

Web Server Security

A secure web server provides a protected foundation for hosting your web applications, and web server configuration plays a critical role in your web application's security. Poorly configured virtual directories, a common mistake, can lead to unauthorized access. A forgotten file share can provide a convenient back door, while an overlooked port can be an attacker's front door. Neglected user accounts can permit an attacker to slip by your defenses unnoticed.

Let's take a look at some of the areas in which you can take immediate steps to ensure that your server is secure. The following are guidelines to help you define specific parameters and general rules that can lead you to a secure configuration:

Patches and Updates

Many security threats are caused by vulnerabilities that are widely published and well known. In many cases, when a new vulnerability is discovered, the code to exploit it is posted on Internet bulletin boards within hours of the first successful attack. If you do not patch and update your server, you provide opportunities for attackers and malicious code. Patching and updating your server software is a critical first step towards securing your web server.

Services

Services are prime vulnerability points for attackers - they know how to exploit the privileges and capabilities of a service to access the local web server or other downstream servers. If a service is not integral to your web server's operation, do not run it on your server. If the service is necessary, secure it and maintain it. Consider monitoring any service to ensure availability. If your service software is not secure, but you require it, try to find a secure alternative.

Protocols

Avoid using clear text protocols that are inherently insecure, for example, Telnet, Post Office Protocol (POP3), Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP). If you cannot avoid using these protocols, take the appropriate measures to provide secure authentication and communication, for example, by using IPSec policies.

Accounts

Accounts grant authenticated access to your computer, and these accounts must be audited. Begin by asking yourself some of the following questions: What is the purpose of the user account? How much access does it have? Is it a common account that can be targeted for attack? Is it a service account that can be compromised and must therefore be contained? Configure accounts with the fewest privileges possible to help prevent elevation of privilege. Remove any accounts that you do not need. Slow down brute force and dictionary attacks with strong password policies, and then audit and alert for logon failures.

Files and Directories

Secure all files and directories with restricted NTFS permissions that only allow access to necessary Windows services and user accounts. Use Windows auditing to allow you to detect when suspicious or unauthorized activity occurs.

Shares

Remove all unnecessary file shares including the default administration shares if they are not required. Secure any remaining shares with restricted NTFS permissions. Although shares may not

be directly exposed to the Internet, a defense strategy — with limited and secured shares — reduces risk if a server is compromised.

Ports

Services that run on the server listen to specific ports so that they can respond to incoming requests. Audit the ports on your server regularly to ensure that an insecure or unnecessary service is not active on your web server. If you detect an active port that was not opened by an administrator, this is a sure sign of unauthorized access and a security compromise.

Registry

Many security-related settings are stored in the registry and as a result, you must secure the registry. You can do this by applying restricted Windows ACLs and by blocking remote registry administration.

Auditing and Logging

Auditing is one of your most important tools for identifying intruders, attacks in progress, and evidence of attacks that have occurred. Use a combination of Windows and IIS auditing features to configure auditing on your web server. Event and system logs also help you to troubleshoot security problems.

Sites and Virtual Directories

Sites and virtual directories are directly exposed to the Internet. Even though secure firewall configuration and defensive ISAPI filters can block requests for restricted configuration files or program executables, an in-depth defensive strategy is recommended. Relocate sites and virtual directories to non-system partitions and use IIS web permissions to further restrict access.

Script Mappings

Remove all unnecessary IIS script mappings for optional file extensions to prevent an attacker from exploiting any bugs in the ISAPI extensions that handle these types of files. Unused extension mappings are often overlooked and represent a major security vulnerability.

IIS Metabase

The IIS metabase maintains IIS configuration settings. You must be sure that the security-related settings are appropriately configured, and that access to the metabase file is restricted with hardened NTFS permissions.

Staying Secure

To help prevent newly discovered vulnerabilities from being exploited, you need to be vigilant in monitoring the security status of your server and updating it regularly. To help keep your server secure:

- Audit group membership
- Monitor audit logs
- Stay current with service packs and patches
- Perform security assessments
- Use security notification services