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.geekcert.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

Which of the following software allows a network administrator to inspect the protocol header in order to troubleshoot network issues?

A. URL filter

B. Spam filter

C. Packet sniffer

D. Switch

Correct Answer: C

Every data packet transmitted across a network has a protocol header. To view a protocol header, you need to capture and view the contents of the packet with a packet sniffer.

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn\\'t generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

Incorrect Answers:

A: A URL filter is used to block URLs (websites) to prevent users accessing the website. It is not used to view protocol headers. Therefore, this answer is incorrect.

B: A spam filter is used for email. All inbound (and sometimes outbound) email is passed through the spam filter to detect spam emails. The spam emails are then discarded or tagged as potential spam according to the spam filter configuration. A spam filter is not used to view protocol headers. Therefore, this answer is incorrect.

D: A switch is a network device. Most computers on the network will be plugged into a switch. Switches maintain a MAC Table that maps individual MAC addresses on the network to the physical ports on the switch. This allows the switch to direct data out of the physical port where the recipient is located, as opposed to indiscriminately broadcasting the data out of all ports as a hub does. The advantage of this method is that data is bridged exclusively to the network segment containing the computer that the data is specifically destined for. A switch is not used to view protocol headers. Therefore, this answer is incorrect.

References: http://www.techopedia.com/definition/4113/sniffer

QUESTION 2

A major security risk with co-mingling of hosts with different security requirements is:

A. Security policy violations.

B. Zombie attacks.

C. Password compromises.

D. Privilege creep.

Correct Answer: A

The entire network is only as strong as the weakest host. Thus with the co-mingling of hosts with different security requirements would be risking security policy violations.

Incorrect Answers:

B: Zombie attacks are the same as botnets and it affects software. Bots itself is software that runs automatically and autonomously and as such is viewed as malicious software.

C: Password compromises on any account would not be best practice and also amounts to a security incident.

D: Privilege creep is usually uncovered during a privilege audit.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 220, 309

QUESTION 3

Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years.

Which of the following should Sara do to address the risk?

A. Accept the risk saving $10,000.

B. Ignore the risk saving $5,000.

C. Mitigate the risk saving $10,000.

D. Transfer the risk saving $5,000.

Correct Answer: D

Risk transference involves sharing some of the risk burden with someone else, such as an insurance company. The cost of the security breach over a period of 5 years would amount to $30,000 and it is better to save $5,000.

Incorrect Answers:

A: Risk acceptance is often the choice you must make when the cost of implementing any of the other four choices exceeds the value of the harm that would occur if the risk came to fruition. In this case there is no saving and the risk already happened.

B: Ignoring the risk will not save you $5,000 since the system is due to be replaced within a 5 year period which will cost your company $30,000.

C: Risk mitigation is accomplished any time you take steps to reduce risk. This category includes installing antivirus software, educating users about possible threats, monitoring network traffic, adding a firewall, and so on. You should

however address the security breach else there will be no saving.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 9

QUESTION 4

A network consists of various remote sites that connect back to two main locations. Pete, the security administrator, needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

A. Block port 23 on the L2 switch at each remote site

B. Block port 23 on the network firewall

C. Block port 25 on the L2 switch at each remote site

D. Block port 25 on the network firewall

Correct Answer: B

Telnet is a terminal-emulation network application that supports remote connectivity for executing commands and running applications but doesn\\'t support transfer of fi les. Telnet uses TCP port 23. Because it\\'s a clear text protocol and

service, it should be avoided and replaced with SSH.

Incorrect Answers:

A, C: L2 switches may interconnect a small number of devices in a home or the office. They are normally used for LANs.

D: Port 25 is used by Simple Mail Transfer Protocol (SMTP) for e-mail routing between mail servers.

References:

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

http://en.wikipedia.org/wiki/Network_switch#Layer_2

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

QUESTION 5

A security administrator must implement a firewall rule to allow remote employees to VPN onto the company network. The VPN concentrator implements SSL VPN over the standard HTTPS port. Which of the following is the MOST secure ACL to implement at the company\\'s gateway firewall?

A. PERMIT TCP FROM ANY 443 TO 199.70.5.25 443

B. PERMIT TCP FROM ANY ANY TO 199.70.5.23 ANY

C. PERMIT TCP FROM 199.70.5.23 ANY TO ANY ANY

D. PERMIT TCP FROM ANY 1024-65535 TO 199.70.5.23 443

Correct Answer: D

Latest JK0-022 Dumps JK0-022 VCE Dumps JK0-022 Practice Test