**Windows Hardening**

Proper hardening can eliminate most, if not all, opportunities for local privilege escalation. The following steps should be taken, at a minimum, to reduce the risk of an attacker gaining system-level access.

**Secure Clean OS Installation**

Taking the time to develop a custom image for your environment can save you tons of time in the future from troubleshooting issues with hosts. You can do this utilizing a clean ISO of the OS version you require, a Windows Deployment server or equivalent application for pushing images via disk or networking media, and System Center Configuration Manager (if applicable in your environment). SCCM and WDS are much larger topics than we have room for here, so let's save them for another time. You can find copies of Windows Operating systems [here](https://www.microsoft.com/en-us/software-download/) or pull them using the Microsoft Media Creation Tool. This image should, at a minimum, include:

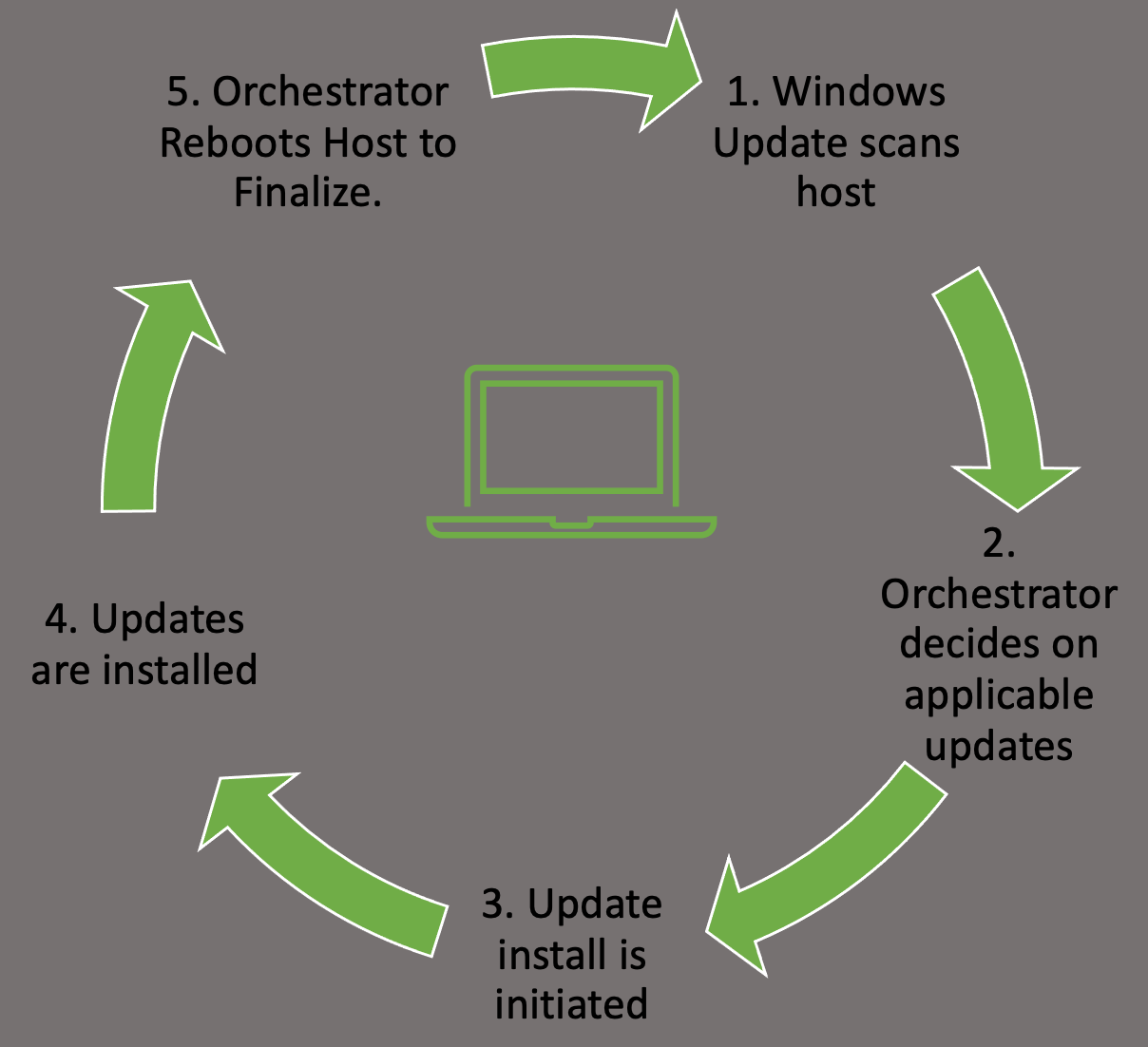
1. Any applications required for your employees' daily duties.
2. Configuration changes needed to ensure the functionality and security of the host in your environment.
3. Current major and minor updates have already been tested for your environment and deemed safe for host deployment.

By following this process, you can ensure you clear out any added bloatware or unwanted software preinstalled on the host at the time of purchase. This also makes sure that your hosts in the enterprise all start with the same base configuration, allowing you to troubleshoot, make changes, and push updates much easier.

**Updates and Patching**

[Microsoft's Update Orchestrator](https://docs.microsoft.com/en-us/windows/deployment/update/how-windows-update-works) will run updates for you in the background based on your configured settings. For most, this means it will download and install the most recent updates for you behind the scenes. Keep in mind some updates require a restart to take effect, so it's a good practice to restart your hosts regularly. For those working in an enterprise environment, you can set up a WSUS server within your environment so that each computer is not reaching out to download them individually. Instead, they can reach out to the configured WSUS server for any updates required.

In a nutshell, the update process looks something like this:

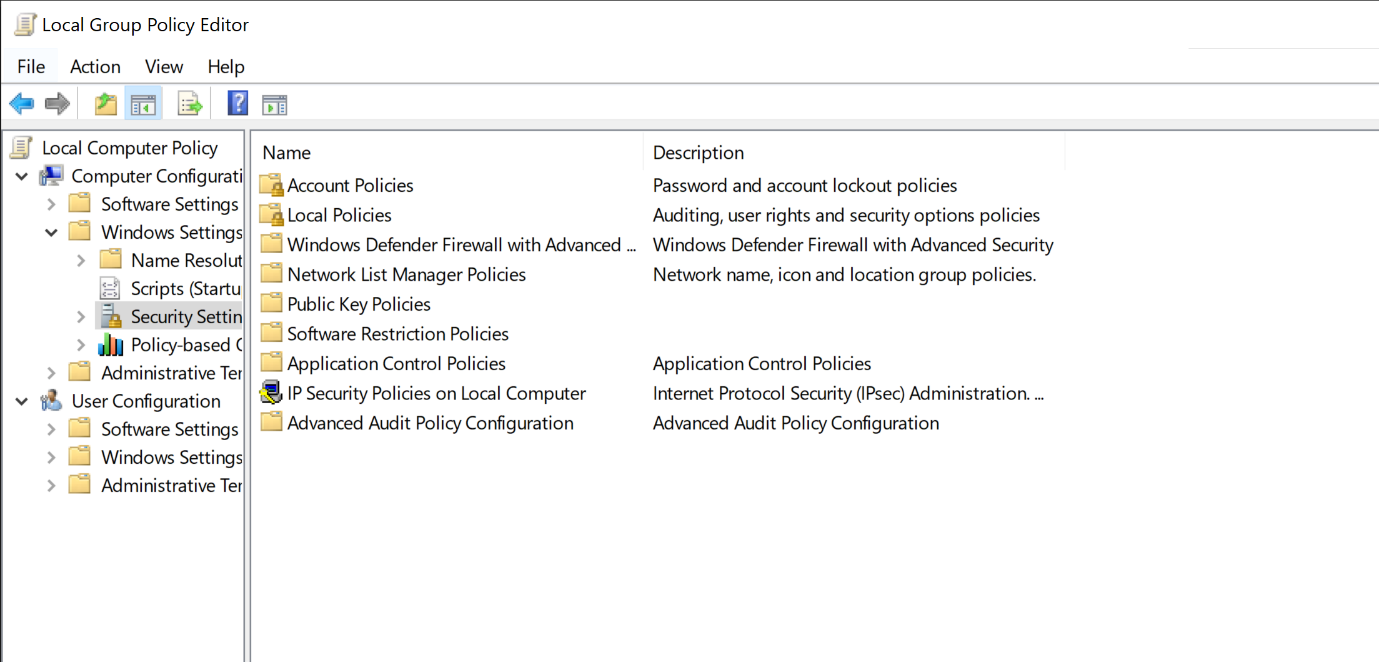


1. Windows Update Orchestrator will check in with the Microsoft Update servers or your own WSUS server to find new updates needed.
   * This will happen at random intervals so that your hosts don't flood the update server with requests all at once.
   * The Orchestrator will then check that list against your host configuration to pull the appropriate updates.
2. Once the Orchestrator decides on applicable updates, it will kick off the downloads in the background.
   * The updates are stored in the temp folder for access. The manifests for each download are checked, and only the files needed to apply it are pulled.
3. Update Orchestrator will then call the installer agent and pass it the necessary action list.
4. From here, the installer agent applies the updates.
   * Note that updates are not yet finalized.
5. Once updates are done, Orchestrator will finalize them with a reboot of the host.
   * This ensures any modification to services or critical settings takes effect.

These actions can be managed by [Windows Server Update Services](https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus), WSUS or through Group Policy. Regardless of your chosen method to apply updates, ensure you have a plan in place, and updates are being applied regularly to avoid any problems that could arise. Like all things in the IT world, test the rollout of your updates first, in a development setting (on a few hosts), before just pushing an update enterprise-wide. This will ensure you don't accidentally break some critical app or function with the updates.

**Configuration Management**

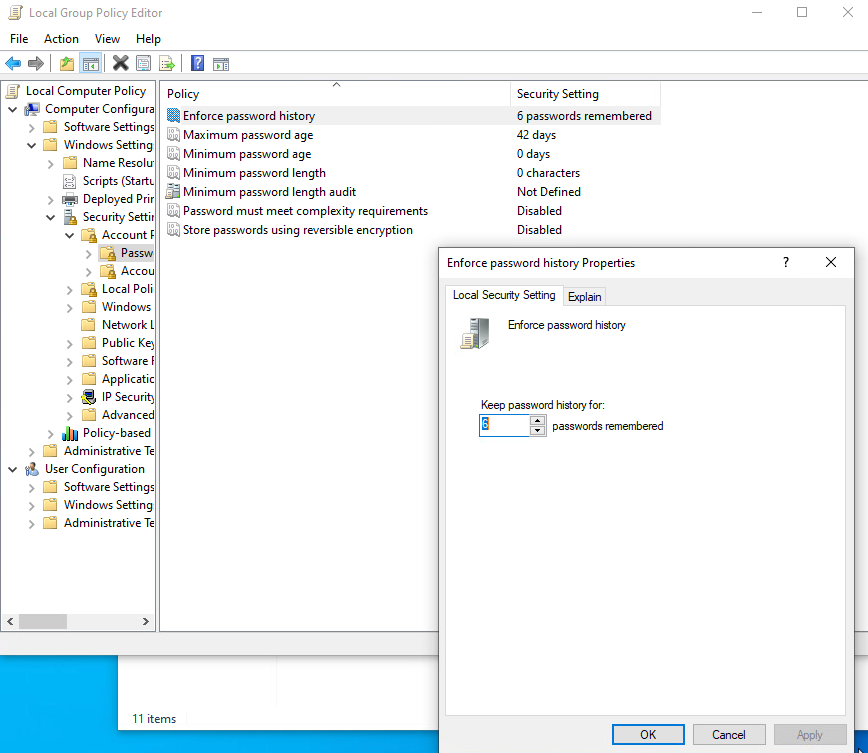
In Windows, configuration management can easily be achieved through the use of Group Policy. Group Policy will allow us to centrally manage user and computer settings and preferences across your environment. This can be achieved by using the Group Policy Management Console (GPMC) or via Powershell.



Group policy works best in an Active Directory environment, but you do have the ability to manage local computer and user settings via local group policy. From here, you can manage everything from the individual users' backgrounds, bookmarks, and other browser settings and how and when Windows Defender scans the host and performs updates. This can be a very granular process, so ensure you have a plan for the implementation of any new group policies created or modified.

**User Management**

Limiting the number of user and admin accounts on each system and ensuring that login attempts (valid/invalid) are logged and monitored can go a long way for system hardening and monitoring potential problems. It is also good to enforce a strong password policy and two-factor authentication, rotate passwords periodically and restrict users from reusing old passwords by using the Password Policy settings in Group Policy. These settings can be found using GPMC in the path Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy. We should also check that users are not placed into groups that give them excessive rights unnecessary for their day-to-day tasks (a regular user having Domain Admin rights, for example) and enforce login restrictions for administrator accounts.

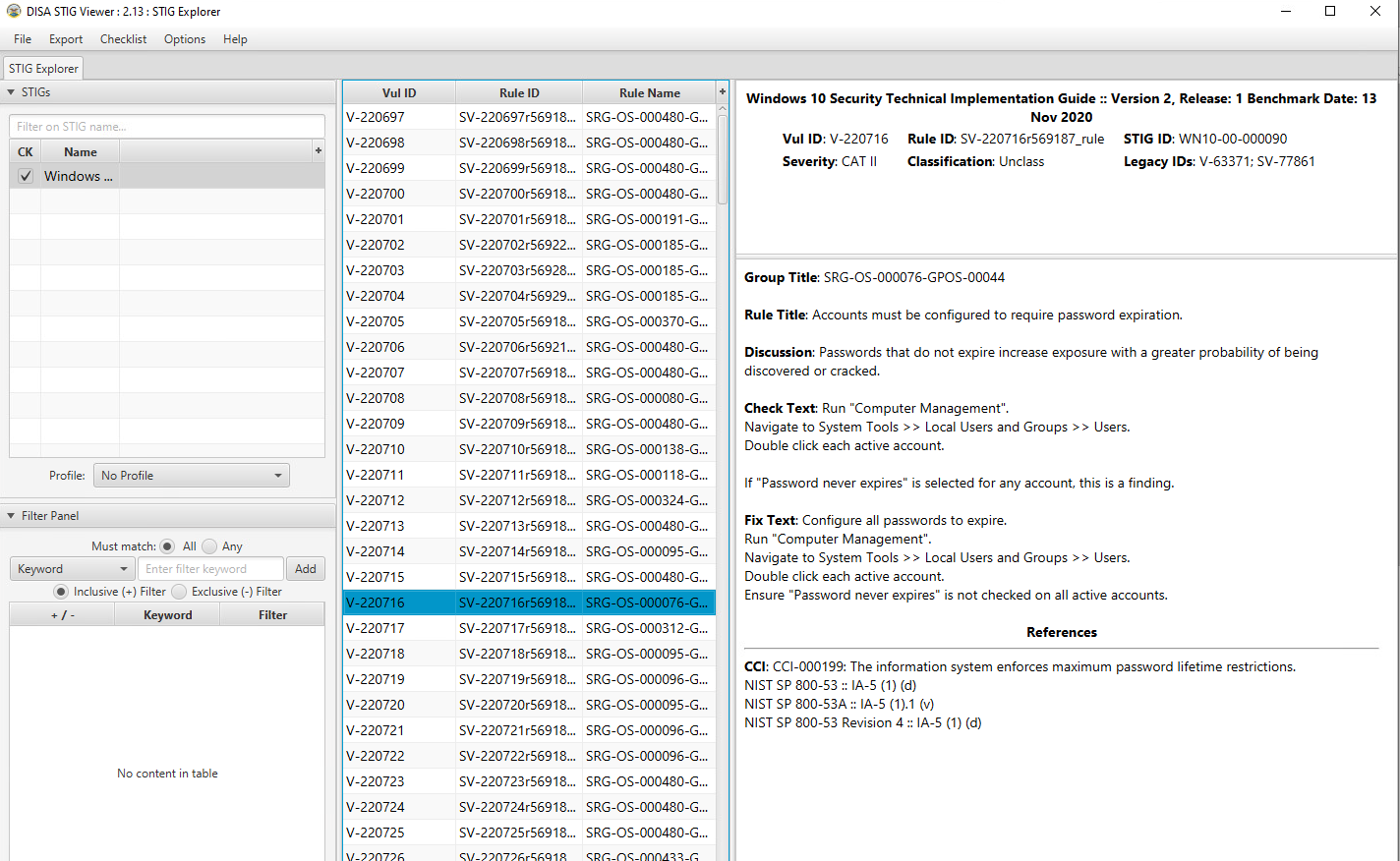


This screenshot shows an example of utilizing the group policy editor to view and modify the password policy in the hive mentioned above.

Two Factor Authentication can help prevent fraudulent logins as well. A quick explanation of 2FA is that it requires something you know password or pin and something you have a token, id card, or authenticator application key code. This step will significantly reduce the ability for user accounts to be used maliciously.

**Audit**

Perform periodic security and configuration checks of all systems. There are several security baselines such as the DISA [Security Technical Implementation Guides (STIGs)](https://public.cyber.mil/stigs/) or Microsoft's [Security Compliance Toolkit](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10) that can be followed to set a standard for security in your environment. Many compliance frameworks exist, such as [ISO27001](https://www.iso.org/isoiec-27001-information-security.html), [PCI-DSS](https://www.pcisecuritystandards.org/pci_security/), and [HIPAA](https://www.hhs.gov/hipaa/for-professionals/security/index.html) which can be used by an organization to help establish security baselines. These should all be used as reference guides and not the basis for a security program. A strong security program should have controls tailored to the organization's needs, operating environment, and the types of data they store and process (i.e., personal health information, financial data, trade secrets, or publicly available information).



The STIG viewer window we can see above is one way to perform an audit of the security posture of a host. We import a Checklist found at the STIG link above and step through the rules. Each rule ID corresponds with a security check or hardening task to help improve the overall posture of the host. Looking at the right pane, you can see details about the actions required to complete the STIG check.

An audit and configuration review is not a replacement for a penetration test or other types of technical, hands-on assessments and is often seen as a "box-checking" exercise in which an organization is "passed" on a controls audit for performing the bare minimum. These reviews can help supplement regular vulnerability scans, penetration tests, strong patch, vulnerability, and configuration management programs.

**Logging**

Proper logging and log correlation can make all the difference when troubleshooting an issue or hunting a potential threat in your network. Below we will discuss some apps and logs that can help improve your security posture on a Windows host.

**Sysmon**

Sysmon is a tool built by Microsoft and included in the Sysinternals Suite that enhances the logging and event collection capability in Windows. Sysmon provides detailed info about any processes, network connections, file reads or writes, login attempts and successes, and much much more. These logs can be correlated and shipped out to a SIEM for analysis and provide a better understanding of what we have going on in our environment. Sysmon is persistent on host and will begin writing logs at startup. It's an extremely helpful tool if appropriately implemented. For more details about Sysmon, check out [sysmon info](https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon).

Any logs Sysmon writes will be stored in the hive: Applications and Service Logs\Microsoft\Windows\Sysmon\Operational. You can view these by utilizing the event viewer application and drilling into the hive.

**Network and Host Logs.**

Tools like [PacketBeat](https://www.elastic.co/beats/packetbeat), IDS\IPS implementations such as Security Onion sensors, and other network monitoring solutions can help complete the picture for your administrators. They collect and ship network traffic logs to your monitoring solutions and SIEMS.

**Key Hardening Measures**

This is by no means an exhaustive list, but some simple hardening measures are:

* Secure boot and disk encryption with BitLocker should be enabled and in use.
* Audit writable files and directories and any binaries with the ability to launch other apps.
* Ensure that any scheduled tasks and scripts running with elevated privileges specify any binaries or executables using the absolute path.
* Do not store credentials in cleartext in world-readable files on the host or in shared drives.
* Clean up home directories and PowerShell history.
* Ensure that low-privileged users cannot modify any custom libraries called by programs.
* Remove any unnecessary packages and services that potentially increase the attack surface.
* Utilize the Device Guard and Credential Guard features built-in by Microsoft to Windows 10 and most new Server Operating Systems.
* Utilize Group Policy to enforce any configuration changes needed to company systems.

You may notice, if you take the time to read through a STIG checklist, many of these measures are included in the checks. Be mindful of what your environments use, and determine how these measures will affect the ability to accomplish the mission. Do not blindly implement widespread hardening measures across your network, as what works for one organization may not work for another. Knowing you are trying to protect and then applying the appropriate measures per the requirements of the business is critical.

**Conclusion**

As we have seen, there are many different ways to escalate privileges on Windows systems - from simple misconfigurations and public exploits for known vulnerable services, to exploit development based on custom libraries and executables. Once administrator or SYSTEM level access is obtained, it becomes easier to use it as a pivot point for further network exploitation. System hardening is equally critical for small companies and large enterprises. Watching the attack trends of this day and age, we can see attackers no longer care who the victim is, as long as they can get what they want out of the exchange. Best practice guidelines and controls exist in many different forms. Reviews should include a mix of hands-on manual testing and automated configuration scanning with tools like Nessus, followed by validation of the results. While patching for the latest and greatest attacks and implementing sophisticated monitoring capabilities, do not forget the basics and "low hanging fruit" covered throughout this module.

Finally, ensure your staff is constantly being challenged and trained and staying at the forefront of new vulnerabilities and exploit PoCs so your organization can remain protected as researchers continue to discover new avenues of attack.