

CompTIA Security + 4.0 Identity and Access Management

Filename: comptia-seclussy0501-4-2-identity_and_access_services

Title: Identity and Access Services

Subtitle: CompTIA Security+ (SY0-501)

4.2 Identity and Access Services

- 4.2 Given a scenario, install and configure identity and access services
 - LDAP
 - Bring up DC
 - Run netstat
 - X.500 Directory Services standard uses LDAP to access directory information
 - Kerberos
 - Explain TGT, Service Ticket
 - Port 88
 - CHAP
 - Handshake Process
 - PAP
 - Unencrypted authentication
 - MSCHAP
 - MSCHAP
 - MS implementation of CHAP used in Windows environments
 - Weak, feasible attacks with current hardware
 - Uses weak DES 56 bit encryption
 - MSCHAPv2
 - Implemented as PEAPv0/EAP-MSCHAPv2
 - Support
 - Apple, Microsoft, Cisco
 - RADIUS
 - Developed by Livingston Ent., Inc.
 - Show diagrams then explain
 - Connectionless services. Uses UDP
 - AAA implementation for dial-up users
 - PPP, PAP, CHAP, MSCHAP/v2 support
 - Port 1645/1812 for authentication messages
 - Port 1646/1813 for accounting
 - Client/Server model with NAS as RADIUS clients
 - Only passwords are hashed
 - TACACS+
 - Cisco proprietary
 - Connection-oriented using TCP
 - Controls access to network devices
 - Username, password, additional attributes can be encryption
 - SAML
 - XML-Based language to implement SSO
 - Allows for the exchange of user information for the purposes on authentication
 - OpenID Connect
 - Administration of many individual databases can be challenging
 - Allows Enterprises to use an Identity Provider(IdP) since millions are already in the IdP's databases
 - Applications can request identity information from the IdP
 - IdP's can issue a secure ID token to the application
 - Secure Token can be used in SSO throughout multiple applications
 - Secure Token = JSON Web Token allows claims to be encrypted, integrity protection and digitally signed
 - OAUTH (mentioned with OpenID Connect)
 - Show website <https://oauth.net/>
 - Shibboleth
 - Very common federated SSO implementation
 - Open source (Apache Software License)
 - Uses SAML
 - Versions
 - Shibboleth 1.0 (2003)
 - Shibboleth 2.0 (2005)
 - Shibboleth 3.0 (2006)
 - Secure token(mentioned with OpenID Connect)
 - NTLM