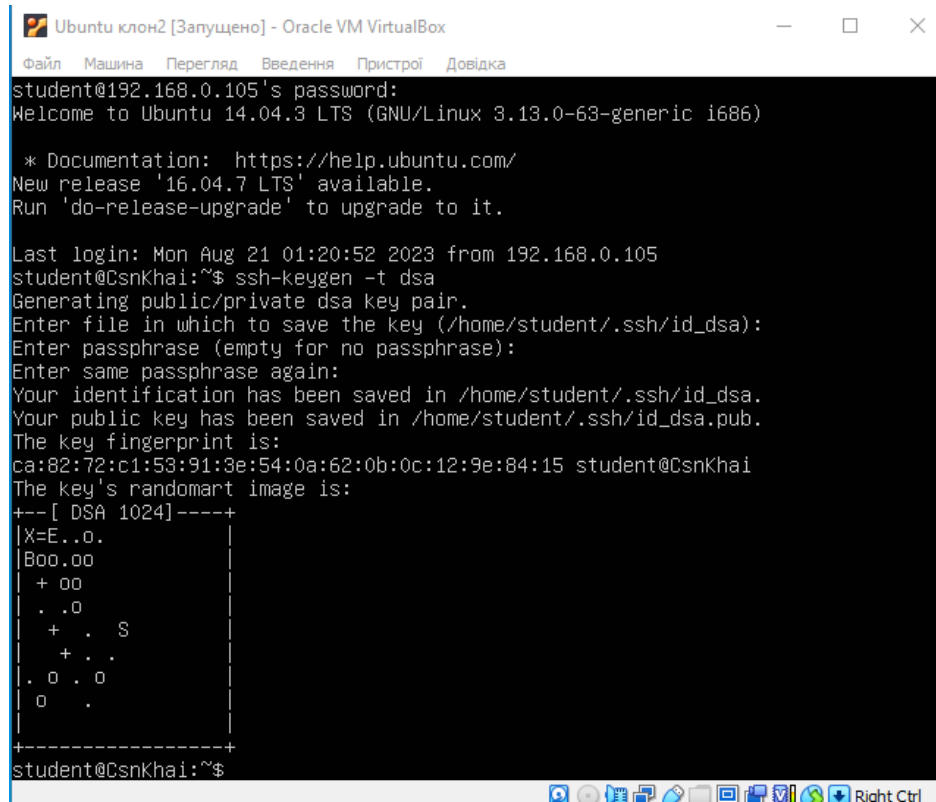
```
Ubuntu клон2 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

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:~$ _
```



```
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.o.               |
| + oo                |
| . .o                |
| + . S               |
| + . .               |
| . o . o             |
| o .                 |
|                      |
+-----+
student@CsnKhai:~$
```

```
Ubuntu клон2 [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

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.o.               |
|+ oo                |
|. .o                 |
|+ . S                |
|+ . .                |
|. o . o              |
|o .                  |
+-----+

student@CsnKhai:~$ ssh-copy-id student@192.168.0.105
/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

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:~$
```

Implement ecdsa:

```
192.168.0.103 (student)
Terminal  Sessions  View  X server  Tools  Games  Settings  Macros  Help

Session  Servers  Tools  Games  Sessions  View  Split  MultiExec  Tunneling  Packages  Settings  Help

Quick connect...
/home/student/
  Name
  .cache
  .ssh
  .bash_history
  .bash_logout
  .bashrc
  .profile
  .Xauthority
  Follow terminal folder
  Remote monitoring

Last login: Mon Aug 21 01:58:09 2023 from 192.168.0.104
student@CsnKhai:~$ ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/student/.ssh/id_ecdsa.
Your public key has been saved in /home/student/.ssh/id_ecdsa.pub.
The key fingerprint is:
82:52:ae:03:42:da:4c:8f:c7:13:8f:14:04:da:03:22 student@CsnKhai
The key's randomart image is:
+--[ECDSA 256]-----+
|E .oo                |
|o+ .                 |
|..+ +                |
|o+ 0 =                |
|+ = 0 o S            |
|..+ . .              |
|o .                  |
|.                    |
+-----+
student@CsnKhai:~$
```

Implement rsa:

```
192.168.0.105 (student)
Terminal Sessions View X server Tools Games Settings Macros Help
Quick connect...
/home/student/
Name
..
.cache
.bash_history
.bash_logout
.bashrc
.profile
.Xauthority
Follow terminal folder
Remote monitoring

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 o o + |
|o .o. |
|. + o |
|E.o |
+-----+
student@CsnKhai:~$
```

```
192.168.0.105 (student)
Terminal Sessions View X server Tools Games Settings Macros Help
Quick connect...
/home/student/
Name
..
.cache
.bash_history
.bash_logout
.bashrc
.profile
.Xauthority
Follow terminal folder
Remote monitoring

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.

