TestkingPDF

Try before you buy

Download a free sample of any of our exam questions and answers

Download Demo

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

Quality and Value

TestkingPDF Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Easy to Pass

If you prepare for the exams using our TestkingPDF testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Try Before Buy

TestkingPDF offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.testkingpdf.com

Valid test online & stable pass king & latest PDF dumps

Exam : **412-79**

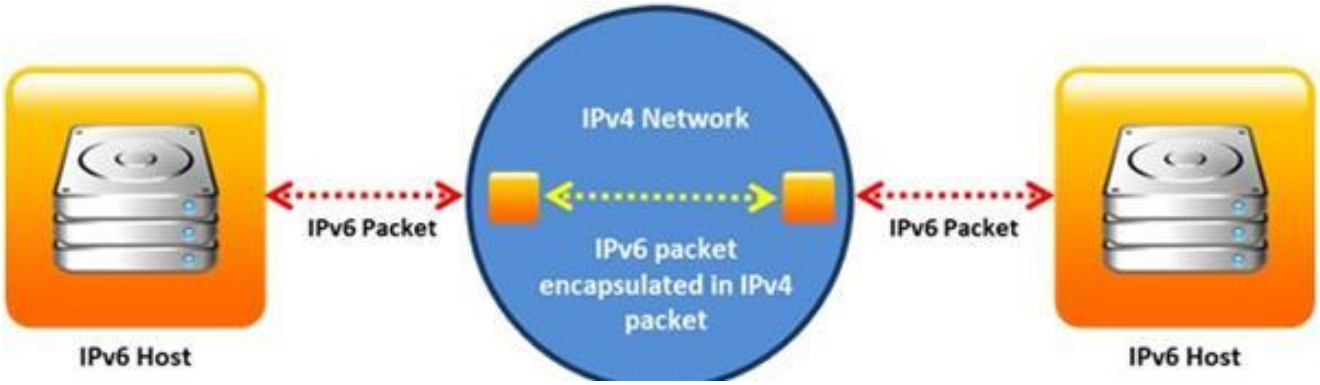
Title : EC-Council Certified Security Analyst (ECSA)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 Which one of the following Snort logger mode commands is associated to run a binary log file through Snort in sniffer mode to dump the packets to the screen?
A. ./snort -dev -l ./log
B. ./snort -dv -r packet.log
C. ./snort -l ./log -b
D. ./snort -dvr packet.log icmp
Answer: B

NO.2 Identify the transition mechanism to deploy IPv6 on the IPv4 network from the following diagram.



A. Tunneling
B. Translation
C. Encapsulation
D. Dual Stacks
Answer: A

NO.3 Variables are used to define parameters for detection, specifically those of your local network and/or specific servers or ports for inclusion or exclusion in rules. These are simple substitution variables set with the var keyword. Which one of the following operator is used to define meta-variables?
A. "*"
B. "$"
C. "?"
D. "#"
Answer: B

NO.4 Which one of the following is a command line tool used for capturing data from the live network and copying those packets to a file?
A. Wireshark: Dumpcap
B. Wireshark: Text2pcap
C. Wireshark: Tcpdump
D. Wireshark: Capinfos
Answer: A

NO.5 You work as an IT security auditor hired by a law firm in Boston. You have been assigned the responsibility to audit the client for security risks. When assessing the risk to the clients network, what step should you take first?

A. Evaluating the existing perimeter and internal security

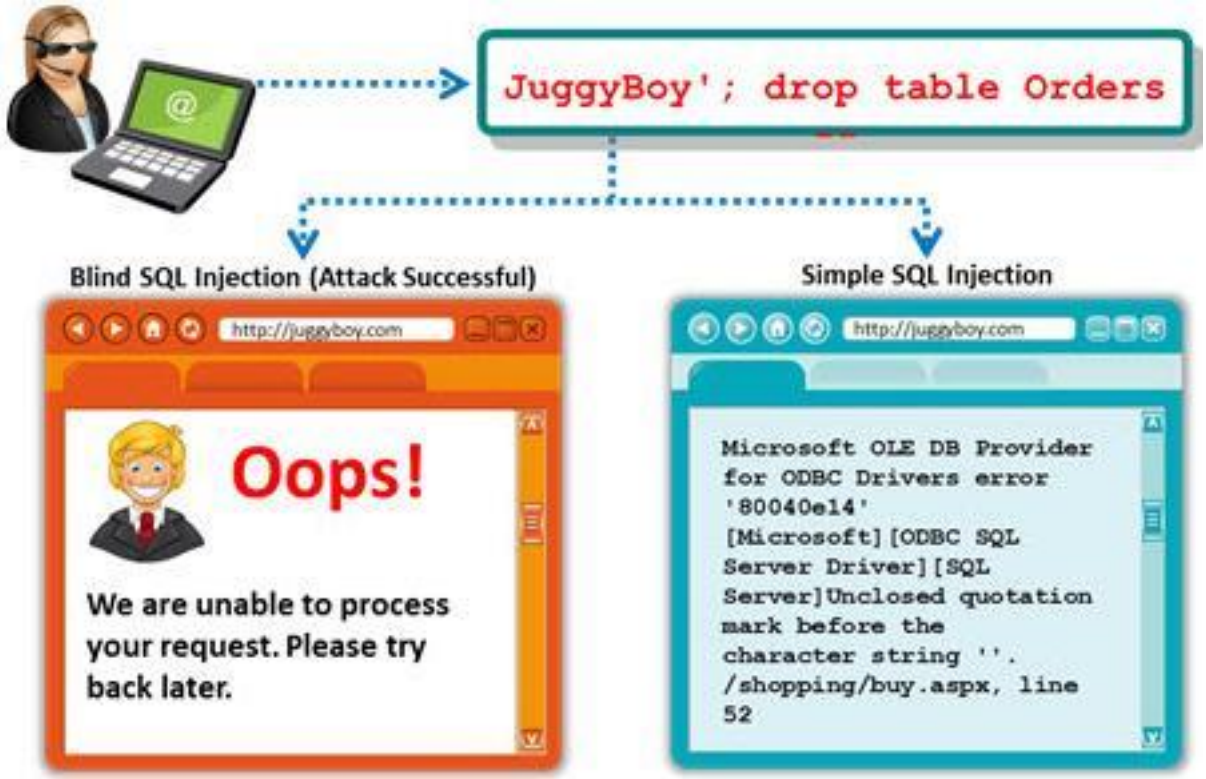
B. Analyzing, categorizing and prioritizing resources

C. Checking for a written security policy

D. Analyzing the use of existing management and control architecture

Answer: C

NO.6 A Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the application response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.



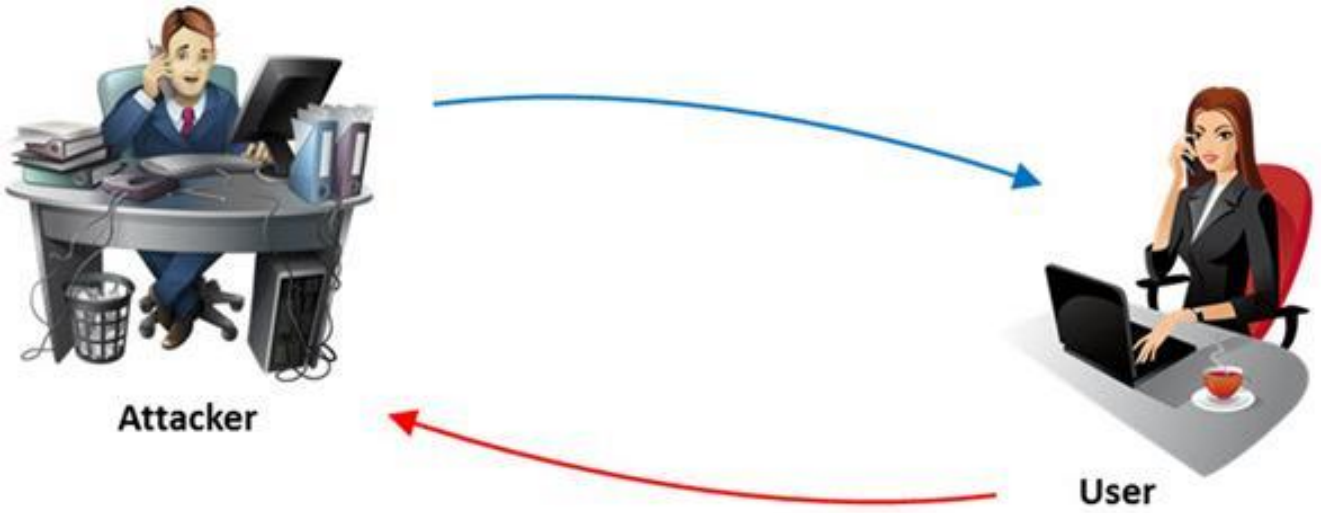
It is performed when an error message is not received from application while trying to exploit SQL vulnerabilities. The developer's specific message is displayed instead of an error message. So it is quite difficult to find SQL vulnerability in such cases.

A pen tester is trying to extract the database name by using a blind SQL injection. He tests the database using the below query and finally finds the database name.

http://juggyboy.com/page.aspx?id=1;
IF (LEN(DB_NAME())=4) WAITFOR DELAY
'00:00:10'--
http://juggyboy.com/page.aspx?id=1;
IF (ASCII(lower(substring((DB_NAME()),1,1)))=97) WAITFOR DELAY
'00:00:10'--
http://juggyboy.com/page.aspx?id=1;
IF (ASCII(lower(substring((DB_NAME()),2,1)))=98) WAITFOR DELAY

'00:00:10'--
http://juggyboy.com/page.aspx?id=1;
IF (ASCII(lower(substring((DB_NAME()),3,1)))=99) WAITFOR DELAY
'00:00:10'--
http://juggyboy.com/page.aspx?id=1;
IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY
'00:00:10'--
What is the database name?
A. WXYZ
B. EFGH
C. ABCD
D. PQRS
Answer: C

NO.7 The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?
A. Spoofing
B. Vishing
C. Phishing
D. Tapping
Answer: B

NO.8 Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?

A. Service-based Assessment Solutions
B. Tree-based Assessment
C. Inference-based Assessment
D. Product-based Assessment Solutions
Answer: B

NO.9 Which of the following has an offset field that specifies the length of the header and data?
A. IP Header
B. UDP Header
C. ICMP Header
D. TCP Header
Answer: D

NO.10 Which of the following will not handle routing protocols properly?
A. "Internet-router-firewall-net architecture"
B. "Internet-firewall -net architecture"
C. "Internet-firewall-router-net architecture"
D. "Internet-firewall/router(edge device)-net architecture"
Answer: C

NO.11 Which of the following information gathering techniques collects information from an organization's web-based calendar and email services?
A. Active Information Gathering

B. Passive Information Gathering
C. Private Information Gathering
D. Anonymous Information Gathering
Answer: A

NO.12 The SnortMain () function begins by associating a set of handlers for the signals, Snort receives. It does this using the signal () function. Which one of the following functions is used as a programspecific signal and the handler for this calls the DropStats() function to output the current Snort statistics?
A. SIGINT
B. SIGHUP
C. SIGUSR1
D. SIGTERM
Answer: C

NO.13 A chipset is a group of integrated circuits that are designed to work together and are usually marketed as a single product." It is generally the motherboard chips or the chips used on the expansion card. Which one of the following is well supported in most wireless applications?
A. Atheros Chipset
B. Prism II chipsets
C. Cisco chipset
D. Orinoco chipsets
Answer: B

NO.14 James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?
A. Smurf
B. Fraggle
C. Trinoo
D. SYN flood
Answer: A

NO.15 Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?
A. 5000-5099
B. 6666-6674
C. 0 - 1023
D. 3001-3100
Answer: C