

Linux lab 245693

Preparation:

```
C:\Users\break\Desktop\routinglab>vboxmanage modifyvm vm2 --nic3 nat
C:\Users\break\Desktop\routinglab>
C:\Users\break\Desktop\routinglab>vboxmanage modifyvm vm2 --nic3 nat
C:\Users\break\Desktop\routinglab>start-vms.cmd
```

```
gdebian GNU/Linux 10 um1 tty1
um1 login: debian
Password:
Last login: Wed Jun 16 19:06:17 CEST 2021 on tty1
Linux um1 4.19.0-16-amd64 #1 SMP Debian 4.19.161-1 (2021-03-19) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
debianum1:~$ ping 0.0.0.0
PING 0.0.0.0 (0.0.0.0) 56(84) bytes of data:
64 bytes from 0.0.0.0: icmp_seq=1 ttl=113 time=26.3 ms
64 bytes from 0.0.0.0: icmp_seq=2 ttl=113 time=26.6 ms
^C
--- 0.0.0.0 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 26.295/26.464/26.634/0.234 ms
debianum1:~$

gdebian GNU/Linux 10 um1 tty1
um1 login: debian
Password:
Last login: Tue Jun 1 13:25:19 CEST 2021 on tty1
Linux um2 4.19.0-16-amd64 #1 SMP Debian 4.19.161-1 (2021-03-19) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
debianum2:~$ sudo -i
rootum2:~# ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
    link/ether 52:54:00:00:00:23 brd ff:ff:ff:ff:ff:ff
    inet 10.2.3.102/24 brd 10.2.3.255 scope global eth1
        valid_lft forever preferred_lft forever
3: emp0:9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
    link/ether 00:00:27:33:79:97 brd ff:ff:ff:ff:ff:ff
    inet 10.0.4.15/24 brd 10.0.4.255 scope global dynamic emp0:9
        valid_lft 86370sec preferred_lft 86370sec
rootum2:~# iptables -t nat -A POSTROUTING -o emp0:9
rootum2:~# iptables -t nat -A POSTROUTING -o emp0:9 -j MASQUERADE
rootum2:~# ping 0.0.0.0
PING 0.0.0.0 (0.0.0.0) 56(84) bytes of data:
64 bytes from 0.0.0.0: icmp_seq=1 ttl=113 time=26.0 ms
64 bytes from 0.0.0.0: icmp_seq=2 ttl=113 time=26.6 ms
^C
--- 0.0.0.0 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1ms
rtt min/avg/max/mdev = 26.597/26.717/26.838/0.203 ms
rootum2:~#

debian@um1:~$ echo "nameserver 8.8.8.8" | sudo tee /etc/resolv.conf
nameserver 8.8.8.8
debian@um1:~$ ping dns.google.com
PING dns.google.com (8.8.4.4) 56(84) bytes of data:
64 bytes from dns.google (8.8.4.4): icmp_seq=1 ttl=113 time=26.5 ms
64 bytes from dns.google (8.8.4.4): icmp_seq=2 ttl=113 time=26.5 ms
^C
--- dns.google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 26.471/26.499/26.528/0.165 ms
debian@um1:~$
```

Task 1

```
root@vm2:~# apt-get update
Hit:1 http://security.debian.org buster/updates InRelease
Hit:2 http://deb.debian.org/debian buster InRelease
Hit:3 http://deb.debian.org/debian buster-updates InRelease
Hit:4 http://deb.debian.org/debian buster-backports InRelease
Reading package lists... Done
root@vm2:~# apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:7.9p1-10+deb10u2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@vm2:~#
```

```
root@vm2:~# sudo systemctl status sshd
■ ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en
   Active: active (running) since Wed 2021-06-16 19:06:25 CEST; 2h 55min left
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 545 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 558 (sshd)
    Tasks: 1 (limit: 393)
   Memory: 2.0M
   CGroup: /system.slice/ssh.service
           └─558 /usr/sbin/sshd -D

Jun 16 19:06:24 vm2 systemd[1]: Starting OpenBSD Secure Shell server...
Jun 16 19:06:25 vm2 sshd[558]: Server listening on 0.0.0.0 port 22.
Jun 16 19:06:25 vm2 systemd[1]: Started OpenBSD Secure Shell server.
Jun 16 19:06:25 vm2 sshd[558]: Server listening on :: port 22.
root@vm2:~#
```

```
root@vm2:~# netstat -tulpn | grep 22
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN     558/sshd
tcp6       0      0 :::22              :::*                  LISTEN     558/sshd
root@vm2:~#
```

```
root@vm2:~# sudo ufw enable
Firewall is active and enabled on system startup
root@vm2:~# sudo ufw allow ssh
Rule added
Rule added (v6)
root@vm2:~#
```

```
root@vm2:~# sudo systemctl list-unit-files | grep enabled | grep ssh
ssh.service                                enabled
sshd.service                              enabled
root@vm2:~# sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
root@vm2:~#
```

Task 2

```
vm2 [Running] - Oracle VM VirtualBox
GNU nano 3.2 /etc/ssh/sshd_config Modified
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
# Ciphers and keying
#RekeyLimit default none
# Logging
#SyslogFacility AUTH
#LogLevel INFO

root@vm2:~# sudo ufw allow from 10.1.2.0/24 to any port 2222
Rule added
root@vm2:~#

vm2 [Running] - Oracle VM VirtualBox
GNU nano 3.2 /etc/ssh/sshd_config Modified

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no_
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

root@vm2:~# systemctl restart sshd
root@vm2:~# systemctl status sshd
■ ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
   Active: active (running) since Wed 2021-06-16 16:17:13 CEST; 4s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 2102 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 2103 (sshd)
      Tasks: 1 (limit: 393)
     Memory: 1.2M
    CGroup: /system.slice/ssh.service
            └─2103 /usr/sbin/sshd -D

Jun 16 16:17:13 vm2 systemd[1]: Starting OpenBSD Secure Shell server...
Jun 16 16:17:13 vm2 sshd[2103]: Server listening on 0.0.0.0 port 2222.
Jun 16 16:17:13 vm2 sshd[2103]: Server listening on :: port 2222.
Jun 16 16:17:13 vm2 systemd[1]: Started OpenBSD Secure Shell server.
root@vm2:~#
```

```
vm2 [Running] - Oracle VM VirtualBox
GNU nano 3.2 /etc/ssh/sshd_config Modified
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    allowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server
ClientAliveInterval 120

X11Forwarding yes
X11DisplayOffset 10
X11UseLocalhost no_
```

Then I got the problem with virtual machine so I couldn't fix it and continue the lab

```
[ Error writing /etc/ssh/sshd_config: No space left on device ]
Write Out  ^M Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
Read File  ^M Replace   ^U Uncut Text ^I To Spell  ^_ Go To Li
```

```
vm2 [Running] - Oracle VM VirtualBox
GNU nano 3.2 New Buffer

[ Error reading lock file /etc/ssh/.sshd_config.swp: Not enough data read ]
^G Get Help  ^O Write Out  ^M Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  ^U Undo
^X Exit      ^R Read File  ^_ Replace   ^U Uncut Text ^I To Spell  ^_ Go To Line ^E Redo
```