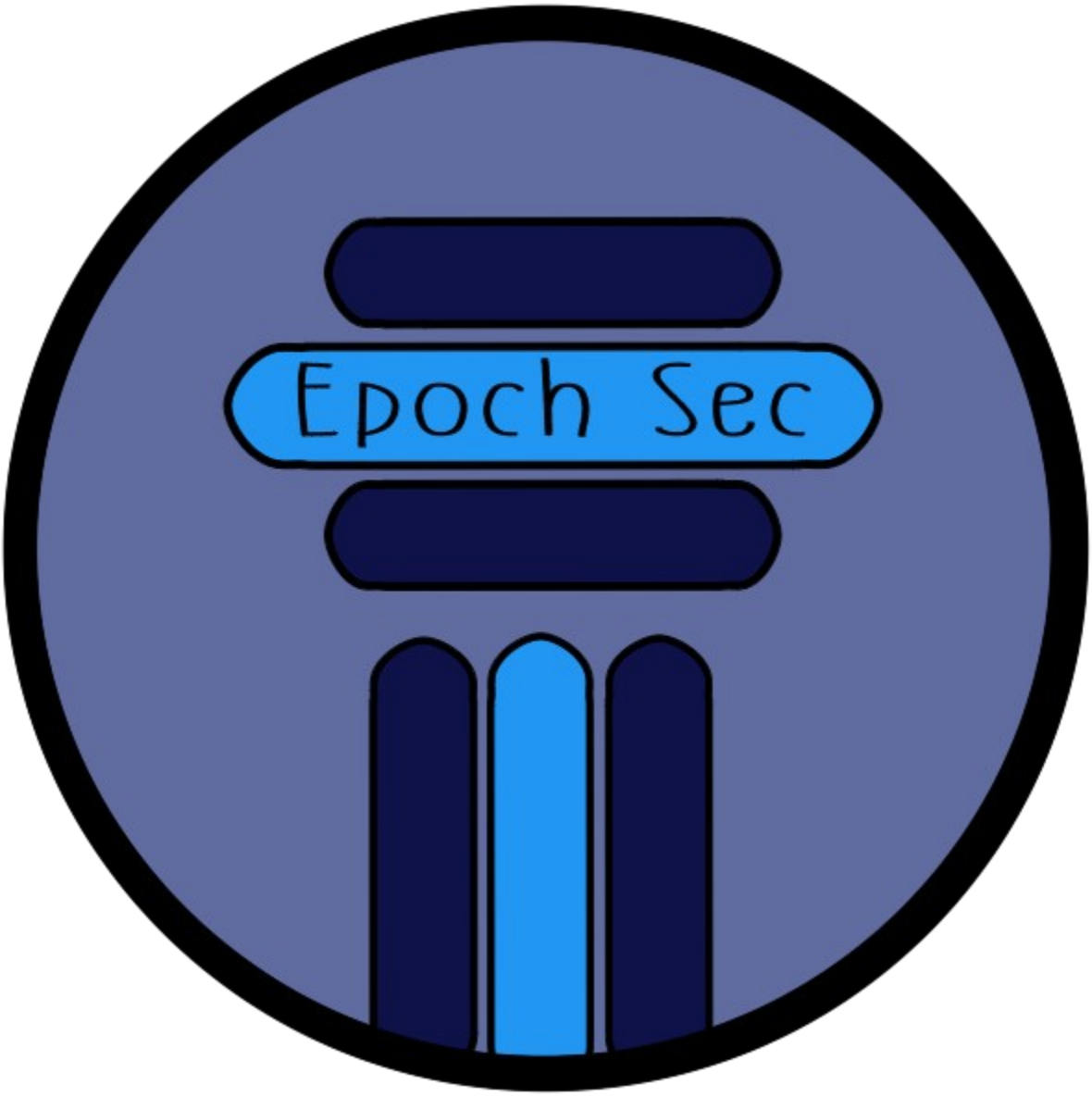

GENERAL OS (OPERATING SYSTEM) HARDENING

TABLE OF CONTENTS

OVERVIEW

The following document will cover topics around hardening your Operating System (i.e. laptop or desktop or server). Includes general OS hardening that applies to all OS's, plus Windows and Linux specific areas.

Hardening as a basic level, means to secure your system to prevent and reduce bad actors from accessing your system or compromising you.

A misconception is that one Operating System is more secure than another. Though in reality, all of them can and do face vulnerabilities. So, ensuring your system is secure is always important. What it boils down to is opportunity and Return of Investment for most Bad Actors.

There is much more that you can do outside of this article. I wanted to provide some key highlight information and a good starting point.

GENERAL OS HARDENING

These topics can generally be applied to most operating systems

USER ACCOUNTS

The term used in managing user accounts is RBAC, or Role Based Access Control.

- On all Operating Systems, create a separate account to be used as your daily user. This account should have minimal priviledges.
    - In Linux, do not use your root account. Use sudo or chmod with your daily account when necessary.
    - On Windows, you can also authenticate elevated privileges when needed and prompted.
        - Also, when setting up Windows for the first time, do not use your Microsoft Account. This is an online account. Instead, create your new user as a local account.

INSTALLS (OS) AND SOFTWARE

General guidance for new installs, new systems, and managing software

- On all Operating Systems, especially Linux distributions and Windows, start with a clean fresh install of the OS.
- In doing so, also ensure (if you have the knowledge, wipe any partitions prior to reformatting (installing new clean OS)
    - For Windows, use custom set up and decline the options. Do not use express. Read what you are choosing.
    - For Windows, a debloater tool can be used (Sycnex).
        - This will run a powershell script to remove all of the "bloatware", search index, unecessary scheduled tasks, remove cortana
    - For Linux, always choose to install minimum requirements

- Keep your installed software clean. Routinely manage your installed software and remove anything no longer being used.
    - Software, especially outdated or no longer support software, can introduce vulnerabilities and attack vectors for bad actors.
- Backup your data and create save points for events where you need to restore.
- Updates: Keep your systems up to date.
    - For the average daily user, simply keep your operating system and software updated. For the more advanced user, you can manage your updates manually.
    - Often zero-day attacks are introduce in updates. Therefor, security updates and patches are released to resolve these.
        - A zero-day attack is an attack using a vulnerability introduced, that has not been patched. Bad actors are always looking for these new vulnerabilities to exploit.

HARDWARE

Protecting and knowing your hardware is a common area overlooked. Take a look at some considerations below. Think of this like having a keypad to enter your yard. Once you can access your yard, then you can access your house (the OS).

- Disk encryption is an easy security measure to take to protect your system. At a high level, the MBR (Master Boot Record) is encrypted. Authentication to that (i.e. a password) is required. Then the OS will load. If you do not authenticate, the OS will not load.
- This protects against someone gaining your system or your drive. For example, if they try to put your drive into another system, the encrypted MBR is not available, therefor your OS will not load.
- Bitlocker for Windows is a good option (do not use Single Sign On for Bitlocker). For my Linux system, I believe it uses LUKS.
- Other considerations and notes provided to me:
- There are other options for encryption for Firmware and OS Level encryption. Suggest researching this for the users with technical knowledge. Otherwise, sticking to the basics above is a good path for daily users.
- Librem (Purism) has a line of products such as laptops, phones, mini computers, and servers. They rewrite and open source the BIOS and firmware.
    - I personally use a system from System76 with Pop_OS (their Ubuntu based OS with open source firmware)

VPN

A VPN is a virtual private network

- VPNs provide privacy and certain levels of anonymity. There is a larger debate to this topic. But for the average daily user, a VPN service is a good addition to your security.

- VPNs are also great privacy tools when on Public Wi-Fi. This will help in protecting you in the event a malicious network is joined.
    - Note: Bad actors will sometimes create a Wi-Fi network where other public Wi-Fi networks may be available. They may also try to use the same SSID (in other words, the name of the public network.) These are generally called man-in-the-middle attacks.
- Options:
    - NordVPN
    - OpenVPN
    - Wireguard

HOME NETWORK

Segmenting your home network

- Consider buying your own router. The routers provided by your ISP (Internet Service Provider are generally designed with poor hardware to save money)
- Create separate home networks. VLANS can be used on your router. A VLAN is a virtual network.
    - Assign categories of home devices to these different networks. For example: Separate TVs, your personal computers and devices, and your work devices. It is also a good idea to keep peripherals such as an Alexa on its own network.
- Look into pfSense if you want to try to build your own router
- Unify is a great option for getting a new router

WINDOWS

Below are some specific options to improve security of your system. Some specific Windows notes were described in the general section.

- Use Antivirus Software. Either use the Microsoft provided applications (Defender and Firewall), or look into third party solutions.
- Disable options that are likely already enabled:
    - Location tracking – Tracks your device
    - “Let Apps user Advertising ID” – This tracks activity and provided ads based on the Application activity.
- Powershell – Ensure your system does not keep older versions. Certain versions can run in parallel. The older a version, the higher the risk.
- Debloat: Earlier I mentioned a debloater tool to clean off unnecessary software on your Windows Computer. This is called Sycnex.
- Also mentioned earlier is to use a local account (you will need to create this), versus using your Microsoft account (which is an online account).
- Do not use automatic login.
- Do not sign into web browsers with your google account. Also do not sync your account across multiple devices. Applies to web browsers on any OS.
- Use SysInternals

    - This a tool distributed by Microsoft, and created by Mark Russinovich in 1996)
    - Provided many tools such as process scanning, monitoring services, monitoring logon sessions, port monitoring, and more. There are also tools such as Psinfo|PSkill|PSexec that you can use for a variety of tasks.

LINUX

Below are some specific options to improve security of your system. Some specific Linux notes were described in the general section.

Below, I will provide a checklist to follow:

- SSH
    - Disable root access for SSH. Use a new user account for SSH.
    - Change the default port (22) for SSH to something other than 22.
    - Disable “Password Login Authentication” for SSH.
        - Use a private/public key pair. Create these with the following encryption methods:
            - rsa 4096 (or above)
            - Or use ed25519
- Enable and configure UFW (Firewall)
    - If using as a server for a specific application, start off with blocking ALL and only allowing what is needed. If using for day to day workstation, this may be harder to achieve. So instead, you can only block what is needed.
- Use an IDS, such as Snort.
- Use an IPS, such as Fail2Ban. Great for intrusions and attacks such as DDOS
- Monitor traffic with tools such as netstat or nmap
    - nestat -tulpn | ss -tulpn | -sT for nmap
- User SELinux – Some benefits are:
    - RBAC (Role Based Access Control for user accounts
    - Rule based access for ports, processes, files, and directories

SCANNING AND PEN TESTING

Below are a few options for scanning your system for vulnerabilities

- Kali Linux
    - Kali Linux is a Linux Distributed which comes with a large list of tools at your disposal to test your system for a wide variety of potential vulnerabilities and flaws in your security.
    - This may be the best tool to begin with. While the learning curve may be steap, you will gain a great deal of knowledge on terminology, understanding activity on your system, better understanding network traffic, acitivity bad actors may use, and more.

    - An option to avoid also needing to know how to install and set up Kail Linux, is to use an image. Linode (another cloud service provider) is one option. They have an image for Kali Linux that makes it easier on you. I do not endorse them. That is simply an example.
- Another interesting example that I learned. Creating your own DOS or DDOS attack. Only use this on your system or application. Do not use this on something you do not own!
    - Hping3 – This is a simple tool for creating your own DOS attack
    - Saphyra – Another tool that can create DOS/DDOS attacks with advanced capabilities such as custom payloads for each ping.
    - Byob.dev
        - This is a build your own botnet service. This can be used along with the above tools to improve your DDOS testing.
        - Use these tools at your own risk. I do not endorse them. And you should not use them maliciously. Only use for personal testing of your own application that you own.

CONCLUSION

DO NOT BE AFRAID TO MISS AN OPPORTUNITY!

If you are not confident in a project or tool, do not engage and participate until you are confident. I would rather miss 9 out of 10 opportunities, instead of getting compromised 1 out of 100 times. It only takes once.

Keep in mind an easy tactic used by bad actors. That is obfuscation and is used along with Social Engineering and Phishing, which are the two most common attack methods (using vehicles such email, websites, and social media). Obfuscating is taking a domain URL, discord user or server, Twitter Account, or Telegram Account and make a very slight change in hopes that the user/target does not notice. So pay attention!