Digital Forensics

2021SM_CS_6419_FRE1A

Assignment-01

Prepared by:
Mohammadali Rahnama

Student number:
3709515

EST. 1785 UNB
UNIVERSITY OF NEW BRUNSWICK

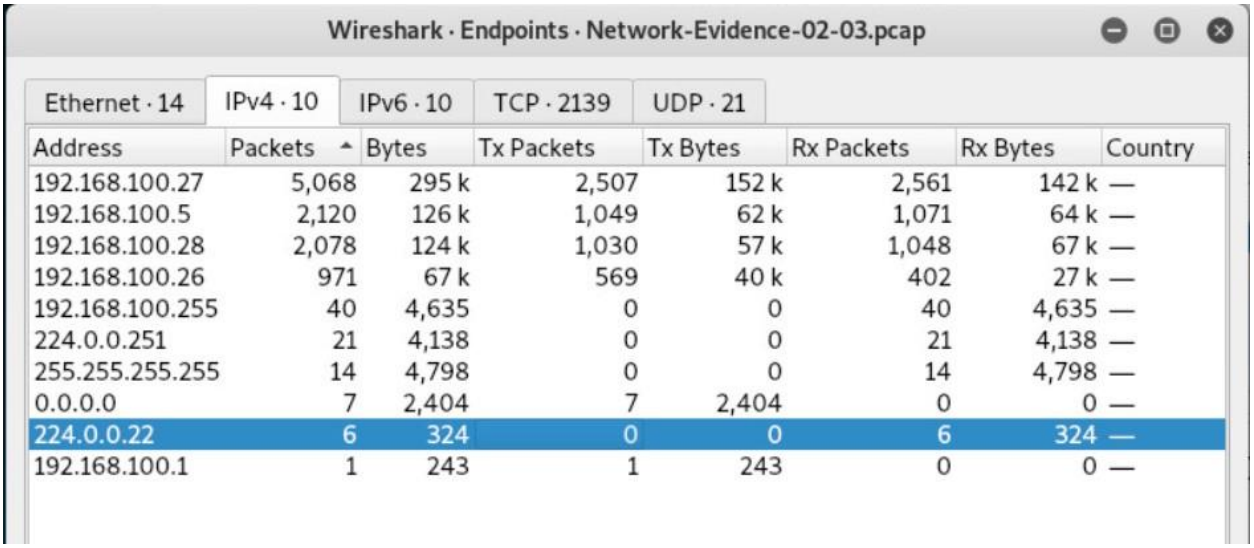
1. What is the network address and subnet mask?

The subnet mask is 255.255.255.0, the network address is 192.168.100

2. For each computer:

   a. What is the IP of the computer?

   There are 4 computers on the network: 192.168.100.5, 192.168.100.26, 192.168.100.27, 192.168.100.28



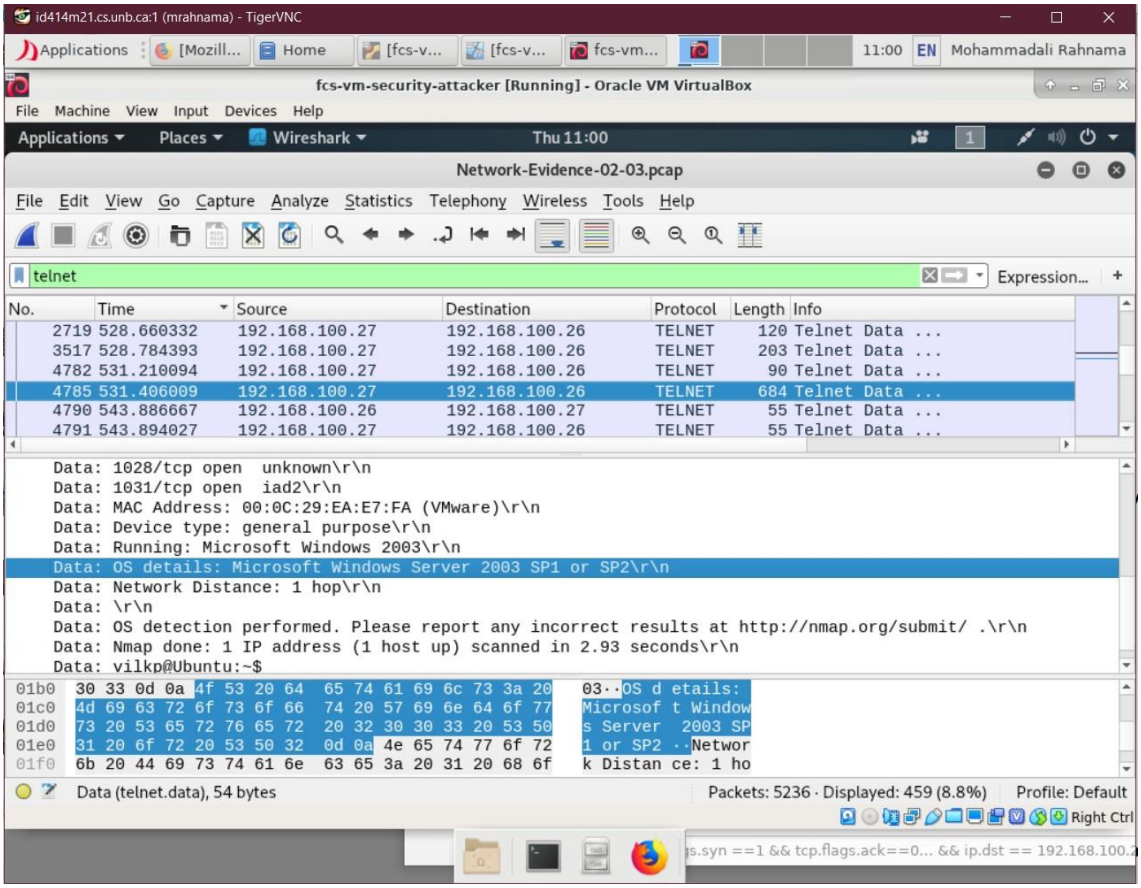
Wireshark · Endpoints · Network-Evidence-02-03.pcap

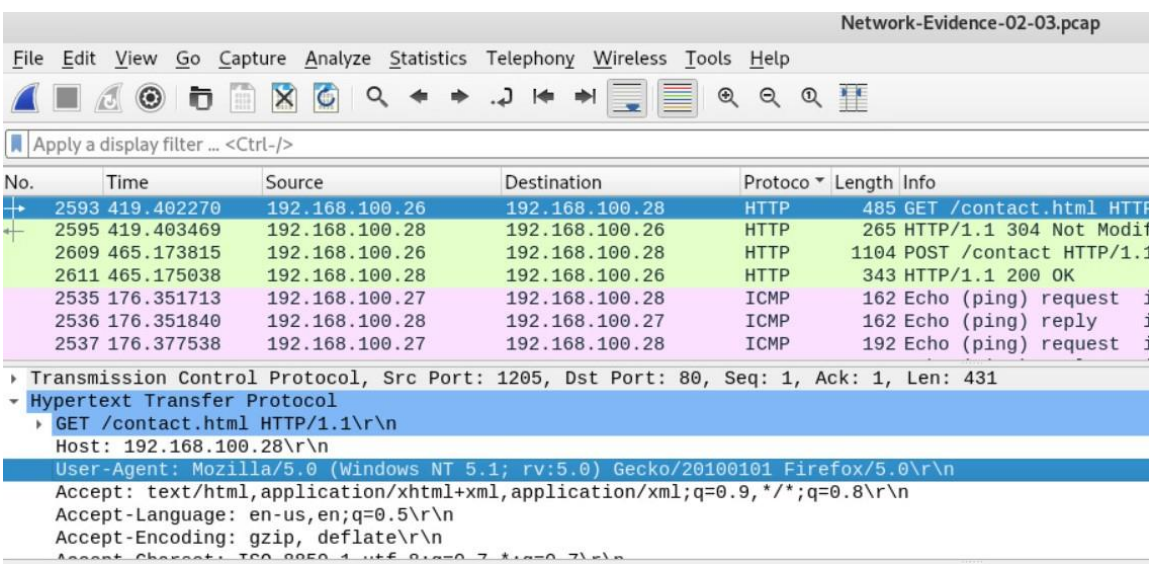
Ethernet · 14 | IPv4 · 10 | IPv6 · 10 | TCP · 2139 | UDP · 21

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country
192.168.100.27	5,068	295 k	2,507	152 k	2,561	142 k	—
192.168.100.5	2,120	126 k	1,049	62 k	1,071	64 k	—
192.168.100.28	2,078	124 k	1,030	57 k	1,048	67 k	—
192.168.100.26	971	67 k	569	40 k	402	27 k	—
192.168.100.255	40	4,635	0	0	40	4,635	—
224.0.0.251	21	4,138	0	0	21	4,138	—
255.255.255.255	14	4,798	0	0	14	4,798	—
0.0.0.0	7	2,404	7	2,404	0	0	—
224.0.0.22	6	324	0	0	6	324	—
192.168.100.1	1	243	1	243	0	0	—

   b. What OS is it running?

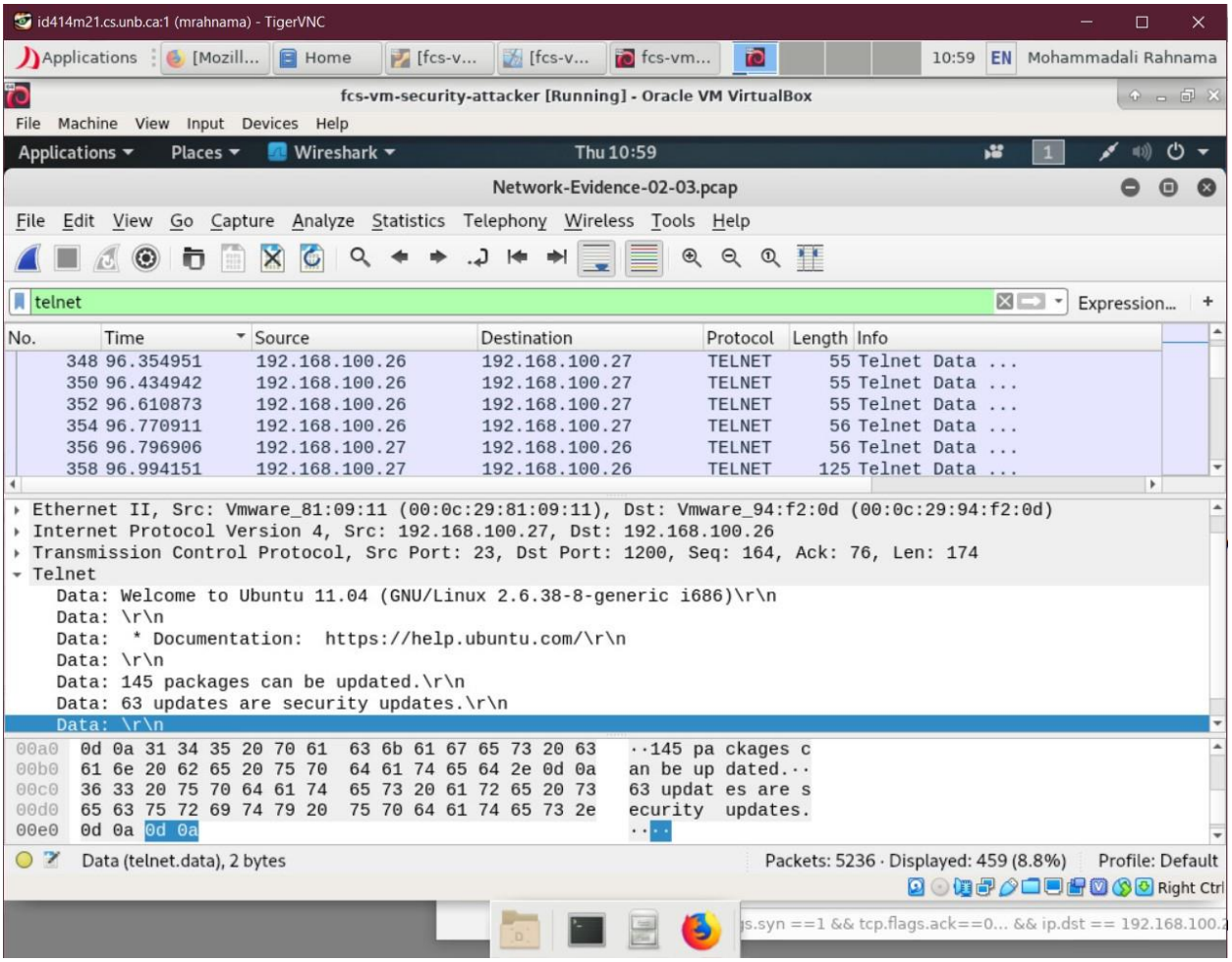
   192.168.100.5 is using Microsoft Windows Server 2003.
   192.168.100.26 is using Microsoft Windows XP.
   192.168.100.27 is using Ubuntu.
   192.168.100.28 is using Ubuntu.

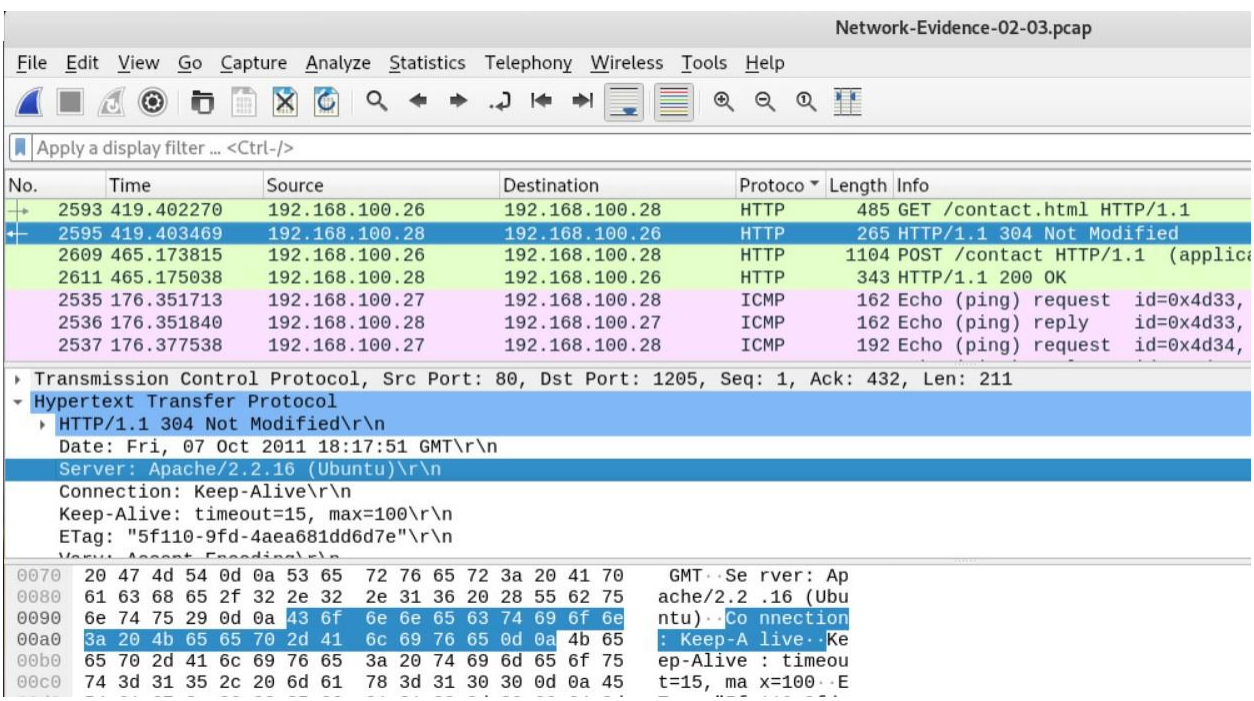




No.	Time	Source	Destination	Protoco	Length	Info
2593	419.402270	192.168.100.26	192.168.100.28	HTTP	485	GET /contact.html HTTP
2595	419.403469	192.168.100.28	192.168.100.26	HTTP	265	HTTP/1.1 304 Not Modif
2609	465.173815	192.168.100.26	192.168.100.28	HTTP	1104	POST /contact HTTP/1.1
2611	465.175038	192.168.100.28	192.168.100.26	HTTP	343	HTTP/1.1 200 OK
2535	176.351713	192.168.100.27	192.168.100.28	ICMP	162	Echo (ping) request
2536	176.351840	192.168.100.28	192.168.100.27	ICMP	162	Echo (ping) reply
2537	176.377538	192.168.100.27	192.168.100.28	ICMP	192	Echo (ping) request

```
Transmission Control Protocol, Src Port: 1205, Dst Port: 80, Seq: 1, Ack: 1, Len: 431
Hypertext Transfer Protocol
  GET /contact.html HTTP/1.1\r\n
  Host: 192.168.100.28\r\n
  User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-us,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
```


id414m21.cs.unb.ca:1 (mrahnama) - TigerVNC
fcs-vm-security-attacker [Running] - Oracle VM VirtualBox
Network-Evidence-02-03.pcap
telnet
No. Time Source Destination Protocol Length Info
348 96.354951 192.168.100.26 192.168.100.27 TELNET 55 Telnet Data ...
350 96.434942 192.168.100.26 192.168.100.27 TELNET 55 Telnet Data ...
352 96.610873 192.168.100.26 192.168.100.27 TELNET 55 Telnet Data ...
354 96.770911 192.168.100.26 192.168.100.27 TELNET 56 Telnet Data ...
356 96.796906 192.168.100.27 192.168.100.26 TELNET 56 Telnet Data ...
358 96.994151 192.168.100.27 192.168.100.26 TELNET 125 Telnet Data ...
Ethernet II, Src: Vmware_81:09:11 (00:0c:29:81:09:11), Dst: Vmware_94:f2:0d (00:0c:29:94:f2:0d)
Internet Protocol Version 4, Src: 192.168.100.27, Dst: 192.168.100.26
Transmission Control Protocol, Src Port: 23, Dst Port: 1200, Seq: 164, Ack: 76, Len: 174
Telnet
Data: Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-generic i686)\r\n
Data: \r\n
Data: * Documentation: https://help.ubuntu.com/\r\n
Data: \r\n
Data: 145 packages can be updated.\r\n
Data: 63 updates are security updates.\r\n
Data: \r\n
00a0 0d 0a 31 34 35 20 70 61 63 6b 61 67 65 73 20 63 ··145 pa ckages c
00b0 61 6e 20 62 65 20 75 70 64 61 74 65 64 2e 0d 0a an be up dated.··
00c0 36 33 20 75 70 64 61 74 65 73 20 61 72 65 20 73 63 updat es are s
00d0 65 63 75 72 69 74 79 20 75 70 64 61 74 65 73 2e ecurity updates.
00e0 0d 0a 0d 0a ····
Data (telnet.data), 2 bytes
Packets: 5236 · Displayed: 459 (8.8%)
Profile: Default


Network-Evidence-02-03.pcap
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
2593 419.402270 192.168.100.26 192.168.100.28 HTTP 485 GET /contact.html HTTP/1.1
2595 419.403469 192.168.100.28 192.168.100.26 HTTP 265 HTTP/1.1 304 Not Modified
2609 465.173815 192.168.100.26 192.168.100.28 HTTP 1104 POST /contact HTTP/1.1 (applic
2611 465.175038 192.168.100.28 192.168.100.26 HTTP 343 HTTP/1.1 200 OK
2535 176.351713 192.168.100.27 192.168.100.28 ICMP 162 Echo (ping) request id=0x4d33,
2536 176.351840 192.168.100.28 192.168.100.27 ICMP 162 Echo (ping) reply id=0x4d33,
2537 176.377538 192.168.100.27 192.168.100.28 ICMP 192 Echo (ping) request id=0x4d34,
Transmission Control Protocol, Src Port: 80, Dst Port: 1205, Seq: 1, Ack: 432, Len: 211
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
Date: Fri, 07 Oct 2011 18:17:51 GMT\r\n
Server: Apache/2.2.16 (Ubuntu)\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=15, max=100\r\n
ETag: "5f110-9fd-4aea681dd6d7e"\r\n
0070 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT··Se rver: Ap
0080 61 63 68 65 2f 32 2e 32 2e 31 36 20 28 55 62 75 ache/2.2 .16 (Ubu
0090 6e 74 75 29 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e ntu)··Co nnection
00a0 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 4b 65 : Keep-A live··Ke
00b0 65 70 2d 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 ep-Alive : timeou
00c0 74 3d 31 35 2c 20 6d 61 78 3d 31 30 30 0d 0a 45 t=15, ma x=100··E

c. What is the MAC address?

192.168.100.5 is 00:0c:29:ea:e7:fa.
192.168.100.26 is 00:0c:29:94:f2:0d.
192.168.100.27 is 00:0c:29:81:09:11.
192.168.100.28 is 00:0c:29:15:09:d5.

Wireshark · Endpoints · Network-Evidence-02-03.pcap

Ethernet · 14 | IPv4 · 10 | IPv6 · 10 | TCP · 2139 | UDP · 21

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:0c:29:81:09:11	5,104	300 k	2,536	157 k	2,568	143 k
00:0c:29:ea:e7:fa	2,127	126 k	1,055	62 k	1,072	64 k
00:0c:29:15:09:d5	2,095	126 k	1,044	58 k	1,051	67 k
00:0c:29:94:f2:0d	995	69 k	586	42 k	409	27 k
ff:ff:ff:ff:ff:ff	70	10 k	0	0	70	10 k
01:00:5e:00:00:fb	21	4,138	0	0	21	4,138
00:50:56:c0:00:01	15	2,567	15	2,567	0	0
33:33:00:01:00:02	14	2,324	0	0	14	2,324
33:33:00:00:00:fb	12	3,379	0	0	12	3,379
01:00:5e:00:00:16	6	324	0	0	6	324
33:33:00:00:00:02	6	420	0	0	6	420
33:33:00:00:00:16	5	470	0	0	5	470
33:33:ff:15:09:d5	1	78	0	0	1	78
33:33:ff:81:09:11	1	78	0	0	1	78

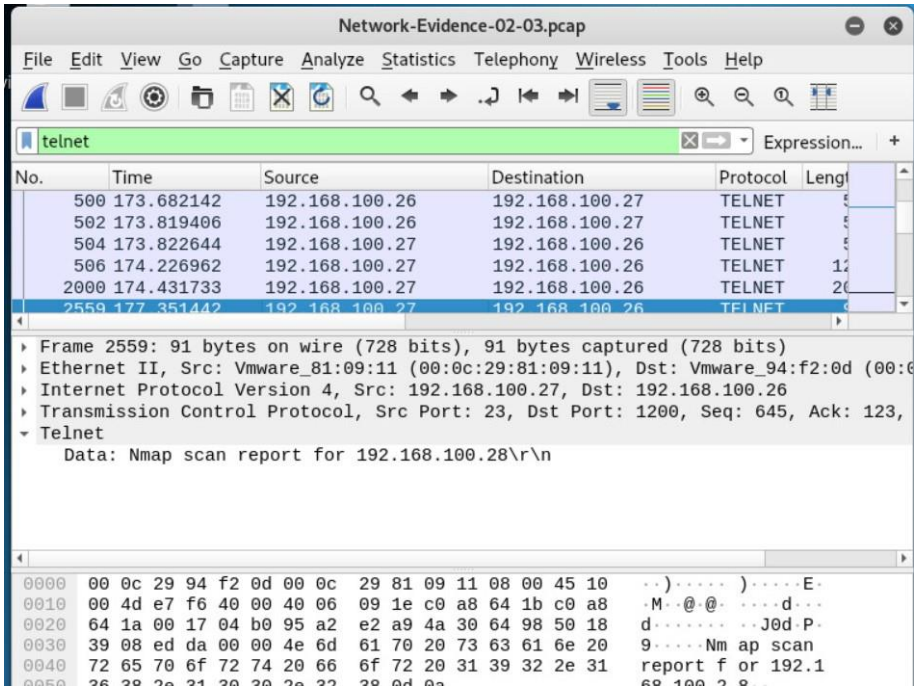
3. What is a port scan?

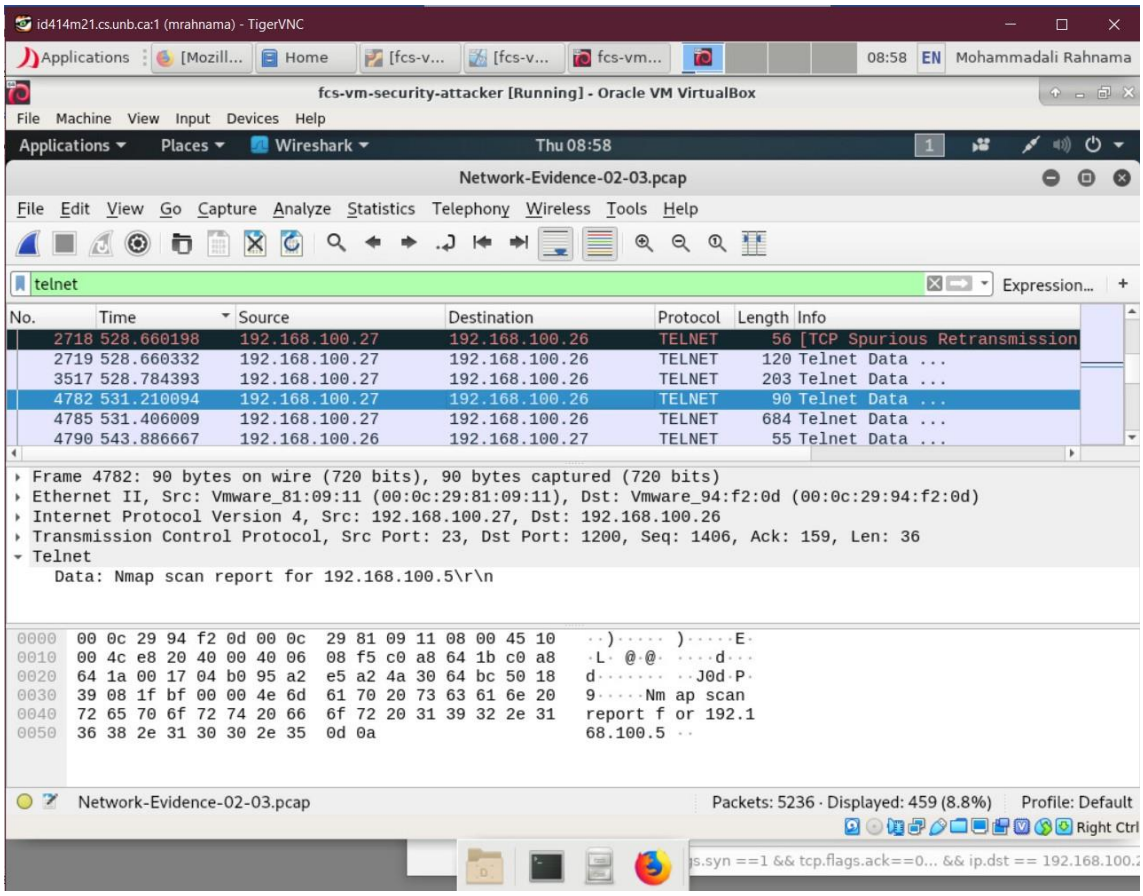
Port scanning is a technique for determining which network ports are open and potentially receiving or sending data. It is also a method of sending packets to specific ports on a host and analyzing the responses to find vulnerabilities.

This scanning cannot take place unless a list of active hosts is identified and mapped to their IP addresses. This activity, known as host discovery, begins with a network scan. The goal of port and network scanning is to identify the organization of IP addresses, hosts, and ports so that open or vulnerable server locations can be determined, and security levels can be diagnosed.

a. How many port scans were run?

Once Using TCP, and twice using Telnet.


Network-Evidence-02-03.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet
Expression...
No. Time Source Destination Protocol Length
500 173.682142 192.168.100.26 192.168.100.27 TELNET
502 173.819406 192.168.100.26 192.168.100.27 TELNET
504 173.822644 192.168.100.27 192.168.100.26 TELNET
506 174.226962 192.168.100.27 192.168.100.26 TELNET
2000 174.431733 192.168.100.27 192.168.100.26 TELNET
2559 177.351442 192.168.100.27 192.168.100.26 TELNET
Frame 2559: 91 bytes on wire (728 bits), 91 bytes captured (728 bits)
Ethernet II, Src: Vmware_81:09:11 (00:0c:29:81:09:11), Dst: Vmware_94:f2:0d (00:0
Internet Protocol Version 4, Src: 192.168.100.27, Dst: 192.168.100.26
Transmission Control Protocol, Src Port: 23, Dst Port: 1200, Seq: 645, Ack: 123,
Telnet
Data: Nmap scan report for 192.168.100.28\r\n
0000 00 0c 29 94 f2 0d 00 0c 29 81 09 11 08 00 45 10
0010 00 4d e7 f6 40 00 40 06 09 1e c0 a8 64 1b c0 a8
0020 64 1a 00 17 04 b0 95 a2 e2 a9 4a 30 64 98 50 18
0030 39 08 ed da 00 00 4e 6d 61 70 20 73 63 61 6e 20
0040 72 65 70 6f 72 74 20 66 6f 72 20 31 39 32 2e 31
9·····Nm ap scan
report f or 192.1

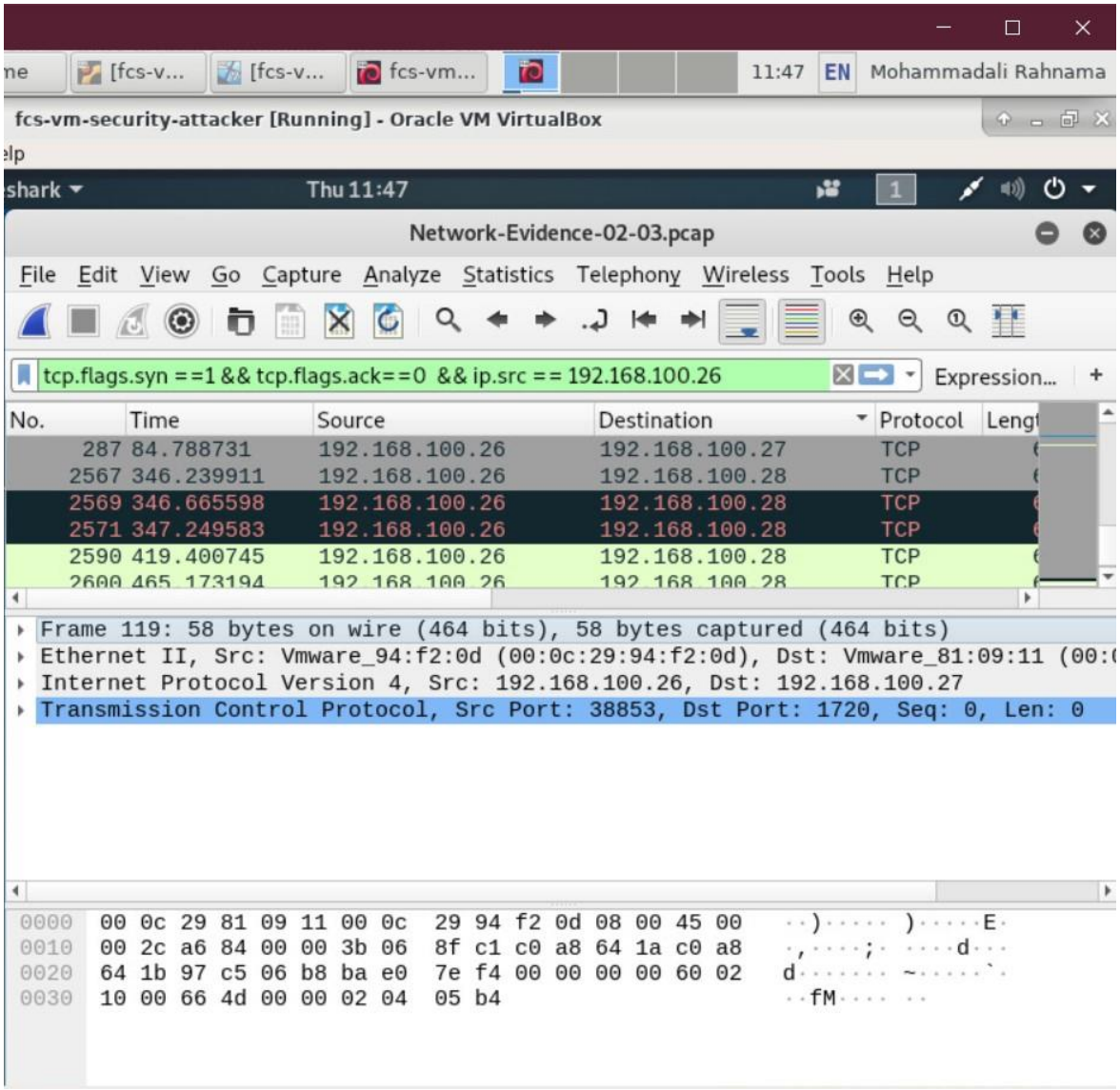

id414m21.cs.unb.ca:1 (mrahnama) - TigerVNC
Applications [Mozill... Home [fcs-v... [fcs-v... fcs-vm...
08:58 EN Mohammadali Rahnama
fcs-vm-security-attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Wireshark Thu 08:58
Network-Evidence-02-03.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet
Expression...
No. Time Source Destination Protocol Length Info
2718 528.660198 192.168.100.27 192.168.100.26 TELNET 56 [TCP Spurious Retransmission
2719 528.660332 192.168.100.27 192.168.100.26 TELNET 120 Telnet Data ...
3517 528.784393 192.168.100.27 192.168.100.26 TELNET 203 Telnet Data ...
4782 531.210094 192.168.100.27 192.168.100.26 TELNET 90 Telnet Data ...
4785 531.406009 192.168.100.27 192.168.100.26 TELNET 684 Telnet Data ...
4790 543.886667 192.168.100.26 192.168.100.27 TELNET 55 Telnet Data ...
Frame 4782: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Vmware_81:09:11 (00:0c:29:81:09:11), Dst: Vmware_94:f2:0d (00:0c:29:94:f2:0d)
Internet Protocol Version 4, Src: 192.168.100.27, Dst: 192.168.100.26
Transmission Control Protocol, Src Port: 23, Dst Port: 1200, Seq: 1406, Ack: 159, Len: 36
Telnet
Data: Nmap scan report for 192.168.100.5\r\n
0000 00 0c 29 94 f2 0d 00 0c 29 81 09 11 08 00 45 10
0010 00 4c e8 20 40 00 40 06 08 f5 c0 a8 64 1b c0 a8
0020 64 1a 00 17 04 b0 95 a2 e5 a2 4a 30 64 bc 50 18
0030 39 08 1f bf 00 00 4e 6d 61 70 20 73 63 61 6e 20
0040 72 65 70 6f 72 74 20 66 6f 72 20 31 39 32 2e 31
0050 36 38 2e 31 30 30 2e 35 0d 0a
9·····Nm ap scan
report f or 192.1
68.100.5 ··
Network-Evidence-02-03.pcap
Packets: 5236 · Displayed: 459 (8.8%)
Profile: Default
Right Ctrl

b. What computer initiated the port scan(s)? What were the target computers?

192.168.100.26 initiated the port scans and 192.168.100.5, 192.168.100.27 and 192.168.100.28 were the targets.

c. What type of port scan(s) did the attacker use (refer to the Nmap)?

They used TCP Half-Open Scan. The TCP half-open port scan, also known as a SYN scan, is one of the more common and popular port scanning techniques. Unlike TCP Connect, Half-Open leaves the target hanging rather than completing the TCP connection.



4. What computer (refer by OS name and last octet of the IP address) is running the telnet service?

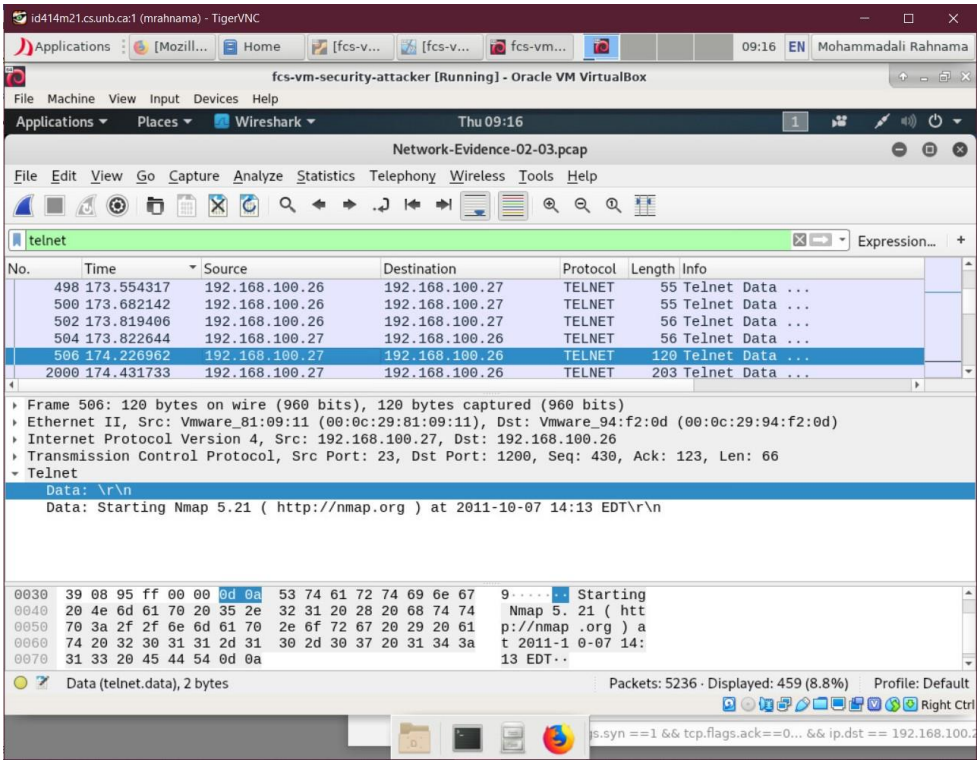
192.168.100.27, Ubuntu

a. Which computer(s) accessed the telnet server?

192.168.100.26, Microsoft Windows XP

b. At what time(s)/date did this access occur?

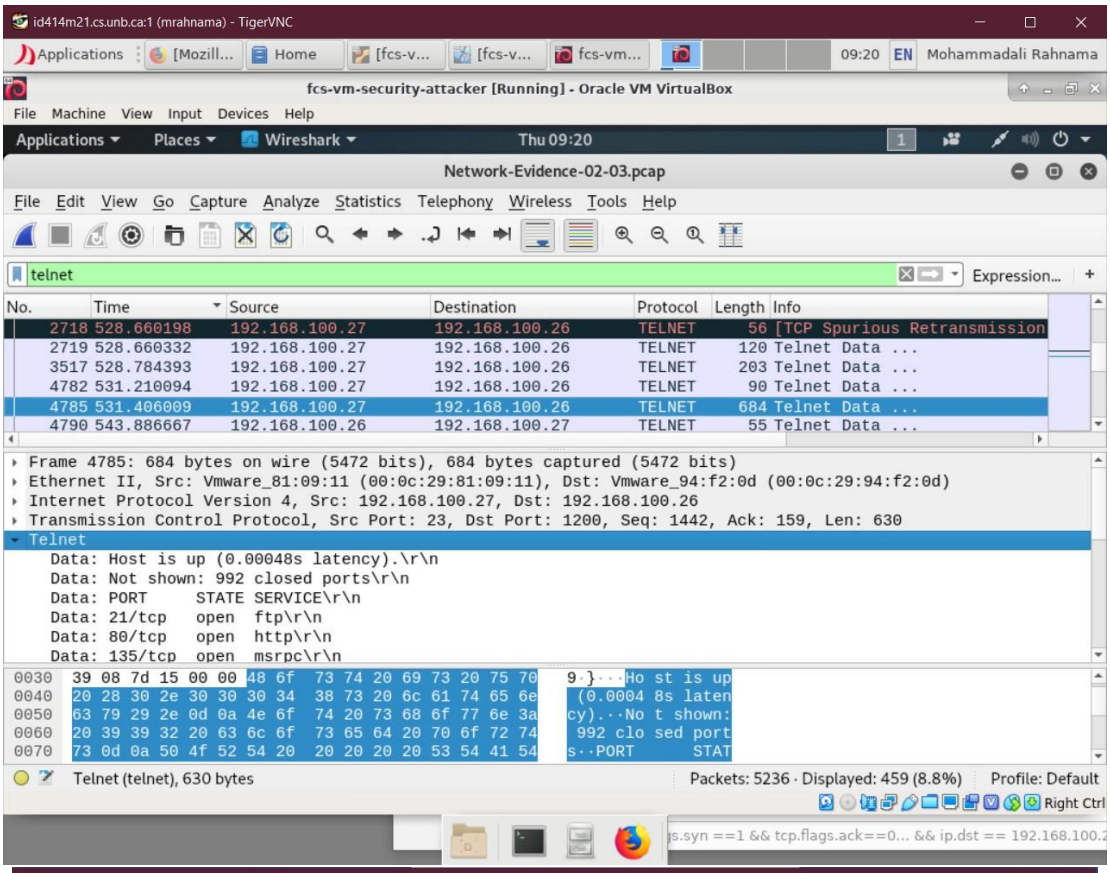
at 2011-10-07 14:13 EDT

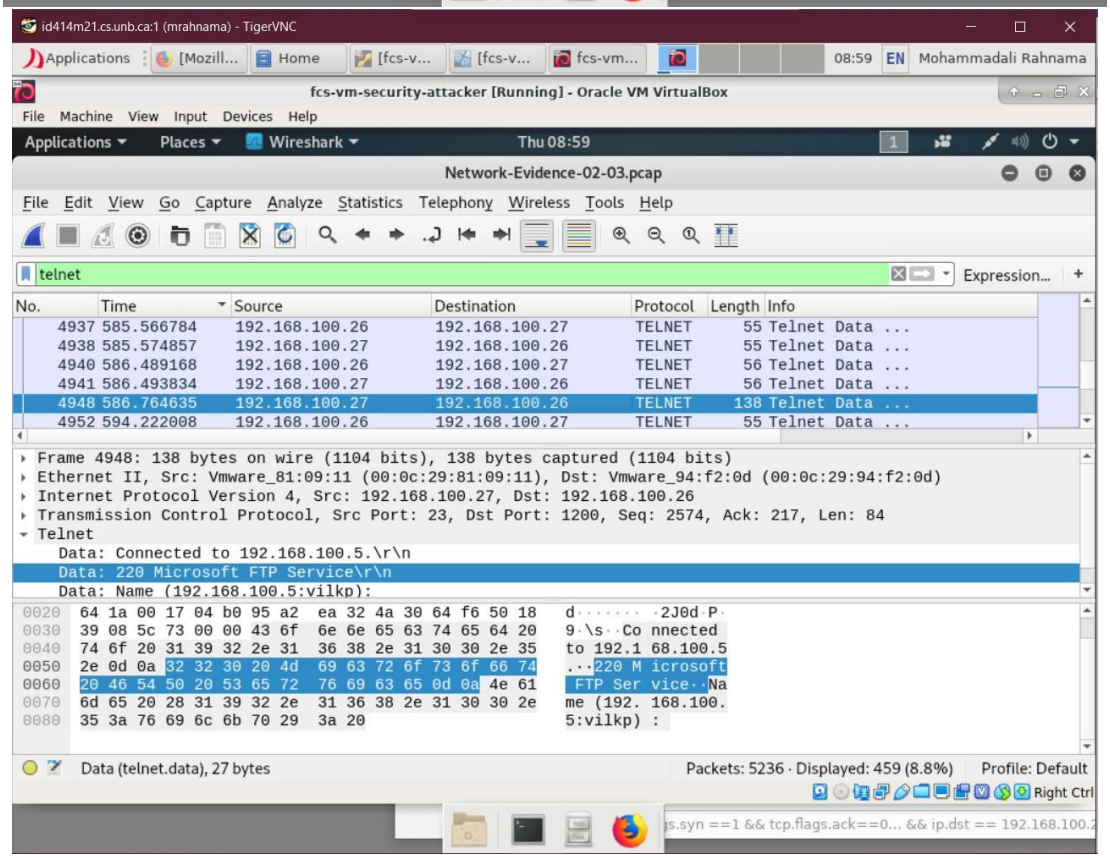


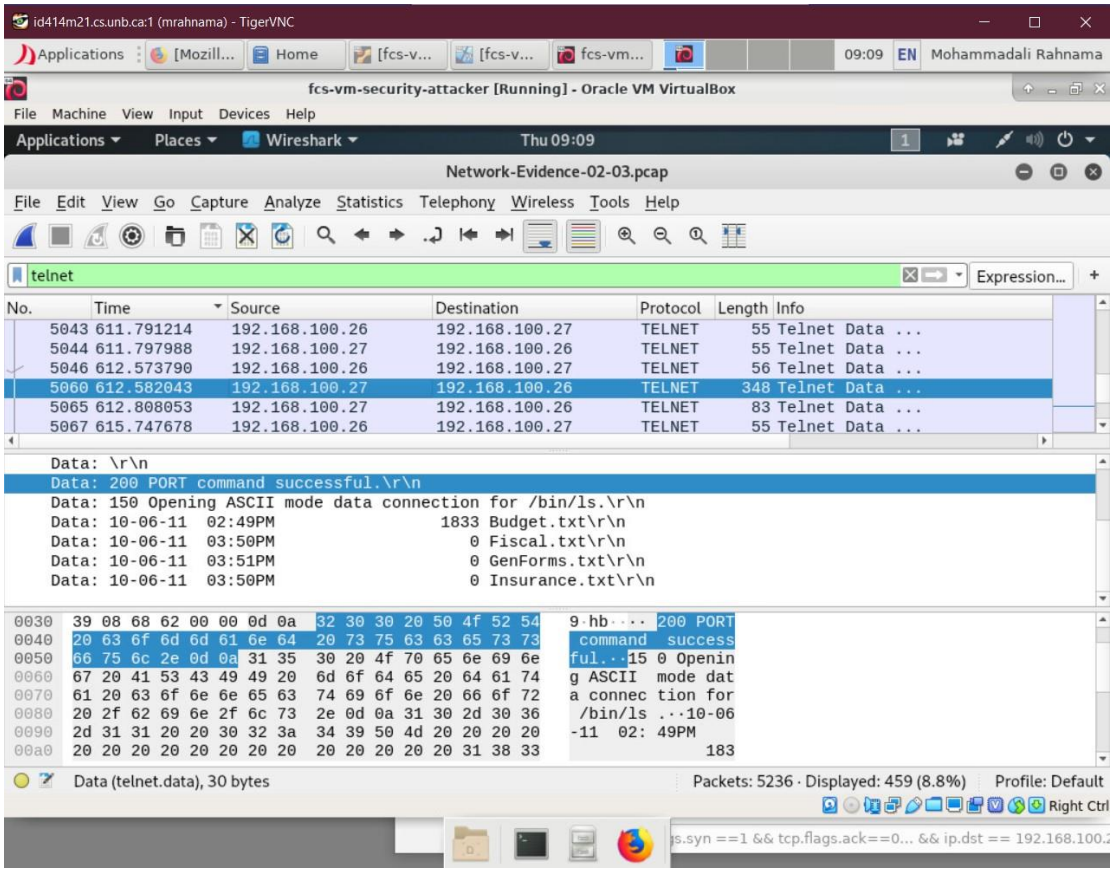
5. What usernames/passwords were used to access the telnet server?
Username: Vilkp, Password: Password, email: yeah@right.com

a. What did the attacker do, if anything, from the telnet server?
b. Explain why the attacker might have done this.

They usen Nmap to check the ports of the computers on the network (192.168.100.5,192.168.100.28) and when they realized that an FTP port is open they used the FTP protocol to retrieve a sensitive file called Budget.txt


id414m21.cs.unb.ca:1 (mrahnama) - TigerVNC
Applications [Mozill... Home [fcs-v... [fcs-v... fcs-vm... 09:20 EN Mohammadali Rahnama
fcs-vm-security-attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Wireshark Thu 09:20
Network-Evidence-02-03.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet
Expression...
No. Time Source Destination Protocol Length Info
2718 528.660198 192.168.100.27 192.168.100.26 TELNET 56 [TCP Spurious Retransmission
2719 528.660332 192.168.100.27 192.168.100.26 TELNET 120 Telnet Data ...
3517 528.784393 192.168.100.27 192.168.100.26 TELNET 203 Telnet Data ...
4782 531.210094 192.168.100.27 192.168.100.26 TELNET 90 Telnet Data ...
4785 531.406009 192.168.100.27 192.168.100.26 TELNET 684 Telnet Data ...
4790 543.886667 192.168.100.26 192.168.100.27 TELNET 55 Telnet Data ...
Frame 4785: 684 bytes on wire (5472 bits), 684 bytes captured (5472 bits)
Ethernet II, Src: Vmware_81:09:11 (00:0c:29:81:09:11), Dst: Vmware_94:f2:0d (00:0c:29:94:f2:0d)
Internet Protocol Version 4, Src: 192.168.100.27, Dst: 192.168.100.26
Transmission Control Protocol, Src Port: 23, Dst Port: 1200, Seq: 1442, Ack: 159, Len: 630
Telnet
Data: Host is up (0.00048s latency).\r\n
Data: Not shown: 992 closed ports\r\n
Data: PORT STATE SERVICE\r\n
Data: 21/tcp open ftp\r\n
Data: 80/tcp open http\r\n
Data: 135/tcp open msrpc\r\n
0030 39 08 7d 15 00 00 48 6f 73 74 20 69 73 20 75 70 9·}···Ho st is up
0040 20 28 30 2e 30 30 30 34 38 73 20 6c 61 74 65 6e (0.0004 8s laten
0050 63 79 29 2e 0d 0a 4e 6f 74 20 73 68 6f 77 6e 3a cy)···No t shown:
0060 20 39 39 32 20 63 6c 6f 73 65 64 20 70 6f 72 74 992 clo sed port
0070 73 0d 0a 50 4f 52 54 20 20 20 20 20 53 54 41 54 s··PORT STAT
Telnet (telnet), 630 bytes
Packets: 5236 · Displayed: 459 (8.8%)
Profile: Default
Right Ctrl


id414m21.cs.unb.ca:1 (mrahnama) - TigerVNC
Applications [Mozill... Home [fcs-v... [fcs-v... fcs-vm... 08:59 EN Mohammadali Rahnama
fcs-vm-security-attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Wireshark Thu 08:59
Network-Evidence-02-03.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet
Expression...
No. Time Source Destination Protocol Length Info
4937 585.566784 192.168.100.26 192.168.100.27 TELNET 55 Telnet Data ...
4938 585.574857 192.168.100.27 192.168.100.26 TELNET 55 Telnet Data ...
4940 586.489168 192.168.100.26 192.168.100.27 TELNET 56 Telnet Data ...
4941 586.493834 192.168.100.27 192.168.100.26 TELNET 56 Telnet Data ...
4948 586.764635 192.168.100.27 192.168.100.26 TELNET 138 Telnet Data ...
4952 594.222008 192.168.100.26 192.168.100.27 TELNET 55 Telnet Data ...
Frame 4948: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
Ethernet II, Src: Vmware_81:09:11 (00:0c:29:81:09:11), Dst: Vmware_94:f2:0d (00:0c:29:94:f2:0d)
Internet Protocol Version 4, Src: 192.168.100.27, Dst: 192.168.100.26
Transmission Control Protocol, Src Port: 23, Dst Port: 1200, Seq: 2574, Ack: 217, Len: 84
Telnet
Data: Connected to 192.168.100.5.\r\n
Data: 220 Microsoft FTP Service\r\n
Data: Name (192.168.100.5:vilkp):
0020 64 1a 00 17 04 b0 95 a2 ea 32 4a 30 64 f6 50 18 d····· ·2J0d·P·
0030 39 08 5c 73 00 00 43 6f 6e 6e 65 63 74 65 64 20 9·\s··Co nnected
0040 74 6f 20 31 39 32 2e 31 36 38 2e 31 30 30 2e 35 to 192.1 68.100.5
0050 2e 0d 0a 32 32 30 20 4d 69 63 72 6f 73 6f 66 74 ···220 M icrosoft
0060 20 46 54 50 20 53 65 72 76 69 63 65 0d 0a 4e 61 FTP Ser vice··Na
0070 6d 65 20 28 31 39 32 2e 31 36 38 2e 31 30 30 2e me (192. 168.100.
0080 35 3a 76 69 6c 6b 70 29 3a 20 5:vilkp) :
Data (telnet.data), 27 bytes
Packets: 5236 · Displayed: 459 (8.8%)
Profile: Default
Right Ctrl



6. What is the IP address of the attacker?

192.168.100.26