PassTest

Bessere Qualität , bessere Dienstleistungen!

Q&A

http://www.passtest.de

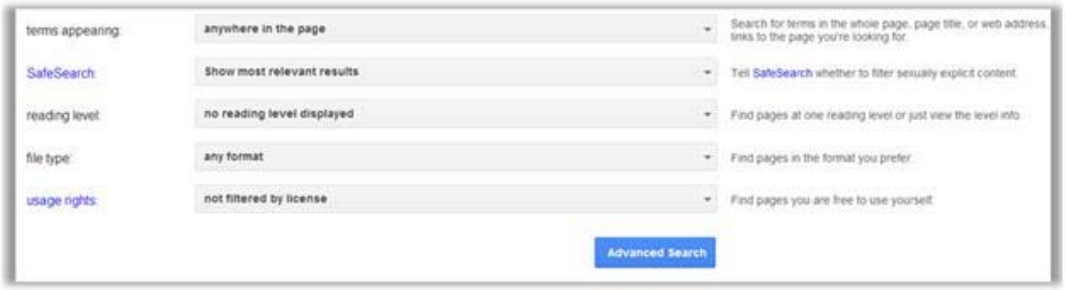
Einjährige kostenlose Aktualisierung

Exam : **ECSAv8**

Title : EC-Council Certified Security Analyst (ECSA)

Version : DEMO

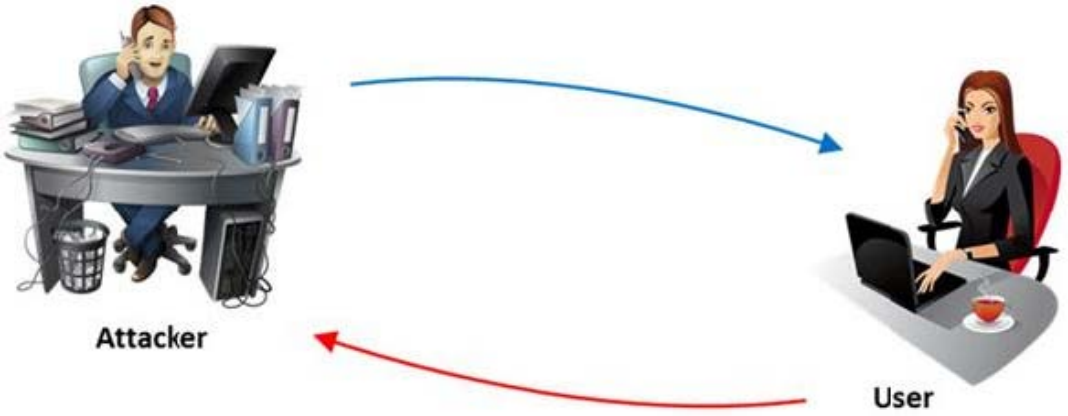
1.One of the steps in information gathering is to run searches on a company using complex keywords in Google.



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

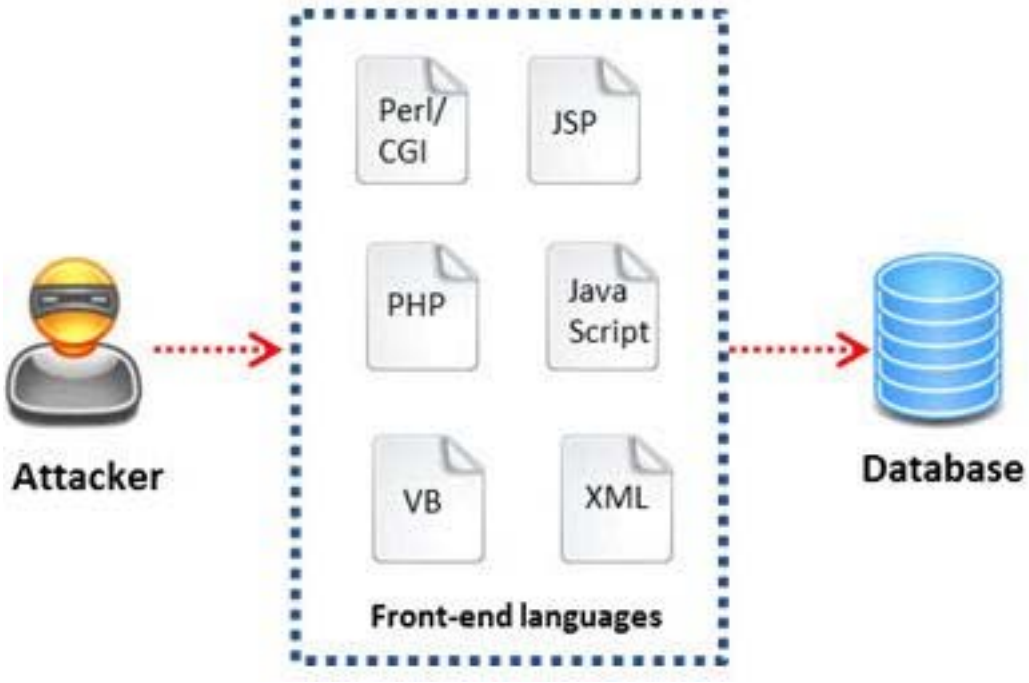
2.What are the scanning techniques that are used to bypass firewall rules and logging mechanisms and disguise themselves as usual network traffic?
A. Connect Scanning Techniques
B. SYN Scanning Techniques
C. Stealth Scanning Techniques
D. Port Scanning Techniques
Answer: C
Explanation: http://wwww.pc-freak.net/tutorials/hacking_info/arkin%20network%20scanning%20techniques.pdf (page 7

3.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. Phishing
B. Spoofing
C. Tapping
D. Vishing
Answer: D

4.A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria. The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a particular table (e.g. StudentTable).
What query does he need to write to retrieve the information?
A. EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000
B. DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1—
C. SELECT * FROM StudentTable WHERE roll_number = '' or '1' = '1‘
D. RETRIVE * FROM StudentTable WHERE roll_number = 1'#
Answer: C

5.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
Answer: A