Vendor: EC-COUNCIL

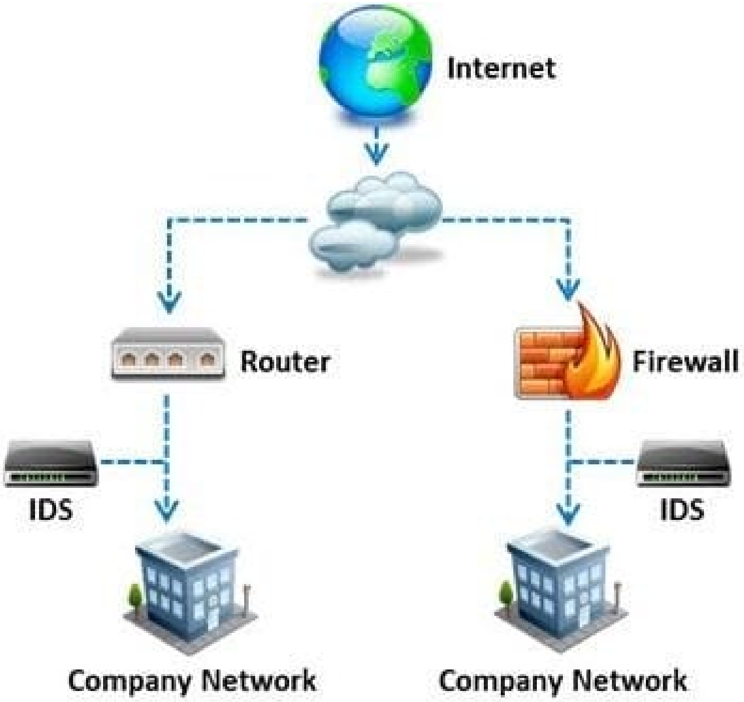
Exam Code: 412-79V10

Exam Name: EC-Council Certified Security Analyst (ECSA) V10

Version: Demo

QUESTION 1

What is a difference between host-based intrusion detection systems (HIDS) and network- based intrusion detection systems (NIDS)?



A. NIDS are usually a more expensive solution to implement compared to HIDS.

B. Attempts to install Trojans or backdoors cannot be monitored by a HIDS whereas NIDS can monitor

and stop such intrusion events.

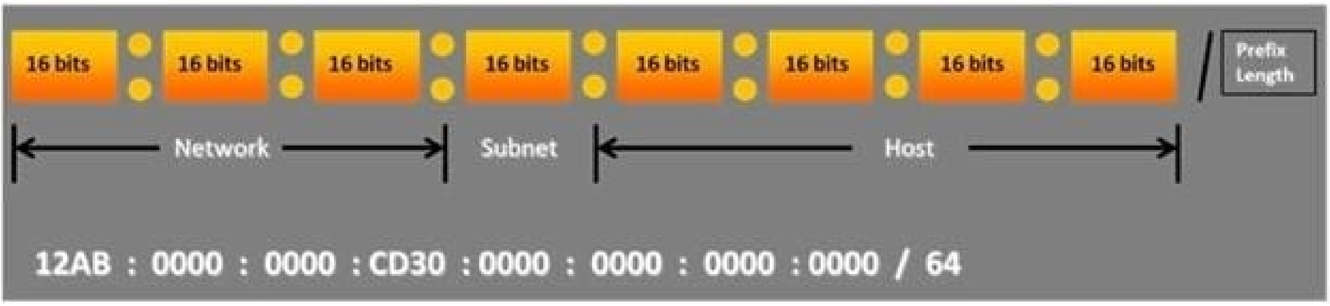
C. NIDS are standalone hardware appliances that include network intrusion detection capabilities whereas HIDS consist of software agents installed on individual computers within the system.

D. HIDS requires less administration and training compared to NIDS.

Correct Answer: C

QUESTION 2

Choose the correct option to define the Prefix Length.



A. Prefix Length = Subnet + Host portions

B. Prefix Length = Network + Host portions

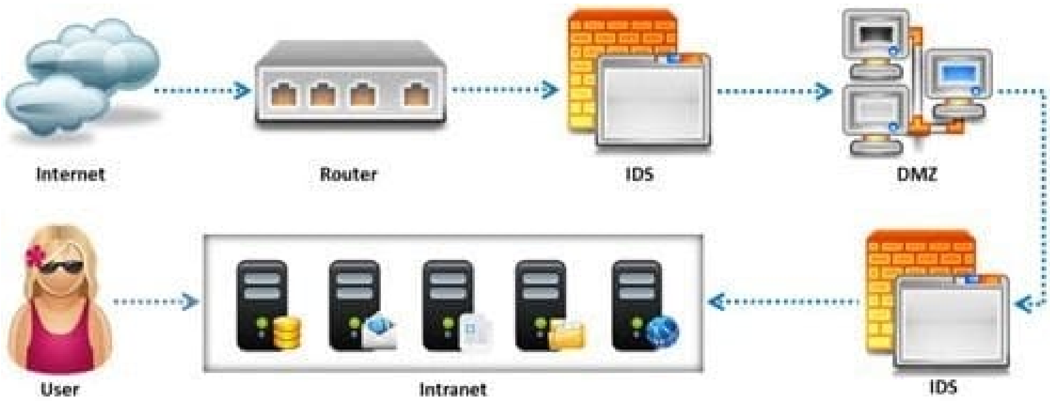
C. Prefix Length = Network + Subnet portions

D. Prefix Length = Network + Subnet + Host portions

Correct Answer: C

QUESTION 3

Due to illegal inputs, various types of TCP stacks respond in a different manner. Some IDSs do not take into account the TCP protocol\\'s urgency feature, which could allow testers to evade the IDS.



Penetration tester needs to try different combinations of TCP flags (e.g. none, SYN/FIN, SYN/RST, SYN/ FIN/ACK, SYN/RST/ACK, and All Flags) to test the IDS.

Which of the following TCP flag combinations combines the problem of initiation, midstream, and termination flags with the PSH and URG?

A. SYN/RST/ACK

B. SYN/FIN/ACK

C. SYN/FIN

D. All Flags

Correct Answer: D

Reference:

http://books.google.com.pk/books?id=tUCumJot0ocCandpg=PA63andlpg=PA63anddq=TCP+flag +combinations

+combines+the+problem+of+initiation,+midstream,+and+termination+flags+ with+the+PSH+and

+URGandsource=blandots=mIGSXBIi15andsig=WMnXlEChVSU4RhK65W_V

3tzNjnsandhl=enandsa=Xandei=H7AfVJCtLaufygO1v4DQDgandved=0CBsQ6AEwAA#v=onepageand q=TCP%

20flag%20combinations%20combines%20the%20problem%20of%20initiation%2 C%20midstream%2C%

20and%20termination%20flags%20with%20the%20PSH%20and% 20URGandf=false (see the highlighted

sentence in Table 3-1 at the end of the page)

QUESTION 4

One needs to run "Scan Server Configuration" tool to allow a remote connection to Nessus from the remote Nessus clients. This tool allows the port and bound interface of the Nessus daemon to be configured. By default, the Nessus daemon listens to connections on which one of the following?

A. Localhost (127.0.0.1) and port 1241

B. Localhost (127.0.0.1) and port 1240

C. Localhost (127.0.0.1) and port 1246

D. Localhost (127.0.0.0) and port 1243

Correct Answer: A

QUESTION 5

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS

B. Active IDS

C. Progressive IDS

D. NIPS

Correct Answer: B

QUESTION 6

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 7

Which of the following defines the details of services to be provided for the client\\'s organization and the list of services required for performing the test in the organization?

A. Draft

B. Report

C. Requirement list

D. Quotation

Correct Answer: D

QUESTION 8

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

Correct Answer: C

Reference: http://blog.hubspot.com/blog/tabid/6307/bid/1264/12-Quick-Tips-To-Search- Google-Like-AnExpert.aspx (specific document types)

QUESTION 9

Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

A. Unannounced Testing

B. Double Blind Testing

C. Announced Testing

D. Blind Testing

Correct Answer: B

QUESTION 10

By default, the TFTP server listens on UDP port 69. Which of the following utility reports the port status of target TCP and UDP ports on a local or a remote computer and is used to troubleshoot TCP/IP connectivity issues?

A. PortQry

B. Netstat

C. Telnet

D. Tracert

Correct Answer: A

Reference: http://support.microsoft.com/kb/832919

QUESTION 11

Which of the following external pen testing tests reveals information on price, usernames and passwords, sessions, URL characters, special instructors, encryption used, and web page behaviors?

A. Check for Directory Consistency and Page Naming Syntax of the Web Pages

B. Examine Server Side Includes (SSI)

C. Examine Hidden Fields

D. Examine E-commerce and Payment Gateways Handled by the Web Server

Correct Answer: C

Reference: http://www.scribd.com/doc/133636402/LPTv4-Module-18-External-Penetration- Testing-NoRestriction (page 71)

QUESTION 12

Which of the following policies helps secure data and protects the privacy of organizational information?

A. Special-Access Policy

B. Document retention Policy

C. Cryptography Policy

D. Personal Security Policy

Correct Answer: C