Section 3: Identity and Access Management

31. Identification

For the Sec+ need to know the difference between:

```
1. Identification: Proves who I am to the Authetication System
2. Authentication: Me proving that I have rights to the system (e.g. Passwords, SmartCards, etc)
3. Authorization: What rights do I have to the system once i've been authenticated
```

Authentication Factors (These and their examples will be on the Sec+)

```
1. Something you know **Knowledge factors**  (Password, pin codes, Captcha, Security Questions)

2. Something you have **Possession factors** (Smart card, RSA Key)

3. Something about you **Inherence factors** (e.g. Biometrics)

4. Something you Do **Location Factors** (e.g. Rythmn of typing)

5. Somewhere you are **behavior-based**  (e.g. Your credit card knows you've purhased something in alabama vs. ohio)
```

Federated Trust: If one system trusts you, all the systems trust you (Sets up facinatingly in Windows Active Directory)

*Multifactor Authenication

Quick Review:

-Authentication requires sharing of something you know, something you have or something you do
-A smartcard is an example of something you have, security questions are an examples you know
-Federated system trust is inherited from a different trusted system

---

32.Authorization Concepts

1. Permissions: (What are the things that are assigned to you that you can do?)
    1. Administrators Assign permissions
2. Rights (and privledges): (Something we assign to systems as a whole)
3. Lease Privledge and Separation of duty
    1. Lease privledge - (Give the users the least amount of privledge they need)
    2. Separation of duties - (One person does one thing so they have privledge for that thing, and another person does another thing so they get privledges for that other thing)

Quick Review:

-permissions are applied to resources
-Two authorized strategies: Lest priviledged and spearation of duties
-Rights and privilages we tend to assign at system level

33.Access Control List

Authorization Models
MAC (Mandatory Access Control)
-MAC
-List
-e.g. When government information is "Top Secret"

```
DAC (Discredtionary Access Controls)
        -DAC
        -Owner of the data defines access


RBAC (Role-Based Access Control)
        -RBAC
        -Access to resources is defined by set of rule
        -Groups
```

**Any good access control list is going to have an "Implicit Deny" (Definition: Unless you specifically allow something to happen, it wont happen.)

Quick Review:

Remember - Understand that anything need to control access will have some kind of access control list
- The type of ACL is going to be controlled by the resource itself
- In any specific case an implicit deny is going to be there
- Access is defined by ACLs
- Implicit deny prevents access unless specifically permitted
- ACLs manifest in many different ways

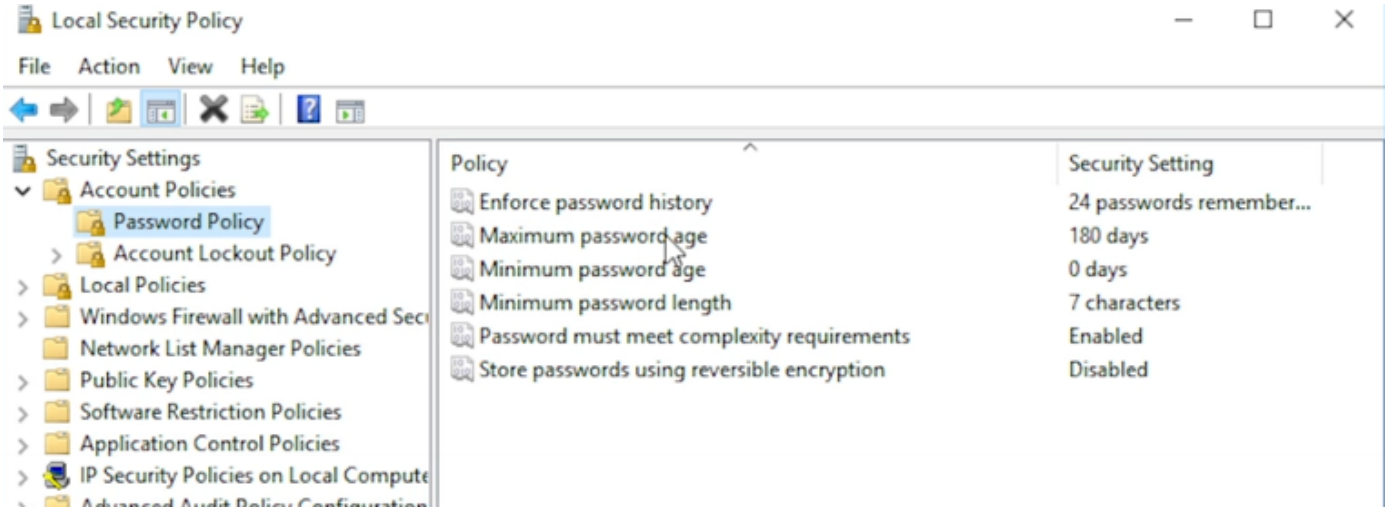
34.Password Security

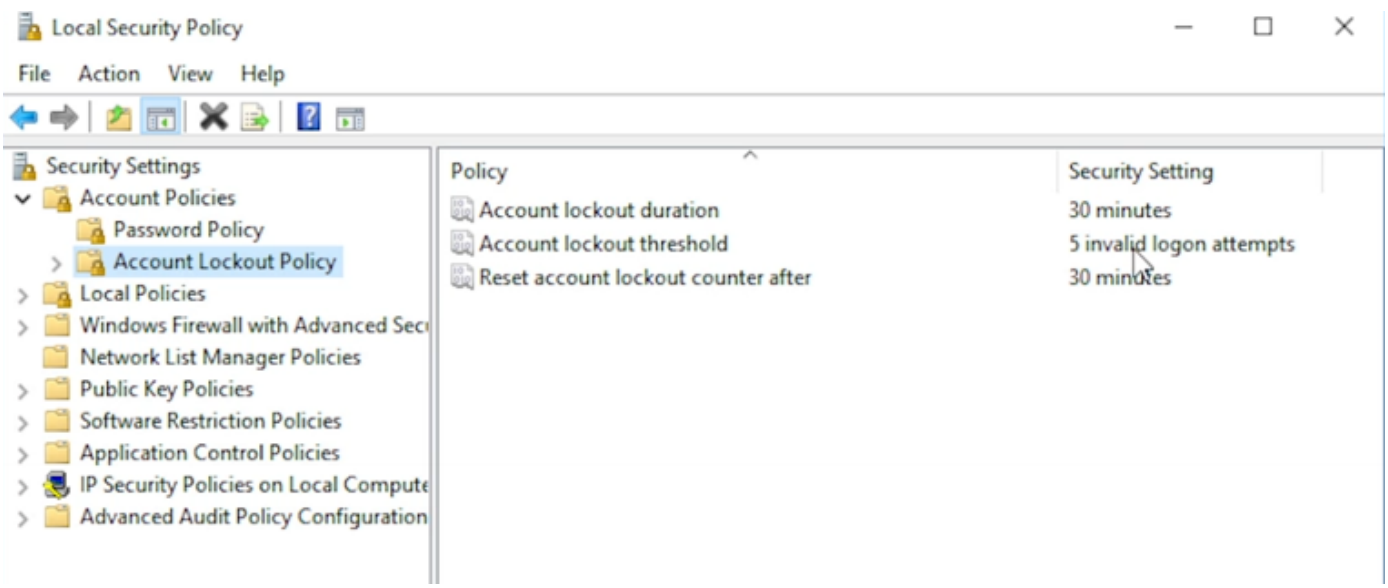
Good Security Policies:

```
1. Complexity
        1. Length and character requirements
2. Expiration
        1. Reset and time triggers
3. Password History
        1. Reusage and retention
```

Local Security Policies:

1. Example: Windows Local Security Policy



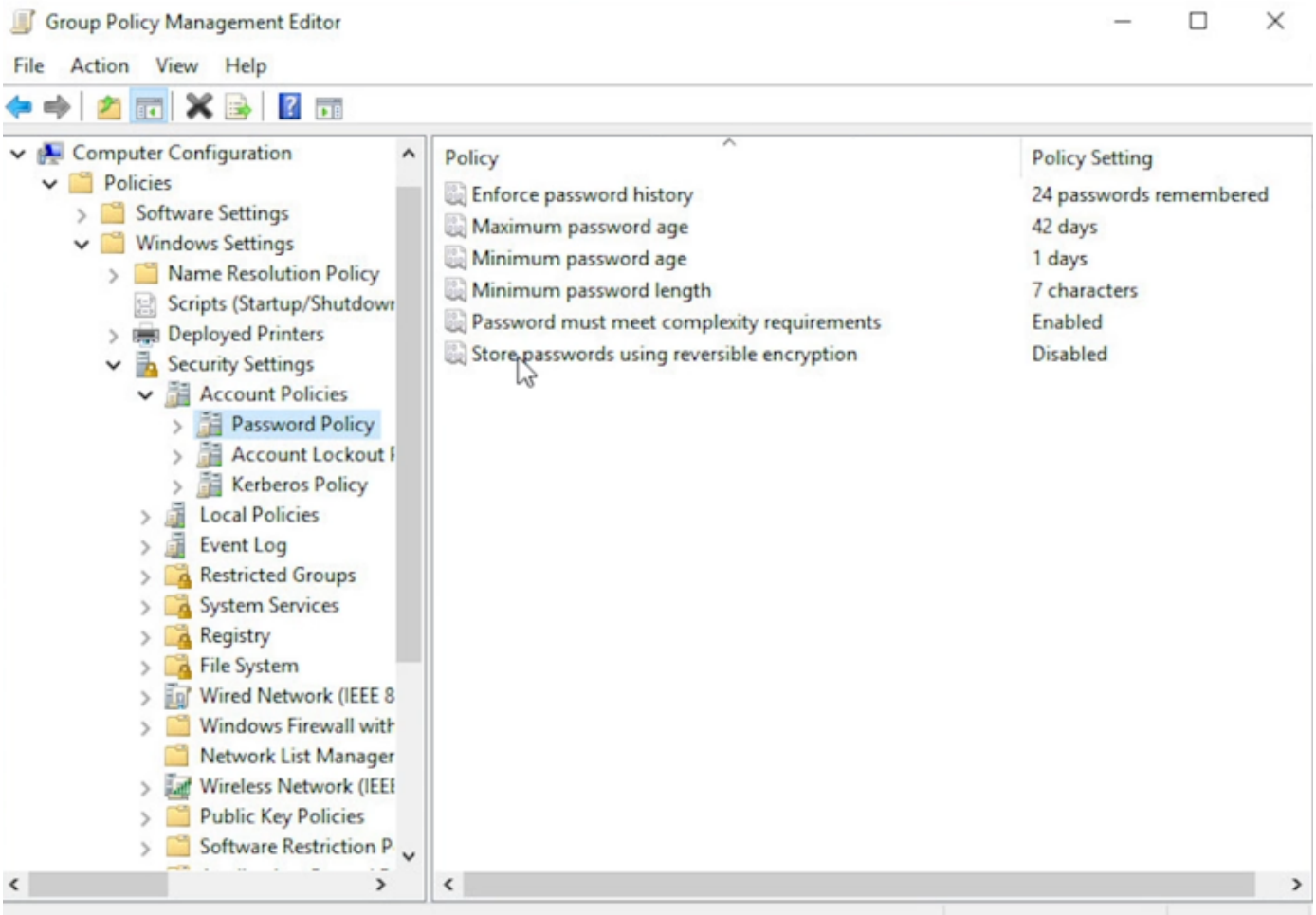


Group Policy Objects (Need a server and active directory (Windows))

Nearly Identical to Local Security Policies (Individual Machines) Except:

1. They Can be applied to:
    1. Domains
    2. Individual sites
    3. Groups
    4. Organizational Units

    **Group Policy objects can apply to an entire directory



Quick Review:

Remember:
- Windows Group Policy Objects
- Establish a good security Policy by using complexity, age, and password History
- Windows local security policy can help you with the complexity of your passwords
- Group policy objects can apply over multiple domains, groups, and OU's

---

35. Linux File Permissions

Command: ls -l (e.g. drwxrwxrwx)

R:
File: Open a file
Directory: View Contents
W:
File: Write/Edit a file
Directory: Add or Delete Files
X:
File: Run a file/script
Directory: Allows you to cd to a different directory

```
1. d=directory, f=file
2. First three rwx apply to the Owner/Creator
```

3. Second three rwx apply to the Group
4. Third three rwx apply to "Other"

chmod: Change Mode

e.g. --> chmod o= FileName (Give Other Group zero permissions)
e.g. --> chmod g=rx FileName (No Read/Write permission to the group)
e.g. --> chmod a=rwx FileName (gives all full permissions away)

Better way to do Chmod (Below)

OCATAL	BINARY	PERMISSIONS
0	000	---
1	001	--x
2	010	-w-
3	011	-wx
4	100	r--
5	101	r-x
6	110	rw-
7	111	rwx

r - 4
w - 2
x - 1

e.g. --> chmod 777 FileName (Everybody gets rwx permissions)
e.g. --> chmod 760 FileName (Owner gets full rwx, Group gets rw-, Everyone else gets zero permissions)

Who Owns a Particular file ---> **chown (Change Owner)**

e.g. sudo chown NewOwner FileName ---> sudo chown root File.pdf

Changing a Password **passwd**

e.g. sudo passwd

Quick Review:

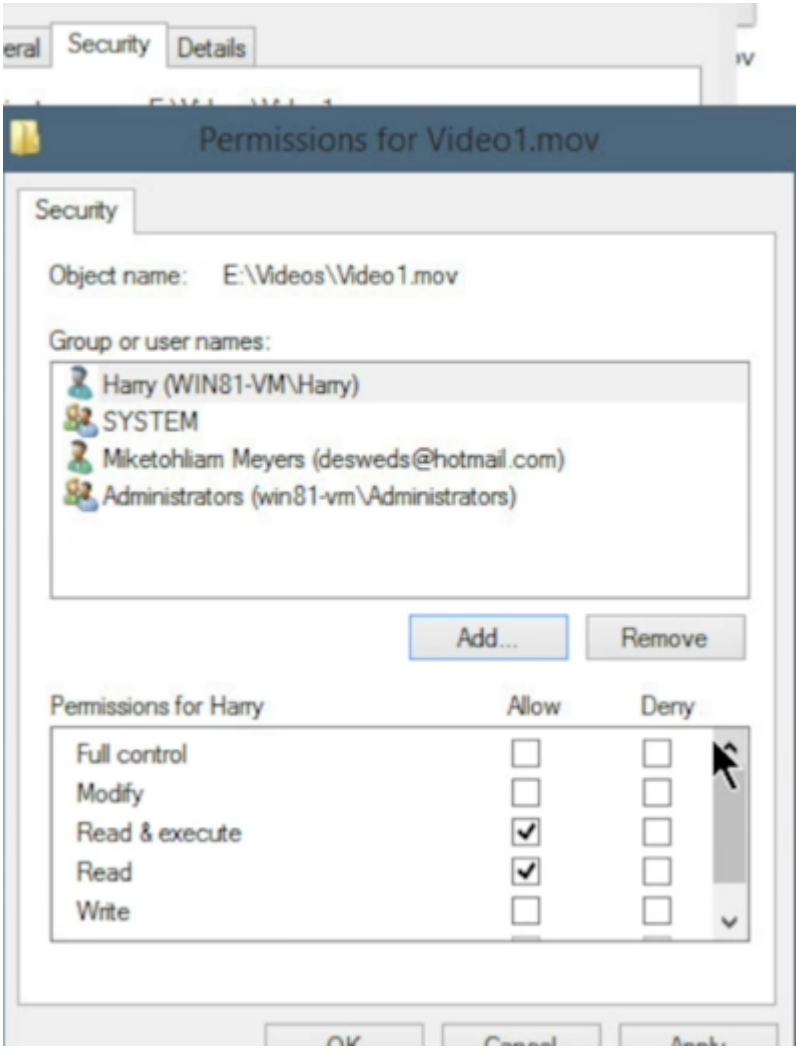
-Linux has three permissions: Read, Write, and Execute, which cna be set for the Owner, Group, or Other
-Use chmod to change permissions
-chmod and passwd both require SUDO user

---

36. Windows File Permissions

NTFS Permissions:

1. Full Control
    1. File - Can do anything
    2. Folder - Can do anything you want
2. Modify
    1. File - Read, Write and delete that file
    2. Folder - Read, Write and Delete Files and Subfolders within that folder
3. Read/Execute
    1. File - Open and Run the file
    2. Folder - See Content and Execute
4. List Folder Contents
    1. Folder - See Contents of Folders and Subfolders
5. Read
    1. File - Open the File
    2. Read - View contents and open Data Files
6. Write
    1. File - Open and write to the file
    2. Read - Write to Files and Create New Files and Folders



Create users, put users into groups, and give groups NTFS Permissions.

Inheritance: When you set any one object with specific permissions anything else you put into that gets the same permissions.

If you dont want inheritance: Click edit and Click Deny checkboxes. DENY BUTTON TURNS OF INHERITANCE.

Copying and Moving NTFS Objects:

1. When copying from one drive to another, the contents will take on the NTSF properties of the destination drive
2. When Moving from one drive to another, the contents will take on the NTSF properties of the destination drive
3. When you copy to a new place on the same drive the new contents will lose the NTSF properties of the original content.
4. When you move to a new place on the same drive the **contents will keep the same NTSF properties**

Quick Review:
Remember:
- Know different permissions
- Know what happens when you move and copy

- NTFS permissions are granted to users and groups on folder and files
- Permissions inherit from folders into the files and folders beneath it
- Copying and moving NTFS objects have different effects on NTFS assignments

---

37. User Account Management

1. Continuous Monitoring
    1. Track log on/off activity
    2. Track File Access
2. Shared Accounts
    1. Shared accounts are **bad**
    2. Don't do shared accounts
3. Multiple Accounts
    1. Use different Usernames and Passwords
    2. Monitor which users belong to which groups
    3. Use least privledge - enough necessary to accomplish a task
    4. Monitor and log activity of users with multiple accounts
4. Default and Generic Usernames/accounts
    1. Don't use. Delete them if possible
    2. Always use dedicated service accounts

*MEMORIZE THE ABOVE
Quick Review:

- You should monitor all user account activity
- Shared account are OK at home, but not at work
- When using multiple accounts use different usernames and passwords

---

38. AAA

AAA (Authentication, Authorization, Accounting)

1. RADIUS (Remote Authentication Dial-In User Service) - Serious authentication for a WIRELESS network.
    1. Dial-in networking
        1. RADIUS SERVER (Bunch of Usernames/Passwords)
        2. RADIUS CLIENT (The Gateway between what we are trying to get authenticate from and those who are trying to get authenticated)
        3. RADIUS SUPPLICANT (Whoever/Whatever is trying to get Authenticated)
    2. The Process:
        1. The Supplicant goes to the client

2. The client knows the IP of the radius server and send the supplicants credendials to the server
3. The radius server decides whether that supplicant can be authenticated or not

Remember:

1. Radius is used for network access
2. Radius can use up to 4 different UDP ports
1. 1812
2. 1813
3. 1645
4. 1646

*Downside to Radius is that it doesn't really handle authorization

2. TACACS+ (Terminal Access Controller Access- Control System Plus)
    1. Really good at managing a bunch of devices (e.g. routers, switches, people access those routers and switches and stuff etc)
    2. Really takes care of authorization really well (Leg up on Radius)
        1. Decouples Authenication from authorization (Defines if you are in and what you can do when you are in)
    3. TACACS+ uses TCP port 49

*BOTH TACACS+ and RADIUS do auditing for log files

QUICK REVIEW

- Radius uses ports 1812, 1813, 1645, 1646
- TACACS+ uses port 49
- Radius is used for wireless authentication and network access
- AAA stands for Authentication, Authorization, and Accounting

---

39. Authentication Methods

1. PAP (Password Authentication Protocol) - old
    1. PAP sends username and password from client to servier in the clear (Unprotected)
2. CHAP (Challenge-Handshake Authentication protocol) - old - uses hashes to authenticate
    1. Server and Client already have a stored key
    2. When the server gets a request for authentication it creates a challenge message and then creates a hash of the key
    3. Sever sends the hash and the challege message to the client
    4. client generates a hash and sends it back to the server
    5. Through comparing hashes they confirm if they have the same key.
3. NTLM (NT LAN Manager) - Somewhat modern
    1. Client and server both have a stored key

    2. Each side has a challenge message
    3. Challenge messages are hashed and sent to each other
    4. They verify the they have the same key
4. Kerberos -
    1. Only used in authenticating to windows domain controllers
    2. Client, File server, and in the middle is a domain controller
    3. In Kerberos the Domain Controller is known as the *KDC (Key Distribution Center)*
        1. Authentication Service
        2. Ticket Granting Service
        3. TCP/UDP Port 88
    4. The client does an initial login to the domain
    5. KDC gives the client a TGT (Ticket Granting Ticket)
        1. TGT shows that the client is authenticated to the domain (TGT also known as SID (Security Identifier))
    6. Client takes TGT back to domain controller except this time to the ticket granting service.
    7. KDC Ticket granting service generates a session key for the client
    8. Session key allows the client to go to a particular place on the server. If they want to go somewhere else a new session key is generated
5. SAML (Security Assertion Markup Language)
    1. Not really an authentiation method
    2. Used exculsively for web applications
6. LDAP (Lightweight Directory Access Protocol)
    1. Not really an authentication method
    2. A structured language that allows one computer to go into someones directory and query it and update it, etc.
    3. Uses TCP/UDP port 389

Quick Review:
- Kerberos is used to authenticate to Windows Domain Controllers
- LDAP uses TCP and UDP port 389
- LDAP is not so much authentication as a structured language to query directories

---

40. Single Sign-On

1. SSO on a LAN
    1. Windows Active Directory
    2. Need a copy of Windows server
    3. Establish a domain

4. All the computers join the domain via an adminitrator going to each computer to do this creating a trust system (aka Federated System)

2. SAML (Security Assertion Markup Language)
    1. Lots of little devices with Web apps to control them
    2. Need to get to these devices securely
    3. SAML is designed for web apps, and allows a single person to sign in to a bunch of different places at once.

    The process:
    1. Client Signs into an Identity Provider
    2. Web apps are all called Service Providers
    3. Identity provider gives the client with a token to access all of the service providers

REMEMBER:

For exam:

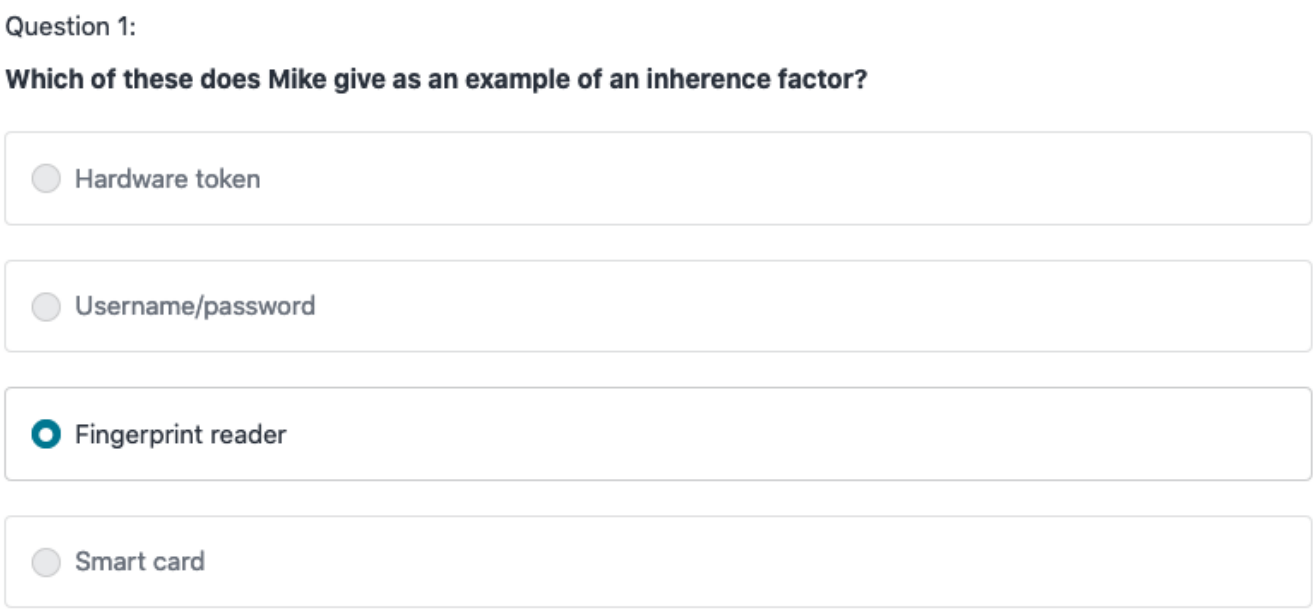
- LAN: Windows Active Directory
- SCADA or things that are all over the place: SAML

Quick Review:

- For Local Area Networks, use Windows Active Directory to Single Sign-On
- SAML is used to manage multiple apps using a single account

---

QUIZ QUESTIONS



Question 2:

Which type of access control is based on data labels?

- DAC
- MAC
- RBAC
- HMAC

Question 3:

What determines the number of times you can unsuccessfully attempt to log in before you are shut out of the system for a specified period?

- Local Security Policy
- Maximum password age
- Account lockout duration
- Account lockout threshold

Question 4:

In Linux file permissions, which action does the letter "r" allow?

- Open a file
- Edit a file
- Run a file or execute a program
- None of the above

Question 5:

True or false: Mike says shared accounts are a good idea in an Enterprise environment.

- ○ True
- ◉ False

Question 6:

What is the RADIUS supplicant?

- ◉ The system trying to authenticate
- ○ The system checking the authentication
- ○ The system acting as the gateway
- ○ The connection between the gateway and the system checking the authentication

Question 7:

Using Kerberos, what is the domain controller called?

- ○ PAP
- ○ CHAP
- ○ Gateway
- ◉ Key distribution center

Question 8:

Which of these is a tool you could use to set up single sign on within a LAN?

- SAML
- Windows Active Directory
- SAMBA
- VPN