A Complete Windows Server Hardening Security Checklist

We will discuss server hardening in this blog, and we will also prepare a checklist that covers the areas that need to be protected against the most common exploits. They run the business and help employees share data and keep up their work. However, they are vulnerable to cyber-attacks. Many small businesses build or deploy physical servers by hand, but fail to protect them from hackers and data breaches. Follow our comprehensive checklist of Windows Server Hardening Security Checklist to reduce costly breaches or your attack surface and improve server security.

What Is Server Hardening?

In server hardening, several components, functions, and ports of a server are protected from security threats. It is a collection of techniques that improve security. By hardening a server, you reduce the probability of a cyber attack by implementing security measures such as firewalls, recovery procedures, and virus protection. In essence, server hardening is the process of putting in place protection mechanisms while also making critical computer systems more difficult to attack.

Windows Server Hardening Security Checklist

As cyber attackers are always trying to access the data and resources hosted on the servers, here are some controls and processes one should always put into practice for server security to protect them in real time. By using our general server security checklist, you will be able to identify vulnerabilities and errors, increase awareness of security issues, and improve the security of your servers.

“ alt=” A Complete Windows Server Hardening Security Checklist” />

1. User Configuration

Users without a defined account and who need occasional access use the Guest account. However, guests are less secure and are more likely to be targeted by attackers. In order to prevent attackers from discovering and misusing guest accounts, it is best to disable them and rename them on each server. In the same way, a local Administrator account is responsible for managing all files, directories, and other resources available to your local computer.

As this account contains a lot of information and is a popular target for hackers, be sure to disable it whenever possible and change its password. You should also use a strong password policy for each server account. To ensure that your system and administrator accounts remain safe and secure, make sure your passwords are at least 15 characters long with both lowercase and uppercase letters, numbers, and special characters.

2. Network Configuration

Make sure that only authenticated users have permission to access systems from the network, and disable all the network services the server is not using. The network firewall should be enabled to protect your system against external attacks and block inbound traffic. Secondly, your production servers should have static IP addresses to facilitate discovery by clients.

In order to protect your system, enable the Windows firewall and set it to block inbound traffic by default. Identify the ports that must remain open. Additionally, restrict access to ports and block them at the network setting level. You should have at least two DNS servers and establish production changes in advance. Also, verify the name resolution with nslookup.

3. Windows Features and Roles Configuration

In order to manage operating systems packages, Microsoft incorporates specific roles and features. Make sure each server role or set of software programs is properly configured and installed. They include customizable features, such as Internet Information Services. Perform the following steps to ensure the functions work smoothly and quickly: Make sure everything you need, such as the .NET framework and IIS, is installed properly. Any unnecessary components should be removed or uninstalled, as they can serve as an entry point for hackers or unauthorized users. Therefore, make sure your server design includes the necessary components.

4. Update Installation

It is important to keep your server secure by updating it from time to time. It doesn’t mean that you update as soon as a new update is released without seeing the results or checking the test reports. However, you will implement critical updates as soon as possible after reviewing the test results. There are various types of server updates rolling out, including:

1. A patch that addresses a single vulnerability.

2. Rollups for addressing multiple but related vulnerabilities.

3. Service packs for various vulnerabilities.

You should not update before checking the test results. To learn more about the updates, join the Microsoft user forums. In these forums, you will find out how the new update rolls out, what its benefits and drawbacks are, etc. It will help you make an informed decision, and based on that, you can make changes to your server.

5. NTP Configuration

A minimal time difference will also break Windows logons and other functions if you use Kerberos authentication. Hence, domain controllers must be synchronized to a time server to avoid any problems. It is common for member servers to be automatically synced with a domain controller after joining a domain, but there are some that stand alone and require NTP to sync with an external source for accurate timing.

It is important for security mechanisms, file system updates, and network management systems to maintain consistent timekeeping across the network. Therefore, if your server is not properly synced, set up Network Time Protocol (NTP). This configuration synchronizes computer clocks across networks.

6. Firewall Configuration

In order to prevent cyberattacks, a firewall must be configured correctly. Improper configuration can allow attackers to access protected network resources. Consequently, domain names and IP addresses must be configured correctly. Firewall policies help restrict incoming traffic to the necessary ports and routes.

As well, Windows firewalls come with a built-in software firewall that keeps network resources safe and limits the attack surface to the allowed ports. These firewalls are usually installed on stand-alone servers with security rules that prevent attackers from exploiting the ports by blocking or allowing access.

“ alt=” A Complete Windows Server Hardening Security Checklist” />

7. Remote Access Configuration

Your server can only be accessed via a VPN if it supports remote desktop (RDP) capabilities. If you leave it open, hackers are likely to get into your server through it. Therefore, it is important to limit access to RDP to authorized users only. RDP can be accessed by all administrators and other users by default. Therefore, make sure it’s only accessible to trusted administrators once it’s enabled on the server. In addition to RDP, you can find numerous other remote access mechanisms only accessible via VPN, such as PowerShell and SSH, which must also be managed carefully. Finally, we recommend using SFTP server or SSH (from a VPN).

8. Service Configuration

By default, the Windows server starts running a set of services in the background. Most of these services are essential to operating properly. However, there are some that should be disabled to prevent hackers from accessing the server or compromising other domains. Make sure to double-check your 2008 or 2003 servers as they may contain unneeded services. Running only vital services also allows you to recover the server without human interaction after a failure.

users with complex applications can set up service dependencies or use Automatic (Delayed Start). Finally, set up service-specific accounts with fewer privileges to keep malicious actors at bay and prevent them from spreading the compromise elsewhere.

9. Logging and Monitoring

As a result of the hectic nature of production schedules, analysts often forget the last and most important point, which is to ensure that all logs and monitoring are configured correctly. You should configure this feature so that if a problem arises, your data can be quickly remedied. It is important to establish an audit policy so that you can track which events are written and gain a better understanding of each activity.

In addition, a centralized event viewer can be useful for troubleshooting and remediating problems in various environments. Alternatively, you can use the built-in performance monitor in Windows or a third-party solution for this purpose. Monitor network activity, disk space, processor, and memory usage to identify hidden problems.

Conclusion

To strengthen server security, we have listed a few other key controls, processes, and practices in this post on Windows Server Hardening Security Checklist. These basic practices help you harden your server and protect it against real-time security threats. A server is used for storing sensitive data and sharing resources over the network. If your server's security is weak, there is a high chance that cyber attackers will target your server and attack it.

As hackers believe servers hold the most valuable information, it is imperative that you implement techniques and tools to safeguard your server. In summary, you can protect your crucial data by implementing strong server security best practices. The server hardening process reduces your attack surface while protecting your vital data.

The Windows firewall should be enabled to block the inbound traffic. Guest accounts should be disabled on the server and a strong password policy applied to each account. The default behavior of the Windows firewall should be configured to block inbound traffic. Keep your server up-to-date and avoid running new updates before confirming the test results. You can also learn more about user experience on Microsoft forums.

https://blog.arashtad.com/blog/a-complete-windows-server-hardening-security-checklist/?feed_id=6866&_unique_id=6663e2ce29275