examunion

Certified IT Exam Material Authority

Accurate study guides, High passing rate!

We offer free update service for one year!

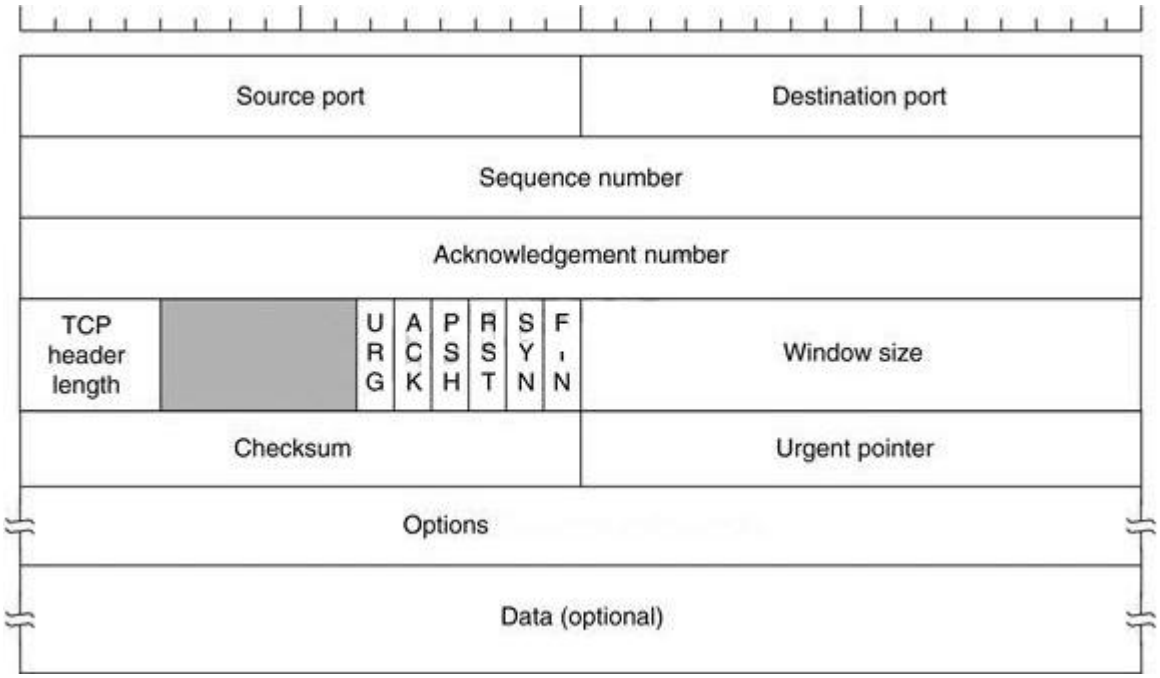
http://www.examunion.com

Exam : ECSAv10

Title : EC-Council Certified Security Analyst

Version : DEMO

1.Transmission control protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment. The TCP header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. It is used to track the state of communication between two TCP endpoints.
For a connection to be established or initialized, the two hosts must synchronize. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of exchange in an acknowledgment (ACK) from the other side
The below diagram shows the TCP Header format:



A. 16 bits
B. 32 bits
C. 8 bits
D. 24 bits
Answer: B

2.Which one of the following tools of trade is a commercial shellcode and payload generator written in Python by Dave Aitel?
A. Microsoft Baseline Security Analyzer (MBSA)
B. CORE Impact
C. Canvas
D. Network Security Analysis Tool (NSAT)
Answer: C

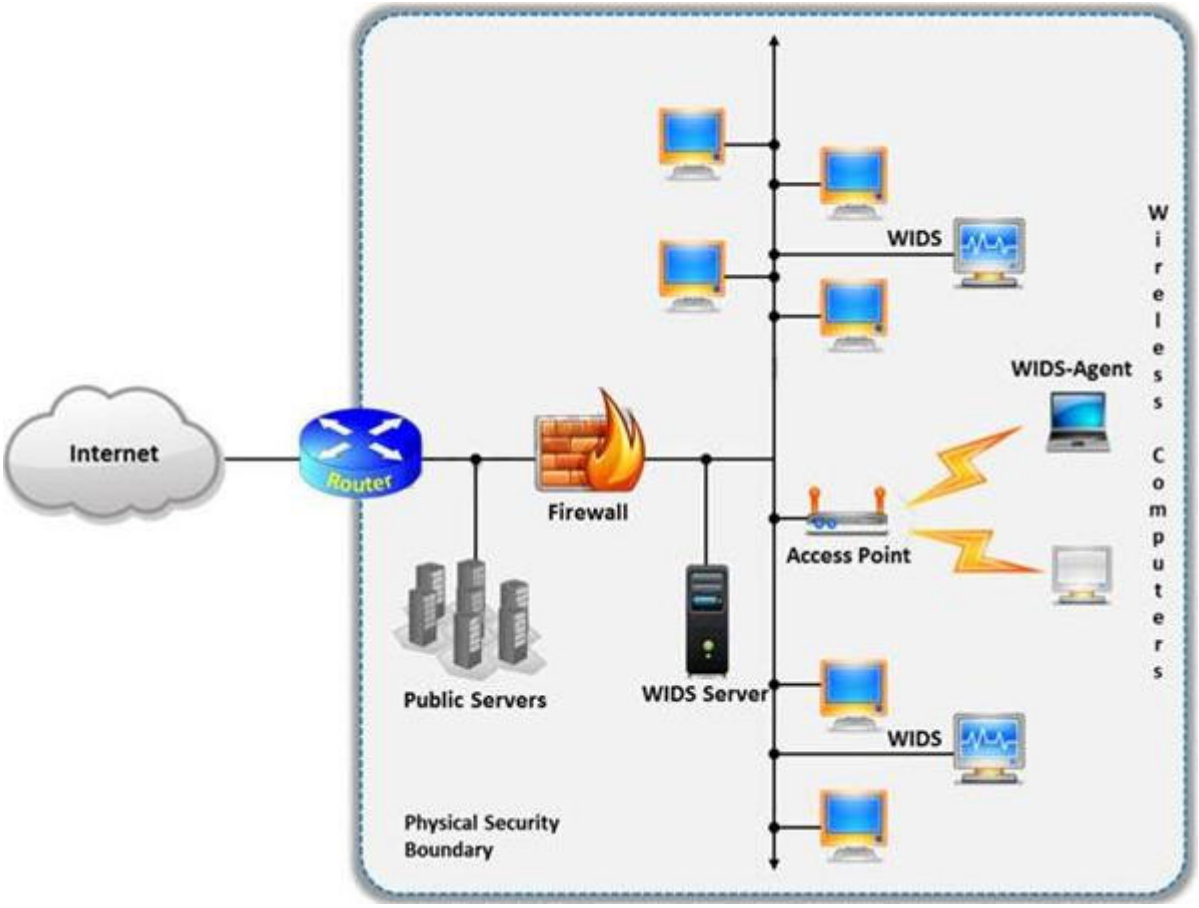
3.A firewall’s decision to forward or reject traffic in network filtering is dependent upon which of the following?
A. Destination address
B. Port numbers
C. Source address

D. Protocol used
Answer: D

4.One of the steps in information gathering is to run searches on a company using complex keywords in Google.

Which search keywords would you use in the Google search engine to find all the PowerPoint presentations containing information about a target company, ROCHESTON?
A. ROCHESTON fileformat:+ppt
B. ROCHESTON ppt:filestring
C. ROCHESTON filetype:ppt
D. ROCHESTON +ppt:filesearch
Answer: C

5.A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools.
The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.
Which of the following attacks can be detected with the help of wireless intrusion detection system (WIDS)?



A. Social engineering
B. SQL injection
C. Parameter tampering
D. Man-in-the-middle attack

Answer: D