[Lead2pass New Lead2pass SY0-401 Exam Dumps New Updated By CompTIA Official Exam Center (601-625)

Lead2pass 2017 October New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! The SY0-401 braindumps are the latest, authenticated by expert and covering each and every aspect of SY0-401 exam. Comparing with others, our exam questions are rich in variety. We offer PDF dumps and SY0-401 VCE dumps. Welcome to choose. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 601Which of the following is an authentication and accounting service that uses TCP for connecting to routers and switches? A. DIAMETERB. RADIUSC. TACACS+D. KerberosAnswer: CExplanation:TACACS+ is an authentication, authorization, and accounting (AAA) service that makes us of TCP only. QUESTION 602A 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 reviewB. Change managementC. Data loss preventionD. Implement procedures to prevent data theft Answer: AExplanation: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+. QUESTION 603Which of the following services are used to support authentication services for several local devices from a central location without the use of tokens? A. TACACS+B. SmartcardsC. BiometricsD. Kerberos Answer: AExplanation:ACACS allows a client to accept a username and password and send a query to a TACACS authentication server. It would determine whether to accept or deny the authentication request and send a response back. The TIP would then allow access or not based upon the response, not tokens. QUESTION 604Which of the following protocols uses TCP instead of UDP and is incompatible with all previous versions? A. TACACSB. XTACACSC. RADIUSD. TACACS+ Answer: DExplanation:TACACS+ is not compatible with TACACS and XTACACS, and makes use of TCP. QUESTION 605Which of the following authentication services should be replaced with a more secure alternative? A. RADIUSB. TACACSC. TACACS+D. XTACACS Answer: BExplanation:Terminal Access Controller Access-Control System (TACACS) is less secure than XTACACS, which is a proprietary extension of TACACS, and less secure than TACACS+, which replaced TACACS and XTACACS. QUESTION 606In Kerberos, the Ticket Granting Ticket (TGT) is used for which of the following? A. IdentificationB. AuthorizationC. AuthenticationD. Multifactor authentication Answer: CExplanation:An authentication ticket, also known as a ticket-granting ticket (TGT), is a small amount of encrypted data that is issued by a server in the Kerberos authentication model to begin the authentication process. When the client receives an authentication ticket, the client sends the ticket back to the server along with additional information verifying the client's identity. The server then issues a service ticket and a session key (which includes a form of password), completing the authorization process for that session.In the Kerberos model, all tickets are time-stamped and have limited lifetimes. This minimizes the danger that hackers will be able to steal or crack the encrypted data and use it to compromise the system. Ideally, no authentication ticket remains valid for longer than the time an expert hacker would need to crack the encryption. Authentication tickets are session-specific, further improving the security of the system by ensuring that no authentication ticket remains valid after a given session is complete. QUESTION 607Which of the following types of authentication packages user credentials in a ticket? A. KerberosB. LDAPC. TACACS+D. RADIUS Answer: AExplanation:The basic process of Kerberos authentication is as follows:The subject provides logon credentials.The Kerberos client system encrypts the password and transmits the protected credentials to the KDC.The KDC verifies the credentials and then creates a ticket-granting ticket (TGT--a hashed form of the subject's password with the addition of a time stamp that indicates a valid lifetime). The TGT is encrypted and sent to the client.The client receives the TGT. At this point, the subject is an authenticated principle in the Kerberos realm.The subject requests access to resources on a network server. This causes the client to request a service ticket (ST) from the KDC.The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a time stamp that indicates its valid lifetime.The client receives the ST.The client sends the ST to the network server that hosts the desired resource. The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved. QUESTION 608Which of the following authentication services requires the use of a ticket-granting ticket (TGT) server in order to complete the authentication process? A. TACACS+B. Secure LDAPC. RADIUSD. Kerberos Answer: DExplanation:The basic process of Kerberos authentication is as follows:The subject provides logon credentials.The Kerberos client system encrypts the password and transmits the protected credentials to the KDC.The KDC verifies the credentials and then creates a ticket-granting ticket (TGT--a hashed form of the subject's password with the addition of a time stamp that indicates a valid lifetime). The TGT is encrypted and sent to the client.The client receives the TGT. At

this point, the subject is an authenticated principle in the Kerberos realm.The subject requests access to resources on a network server. This causes the client to request a service ticket (ST) from the KDC.The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a time stamp that indicates its valid lifetime.The client receives the ST.The client sends the ST to the network server that hosts the desired resource. The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved. QUESTION 609A security administrator has installed a new KDC for the corporate environment. Which of the following authentication protocols is the security administrator planning to implement across the organization? A. LDAPB. RADIUSC. KerberosD. XTACACS Answer: CExplanation:The fundamental component of a Kerberos solution is the key distribution centre (KDC), which is responsible for verifying the identity of principles and granting and controlling access within a network environment through the use of secure cryptographic keys and tickets. QUESTION 610Jane, a security administrator, has been tasked with explaining authentication services to the company's management team. The company runs an active directory infrastructure. Which of the following solutions BEST relates to the host authentication protocol within the company's environment? A. KerberosB. Least privilegeC. TACACS+D. LDAP Answer: AExplanation:Kerberos was accepted by Microsoft as the chosen authentication protocol for Windows 2000 and Active Directory domains that followed. QUESTION 611Which of the following types of authentication solutions use tickets to provide access to various resources from a central location? A. BiometricsB. PKIC. ACLsD. Kerberos Answer: DExplanation:The basic process of Kerberos authentication is as follows:The subject provides logon credentials.The Kerberos client system encrypts the password and transmits the protected credentials to the KDC.The KDC verifies the credentials and then creates a ticket-granting ticket (TGT--a hashed form of the subject's password with the addition of a time stamp that indicates a valid lifetime). The TGT is encrypted and sent to the client.The client receives the TGT. At this point, the subject is an authenticated principle in the Kerberos realm.The subject requests access to resources on a network server. This causes the client to request a service ticket (ST) from the KDC.The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a time stamp that indicates its valid lifetime.The client receives the ST.The client sends the ST to the network server that hosts the desired resource. The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved. QUESTION 612Which of the following authentication services uses a ticket granting system to provide access? A. RADIUSB. LDAPC. TACACS+D. Kerberos Answer: DExplanation:The basic process of Kerberos authentication is as follows:The subject provides logon credentials.The Kerberos client system encrypts the password and transmits the protected credentials to the KDC.The KDC verifies the credentials and then creates a ticket-granting ticket (TGT--a hashed form of the subject's password with the addition of a time stamp that indicates a valid lifetime). The TGT is encrypted and sent to the client.The client receives the TGT. At this point, the subject is an authenticated principle in the Kerberos realm.The subject requests access to resources on a network server. This causes the client to request a service ticket (ST) from the KDC.The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a time stamp that indicates its valid lifetime.The client receives the ST.The client sends the ST to the network server that hosts the desired resource. The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved. QUESTION 613An information bank has been established to store contacts, phone numbers and other records.An application running on UNIX would like to connect to this index server using port 88. Which of the following authentication services would this use this port by default? A. KerberosB. TACACS+C. RadiusD. LDAP Answer: AExplanation: Kerberos makes use of port 88. QUESTION 614Which of the following was based on a previous X.500 specification and allows either unencrypted authentication or encrypted authentication through the use of TLS? A. KerberosB. TACACS+C. RADIUSD. LDAP Answer: DExplanation:The Lightweight Directory Access Protocol is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number. A common usage of LDAP is to provide a "single sign on" where one password for a user is shared between many services, such as applying a company login code to web pages (so that staff log in only once to company computers, and then are automatically logged into the company intranet).LDAP is based on a simpler subset of the standards contained within the X.500 standard. Because of this relationship, LDAP is sometimes called X.500-lite. A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP and UDP port 389, or on port 636 for LDAPS. Global Catalog is available by default on ports 3268, and 3269 for LDAPS. The client then sends an operation request to the server, and the server sends responses in return.The client may request the

following operations:StartTLS -- use the LDAPv3 Transport Layer Security (TLS) extension for a secure connection QUESTION 615A system administrator is configuring UNIX accounts to authenticate against an external server. The configuration file asks for the following information DC=ServerName and DC=COM. Which of the following authentication services is being used? A. RADIUSB. SAMLC. TACACS+D. LDAP Answer: DExplanation:The Lightweight Directory Access Protocol is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number. An entry can look like this when represented in LDAP Data Interchange Format (LDIF) (LDAP itself is a binary protocol):dn: cn=John Doe,dc=example,dc=comcn: John DoegivenName: Johnsn: DoetelephoneNumber: +1 888 555 6789telephoneNumber: +1 888 555 1232mail: john@example.commanager: cn=Barbara Doe,dc=example,dc=comobjectClass: inetOrgPersonobjectClass: organizationalPersonobjectClass: personobjectClass: top "dn" is the distinguished name of the entry; it is neither an attribute nor a part of the entry. "cn=John Doe" is the entry's RDN (Relative Distinguished Name), and "dc=example,dc=com" is the DN of the parent entry, where "dc" denotes 'Domain Component'. The other lines show the attributes in the entry. Attribute names are typically mnemonic strings, like "cn" for common name, "dc" for domain component, "mail" for e-mail address, and "sn" for surname. QUESTION 616Which of the following is an XML based open standard used in the exchange of authentication and authorization information between different parties? A. LDAPB. SAMLC. TACACS+D. Kerberos Answer: BExplanation:Security Assertion Markup Language (SAML) is an open-standard data format centred on XML. It is used for supporting the exchange of authentication and authorization details between systems, services, and devices. QUESTION 617Which of the following is an authentication method that can be secured by using SSL? A. RADIUSB. LDAPC. TACACS+D. Kerberos Answer: BExplanation:With secure LDAP (LDAPS), all LDAP communications are encrypted with SSL/TLS QUESTION 618A user ID and password together provide which of the following? A. AuthorizationB. AuditingC. AuthenticationD. Identification Answer: CExplanation:Authentication generally requires one or more of the following:Something you know: a password, code, PIN, combination, or secret phrase. Something you have: a smart card, token device, or key. Something you are: a fingerprint, a retina scan, or voice recognition; often referred to as biometrics, discussed later in this chapter.Somewhere you are: a physical or logical location.Something you do: typing rhythm, a secret handshake, or a private knock. QUESTION 619The fundamental information security principals include confidentiality, availability and which of the following? A. The ability to secure data against unauthorized disclosure to external sourcesB. The capacity of a system to resist unauthorized changes to stored informationC. The confidence with which a system can attest to the identity of a userD. The characteristic of a system to provide uninterrupted service to authorized users Answer: BExplanation: Confidentiality, integrity, and availability, which make up the CIA triad, are the three most important concepts in security. In this instance, the answer describes the Integrity part of the CIA triad. QUESTION 620Which of the following is the difference between identification and authentication of a user? A. Identification tells who the user is and authentication tells whether the user is allowed to logon to a system.B. Identification tells who the user is and authentication proves it.C. Identification proves who the user is and authentication is used to keep the users data secure.D. Identification proves who the user is and authentication tells the user what they are allowed to do. Answer: BExplanation:Identification is described as the claiming of an identity, and authentication is described as the act of verifying or proving the claimed identity. QUESTION 621A network administrator has a separate user account with rights to the domain administrator group. However, they cannot remember the password to this account and are not able to login to the server when needed. Which of the following is MOST accurate in describing the type of issue the administrator is experiencing? A. Single sign-onB. AuthorizationC. Access controlD. Authentication Answer: DExplanation:Authentication generally requires one or more of the following:Something you know: a password, code, PIN, combination, or secret phrase.Something you have: a smart card, token device, or key.Something you are: a fingerprint, a retina scan, or voice recognition; often referred to as biometrics, discussed later in this chapter.Somewhere you are: a physical or logical location.Something you do: typing rhythm, a secret handshake, or a private knock. Incorrect Answers:A: Authorization occurs after authentication, and ensures that the requested activity or object access is possible given the rights and privileges assigned to the authenticated identity. Authorization indicates who is trusted to perform specific operations.B: Auditing is generally used for compliance testing.D: Identification is the claiming of an identity, only has to take place once per authentication or access process. QUESTION 622A security technician is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the network technicians asks the security technician to explain the access control type found in a

firewall. With which of the following should the security technician respond? A. Rule based access controlB. Role based access controlC. Discretionary access controlD. Mandatory access control Answer: AExplanation:Rule-based access control is used for network devices, such as firewalls and routers, which filter traffic based on filtering rules. QUESTION 623During the information gathering stage of a deploying role-based access control model, which of the following information is MOST likely required? A. Conditional rules under which certain systems may be accessedB. Matrix of job titles with required access privilegesC. Clearance levels of all company personnelD. Normal hours of business operation Answer: BExplanation:Role-based access control is a model where access to resources is determines by job role rather than by user account. Within an organization, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Members or staff (or other system users) are assigned particular roles, and through those role assignments acquire the computer permissions to perform particular computer-system functions. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user's account; this simplifies common operations, such as adding a user, or changing a user's department. To configure role-based access control, you need a list (or matrix) of job titles (roles) and the access privileges that should be assigned to each role. QUESTION 624A company hired Joe, an accountant. The IT administrator will need to create a new account for Joe. The company uses groups for ease of management and administration of user accounts. Joe will need network access to all directories, folders and files within the accounting department.Which of the following configurations will meet the requirements? A. Create a user account and assign the user account to the accounting group.B. Create an account with role-based access control for accounting.C. Create a user account with password reset and notify Joe of the account creation.D. Create two accounts: a user account and an account with full network administration rights. Answer: BExplanation:Role-based Access Control is basically based on a user's job description. When a user is assigned a specific role in an environment, that user's access to objects is granted based on the required tasks of that role. The IT administrator should, therefore, create an account with role- based access control for accounting for Joe. QUESTION 625Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server? A. Common access cardB. Role based access controlC. Discretionary access controlD. Mandatory access control Answer: BExplanation:Role-based Access Control is basically based on a user's job description. When a user is assigned a specific role in an environment, that user's access to objects is granted based on the required tasks of that role. More free Lead2pass SY0-401 exam new questions on Google Drive:
https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E CompTIA SY0-401 is often called the hardest of all CompTIA exams. Lead2pass helps you kill the CompTIA SY0-401 exam challenge and achieve the perfect passing score with its latest practice test, packed into the revolutionary interactive VCE. This is the best way to prepare and pass the SY0-401 exam. 2017 CompTIA SY0-401 (All 1868 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]