312-50V10$^{\text{Q\&As}}$

Certified Ethical Hacker Exam (C|EH v10)

Pass EC-COUNCIL 312-50V10 Exam with 100% Guarantee

QUESTION 1

Let\\'s imagine three companies (A, B and C), all competing in a challenging global environment. Company

A and B are working together in developing a product that will generate a major competitive advantage for

them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing.

With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails

from company B.

How do you prevent DNS spoofing?

A. Install DNS logger and track vulnerable packets

B. Disable DNS timeouts

C. Install DNS Anti-spoofing

D. Disable DNS Zone Transfer

Correct Answer: C

QUESTION 2

During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

A. The tester must capture the WPA2 authentication handshake and then crack it.

B. The tester must use the tool inSSIDer to crack it using the ESSID of the network.

C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.

D. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

Correct Answer: A

QUESTION 3

Which of the following programming languages is most vulnerable to buffer overflow attacks?

A. Perl

B. C++

C. Python

D. Java

Correct Answer: B

QUESTION 4

The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

What is the closest approximate cost of this replacement and recovery operation per year?

A. $146

B. $1320

C. $440

D. $100

Correct Answer: A

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the

single loss expectancy (SLE).

Suppose than an asset is valued at $100,000, and the Exposure Factor (EF) for this asset is 25%. The

single loss expectancy (SLE) then, is 25% * $100,000, or $25,000. In our example the ARO is 33%, and

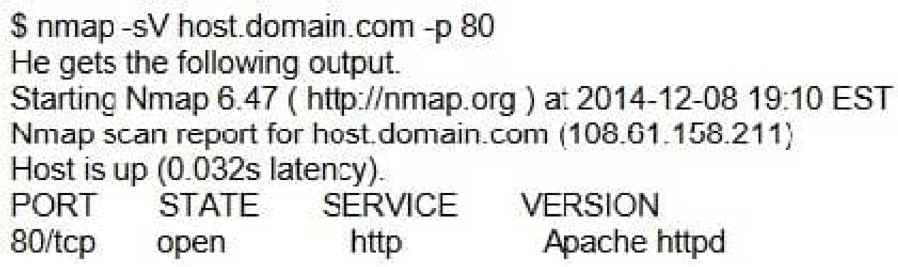
the SLE is 300+14*10 (as EF=1). The ALO is thus:

33%*(300+14*10) which equals 146.

References: https://en.wikipedia.org/wiki/Annualized_loss_expectancy

QUESTION 5

An attacker tries to do banner grabbing on a remote web server and executes the following command.



```
$ nmap -sV host.domain.com -p 80
He gets the following output.
Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-08 19:10 EST
Nmap scan report for host.domain.com (108.61.158.211)
Host is up (0.032s latency).
PORT      STATE      SERVICE      VERSION
80/tcp    open          http          Apache httpd
```

Service detection performed. Please report any incorrect results at http://nmap.org/submit/.

Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds

What did the hacker accomplish?

A. nmap can\\'t retrieve the version number of any running remote service.

B. The hacker successfully completed the banner grabbing.

C. The hacker should\\'ve used nmap -O host.domain.com.

D. The hacker failed to do banner grabbing as he didn\\'t get the version of the Apache web server.

Correct Answer: B