

---

## Certified Secure Server Security Test 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 when performing a remote security test on a server. For system administrators and auditors a separate Server Configuration Checklist is available from <https://www.certifiedsecure.com/checklists>.

### Usage




Security testers should use this checklist when performing a remote security test of a server. A risk analysis for the server should be performed before starting with the checklist. Every test on the checklist should be completed or explicitly marked as being not applicable. Once a test 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 and the scope and context of the performed remote security test.

### License

This work is licensed under a Creative Commons Attribution No Derivatives 4.0 International License. The complete Creative Commons license text can be found online at <https://creativecommons.org/licenses/by-nd/4.0/legalcode>

### 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 Security Test Checklist	Result	Ref
<b>1.0</b>	<b>Version Management</b>		
1.1	Test all services for missing security updates		
1.2	Test all services for unsupported or end-of-life software versions		
<b>2.0</b>	<b>Network Security</b>		
2.1	Test for extraneous services		
2.2	Test for extraneous ICMP functionality		
2.3	Test for extraneous enabled network protocols		
2.4	Test for firewall evasion using common techniques		
2.5	Test for dangling DNS records		
2.6	Test for missing DNS record signing		
<b>3.0</b>	<b>Authentication and Authorization</b>		
3.1	Test all services for missing authentication		
3.2	Test all services for missing authorization		
3.3	Test all services for predictable credentials		
3.4	Test all services for default, test, guest and obsolete accounts		
3.5	Test all services for missing rate limiting on authentication functionality		
<b>4.0</b>	<b>Privacy and Confidentiality</b>		
4.1	Test all services for disclosure of extraneous information		
4.2	Test all services for insecure transmission of sensitive information		
4.3	Test all services for weak, untrusted or expired SSL certificates		
4.4	Test all services for known vulnerabilities in SSL/TLS		
4.5	Test for a missing or incorrectly configured CAA record in DNS		
4.6	Test all services for the usage of unproven cryptographic primitives		



#	Certified Secure Server Security Test Checklist	Result	Ref
4.7	Test all services for incorrect usage of cryptographic primitives		
4.8	Test for publicly accessible test, development and acceptance systems		
4.9	Test for production data stored on non-production systems		
<b>5.0</b>	<b>Service Specific</b>		
5.1	Test web services using the Web Application Security Test Checklist		
5.2	Test mail services for open relaying		
5.3	Test mail services for email address enumeration		
5.4	Test FTP services for anonymous file uploading		
5.5	Test DNS services for unauthorized AXFR transfers		
<b>6.0</b>	<b>Miscellaneous</b>		
6.1	Test for missing rate limiting on resource-intensive functionality		
6.2	Test for inappropriate rate limiting resulting in a denial of service		
6.3	Test all services for service-specific issues		
6.4	Test for server- or setup-specific problems		