User Management

Group 7 / Week 4

User
management

Members

Sebastian Onnagan

Raph Kenneth Zambrona

Alejandro Cruz

Rommel Tommas

Group 7 / Week 4

Introduction to User Management

User management is the process of controlling and organizing how people access and use a computer system. It is important because it ensures security, makes work easier, and helps keep data safe.

User Accounts

What they are: user accounts are digital identities that allow people to log in and use a computer or network. Each account has its own settings, files, and permissions.

Types of Accounts

Local Account	Exists only on one computer. Your account has your own files, your own settings (like wallpaper or apps), and your own access rights.
Domain Account	Used in organizations, managed by a central server for multiple computers.
Standard Account	Regular users with limited permissions.
Administrator Account	Has full control over the system, including installing software and changing settings.

Why Accounts Matter

User accounts are important because they help protect the system from unauthorized access, keep personal data separate, and allow administrators to control what users can and cannot do.

Definition of Groups

A group in user management is a collection of user accounts that are managed together as a single unit.

- Users = individual accounts
- Groups = container of users for easier management

Types/Examples of Groups

- **Administrators Group** – has full control over the system (can install software, manage users, change settings).
- **Students Group** – limited access, can only use learning resources.
- **HR Group** – access to employee records and HR tools.
- **Finance Group** – access to financial data and accounting systems.

Relation of Groups to User Accounts

- A **user account** represents an individual person or computer in the system.
- A **group** is a collection of user accounts**.**
- **Users** are added to **groups** so that permissions and policies can be applied to many users at once.
- A **single** user account can belong to one or multiple **groups.**
- **Groups** act like a shortcut: **instead of giving rights to each user** one by one, the administrator gives them to the **group,** and all **users** in it inherit those rights.

Permissions in User Management

- Key part of access control.
- Protects systems, files, and data.
- Helps ensure only the right people do the right tasks.

What are Permissions?

- Rules that define what actions users can perform.
- Used to control access to files, folders, and applications
- Prevents unauthorized users from reading or changing data.

Types of Permissions

- **Read - View or open files.**
- **Write - Create, edit, or delete files.**
- **Execute - Run programs or scripts.**

Principle of Least Privilege

- Users should only get the access needed for their role.
- Prevents misuse, accidents, or attacks.
- Example: A cashier doesn’t need admin rights on the company server.

Real-World Example

- Student Can only read study materials.
- Teacher Can read and update lesson files
- Admin IT Full control read, write, execute.
- More privileges = higher responsibility and risk

Security Policies
&
Active Directory

Rules & Guidelines for protection

✓ Password Rules

✓ Lockout

✓ Multi-Factor Authentication

Importance of Security Policies

📂 **Protect Data & Systems**

⚠️ **Prevent Threats**

🤝 **Build Trust**

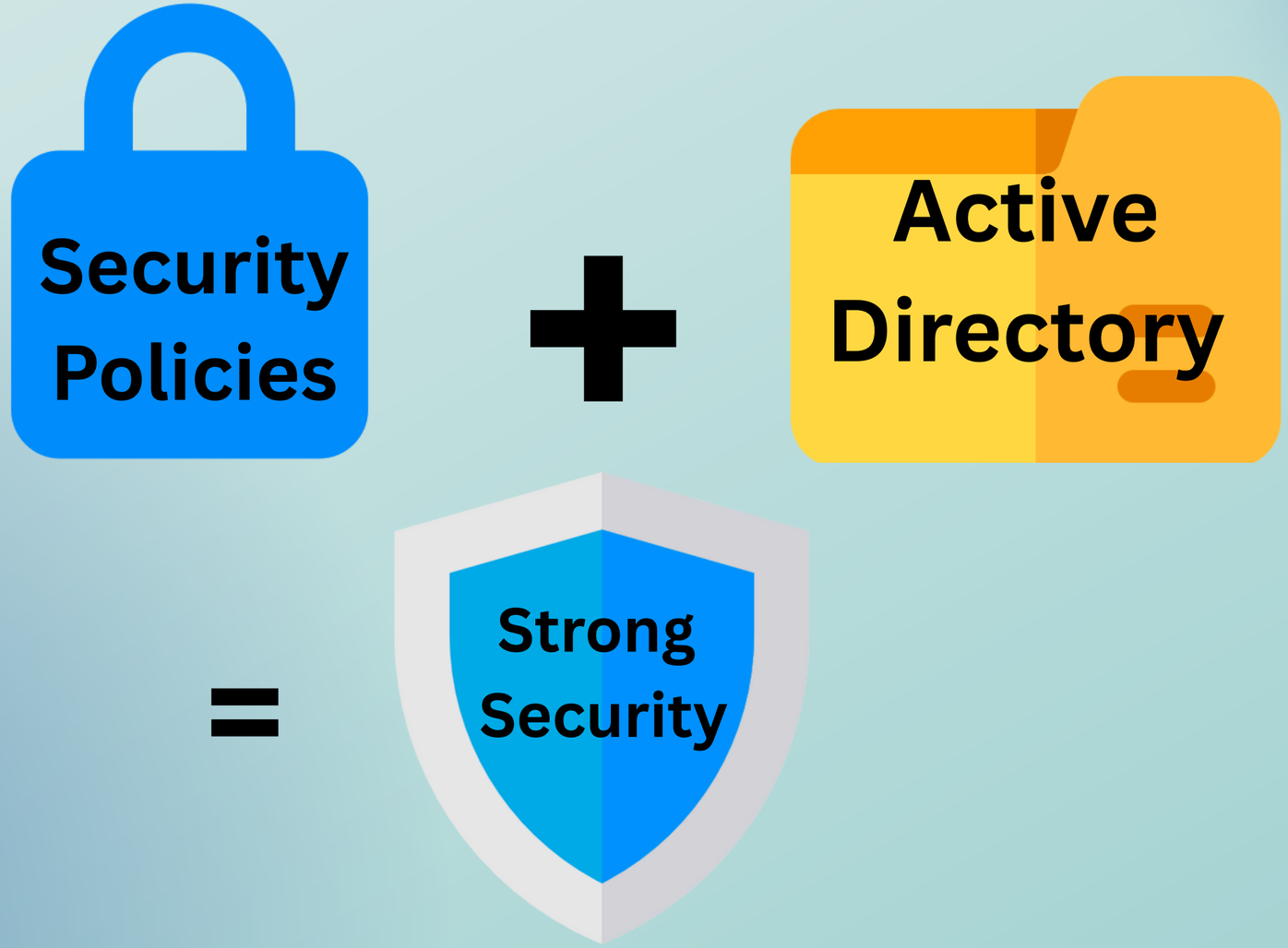
Active Directory (AD)

Centralized Management

Accounts & Group Policies

Authentication & Authorization

Connection & Conclusion



Thank you for listening!