**Explanation of the Windows Server 2019 Hardening Script**

This document explains the steps implemented in the provided PowerShell script to harden a Windows Server 2019 machine. Each section is designed to enhance security and minimize vulnerabilities during a cybersecurity competition such as CCDC.

**1. Define Constants**

* **$NewPassword**: This sets the new password for all local accounts. The variable is cleared from memory at the end to prevent red team access.
* **$FirewallAllowedPorts**: Specifies the ports allowed through the firewall.
* **$UserLogPath and $ServiceLogPath**: Define paths for logging user and service changes.

**2. Gather and Log All Local Users**

* **Purpose**: Collects all local users and logs their details (name and enabled status) to C:\UserAuditLog.txt for auditing and troubleshooting.
* **Command**: Uses Get-LocalUser to enumerate users.

**3. Remove Non-Native Accounts**

* **Purpose**: Identifies and removes accounts that do not match the default native accounts (DefaultAccount, WDAGUtilityAccount, Guest, Administrator).
* **Command**: Filters accounts with a regex pattern and removes them using Remove-LocalUser.

**4. Reset Passwords for All Users**

* **Purpose**: Sets a new secure password for all local user accounts.
* **Command**: Uses Set-LocalUser with a secure string for password updates.

**5. Revoke Login Certificates and Tokens**

* **Purpose**: Ensures any compromised or unused certificates are revoked.
* **Command**: Enumerates certificates in Cert:\LocalMachine\My and removes them with Remove-Item.

**6. Configure and Enable Windows Firewall**

* **Purpose**: Blocks all inbound and outbound traffic except for HTTP (port 80) and HTTPS (port 443). Enables the firewall for all profiles (Domain, Public, Private).
* **Commands**:
  + New-NetFirewallRule: Adds rules for HTTP/HTTPS traffic.
  + Set-NetFirewallProfile: Configures default actions for inbound and outbound traffic.

**7. Enable Audit Logging**

* **Purpose**: Enables auditing for all categories of events (success and failure).
* **Command**: AuditPol /set /category:\* /success:enable /failure:enable.

**8. Disable Unused Services**

* **Purpose**: Disables services that are not necessary for the competition environment.
* **Command**:
  + Logs disabled services to C:\DisabledServicesLog.txt.
  + Uses Set-Service to disable services and Stop-Service to ensure they are stopped.
* **Disabled Services**: Includes services like wuauserv (Windows Update), bits (Background Intelligent Transfer), and Dnscache (DNS Client).

**9. Disable SMBv1**

* **Purpose**: Disables the insecure SMBv1 protocol to prevent exploitation.
* **Command**: Set-SmbServerConfiguration -EnableSMB1Protocol $false.

**10. Remove Rogue Scheduled Tasks**

* **Purpose**: Identifies and removes unauthorized scheduled tasks that could be used by attackers.
* **Command**: Filters tasks not in the \Microsoft\ path and removes them using Unregister-ScheduledTask.

**11. Remove Suspicious Startup Programs**

* **Purpose**: Cleans up registry entries for startup programs that could introduce vulnerabilities.
* **Command**: Enumerates registry paths for startup programs and removes suspicious entries.

**12. Set Secure DNS Settings**

* **Purpose**: Configures DNS to use Google’s public DNS servers for reliability and security.
* **Command**: Set-DnsClientServerAddress updates DNS server addresses.

**13. Disable File Sharing and Network Discovery**

* **Purpose**: Eliminates unnecessary file sharing and network discovery features to reduce attack surfaces.
* **Commands**:
  + Disable-NetAdapterBinding: Disables File and Printer Sharing on all adapters.
  + Set-ItemProperty: Disables administrative shares.
  + Disables related services such as fdPHost, fdResPub, upnphost, and SSDPSRV.

**14. Run Windows Updates**

* **Purpose**: Ensures the system is fully patched with the latest updates. Placed at the end to prevent delays in critical hardening steps.
* **Command**: Install-WindowsUpdate runs updates silently and ignores reboots.

**15. Clear Password from Memory**

* **Purpose**: Removes the $NewPassword variable from memory to prevent it from being accessed by attackers.
* **Command**: $NewPassword = $null.

**Final Note:**

* Logs created during the process are stored in C:\UserAuditLog.txt and C:\DisabledServicesLog.txt for post-competition review.
* The script is designed to balance functionality and security, focusing on a minimal attack surface while maintaining necessary operations.