# [March 2018 2018 Exam CISSP Dumps From Lead2pass Cover All New CISSP New Questions 2873q

2018 Lead2pass New Updated CISSP Exam Questions: https://www.lead2pass.com/cissp.html QUESTION 11Which one of the following factors is NOT one on which Authentication is based? A. Type 1 Something you know, such as a PIN or passwordB. Type 2 Something you have, such as an ATM card or smart cardC. Type 3 Something you are (based upon one or more intrinsic physical or behavioral traits), such as a fingerprint or retina scanD. Type 4 Something you are, such as a system administrator or security administratorAnswer: DExplanation:Authentication is based on the following three factor types:Type 1. Something you know, such as a PIN or passwordType 2. Something you have, such as an ATM card or smart card Type 3. Something you are (Unique physical characteristic), such as a fingerprint or retina scan QUESTION 12The act of requiring two of the three factors to be used in the authentication process refers to: A. Two-Factor AuthenticationB. One-Factor AuthenticationC. Bi-Factor AuthenticationD. Double Authentication Answer: AExplanation:Two-Factor Authentication refers to the act of requiring two of the three factors to be used in the authentication process. QUESTION 13Which type of password provides maximum security because a new password is required for each new log-on? A. One-time or dynamic passwordB. Congnitive passwordC. Static passwordD. Passphrase Answer: AExplanation:"One-time password" provides maximum security because a new password is required for each new log-on. QUESTION 14What is called a password that is the same for each log-on session? A. "one-time password"B. "two-time password"C. static passwordD. dynamic password Answer: C QUESTION 15What is called a sequence of characters that is usually longer than the allotted number for a password? A. passphraseB. cognitive phraseC. anticipated phraseD. Real phrase Answer: AExplanation:A passphrase is a sequence of characters that is usually longer than the allotted number for a password. QUESTION 16Which best describes a tool (i.e. keyfob, calculator, memory card or smart card) used to supply dynamic passwords? A. TicketsB. TokensC. Token passing networksD. Coupons Answer: BExplanation:Tokens; Tokens in the form of credit card-size memory cards or smart cards, or those resembling small calculators, are used to supply static and dynamic passwords. QUESTION 17Which of the following would be true about Static password tokens? A. The owner identity is authenticated by the tokenB. The owner will never be authenticated by the token.C. The owner will authenticate himself to the system.D. The token does not authenticates the token owner but the system. Answer: AExplanation:Tokens are electronic devices or cards that supply a user's password for them. A token system can be used to supply either a static or a dynamic password. There is a big difference between the static and dynamic systems, a static system will normally log a user in but a dynamic system the user will often have to log themselves in. Static Password Tokens: The owner identity is authenticated by the token. This is done by the person who issues the token to the owner (normally the employer). The owner of the token is now authenticated by "something you have". The token authenticates the identity of the owner to the information system. An example of this occurring is when an employee swipes his or her smart card over an electronic lock to gain access to a store room. Synchronous Dynamic Password Tokens: This system is a lot more complex then the static token password. The synchronous dynamic password tokens generate new passwords at certain time intervals that are synched with the main system. The password is generated on a small device similar to a pager or a calculator that can often be attached to the user's key ring. Each password is only valid for a certain time period, typing in the wrong password in the wrong time period will invalidate the authentication. The time factor can also be the systems downfall. If a clock on the system or the password token device becomes out of synch, a user can have troubles authenticating themselves to the system. Asynchronous Dynamic Password Tokens: The clock synching problem is eliminated with asynchronous dynamic password tokens. This system works on the same principal as the synchronous one but it does not have a time frame. A lot of big companies use this system especially for employee's who may work from home on the companies VPN (Virtual private Network). Challenge Response Tokens: This is an interesting system. A user will be sent special "challenge" strings at either random or timed intervals. The user inputs this challenge string into their token device and the device will respond by generating a challenge response. The user then types this response into the system and if it is correct they are authenticated. QUESTION 18In Synchronous dynamic password tokens: A. The token generates a new password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).B. The token generates a new non-unique password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).C. The unique password is not entered into a system or workstation along with an owner's PIN.D. The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is invalid and that it was entered during the invalid time window. Answer: AExplanation:Synchronous dynamic password tokens:The token generates a new password value at fixed time intervals (this password could be the time of day encrypted with a secret key).The unique password is entered into a system or workstation along with an owner's PIN. The authentication entity in a system or workstation knows an owner's secret key and PIN,

and the entity verifies that the entered password is valid and that it was entered during the valid time window. QUESTION 19In biometrics, "one-to-many" search against database of stored biometric images is done in: A. AuthenticationB. IdentificationC. IdentitiesD. Identity-based access control Answer: BExplanation:In biometrics, identification is a "one-to-many" search of an individual's characteristics from a database of stored images. QUESTION 20Which of the following is true of biometrics? A. It is used for identification in physical controls and it is not used in logical controls.B. It is used for authentication in physical controls and for identification in logical controls.C. It is used for identification in physical controls and for authentication in logical controls.D. Biometrics has not role in logical controls. Answer: CExplanation:When used in physical control biometric Identification is performed by doing a one to many match. When you submit your biometric template a search is done through a database of templates until the matching one is found. At that point your identity is revealed and if you are a valid employee access is granted. When used in logical controls the biometric template is used to either confirm or deny someone identity. For example if I access a system and I pretend to be user Nathalie then I would provide my biometric template to confirm that I really am who I pretend to be. Biometric is one of the three authentication factor (somethin you are) that can be use. The other two are something you know and something you have. **CISSP dumps full version (PDF&VCE):** https://www.lead2pass.com/cissp.html Large amount of free **CISSP** exam questions on Google Drive: https://drive.google.com/open?id=1393N8RayZN4QJ8sxg6_3cIRxwNv8QGTq