Wireshark

WCNA

Wireshark Certified Network Analyst

Question: 63

How many handshakes are involved while establishing a TCP connection?
A. 5
B. 3
C. 1
D. 6

Answer: B

Question: 64

What is the default protocol used by linux traceroute program?
A. ICMP
B. HTTP
C. IP
D. None of the above

Answer: D

Question: 65

SSH is layer 4 Protocol
A. True
B. False

Answer: B

Question: 66

HTTPS is a layer —— Protocol?
A. 3
B. 5
C. 7
D. 6

Answer: C

Question: 67

Which function in Wireshark provides the summary of IPv4 and IPv6 packets?
A. Analyze
B. Capture
C. Telephony
D. Statistics

Answer: D

Question: 68

Choose a display filter expression for the packets displayed in the below image

Source	Destination	Protocol	Length	Info
192.168.0.106	46.19.210.27	SIP/SDP	336	Request: INVITE
192.168.0.106	46.19.210.27	SIP/SDP	336	Request: INVITE
192.168.0.106	46.19.210.27	SIP/SDP	1166	Request: INVITE
192.168.0.106	46.19.210.27	SIP/SDP	1429	Request: INVITE

A. sip.method == "ACK"
B. sip.method == invite
C. sip.Method == "INVITE"
D. sip ==INVITE

Answer: C

Question: 69

What's the terminal based Wireshark called?
A. Webshark
B. Terminalshark
C. Dshark
D. Tshark

Answer: D

Question: 70

What is the destination MAC address in below image:

```
> Frame 69369: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
v Ethernet II, Src: PcsCompu_0b:17:ba (08:00:27:0b:17:ba), Dst: IPv6mcast_16 (33:33:00:00:00:16)
  > Destination: IPv6mcast_16 (33:33:00:00:00:16)
  > Source: PcsCompu_0b:17:ba (08:00:27:0b:17:ba)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: fe80::3831:dca3:3317:c4f7, Dst: ff02::16
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 96
    Next Header: IPv6 Hop-by-Hop Option (0)
    Hop Limit: 1
    Source: fe80::3831:dca3:3317:c4f7
    Destination: ff02::16
```

A. ff02::16
B. 08:00:27:0b:17:ba
C. 33:33:00:00:00:16
D. Fe80::3831:dca3:3317:c4f7

Answer: C

Question: 71

What is the significance of || operator in a display filter expression in Wireshark?
A. And
B. Not
C. or
D. Equal to

Answer: C

Question: 72

Specify the count of Bytes for an unknown protocol from the below image.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
v Frame	100.0	128	100.0	15495	768	0	0	0
v Ethernet	100.0	128	11.6	1792	88	0	0	0
v Internet Protocol Version 4	64.8	83	10.7	1660	82	0	0	0
v User Datagram Protocol	7.0	9	0.5	72	3	5	40	1
v NetBIOS Datagram Service	0.8	1	1.3	201	9	0	0	0
v SMB (Server Message Block Protocol)	0.8	1	0.8	119	5	0	0	0
v SMB MailSlot Protocol	0.8	1	0.2	25	1	0	0	0
v Microsoft Windows Browser Protocol	0.8	1	0.2	33	1	0	0	0
TRANSUM RTE Data	0.8	1	1.6	243	12	1	243	12
Dynamic Host Configuration Protocol	0.8	1	2.0	304	15	1	304	15
v Domain Name System	1.6	2	0.8	121	5	1	91	4
TRANSUM RTE Data	0.8	1	0.5	72	3	1	72	3
v Transmission Control Protocol	57.8	74	63.7	9867	489	42	2360	116
TRANSUM RTE Data	2.3	3	1.3	199	9	3	199	9
v Transport Layer Security	21.1	27	61.4	9514	471	18	4835	239
TRANSUM RTE Data	6.3	8	12.8	1981	98	8	1981	98
Data	3.1	4	0.0	4	0	3	3	0
Address Resolution Protocol	35.2	45	8.2	1278	63	45	1278	63

A. 201
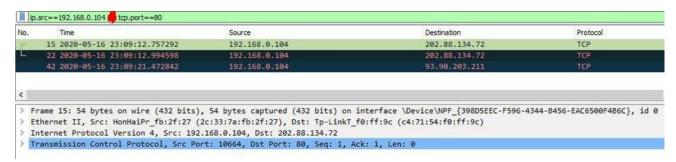B. 304

C. 4
D. 15495

Answer: C

Question: 73

Wireshark can decode NetFlow Packets
A. True
B. False

Answer: A

Question: 74

There is a filter expression for displaying packets having IP address 192.168.0.104 with TCP Port 80, find the masked/hidden operator for applied filter expression in below image:-

A. or
B. and
C. &&
D. ==

Answer: C

Question: 75

If the Client initiates the Data connection, the FTP connection is
A. Active
B. Passive
C. Can be Active or Passive
D. None of the above

Answer: B

Question: 76

Which of the following is not a type of HTTP response codes?
A. 1xx Informational
B. 5xx Server Error
C. 6xx User Error
D. 3xx Redirection

Answer: C

Question: 77

What is the transport layer protocol and port used by Telnet?
A. TCP 100
B. UDP 23
C. UDP 25
D. TCP 23

Answer: D

Question: 78

This is a key parameter for TraceRoute, Identify this parameter.
A. DSCP
B. TTL
C. Flags
D. None of the above

Answer: B

Question: 79

What is the purpose of DHCP Protocol?
A. To send error messages and operational information indicating success or failure when communicating with another IP address.
B. Dynamic assignment of an IP address and other network configuration parameters.
C. Transfer of computer files between a client and server on a computer network.
D. Clock synchronization between computer systems over packet-switched, variable-latency data networks.

Answer: B

Question: 80

What should be the correct capture filter for 'non HTTPS & non POP3 traffic' to/from www.google.com?
A. not https && not pop3 and www.google.com
B. not https and not pop3 and www.google.com
C. not port 443 and not port 25 and host www.google.com
D. not port 443 and not port 110 and host www.google.com

Answer: C

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.

Exam Dumps: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.

Practice Tests: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.

Updated Content: Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.

Technical Support: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.