

Table of Contents

Lab 1 2

Part 1 2

 Observations2

 Reflections2

Part 2 2

 Observations2

 Reflections2

Part 3 2

 Observations2

 Screenshots3

 Reflections3

Lab 2 4

Part 1 4

 Observations4

 Screenshots4

 Reflections6

Part 2 6

 Observations6

 Screenshots6

 Reflections7

Part 3 8

 Observations8

 Screenshots8

 Reflections9

Part 4 9

 Observations9

 Screenshots9

 Reflections9

Lab 1

Part 1

Observations

In the VMware Workstation a new VM was created. Virtual hardware configuration is as follows: 2 Gb RAM, 2 processors, 20 Gb hard disk with thin provisioning.

CentOS 7 was chosen as a guest operating system. Installation type is server with GUI without any additional features.

During installation process, password for the root account was specified. Besides, additional admin account was created.

Reflections

Before creating Master VM, operation system should be fully installed and configured. After that, all the security updates and required patches, that add new functionality, must be installed.

In out case, CentOS does not require any actions after installation to run properly and there is no additional software that must be installed on all the VMs.

Part 2

Observations

VMware workstation has an option “Export to OVF”. It creates an OVF image of already existing VM. After that, we can create from that OVF package as much identical VMs as we want omitting long installation process.

Reflections

OVF image consists of disk images, descriptor file and other required files. Descriptor is and XML file that contains all the configurations of the VM, virtual hardware configurations and references to other files.

OVA is a tar archive that contains OVF package.

Part 3

Observations

Two new VMs were deployed using OVF image created in the previous task. Network settings and connectivity check are shown on the screenshots (Figure 1, Figure 2).

Screenshots

```
[admin@vm1 ~]$ ip address show dev ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:3b:e3:e8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.232.128/24 brd 192.168.232.255 scope global noprefixroute dynamic ens33
        valid_lft 1001sec preferred_lft 1001sec
    inet6 fe80::1108:56b4:5da6:e33d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[admin@vm1 ~]$ ping google.com
PING google.com (172.217.0.238) 56(84) bytes of data.
64 bytes from dfw06s38-in-f14.1e100.net (172.217.0.238): icmp_seq=1 ttl=128 time=58.7 ms
64 bytes from dfw06s38-in-f14.1e100.net (172.217.0.238): icmp_seq=2 ttl=128 time=20.4 ms
64 bytes from dfw06s38-in-f14.1e100.net (172.217.0.238): icmp_seq=3 ttl=128 time=58.7 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 20.430/45.981/58.773/18.068 ms
[admin@vm1 ~]$ ping 192.168.232.129
PING 192.168.232.129 (192.168.232.129) 56(84) bytes of data.
64 bytes from 192.168.232.129: icmp_seq=1 ttl=64 time=0.699 ms
64 bytes from 192.168.232.129: icmp_seq=2 ttl=64 time=2.10 ms
64 bytes from 192.168.232.129: icmp_seq=3 ttl=64 time=1.90 ms
```

Figure 1. VM 1 network settings

```
[admin@vm2 ~]$ ip addr show dev ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:3c:e3:db brd ff:ff:ff:ff:ff:ff
    inet 192.168.232.129/24 brd 192.168.232.255 scope global noprefixroute dynamic ens33
        valid_lft 1540sec preferred_lft 1540sec
    inet6 fe80::alb8:2004:54d8:e566/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[admin@vm2 ~]$ ping google.com
PING google.com (172.217.164.238) 56(84) bytes of data.
64 bytes from yyz12s05-in-f14.1e100.net (172.217.164.238): icmp_seq=1 ttl=128 time=42.0 ms
64 bytes from yyz12s05-in-f14.1e100.net (172.217.164.238): icmp_seq=2 ttl=128 time=18.7 ms
64 bytes from yyz12s05-in-f14.1e100.net (172.217.164.238): icmp_seq=3 ttl=128 time=16.4 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 16.470/25.754/42.030/11.547 ms
[admin@vm2 ~]$ ping 192.168.232.128
PING 192.168.232.128 (192.168.232.128) 56(84) bytes of data.
64 bytes from 192.168.232.128: icmp_seq=1 ttl=64 time=0.633 ms
64 bytes from 192.168.232.128: icmp_seq=2 ttl=64 time=1.36 ms
64 bytes from 192.168.232.128: icmp_seq=3 ttl=64 time=2.01 ms
```

Figure 2. VM 2 network settings

Reflections

VMs use DHCP protocol to obtain IP addresses. We can configure DHCP protocol for each adapter in the VMWare Network Editor. This will provide VMs with the unique IP addresses.

Lab 2

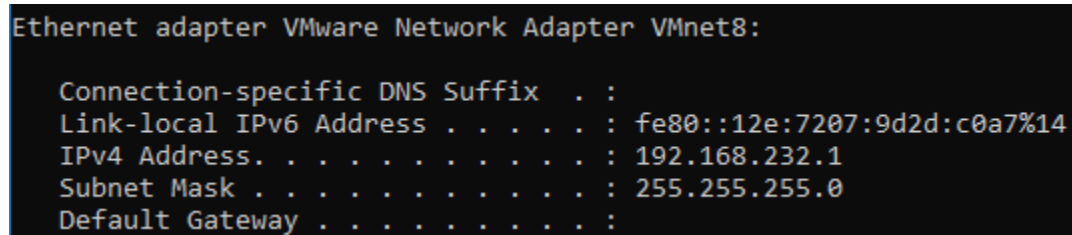
Part 1

Observations

Both VMs were connected to the NAT network. Their IP addresses can be seen on (Figure 1, Figure 2). Host configuration is shown on (Figure 3. Figure 3). Connectivity check is shown on (Figure 4, Figure 5).

Remote into one of the VMs from the host is shown on (Figure 6). Remote from remote host is shown on (Figure 8).

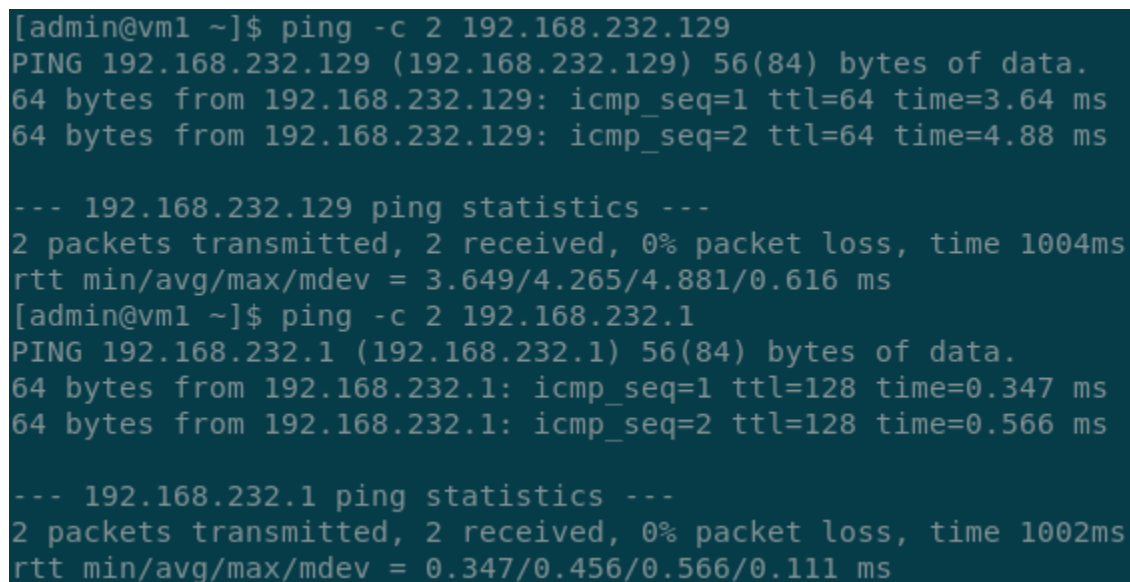
Screenshots



```
Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::12e:7207:9d2d:c0a7%14
IPv4 Address. . . . . : 192.168.232.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Figure 3. Virtual adapter settings



```
[admin@vm1 ~]$ ping -c 2 192.168.232.129
PING 192.168.232.129 (192.168.232.129) 56(84) bytes of data.
64 bytes from 192.168.232.129: icmp_seq=1 ttl=64 time=3.64 ms
64 bytes from 192.168.232.129: icmp_seq=2 ttl=64 time=4.88 ms

--- 192.168.232.129 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 3.649/4.265/4.881/0.616 ms
[admin@vm1 ~]$ ping -c 2 192.168.232.1
PING 192.168.232.1 (192.168.232.1) 56(84) bytes of data.
64 bytes from 192.168.232.1: icmp_seq=1 ttl=128 time=0.347 ms
64 bytes from 192.168.232.1: icmp_seq=2 ttl=128 time=0.566 ms

--- 192.168.232.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.347/0.456/0.566/0.111 ms
```

Figure 4. Ping from VM 1

```
[admin@vm2 ~]$ ping -c 2 192.168.232.128
PING 192.168.232.128 (192.168.232.128) 56(84) bytes of data.
64 bytes from 192.168.232.128: icmp_seq=1 ttl=64 time=0.615 ms
64 bytes from 192.168.232.128: icmp_seq=2 ttl=64 time=2.57 ms

--- 192.168.232.128 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.615/1.593/2.572/0.979 ms
[admin@vm2 ~]$ ping -c 2 192.168.232.1
PING 192.168.232.1 (192.168.232.1) 56(84) bytes of data.
64 bytes from 192.168.232.1: icmp_seq=1 ttl=128 time=0.483 ms
64 bytes from 192.168.232.1: icmp_seq=2 ttl=128 time=0.441 ms

--- 192.168.232.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.441/0.462/0.483/0.021 ms
```

Figure 5. Ping from VM 2

```
C:\Users\seba_>ssh admin@192.168.232.129
admin@192.168.232.129's password:
Last login: Sun May 12 14:14:33 2019 from vm2
[admin@vm2 ~]$
```

Figure 6. SSH from the host to VM 2

| Port Forwarding | | | |
|-----------------|------|----------------------------|-------------|
| Host Port | Type | Virtual Machine IP Address | Description |
| 10022 | TCP | 192.168.232.129:22 | SSH |

Figure 7. Port mapping

```
C:\Users\laksh>ssh -p 10022 admin@10.192.219.51
admin@10.192.219.51's password:
Last login: Tue May 14 08:32:24 2019
[admin@vm2 ~]$
```

Figure 8. SSH from remote host

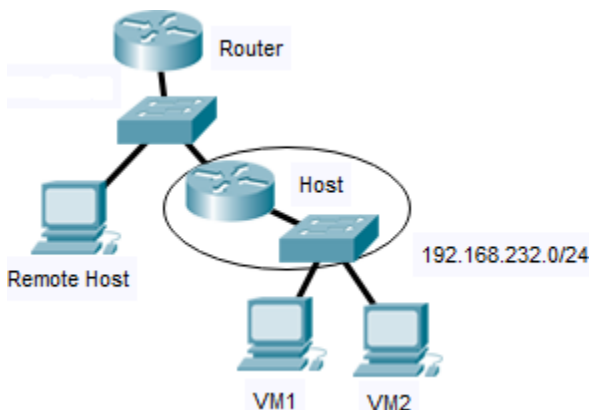


Figure 9. Topology

Reflections

Host acts as a router with “external” interface connected to the real router and “internal” interface connected to the VMs. Logical topology is shown on (Figure 9).

In the case of connection from the host, traffic goes from virtual adapter (Figure 3. Figure 3) directly to the VMs.

In the case, when connection initiates from another host, traffic goes through the router to the host with the VMs and after that, to the particular VM.

In order to have remote access to the VM, it was necessary to map “external” port of the host to a certain “internal” IP address and port (Figure 7). In addition to it, external port must be opened in the firewall configuration. Unfortunately, it opens new surfaces for attacks.

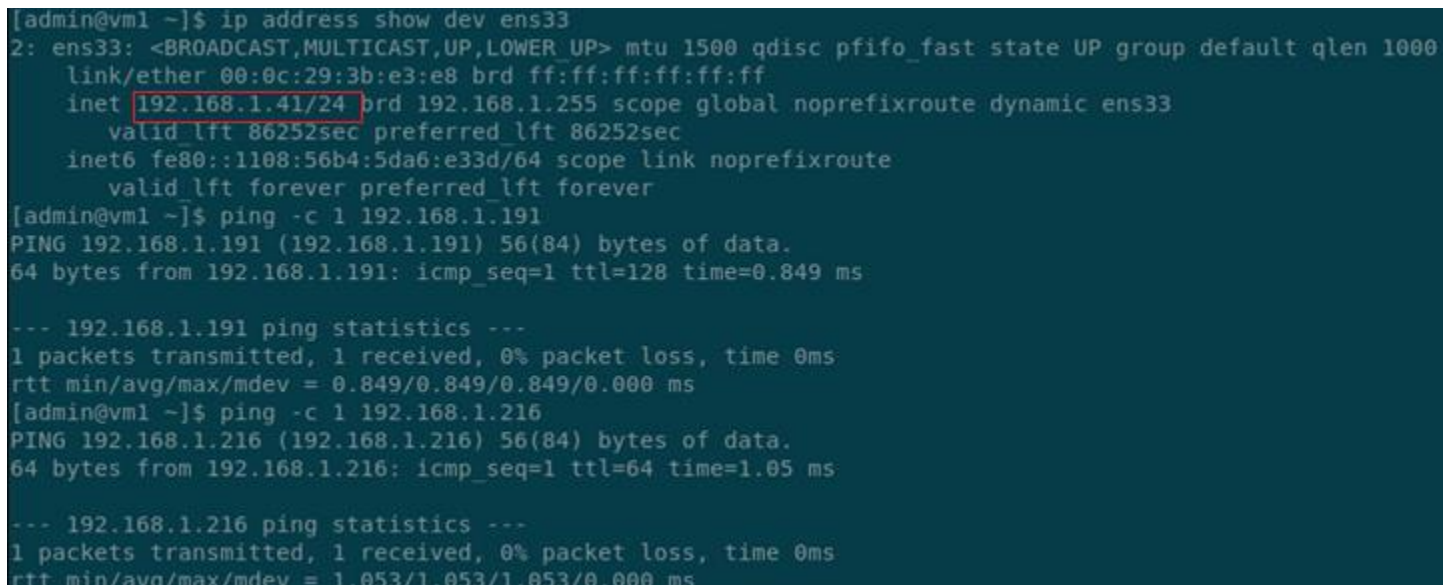
Hiding VMs behind the NAT allows VMs to have access to external networks while no one can access VMs remotely. It is quite a secure configuration, however, it does not always suit the requirements.

Part 2

Observations

Connectivity check is shown on (Figure 10, Figure 11). Remote into the VM from the host is shown on (Figure 12). Screenshot (Figure 13) shows SSH from remote host.

Screenshots



```
[admin@vml ~]$ ip address show dev ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:3b:e3:e8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.41/24 brd 192.168.1.255 scope global noprefixroute dynamic ens33
        valid_lft 86252sec preferred_lft 86252sec
    inet6 fe80::1108:56b4:5da6:e33d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[admin@vml ~]$ ping -c 1 192.168.1.191
PING 192.168.1.191 (192.168.1.191) 56(84) bytes of data.
64 bytes from 192.168.1.191: icmp_seq=1 ttl=128 time=0.849 ms

--- 192.168.1.191 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.849/0.849/0.849/0.000 ms
[admin@vml ~]$ ping -c 1 192.168.1.216
PING 192.168.1.216 (192.168.1.216) 56(84) bytes of data.
64 bytes from 192.168.1.216: icmp_seq=1 ttl=64 time=1.05 ms

--- 192.168.1.216 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.053/1.053/1.053/0.000 ms
```

Figure 10. Network settings and connectivity check, VM 1

```
[admin@vm2 ~]$ ip address show dev ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:3c:e3:db brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.216/24 brd 192.168.1.255 scope global noprefixroute dynamic ens33
        valid_lft 86201sec preferred_lft 86201sec
    inet6 fe80::alb8:2004:54d8:e566/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[admin@vm2 ~]$ ping -c 1 192.168.1.41
PING 192.168.1.41 (192.168.1.41) 56(84) bytes of data.
64 bytes from 192.168.1.41: icmp_seq=1 ttl=64 time=1.94 ms

--- 192.168.1.41 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.940/1.940/1.940/0.000 ms
[admin@vm2 ~]$ ping -c 1 192.168.1.191
PING 192.168.1.191 (192.168.1.191) 56(84) bytes of data.
64 bytes from 192.168.1.191: icmp_seq=1 ttl=128 time=0.968 ms

--- 192.168.1.191 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.968/0.968/0.968/0.000 ms
```

Figure 11. Network settings and connectivity check, VM 2

```
C:\Users\seba>ssh admin@192.168.1.216
admin@192.168.1.216's password:
Last login: Sun May 12 16:15:47 2019 from laptop-h7dhehce
[admin@vm2 ~]$
```

Figure 12. SSH from host to VM 2

```
C:\Users\laksh>ssh admin@10.192.122.83
admin@10.192.219.51's password:
Last login: Tue May 14 08:34:12 2019
[admin@vm2 ~]$
```

Figure 13. SSH from remote host to VM2

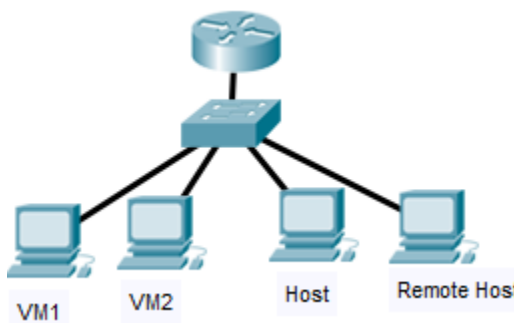


Figure 14. Topology

Reflections

Now, host and VMs act as separate workstations in the external network. Logical topology is shown on (Figure 14).

For both cases of remote access, traffic firstly goes to the router, then to the host and then to the VM.

VMs are completely opened for connections from the outside. Security of the VMs now completely depends on the guest operating systems and their configurations.

Part 3

Observations

Connectivity check is shown on (Figure 15, Figure 16). Remote into the VM from the host is shown on (Figure 17).

Virtual Network Editor has a checkbox “Connect a host virtual adapter to this network”. After unchecking it, VMs cannot communicate with the host and vice versa.

Screenshots

```
[admin@vm1 ~]$ ip address show dev ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:3b:e3:e8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.228.129/24 brd 192.168.228.255 scope global noprefixroute dynamic ens33
        valid_lft 1632sec preferred_lft 1632sec
    inet6 fe80::1108:56b4:5da6:e33d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[admin@vm1 ~]$ ping -c 1 192.168.228.128
PING 192.168.228.128 (192.168.228.128) 56(84) bytes of data:
64 bytes from 192.168.228.128: icmp_seq=1 ttl=64 time=0.809 ms

--- 192.168.228.128 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.809/0.809/0.809/0.000 ms
```

Figure 15. Network settings and connectivity check, VM 1

```
[admin@vm2 ~]$ ip address show dev ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:3c:e3:db brd ff:ff:ff:ff:ff:ff
    inet 192.168.228.128/24 brd 192.168.228.255 scope global noprefixroute dynamic ens33
        valid_lft 1634sec preferred_lft 1634sec
    inet6 fe80::a1b8:2004:54d8:e566/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[admin@vm2 ~]$ ping -c 1 192.168.228.129
PING 192.168.228.129 (192.168.228.129) 56(84) bytes of data:
64 bytes from 192.168.228.129: icmp_seq=1 ttl=64 time=2.19 ms

--- 192.168.228.129 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.194/2.194/2.194/0.000 ms
```

Figure 16. Network settings and connectivity check, VM 2

```
C:\Users\seba_>ssh admin@192.168.228.128
admin@192.168.228.128's password:
Last login: Sun May 12 16:20:01 2019 from 192.168.228.1
[admin@vm2 ~]$
```

Figure 17. SSH from host to VM 2


```
Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::6de1:d0d1:f677:3e91%2
IPv4 Address. . . . . : 192.168.228.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Figure 18. Virtual adapter configuration

Reflections

Traffic goes from virtual adapter (Figure 18) directly to the VMs.

After disconnecting host from the network, corresponding virtual adapter disappeared from the *ipconfig* command output.

Part 4

Observations

In the VM 2 settings, virtual hard disk from the VM 1 was added.

It can be seen on the screenshot (Figure 19) that VM 2 now has two disks: sda – native one, and sdb – disk of the VM 1. Then, one of the partitions on the new disk was mounted to the newly created folder. After that, we have access to the disk content.

Screenshots

```
[admin@vm2 ~]$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda          8:0    0   20G  0 disk
├─sda1       8:1    0    1G  0 part /boot
├─sda2       8:2    0   19G  0 part
│   ├─centos-root 253:0    0   17G  0 lvm  /
│   └─centos-swap 253:1    0    2G  0 lvm  [SWAP]
sdb          8:16   0   20G  0 disk
├─sdb1       8:1    0    1G  0 part
└─sdb2       8:2    0   19G  0 part
sr0         11:0    1 1024M  0 rom
[admin@vm2 ~]$ sudo mount /dev/sdb1 nd
[sudo] password for admin:
[admin@vm2 ~]$ cd nd
[admin@vm2 nd]$ ls
bin  dev  home  lib64  mnt  proc  run  srv  tmp  var
boot  etc  lib  media  opt  root  sbin  sys  usr
```

Figure 19. Mounting new disk

Reflections

As it was shown, files on virtual hard disk can be accessed from another VMs. This can lead to sensitive data leakage. To prevent this, or at least mitigate, files on the virtual disk must be encrypted. Another option is to encrypt entire virtual hard disk file. Even if someone is able to copy virtual disk, he will not be able to get any valuable data.