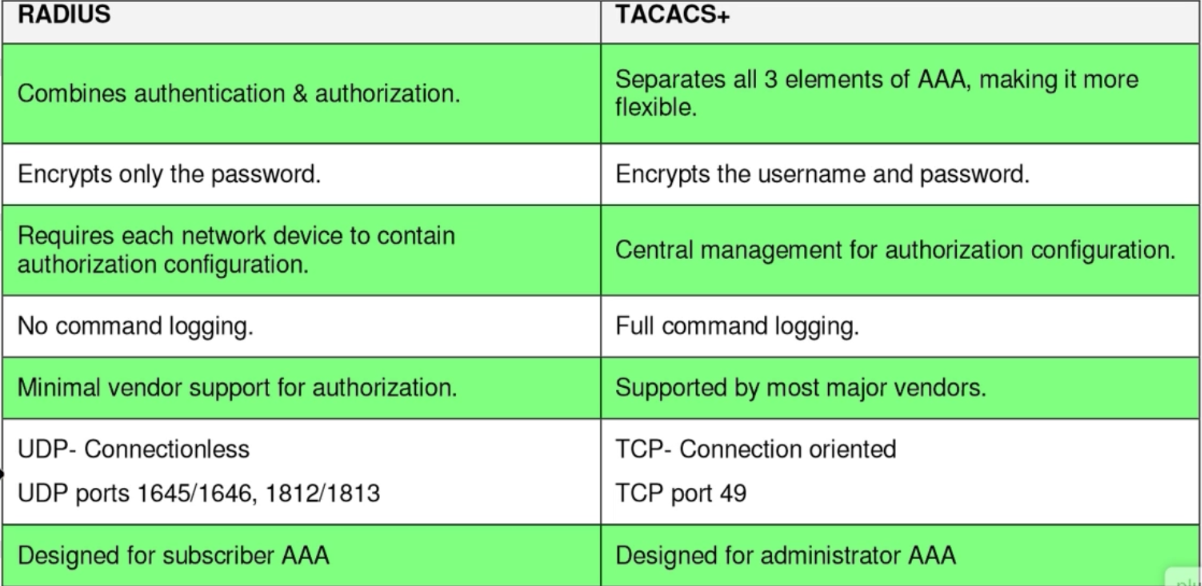
# CompTia Notes: Access Control and Identity Management

* Authentication Services
  + Authentication
    - Verify the user and control access to resources
    - Verify the identity of servers and resources being accessed
    - Provide Security for Data (CIA triad)
  + RADIUS
    - Remote Authentication Dial-in User Service
    - Provides AAA capabilities
      * Authentication
      * Authorization
      * Accounting
  + TACACS and XTACACS
    - Terminal Access Controller Access-Control System
    - Developing in 1984 for controlling access to MILNET
    - Not really used any more, replaced by XTACACS
      * Added AAA
      * Not backwards compatible from TACACS
  + TACACS+
    - Most common implementation
    - Runs on TCP over port 49
    - Encrypts entire communication
      * Not vulnerable to security issues associated with RADIUS
    - Separates authentication and authorization to more granular control



* + Kerberos
    - Network Authentication service
    - Used for mutual authentication between client/server
    - Key terms:
      * KDC: Key Distribution Center
      * AS: Authentication Service
      * TGT: Ticket Granting Ticket
      * GTS: Ticket Granting Service
      * Principle
      * Authenticator
  + LDAP
    - Lightweight Directory Access Protocol
    - Hierarchical in structure
    - CN: Common Name
    - OU: Organizational unit
    - DC: Domain Component
    - Port 389
  + Secure LDAP
    - LDAP over SSL/TLS
      * TCP port 636
      * Mitigates vulnerability of sending LDAP queries in clear text
  + SAML
    - Secure Association Markup Language
    - Authentication through a third party to gain access
    - The resource being accessed isn’t responsible for authentication
    - User authenticates to the 3rd party server and token is then passed to the original resource
* Authentication, Authorization, and Access Controls
  + Identification vs. Authentication vs. Authorization
    - Identification: Who you are
    - Authentication: Proving you are who you say you are
    - Authorization: Permissions
  + Identification
    - Biometrics
  + Personal Identification Verification Card
    - Smart card issued by U.S. Federal Government
    - Grant cardholder access to federal facilities
  + Username
  + Authentication
  + Tokens
    - Can identify and authenticate
  + Common Access Card
  + Multifactor Authentication
    - Two or more pieces needed to authenticate
    - Must be from different categories (password and pin both fall under something you know)
    - Password and RSA fob or password and code that gets texted to you
  + TOTP
    - Time based one-time password
  + HOTP
    - HMAC-Based One-time password
    - Hash Message Authentication Code algorithm
  + CHAP
    - Challenge handshake authentication Protocol
    - Used to authenticate PPP clients to a server
    - One-way hash based on shared secret (user’s pw) is compared on both client and server
    - Plaintext is never sent over the wire
  + PAP
    - Password Authentication Protocol
    - Not used anymore because username and pw is sent in plain text (vulnerable to wireshark)
  + Single Sign-on
    - Method of allowing users access to all resources they need within an environment with a single username and pw
    - Negates having to remember multiple usernames and pws
    - Mitigates risk by keeping users from writing down credentials
  + Access Control
    - Mandatory Access Control
      * Inflexible, rigid, most secure
    - Discretional Access Control
      * Flexible, dynamic access, least secure
    - Role-Based Access Control
      * Access based on role or group membership
    - Rule-Based access control
      * Access based on predefined lists
  + Implicit Deny
    - Used as a catch all stating if permission isn’t explicitly granted, then deny
  + Trusted OS
  + Authentication Factors
    - Something you know (password)
    - Something you have (smartcard, token generator)
    - Something you are (biometric)
  + Authorization
    - What you are allowed to access
  + Separation of Duties
    - Separate audit and logging responsibilities from the System Administrator
    - Keep System Administrator accounts limited
  + ACLS
    - Access control list
  + Mandatory Access Control
    - Pre-defined set of capabilities and access to information (who can share what to who)
    - Very rigid so must be very well thought out
    - Easy to spot breaches and deviations
  + Discretionary Access Control
    - Allows users to dynamically share information with others
    - Less secure and harder to control information leakage
  + Role Based and Rule based access control
    - Make sure to change a person’s access levels when they change roles
  + Time of Day Restrictions
  + Federation
    - Allowing access to company resources to outside parties
  + Transitive Trust/Authentication
    - One-way trust
    - Two-way trust
    - Non-transitive trust
    - Transitive trust
* Account Management Security Controls
  + Users with multiple accounts
    - Generally, don’t want a user to have to maintain different passwords across many different accounts
    - Mitigate by assigning one sign on that gives him permissions to other domains
  + Shared Accounts
    - Avoid if possible
  + Account Policy Management
    - Credential Management:
      * Have centralized account management repo
      * Credential managers to ensure they are encrypted
      * Encrypted connection when entering websites (SSL/TLS)
      * Enforce password rules to make them change every x number of days
  + Group Policy
    - Can be used to enforce password rules
      * Complexity
      * Expiration time
  + Password Complexity
    - Not so long or complex users need to write them down
    - Passphrases are often easier and just as secure
    - Enforce minimum length
    - Special chars
  + Expiration
    - Temp accounts should have expiration dates set when they’re created
    - Leave accounts intact, just disabled in case you need it later
  + Recovery
    - Can users recover their own passwords
    - Ensure security questions aren’t easily discovered via social engineering
    - Favorite dog, children’s name, favorite car, etc. should never be used
  + Disablement
    - Disable instead of delete accounts to preserve security ID’s and in case they are needed later
  + Lockout
    - Lock a user’s account have x number of incorrect attempts to log in
    - Lockout duration should be long enough to discourage brute force
  + Password History
    - How many passwords are remembered and if a use is ever allowed to reuse old passwords
    - Set a minimum amount of time before a user can change password is useful to prevent a user from quickly cycling through password history requirement
  + Password Reuse
  + Password Length
  + Generic Account Prohibition
  + Group Based Privileges
    - Users gain/lose permissions automatically based on group membership
    - Access management becomes very difficult at scale
    - Avoid explicitly denying permission when possible (might come in handy later, makes troubleshooting difficult)
  + User Assigned Privileges
    - User assigned privileges are harder to manage
    - Difficult to troubleshoot when issues arise
    - Better to manage at the group level
  + User access reviews
    - Periodic auditing of user rights to ensure least privileges
  + Continuous Monitoring
    - Check access times, successful and failed access
    - Check time of day, length of connection for irregularities
    - What types of resources are being accessed
    - If people are aware they are being monitored it will cut down on attempted attacks
    - Alerts/triggers can automate the process and make sure you are consistent across the board