



سبر 1213  
Network Defense

Lecture #2 Part 3  
Understanding Identity and Access Management

# Role-Based Access Control

Roles Based  
on Jobs and  
Functions

- Administrators
- Executives
- Project Managers
- Team Members

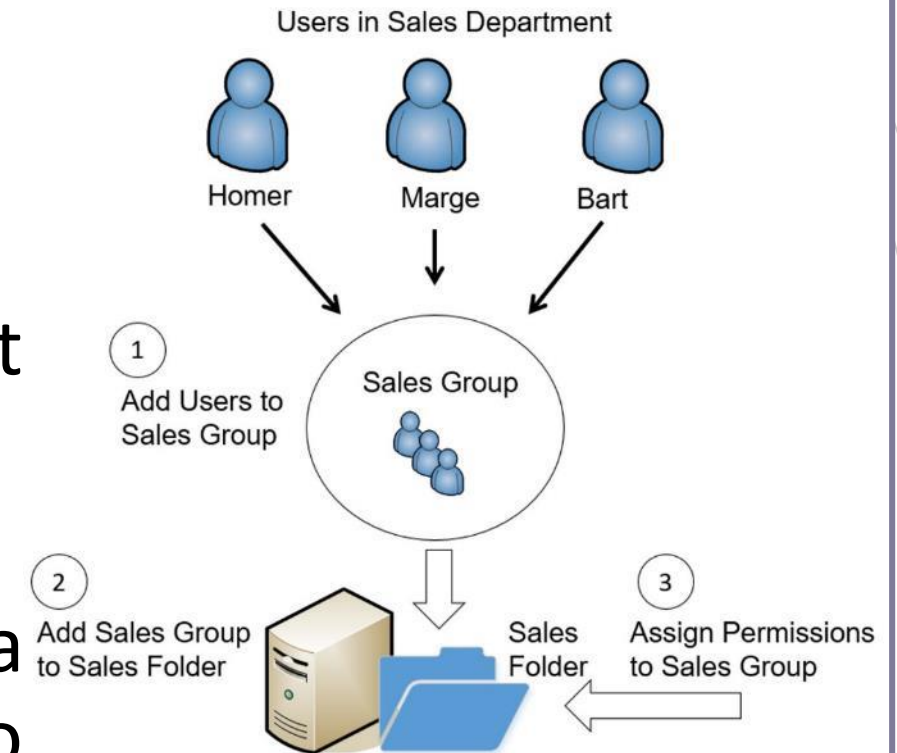
Can be

- Hierarchy-based
- Job-, task-, or function-based



# Group-Based Privileges

1. Create a Sales group and add each of the user accounts to the Sales group
2. Add the Sales group to the Sales folder
3. Assign appropriate permissions to the Sales group for the Sales folder



# Rule-Based Access Control

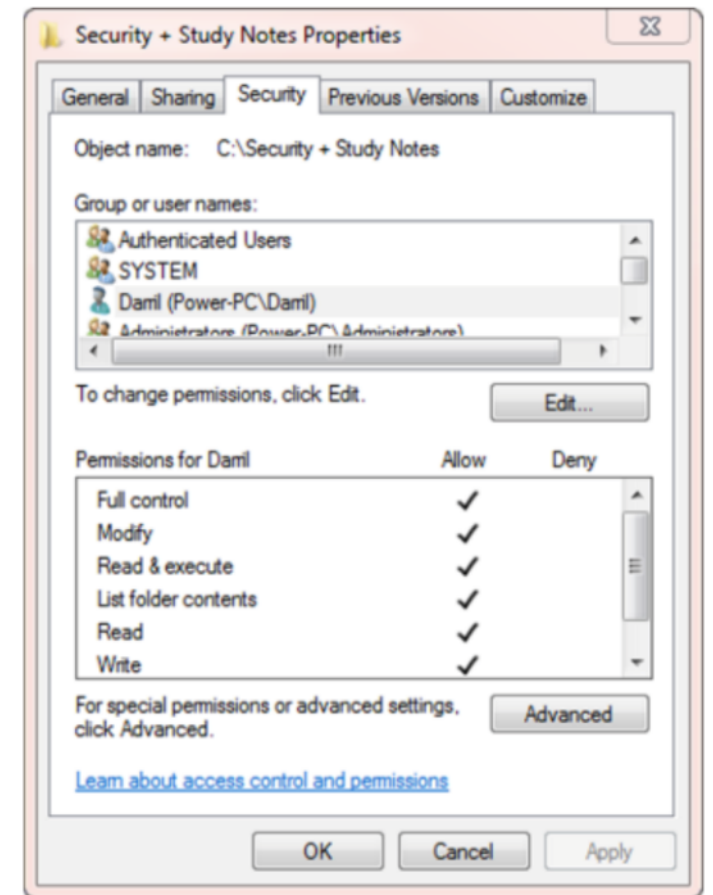
- **Rule-Based Access Control**
  - Based on a set of approved instructions, such as an access control list
  - Can use triggers to respond to an event

# Discretionary Access Control

- **Resources identified as objects**
  - Files, folders, shares
- **Specifies that every object has an owner**
- **Owner has full, explicit control of the object**
- **Beware of Trojans**
  - Dual accounts for administrators

# Discretionary Access Control

- **Filesystem Permissions**
  - Write
  - Read
  - Read & execute
  - Modify
  - Full control
  
- **SIDs and DACLs**





# Mandatory Access Control

- Uses labels to determine access
- Subjects and objects are assigned labels
- Permissions granted when the labels match
- SELinux (Security-Enhanced Linux)
  - Uses MAC model
  - Helps prevent malicious or suspicious code from executing

# Mandatory Access Control

- **Lattice**

Nuclear Power Plant	007	Happy Sumo	←	Top Secret Level
Research	Three-Eyed Fish	Legal Issues	←	Secret Level
Payroll	Budget	Safety Issues	←	Confidential Level
Training	Job Openings	Holidays	←	For Official Use Level

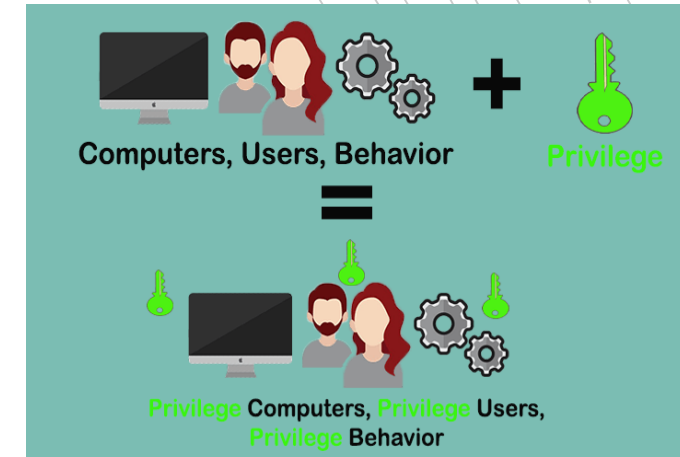


# Attribute-Based Access Control

- **Commonly used in SDNs**
- **Evaluates attributes and grants permissions based on attributes**
- **Often implemented with plain language policy statements**
- **Policy statements typically include four elements**
  - Subject
  - Object

# Conditional Access

- User or group membership
- IP location
- Device



# Chapter 2 Summary



- **Exploring Authentication Management**
- **Managing Accounts**
- **Comparing Authentication Services**
- **Comparing Access Control Schemes**
- **Check out the free online labs**

# End of Part Three