Security

TestOut Modules 12.6 – 12.10

Authentication

Authentication is the process of submitting and checking credentials to validate or prove user identity.

1. Username
2. Credentials
   - Password
   - Smart card
   - Biometric

Many authentication systems also use cognitive information about you to help prove your identity.

Stronger authentication

Stronger authentication processes require the user to provide multiple authentication factors. There are three general categories of authentication factors:

1. **Something the user knows**: username, password, or PIN number.
2. **Something the user has**: smart card.
3. **Something the user is**: fingerprint or a retina scan.

True multifactor authentication requires the user to provide an authentication factor from more than one category

Password Policy

A ***password policy*** is a *system configuration* that prevents users from choosing easy passwords.

- Requires passwords 8 characters or longer.
- Prevents the use of the username or a dictionary word in the password.
- Requires the use of numbers and symbols in addition to letters.
- Forces periodic password changes and prevents the reuse of recent passwords.
- In Windows, edit the **Local Security Policy** to modify password settings for a local computer, or the Default Domain Policy to control passwords for all computers in an Active Directory domain.

Authentication Management

- Usernames *are not* case sensitive.
- Passwords *are* case sensitive.
- A disabled account cannot be used for logon.
- To access a shared folder or use Remote Desktop for a workgroup computer, you must supply a username and password that matches a user account configured on the computer you are trying to access.
  - User accounts with blank passwords cannot be used to gain network access to a computer (configure a password first, logon, then to reconnect).
- By default, members of the Administrators group are allowed Remote Desktop access. To allow non-administrators access, add them to the Remote Desktop Users group.

Encryption

File – EFS (Encrypting File Service)

- Encrypts individual files or folders on NTFS partitions.
- You can add other users who can also open the encrypted file.
- Files remain encrypted even if the drive is moved to another computer or another operating system.
- Encryption cannot be used together with compression (you can use either, but not both).

Disk

- BitLocker provides whole disk encryption with Microsoft Vista or Windows 7 Ultimate or Enterprise.

Data Transmission

- A Virtual Private Network (VPN) uses IPSec, PPTP, and L2TP encryption to establish a secure communication channel between two hosts, or between one site and another site.
- Secure Sockets Layer (SSL) is a protocol that can be added to other protocols to provide security and encryption. For example, HTTPS uses SSL to secure Web transactions.
- Use WPA, WPA2, or WEP to secure wireless communications.
- When implementing network services, do not use protocols such as FTP or Telnet that pass logon credentials and data in clear text. Instead, use a secure alternative such as FTP-S or SSH.

Wired Network Security

- Physical security
- Unnecessary software
- User accounts
- Usernames and passwords
- MAC address filtering
- Static IP addressing
- Disabling ports

Wireless Network Security

- Usernames and passwords
- SSID names
- SSID broadcast
- Encryption
- MAC address filtering
- Static IP addressing
- Data emanation

Firewalls

A ***firewall*** is a device or software running on a device that inspects network traffic and allows or blocks traffic based on a set of rules.

- A ***network-based*** firewall
- A ***host-based*** firewall
  - By default, the firewall allows all outgoing Web traffic and responses but blocks all incoming traffic.
  - Configure *exceptions* to allow incoming traffic. In Windows Firewall, you can configure two exception types:
    - Program
    - Port

Firewalls

Most SOHO routers and access points include a firewall to protect your private network.

- Configure *port triggering* to allow the firewall to dynamically open incoming ports based on outgoing traffic from a specific private IP address and port.
- Configure *port forwarding* to allow incoming traffic directed to a specific port to be allowed through the firewall and sent to a specific device on the private network.

Proxy Server

A ***proxy server*** is a device that stands as an intermediary between a host and the Internet.

- A proxy server is a specific implementation of a firewall that uses filter rules to allow or deny Internet traffic. With a proxy, every packet is stopped and inspected at the firewall which causes a break between the client and the source server.
- Can control Internet access based on user account and time of day.
- Prevent users from accessing certain Web sites. For example, proxy servers used in schools or at home protect children from viewing inappropriate sites.
- Restrict users from using certain protocols. For example, a proxy server at work might prevent instant messaging, online games, or streaming media.
- Cache heavily accessed Web content to improve performance.