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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A technician is unable to manage a remote server. Which of the following ports should be opened on the firewall for remote server management? (Select TWO).

A. 22

B. 135

C. 137

D. 143

E. 443

F. 3389

Correct Answer: AF

A secure remote administration solution and Remote Desktop protocol is required. Secure Shell (SSH) is a secure remote administration solution and makes use of TCP port 22. Remote Desktop Protocol (RDP) uses TCP port 3389.

Incorrect Answers:

B: Port 135 is used by Microsoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service, which is used to remotely manage services including DHCP server, DNS server and WINS.

C: NetBIOS Name Service uses TCP port 137.

D: Internet Message Access Protocol v4 (IMAP4) uses TCP port 143.

E: HTTPS uses TCP port 443

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 51, 52.

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

QUESTION 2

Which of the following is characterized by an attacker attempting to map out an organization\\'s staff hierarchy in order to send targeted emails?

A. Whaling

B. Impersonation

C. Privilege escalation

D. Spear phishing

Correct Answer: A

A whaling attack is targeted at company executives. Mapping out an organization\\'s staff hierarchy to determine who the people at the top are is also part of a whaling attack. 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.

Incorrect Answers:

B: 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. No examples of impersonation occurred in this question. Therefore, this answer is incorrect.

C: Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The attack described in the question is not an example of privilege escalation. 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. Mapping out an organization\\'s staff hierarchy could be used for a spear phishing attack. However, the emails in a spear phishing attack would be sent to everyone in the company (not targeted to specific people) with the sender ID spoofed to appear to be from someone in authority. In this question, it\\'s likely that the emails would be targeted to the executives and that would be an example of whaling. Therefore, this answer is incorrect.

References: http://www.techopedia.com/definition/28643/whaling http://searchsecurity.techtarget.com/definition/spear-phishing

QUESTION 3

Several employee accounts appear to have been cracked by an attacker. Which of the following should the security administrator implement to mitigate password cracking attacks? (Select TWO).

A. Increase password complexity

B. Deploy an IDS to capture suspicious logins

C. Implement password history

D. Implement monitoring of logins

E. Implement password expiration

F. Increase password length

Correct Answer: AF

The more difficult a password is the more difficult it is to be cracked by an attacker. By increasing the password

complexity you make it more difficult. Passwords that are too short can easily be cracked. The more characters used in a password, combined with the increased complexity will mitigate password cracking attacks.

Incorrect Answers:

B: IDS (intrusion detection systems) can be implemented to capture suspicious logins, but that assumes that the passwords are already cracked.

C: Password history implementation is used to prevent users changing their password to the same value as the old one, or to one that they used the last time around, this might also be used by some crackers to hack passwords and thus is not mitigating password attacks.

D: Monitoring the logins is part of auditing and does not mitigate the password cracking attacks.

E: Password expiration refers to the period of validity of passwords. Some crackers will even make use of these expiry periods to crack passwords.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 139-140

QUESTION 4

A security administrator has deployed all laptops with Self Encrypting Drives (SED) and enforces key encryption. Which of the following represents the greatest threat to maintaining data confidentiality with these devices?

A. Full data access can be obtained by connecting the drive to a SATA or USB adapter bypassing the SED hardware.

B. A malicious employee can gain the SED encryption keys through software extraction allowing access to other laptops.

C. If the laptop does not use a Secure Boot BIOS, the SED hardware is not enabled allowing full data access.

D. Laptops that are placed in a sleep mode allow full data access when powered back on.

Correct Answer: D

QUESTION 5

An achievement in providing worldwide Internet security was the signing of certificates associated with which of the following protocols?

A. TCP/IP

B. SSL

C. SCP

D. SSH

Correct Answer: B

SSL (Secure Sockets Layer) is used for establishing an encrypted link between two computers, typically a web server and a browser. SSL is used to enable sensitive information such as login credentials and credit card numbers to be transmitted securely.

Incorrect Answers:

A: TCP/IP (Transmission Control Protocol/Internet Protocol) is a layered suite of protocols used to enable network communications between computers. All communications over the Internet between a Web browser and a Web server use

TCP/IP. HTTP and SSL run in the Application layer of the TCP/IP protocol suite.

TCP/IP itself does not use digitally signed certificates.

C: SCP (Secure Copy) uses SSH (Secure Shell) to copy files between computers using a secure encrypted connection. SSH uses public and private keys in a similar way to SSL to encrypt the connection, however SCP/SSH are not the

protocols used to provide the "worldwide Internet security" that this question is asking about.

D: SSH (Secure Shell) is commonly used to log into a remote machine and execute commands over a secure encrypted connection. SSH uses public and private keys in a similar way to SSL to encrypt the connection. However SSH is not the

protocol used to provide the "worldwide Internet security" that this question is asking about.

References: https://www.digicert.com/ssl.htm