System Hardening Guidelines: Critical Best Practices

Wouldn’t it be amazing if our laptops were as secure as Fort Knox? Where it’s so hard for bad actors to access your sensitive data, that they don’t even try?

While operating systems, like Microsoft Windows, have become more secure over time, they’re nowhere close to being impenetrable. That’s why enterprises need to be hyper-vigilant about how they secure their endpoints. Endpoints – like employee workstations, servers and cloud VMs – are the gateways to your corporate network, which can and will be exploited by attackers.

Related content: Read our guide to Windows hardening.

System hardening is an even bigger challenge, as more sensitive devices move outside the secure office environments—and employees and contractors log in to sensitive corporate assets via unsecured or untrusted personal devices, or corporate devices that they use for mixed usage, and therefore also have a high level of risk.

This is part of an extensive series of guides about hacking.

What is a Hardened System?

Hardened systems are computing systems that are secured, with the goal of making them hack-proof. The process of hardening devices and systems involves eliminating or mitigating vulnerabilities. The term vulnerability refers to software flaws and weaknesses, which may occur in the implementation, configuration, design, or administration of a system. Threat actors exploit these vulnerabilities to hack into devices, systems, and networks.

Hardening techniques typically involve locking down configurations, achieving a balance between operational functionality and security. Vulnerability management and change control is another critical component of this effort. It introduces visibility and controls that can help you maintain a hardened build standard.

Tal Zamir
CTO, Perception Point

Tal Zamir is a 20-year software industry leader with a track record of solving urgent business challenges by reimagining how technology works.

TIPS FROM THE EXPERTS

1. **Utilize a zero-trust model for access control**
   Move beyond traditional perimeter-based defenses by adopting a zero-trust model, which requires continuous verification of user identity, device health, and application behavior, regardless of network location.
2. **Conduct regular red team exercises**
   Engage in adversarial simulation or red team exercises to identify weaknesses in your hardened systems. These simulations help uncover vulnerabilities that automated tools may miss, particularly in areas like user behavior and incident response.
3. **Deploy application allowlisting**
   Instead of just blocking known malicious applications, use allowlisting to ensure that only pre-approved, legitimate applications can execute on your systems. This drastically reduces the attack surface from unknown or new malware.

4. **Incorporate behavior analytics**
   Utilize User and Entity Behavior Analytics (UEBA) to detect deviations from normal behavior, which could indicate a compromised account or insider threat. This proactive approach can identify sophisticated attacks that bypass traditional security controls.

How Does System Hardening Reduce the Attack Surface?

The term “attack surface” refers to all potential flaws that threat actors can exploit to hack into a technological device, system, or network. The purpose of system hardening tools and techniques is to mitigate as many vulnerabilities as possible and reduce the attack surface.

There are several ways in which vulnerabilities may occur. Unpatched firmware and software, for example, can be exploited by attackers. Password vulnerabilities, such as hardcoded and default passwords or any credentials stored in plain text, can also create an exploitable attack surface.

Additional common vulnerabilities include unencrypted data-at-rest or network traffic, missing or poorly configured access controls, and misconfiguration of BIOS, ports, servers, firewalls, routers, switches, or any other infrastructure component. System hardening identifies these vulnerabilities and remediates them, thereby minimizing and hopefully eliminating the system’s attack surface.

The Benefits of System Hardening

The benefits of system hardening include:

1. **Enhanced Security:** By hardening a system, you reduce the potential attack surface and strengthen its defenses against various threats, such as malware, unauthorized access, and data breaches. This helps in safeguarding sensitive information and ensuring the privacy of users.
2. **Reduced Exploitation:** System hardening aims to eliminate or mitigate common vulnerabilities and weaknesses in software, operating systems, and network configurations. By doing so, it decreases the likelihood of successful exploitation by malicious actors, including hackers and malware.
3. **Improved System Performance:** Hardening measures often involve optimizing system resources, removing unnecessary services and software, and applying security patches and updates. These actions can lead to improved system performance, as fewer resources are wasted on unused or vulnerable components.
4. **Compliance with Security Standards:** Many industries and organizations have specific security standards and regulations that must be followed to protect sensitive data. System hardening helps meet these requirements and ensures compliance with industry-specific standards, such as the Payment Card Industry Data Security Standard (PCI DSS) or the Health Insurance Portability and Accountability Act (HIPAA).
5. **Business Continuity:** By hardening systems, you can enhance the resilience of your infrastructure against cyber threats. This reduces the likelihood of system disruptions, downtime, and financial losses resulting from successful attacks. It allows your business to maintain continuity, provide uninterrupted services, and protect its reputation.
6. **Defense in Depth:** System hardening contributes to a defense-in-depth strategy, where multiple layers of security measures are implemented. By employing various security controls, such as strong access controls, encryption, firewalls, intrusion detection systems, and regular security audits, you create multiple barriers that increase the difficulty for attackers to compromise your system.
7. **Proactive Security Posture:** System hardening is a proactive approach to security. It involves regular assessments and updates to address emerging threats and vulnerabilities. By continuously monitoring and improving the security of your systems, you can stay ahead of potential attackers and reduce the risk of successful attacks.

Overall, system hardening is an essential practice to mitigate risks, protect sensitive information, and ensure the secure operation of computer systems. It strengthens the overall security posture and contributes to a safer computing environment.

Types of System Hardening

There are several different types of system hardening techniques that can be implemented to enhance the security of a computer system. Here are some common types of system hardening:

1. **Operating System Hardening:** This involves securing the operating system by configuring it to minimize vulnerabilities. It includes actions such as disabling unnecessary services, closing unused ports, enabling security features like firewalls and intrusion detection systems, enforcing strong password policies, and regularly applying security patches and updates.
2. **Application Hardening:** Application hardening focuses on securing individual software applications running on the system. It involves actions such as removing or disabling unnecessary features and functionalities, applying application-specific security patches and updates, using secure coding practices, and enabling application-level access controls and authentication mechanisms.
3. **Network Hardening:** Network hardening aims to secure the network infrastructure and communication channels. It involves actions such as configuring firewalls, implementing intrusion prevention systems (IPS) and intrusion detection systems (IDS), enabling encryption protocols like SSL/TLS, segmenting the network to reduce the impact of a breach, and implementing strong network access controls.
4. **User Account Hardening:** User account hardening focuses on securing user accounts and their privileges. It includes actions such as enforcing strong password policies, implementing multi-factor authentication (MFA), limiting user privileges to only what is necessary, regularly reviewing and disabling unused accounts, and monitoring user activities for suspicious behavior.
5. **Patch Management:** Regularly applying security patches and updates is crucial for system hardening. Patch management involves monitoring and installing software updates, including operating system patches, firmware updates, and application patches. This helps to address known vulnerabilities and protect the system from exploitation.
6. **System Monitoring and Logging:** Implementing robust monitoring and logging mechanisms is essential for system hardening. It involves setting up security event logging, monitoring system logs for suspicious activities, implementing intrusion detection systems, and conducting regular security audits and reviews to identify and respond to potential threats in a timely manner.
7. **Secure Configuration Management:** Secure configuration management involves establishing and maintaining secure configurations for various system components, such as hardware, operating systems, and software applications. It includes actions like disabling unnecessary services and protocols, configuring access controls, enabling encryption, and implementing secure communication protocols.
8. **Security Awareness and Training:** System hardening also involves educating users and administrators about security best practices and potential threats. Conducting security awareness programs and training sessions helps to raise awareness about security risks, phishing attacks, social engineering, and other common attack vectors. It enables users to make informed decisions and follow secure practices.

These are some of the key types of system hardening techniques that can be employed to strengthen the security of computer systems. Implementing a combination of these techniques can significantly reduce the risk of successful attacks and enhance the overall security posture of a system.

Related content: Read our guide to Windows 10 hardening.

System Hardening Best Practices

While system hardening requires a large, continuous effort, it provides substantial benefits for organizations. Here are several notable benefits:

- **A higher level of security**: The main purpose of system hardening techniques and tools is to reduce the attack surface. This translates into a significantly lower risk of malware, unauthorized access, data breaches, or other malicious activity.
- **Better system functionalit**y: System hardening best practices often involve reducing the amount of programs and functionality. This translates into less operational issues, reduced chance of misconfiguration which can affect user operations, less incompatibilities, and also reduced change of cyber attacks, which in themselves hurt user functionality.
- **Simplified compliance and auditing**: System hardening techniques can help turn a complex environment into a simpler one with less programs and accounts, and stable, predictable configuration. This translates into a more straightforward and transparent environment which is simpler to monitor and audit.

Server Hardening and OS Hardening Best Practices

This strategy focuses on securing the operating system of a workstation or server. You can maintain a hardened state for an operating system by automating updates and patches. While operating systems are also a form of software, operating system hardening differs from regular application hardening in that the software here is responsible for granting permissions to other applications.

Operating system hardening methods include:

- Applying the latest updates released from the operating system developer (i.e. Microsoft, Apple)
- Enabling built-in security features such as Microsoft Defender or using 3rd party EPP/EDR software
- Deleting unneeded drivers and updating the ones that are used
- Restricting the peripherals that are allowed to be connected
- Encrypting the host drive using a hardware TPM
- Enabling Secure Boot
- Restricting system access privileges
- Using biometrics or FIDO authentication on top of passwords

Additional methods for hardening server systems include establishing a strong password policy, protecting sensitive data with AES encryption or self-encrypting drives, implementing firmware resilience technology and multi-factor authentication.

Related content: Read our guide to OS hardening.

Software Application Hardening Best Practices

This involves implementing software-based security measures to protect any standard or third-party application installed on a server. While server hardening seeks to secure the overall server system by design, application hardening focuses on securing specific applications, such as web browsers, spreadsheet programs, or custom software.

Application hardening techniques may include:

- Allowing installation only from trusted application repositories such as the Microsoft Store

- Automated patches of standard and third-party applications
- Firewalls, antivirus, and malware or spyware protection programs
- Software-based data encryption
- Password encryption and management applications such as LastPass

Network Hardening Best Practices

This approach secures the communication infrastructure for multiple systems and servers. You can achieve a hardened network state by implementing an intrusion prevention or detection system (IPS/DPS), which identifies suspicious network traffic.

These network hardening methods, when combined with an IPS or IDS, can help reduce the network's attack surface:

- Proper configuration of network firewalls
- Audits of network rules and access privileges
- Disabling unneeded network ports and network protocols
- Disabling unused network services and devices
- Network traffic encryption
- Intrusion prevention and detection systems (IPS/IDS)

Database Hardening Best Practices

This is the process of securing the contents of a digital database as well as the database management system (DBMS), which allows users to store and analyze the data in the database.

Database hardening techniques may include:

- Restricting administrative privileges
- Implementing role-based access control (RBAC) policies
- Maintaining regular software updates for the database and DBMS
- Restricting unnecessary database functions
- Locking database accounts with suspicious login activity

Using System Hardening Standards

An important first step when hardening a system is to establish a baseline. The baseline is a hardened state of the system, which you should aim to achieve, and then monitor the system to detect any deviation from this hardened state.

Usually, the hardening baseline is determined using a benchmark—a set of security best practices provided by security researchers. There are many reference sources for security benchmarks, including the SANS Institute, the National Institute of Standards and Technology (NIST), Microsoft, and Oracle. There are also many guides and forums on the Internet for hardening best practices. However, these different sources can provide inconsistent advice in an inconsistent format.

Which Benchmark Should You Use?

Many organizations are focusing their hardening baselines on the Internet Security Center (CIS) benchmarks. The CIS Benchmarks are a set of best practice configuration standards developed through consensus among various cybersecurity experts.

There are over 100 benchmarks available—covering most operating systems, server software, databases, desktop software, printers, and public cloud infrastructure. Because they have wide coverage and are highly authoritative, CIS benchmarks are an ideal starting point for hardening your systems.

Using a Benchmark to Harden Your Systems

The first step to using a benchmark is to perform an assessment of the target system, to understand how well the current configuration matches the relevant CIS benchmark. This initial assessment lets you identify areas where the system is not aligned with the required hardening baseline.

Manual assessment can be time consuming, especially for complex systems, but automated tools have been developed for many CIS benchmarks, which can allow you to test systems automatically.

Based on the assessment, you should modify system configuration to meet security recommendations.

Ongoing Assessment

Hardening a system to meet benchmark standards is only the first step. You should conduct periodic follow-up assessments to ensure that the system is still aligned with the hardening baseline. Any configuration or file changes could make it vulnerable to attack.

In order to maintain a hardened state, you should constantly re-evaluate and remediate any change to the system that violates the security benchmark.

8-Step System Hardening Checklist

System hardening differs between computing systems, and there may be different hardening procedures for each component of the same system (for example, for a BIOS, operating system and a database running on the same machine). However, there are general hardening tasks applicable to most computing systems. Here is a list of the most important tasks:

1. **Manage access**—ensure the system is physically secured, and staff are informed about security procedures. Set up custom roles and strong passwords. Delete unnecessary operating system users, and avoid the use of root or “super admin” accounts with excessive privileges. Limit membership of admin groups. Grant elevated privileges on an as-needed basis.
2. **Control network traffic—**install hardened systems behind a firewall, or if possible, isolated from public networks. Require VPN or reverse proxy to connect. Encrypt communications. Set firewall rules to restrict access to known IP ranges.
3. **Patch vulnerabilities**—keep operating systems, browsers and any other applications up to date and apply all security patches. Keep track of security advisories from vendors and latest CVEs.
4. **Remove unnecessary software**—uninstall any unnecessary software, remove redundant operating system components, disable unneeded services, and turn off any component or application feature that is not required and could expand the threat surface.

5. **Ongoing monitoring**—regularly review logs for anomalous activity, with a special focus on authentications, user access, and privilege escalation. Mirror logs to a separate location to protect log integrity and avoid tampering. Perform regular vulnerability and malware scans, and if possible, conduct an external audit or penetration test.
6. **Secure communications**—encrypt data transfer using strong ciphers. Close all but essential network ports, and disable insecure protocols like SMBv1, Telnet, and HTTP.
7. **Regular backups—**hardened systems are by definition sensitive resources, and must be regularly backed up using the 3-2-1 rule (three copies of the backup, on two types of media, with one copy stored off site).
8. **Harden remote sessions**—if you must allow SSH, ensure it uses a secure password or certificate, do not use the default port, and disable elevated privileges for SSH access. Monitor SSH logs to identify anomalous use or privilege escalation.

Challenges of System Hardening

System hardening is complex and labor intensive. Frustratingly, it is often not enough to prevent hackers from accessing sensitive company resources. The majority of malware comes from users clicking on emails, downloading files, and visiting websites that, unbeknownst to them, load viruses onto their systems. Once inside the operating system, attackers can easily gain access to privileged information.

To help combat this, some enterprises lock down users' devices so they can't access the internet, install software, print documents remotely, and more. However, this makes employees, and thus the business, much less productive. It's also incredibly frustrating to people just trying to do their jobs. As a result, users sometimes try to bypass those restrictions without understanding the implications.

IT teams trying to harden the endpoint OS, therefore, continually struggle between security and productivity requirements, especially when so much of the workforce is working remotely and BYOD has become more prevalent.

Another Way to Think About System Hardening with Perception Point Advanced Browser Security

The web has become cybercriminals' attack surface of choice. Thus, providing internet access to users while protecting against web attacks is the most persistent security challenge organizations face today. One way to harden enterprise networks and systems is to protect the enterprise browser ensuring that no malicious content ever penetrates the endpoint.

Perception Point Advanced Browser Security adds enterprise-grade security to standard browsers like Chrome, Edge, and Safari. The solution fuses advanced threat detection with browser-level governance and DLP controls providing organizations of all sizes with unprecedented ability to detect, prevent and remediate web threats including sophisticated phishing attacks, ransomware, exploits, Zero-Days, and more.

By transforming the organizational browser into a protected work environment, the access to sensitive corporate infrastructure and SaaS applications is secure from data loss and insider threats. The solution is seamlessly deployed on the endpoints via a browser extension and is managed centrally from a cloud-based console. There is no need to tunnel/proxy traffic through Perception Point.

An all-included managed Incident Response service is available for all customers 24/7. Perception Point's team of cybersecurity experts will manage incidents, provide analysis and reporting, and optimize detection on-the-fly. The service drastically minimizes the need for internal IT or SOC team resources, reducing the time required to react and mitigate web-borne attacks by up to 75%.

Customers deploying the solution will experience fewer breaches, while providing their users with a better experience as they have the freedom to browse the web, use SaaS applications that they require, and access privileged corporate data, confidently, securely, and without added latency.

Contact us for a demo of the Advanced Browser Security solution.

PERCEPTION POINT™
2024 ANNUAL REPORT:
CYBERSECURITY TRENDS & INSIGHTS
READ THE REPORT
PERCEPTION POINT™
2024 ANNUAL REPORT
Cybersecurity Trends & Insights
Presented by Perception Point

See Our Additional Guides on Key Hacking Topics

Together with our content partners, we have authored in-depth guides on several other topics that can also be useful as you explore the world of hacking.

Malware

Authored by Perception Point

Ransomware

Authored by Perception Point

Advanced Persistent Threat

Authored by Cynet