312-50$^{\text{Q\&As}}$

Ethical Hacker Certified

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

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

https://www.leads4pass.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

Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

A. 69

B. 150

C. 161

D. 169

Correct Answer: C

The SNMP default port is 161. Port 69 is used for tftp, 150 is for SQL-NET and 169 is for SEND.

QUESTION 2

Charlie is an IT security consultant that owns his own business in Denver. Charlie has recently been hired by Fleishman Robotics, a mechanical engineering company also in Denver. After signing service level agreements and other contract papers, Charlie asks to look over the current company security policies. Based on these policies, Charlie compares the policies against what is actually in place to secure the company\\'s network. From this information, Charlie is able to produce a report to give to company executives showing which areas the company is lacking in. This report then becomes the basis for all of Charlie\\'s remaining tests.

What type of initial analysis has Charlie performed to show the company which areas it needs improvements in?

A. Charlie has performed a BREACH analysis; showing the company where its weak points are

B. This analysis would be considered a vulnerability analysis

C. This type of analysis is called GAP analysis

D. This initial analysis performed by Charlie is called an Executive Summary

Correct Answer: C

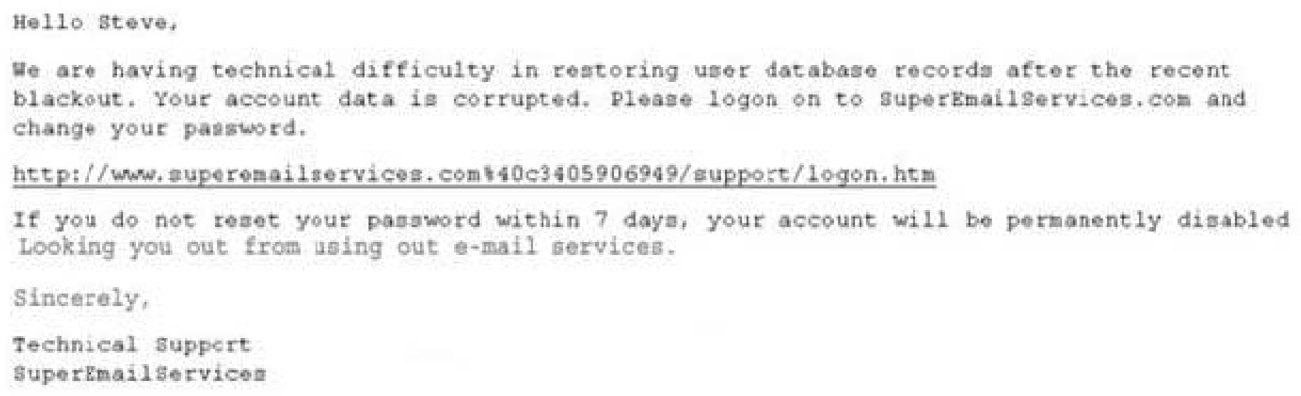
In business and economics, gap analysis is a tool that helps a company to compare its actual performance with its potential performance.

At its core are two questions: "Where are we?" and "Where do we want to be?".

http://en.wikipedia.org/wiki/Gap_analysis

QUESTION 3

Exhibit



Hello Steve,

We are having technical difficulty in restoring user database records after the recent blackout. Your account data is corrupted. Please logon on to SuperEmailServices.com and change your password.

http://www.superemailservices.com%40c3405906949/support/logon.htm

If you do not reset your password within 7 days, your account will be permanently disabled Looking you out from using out e-mail services.

Sincerely,

Technical Support
SuperEmailServices

You receive an e-mail with the message displayed in the exhibit. From this e-mail you suspect that this message was sent by some hacker since you have using their e- mail services for the last 2 years and they never sent out an e-mail as

this. You also observe the URL in the message and confirm your suspicion about 340590649. You immediately enter the following at the Windows 2000 command prompt.

ping 340590649

You get a response with a valid IP address. What is the obstructed IP address in the e-mail URL?

A. 192.34.5.9

B. 10.0.3.4

C. 203.2.4.5

D. 199.23.43.4

Correct Answer: C

Convert the number in binary, then start from last 8 bits and convert them to decimal to get the last octet (in this case .5)

QUESTION 4

An Nmap scan shows the following open ports, and nmap also reports that the OS guessing results to match too many signatures hence it cannot reliably be identified:

21 ftp 23 telnet 80 http 443 https

What does this suggest ?

A. This is a Windows Domain Controller

B. The host is not firewalled

C. The host is not a Linux or Solaris system

D. The host is not properly patched

Correct Answer: D

If the answer was A nmap would guess it, it holds the MS signature database, the host not being firewalled makes no difference. The host is not linux or solaris, well it very well could be. The host is not properly patched? That is the closest; nmaps OS detection architecture is based solely off the TCP ISN issued by the operating systems TCP/IP stack, if the stack is modified to show output from randomized ISN\\'s or if your using a program to change the ISN then OS detection will fail. If the TCP/IP IP ID\\'s are modified then os detection could also fail, because the machine would most likely come back as being down.

QUESTION 5

A file integrity program such as Tripwire protects against Trojan horse attacks by:

A. Automatically deleting Trojan horse programs

B. Rejecting packets generated by Trojan horse programs

C. Using programming hooks to inform the kernel of Trojan horse behavior

D. Helping you catch unexpected changes to a system utility file that might indicate it had been replaced by a Trojan horse

Correct Answer: D

Tripwire generates a database of the most common files and directories on your system. Once it is generated, you can then check the current state of your system against the original database and get a report of all the files that have been modified, deleted or added. This comes in handy if you allow other people access to your machine and even if you don\\'t, if someone else does get access, you\\'ll know if they tried to modify files such as /bin/login etc.