

Part2

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)

```
PS C:\Users\sveta> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\sveta/.ssh/id_rsa):
Created directory 'C:\Users\sveta/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\sveta/.ssh/id_rsa.
Your public key has been saved in C:\Users\sveta/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:ds+6RHBTPdiq/tKxtpTCfxODhjcBODfK+u0DSfcatyc sveta@WIN-CGSD9BNQIGK
The key's randomart image is:
+----[RSA 2048]-----+
|
|  . . +
|  o +.. +
| +. +oo . .
| =o .o
| =S.o o
| +. + +oo*.o
| o =+ + =+ o
| E.* =+ o
| + +* +o .
+----[SHA256]-----+
PS C:\Users\sveta> ssh root@192.168.31.211
The authenticity of host '192.168.31.211 (192.168.31.211)' can't be established.
ECDSA key fingerprint is SHA256:2S9FMKCQWMloq/JyiIGdJnAZOSUBzt1DDI/4dzsRpEI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.31.211' (ECDSA) to the list of known hosts.
root@192.168.31.211's password:
Last login: Mon Jul 11 07:47:19 2022
Last login: Mon Jul 11 07:47:19 2022
[root@oracle ~]#
PS C:\Users\sveta> cat ~/.ssh/id_rsa.pub | ssh davig@192.168.31.211 "cat >> ~/.ssh/authorized_keys"
davig@192.168.31.211's password:
PS C:\Users\sveta> ssh davig@192.168.31.211
Last login: Tue Jul 12 14:24:28 2022 from 192.168.31.80
[davig@oracle ~]$
```

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

```
#
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

# This system is following system-wide crypto policy. The changes to
# crypto properties (Ciphers, MACs, ...) will not have any effect here.
# They will be overridden by command-line options passed to the server
# on command line.
# Please, check manual pages for update-crypto-policies(8) and sshd_config(5).

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
```

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

```
[davig@oracle ~]$ ssh-keygen -t dsa -f ./keys/key_dsa
Generating public/private dsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ./keys/key_dsa.
Your public key has been saved in ./keys/key_dsa.pub.
The key fingerprint is:
SHA256:czw1gG32bv7Dn7WdXq10d0LplWH0XyMTsilerwc2Fq0 davig@oracle.vm
The key's randomart image is:
+---[DSA 1024]-----+
|      o.      |
|     . +.     |
|    o o+. .   |
|     . o=oo .  |
|    S.+ =oo.+ =|
|     .ooE+.++0|
|     .oooo+.B  |
|      o+o+B    |
|     ...=Bo    |
+-----[SHA256]-----+
[davig@oracle ~]$ ssh-keygen -t rsa -b 4096 -f ./keys/key_rsa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ./keys/key_rsa.
Your public key has been saved in ./keys/key_rsa.pub.
The key fingerprint is:
SHA256:8LrriynYECT+D9xGb7mt7uiL7FjU9q10fR3R5JnQNSc davig@oracle.vm
The key's randomart image is:
+---[RSA 4096]-----+
|      .Eo+    |
|      =o=     |
|      . =     |
| . . . o      |
| o . + S      |
| + o + o.+    |
| o+ + o.* o . |
| ..*+.o+.+ . |
| .o==*XX..    |
+-----[SHA256]-----+
[davig@oracle ~]$ ssh-keygen -t ed25519 -f ./keys/key_ed25519
Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ./keys/key_ed25519.
Your public key has been saved in ./keys/key_ed25519.pub.
The key fingerprint is:
SHA256:0a6zBfCjMi57ZfkrF1ssewQbPGmY4EtMzexAibmgkB0 davig@oracle.vm
The key's randomart image is:
+--[ED25519 256]--+
| oE=. =       |
| + + = + .    |
| o. = +. +...  |
| . . + +oBo    |
| . . oS*.      |
| + + + +      |
```

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

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2222 -j REDIRECT --to-port 22
Client need connect to port 2222.
```

5*. Intercept (capture) traffic (tcpdump, wireshark) while authorizing the remote client on the server using ssh, telnet, rlogin. Analyze the result.

```
[david@oracle ~]$ sudo tcpdump port 22 -w capture_file
dropped privs to tcpdump
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C172 packets captured
173 packets received by filter
0 packets dropped by kernel
[david@oracle ~]$ sudo tcpdump -r capture_file
reading from file capture_file, link-type EN10MB (Ethernet)
dropped privs to tcpdump
12:48:01.589186 IP oracle.vm.ssh > _gateway.60364: Flags [P.], seq 1810419161:1810419209, ack 1070989614, win 64056, length 48
12:48:01.589632 IP _gateway.60364 > oracle.vm.ssh: Flags [.], ack 48, win 65535, length 0
12:48:06.927127 IP _gateway.60387 > oracle.vm.ssh: Flags [S], seq 1095432705, win 65535, options [mss 1460], length 0
12:48:06.927293 IP oracle.vm.ssh > _gateway.60387: Flags [S.], seq 2852923409, ack 1095432706, win 64240, options [mss 1460], length 0
12:48:06.927597 IP _gateway.60387 > oracle.vm.ssh: Flags [.], ack 1, win 65535, length 0
12:48:06.981708 IP oracle.vm.ssh > _gateway.60387: Flags [P.], seq 1:22, ack 1, win 64240, length 21
12:48:06.982775 IP _gateway.60387 > oracle.vm.ssh: Flags [.], ack 22, win 65535, length 0
12:48:06.988602 IP _gateway.60387 > oracle.vm.ssh: Flags [P.], seq 1:29, ack 22, win 65535, length 28
12:48:06.988671 IP oracle.vm.ssh > _gateway.60387: Flags [.], ack 29, win 64212, length 0
12:48:06.988955 IP _gateway.60387 > oracle.vm.ssh: Flags [P.], seq 29:1285, ack 22, win 65535, length 1256
12:48:06.989001 IP oracle.vm.ssh > _gateway.60387: Flags [.], ack 1285, win 64056, length 0
12:48:06.992445 IP oracle.vm.ssh > _gateway.60387: Flags [P.], seq 22:1070, ack 1285, win 64056, length 1048
12:48:06.993003 IP _gateway.60387 > oracle.vm.ssh: Flags [.], ack 1070, win 65535, length 0
12:48:06.993929 IP _gateway.60387 > oracle.vm.ssh: Flags [P.], seq 1285:1309, ack 1070, win 65535, length 24
12:48:06.993964 IP oracle.vm.ssh > _gateway.60387: Flags [.], ack 1309, win 64056, length 0
12:48:07.011603 IP oracle.vm.ssh > _gateway.60387: Flags [P.], seq 1070:1606, ack 1309, win 64056, length 536
12:48:07.012058 IP _gateway.60387 > oracle.vm.ssh: Flags [.], ack 1606, win 65535, length 0
12:48:07.347354 IP _gateway.60387 > oracle.vm.ssh: Flags [P.], seq 1309:1837, ack 1606, win 65535, length 528
12:48:07.347402 IP oracle.vm.ssh > _gateway.60387: Flags [.], ack 1837, win 64056, length 0
12:48:07.357868 IP oracle.vm.ssh > _gateway.60387: Flags [P.], seq 1606:2486, ack 1837, win 64056, length 880
12:48:07.358406 IP _gateway.60387 > oracle.vm.ssh: Flags [.], ack 2486, win 65535, length 0
12:48:07.765563 IP _gateway.60387 > oracle.vm.ssh: Flags [P.], seq 1837:1917, ack 2486, win 65535, length 80
12:48:07.765761 IP oracle.vm.ssh > _gateway.60387: Flags [P.], seq 2486:2550, ack 1917, win 64056, length 64
12:48:07.766241 IP _gateway.60387 > oracle.vm.ssh: Flags [.], ack 2550, win 65535, length 0
12:48:07.766999 IP _gateway.60387 > oracle.vm.ssh: Flags [P.], seq 1917:1997, ack 2550, win 65535, length 80
12:48:07.776467 IP oracle.vm.ssh > _gateway.60387: Flags [P.], seq 2550:2646, ack 1997, win 64056, length 96
12:48:07.776895 IP _gateway.60387 > oracle.vm.ssh: Flags [.], ack 2646, win 65535, length 0
12:48:07.777275 IP _gateway.60387 > oracle.vm.ssh: Flags [P.], seq 1997:2109, ack 2646, win 65535, length 112
12:48:07.818354 IP oracle.vm.ssh > _gateway.60387: Flags [.], ack 2109, win 64056, length 0
12:48:07.847626 IP oracle.vm.ssh > _gateway.60387: Flags [P.], seq 2646:2742, ack 2109, win 64056, length 96
12:48:07.848383 IP _gateway.60387 > oracle.vm.ssh: Flags [.], ack 2742, win 65535, length 0
12:48:07.853283 IP _gateway.60387 > oracle.vm.ssh: Flags [P.], seq 2109:2381, ack 2742, win 65535, length 272
```

capture_file

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
8	5.838558	10.0.2.2	10.0.2.15	SSHv2	82	Client: Protocol (SSH-2.0-MoTTY_Release_0.76)
9	5.838597	10.0.2.15	10.0.2.2	TCP	54	22 → 61145 [ACK] Seq=22 Ack=29 Win=64212 Len=0
10	5.838852	10.0.2.2	10.0.2.15	SSHv2	1310	Client: Key Exchange Init
11	5.838891	10.0.2.15	10.0.2.2	TCP	54	22 → 61145 [ACK] Seq=22 Ack=1285 Win=64056 Len=0
12	5.842510	10.0.2.15	10.0.2.2	SSHv2	1102	Server: Key Exchange Init
13	5.843642	10.0.2.2	10.0.2.15	TCP	60	61145 → 22 [ACK] Seq=1285 Ack=1070 Win=65535 Len=0
14	5.844321	10.0.2.2	10.0.2.15	SSHv2	78	Client: Diffie-Hellman Group Exchange Request
15	5.844359	10.0.2.15	10.0.2.2	TCP	54	22 → 61145 [ACK] Seq=1070 Ack=1309 Win=64056 Len=0
16	5.861188	10.0.2.15	10.0.2.2	SSHv2	590	Server: Diffie-Hellman Group Exchange Group
17	5.861755	10.0.2.2	10.0.2.15	TCP	60	61145 → 22 [ACK] Seq=1309 Ack=1606 Win=65535 Len=0
18	6.200647	10.0.2.2	10.0.2.15	SSHv2	582	Client: Diffie-Hellman Group Exchange Init
19	6.200700	10.0.2.15	10.0.2.2	TCP	54	22 → 61145 [ACK] Seq=1606 Ack=1837 Win=64056 Len=0
20	6.211100	10.0.2.15	10.0.2.2	SSHv2	934	Server: Diffie-Hellman Group Exchange Reply, New Keys,
21	6.211539	10.0.2.2	10.0.2.15	TCP	60	61145 → 22 [ACK] Seq=1837 Ack=2486 Win=65535 Len=0
22	6.616926	10.0.2.2	10.0.2.15	SSHv2	134	Client: New Keys, Encrypted packet (len=64)
23	6.617104	10.0.2.15	10.0.2.2	SSHv2	118	Server: Encrypted packet (len=64)
24	6.617607	10.0.2.2	10.0.2.15	TCP	60	61145 → 22 [ACK] Seq=1917 Ack=2550 Win=65535 Len=0
25	6.618499	10.0.2.2	10.0.2.15	SSHv2	134	Client: Encrypted packet (len=80)
26	6.627572	10.0.2.15	10.0.2.2	SSHv2	150	Server: Encrypted packet (len=96)
27	6.628173	10.0.2.2	10.0.2.15	TCP	60	61145 → 22 [ACK] Seq=1997 Ack=2646 Win=65535 Len=0
28	6.628363	10.0.2.2	10.0.2.15	SSHv2	166	Client: Encrypted packet (len=112)
29	6.669067	10.0.2.15	10.0.2.2	TCP	54	22 → 61145 [ACK] Seq=2646 Ack=2109 Win=64056 Len=0
30	6.698205	10.0.2.15	10.0.2.2	SSHv2	150	Server: Encrypted packet (len=96)
31	6.698685	10.0.2.2	10.0.2.15	TCP	60	61145 → 22 [ACK] Seq=2109 Ack=2742 Win=65535 Len=0
32	6.700547	10.0.2.2	10.0.2.15	SSHv2	326	Client: Encrypted packet (len=272)
33	6.700587	10.0.2.15	10.0.2.2	TCP	54	22 → 61145 [ACK] Seq=2742 Ack=2381 Win=64056 Len=0
34	6.719735	10.0.2.15	10.0.2.2	SSHv2	102	Server: Encrypted packet (len=48)
35	6.720578	10.0.2.2	10.0.2.15	TCP	60	61145 → 22 [ACK] Seq=2381 Ack=2790 Win=65535 Len=0

Frame 20: 934 bytes on wire (7472 bits), 934 bytes captured (7472 bits)

Ethernet II, Src: PcsCompu_65:0d:9a (08:00:27:65:0d:9a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.2

Transmission Control Protocol, Src Port: 22, Dst Port: 61145, Seq: 1606, Ack: 1837, Len: 880

SSH Protocol

- SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:zlib@openssh.com)
- SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:zlib@openssh.com)
- SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:zlib@openssh.com)

[Direction: server-to-client]

0000 52 54 00 12 35 02 08 00 27 65 0d 9a 08 00 45 00 RT.5... 'e---E-

0010 03 98 0a cd 40 00 04 06 14 83 0a 00 02 0f 0a 00@.@

0020 02 02 00 16 ee d9 5e 77 2a c5 58 bd ef 2e 50 18^w *.X...P-