JK0-022$^{\text{Q\&As}}$

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

Company XYZ has encountered an increased amount of buffer overflow attacks. The programmer has been tasked to identify the issue and report any findings. Which of the following is the FIRST step of action recommended in this scenario?

A. Baseline Reporting

B. Capability Maturity Model

C. Code Review

D. Quality Assurance and Testing

Correct Answer: C

QUESTION 2

A hacker has discovered a simple way to disrupt business for the day in a small company which relies on staff working remotely. In a matter of minutes the hacker was able to deny remotely working staff access to company systems with a script. Which of the following security controls is the hacker exploiting?

A. DoS

B. Account lockout

C. Password recovery

D. Password complexity

Correct Answer: B

B: Account lockout automatically disables an account due to repeated failed log on attempts. The hacker must have executed a script to repeatedly try logging on to the remote accounts, forcing the account lockout policy to activate.

Incorrect Answers:

A: Denial of service (DoS) is a form of attack whose principal objective is preventing the victimized system from performing valid actions or responding to valid traffic.

C: The users did not forget their passwords, they were locked out. Furthermore, most times users would be required to change their passwords instead of recovering them as it is not a secure solution.

D: since the hacker did not gain access to the system, password complexity would not be exploited as it forms part of the company\\'s password policy.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 2913- 293.

QUESTION 3

One of the servers on the network stops responding due to lack of available memory. Server administrators did not have a clear definition of what action should have taken place based on the available memory. Which of the following would have BEST kept this incident from occurring?

A. Set up a protocol analyzer

B. Set up a performance baseline

C. Review the systems monitor on a monthly basis

D. Review the performance monitor on a monthly basis

Correct Answer: B

A performance baseline provides the input needed to design, implement, and support a secure network. The performance baseline would define the actions that should be performed on a server that is running low on memory.

Incorrect Answers:

A: A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. It is not used to provide guidance on the actions that should be performed on a server that is running low on memory. Therefore, this answer is incorrect.

C: Reviewing the systems monitor on a monthly basis may help to determine that the server is running low on memory. However, the server could run out of memory in between reviews. The system monitor also does not provide guidance on the actions that should be performed on a server that is running low on memory. Therefore this is not the best answer and is therefore incorrect.

D: Reviewing the performance monitor on a monthly basis may help to determine that the server is running low on memory. However, the server could run out of memory in between reviews. The performance monitor also does not provide guidance on the actions that should be performed on a server that is running low on memory. Therefore this is not the best answer and is therefore incorrect.

QUESTION 4

A set of standardized system images with a pre-defined set of applications is used to build end-user workstations. The security administrator has scanned every workstation to create a current inventory of all applications that are installed on active workstations and is documenting which applications are out- of-date and could be exploited. The security administrator is determining the:

A. attack surface.

B. application hardening effectiveness.

C. application baseline.

D. OS hardening effectiveness.

Correct Answer: A

QUESTION 5

At the outside break area, an employee, Ann, asked another employee to let her into the building because her badge is missing. Which of the following does this describe?

A. Shoulder surfing

B. Tailgating

C. Whaling

D. Impersonation

Correct Answer: B

Although Ann is an employee and therefore authorized to enter the building, she does not have her badge and therefore strictly she should not be allowed to enter the building. Just as a driver can tailgate another driver\\'s car by following too

closely, in the security sense, tailgating means to compromise physical security by following somebody through a door meant to keep out intruders. Tailgating is actually a form of social engineering, whereby someone who is not authorized to

enter a particular area does so by following closely behind someone who is authorized.

Incorrect Answers:

A: Shoulder surfing is using direct observation techniques, such as looking over someone\\'s shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it\\'s relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. Incinerating documents will not prevent shoulder surfing. Ann is not trying to view sensitive information. Therefore this answer is incorrect.

C: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats. There is no malicious intent by Ann entering the building. Therefore this answer is incorrect.

D: Impersonation is where a person, computer, software application or service pretends to be someone it\\'s not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat. Ann is not trying to `impersonate\\' someone else. Therefore this answer is incorrect.

References: http://www.yourdictionary.com/tailgating http://searchsecurity.techtarget.com/definition/shoulder-surfing http://www.techopedia.com/definition/28643/whaling