Student L11A2

Now that you have learned some basic tips for hardening a Linux server, we're going to move on to Windows servers. This activity focuses on hardening your Windows server to protect it in a basic sense. This focuses on Windows servers in general, whereas there are more steps to hardening your servers if you have different services on them, such as a web server, DNS server, or others.

Tips for hardening a Windows Server

- Make sure the base install of all operating system and post-operating system software comes from a trusted source.
- Servers are only connected to a completely trusted network during the install and hardening processes.
- Make sure to install all of the latest security patches and updates
- Use NTFS Only
  - The Windows NTFS file system (NTFS) partitions offer access controls and protections that are not available with the file allocation table (FAT), FAT32, or FAT32x file systems. Make sure that you format all partitions on your server using NTFS. If necessary, use the Convert tool to convert your FAT partitions to NTFS.
  - Note: If you convert, then make sure you pay attention to what the Access Controls for the shares are. Often converting will change the Access Controls to being wide open to where everyone can read and write.
- Use a Strong Password on the Administrator Account
  - Windows Server allows passwords of up to 127 characters. In general, longer passwords are stronger than shorter ones, and passwords with several character types (letters, numbers, punctuation marks, and nonprinting ASCII characters generated by using the ALT key and three-digit key codes on the numeric keypad) are stronger than alphabetic or alphanumeric-only passwords.
  - For maximum protection, ensure the Administrator account password is at least nine characters long and that it includes at least one punctuation mark or nonprinting ASCII character in the first seven characters. In addition, the Administrator account password should not be synchronized across multiple servers. You should use different passwords on each server to raise the level of security in the workgroup or domain.

- Rename the Administrator Account
  - A very simple yet effective procedure that should be a standard part of the hardening process for all servers is to rename the built-in administrator account.
  - This account is the primary point for attacks, because if successful, the account provides the attacker with virtually unlimited rights. Rename the account, and create a new user account named Administrator that has not been granted special privileges. You should give this latter account a strong and complex password. You do not need to use this account; it merely serves as a decoy for attack efforts. Do this at the domain and local computer levels.
  - The best policy is to rename the Administrator account to a unique user name that is different on all servers; this minimizes the potential that somehow an attacker will be successful in determining that this new account is the Administrator account in disguise and also managing to crack its password. Because this account is so central to legitimate management tasks, you may view using unique names on every server as unmanageable in practice. In any case, the password for the disguised Administrator account should be unique and different from the other Administrator accounts in the enterprise.

- Disable the Guest Account
  - By default, the Guest account is disabled. If the Guest account is enabled, you should disable it.

- Set Account Lockout Policy
  - For maximum security, enable lockout after 3 to 5 failed attempts, reset the count after not less than 30 minutes, and set the lockout duration to Forever (until admin unlocks).

- Remove All Unnecessary File Shares
  - Remove all unnecessary file shares on the system to prevent possible information disclosure and to prevent malicious users from using the shares as an entry to the local system.

- Set Appropriate ACLs on All Necessary File Shares
  - By default all users have Full Control permissions on newly created file shares. You should set ACLs on all shares that are required on the system so that users have the appropriate share-level access (for example, Everyone = Read).

- Install Antivirus Software and Updates
  - You should use antivirus software and processes to keep up to date on the latest virus threats. Such protection will only offer value if it is both possible to install and execute code on the target computer; and the protection technology is able to detect and neutralize such efforts.

Now you should be able to harden any server you have in a very basic sense. Once again, you are encouraged to find more ways to harden your specific server setup to best protect against potential attackers.
