312-50Q&As

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

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

https://www.pass2lead.com/312-50.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Daryl is a network administrator working for Dayton Technologies. Since Daryl\\'s background is in web application development, many of the programs and applications his company uses are web-based. Daryl sets up a simple forms-based logon screen for all the applications he creates so they are secure.

The problem Daryl is having is that his users are forgetting their passwords quite often and sometimes he does not have the time to get into his applications and change the passwords for them. Daryl wants a tool or program that can monitor web-based passwords and notify him when a password has been changed so he can use that tool whenever a user calls him and he can give them their password right then.

What tool would work best for Daryl\\'s needs?

A. Password sniffer

B. L0phtcrack

C. John the Ripper

D. WinHttrack

Correct Answer: A

L0phtCrack is a password auditing and recovery application (now called LC5), originally produced by Mudge from L0pht Heavy Industries. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords.

John the Ripper is one of the most popular password testing/breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customisable cracker. It can be run against

various encrypted password formats including several crypt password hash types WinHttrack is a offline browser.

A password sniffer would give Daryl the passwords when they are changed as it is a web based authentication over a simple form but still it would be more correct to give the users new passwords instead of keeping a copy of the passwords

in clear text.

QUESTION 2

There are two types of honeypots- high and low interaction. Which of these describes a low interaction honeypot? Select the best answers.

A. Emulators of vulnerable programs

B. More likely to be penetrated

C. Easier to deploy and maintain

D. Tend to be used for production

E. More detectable

F. Tend to be used for research

Correct Answer: ACDE

A low interaction honeypot would have emulators of vulnerable programs, not the real programs. A high interaction honeypot is more likely to be penetrated as it is running the real program and is more vulnerable than an emulator.

Low interaction honeypots are easier to deploy and maintain. Usually you would just use a program that is already available for download and install it. Hackers don\\'t usually crash or destroy these types of programs and it would require little

maintenance. A low interaction honeypot tends to be used for production. Low interaction honeypots are more detectable because you are using emulators of the real programs. Many hackers will see this and realize that they are in a

honeypot. A low interaction honeypot tends to be used for production. A high interaction honeypot tends to be used for research.

QUESTION 3

Leesa is the senior security analyst for a publicly traded company. The IT department recently rolled out an intranet for company use only with information ranging from training, to holiday schedules, to human resources data. Leesa wants to make sure the site is not accessible from outside and she also wants to ensure the site is Sarbanes-Oxley (SOX) compliant. Leesa goes to a public library as she wants to do some Google searching to verify whether the company\\'s intranet is accessible from outside and has been indexed by Google. Leesa wants to search for a website title of "intranet" with part of the URL containing the word "intranet" and the words "human resources" somewhere in the webpage.

What Google search will accomplish this?

A. related:intranet allinurl:intranet:"human resources"

B. cache:"human resources" inurl:intranet(SharePoint)

C. intitle:intranet inurl:intranet+intext:"human resources"

D. site:"human resources"+intext:intranet intitle:intranet

Correct Answer: C

QUESTION 4

Your are trying the scan a machine located at ABC company\\'s LAN named mail.abc.com. Actually that machine located behind the firewall. Which port is used by nmap to send the TCP synchronize frame to on mail.abc.com?

A. 443

B. 80

C. 8080

D. 23

Correct Answer: A

QUESTION 5

Which type of password cracking technique works like dictionary attack but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

A. Dictionary attack

B. Brute forcing attack

C. Hybrid attack

D. Syllable attack

E. Rule-based attack

Correct Answer: C