Intro to Machine Hardening: Concepts and Principles

September 2019

Max E

1 Preamble

From various Online sources I have researched, guides pertaining to machine hardening are either very high-level (optimised for beginner users) or incredibly sophisticated (technical specifics to be implemented by system administrators and advanced users with computer security as a primary interest). This guide is aimed at an intermediate user between these extremes with an interest for personal security and optimising the security of their personal information assets. It is delivered in an informal manner with an emphasis on realistic security policies and freely available software solutions.

This guide may be used for advanced users and those within enterprise environments as a starting point for additional research – machines that are a part of networks where incredibly sensitive information assets are contained (medical records, banking information) must undergo a hardening process in accordance with international data assurance standards (ISO/IEC 27001 as a minimum).

2 Abstract

This guide is primarily aims to provide a comprehensive guide to a secure Windows 10 installation. It also contains information pertaining to generic machine hardening, living Online securely, and personal policy you may choose to implement.

'Hardening' in a cyber security context, is the process of optimising a computer's configuration in such a way that its attack surface is minimized. 'Attack surface' pertains to the applications, policy, and configurations of a computer that are potentially exploitable. That is to say, a large attack surface presents an attacker with many different exploitable computer attributes (software, policy, etc.).

This guide presents the means as well as the knowledge for each hardening step – this will naturally produce a guide that the reader may or may not fully implement - steps may be ignored if an individual's personal security policy do not pertain to the steps given.

3 Windows 10

Windows 10 is infamous for its poor out-of-the-box security, so much so, it is commonplace in the cyber security industry to avoid it at all costs unless absolutely necessary. This could be because of rumoured governmental snooping at the kernel level, inherent malware vulnerability, or Windows networking protocols. Despite the implicit risks of the Windows operating system, Windows 10 can be configured in a way such that its inherent vulnerabilities are mitigated, even if third party solutions must be used.

3.1 Installation

A basic version of the Windows 10 operating system is freely available for public download on the Microsoft website.

https://www.microsoft.com/en-gb/software-download/windows10ISO

This version can be saved to a USB disk - keep in mind that once the bootable version is saved to this disk, nothing else can be stored on it. Installation at this point will depend upon the BIOS options immediately available to you upon power-on - research the BIOS, and, in particular, boot options your machine gives you in order to select that you want to boot from the USB you have plugged into your device. To open BIOS settings, some kind of keyboard interrupt is required during the boot process - this keyboard interrupt is dependent on the machine you are using and will usually be indicated on the monitor you have plugged in immediately after the machine is switched on. Once installed and the appropriate accessibility options are chosen, the following guide provides information on activating your Windows 10 version, assuming that is something you are interested in doing:

https://support.microsoft.com/en-gb/help/12440/windows-10-activate

Microsoft also provides specific terms of usage for Windows 10 that you may wish to look into if you are concerned with how you are using your copy of Windows 10. Non-activated Windows 10 versions prevent you from accessing some desktop customisation options that can be easily bypassed. The grey watermark in the bottom right corner of the screen is there permanently if you have not activated your Windows version - there are scripts that can remove it from your screen, but its existence does not effect your operating system.

4 Password Policies

To many, personal privacy policy extends exclusively to the realm of passwords. Although important, there are many misconceptions regarding how passwords and password policy are supposed to be implemented. That being said, there is no perfect password policy for every user - through the evaluation of the information assets you plan on controlling, your password policy should be implemented realistically.

There are innumerable tools and information sources in the public domain at your immediate disposal for password management, creation, security, and convenience - these include, but are not limited to: password generators, password managers, and strength checkers. Should you be educated enough in the issue, feel free to generate your own password policy or use a password manager, do be aware of the risks that come with using this software, however. Many password managers have single points of failure (the password that acts as your 'master') and may store your passwords on a potentially unsecured machine - the storage of these passwords and the policy surrounding their encryption, control, and distribution among their own servers is out of your control - make sure that you can trust the companies you are handing your information.

Strength checkers and generators may also be storing the passwords you generate/store with them - research these tools to ensure non-repudiation that your data is secure/not being sent in the first place (Wireshark packet analysis for instance).

For an intermediate user, many passwords need be used for the Online services they consume as well as offline applications among their devices. My policy for these kinds of services is to generate passphrases (memorable sentences) as opposed to passwords - these inherently have higher entropies as their length is longer, while still being memorable to some extent. And, despite it being frequently looked down upon, it is okay to write down the passwords you cannot remember (especially the ones where sites enforce the use of special characters - a futile password design trope of the past that continues to this day). If you must write your passwords in plaintext, do so in private places that only you know the location of, and preferably aren't available for anyone else to visit.

It is also good practice to change your passwords semi-frequently (the timings for each service you plan on changing the password for are up to you) - this is useful for a number of reasons: If the service you have an account for experiences a data breach, it is usually only a matter of time before your password could become jeopardised (there are a lot of factors to this - an attacker may have to apply specialised password cracking software to reverse password hashes and uncover yours) - GDPR makes it mandatory (within the EU) for companies to warn their clients of data breaches within a given time frame, change your password as soon as this occurs - companies usually do not fully understand the severity of data breaches at the time that they publicise the knowledge of the data breach - it is best being safe.

Even though this new level of transparency exists (again, only within the EU), it is still necessary to frequently change your password - attackers can become aware of your password in simpler ways than stealing them from the databases of companies and performing hash cracks, and you will not necessarily be as aware of this.

5 Initial User Control

Upon account creation, the user account that will be created for you may be granted with Administrator capabilities, this is inherently dangerous from a security standpoint. As you may or may not know, administrator privileges – on a Windows computer - are required for changing OS (Operating System) configuration options from the Windows registry etc. Having your main account not contain administrator privileges prevents you from accidentally changing the fundamental way in which the OS runs. Separating your user account from the computer's Administrator account prevents an attacker from having these privileges if your account is compromised.

The implications of this action are simple - if an attacker were to gain access to your account through a running process on that account, post-exploitation measures that require administrator privileges become much more difficult to achieve (privilege escalation would now have to be performed by the attacker). User account control settings can be accessed by the initial administrator account to a) change the password of the administrator account and b) to create the user account you plan on using as your main platform with no administrator privileges.

Once the machine exists in a state where just the user account and the administrator account exist, adjust the memory assigned to both accounts individually depending on your need to access the administrator account. This amount will depend on how often you need to change the configuration of your operating system - this is more relevant for developers and sysadmins looking to access the administrator account regularly. Disk volumes can be configured via Windows Disk Management and visibility can be assigned from User Account Controls.

If at any point you are prompted to enable your account information with a Microsoft account, do not do so - this is a feature designed for sharing your computer account in its current state across the devices you use with Windows 10 via Microsoft's cloud platform. Having your information assets present on an unwanted platform is another possible attack surface, follow this guide to ensure your device has local account enabled, or, in the case that a Microsoft account has already been set up, follow the guide to enable local account:

https://www.webnots.com/how-to-setup-local-account-login-in-windows-10/

6 Secure Boot and Bitlocker

This section covers relatively accessible boot options that may or may not be relevant to the user specified with this guide in mind. For machines that may be used in public spaces: kiosks, laptops, mobile devices, etc., physical security of the device itself becomes more of an issue. The implementation of Bitlocker and Secure Boot (both Windows 10 enabled tools) allows for improved security in the environment specified - should the machine you plan on hardening be in an environment where you feel it is unlikely that other, unwanted users may have access to the machine, you may choose not to implement these security features.

Secure Boot is a Windows 10 enabled mechanism that prevents the hardware of the device from being altered such that a malicious user can change the hardware configuration of the device. Secure Boot prevents the device from being accessed if the initial machine configuration has been changed. Without Secure Boot, if the physical security of a device were to be compromised, its hardware may be switched out for malicious components - detailed installation is available via the official Microsoft documentation.

https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot - starting point

Bitlocker is a proprietary Windows 10 solution for device encryption. Bitlocker (when set up), will encrypt selected disk volumes when the machine is turned off. This means that if the physical security of the device is compromised, the information assets present on the selected Bitlocker drives is encrypted. Bitlocker requires a password post-boot (different than your account password) to decrypt your selected disk volumes, and access your data normally. This guide is useful in detailing Bitlocker specifics (including additional features I have not mentioned) and set-up.

https://www.pcworld.com/article/2308725/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html

The above guide also notes the proprietary nature of Bitlocker and the security issues that are relevant to such software - again, like all aspects of security and personal device hardening, if you wish to use this software, evaluate its privacy in conjunction with the sensitivity of your personal information assets and personal ethics.

7 Patching

Hackers look for vulnerabilities in both the operating system of the target machine or the software the machine has installed - this can then allow them to perform exploits and jeopardise the security of the information assets present on machines. These vulnerabilities are often present as a part of the design of the software or have existed as a part of the implementation since its birth (zero days) - software can also contain these vulnerabilities as a part of updates, implemented interfaces with other applications, or by the services the software uses. Regardless of how these vulnerabilities exist, to minimise the opportunity for their existence, the operating system of your device, the drivers it has installed, and any software the device uses should be updated as soon as updates become available.

These updates are generally released at some kind of constant interval (Microsoft's patch Tuesday for instance), or when a significant vulnerability is discovered. These updates provide software fixes (or 'patches') for the software that has been affected by the vulnerability and are released by those that maintain the software - these updates may also contain features which improve the software in different ways, e.g. performance.

On your device, configure all added software to update as soon as updates are released - if this option is not available, it may be the case that these updates will have to be installed manually by the user. If the latter is the only option available, remain vigilant for when these updates are released. By default, Windows 10 updates are installed as soon as they are available - for a guide on how to turn on this feature if it was somehow disabled, see the following guide:

https://answers.syr.edu/display/os/Turn+on+Automatic+Updates+in+Windows+10

8 Bloatware

This guide ultimately looks to minimise the attack surface of a newly installed Windows 10 machine - unneeded software present upon the fresh installation of Windows 10 presents a variety of attack surfaces that can be easily removed. Much of this software is not needed by intermediate users anyway (video games, Phone, social media applications) and can always be added back to the machine if needed - this also allows the user to selectively vet each software they add back to the machine.

There are a variety of free, open-source Powershell scripts capable of removing Windows 10 bloatware - these should all specify precisely what is removed from the machine, some will remove more than others, it is up to you what software you choose to rid your system of the bloatware it has installed. This bloatware remover seems to be very lenient in what is removed and provides fairly comprehensive run instructions - you may wish to choose another remover solution if this software is too lenient:

https://github.com/Sycnex/Windows10Debloater

9 OS Configuration Settings and Short-cuts

In regards to the base configuration of the operating system 'out-of-the-box', Windows 10 has inherently non-secure OS configurations enabled. Windows 10 makes it difficult for an end user to individually change each of these options as they are hidden behind multiple dialogue boxes and settings menus.

Thankfully, there are third party script suites capable of changing these settings autonomously as well as providing other OS configurations you may plan on altering (enabling 'God-mode' for instance). These security settings can involve things like Windows network sharing and networking protocols that increase your attack surface, but are left enabled by default. W10 privacy is a solution I've found to be effective, although the GUI seems to be fairly outdated:

https://www.winprivacy.de/english-home/

This program has script short-cuts for many of the OS configurations that hardening guides insist on being changed manually. This program will require administrative privileges to run, and may be flagged as malware by your antivirus - this is because the scripts it contains to change OS configurations (for the better) are marked as malicious.

10 Antivirus

The world of antivirus is diverse and misunderstood among a consumer audience. For this guide, it is recommended to use the default, free Windows 10 antivirus program - Windows Defender. Among the world of antivirus, freeware is often discarded as a viable option due to its purported effectiveness and

forced advertisement, but Windows Defender does not contain any advertisement and is ranked as one of the best current antivirus programs on the market by AVTest, an independent antivirus laboratory:

https://www.av-test.org/en/antivirus/home-windows/windows-10/february-2019/microsoft-windows-defender-4.18-190516/

11 Living Online

Now that a large portion of your device's attack surface relating to the OS is reduced, the privacy of your browsing data and information collated, generated, and collected as a part of your online persona must be evaluated. These are still sensitive personal information assets, as such, steps must be taken to mitigate their jeopardy on an optimised online platform.

It is still important to remember that the steps listed are taken in accordance with variable asset control standards, for instance, if you are a user with no concern for the big data ecosystem Google harbours, then feel free to use their platform in accordance with your own security standards. The following information regarding browsers, add-ons, browser configuration and policy is optimised for users with a privacy interest, but a need for performance and data-enhanced online experiences (limited cookie usage).

For users with a heightened security concern, the following resource provides useful articles that evaluate the spyware threat of software platforms and has a particular emphasis on data collection moderation. This guides browser configuration is in accordance with this site's Firefox mitigation guide - there is plenty of information available on this site for more robust security strategies:

https://spyware.neocities.org/

11.1 Data Collection

Many browsers and websites look to collect as much data about you as possible for a number of reasons that vary in severity. For the most part, this information is collated and distributed so as to optimise advertisement targeting and maximise revenue for sites that run advertisements to profit. This information is gathered, for the most-part, by a mechanism known as 'cookies'. Cookies collect information regarding your past online activity and can vary wildly in the kinds of activity they store - despite recent policy implementations such as GDPR, many sites will freely collect and alter the cookies that are stored on your device.

Cookies as an engineering aspect of the web are lightweight and easy to implement - although the privacy implications of their continued use are significant, privacy concerns regarding personal data collection among content platforms such as Facebook and Youtube are even more worrying upon inspection. Despite the implementation of GDPR in the European Union, the transparency these kinds of platforms must give in terms of data collection and breaches is limited. Should you use these services, evaluate their privacy and data retention policies on a case-by-case basis and ensure that you fully understand what can be done with your data and its sensitivity when submitted to these platforms.

11.2 Browsers

Firefox is a high-performance, privacy-focussed browser that is highly customisable and boasts lower memory usage than competitors. Although its claims regarding performance might be true, many additional steps may be taken to ensure the minimisation of your online footprint. Although not as implicitly secure

as browsers like Pale Moon, its performance and developer tools are unrivalled as of September 2019. For security configuration options, implement some or all of the following spyware mitigation steps:

https://spyware.neocities.org/guides/firefox.html

11.3 Search Engines

This guide recommends the use of DuckDuckGo as a search engine choice - DuckDuckGo is a privacy-centred search engine that professes privacy enabled features like anti-tracking and search history deletion. With any search engine, its operation is completely out of your control in terms of its web search procedure, you are simply presented with search results in conjunction with a query - the 'back-end' could host a variety of other services that you are made unaware of where tracking could occur. As of now, DuckDuckGo has a good reputation for privacy controls among its users and independent investigators, but there is no real way of identifying its search procedure - even as an advanced user utilising network analysis tools such as Wireshark. With this in mind, it is still better to utilise the tool that has not yet been proven to contain major privacy flaws than to use a competitor such as the Google search engine, which is identified by some security researchers to be definite spyware.

DuckDuckGo Privacy Statement: https://duckduckgo.com/privacy

Google Search Reported as Spyware: https://spyware.neocities.org/articles/google_search.html

11.4 Add-ons

Minimisation of tracking techniques and cookie controls as well as advertisement blockers can be achieved by various security add-ons that are available for free on the Firefox platform.

11.4.1 UBlock Origin

An industry favourite for advertisement blocking and performance increase - UBlock Origin also allows users to create their own custom filter lists for advertisement blocking.

https://addons.mozilla.org/en-GB/firefox/addon/ublock-origin/

11.4.2 Ghostery

Ghostery provides additional advertisement blocking and provides anti-tracking services via track blocks on the sites you visit.

https://addons.mozilla.org/en-GB/firefox/addon/ghostery/

11.4.3 Lightbeam

Lightbeam provides a cookie tracking function that measures the cookies the sites you visit use and how they are shared. Lightbeam can generate a spider-like visualisation of your cookies and their relation to the sites you visit - this is a useful tool in further understanding where your information assets are distributed.

https://addons.mozilla.org/en-GB/firefox/addon/lightbeam/

11.5 VPN and other Networking Technologies

Virtual Private Networks are a networking means to many ends, and, although incredibly useful and beneficial, are not a 'be-all-end-all' security solution (as occasionally advertised). VPNs, from a networking perspective, create an encrypted 'tunnel' between your device and a secured endpoint from which all your traffic is forwarded. The physical endpoints from which your device's traffic use as an endpoint depends on the VPN you choose. Some VPNs offer endpoints across many countries - this may allow you to access services that are only available in other countries.

This has a lot of benefits when it comes to network security, for instance, connecting to public networks is more secure as your traffic is encrypted during its relay across public routers. This stops potential attackers from sitting on the network and sniffing your traffic for exploitable information. VPNs also prevent your internet service provider, or other organisations, from collecting the data associated with your IP address. Despite the fact that your data is forwarded through your internet service provider to provide internet access in the first place, the traffic itself is encrypted via the secure connection with your chosen endpoint.

However, VPNs do come with downsides, for instance, most good quality VPNs (ones that do not make logs regarding your activity, for instance) require a paid subscription for their services. This, again, is a personal decision that you have to make in accordance with the sensitivity of your information assets and your compliance with organisations, like internet service providers stealing your information. VPNs can also slow down your internet performance, especially if you choose an endpoint in a country far away from your own. This is because your traffic must undergo additional network 'hops' every time a resource is requested.

My personal recommendation for a VPN would be Nord. They host endpoint servers in multiple countries across most continents and provide fast, stable connections from my experience with them. They also have mobile versions and are based out of Panama - Panama do not require VPN services to store logs of their users' activity, this is a potential benefit if privacy is of particular interest to you.

11.5.1 Tor

For a more heavyweight network privacy solution, onion routing and the solutions it offers in terms of browsers and services may be worth your time. Tor is an open source anonymity network that provides an optimised anonymity approximation amongst its users - the Tor Browser is one of the simplest ways of accessing this network for the security and service benefits. The Tor Browser does not require the same hardening procedure as the Firefox browser mentioned earlier in this guide, but is slow due to the complex network procedure that must be completed for connections to be stable (use this article as a starting point for research regarding Tor and its benefits - https://en.wikipedia.org/wiki/Tor_(anonymity_network)).

If there is any take away from the use of Tor, it is that despite the fact that Tor can often provide the best approximation of network anonymity, this is a feature that cannot be guaranteed. Dark web services accessed through Tor can be malicious, illegal, disturbing, and host software that can monitor your activity and identity even despite the privacy measures the network goes to.

12 Restore Points

Once you have reached a point where you are happy with the hardening extent that you have gone to with your machine, you can create a Windows Restore Point. This is an in-built Windows roll-back mechanism for if you ever want to return your machine to the state that it is currently in. This provides a simple

way to return to a machine state that you know is completely secure - you may wish to do this if you accidentally install software that jeopardises the security of your device.

https://windowsreport.com/system-restore-point-windows-10/

13 Backups

There is no perfect guide for backups, the kind of information you plan on storing on your device (important documents, precious photographs, etc.) should direct your backup strategy as a whole. Backup strategies, along with password policies, can vary wildly. Unlike passwords, however, there are fewer hard truths and solid research surrounding the full extent that you must go to to back up your information assets. This is because their sensitivity, content, volatility, and environment are hugely variable - backups can also be controlled exclusively by you, should that be the strategy you choose. Passwords do not have this inherent attribute as their storage is never going to be exclusively controlled by you (in the case of online services).

For inspiration, some strategies are: cloud based, external hard drive oriented, distributed across multiple platforms (USBs, cloud, external hard drives), and system oriented (shadow drives on a working machine). Generally speaking, the more sensitive your information assets, the more frequently and diversely they should be backed up. Working files, e.g. important documents with impending time constraints, should also be backed up more frequently on some kind of trusted platform.

No one in the world of cyber security should convince you that a proper backup strategy is not required - these are massively important aspects of your personal security and can often be the only way to prevent mass data loss (unexpected ransomware). On a lighter note, there's an old saying: "If you haven't burned a roux, you've never made one", which is to say, if you haven't experienced a data breach of your own, you've not implemented your own backup strategy. Don't be in the majority, implement a backup strategy before the worst occurs (or, watch your roux's closely so they don't stick).

https://gardenandgun.com/articles/how-to-make-a-roux/

14 Encryption

Windows 10 has an in-built encryption mechanism for drive encryption (Bitlocker) - if you are looking to encrypt individual files, Windows 10 also provides an encryption service - this can be accessed under 'properties', and then 'advanced attributes' of the files in question (both can be accessed by right clicking the files you wish to encrypt).