Understanding Authentication, Authorization, and Accounting

Lesson 2

Objectives

Skill/Concept	Exam Objective	Objective Number
Starting Security with Authentication	Understand user authentication	2.1
Introducing Directory Services with Active Directory	Understand user authentication	2.1
Comparing Rights and Permissions	Understand permissions	2.2
Understanding NTFS	Understand permissions	2.2
Sharing Drives and Folders	Understand permissions	2.2
Introducing the Registry	Understand permissions	2.2
Using Encryption to Protect Data	Understand encryption	2.5
Understanding IPsec	Understand protocol security	3.3
Introducing Smart Cards	Understand user authentication	2.1
Configuring Biometrics, Windows Hello, and Microsoft Passport	Understand user authentication	2.1
Using Auditing to Complete the Security Picture	Understand audit policies	2.4

AAA

- AAA (Authentication, Authorization, and Accounting) is a model for access control.
  - ***Authentication*** is the process of identifying an individual, usually based on a username and password. After a user is authenticated, users can access network resources based on the user's authorization.
  - ***Authorization*** is the process of giving individuals access to system objects based on their identity.

Accounting

- ***Accounting***, also known as ***Auditing***, is the process of keeping track of a user's activity while accessing the network resources, including the amount of time spent in the network, the services accessed while there and the amount of data transferred during the session.

Nonrepudiation

- *Nonrepudiation* prevents one party for denying actions they carry out.
- If you have established proper authentication, authorization and accounting, a person cannot deny actions that they carried out.

Login

- A login is the process that you are recognized by a computer system or network so that you can begin a session.
- A user can authenticate using one or more of the following methods:
  - What a user knows such us a using a password or Personal Identity Number (PIN).
  - What a user owns or possesses such as a passport, smart card or ID-card.
  - What a user is usually using biometric factors based on fingerprints, retinal scans, voice input or other forms.

Multifactor Authentication

- When two or more authentication methods are used to authenticate someone, you are implementing a ***multifactor authentication*** system.
- Of course, a system that uses two authentication methods such as smart cards and a password can be referred to as a two-factor authentication.

Password

- The most common method of authentication with computers and networks is the password.
- A ***password*** is a secret series of characters that enables a user to access a file, computer, or program.
- A ***personal identification number (PIN)*** is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system.

Digital Certificate

- The digital certificate is an electronic document that contains an identity such as a user or organization and a corresponding public key.
- Since a digital certificate is used to prove a person's identity, it can be used for authentication.

Smart Card

- A ***smart card*** is a pocket-sized card with embedded integrated circuits consisting of non-volatile memory storage components, and perhaps dedicated security logic.
- They can contain digital certificates to prove the identity of someone carrying the card and may also contain permissions and access information.
- Since a smart card can be stolen, some smart cards will not have any markings on it so that it cannot be easily identified on what it can open.
- In addition, many organizations will usually use a password or PIN in combination of the smart card.

Security Token

- A ***security token*** (or sometimes a hardware token, hard token, authentication token, USB token, cryptographic token, or key fob) is a physical device that an authorized user of computer services is given to ease authentication.

Biometrics

- ***Biometrics*** is an authentication method that identifies and recognizes people based on physical trait such as fingerprint, face recognition, iris recognition, retina scan and voice recognition.

RADIUS and TACACS+

- Remote Authentication Dial In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+) are two protocols that provide centralized authentication, authorization, and Accounting management for computers to connect and use a network service.
- The RADIUS or TACACS+ server resides on a remote system and responds to queries from clients such as VPN clients, wireless access points, routers and switches.
- The server then authenticates a username/password combination (authentication), determine if a user is allowed to connect to the client (authorization), and log the connection (accounting).

Using RUNAS

- Since administrators have full access to a computer or the network, it is recommended that you use a standard non-administrator user to perform most tasks.
- Then if you need to perform administrative tasks, you would then use the RUNAS command or built-in options that are included with the Windows operating system.

Active Directory

- A directory service stores, organizes and provides access to information in a directory.
- Active Directory is a technology created by Microsoft that provides a variety of network services, including:
  - LDAP
  - Kerberos-based and single sign-on authentication
  - DNS-based naming and other network information
  - Central location for network administration and delegation of authority

Domain Controller

- A ***domain controller*** is a Windows server that stores a replica of the account and security information of the domain and defines the domain boundaries.
- A server that is not running as a domain controller is known as a ***member server***.

NTLM

- *NTLM* is the default authentication protocol for Windows NT, stand-alone computers that are not part of a domain or when you are authenticating to a server using an IP address.
- It also acts a fall-back authentication if it cannot complete Kerberos authentication such as being blocked by a firewall.
- NTLM uses a challenge-response mechanism for authentication, in which clients are able to prove their identities without sending a password to the server.

Kerberos

- With Kerberos, security and authentication is based on secret key technology where every host on the network has its own secret key.
- The Key Distribution Center maintains a database of secret keys.
- For all of this to work and to ensure security, the domain controllers and clients must have the same time.

Organizational Units

- To help organize objects within a domain and minimize the number of domains, you can use ***organizational units***, commonly seen as OU.
- You can delegate administrative control to any level of a domain tree by creating organizational units within a domain and delegating administrative control for specific organizational units to particular users or groups.

Objects

- An ***object*** is a distinct, named set of attributes or characteristics that represent a network resource.
- Examples:
  - Users
  - Computers

Groups (1 of 2)

- A ***group*** is a collection or list of user accounts or computer accounts.
- Different from a container, the group does not store the user or computer, it just lists them.
- The advantage of using groups is to simplify administration, especially when assigning right and permissions.

Groups (2 of 2)

- In Windows Active Directory, there are there are two types of groups: security and distribution.
- Any group, whether it is a security group or a distribution group, is characterized by a scope that identifies the extent to which the group is applied in the domain tree or forest.
  - Domain Local Group
  - Global Group
  - Universal Group

Rights

- A ***right*** authorizes a user to perform certain actions on a computer such as logging on to a system interactively or backing up files and directories on a system.
  - User rights are assigned through local policies or Active Directory group policies.

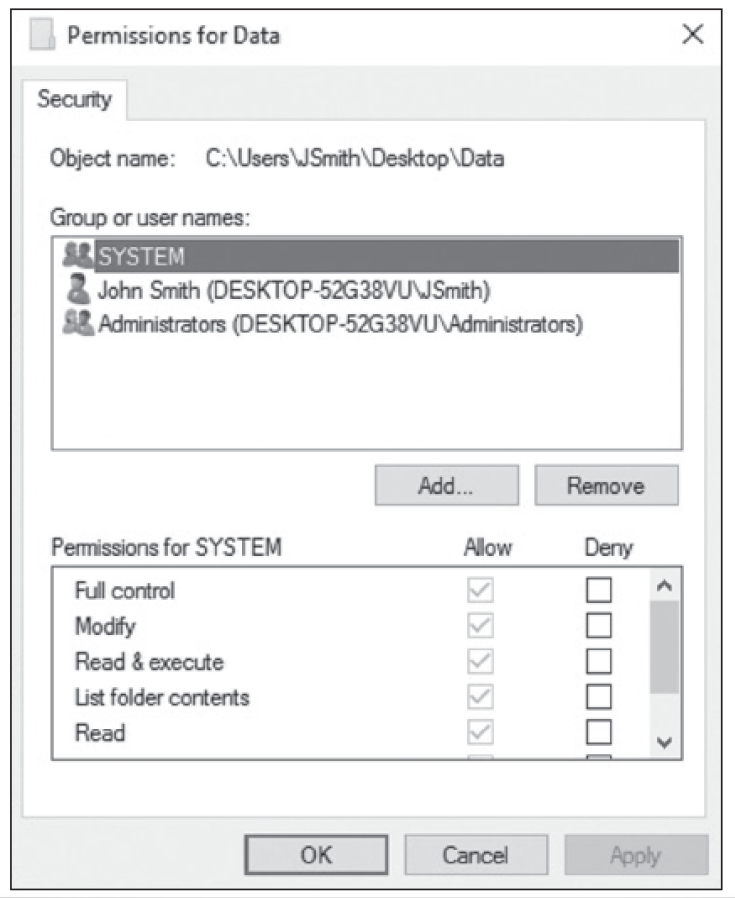
Permission

- A ***permission*** defines the type of access that is granted to an object (an object can be identified with a security identifier) or object attribute.
- To keep track of which user can access an object and what the user can do is stored in the ***access control list (ACL)*** which lists all users and groups that have access to the object. NTFS and printer permissions will be discussed in the next lesson.

NTFS

- *NTFS* is the preferred file system to be used in today's operating systems.
- *NTFS permissions* allow you to control which users and groups can gain access to files and folders on an NTFS volume.
  - The advantage with NTFS permissions is that they affect local users as well as network users.

NTFS Permissions (1 of 2)



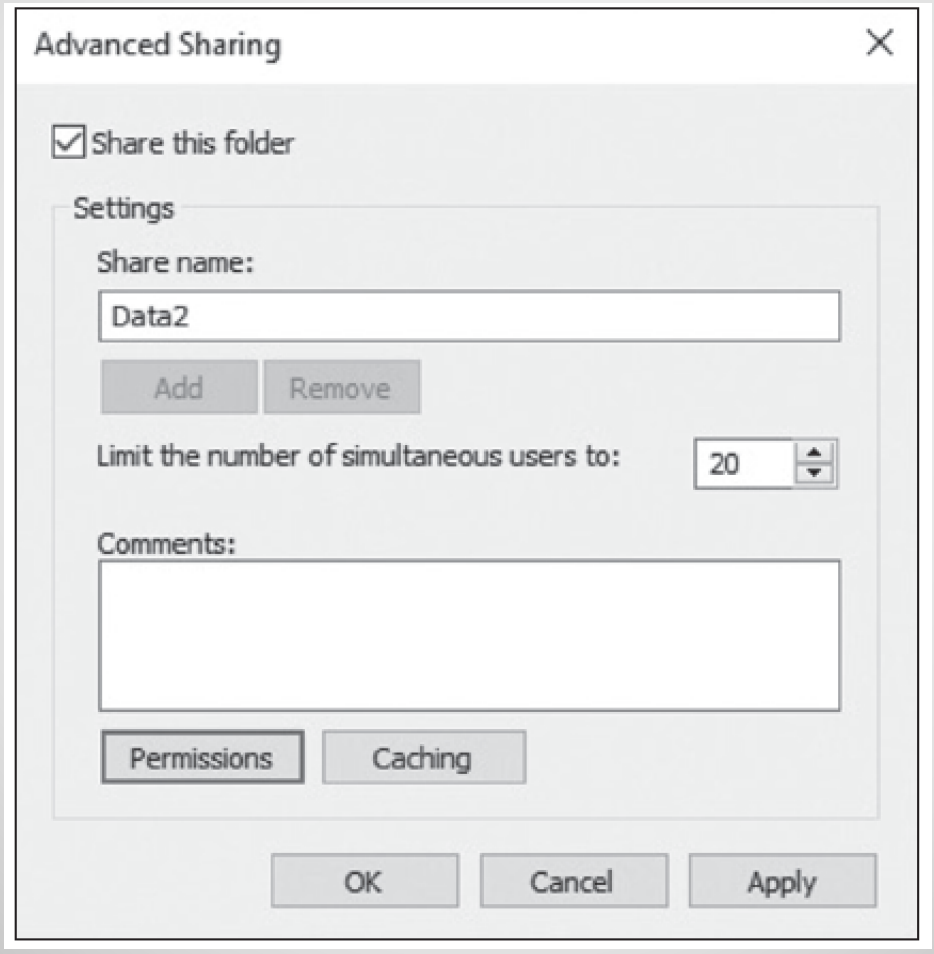
NTFS Permissions (2 of 2)

- There are two types of permissions used in NTFS:
  - Explicit permission – Permissions granted directly to the file or folder.
  - Inherited – Permissions that are granted to a folder (parent object or container) that flow into a child objects (sub-folders or files inside the parent folder).
- Effective permissions, which are the actual permissions when logging in and accessing a file or folder.
  - They consist of explicit permissions plus any inherited permissions.

Sharing Drives and Folders

- Most users are not going to log onto a server directly to access their data files. Instead, a drive or folder will be shared (known as a shared folder) and they will access the data files over the network.
- To help protect against unauthorized access, you will use share permissions along with NTFS permissions (assuming the shared folder is on an NTFS volume). When a user needs to access a network share, they would use the UNC, which is \\servername\sharename.

Sharing a Folder



Encryption

- Encryption is the process of converting data into a format that cannot be read by another user.
- Once a user has encrypted a file, it automatically remains encrypted when the file is stored on disk.
- Decryption is the process of converting data from encrypted format back to its original format.
- A key, which can be thought of as a password, is applied mathematical to plain text to provide cipher or encrypted text.

Public Key Infrastructure

- ***Public Key Infrastructure (PKI)*** is a system consisting of hardware, software, policies and procedures that create, manage, distribute, use, store, and revoke digital certificates.
- Within the PKI, the certificate authority (CA) binds a public key with respective user identities and issues digital certificates containing the public key.
- A ***certificate revocation list (CRL)*** is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked or are no longer valid, and therefore should not be relied upon.

Digital Certificates and Signatures

- A ***digital certificate*** is an electronic document that contains a person's or organization's name, a serial number, expiration date, a copy of the certificate holder's public key (used for encrypting messages and to create digital signatures) and the digital signature of the CA that assigned the digital certificate so that a recipient can verify that the certificate is real.
  - The most common digital certificate is the X.509 version 3.
- A ***digital signature*** is a mathematical scheme that is used to demonstrate the authenticity of a digital message or document.

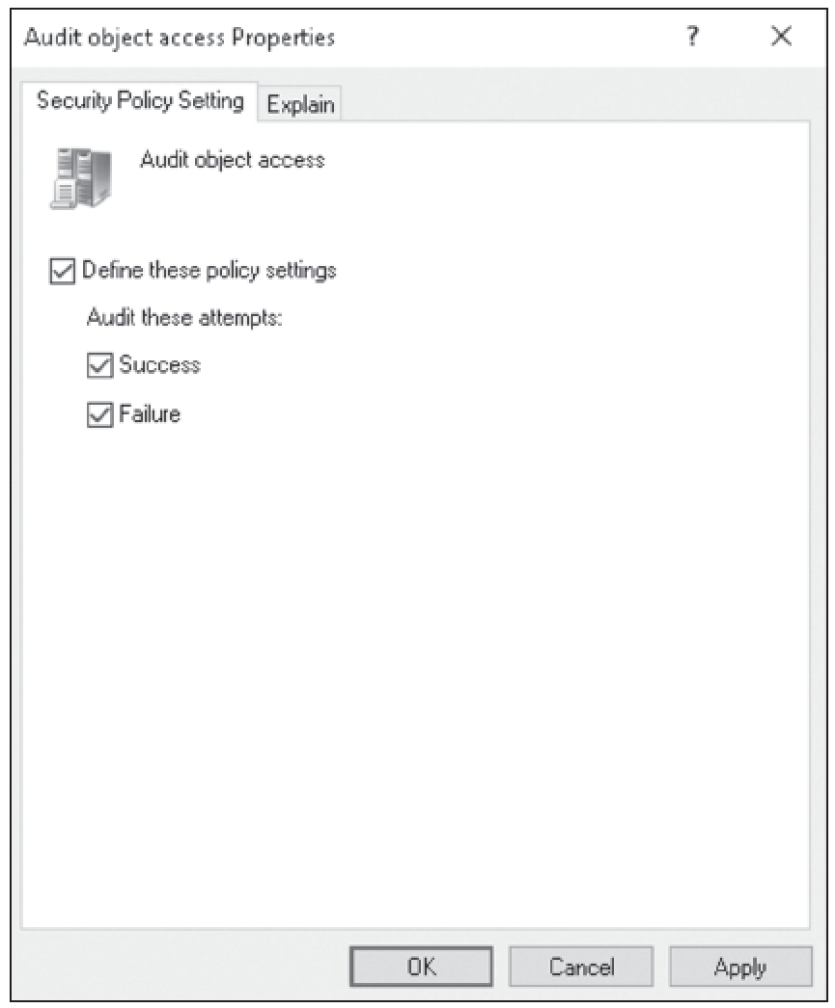
Forms of Encryption

- Secure Sockets Layer (SSL)
- Secure multipurpose Internet Mail Extension (S/MIME)
- Pretty Good Privacy (PGP)
- Encrypting File System (EFS)
- BitLocker
- Virtual Private Network (VPN)

Auditing (1 of 2)

- Gives access to the user that was authenticated. To complete the security picture, you need to enable auditing so that you can have a record of the users who have logged in and what the user accessed or tried to access.

Auditing (2 of 2)



Syslog

- Syslog is a standard for logging program messages that can be accessed by devices that would not otherwise have a method for communications.

Summary (1 of 9)

- AAA (Authentication, Authorization, and Accounting) is a model for access control.
- Authentication is the process of identifying an individual.
- After a user is authenticated, users can access network resources based on the user's authorization. Authorization is the process of giving individuals access to system objects based on their identity.

Summary (2 of 9)

- Accounting, also known as Auditing is the process of keeping track of a user's activity while accessing the network resources, including the amount of time spent in the network, the services accessed while there and the amount of data transferred during the session.
- When two or more authentication methods are used to authenticate someone, you are implementing a multifactor authentication system.
- The most common method of authentication with computers and networks is the password.

Summary (3 of 9)

- Active Directory is a technology created by Microsoft that provides a variety of network services, including LDAP, Kerberos-based and single sign-on authentication, DNS-based naming and other network information and Central location for network administration and delegation of authority.
- A user account enables a user to log onto a computer and domain.

Summary (4 of 9)

- A right authorizes a user to perform certain actions on a computer such as logging on to a system interactively or backing up files and directories on a system.
- A permission defines the type of access that is granted to an object (an object can be identified with a security identifier) or object attribute.
- Encryption is the process of converting data into a format that cannot be read by another user. Once a user has encrypted a file, it automatically remains encrypted when the file is stored on disk.

Summary (5 of 9)

- Decryption is the process of converting data from encrypted format back to its original format.
- Encryption algorithms can be divided into three classes: Symmetric, Asymmetric, and Hash function.
- Symmetric encryption uses a single key to encrypt and decrypt data. Therefore, it is also referred to as secret-key, single-key, shared-key, and private-key encryption.

Summary (6 of 9)

- Asymmetric encryption, also known as public key cryptography, uses two mathematically related keys.
- One key is used to encrypt the data, while the second key is used to decrypt the data.
- Different from the symmetric and asymmetric algorithms, a hash function is meant as a one-way encryption.
- This means that after it has been encrypted, it cannot be decrypted.

Summary (7 of 9)

- PKI is a system consisting of hardware, software, policies, and procedures that create, manage, distribute, use, store, and revoke digital certificates.
- The most common digital certificate is the X.509 version 3.
- The certificate chain, also known as the certification path, is a list of certificates used to authenticate an entity. It begins with the certificate of the entity and ends with the root CA certificate.

Summary (8 of 9)

- A digital signature is a mathematical scheme that is used to demonstrate the authenticity of a digital message or document. It is also used to confirm that the message or document has not been modified.
- When surfing the internet and needing to transmit private data over the internet, use SSL over HTTPS (https) to encrypt the data sent over the internet. By convention, URLs that require an SSL connection start with https: instead of http:

Summary (9 of 9)

- IPsec is a suite of protocols that provide a mechanism for data integrity, authentication, and privacy for the Internet Protocol.
- VPN links two computers through a wide-area network, such as the internet.
- Windows Hello is a Windows 10 biometric authentication system that uses a user's face, iris, or fingerprint to unlock devices.
- Syslog is a standard for logging program messages that can be accessed by devices that would not otherwise have a method for communications.