Microsoft® Official Course

Module9

Implementing Security in Windows Server

Microsoft®

Module Overview

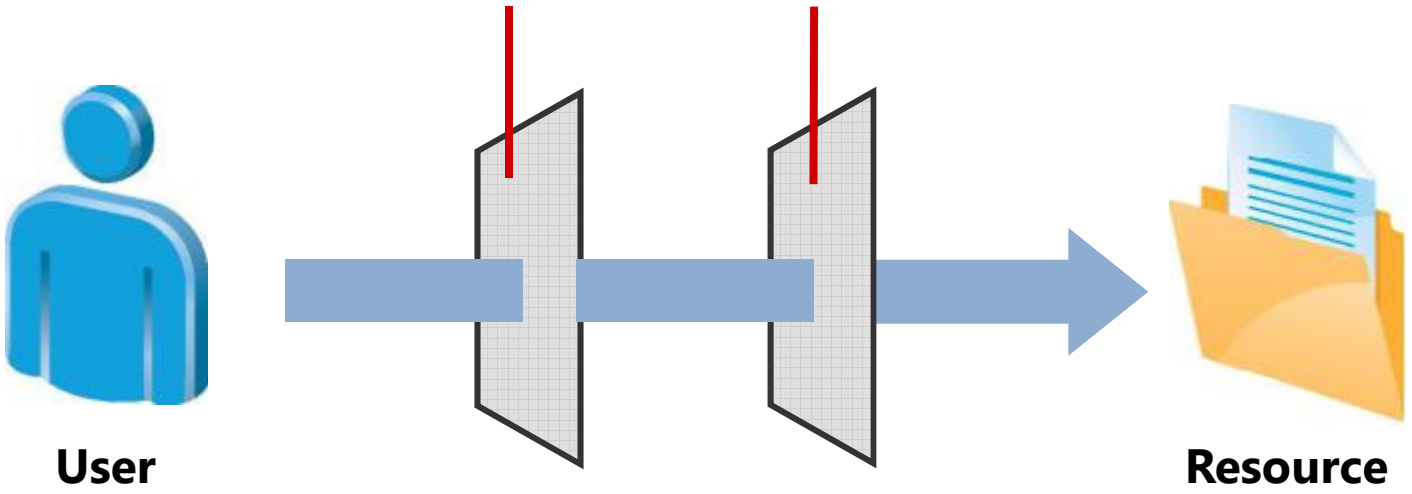
- Overview of Windows Security
- Securing Files and Folders
- Implementing Encryption

Lesson 1: Overview of Windows Security

- What Is Authentication and Authorization?
- What Is User Access Control?
- File and Folder Permissions
- Account Policies
- Fine-Grained Password Policies
- Auditing Features
- Digital Certificates

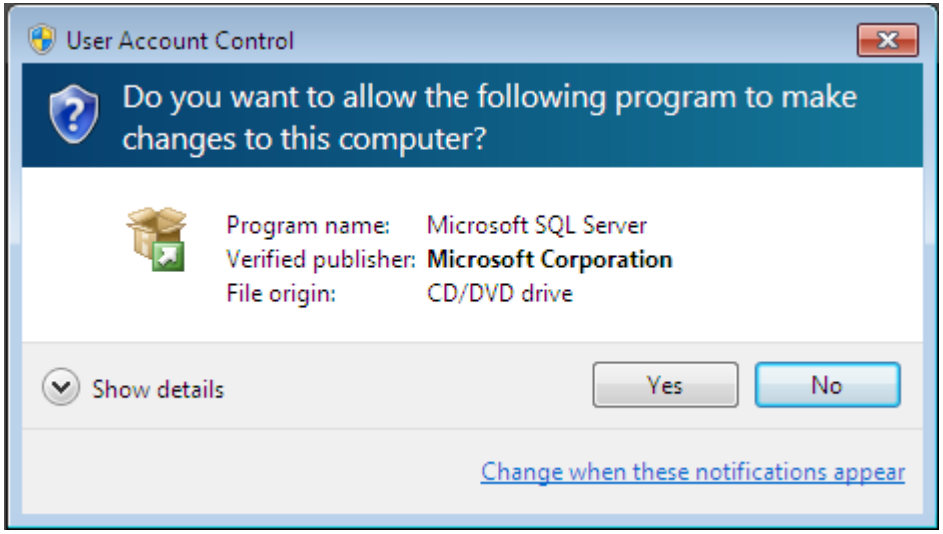
What Is Authentication and Authorization?

Authentication	Authorization
Who are you? Verifying the identity of something or someone	What level of access should you have? Determining whether something or someone has permission to access a resource



What Is User Access Control?

- UAC is a security feature that simplifies the ability of users to run as standard users and perform all necessary daily tasks
- UAC prompts the user for an administrative user's credentials if the task requires administrative permissions



File and Folder Permissions

- File and folder permissions:
  - Available with NTFS or ReFS
  - Define local access rights for files and folders
  - Always apply
- Shared folder permissions:
  - Available with FAT32, NTFS, and ReFS
  - Define network access rights for folder contents
  - Only apply when files and folders are accessed over the network
- Dynamic Access Control
  - Builds on file, folder, and share permissions
  - Uses centrally defined policies for more granularity

Account Policies

Account and password policies help to mitigate the threat of unauthorized account access

Policies	Default Settings
Password Controls complexity and lifetime of passwords	• Complex Password: enabled • Enforce password history: 24 • Maximum password age: 42 days • Minimum password age: 1 day • Minimum password length: 7 characters • Store password using reversible encryption: disabled
Account Lockout Controls how many incorrect attempts can be made	• Lockout threshold: 0 invalid logon attempts • Lockout duration: not defined • Reset account lockout after: not defined

Fine-Grained Password Policies

- Fine-grained password policies allow for assigning multiple password and account lockout policies to individual Active Directory users or groups within the same domain
- Fine-grained password policy components:
  - Password Settings Container
  - Password Settings objects

Auditing Features

- Auditing tracks user and operating system activities, and records selected events in security logs, such as:
  - What occurred?
  - Who did it?
  - When?
  - What was the result?
- Enable auditing to:
  - Detect threats and attacks
  - Determine damages
  - Prevent further damage

Digital Certificates

- Digital certificates use asymmetric encryption
- Digital certificates bind a *public* key to an entity that holds the corresponding *private* key
- A digital certificate typically contains:
  - Information about the owner
  - The owner's public key
  - Information about the issuer
  - Issue and expiry date of the public key
  - Serial number of the digital certificate
  - Digital signature of the issuer

Lesson 2: Securing Files and Folders

- Access Control
- File and Folder Permissions
- Permissions Inheritance
- Shared Folder Permissions
- Evaluating Combined, Shared, and Local Permissions
- Demonstration: How to Secure a Shared Folder
- File and Folder Auditing
- Demonstration: How to Configure File Auditing
- Dynamic Access Control

Access Control

- Access control entry (ACE)
  - Single entry
  - Allowing or denying access to a specific user, group, or computer
- Discretionary access control list (DACL) and system access control list (SACL)
  - Made up of ACEs
  - Is the entire permission set for a particular object and defines who can access it and how

File and Folder Permissions

- Deny permissions override Allow permissions

Standard Permissions	Advanced Permissions
• Full Control • Modify • Read & Execute • List Folder Contents • Read • Write • Special Permissions	• Full Control • Traverse Folder/Execute File • List Folder/Read Data • Read Attributes • Read Extended Attributes • Create Files/Write Data • Create Folders/Append Data • Write Attributes • Write Extended Attributes • Delete Subfolders and Files • Delete • Read Permissions • Change Permissions • Take Ownership • Synchronize

Permissions Inheritance

- Inheritance is used to manage access to resources without assigning explicit permissions to each object
- By default, NTFS permissions are inherited in a parent/child relationship
- Blocking:
  - Stops a folder from inheriting parent permissions
  - Can be performed at the file or folder level
- When moving and copying, remember:
  - Relocating folders and files can change permissions
  - Moving files can have different results than copying files

Shared Folder Permissions

- Shared folder permissions apply only to folders shared on the network
  - Read
  - Change
  - Full Control
- Combine with NTFS permissions to determine the level of access allowed when a folder is accessed over the network
- Can use File and Storage Services to create and manage shares in Windows Server 2012

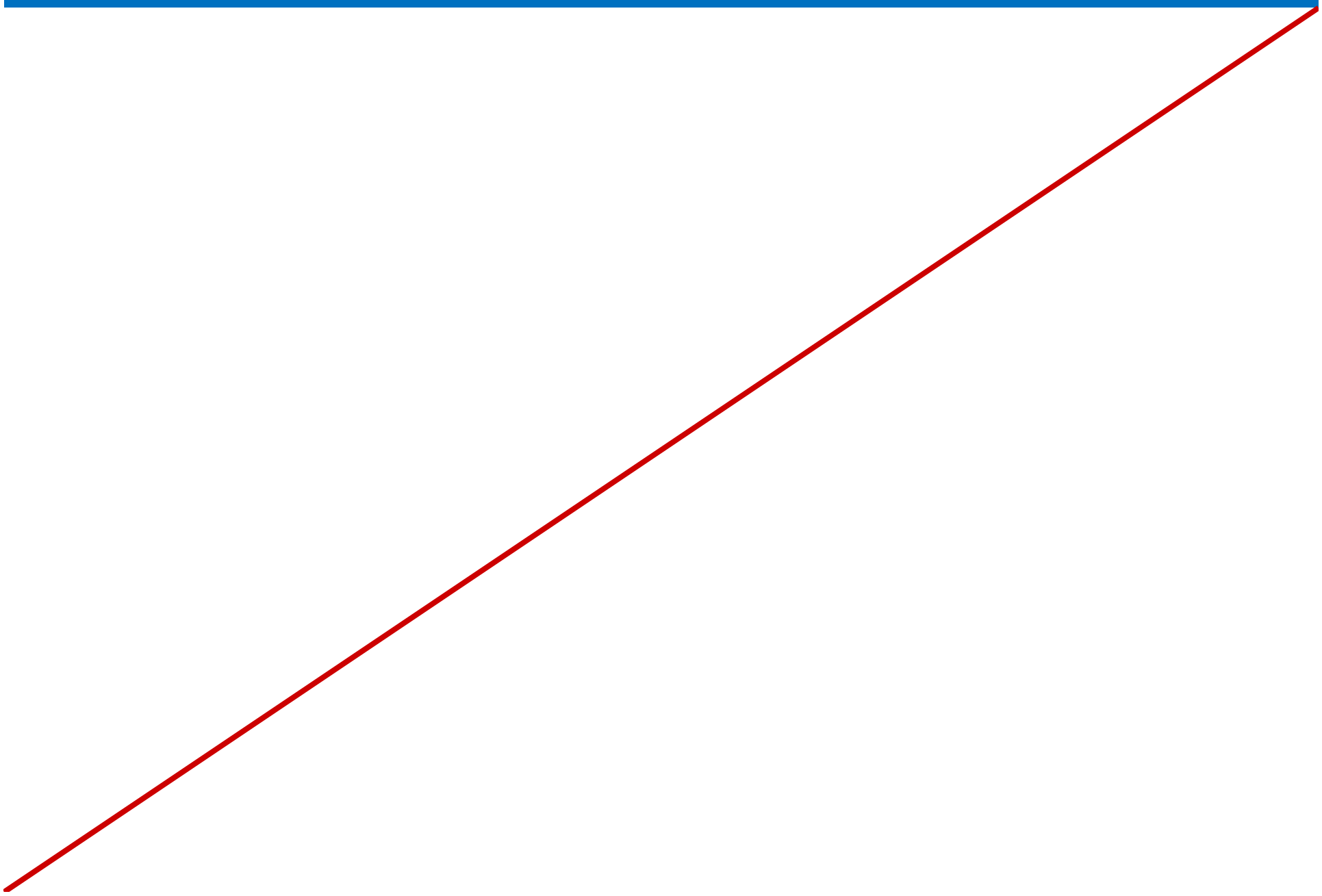
Evaluating Combined, Shared, and Local Permissions

- When you create a shared folder on an NTFS-formatted partition, both the shared folder permissions and the NTFS file system permissions are combined to secure file resources
- Combining NTFS and shared folder permissions results in the most restrictive effective permissions of the two permission sets
- Applies to all files in that folder, and to all files in subfolders

Demonstration: How to Secure a Shared Folder

- In this demonstration, you will see how to create, secure, and share a folder

Notes Page Over-flow Slide. Do Not Print Slide.



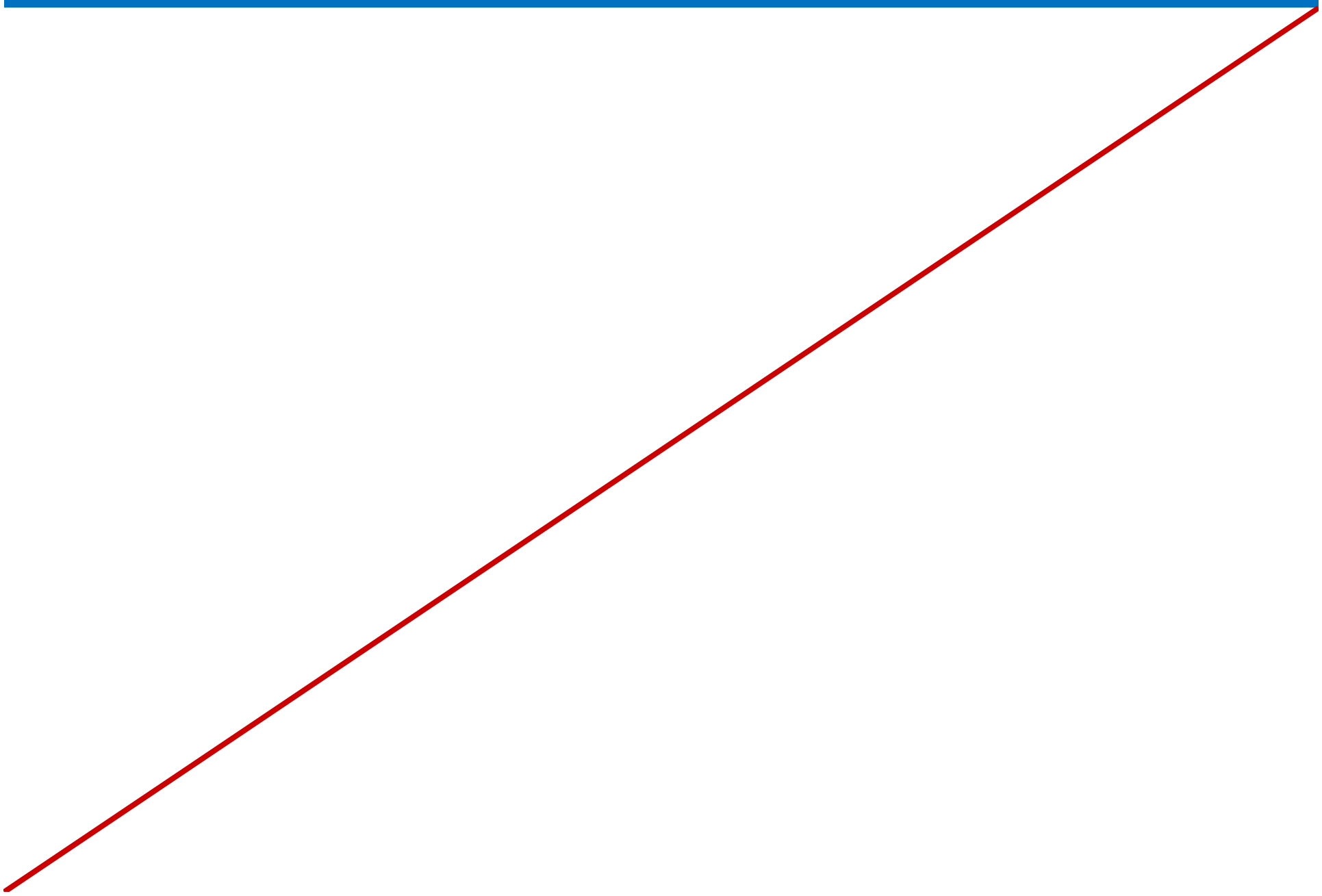
File and Folder Auditing

- File auditing allows you to:
  - Track the use of permissions to access files and folders
  - Determine who has modified files or folders
  - Ensure that file and folder permissions are working
  - Prevent continued unauthorized access to resources
  - Provide reporting on file and folder usage
- Two components to successful auditing
  - Enabling auditing for the area on the server
  - Configuring SACLs on the resources to be audited
- Auditing must be enabled for any files or folders you want audited

Demonstration: How to Configure File Auditing

- In this demonstration, you will see how to enable and then test file auditing

Notes Page Over-flow Slide. Do Not Print Slide.



Dynamic Access Control

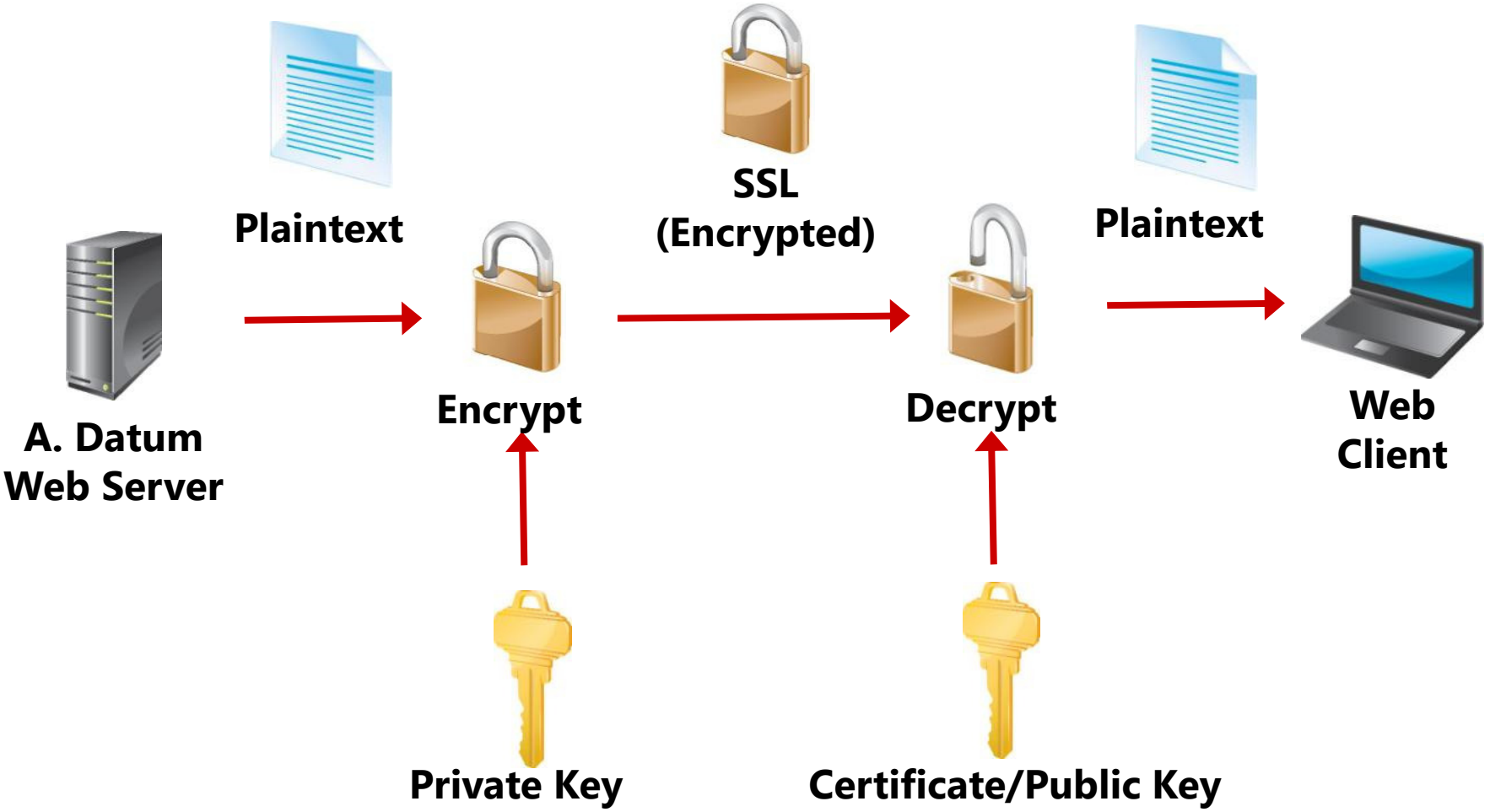
- Dynamic Access Control provides:
  - A Data access control mechanism on data within an organization.
  - An additional layer of access protection control on top of NTFS
  - Can create Central access rules and policies to apply across your organization
  - More granular control over resource access. i.e. can be at attribute level; Full Time employee, location, department etc

Lesson 3: Implementing Encryption

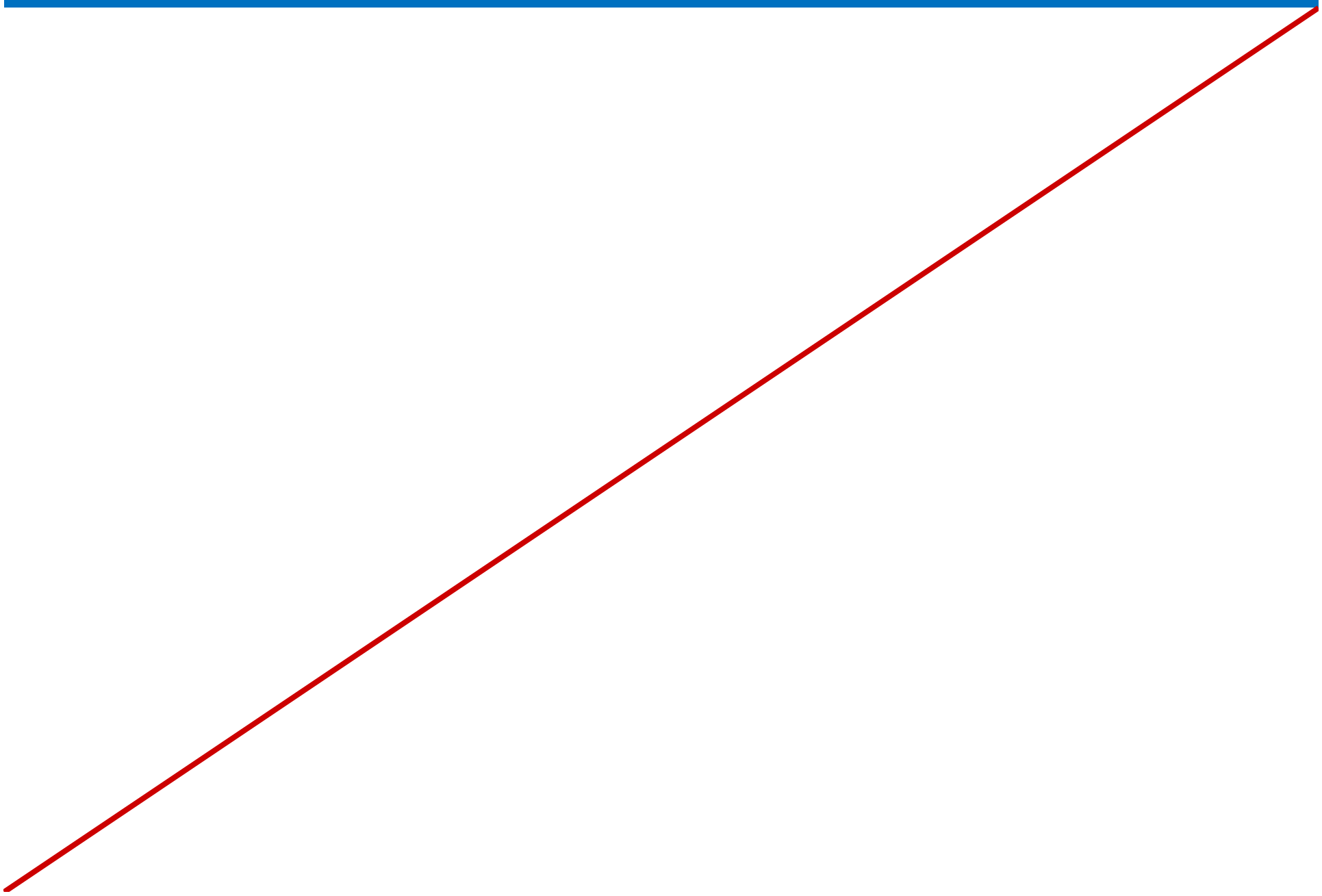
- How Are Digital Certificates Used?
- Encrypting File System
- BitLocker Drive Encryption
- BitLocker and EFS Comparison

How Are Digital Certificates Used?

- Different keys are used to encrypt and decrypt the message



Notes Page Over-flow Slide. Do Not Print Slide.



Encrypting File System

- Encrypting File System (EFS) is a file and folder encryption technology
  - Is supported on NTFS volumes only
  - Enables transparent file and folder encryption and decryption
  - Uses public-key and symmetric-key encryption

- Implementation
  - Enabled by default; no administrative intervention required to enable it
  - Can disable via Group Policy
  - Can share files that have been encrypted

BitLocker Drive Encryption

- BitLocker provides for disk, volume, and start up protection:
  - Provides data encryption protection
  - Verifies the integrity of the startup process
  - Can encrypt removable media by using BitLocker To Go

- Installation:
  - Installed as feature in Windows Server 2012 via Server Manager
  - Configurable through Group Policy
  - Installed and configured by using Windows PowerShell

BitLocker and EFS Comparison

BitLocker	EFS
Encrypts entire drives and volumes	Encrypts individual files or folders
Implemented for all users or groups	Implemented by individuals
Enabled by the administrator	Enabled by the user
Requires TPM for full functionality	Does not require special hardware
Does not require user certificates	Requires user certificates
Support for ReFS	No support for ReFS
Windows PowerShell cmdlets available	No dedicated Windows PowerShell cmdlets

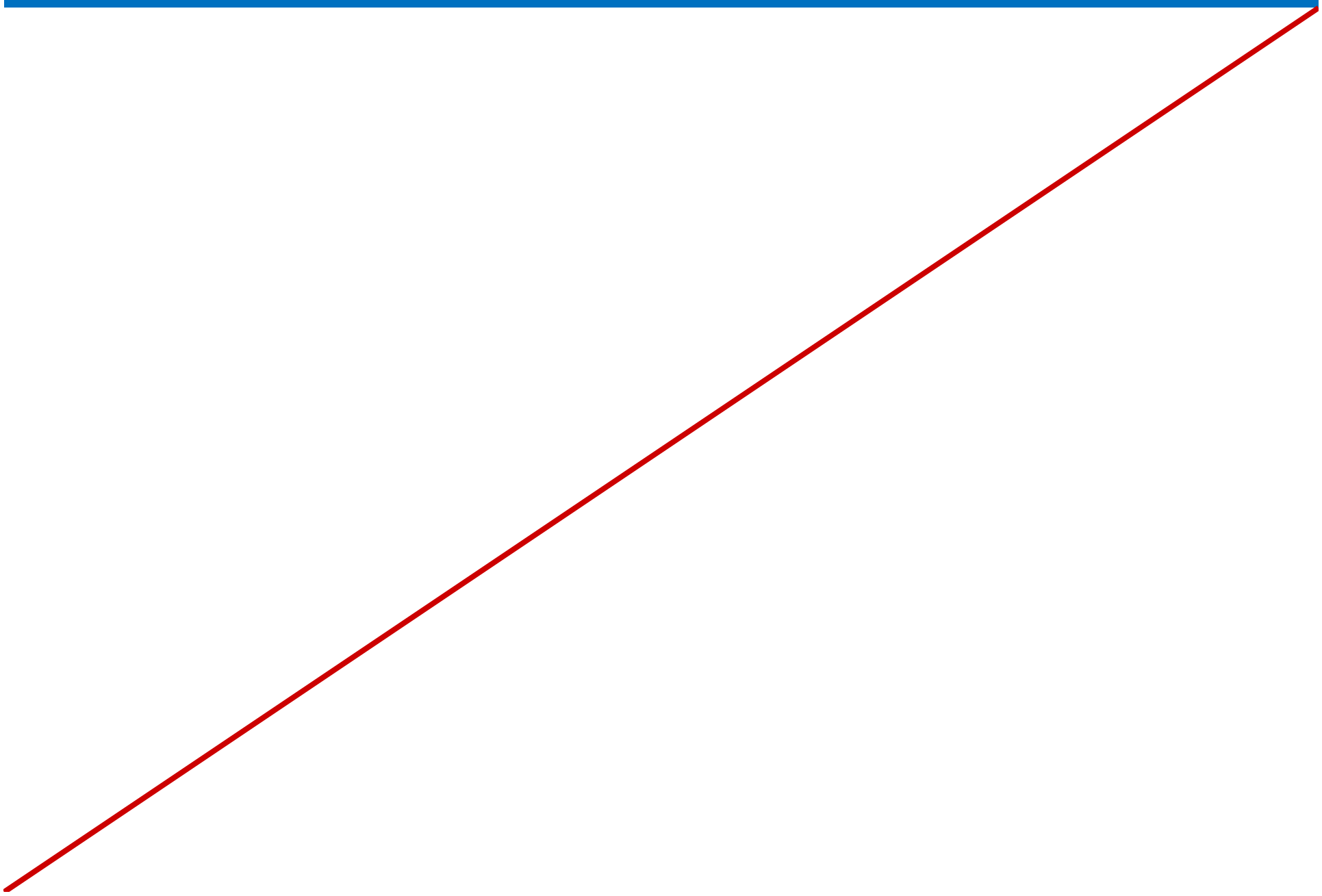
Lab: Implementing Security in Windows Server

- Exercise 1: Configuring a Fine Grained Password Policy
- Exercise 2: Securing NTFS Files and Folders
- Exercise 3: Encrypting Files and Folders

Logon Information
Virtual Machines: 10967A-LON-DC1, 10967A-LON-SVR1 and 10967A-LON-CL1
User Name: ADATUM\Administrator
Password: Pa$$w0rd

Estimated Time: 60 minutes

Notes Page Over-flow Slide. Do Not Print Slide.



Lab Scenario

You are asked to implement a stricter password policy for the Research group in order to meet the requirements of new A. Datum company security policies to ensure the integrity of the companies intellectual property.

You have also been asked by your supervisor to create a shared folder structure on LON-SVR1 that satisfies the Research team's request for access.

And, on LON-SV1, specific files containing sensitive information in the Classified subfolder of the new Research shared folder should be encrypted to prevent unauthorized access. You have been asked to test encryption on the Classified folder.

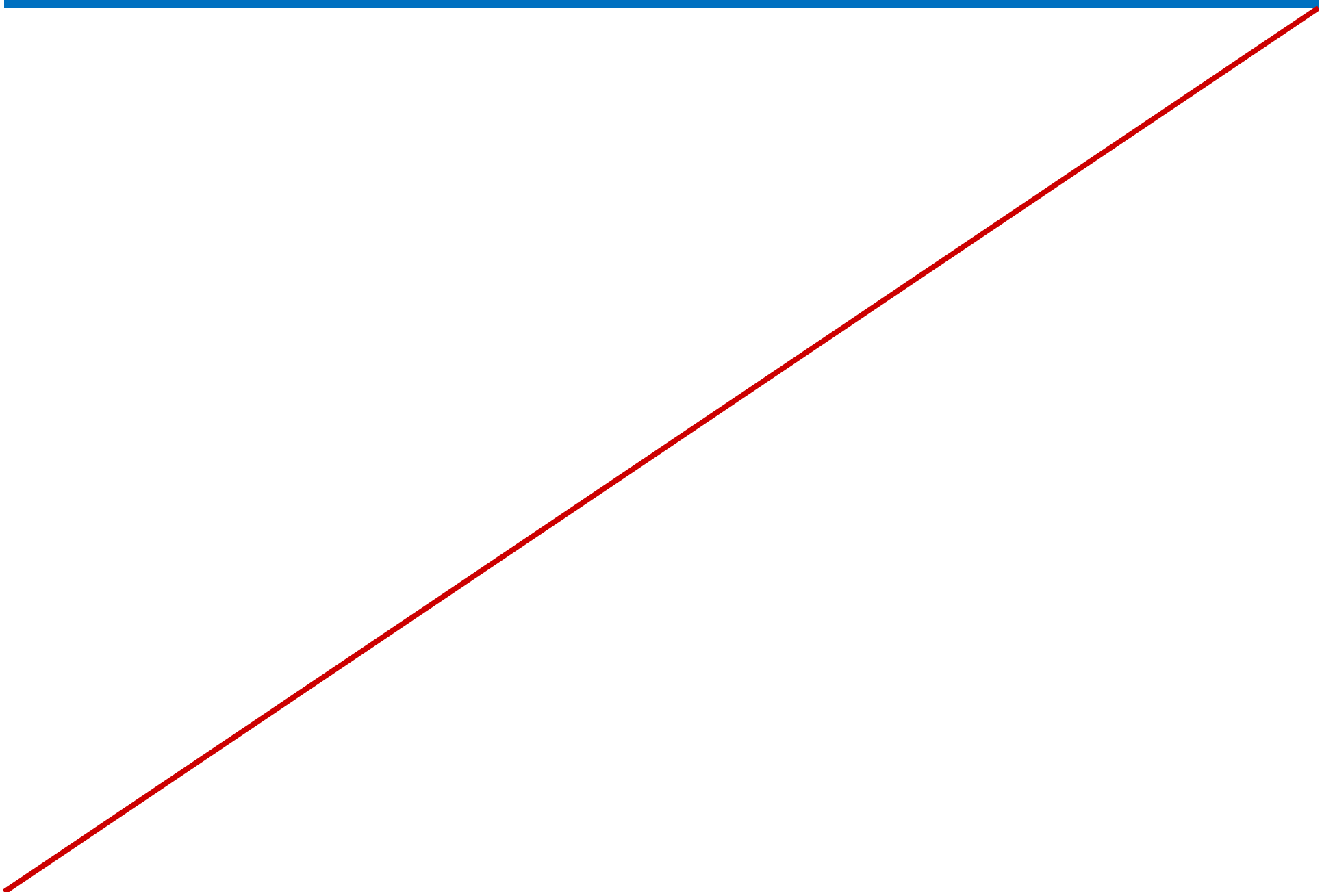
Lab Review

- What is the most efficient way to give several users who all require the same permissions access to a shared folder?
- What are some of the ways of protecting sensitive data in Windows Server?

Module Review and Takeaways

- Tools
- Best Practices

Notes Page Over-flow Slide. Do Not Print Slide.



Notes Page Over-flow Slide. Do Not Print Slide.