

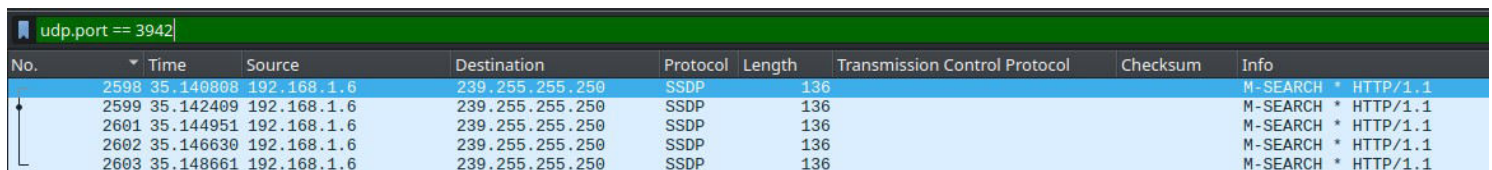
Wireshark Challenge [Activity]

PCAP 1

1. Which protocol was used over port 3942?

Check for the port number using the display filter. Apply the filter 'tcp.port==3942' and check if any packet with the desired port number is displayed. If not then apply the filter 'udp.port==3942' to get the desired packet. No packets will be displayed on the packet list menu for the filter 'tcp.port==3942' but for the filter 'udp.port==3942', the following packets in your packet list menu.

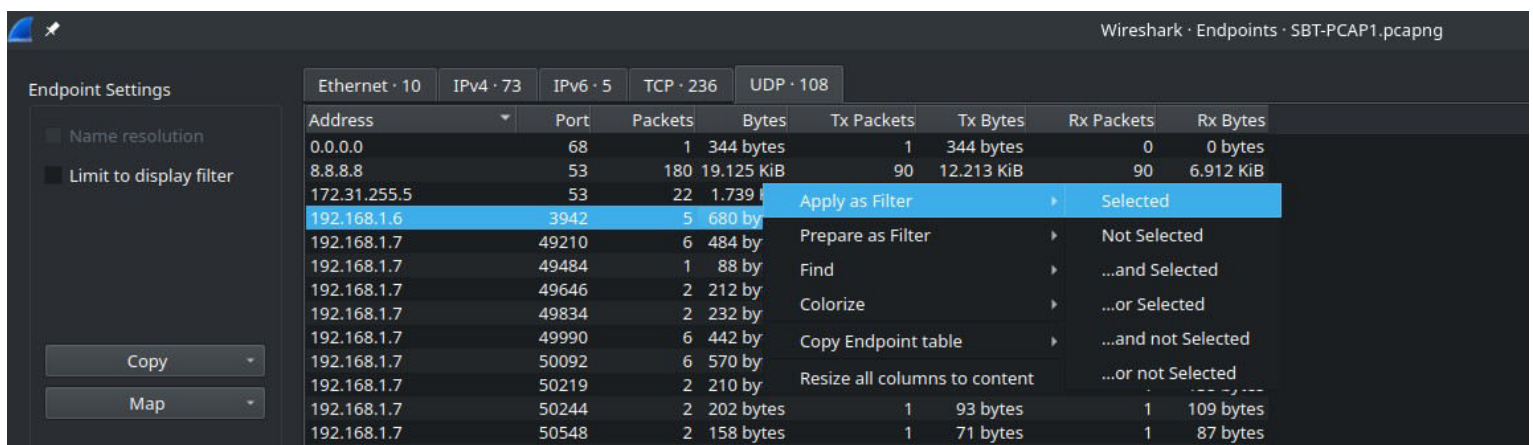
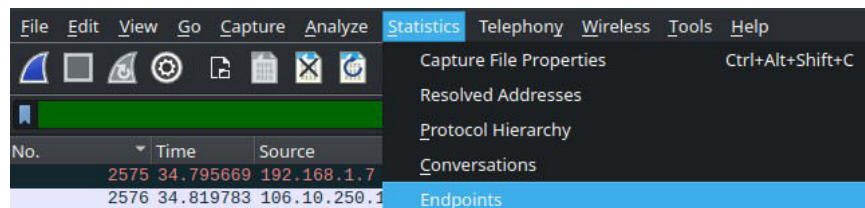
And here we finally go the service which is SSDP running on port 3942.



The image shows a Wireshark packet list with a display filter of 'udp.port == 3942'. The list contains five packets, all of which are SSDP M-SEARCH messages. The source IP is 192.168.1.6 and the destination IP is 239.255.255.250 for all packets. The length of each packet is 136 bytes.

No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Checksum	Info
2598	35.140808	192.168.1.6	239.255.255.250	SSDP	136			M-SEARCH * HTTP/1.1
2599	35.142409	192.168.1.6	239.255.255.250	SSDP	136			M-SEARCH * HTTP/1.1
2601	35.144951	192.168.1.6	239.255.255.250	SSDP	136			M-SEARCH * HTTP/1.1
2602	35.146630	192.168.1.6	239.255.255.250	SSDP	136			M-SEARCH * HTTP/1.1
2603	35.148661	192.168.1.6	239.255.255.250	SSDP	136			M-SEARCH * HTTP/1.1

Another way is that choose endpoints property from the statistics properties. Click the UDP tab, find the packet with port number 3942 and right click on the packet, choose the apply as filter option and then click 'selected' option. After this procedure you will get the above packets in your packet list.



The image shows the 'Endpoints' table in Wireshark. The table lists the source and destination IP addresses and the port number for each endpoint. The port number 3942 is highlighted in blue. The table also shows the number of packets and bytes for each endpoint. The 'Apply as Filter' button is visible next to the highlighted row.

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
0.0.0.0	68	1	344 bytes	1	344 bytes	0	0 bytes
8.8.8.8	53	180	19.125 KiB	90	12.213 KiB	90	6.912 KiB
172.31.255.5	53	22	1.739 KiB				
192.168.1.6	3942	5	680 bytes				
192.168.1.7	49210	6	484 bytes				
192.168.1.7	49484	1	88 bytes				
192.168.1.7	49646	2	212 bytes				
192.168.1.7	49834	2	232 bytes				
192.168.1.7	49990	6	442 bytes				
192.168.1.7	50092	6	570 bytes				
192.168.1.7	50219	2	210 bytes				
192.168.1.7	50244	2	202 bytes	1	93 bytes	1	109 bytes
192.168.1.7	50548	2	158 bytes	1	71 bytes	1	87 bytes

2.What is the IP address of the host that was pinged twice?

Asked to find the IP address that was pinged twice, so try using the display filter here . Search 'ICMP' in the display filter. Tried using ICMP here because ping operates because ping operates by means of Internet Control Message Protocol protocol. Pinging involves sending an ICMP echo request to the target host and waiting for an ICMP echo reply.

192.168.1.7 pinged 8.8.8.8 twice but the destination was unreachable. 192.168.1.7 pinged 8.8.4.4 twice and it was successful. So the final answer will be 8.8.4.4.

icmp									
No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Checksum	Info	
127	4.331987	192.168.1.7	8.8.8.8	ICMP	70			Destination unreachable (Port unreachable)	
128	4.331987	192.168.1.7	8.8.8.8	ICMP	70			Destination unreachable (Port unreachable)	
1632	22.769823	192.168.1.7	8.8.4.4	ICMP	98			Echo (ping) request id=0x4728, seq=0/0, t	
1665	23.353519	8.8.4.4	192.168.1.7	ICMP	98			Echo (ping) reply id=0x4728, seq=0/0, t	
1671	23.774920	192.168.1.7	8.8.4.4	ICMP	98			Echo (ping) request id=0x4728, seq=1/256,	
1708	24.477631	8.8.4.4	192.168.1.7	ICMP	98			Echo (ping) reply id=0x4728, seq=1/256,	

3.How many DNS query response packets were captured?

Search for DNS in the display filter and many packets will be displayed. It will contain standard query packets as well as standard query response packets in the packet list. We want only the DNS query response packets that was captured. Double left click on the info of a standard query response packet and under the flags domain right click and message as response and select the apply as filter property and choose the selected option from drop down menu. Now all standard query response packets will be displayed. Total packets displayed in the packets list window can be seen in bottom right corner. By following the above steps, the number of response packets is. 90.

dns									
No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Checksum	Info	
48	1.549630	192.168.1.7	8.8.8.8	DNS	79			Standard query 0xf7e1 A	
49	1.551206	192.168.1.7	8.8.8.8	DNS	87			Standard query 0xde4e A	
50	1.584401	8.8.8.8	192.168.1.7	DNS	119			Standard query response	
51	1.585019	8.8.8.8	192.168.1.7	DNS	103			Standard query response	

Wireshark · Packet 51 · SBT-PCAP1.pcapng

- Frame 51: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface en0, id 0
- Ethernet II, Src: Netcomm_8f:82:2b (00:60:64:8f:82:2b), Dst: Apple_93:ad:f0 (8c:85:90:93:ad:f0)
- Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.7
- User Datagram Protocol, Src Port: 53, Dst Port: 59263
- Domain Name System (response)
 - Transaction ID: 0xde4e
 - Flags: 0x8180 Standard query response, No error

1... .. = Response: Message

.000 0... .. = Opcode: Standard query

... ..0... .. = Authoritative: Server is not authenticat

... ..0... .. = Truncated: Message is not truncated

... ..1... .. = Recursion desired: Do query

... ..1... .. = Recursion available: Server has recursive queries

... ..0... .. = Z: reserved (0)

... ..0... .. = Answer authenticated by the server

... ..0... .. = Non-authenticated

... ..0000 = Reply code: No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

0000 8c 85 90 93 ad f0 00 60 64 8f 82 2b 08 00

0010 00 59 c0 30 00 00 7a 11 ae a4 08 08 08 00

0020 01 07 00 35 e7 7f 00 45 32 88 de 4e 81 80

0030 00 01 00 00 00 00 0b 61 70 69 2d 67 6c 62 00 00

0040 79 64 05 73 6d 6f 6f 74 05 61 70 70 6c 65 03 63

0050 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00

0060 b8 00 04 11 fc f9 f6

Expand Subtrees

Collapse Subtrees

Expand All

Collapse All

Apply as Filter

Prepare as Filter

Copy

Wiki Protocol Page

Filter Field Reference

Protocol Preferences

Apply as Filter: dns.flags.response == 1

Selected

Not Selected

...and Selected

...or Selected

...and not Selected

...or not Selected

dns.flags.response == 1

No.	Time	Source	Destination	Protocol	Length	Transmission Cor
50	1.584401	8.8.8.8	192.168.1.7	DNS	119	
51	1.585019	8.8.8.8	192.168.1.7	DNS	103	
112	3.623665	8.8.8.8	192.168.1.7	DNS	161	
113	3.623669	8.8.8.8	192.168.1.7	DNS	90	
124	4.331934	8.8.8.8	192.168.1.7	DNS	90	
126	4.331938	8.8.8.8	192.168.1.7	DNS	161	
402	7.800223	8.8.8.8	192.168.1.7	DNS	184	
445	8.004306	8.8.8.8	192.168.1.7	DNS	136	
501	8.413789	8.8.8.8	192.168.1.7	DNS	91	
529	8.623308	8.8.8.8	192.168.1.7	DNS	139	
568	9.102607	8.8.8.8	192.168.1.7	DNS	128	
643	10.471314	8.8.8.8	192.168.1.7	DNS	171	

Frame 51: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface en0, id 0

Ethernet II, Src: Netcomm_8f:82:2b (00:60:64:8f:82:2b), Dst: Apple_93:ad:f0 (8c:85:90:93:ad:f0)

Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.7

User Datagram Protocol, Src Port: 53, Dst Port: 59263

Domain Name System (response)

Transaction ID: 0xde4e

Flags: 0x8180 Standard query response, No error

1... .. = Response: Message is a response

.000 0... .. = Opcode: Standard query (0)

... ..0... .. = Authoritative: Server is not authenticat

... ..0... .. = Truncated: Message is not truncated

... ..1... .. = Recursion desired: Do query

... ..1... .. = Recursion available: Server has recursive queries

... ..0... .. = Z: reserved (0)

0000 8c 85 90 93 ad f0 00 60 64 8f 82 2b 08 00

0010 00 59 c0 30 00 00 7a 11 ae a4 08 08 08 00

0020 01 07 00 35 e7 7f 00 45 32 88 de 4e 81 80

0030 00 01 00 00 00 00 0b 61 70 69 2d 67 6c 62 00 00

0040 79 64 05 73 6d 6f 6f 74 05 61 70 70 6c 65 03 63

0050 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00

0060 b8 00 04 11 fc f9 f6

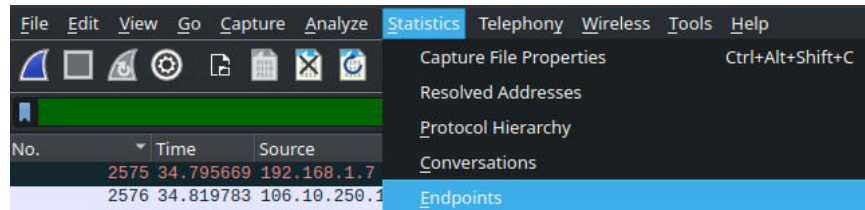
Is the message a response? (dns.flags.response), 2 bytes

Packets: 9515 · Displayed: 90 (0.9%)

Profile: Default

4.What is the IP address of the host which sent the most number of bytes?

Select the statistics tab from main menu and choose end point property of the statistics tab. Select IPV4 address tab from the pop up window (I chose IPV4 since the format is of a IPV4 address). Double click on the Txbytes column header to sort it in descending order and the first ip address displayed will be the answer. By following the above procedure we get 115.178.9.18.

A screenshot of the Wireshark 'Endpoints' window. The window title is 'Wireshark - Endpoints - SBT-PCAP1.pcapng'. It shows a table of endpoints sorted by 'Tx Bytes' in descending order. The table has columns for Address, Packets, Bytes, Tx Packets, Tx Bytes, Rx Packets, Rx Bytes, Country, City, AS Number, and AS Organization. The first entry is 115.178.9.18 with 2,993 packets and 1.883 MiB of data. Other entries include 192.168.1.7, 216.58.199.68, 104.16.142.228, 104.95.133.46, 106.10.250.10, 216.58.196.131, 172.217.25.162, 104.16.143.228, 216.58.203.104, 17.252.249.246, 216.58.199.78, and 216.58.196.142.

Endpoint Settings										
Ethernet · 10 IPv4 · 73 IPv6 · 5 TCP · 236 UDP · 108										
Limit to display filter										
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
115.178.9.18	2,993	1.883 MiB	1,409	1.685 MiB	1,584	202.345 KiB	Australia	Sydney		
192.168.1.7	9,455	4.739 MiB	5,043	714.535 KiB	4,412	4.042 MiB				
216.58.199.68	727	436.187 KiB	356	376.429 KiB	371	59.758 KiB	United States	Mountain View		
104.16.142.228	614	356.377 KiB	295	319.772 KiB	319	36.604 KiB	United States			
104.95.133.46	419	280.704 KiB	196	260.797 KiB	223	19.907 KiB	United States			
106.10.250.10	371	226.123 KiB	186	203.563 KiB	185	22.560 KiB	Singapore			
216.58.196.131	300	168.012 KiB	139	150.546 KiB	161	17.466 KiB	United States	Mountain View		
172.217.25.162	379	160.686 KiB	179	132.569 KiB	200	28.116 KiB	United States			
104.16.143.228	201	131.394 KiB	91	121.755 KiB	110	9.639 KiB	United States			
216.58.203.104	172	109.976 KiB	77	100.531 KiB	95	9.444 KiB	United States	Mountain View		
17.252.249.246	427	152.433 KiB	184	87.882 KiB	243	64.551 KiB	United States			
216.58.199.78	554	114.905 KiB	244	84.150 KiB	310	30.755 KiB	United States	Mountain View		
216.58.196.142	167	81.465 KiB	77	68.538 KiB	90	12.927 KiB	United States	Mountain View		

PCAP 2

1.What is the WebAdmin password?

To get the password, so start with searching http in the display filter. Four packets will be displayed in the packet display window. Read through the the info column of all the packets. There is a packet with get request for password.txt file. Then analyze the get request from the client and response from the server in human readable format. Now right click on the packet and select follow property and click tcp stream option to get the human readable format the conversation.

By following the above procedure we will the web admin password as sbt123.

The image shows the Wireshark network protocol analyzer interface. The top section displays a list of captured packets filtered by 'http'. The bottom section shows the details of a selected packet (No. 4121) with the 'Follow' option selected, displaying the TCP stream data.

No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Checksum	Info
4100	14.300943	192.168.56.1	192.168.56.111	HTTP	154	✓	0x38a4	GET /index.html HTTP/1.1
4111	14.301688	192.168.56.111	192.168.56.1	HTTP	974	✓	0xd95e	HTTP/1.1 200 OK (text/html)
4121	33.097733	192.168.56.1	192.168.56.111	HTTP	156	✓	0x9ef4	GET /password.txt HTTP/1.1
4123	33.098392	192.168.56.111	192.168.56.1	HTTP	320	✓	0xda93	HTTP/1.1 200 OK (text/plain)

Offset	Hex	ASCII
0x9ef4	GET /password.txt HTTP/1.1	
0xda93	HTTP/1.1 200 OK (text/plain)	

Offset	Hex	ASCII
0x0000	10 15 9e f4 00 00 01 01 08 0a 22 a9 89 b...	
0x0010	a3 af 47 45 54 20 2f 70 61 73 73 77 6f 7...	
0x0020	74 78 74 20 48 54 54 50 2f 31 2e 31 0d 0...	
0x0030	73 74 3a 20 31 39 32 2e 31 36 38 2e 35 3...	
0x0040	31 31 0d 0a 55 73 65 72 2d 41 67 65 6e 7...	
0x0050	63 75 72 6c 2f 37 2e 35 34 2e 30 0d 0a 41 63 63	
0x0060	65 70 74 3a 20 2a 2f 2a 0d 0a 0d 0a	

Stream	Offset	Hex	ASCII
TCP Stream	0	0x9ef4	GET /password.txt HTTP/1.1
TCP Stream	1	0xda93	HTTP/1.1 200 OK (text/plain)

```
Wireshark · Follow TCP Stream (tcp.stream eq 2074) · SBT-PCAP2.pcapng

GET /password.txt HTTP/1.1
Host: 192.168.56.111
User-Agent: curl/7.54.0
Accept: */*

HTTP/1.1 200 OK
Date: Sun, 09 Feb 2020 00:11:21 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Sat, 08 Feb 2020 23:53:54 GMT
ETag: "1a-59e19380137c2"
Accept-Ranges: bytes
Content-Length: 26
Content-Type: text/plain

WebAdmin Password: sbt123
```

2.What is the version number of the attacker's FTP server?

Search ftp in the display filter and go to the file transfer protocol header in packet header window. There you will find the version of the ftp i.e. 1.5.5.

SBT-PCAP2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

No.	Time	Source	Destination	Protocol	Length	Transmission Cor
4243	186.7329...	192.168.56.1	192.168.56.103	FTP	82	✓
4244	186.7352...	192.168.56.103	192.168.56.1	FTP	70	✓
4246	186.7356...	192.168.56.1	192.168.56.103	FTP	87	✓
4247	186.7358...	192.168.56.103	192.168.56.1	FTP	74	✓
4249	186.7361...	192.168.56.1	192.168.56.103	FTP	77	✓
4255	192.2152...	192.168.56.103	192.168.56.1	FTP	62	✓
4257	192.2155...	192.168.56.1	192.168.56.103	FTP	80	✓
4263	195.2729...	192.168.56.103	192.168.56.1	FTP	82	✓
4268	195.2802...	192.168.56.1	192.168.56.103	FTP	95	✓
4269	195.2811...	192.168.56.103	192.168.56.1	FTP	72	✓
4271	195.2828...	192.168.56.1	192.168.56.103	FTP	108	✓

Frame 4243: 82 bytes on wire (656 bits), 82 bytes captured on interface (656 bits) on 0a:00:27:00:00:00 (0a:00:27:00:00:00), Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.103, Transmission Control Protocol, Src Port: 21, Dst Port: 4243, File Transfer Protocol (FTP)

220 pyftplib 1.5.5 ready.\r\n

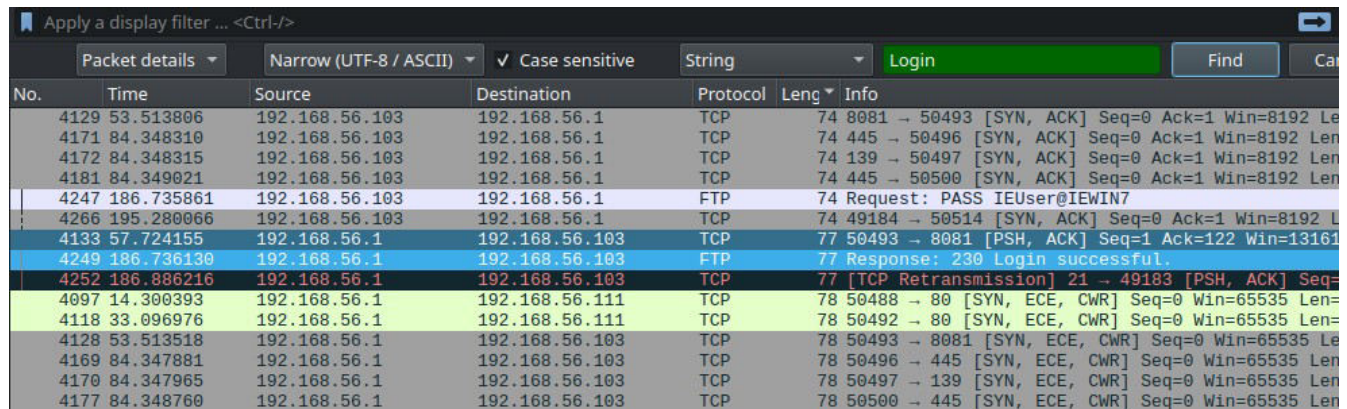
Response code: Service ready for new user (220)

Response arg: pyftplib 1.5.5 ready.

[Current working directory:]

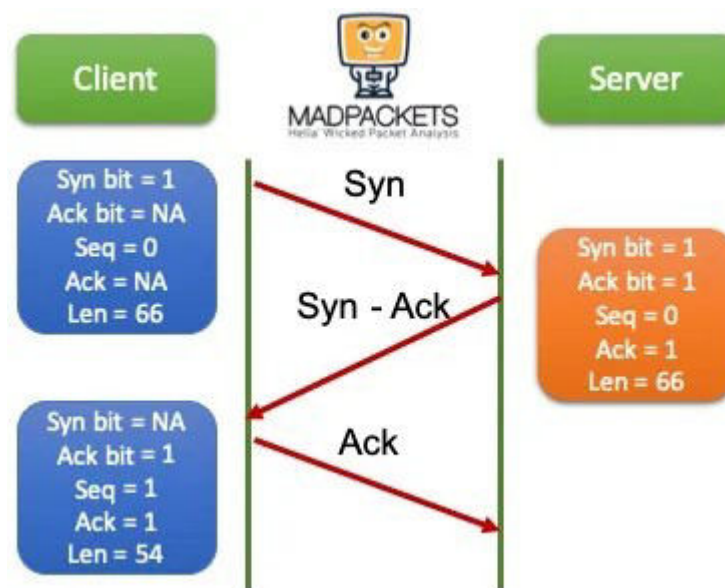
3. Which port was used to gain access to the victim Windows host?

Click the edit tab in top menu bar and choose find the packet option. Search for login in string mode.(If the hacker entered the network then he should have logged in successfully so searched login). See ACK packet before the login successful packet. Then found the port number 8081.



No.	Time	Source	Destination	Protocol	Leng	Info
4129	53.513806	192.168.56.103	192.168.56.1	TCP	74	8081 → 50493 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
4171	84.348310	192.168.56.103	192.168.56.1	TCP	74	445 → 50496 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
4172	84.348315	192.168.56.103	192.168.56.1	TCP	74	139 → 50497 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
4181	84.349021	192.168.56.103	192.168.56.1	TCP	74	445 → 50500 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
4247	186.735861	192.168.56.103	192.168.56.1	FTP	74	Request: PASS IEUser@IEWIN7
4266	195.280066	192.168.56.103	192.168.56.1	TCP	74	49184 → 50514 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
4133	57.724155	192.168.56.1	192.168.56.103	TCP	77	50493 → 8081 [PSH, ACK] Seq=1 Ack=122 Win=13161 Len=0
4249	186.736130	192.168.56.1	192.168.56.103	FTP	77	Response: 230 Login successful.
4252	186.886216	192.168.56.1	192.168.56.103	TCP	77	[TCP Retransmission] 21 → 49183 [PSH, ACK] Seq=1 Ack=122 Win=13161 Len=0
4097	14.300393	192.168.56.1	192.168.56.111	TCP	78	50488 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0
4118	33.096976	192.168.56.1	192.168.56.111	TCP	78	50492 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0
4128	53.513518	192.168.56.1	192.168.56.103	TCP	78	50493 → 8081 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0
4169	84.347881	192.168.56.1	192.168.56.103	TCP	78	50496 → 445 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0
4170	84.347965	192.168.56.1	192.168.56.103	TCP	78	50497 → 139 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0
4177	84.348760	192.168.56.1	192.168.56.103	TCP	78	50500 → 445 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0

Note: To get a clear understanding of this question. Learn how the tcp protocol/three way handshake works.



4.What is the name of a confidential file on the Windows host?

Check out the packet with the port 8081 immediately above the login successful packet. Click the follow option and tcp stream. The pop-up window will display the name of the file. That is Employee_Information_CONFIDENTIAL.txt

09/16/2019	05:22 PM	0	.lock
08/22/2019	04:59 AM	30,000	B0F.m3u
04/20/1997	03:43 PM	9,728	CODBCLog.dll
12/04/1995	02:08 PM	27,136	Ctl3d32.dll.nt
01/31/1996	01:28 PM	26,624	Ctl3d32.dll.Win95
08/20/2019	01:40 AM	1,041	Easy RM to MP3 Converter.lnk
08/22/2019	04:59 AM	107	EasyRM.py
02/08/2020	03:44 PM	379	Employee_Information_CONFIDENTIAL.txt
01/02/2018	05:21 PM	830	eula.lnk
09/16/2019	06:28 PM	2,247	faq.html

5.What is the name of the log file that was created at 4:51 AM on the Windows host?

In the previous window itself, the name was displayed. The file name is LogFile.log

07/16/2019	04:51 AM	585	LogFile.log
------------	----------	-----	-------------