# Braindump2go Offers The Latest CompTIA SY0-401 Questions and Answers For Free Download

QUESTION 1 Which of the following protocols operates at the HIGHEST level of the OSI model? A.    ICMP B.    IPSec C.    SCP D.    TCP Answer: CQUESTION 2 Joe, the system administrator, has been asked to calculate the Annual Loss Expectancy (ALE) for a $5,000 server, which often crashes. In the past year, the server has crashed 10 times, requiring a system reboot to recover with only 10% loss of data or function. Which of the following is the ALE of this server? A.    $500 B.    $5,000 C.    $25,000 D.    $50,000 Answer: B QUESTION 3 Which of the following should an administrator implement to research current attack methodologies? A.    Design reviews B.    Honeypot C.    Vulnerability scanner D.    Code reviews Answer: B QUESTION 4 Which of the following can be implemented in hardware or software to protect a web server from cross-site scripting attacks? A.    Intrusion Detection System B.    Flood Guard Protection C.    Web Application Firewall D.    URL Content Filter Answer: C QUESTION 5 Which of the following means of wireless authentication is easily vulnerable to spoofing? A.    MAC Filtering B.    WPA - LEAP C.    WPA - PEAP D.    Enabled SSID Answer: A QUESTION 6 The BEST methods for a web developer to prevent the website application code from being vulnerable to cross-site request forgery (XSRF) are to: (Select TWO). A.    permit redirection to Internet-facing web URLs. B.    ensure all HTML tags are enclosed in angle brackets, e.g., "<" and ">". C.    validate and filter input on the server side and client side. D.    use a web proxy to pass website requests between the user and the application. E.    restrict and sanitize use of special characters in input and URLs. Answer: CE QUESTION 7 Jane, a security administrator, needs to implement a secure wireless authentication method that uses a remote RADIUS server for authentication. Which of the following is an authentication method Jane should use? A.    WPA2-PSK B.    WEP-PSK C.    CCMP D.    LEAP Answer: D QUESTION 8 Computer evidence at a crime scene is documented with a tag stating who had possession of the evidence at a given time. Which of the following does this illustrate? A.    System image capture B.    Record time offset C.    Order of volatility D.    Chain of custody Answer: D QUESTION 9 A network administrator is configuring access control for the sales department which has high employee turnover. Which of the following is BEST suited when assigning user rights to individuals in the sales department? A.    Time of day restrictions B.    Group based privileges C.    User assigned privileges D.    Domain admin restrictions Answer: B QUESTION 10 Which of the following is being tested when a company's payroll server is powered off for eight hours? A.    Succession plan B.    Business impact document C.    Continuity of operations plan D.    Risk assessment plan Answer: C QUESTION 11 Which of the following preventative controls would be appropriate for responding to a directive to reduce the attack surface of a specific host? A.    Installing anti-malware B.    Implementing an IDS C.    Taking a baseline configuration D.    Disabling unnecessary services Answer: D QUESTION 12 A security manager must remain aware of the security posture of each system. Which of the following supports this requirement? A.    Training staff on security policies B.    Establishing baseline reporting C.    Installing anti-malware software D.    Disabling unnecessary accounts/services Answer: B QUESTION 13 Deploying a wildcard certificate is one strategy to: A.    secure the certificate's private key. B.    increase the certificate's encryption key length. C.    extend the renewal date of the certificate. D.    reduce the certificate management burden. Answer: D QUESTION 14 The security administrator needs to manage traffic on a layer 3 device to support FTP from a new remote site. Which of the following would need to be implemented? A.    Implicit deny B.    VLAN management C.    Port security D.    Access control lists Answer: D QUESTION 15 Which of the following ports is used for SSH, by default? A.    23 B.    32 C.    12 D.    22 Answer: D QUESTION 16 A network administrator has been tasked with securing the WLAN. Which of the following cryptographic products would be used to provide the MOST secure environment for the WLAN? A.    WPA2 CCMP B.    WPA C.    WPA with MAC filtering

D.    WPA2 TKIP Answer: A QUESTION 17 A server with the IP address of 10.10.2.4 has been having intermittent connection issues. The logs show repeated connection attempts from the following IPs: 10.10.3.16 10.10.3.23 212.178.24.26 217.24.94.83 These attempts are overloading the server to the point that it cannot respond to traffic. Which of the following attacks is occurring? A.    XSS B.    DDoS C.    DoS D.    Xmas Answer: B QUESTION 18 Which of the following ciphers would be BEST used to encrypt streaming video? A.    RSA B.    RC4 C.    SHA1 D.    3DES Answer: B QUESTION 19 A user attempting to log on to a workstation for the first time is prompted for the following information before being granted access: username, password, and a four-digit security pin that was mailed to him during account registration. This is an example of which of the following? A.    Dual-factor authentication B.    Multifactor authentication C.    Single factor authentication D.    Biometric authentication Answer: C QUESTION 20 After analyzing and correlating activity from multiple sensors, the security administrator has determined that a group of very well organized individuals from an enemy country is responsible for various attempts to breach the company network, through the use of very sophisticated and targeted attacks. Which of the following is this an example of? A.    Privilege escalation B.    Advanced persistent threat C.    Malicious insider threat D.    Spear phishing Answer: B Download the Latest CompTIA SY0-301 Exam Dumps from Braindump2go http://www.braindump2go.com/sy0-401.html