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.pass2lead.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

A recent spike in virus detections has been attributed to end-users visiting www.compnay.com. The business has an established relationship with an organization using the URL of www.company.com but not with the site that has been causing the infections. Which of the following would BEST describe this type of attack?

A. Typo squatting

B. Session hijacking

C. Cross-site scripting

D. Spear phishing

Correct Answer: A

Typosquatting, also called URL hijacking or fake url, is a form of cybersquatting, and possibly brandjacking which relies on mistakes such as typographical errors made by Internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to any URL (including an alternative website owned by a cybersquatter).

The typosquatter\\'s URL will usually be one of four kinds, all similar to the victim site address: (In the following, the intended website is "example.com") ?A common misspelling, or foreign language spelling, of the intended site: exemple.com ?A misspelling based on typing errors: xample.com or examlpe.com ?A differently phrased domain name: examples.com ?A different top-level domain: example.org Once in the typosquatter\\'s site, the user may also be tricked into thinking that they are in fact in the real site; through the use of copied or similar logos, website layouts or content.

Incorrect Answers:

B: In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session--sometimes also called a session key--to gain unauthorized access to information or services in a computer

system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be

easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim\\'s computer. In this question, the users went to www.compnay.com instead of www.company.com. Therefore, this is not a case of

hijacking a valid session; it\\'s a case of users going to the wrong URL.

Therefore, this answer is incorrect.

C: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug- in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised

site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user. The question is not describing an XSS attack.

Therefore, this answer is incorrect.

D: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear

to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent

source of the e-mail is likely to be an individual within the recipient\\'s own company and generally someone in a position of authority. The attack described in the question is not an example of spear phishing. Therefore, this answer is incorrect.

References: http://en.wikipedia.org/wiki/Typosquatting http://en.wikipedia.org/wiki/Session_hijacking http://searchsecurity.techtarget.com/definition/spear-phishing

QUESTION 2

An organization has introduced token-based authentication to system administrators due to risk of password compromise. The tokens have a set of numbers that automatically change every 30 seconds. Which of the following type of authentication mechanism is this?

A. TOTP

B. Smart card

C. CHAP

D. HOTP

Correct Answer: A

Time-based one-time password (TOTP) tokens are devices or applications that generate passwords at fixed time intervals. In this case, it\\'s every 30 seconds.

Incorrect Answers:

B: A smart card is sometimes referred to as an identity token containing integrated circuits. It does not generate passwords based on time.

C: The Challenge-Handshake Authentication Protocol (CHAP) is used primarily over dial-up connections to provide a secure transport mechanism for logon credentials. It does not generate passwords based on time.

D: HMAC-based one-time password (HOTP) tokens are devices that generate passwords based on a nonrepeating one-way function.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 282,283.

QUESTION 3

A security administrator is aware that a portion of the company\\'s Internet-facing network tends to be non-secure due to poorly configured and patched systems. The business owner has accepted the risk of those systems being compromised, but the administrator wants to determine the degree to which those systems can be used to gain access to the company intranet. Which of the following should the administrator perform?

A. Patch management assessment

B. Business impact assessment

C. Penetration test

D. Vulnerability assessment

Correct Answer: C

Penetration testing is the most intrusive type of testing because you are actively trying to circumvent the system\\'s security controls to gain access to the system. It is also used to determine the degree to which the systems can be used to gain

access to the company intranet (the degree of access to local network resources). Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker

could exploit. Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry

points, attempting to break in (either virtually or for real) and reporting back the findings. The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization\\'s security policy

compliance, its employees\\' security awareness and the organization\\'s ability to identify and respond to security incidents. Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break

in.

Pen test strategies include:

Targeted testing

Targeted testing is performed by the organization\\'s IT team and the penetration testing team working together. It\\'s sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out.

External testing

This type of pen test targets a company\\'s externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can

get in once they\\'ve gained access.

Internal testing

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

Blind testing

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that\\'s performing the test beforehand. Typically, they may only be given the name of the company.

Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

Double blind testing

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double- blind tests can be useful for testing an

organization\\'s security monitoring and incident identification as well as its response procedures.

Incorrect Answers:

A: Patch management is the process of managing the installation of security patches and updates on computer systems. An assessment of the patch management process is not performed to determine the degree to which computer systems

can be used to gain access to the company intranet. Therefore, this answer is incorrect.

B: A Business impact assessment is the assessment an event will have on the business; for example, a server failure. You could even perform a business impact assessment to assess the impact of a network intrusion. However, to test the

possible extent of an intrusion, you need to perform a penetration test. Therefore, this answer is incorrect.

D: A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and

vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates. A vulnerability scan is considered passive in that it doesn\\'t actually attempt to circumvent the security controls of a system to gain

access (unlike a penetration test). It can therefore not be used to determine the degree to which computer systems can be used to gain access to the company intranet.

Therefore, this answer is incorrect.

References: http://searchsoftwarequality.techtarget.com/definition/penetration-testing

QUESTION 4

An information bank has been established to store contacts, phone numbers and other records.

An application running on UNIX would like to connect to this index server using port 88. Which of the following authentication services would this use this port by default?

A. Kerberos

B. TACACS+

C. Radius

D. LDAP

Correct Answer: A

Kerberos makes use of port 88.

Incorrect Answers:

B: TACACS makes use of TCP port 49 by default.

C: RADIUS makes use of various UDP ports.

D: LDAP makes use of port 389.

References: http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 5

Which of the following controls should critical application servers implement to protect themselves from other potentially compromised application services?

A. NIPS

B. Content filter

C. NIDS

D. Host-based firewalls

Correct Answer: D