Lab04 Packet Sniffing and Analysis

Prepared By Professor Sean He

1. Clone a new Client Machine (we named it as Sean-Client) follow this video
https://video.nottingham.edu.cn/Panopto/Pages/Viewer.aspx?id=84d40490-bbf2-4c1d-a100-afc2007c7ef7&start=0

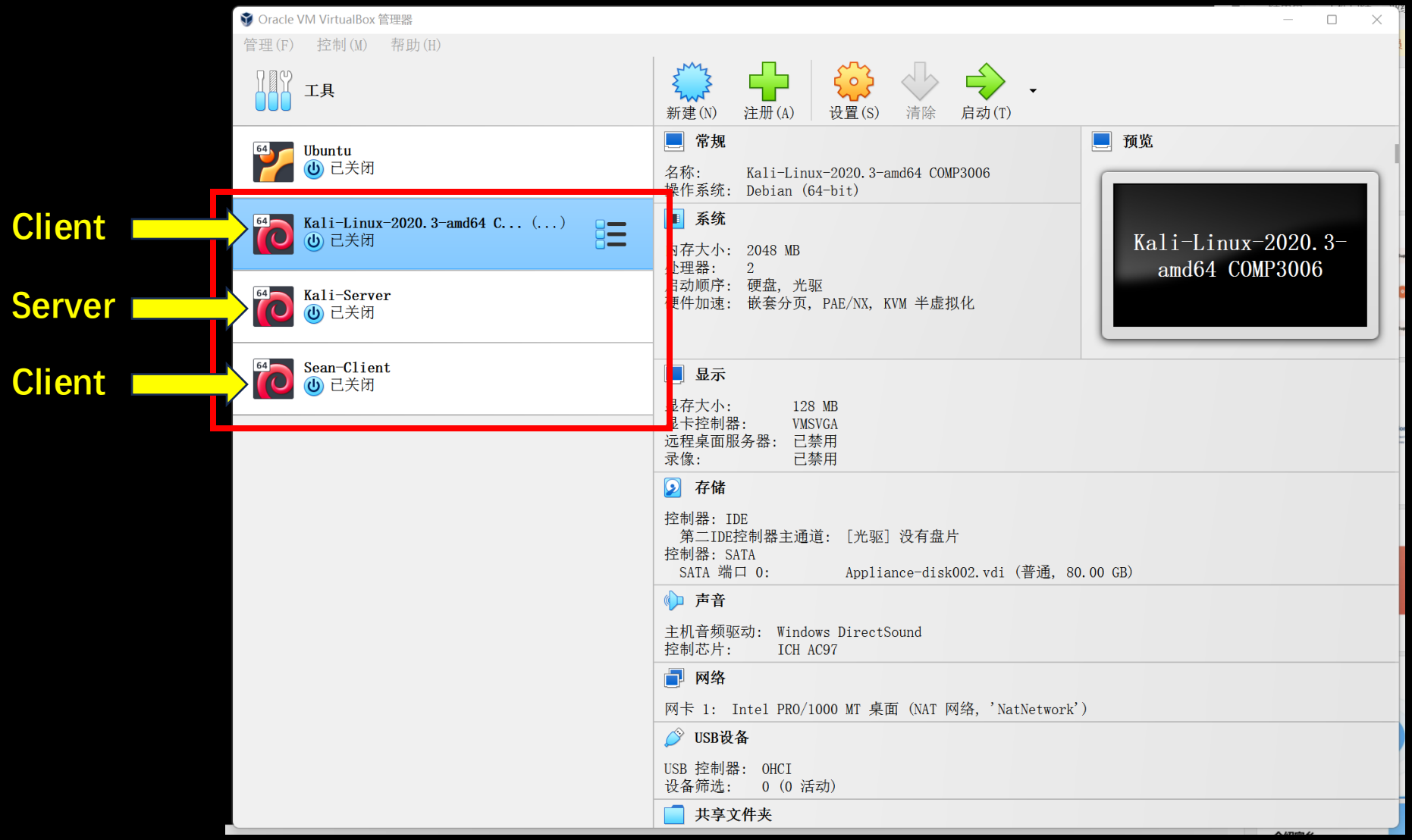
2. Next, you need to configure the virtual machines by following the steps described in one the following videoclips, depending on whether you are using Oracle VM VirtualBox V6 or V7:

V6 - https://video.nottingham.edu.cn/Panopto/Pages/Viewer.aspx?id=19d691b1-c30f-4d7c-8993-afc2007de859&start=0

V7 - https://video.nottingham.edu.cn/Panopto/Pages/Viewer.aspx?id=2b83a6a0-e8d8-45d5-b06f-afc2007f3344&start=0

3. ***Refresh the MAC address, then use "*sudo ifconfig*" to check the address.
(make sure the address of the server machine and two client machines are different)

Now we have three machines



Kali-Server Machine

Type in *"sudo ifconfig"*

Remember the IP address of your own server.

Then Type in those two commands to set up the server.

Sean_VM [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~

```
sec@kali:~$ sudo ifconfig
[sudo] password for sec:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fee1:bc91  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e1:bc:91  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 2123 (2.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec@kali:~$ sudo service xinetd start
sec@kali:~$ sudo service ssh start
[sudo] password for sec:
sec@kali:~$
```

Sean-Client [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~

sec@kali: ~

File Actions Edit View Help

```
sec@kali:~$ sudo tcpdump
[sudo] password for sec:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
23:21:27.749369 IP 10.0.2.4.bootpc > 10.0.2.3.bootps: BOOTP/DHCP, Request f
rom 08:00:27:e1:bc:91 (oui Unknown), length 282
23:21:27.763441 IP 10.0.2.3.bootps > 10.0.2.4.bootpc: BOOTP/DHCP, Reply, le
ngth 548
23:21:32.777339 ARP, Request who-has 10.0.2.3 tell 10.0.2.4, length 46
23:21:32.777560 ARP, Reply 10.0.2.3 is-at 08:00:27:54:de:c1 (oui Unknown),
length 46
```

First, Open up two terminals on the client machine.
Type in *"sudo tcpdump"* to monitor infos.
Then, in the other window, send a few pings to the server, then cancel both using Ctrl+C.

Client: Kali-Linux-2020.3
Ping the server

Kali-Linux-2020.3-amd64 COMP3006 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~

sec@kali: ~

File Actions Edit View Help

```
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec@kali:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.837 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.671 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.851 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.956 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.667 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=64 time=1.19 ms
64 bytes from 10.0.2.4: icmp_seq=7 ttl=64 time=1.25 ms
64 bytes from 10.0.2.4: icmp_seq=8 ttl=64 time=1.15 ms
64 bytes from 10.0.2.4: icmp_seq=9 ttl=64 time=0.461 ms
64 bytes from 10.0.2.4: icmp_seq=10 ttl=64 time=0.937 ms
64 bytes from 10.0.2.4: icmp_seq=11 ttl=64 time=0.638 ms
64 bytes from 10.0.2.4: icmp_seq=12 ttl=64 time=0.665 ms
64 bytes from 10.0.2.4: icmp_seq=13 ttl=64 time=0.301 ms
64 bytes from 10.0.2.4: icmp_seq=14 ttl=64 time=0.531 ms
```

Output of
"sudo tcpdump"

Sean-Client [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

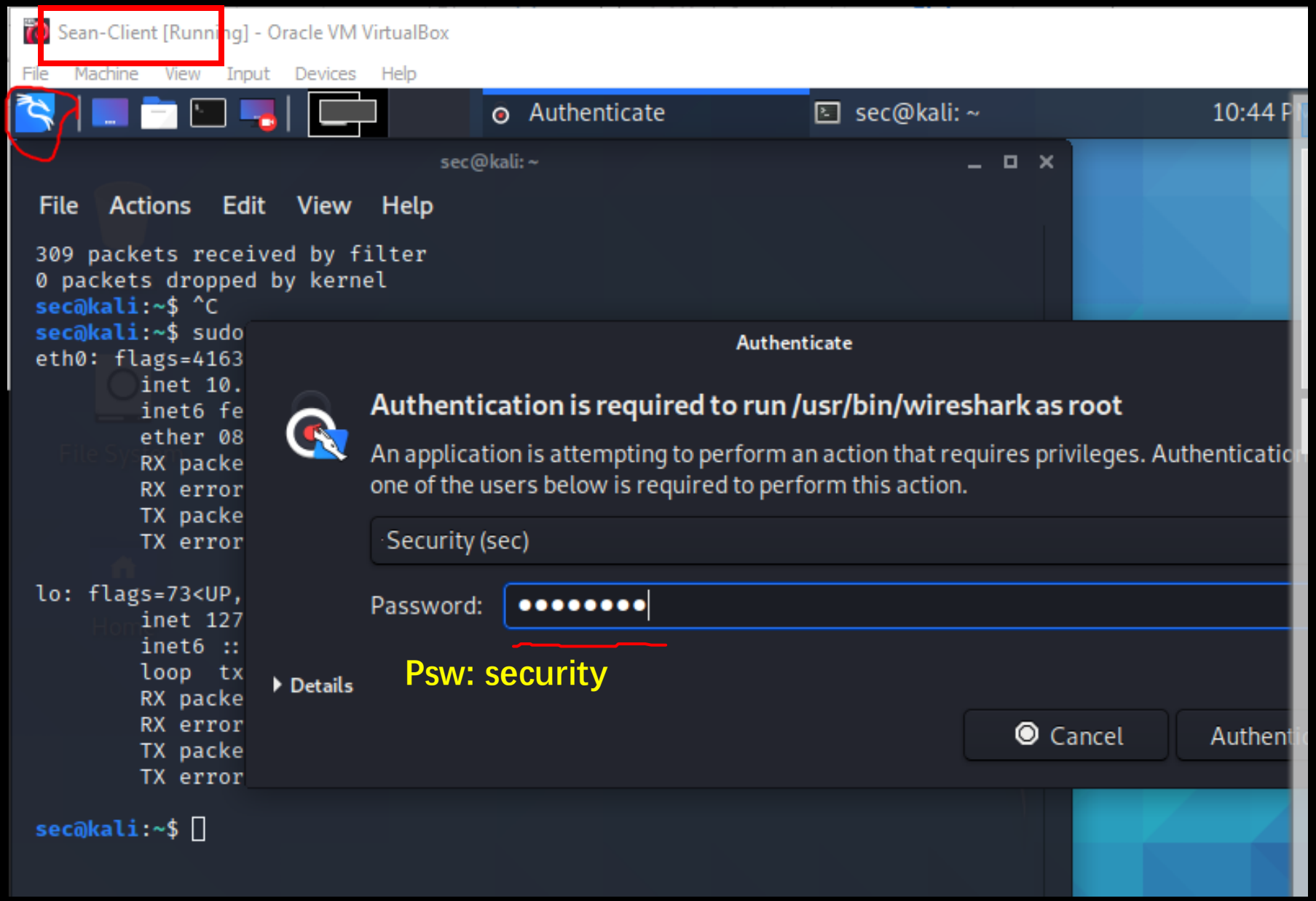
sec@kali: ~

sec@kali: ~

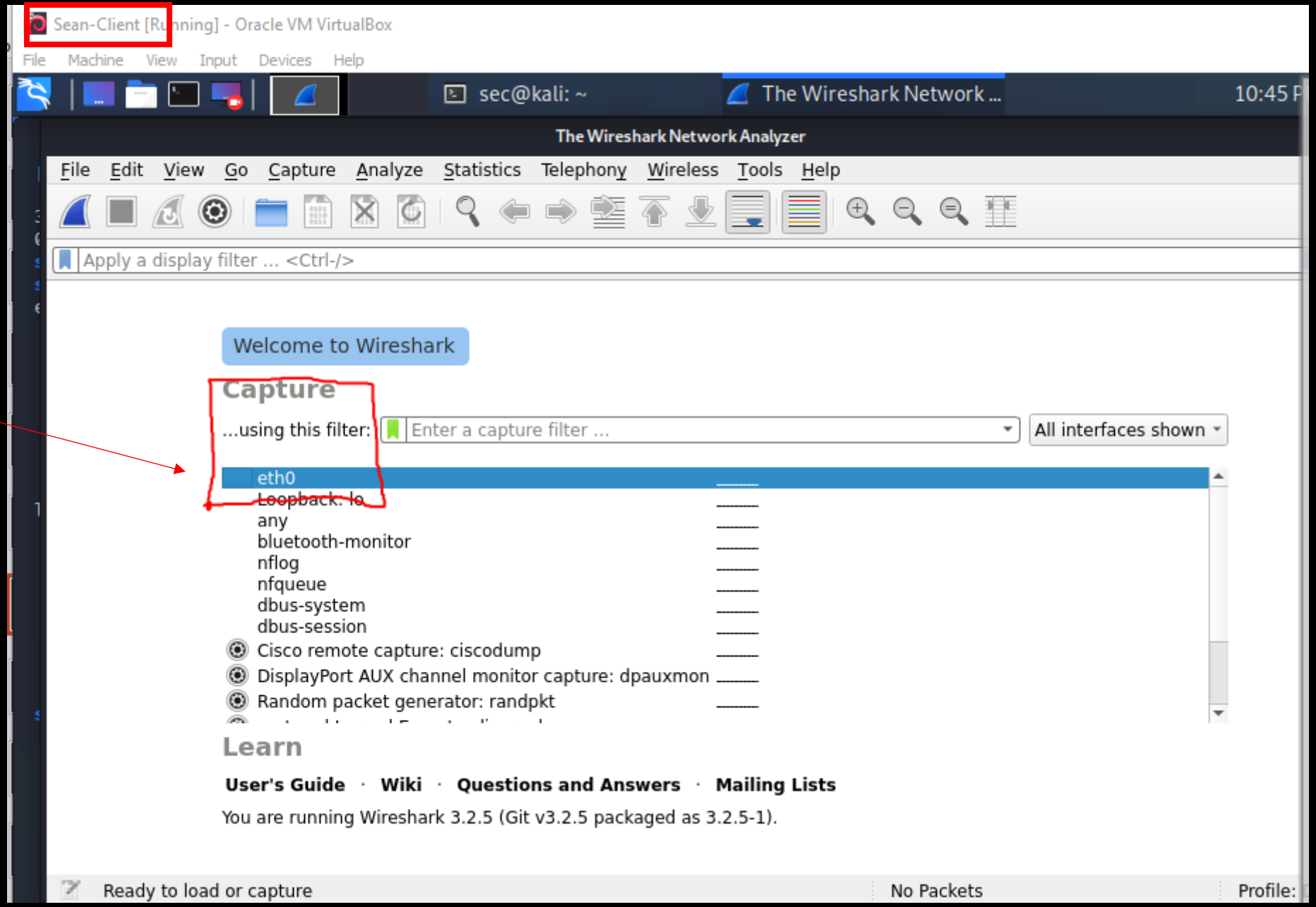
File Actions Edit View Help

```
system.sysDescr.0 system.sysObjectID.0 interfaces.ifTable.ifEntry.ifPhysAdd
ress.1
23:23:37.291581 IP 10.0.2.5.33239 > 255.255.255.255.3289: UDP, length 15
23:23:38.302373 IP 10.0.2.5.55978 > 255.255.255.255.3289: UDP, length 15
23:23:39.310927 IP 10.0.2.5.56785 > 255.255.255.255.1124: UDP, length 37
23:24:42.633033 ARP, Request who-has 10.0.2.4 tell 10.0.2.5, length 46
23:24:42.633228 ARP, Reply 10.0.2.4 is-at 08:00:27:e1:bc:91 (oui Unknown),
length 46
23:24:42.633231 IP 10.0.2.5 > 10.0.2.4: ICMP echo request, id 1084, seq 1,
length 64
23:24:42.633368 IP 10.0.2.4 > 10.0.2.5: ICMP echo reply, id 1084, seq 1, le
ngth 64
23:24:43.659681 IP 10.0.2.5 > 10.0.2.4: ICMP echo request, id 1084, seq 2,
length 64
23:24:43.659857 IP 10.0.2.4 > 10.0.2.5: ICMP echo reply, id 1084, seq 2, le
ngth 64
23:24:44.684486 IP 10.0.2.5 > 10.0.2.4: ICMP echo request, id 1084, seq 3,
length 64
23:24:44.684687 IP 10.0.2.4 > 10.0.2.5: ICMP echo reply, id 1084, seq 3, le
ngth 64
23:24:45.708103 IP 10.0.2.5 > 10.0.2.4: ICMP echo request, id 1084, seq 4,
length 64
23:24:45.708384 IP 10.0.2.4 > 10.0.2.5: ICMP echo reply, id 1084, seq 4, le
```

Click and search for “wireshark”



Double click



Sean-Client [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~ | Capturing from eth0 | 10:47 P

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.5	10.0.2.4	ICMP	98	Echo (ping) request id=0x043c, seq=16836/50
2	0.000190654	10.0.2.4	10.0.2.5	ICMP	98	Echo (ping) reply id=0x043c, seq=16836/50
3	1.023158108	10.0.2.5	10.0.2.4	ICMP	98	Echo (ping) request id=0x043c, seq=16837/50
4	1.023410802	10.0.2.4	10.0.2.5	ICMP	98	Echo (ping) reply id=0x043c, seq=16837/50
5	1.136147438	PcsCompu_e1:bc:91	PcsCompu_5c:65:26	ARP	60	Who has 10.0.2.5? Tell 10.0.2.4
6	1.136299943	PcsCompu_5c:65:26	PcsCompu_e1:bc:91	ARP	60	10.0.2.5 is at 08:00:27:5c:65:26
7	2.064811299	10.0.2.5	10.0.2.4	ICMP	98	Echo (ping) request id=0x043c, seq=16838/50
8	2.064811358	10.0.2.4	10.0.2.5	ICMP	98	Echo (ping) reply id=0x043c, seq=16838/50

```
▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_5c:65:26 (08:00:27:5c:65:26), Dst: PcsCompu_e1:bc:91 (08:00:27:e1:bc:91)
▸ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.4
▸ Internet Control Message Protocol
```

```
0000  08 00 27 e1 bc 91 08 00  27 5c 65 26 08 00 45 00   ··'····· '\e&··E·
0010  00 54 60 ac 40 00 40 01  c1 f4 0a 00 02 05 0a 00   ·T`·@·@· ********
0020  02 04 08 00 74 08 04 3c  41 c4 0d 3e 2a 64 00 00   ····t··< A··>*d··
0030  00 00 3a 82 0d 00 00 00  00 00 10 11 12 13 14 15   ··:····· ********
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ******** ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

eth0: <live capture in progress> | Packets: 74 · Displayed: 74 (100.0%) | Profile:

Use ctrl+C to stop the ping and type in *"telnet xxxx"*

xxxx is your server address

Sean-Client [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~ | Capturing from eth0 | 10:49 P

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
256	121.887632146	10.0.2.4	10.0.2.5	ICMP	98	Echo (ping) reply id=0x043c, seq=16955/15
257	144.071172275	10.0.2.5	10.0.2.4	TCP	74	49358 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1
258	144.071334104	10.0.2.4	10.0.2.5	TCP	74	23 → 49358 [SYN, ACK] Seq=0 Ack=1 Win=65160
259	144.071553925	10.0.2.5	10.0.2.4	TCP	66	49358 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0
260	144.071844496	10.0.2.5	10.0.2.4	TELNET	93	Telnet Data ...
261	144.071844561	10.0.2.4	10.0.2.5	TCP	66	23 → 49358 [ACK] Seq=1 Ack=28 Win=65152 Len=
262	144.075633788	10.0.2.4	10.0.2.5	TELNET	78	Telnet Data ...
263	144.075854547	10.0.2.5	10.0.2.4	TCP	66	49358 → 23 [ACK] Seq=28 Ack=13 Win=64256 Len

```
▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_5c:65:26 (08:00:27:5c:65:26), Dst: PcsCompu_e1:bc:91 (08:00:27:e1:bc:91)
▸ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.4
▸ Internet Control Message Protocol
```

```
0000  08 00 27 e1 bc 91 08 00  27 5c 65 26 08 00 45 00   ··'····· '\e&··E·
0010  00 54 60 ac 40 00 40 01  c1 f4 0a 00 02 05 0a 00   ·T`·@·@· ********
0020  02 04 08 00 74 08 04 3c  41 c4 0d 3e 2a 64 00 00   ····t··< A··>*d··
0030  00 00 3a 82 0d 00 00 00  00 00 10 11 12 13 14 15   ··:····· ********
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ******** ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

eth0: <live capture in progress> | Packets: 324 · Displayed: 324 (100.0%) | Profile:

Sean-Client [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~ | *eth0 | 10:53 P

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
260	144.071844496	10.0.2.5	10.0.2.4	TELNET	93	Telnet Data ...
262	144.075633788	10.0.2.4	10.0.2.5	TELNET	78	Telnet Data ...
264	144.075977652	10.0.2.4	10.0.2.5	TELNET	105	Telnet Data ...
266	144.076163769	10.0.2.5	10.0.2.4	TELNET	149	Telnet Data ...
268	144.076429248	10.0.2.4	10.0.2.5	TELNET	69	Telnet Data ...
270	144.076740313	10.0.2.5	10.0.2.4	TELNET	69	Telnet Data ...
272	144.077110800	10.0.2.4	10.0.2.5	TELNET	69	Telnet Data ...
274	144.077295626	10.0.2.5	10.0.2.4	TELNET	69	Telnet Data ...

```
▸ Frame 260: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_5c:65:26 (08:00:27:5c:65:26), Dst: PcsCompu_e1:bc:91 (08:00:27:e1:bc:91)
▸ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.4
▸ Transmission Control Protocol, Src Port: 49358, Dst Port: 23, Seq: 1, Ack: 1, Len: 27
▸ Telnet
```

```
0000  08 00 27 e1 bc 91 08 00  27 5c 65 26 08 00 45 10   ··'····· '\e&··E·
0010  00 4f 25 ad 40 00 40 06  fc e3 0a 00 02 05 0a 00   ·O%·@·@· ........
0020  02 04 c0 ce 00 17 f6 db  4e 81 00 22 1f 59 80 18   ........ N··"·Y··
0030  01 f6 db de 00 00 01 01  08 0a 17 50 81 79 09 96   ........ ···P·y··
0040  39 52 ff fd 03 ff fb 18  ff fb 1f ff fb 20 ff fb   9R...... ..... ··
0050  21 ff fb 22 ff fb 27 ff  fd 05 ff fb 23            !··"··'· ····#
```

Telnet: Protocol | Packets: 332 · Displayed: 33 (9.9%) | Profile:

You can analyze the inner details of a single packet by double-clicking on it.

Sean-Client [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~ | *eth0 | Wireshark · Packet 26... | 10:54 P

Wireshark · Packet 260 · eth0

```
▸ Frame 260: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_5c:65:26 (08:00:27:5c:65:26), Dst: PcsCompu_e1:bc:91 (08:00:27:e1:bc:91
▾ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 79
    Identification: 0x25ad (9645)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xfce3 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.5
    Destination: 10.0.2.4
▸ Transmission Control Protocol, Src Port: 49358, Dst Port: 23, Seq: 1, Ack: 1, Len: 27
▸ Telnet
```

```
0000  08 00 27 e1 bc 91 08 00  27 5c 65 26 08 00 45 10   ··'····· '\e&··E·
0010  00 4f 25 ad 40 00 40 06  fc e3 0a 00 02 05 0a 00   ·O%·@·@· ........
0020  02 04 c0 ce 00 17 f6 db  4e 81 00 22 1f 59 80 18   ........ N··"·Y··
0030  01 f6 db de 00 00 01 01  08 0a 17 50 81 79 09 96   ........ ···P·y··
0040  39 52 ff fd 03 ff fb 18  ff fb 1f ff fb 20 ff fb   9R...... ····· ··
0050  21 ff fb 22 ff fb 27 ff  fd 05 ff fb 23            !··"··'· ····#
```

Close | Help

File Edit View Go

telnet

No.	Time
260	144.071844
262	144.075633
264	144.075977
266	144.076163
268	144.076429
270	144.076740
272	144.077110
274	144.077295

Frame 260: 93 by
Ethernet II, Src
Internet Protoco
Transmission Con
Telnet

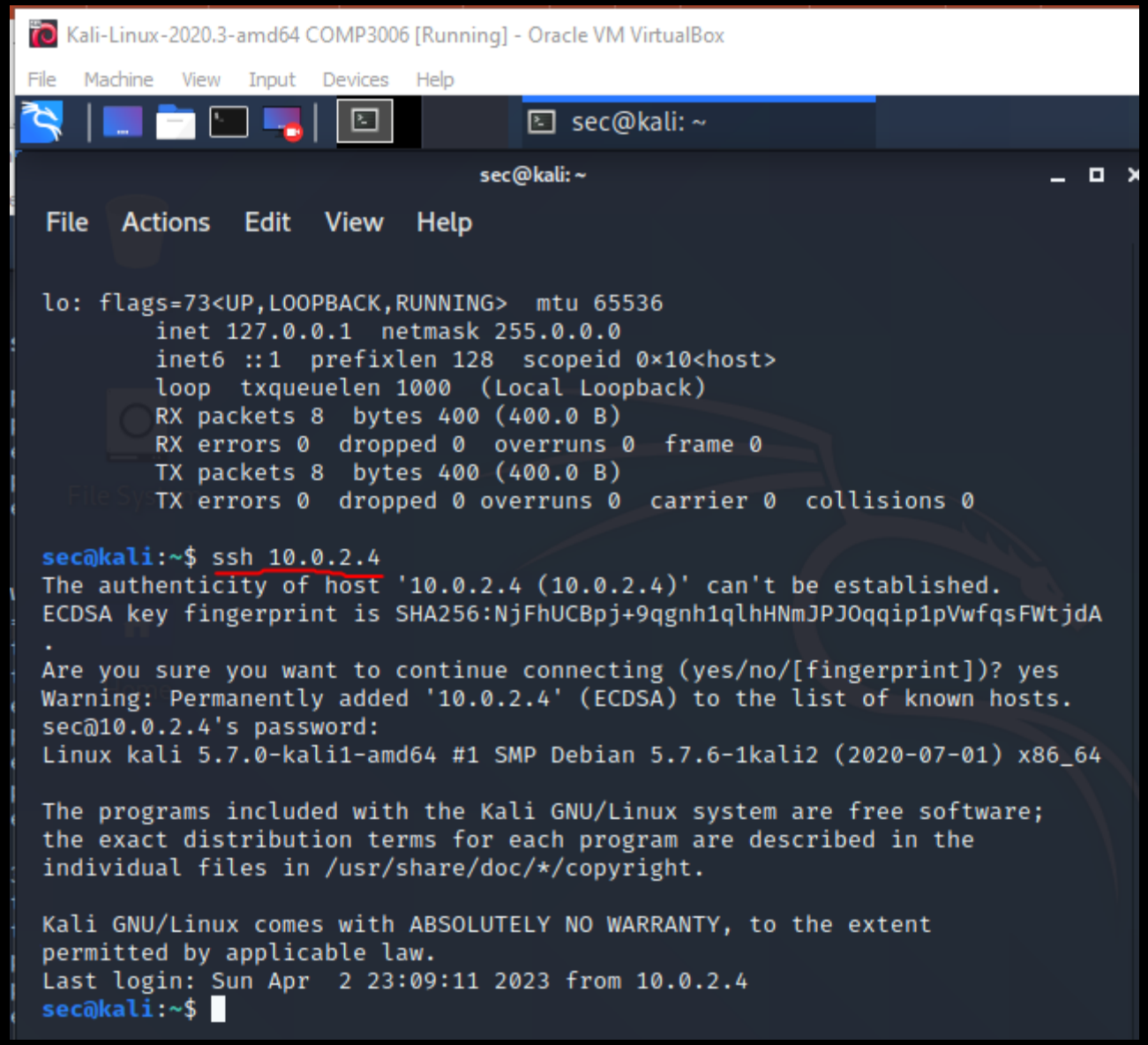
Telnet: Protocol | Packets: 336 · Displayed: 33 (9.8%) | Profile:

***Important

1. Start a new Wireshark capture

2. Open a new terminal and typed in *"ssh xxxx"*

xxxx is your server address.



Sean-Client [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~ | Capturing from eth0 | Wireshark · Packet 260 · ...

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: ssh

No.	Time	Source	Destination	Protocol	Length	Info
624	1057.8735935…	10.0.2.4	10.0.2.5	SSHv2	158	Server: Encrypted packet (len=92)
627	1062.8466574…	10.0.2.5	10.0.2.4	SSHv2	102	Client: Encrypted packet (len=36)
628	1062.8470688…	10.0.2.4	10.0.2.5	SSHv2	102	Server: Encrypted packet (len=36)
630	1063.1023076…	10.0.2.5	10.0.2.4	SSHv2	102	Client: Encrypted packet (len=36)
631	1063.1026572…	10.0.2.4	10.0.2.5	SSHv2	102	Server: Encrypted packet (len=36)
633	1063.9984562…	10.0.2.5	10.0.2.4	SSHv2	102	Client: Encrypted packet (len=36)
634	1063.9988063…	10.0.2.4	10.0.2.5	SSHv2	102	Server: Encrypted packet (len=36)
636	1064.1583996…	10.0.2.5	10.0.2.4	SSHv2	102	Client: Encrypted packet (len=36)
637	1064.1588507…	10.0.2.4	10.0.2.5	SSHv2	102	Server: Encrypted packet (len=36)
639	1064.3505722…	10.0.2.5	10.0.2.4	SSHv2	102	Client: Encrypted packet (len=36)
640	1064.3512252…	10.0.2.4	10.0.2.5	SSHv2	110	Server: Encrypted packet (len=44)
642	1064.3534600…	10.0.2.4	10.0.2.5	SSHv2	242	Server: Encrypted packet (len=176)
644	1064.3536943…	10.0.2.5	10.0.2.4	SSHv2	102	Client: Encrypted packet (len=36)
645	1064.3536943…	10.0.2.5	10.0.2.4	SSHv2	126	Client: Encrypted packet (len=60)

```
▸ Frame 645: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface eth0, id 0
▾ Ethernet II, Src: PcsCompu_5c:65:26 (08:00:27:5c:65:26), Dst: PcsCompu_e1:bc:91 (08:00:27:e1:bc:91)
  ▾ Destination: PcsCompu_e1:bc:91 (08:00:27:e1:bc:91)
      Address: PcsCompu_e1:bc:91 (08:00:27:e1:bc:91)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: PcsCompu_5c:65:26 (08:00:27:5c:65:26)
      Address: PcsCompu_5c:65:26 (08:00:27:5c:65:26)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 112
    Identification: 0xbd9c (48540)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
```

```
0000  08 00 27 e1 bc 91 08 00 27 5c 65 26 08 00 45 10   ··'····· '\e&··E·
0010  00 70 bd 9c 40 00 40 06 64 d3 0a 00 02 05 0a 00   ·p··@·@· d·******
0020  02 04 8c 0e 00 16 5f 64 b9 a4 88 39 90 78 80 18   ******_d ···9·x··
0030  01 f5 2f 9c 00 00 01 01 08 0a 74 b5 8f 59 09 b7   ··/····· ··t··Y··
0040  7f f3 53 e8 e0 1b 70 17 28 c1 a6 6d cd 96 da 79   ··S···p· (··m···y
0050  3e de 98 ce d6 c0 f8 ab 9d be 49 62 4e eb d1 e1   >******· ··IbN···
0060  b1 b0 c5 b6 94 26 ee bf a7 6e 07 8b f6 9d 36 ad   ·····&·· ·n····6·
0070  c4 06 63 c3 26 33 a7 2d 64 72 62 9a 84 19         ··c·&3·- drb···
```

Please Remember to Shut Down the Virtual Machines

Additional Tasks:

Read the document COMP3052.SEC.LAB.04.Packet.Sniffing originally prepared by Mike Pound.

Work on the exercises described under the following sections from pages 2-5 for:

SETTING UP THE SERVER

PACKET CAPTURE

PACKET ANALYSIS