JK0-022 Q&As

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

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

https://www.leads4pass.com/jk0-022.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Ann, a software developer, has installed some code to reactivate her account one week after her account has been disabled. Which of the following is this an example of? (Select TWO).

A. Rootkit

B. Logic Bomb

C. Botnet

D. Backdoor

E. Spyware

Correct Answer: BD

This is an example of both a logic bomb and a backdoor. The logic bomb is configured to `go off\\' or activate one week after her account has been disabled. The reactivated account will provide a backdoor into the system. A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool\\'s Day. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs. A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit. A backdoor in a login system might take the form of a hard coded user and password combination which gives access to the system.

Incorrect Answers:

A: A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network. In this question, a program hasn\\'t been installed. Therefore, a rootkit is not what is described in the question so this answer is incorrect.

C: A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation. Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment. This malware will typically install modules that allow the computer to be commanded and controlled by the botnet\\'s operator. Many computer users are unaware that their computer is infected with bots. Depending on how it is written, a Trojan may then delete itself, or may remain present to update and maintain the modules. In this question, no software has been installed. Therefore, a botnet is not what is described in the question so this answer is incorrect.

E: Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer\\'s consent, or that asserts control over a

computer without the consumer\\'s knowledge. "Spyware" is mostly classified into four types: system monitors, trojans, adware, and tracking cookies. Spyware is mostly used for the purposes of tracking and storing Internet users\\' movements on the Web and serving up pop-up ads to Internet users. Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users. In this question, no software has been installed. Therefore, spyware is not what is described in the question so this answer is incorrect.

References: http://en.wikipedia.org/wiki/Logic_bomb http://en.wikipedia.org/wiki/Botnet http://www.webopedia.com/TERM/V/virus.html http://en.wikipedia.org/wiki/Backdoor_%28computing%29 http://searchmidmarketsecurity.techtarget.com/definition/rootkit

---

QUESTION 2

An administrator needs to secure RADIUS traffic between two servers. Which of the following is the BEST solution?

A. Require IPSec with AH between the servers

B. Require the message-authenticator attribute for each message

C. Use MSCHAPv2 with MPPE instead of PAP

D. Require a long and complex shared secret for the servers

Correct Answer: A

QUESTION 3

What is a system that is intended or designed to be broken into by an attacker?

A. Honeypot

B. Honeybucket

C. Decoy

D. Spoofing system

Correct Answer: A

A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies.

According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the

system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

There are two main types of honeypots:

Production - A production honeypot is one used within an organization\\'s environment to help mitigate risk. Research - A research honeypot add value to research in computer security by providing a platform to study the threat.

Incorrect Answers:

B: A honey bucket is not an IT term. It\\'s a term for a waterless toilet. A honeypot is a system designed to be attacked. Therefore, this answer is incorrect.

C: A honeypot could be described as a decoy. It is a system often imitating another system but designed to be attacked. However, a honeypot is the specific name for a system designed to be attacked. Therefore, this answer is incorrect.

D: Spoofing system is not the correct term for a system that is designed to be attacked. A honeypot could be described as a spoofing system in that a honeypot often imitates another system. However, a honeypot is the specific name for a

system designed to be attacked.

Therefore, this answer is incorrect.

References: https://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study.php

---

QUESTION 4

Which of the following technologies can store multi-tenant data with different security requirements?

A. Data loss prevention

B. Trusted platform module

C. Hard drive encryption

D. Cloud computing

Correct Answer: D

One of the ways cloud computing is able to obtain cost efficiencies is by putting data from various clients on the same machines. This "multitenant" nature means that workloads from different clients can be on the same system, and a flaw in

implementation could compromise security.

Incorrect Answers:

A, B, C: None of these options offer multitenancy.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p 37.

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

QUESTION 5

Which of the following security account management techniques should a security analyst implement to prevent staff,

who has switched company roles, from exceeding privileges?

A. Internal account audits

B. Account disablement

C. Time of day restriction

D. Password complexity

Correct Answer: A

Internal account auditing will allow you to switch the appropriate users to the proper accounts required after the switching of roles occurred and thus check that the principle of least privilege is followed.

Incorrect Answers:

B: Account disablement will prevent staff from being able to log on in any capacity which means that they will not be able to perform their duties.

C: Almost every operating system--server and workstation--allows you to configure WHEN an account can have access to the system. `When\\' is a time restraint and not switching roles. These will only make accounts valid for certain times as per the policy.

D: Password complexity will make passwords more secure and more difficult for miscreants to break it and log in to that user\\'s account.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 140, 154