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

CompTIA Security+ Certification

QUESTION 1

Which of the following can use RC4 for encryption? (Select TWO).

A. CHAP

B. SSL

C. WEP

D. AES

E. 3DES

Correct Answer: BC

B: In cryptography, RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4) is the most widely used software stream cipher and is used in popular Internet protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

C: WEP also uses RC4, however WEP is still unsecure.

Incorrect Answers:

A: the Challenge-Handshake Authentication Protocol (CHAP) does not use RC4.

D: The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. AES make no use of RC4.

E: Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of electronic data. DES make no use of RC4. Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 143, 250, 258, 268-269

QUESTION 2

How must user accounts for exiting employees be handled?

A. Disabled, regardless of the circumstances

B. Disabled if the employee has been terminated

C. Deleted, regardless of the circumstances

D. Deleted if the employee has been terminated

Correct Answer: A

You should always disable an employee\\'s account as soon as they leave. The employee knows the username and password of the account and could continue to log in for potentially malicious purposes. Disabling the account will ensure that no one can log in using that account.

Incorrect Answers:

B: You should always disable an employee\\'s account as soon as they leave regardless of why they are leaving. A terminated employee might be more likely to log in for malicious purposes but should you also disable the accounts of

employees leaving through their own choice. Disabling any unused account is always best practice. Therefore, this answer is incorrect.

C: There is no need to delete the account. The employee may come back to the company or a new employee may join the company to replace the leaving employee. In this case, you could just rename the disabled account, change the

password and re-enable the account. The new employee would then have the same access to resources as the ex-employee. Therefore, this answer is incorrect.

D: There is no need to delete the account. A new employee may join the company to replace the leaving employee. In this case, you could just rename the disabled account, change the password and re-enable the account. The new

employee would then have the same access to resources as the ex-employee.

Therefore, this answer is incorrect.

QUESTION 3

Sara, the Chief Information Officer (CIO), has requested an audit take place to determine what services and operating systems are running on the corporate network. Which of the following should be used to complete this task?

A. Fingerprinting and password crackers

B. Fuzzing and a port scan

C. Vulnerability scan and fuzzing

D. Port scan and fingerprinting

Correct Answer: D

Different services use different ports. When a service is enabled on a computer, a network port is opened for that service. For example, enabling the HTTP service on a web server will open port 80 on the server. By determining which ports are open on a remote server, we can determine which services are running on that server. A port scanner is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it. A port scan or portscan can be defined as a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. While not a nefarious process in and of itself, it is one used by hackers to probe target machine services with the aim of exploiting a known vulnerability of that service. However the majority of uses of a port scan are not attacks and are simple probes to determine services available on a remote machine.

Fingerprinting is a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished "passively" by sniffing network packets passing between hosts, or it can be accomplished "actively" by transmitting specially created packets to the target machine and analyzing the response

Incorrect Answers:

A: Fingerprinting is a means of ascertaining the operating system of a remote computer on a network. However, a password cracker is not used to determine which services are running on network computers. Therefore, this answer is incorrect.

B: A port scan can be used to determine which services are running on network computers. However fuzzing is not used to determine which operating system the computers are running. Fuzzing is a security assessment technique that allows testers to analyze the behavior of software applications by entering unexpected input. Therefore, this answer is incorrect.

C: A vulnerability scanner is software designed to assess computers, computer systems, networks or applications for weaknesses. A vulnerability scan will scan for weaknesses (vulnerabilities) in a system. It could provide information about which services are running but it is not specifically designed for this purpose. Fuzzing is not used to determine which operating system the computers are running or which services are running on the computers. Fuzzing is a security assessment technique that allows testers to analyze the behavior of software applications by entering unexpected input. Therefore, this answer is incorrect.

References: http://en.wikipedia.org/wiki/Port_scanner http://www.yourdictionary.com/fingerprinting

QUESTION 4

Each server on a subnet is configured to only allow SSH access from the administrator\\'s workstation. Which of the following BEST describes this implementation?

A. Host-based firewalls

B. Network firewalls

C. Network proxy

D. Host intrusion prevention

Correct Answer: A

A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet. These firewalls manage network traffic using filters to block certain ports and protocols while allowing others to pass through the system.

Incorrect Answers:

B: A network firewall protects the entire network from an untrusted public network, such as the Internet by filtering network traffic. It does not filter network traffic on the internal network.

C: A network proxy is used to protect the local network from external attacks by hiding the IP configuration of the internal clients. It does not filter network traffic.

D: A host-based IPS (HIPS) is an intrusion detection and prevention system that runs as a service on a host computer system. It is used to monitor the machine logs, system events, and application activity for signs of intrusion.

References:

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

111-112, 116-117 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 11, 13-16

QUESTION 5

Ann was reviewing her company\\'s event logs and observed several instances of GUEST accessing the company print server, file server, and archive database. As she continued to investigate, Ann noticed that it seemed to happen at random intervals throughout the day, but mostly after the weekly automated patching and often logging in at the same time. Which of the following would BEST mitigate this issue?

A. Enabling time of day restrictions

B. Disabling unnecessary services

C. Disabling unnecessary accounts

D. Rogue machine detection

Correct Answer: C

QUESTION 6

Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?

A. Input validation

B. Network intrusion detection system

C. Anomaly-based HIDS

D. Peer review

Correct Answer: A

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

Incorrect Answers:

B: A network-based IDS (NIDS) is an intrusion detection system that scans network traffic in real time and is useful for detecting network-based attacks.

C: A host-based IDS (HIDS) is an intrusion detection system that runs as a service on a host computer system. It is used to monitor the machine logs, system events, and application activity for signs of intrusion. It does not prevent attacks, such as cross-site scripting attacks and buffer overflows, but detects it.

D: Peer review is the process of reviewing source code before the software is released. This is performed by a peer rather than by the programmer.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 111-112, 116-117, 257, 338 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp

21,

197, 216, 319

QUESTION 7

A company is trying to limit the risk associated with the use of unapproved USB devices to copy documents. Which of the following would be the BEST technology control to use in this scenario?

A. Content filtering

B. IDS

C. Audit logs

D. DLP

Correct Answer: D

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

Incorrect Answers:

A: Content filtering is the process of inspecting the content of a web page as it is downloaded. The content can then be blocked if it doesn\\'t comply with the company\\'s web policy. Content- control software determines what content will be

available or perhaps more often what content will be blocked. Content filtering will not prevent documents being copied to a USB device.

B: An IDS (Intrusion Detection System) is used to detect attempts to access a computer system or network. An IDS will not prevent documents being copied to a USB device.

C: Audit logs are used to record events such as account logons, file access etc. An audit log may record when a file is accessed (if auditing is enabled for the file) but it will not prevent a file being copied to a USB device.

References:

http://whatis.techtarget.com/definition/data-loss-prevention-DLP

QUESTION 8

The act of magnetically erasing all of the data on a disk is known as:

A. Wiping

B. Dissolution

C. Scrubbing

D. Degaussing

Correct Answer: D

Degaussing is a form a data wiping that entails the use of magnets to alter the magnetic structure of the storage medium.

Incorrect Answers:

A: Data wiping is the process of securely removing data remnants from a storage device so that the data cannot be recovered. This is usually done when a device is to be disposed or can be done remotely, when a mobile device is stolen. B, C: Dissolution and scrubbing are not related to erasing data on a disk.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 256
http://pcsupport.about.com/od/toolsofthetrade/tp/erase-hard- drive.htm

---

QUESTION 9

Which of the following are examples of detective controls?

A. Biometrics, motion sensors and mantraps.

B. Audit, firewall, anti-virus and biometrics.

C. Motion sensors, intruder alarm and audit.

D. Intruder alarm, mantraps and firewall.

Correct Answer: C

QUESTION 10

Certificates are used for: (Select TWO).

A. Client authentication.

B. WEP encryption.

C. Access control lists.

D. Code signing.

E. Password hashing.

Correct Answer: AD

Certificates are used in PKI to digitally sign data, information, files, email, code, etc. Certificates are also used in PKI for client authentication.

Incorrect Answers:

B: Wired Equivalent Privacy (WEP) encryption is used with TKIP which placed a 128-bit wrapper around the WEP encryption and is based on the MAC address of the host device and the serial number of the packet.

C: Access control lists are used to allow individual and highly controllable access to resources in a network.

E: Hashing refers to the hash algorithms used in cryptography. It is used to derive a key mathematically from a message.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 156, 278, 281

QUESTION 11

Which of the following controls mitigates the risk of Matt, an attacker, gaining access to a company network by using a former employee\\'s credential?

A. Account expiration

B. Password complexity

C. Account lockout

D. Dual factor authentication

Correct Answer: A

Account expiration is a secure feature to employ on user accounts for temporary workers, interns, or consultants. It automatically disables a user account or causes the account to expire at a specific time and on a specific day.

Incorrect Answers:

B: Implementing password complexity would not work, as the user is a former employee and would not be there to change their password to a more complex one.

C: Account lockout automatically disables an account due to repeated failed log on attempts. Matt could get the password before reaching the log on attempt threshold.

D: Matt could still discover both authentication factors to gain access. With the account disabled, there is no chance of that happening.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292- 294.

QUESTION 12

Which of the following components of an all-in-one security appliance would MOST likely be configured in order to restrict access to peer-to-peer file sharing websites?

A. Spam filter

B. URL filter

C. Content inspection

D. Malware inspection

Correct Answer: B

QUESTION 13

Which of the following network architecture concepts is used to securely isolate at the boundary between networks?

A. VLAN

B. Subnetting

C. DMZ

D. NAT

Correct Answer: C

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

Incorrect Answers:

A: A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments.

B: Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.

D: NAT converts the IP addresses of internal systems found in the header of network packets into public IP addresses. A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 23, 39.

QUESTION 14

A security administrator has been tasked to ensure access to all network equipment is controlled by a central server such as TACACS+. This type of implementation supports which of the following risk mitigation strategies?

A. User rights and permissions review

B. Change management

C. Data loss prevention

D. Implement procedures to prevent data theft

Correct Answer: A

Terminal Access Controller Access-Control System (TACACS, and variations like XTACACS and TACACS+) is a client/server-oriented environment, and it operates in a manner similar to RADIUS. Furthermore TACACS+ allows for credential to be accepted from multiple methods. Thus you can perform user rights and permission reviews with TACACS+.

Incorrect Answers:

B: Change management is the structured approach that is followed to secure a company\\'s assets and not a risk mitigation strategy.

C: Data loss prevention systems are used mainly to monitor the contents of systems and to make sure that key content is not deleted or removed.

D: Data theft prevention is similar to data loss prevention systems.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 9-10, 146

QUESTION 15

Ann, a security technician, is reviewing the IDS log files. She notices a large number of alerts for multicast packets from the switches on the network. After investigation, she discovers that this is normal activity for her network. Which of the following BEST describes these results?

A. True negatives

B. True positives

C. False positives

D. False negatives

Correct Answer: C

False positives are essentially events that are mistakenly flagged and are not really events to be concerned about.

Incorrect Answers:

A: True negatives would be non-events.

B: True positives would be real alerts and alarms.

D: With a false negative, you are not alerted to a situation when you should be alerted - The opposite of false negatives.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 28

JK0-022 VCE Dumps JK0-022 Practice Test JK0-022 Exam Questions