7.5.2 File System Security Facts

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

- 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 then use a host-based firewall to close the NetBIOS ports 135 and 137-139.
- Methods to secure file servers include:
  - Preventing physical access
  - The principle of least privilege
  - Full-disk encryption on backups
  - Strong authentication
  - Removing unnecessary software and disabling unused services
  - Implicit deny ACLs (Access Control Lists)
  - Hidden folders and files
  - File system auditing
- A *shared folder* is a folder whose contents are available over the network.
  - An *administrative* share is a shared folder that is only available to an administrator user.
  - Administrative shares are hidden (meaning that the share will not show up when a user browses to a network computer). Users must know the name of the share to access it, as well as have the appropriate access permissions.
  - By default, the root of every drive is an administrative share.
  - In Windows, you can create hidden shares by appending a $ to the end of the share name (for example, DataFiles$).
  - Do not share the root directory with regular users.
- In modern network environments, many organizations must store extremely large amounts of data, referred to as *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.
- Network-Attached Storage (NAS) is a standalone storage device or appliance that acts as a file server.
  - 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 could be 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.
- A Storage Area Network (SAN) is a special network composed of high-speed storage that is shared by multiple servers. A SAN is typically a separate network where only file servers attach. Security for a SAN is provided by the following:
  - *LUN masking*, which identifies devices that are allowed to attach to a logical unit.
  - *SAN zoning*, which 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.

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

Protocol	Description
File Transfer Protocol (FTP)	Be aware of the following when using 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 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. Even though TFTP might be faster than FTP, it does not perform error detection, so it could result in file errors.
Secure Copy Protocol (SCP)	SCP uses the Secure Shell protocol (SSHv1) to secure file transfers and login credentials.
Secure Shell File Transfer Protocol (SFTP)	SFTP is a file transfer protocol that uses Secure Shell (SSHv2) 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)	FTP Secure (FTPS) adds SSL or TLS to FTP in order to secure logon credentials and encrypt data transfers. FTPS requires a server certificate.

- 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 saving media files (audio and video) or files with specific file extensions. 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.

TestOut Corporation All rights reserved.