www.certifiedsecure.com
info@certifiedsecure.com
Tel.: +31 (0)70 310 13 40
Loire 128-A
2491 AJ The Hague
The Netherlands

Certified Secure Server Configuration Checklist

About

Certified Secure exists to encourage and fulfill the growing interest in IT security knowledge and skills. We stand for openness, transparency and the sharing of knowledge; making sure everybody can experience and enjoy IT security. Security is serious fun!

All Certified Secure certifications, products and training are developed by IT security professionals with international recognized expertise. Our involvement in the IT security community worldwide, ensures relevant and high-quality standards. Delivering a wide variety of online challenges, videos, tools and more, Certified Secure is the authoritative source for practical IT security know-how.

Scope

This checklist can be used as a standard for installing, configuring or auditing a server. For performing a remote server security test a separate Server Security Test Checklist is available from https://www.certifiedsecure.com/checklists.

Usage

System administrators should use this checklist when installing or configuring a server. Server auditors should use this checklist when performing a white box audit of a server. A risk analysis for the server should be performed before starting with the checklist. Every control on the checklist should be completed or explicitly marked as being not applicable. Once a control is completed the checklist should be updated with the appropriate result icon and a document cross-reference.

The completed checklist should never be delivered standalone but should be incorporated in a report detailing the risk analysis and checklist results. When performing a white box server audit the report should also include the scope and context of the performed audit.

License

Result Icon Legend

Icon	Explanation
✓	Test was performed and results are okay
✗	Test was performed and results require attention
■	Test was not applicable

#	Certified Secure Server Configuration Checklist	Result	Ref
1.0	**Generic**		
1.1	Always adhere to the principle of least privilege		
2.0	**Version Management**		
2.1	Install security updates for all software		
2.2	Never install unsupported or end-of-life software		
2.3	Install software from a trusted and secure repository		
2.4	Verify the integrity of software before installation		
2.5	Configure an automatic update policy for security updates		
3.0	**Network Security**		
3.1	Disable all extraneous services		
3.2	Disable all extraneous ICMP functionality		
3.3	Disable all extraneous network protocols		
3.4	Install a firewall with a default deny policy		
3.5	Firewall both incoming and outgoing connections		
3.6	Disable IP forwarding and routing unless explicitly required		
3.7	Separate servers with public services from the internal network		
3.8	Remove all dangling DNS records		
3.9	Enable DNS record signing		
4.0	**Authentication and Authorization**		
4.1	Configure authentication for access to single user mode		
4.2	Configure mandatory authentication for all non-public services		
4.3	Configure mandatory authorization for all non-public services		
4.4	Configure mandatory authentication for all users		

#	Certified Secure Server Configuration Checklist	Result	Ref
4.5	Enforce the usage of strong passwords		
4.6	Remove all default, test, guest and obsolete accounts		
4.7	Configure rate limiting for all authentication functionality		
4.8	Disable remote login for administrator accounts		
4.9	Never implement authorization based solely on IP address		
5.0	**Privacy and Confidentiality**		
5.1	Configure services to disclose a minimal amount of information		
5.2	Transmit sensitive information via secure connections		
5.3	Deny access to sensitive information via insecure connections		
5.4	Store sensitive information on encrypted storage		
5.5	Never use untrusted or expired SSL certificates		
5.6	Configure SSL/TLS to accept only strong keys, ciphers and protocols		
5.7	Configure an accurate and restrictive CAA DNS record		
5.8	Use only widely accepted and proven cryptographic primitives		
5.9	Use existing, well-tested implementations of cryptographic primitives		
5.10	Separate test, development, acceptance and production systems		
5.11	Never allow public access to test, development and acceptance systems		
5.12	Never store production data on non-production systems		
5.13	Configure a secure default for file permissions		
5.14	Configure file permissions as restrictive as possible		
5.15	Disable the indexing of files with sensitive information		
5.16	Configure automated removal of temporary files		
6.0	**Logging Facilities**		

#	Certified Secure Server Configuration Checklist	Result	Ref
6.1	Restrict access to logging information		
6.2	Configure logging for all relevant services		
6.3	Configure logging for all authentication and authorization failures		
6.4	Configure remote logging for all security related events		
6.5	Routinely monitor and view the logs		
6.6	Never log sensitive information, passwords or authorization tokens		
7.0	**Service Specific**		
7.1	Complete the Secure Development Checklist for Web Applications		
7.2	Disable open relaying for mail services		
7.3	Disable email address enumeration for mail services		
7.4	Disable anonymous uploading for FTP services		
7.5	Disable unauthorized AXFR transfers in the DNS		
8.0	**Miscellaneous**		
8.1	Configure rate limiting for all resource-intensive functionality		
8.2	Prevent unintended denial of service when configuring rate limiting		
8.3	Check configuration of all services for service-specific issues		
8.4	Check for and mitigate server- or setup-specific problems		