4.3.2 File System Security Facts

Managing the file system is a primary concern of IT professionals. The file system is responsible for storing and securing data. An organization depends on data and requires that it be secure and easily accessible.

This lesson covers the following topics.

- File system security
- Big data storage
- Data transfer security protocols

File System Security

Tasks to secure file servers include:

- Prevent physical access
- Implement the principle of least privilege
- Use full-disk encryption on backups
- Implement strong authentication
- Remove unnecessary software and disable unused services
- Use implicit deny access control lists (ACLs)
- Use hidden folders and files
- Audit the file system

When managing the security of the file system, be aware of the following:

- The transfer of files between a client and a server is often unsecured. Use IPSec or a VPN between the server and the client to secure data as it travels through the network.
- File and print resources are primarily vulnerable to denial-of-service (DoS) and access attacks.
- Attacks on file servers are often directed against the NetBIOS protocol. To protect the server, verify that NetBIOS is not required on the server, disable the NetBIOS protocol on the server, and use a host-based firewall to close NetBIOS ports 135 and 137 - 139.
- A *shared folder* is a folder whose contents are available over the network.
  - An *administrative* share is a shared folder that is available only to an administrative user.
  - Administrative shares are hidden. This means that the share will not display when a user browses a network computer.
  - By default, the root of every drive is an administrative share.
  - In Windows, you can create hidden shares by appending a $ sign; to the end of the share name (for example, DataFiles$).
  - Users must know the name of the share to access it, as well as, have the appropriate access permissions.
  - Do not share the root directory with regular users.
- With Windows Server 2008 and later, you can use File Server Resource Manager (FSRM) to control files saved on a file server.
  - Quotas limit the amount of data that can be saved within a folder. A hard limit prevents exceeding the quota limit, while a soft limit sends a message when the limit is exceeded.
  - File screens restrict the type of files that can be saved in a folder. For example, you can prevent media files (audio and video) or files with specific file extensions from being saved. An *active* file

screen prevents saving the specified file types, while a *passive* screen monitors when the specified file types are added to the folder.

Big Data Storage

In modern network environments, many organizations must store extremely large amounts of data, referred to as *big data*. Be aware of the following regarding big data:

- The size of the dataset can be measured in exabytes.
- Big data can be analyzed to provide a wealth of information. Businesses use big data to identify business trends, create computer models, and isolate network attacks.
- The data set is so large that it is usually stored on NAS or SAN devices.
- The key problem associated with big data is that the data set can become so large that it can no longer be managed.

The following table describes solutions for storing large amounts of data.

Solution	Description
Network attached storage (NAS)	NAS is a standalone storage device or appliance that acts as a file server. Be aware of the following: - The NAS device is connected to the same network as all other network devices. Therefore, it is exposed to attacks from all network hosts. - NAS devices typically use standard protocols for file sharing. Because standard protocols are well-known, they are subject to attacks. - The NAS device often has a limited operating system capable of sharing files and controlling access to those files using access control lists (ACLs). - NAS administration should be secured with a strong password and strong authentication.
Storage area network (SAN)	A SAN is a special network composed of high-speed storage that is shared by multiple servers. A SAN is typically a separate network that only file servers attach to. Security for a SAN is provided by the following: - *Logical Unit Number (LUN) masking* identifies devices that are allowed to attach to a logical unit. - *SAN zoning* groups SAN devices and servers into security zones. Only devices within the security zone can access data on the storage unit. - The Fibre Channel Authentication Protocol (FCAP) provides a method for mutual authentication of devices within the SAN. SANs are typically more secure than NAS solutions.

Data Transfer Security Protocols

The following table describes considerations for securing file transfer using TCP/IP protocols:

Protocol	Description
File Transfer Protocol	Be aware of the following when using FTP: - *Anonymous login* (also known as *blind or anonymous FTP*) allows unrestricted access to

(FTP)	▪ *Anonymous login* (also known as *blind* or *anonymous FTP*) allows unrestricted access to the FTP server. Disable anonymous login to control access based on username. ▪ The username and password are transferred in cleartext and can be captured in transit by a sniffer. To protect logon credentials, implement a secure protocol, such as Secure Socket Layer (SSL). ▪ Use IPSec or a VPN tunnel to protect data transfers. ▪ The write permission allows users to upload files to the FTP server. Carefully restrict which users have the write permission. ▪ FTP uses port 21 for control information (such as logon) and port 20 for data transfer.
Trivial File Transfer Protocol (TFTP)	TFTP provides no authentication, encryption, or error detection. In addition, TFTP uses UDP instead of TCP. TFTP might be faster than FTP, but it does not perform error detection, so it could result in file errors.
Secure Copy Protocol (SCP)	SCP uses Secure Shell version 1 (SSH1) to secure file transfers and login credentials.
Secure Shell File Transfer Protocol (SFTP)	SFTP is a file transfer protocol that uses Secure Shell version 2 (SSH2) to secure data transfers. SFTP is not FTP that uses SSH, but rather a secure transfer protocol that is different from FTP.
Secure FTP	Secure FTP (also known as FTP over SSH) tunnels FTP traffic through an SSH tunnel.
FTP Secure (FTPS)	FTPS adds SSL or Transport Layer Security (TLS) to FTP in order to secure logon credentials and encrypt data transfers. FTPS requires a server certificate.