Identification, Authentication and Authorization

- Password Authentication Protocol
  - Clear text exchange of username and password
  - Don't ever use this
- File permissions (Windows)
  - NTFS
  - Active Directory allows more granular control
  - Utilization of inheritance is essential for scalable and efficient setting of permissions
  - If file or directory is moved in the same drive, permissions are maintained. Otherwise you lose permisions
- Authorization Model
  - Mandatory Access Control
    - Based on labels. Depending on level of clearance you can read certain levels information
  - Discretionary Access Control
    - Owner defines access to item
    - Does not account for Roles
  - Role based Access Control
    - Depending on job, you will get specific rights and privileges.
- Permissions
  - Administrators assign
  - Usually group based
- Rights
  - Something applied to the system itself as a whole
  - Windows: Configured under group policy
- File Permissions (Linux)
  - Basic Model
    - R = Read, W =Write, X = Execute
      - Execute allows execution of scripts and programs, and the ability to change directories
      - Read allows to read a file and view content of a directory
      - Write allows modification, addition, and deletion of files
    - Each of the three 'UGO' groups have very distinctive permission
    - U =Users, G = Group, O = Other,
  - passwd
    - Change user password
  - chown
    - Change ownership of file or directory
    - Requires super user permissions
  - chmod
    - EX: chmod 777 gives full access to target file or directory
    - 4 = read, 2= write, 1 = execute
    - EX: chmod 733 gives full access to user/owner and only write and execute permissions to group and other
    - Command allows user to change permissions on the basis of the above model
- NT LAN Manager
  - Used when authenticating without domain controller
  - Each side has challenge message
- Kerberos
  - Domain Controller is Key Distribution Center
  - Once authenticated ticket granting ticket is issued (SID)
  - Ticket granting service generates session key which allows access to one set of resources
- Security Assertion Markup Language
  - Used in web applications for authentication
- LDAP
  - Port: 389
  - Language model for accessing other users directories and files
- Challenge-Handshake Authentication Protocol
  - First utilized method of ensuring protection in authentication process
  - Works by sending key hash and challenge question to user
  - User then sends hashed answering gets authenticated
- Base Concepts
  - Least Priviledge
  - Something you do
    - EX: Keyboard typing rythm
    - Some security controls can be used to figure out if actions are being performed outside of a normal pattern
    - Principle where users are given the least amount of rights and permissions to do there job
  - Something you have
    - Keys
      - RSA: Stores a token that changes within a given interval
    - ID cards
  - Something you are
    - Biometrics
      - Fingerprint scanners
      - Retinal scans
      - Facial recognition
  - Something you know
    - PIN
    - Captcha Portal
    - Security Questions
    - Username and Passwords
- Terminal Access Controller Access-Control System Plus
  - Takes care of authorization process a lot better than RADIUS
  - Real time authorization monitoring
  - Port: 49
- User Account Management
  - Default Credentials
    - Never use these
  - Group policy Objects
    - Used in Windows Active Directory
    - Can be applied to domains
    - Allows granular control of account rights and prvileges
  - Multiple Accounts
    - Don't user same password for two accounts
    - Least Privilege is key
    - Don't user Privileged account to do normal work
  - Continous Monitoring
    - Login/ Logout
    - File Access
  - Local security policy
    - Passwords
      - Password age
      - Length
      - Account lockout policy
  - Shared Accounts
    - Wtf?..?
    - Just don't do it... like ever
- Geotagging
  - Credit card companies will usually block payments that are way outside the proximity of your billing location
  - Websites may perform additional challenges if login is performed outside of normal proximity
- Remote Authentication Dialing User Service
  - Doesn't do much for authorization
  - Server stores a bunch of user names and passwords
  - RADIUS client is the gateway.
  - Supplicant is the client trying to get authenticated
  - Used for network access
    - Ports: 1812, 1813, 1645, 1646