412-79V10$^{\text{Q\&As}}$

EC-Council Certified Security Analyst (ECSA) V10

Pass EC-COUNCIL 412-79V10 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/412-79v10.html

100% Passing Guarantee
100% Money Back Assurance

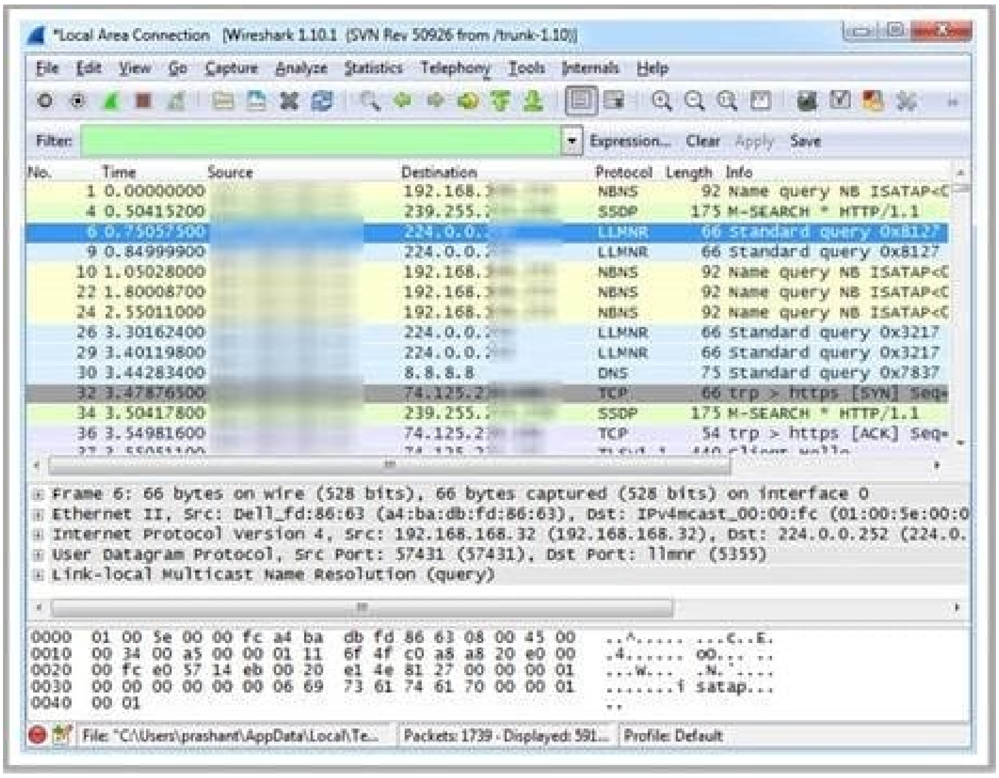
Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

Which Wireshark filter displays all the packets where the IP address of the source host is 10.0.0.7?



```
No.   Time        Source      Destination          Protocol Length Info
    1 0.00000000  [redacted]  192.168.[redacted]   NBNS        92 Name query NB ISATAP<C
    4 0.50415200  [redacted]  239.255.[redacted]   SSDP       175 M-SEARCH * HTTP/1.1
    6 0.75057500  [redacted]  224.0.0.[redacted]   LLMNR       66 Standard query 0x8127
    9 0.84999900  [redacted]  224.0.0.[redacted]   LLMNR       66 Standard query 0x8127
   10 1.05028000  [redacted]  192.168.[redacted]   NBNS        92 Name query NB ISATAP<C
   22 1.80008700  [redacted]  192.168.[redacted]   NBNS        92 Name query NB ISATAP<C
   24 2.55011000  [redacted]  192.168.[redacted]   NBNS        92 Name query NB ISATAP<C
   26 3.30162400  [redacted]  224.0.0.[redacted]   LLMNR       66 Standard query 0x3217
   29 3.40119800  [redacted]  224.0.0.[redacted]   LLMNR       66 Standard query 0x3217
   30 3.44283400  [redacted]  8.8.8.8              DNS         75 Standard query 0x7837
   32 3.47876500  [redacted]  74.125.2[redacted]   TCP         66 trp > https [SYN] Seq=
   34 3.50417800  [redacted]  239.255.[redacted]   SSDP       175 M-SEARCH * HTTP/1.1
   36 3.54981600  [redacted]  74.125.2[redacted]   TCP         54 trp > https [ACK] Seq=
```

```
⊞ Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: Dell_fd:86:63 (a4:ba:db:fd:86:63), Dst: IPv4mcast_00:00:fc (01:00:5e:00:0
⊞ Internet Protocol Version 4, Src: 192.168.168.32 (192.168.168.32), Dst: 224.0.0.252 (224.0.
⊞ User Datagram Protocol, Src Port: 57431 (57431), Dst Port: llmnr (5355)
⊞ Link-local Multicast Name Resolution (query)
```

```
0000  01 00 5e 00 00 fc a4 ba  db fd 86 63 08 00 45 00   ..^..... ...c..E.
0010  00 34 00 a5 00 00 01 11  6f 4f c0 a8 a8 20 e0 00   .4...... oO... ..
0020  00 fc e0 57 14 eb 00 20  e1 4e 81 27 00 00 00 01   ...W...  .N.'....
0030  00 00 00 00 00 00 06 69  73 61 74 61 70 00 00 01   .......i satap...
0040  00 01                                              ..
```

File: "C:\Users\prashant\AppData\Local\Te... | Packets: 1739 · Displayed: 591... | Profile: Default

A. ip.dst==10.0.0.7

B. ip.port==10.0.0.7

C. ip.src==10.0.0.7

D. ip.dstport==10.0.0.7

Correct Answer: C

QUESTION 2

Which one of the following log analysis tools is a Cisco Router Log Format log analyzer and it parses logs, imports them into a SQL database (or its own built-in database), aggregates them, and generates the dynamically filtered reports, all through a web interface?

A. Event Log Tracker

B. Sawmill

C. Syslog Manager

D. Event Log Explorer

Correct Answer: B

QUESTION 3

How many possible sequence number combinations are there in TCP/IP protocol?

A. 320 billion

B. 32 million

C. 4 billion

D. 1 billion

Correct Answer: C

QUESTION 4

Timing is an element of port-scanning that can catch one unaware. If scans are taking too long to complete or obvious ports are missing from the scan, various time parameters may need to be adjusted. Which one of the following scanned timing options in NMAP\\'s scan is useful across slow WAN links or to hide the scan?

A. Paranoid

B. Sneaky

C. Polite

D. Normal

Correct Answer: C

QUESTION 5

A firewall\\'s decision to forward or reject traffic in network filtering is dependent upon which of the following?

A. Destination address

B. Port numbers

C. Source address

D. Protocol used

Correct Answer: D

Reference: http://www.vicomsoft.com/learning-center/firewalls/ (what does a firewall do)

412-79V10 PDF Dumps 412-79V10 VCE Dumps 412-79V10 Braindumps