

Exam requirements

Security Certified Network Professional (SCNP.EN)

Publication date 01.12.2009

Start date 01.06.2009

Summary

The Strategic Infrastructure Security (SIS) exam SC0-471 tests the knowledge and skills for the Security Certified Network Professional (SCNP) certification. It focuses on prevention techniques and the understanding of risk analysis and security policy creation in a blended technology environment.

Strategic Infrastructure Security begins where Tactical Perimeter Defense ends. The subjects are:

- Cryptography
- Hardening Linux
- Hardening Windows
- Ethical Hacking Techniques
- Security on the Internet and WWW
- Risk Analysis
- Security Policy
- Analyzing Packets

Target group

Security Certified Network Professional (SCNP) gives network administrators the additional hands on skills needed to protect their network from the inside out.

Context

The SCNP module fits in EXIN's Information Security program, which has a managerial and a technical stream. SCNP is positioned in the technical stream of the qualification scheme. The Security Certified Program in the technical stream offers three certifications to validate IT professionals' security skill sets, of which SCNS is the first. SCNS is a required pre-requisite for going further towards the SCNP and SCNA certifications.

Prerequisites

Candidates must have successfully completed the Tactical Perimeter Defense exam, SC0-451, and hold an SCNS certification in good standing. The SCNP Strategic Infrastructure Security Course, delivered by an SCP Authorized Training Partner, is recommended. As the security industry moves quickly, skills require consistent validation. The SCNP credential is valid for two years from the pass date. Recertification is required to maintain good standing.

Practical assignment

Not applicable

Examination details

| | |
|--|---|
| Examination type: | Computer-based or paper-based multiple-choice and multiple-response questions |
| Time allotted for examination: | 90 minutes |
| Number of multiple-choice/response questions | 60 |
| Pass mark: | 75% |

(45 marks out of 60 marks)

Open book: No
Electronic equipment permitted: no

Sample questions A sample exam (cd-rom or online usage) can be bought from MeasureUp at www.measureup.com.

| | | |
|--------------------------|----------------------------------|-----|
| Exam requirements | 1. Analyzing Packet Structures | 5% |
| | 2. Creating Security Policies | 5% |
| | 3. Performing Risk Analysis | 5% |
| | 4. Ethical Hacking Techniques | 10% |
| | 5. Internet and WWW Security | 15% |
| | 6. Cryptography | 20% |
| | 7. Hardening Linux Computers | 20% |
| | 8. Hardening Windows Server 2003 | 20% |

Specification of the exam requirements

| | |
|---------------------------------------|--|
| 1. Analyzing Packet Structures | 1.1 Describe the Concepts of Signatures Analysis |
| | 1.2 Examine the Common Vulnerabilities and Exposures (CVE) |
| | 1.3 Examine Normal Network Traffic Signatures |
| | 1.4 Examine Abnormal Network Traffic Signatures |
| 2. Creating Security Policies | 2.1 Examine the Concepts of Security Policies |
| | 2.2 Identify Security Policy Categories |
| | 2.3 Define Incident Handling Procedures |
| 3. Performing Risk Analysis | 3.1 Examine the Concepts of Risk Analysis |
| | 3.2 Define the Methods of Risk Analysis |
| | 3.3 Describe the Process of Risk Analysis |
| | 3.4 Examine Techniques to Minimize Risk |
| 4. Ethical Hacking Techniques | 4.1 Perform Network Scanning and Discovery |
| | 4.2 Describe Network Viruses, Trojans, and Worms |
| | 4.3 Examine Social Engineering |
| | 4.4 Describe Privilege Escalation |
| | 4.5 Examine the Concepts of Denial of Service |
| | 4.6 Exploiting Password Weaknesses |
| 5. Internet and WWW Security | 5.1 Identify and Define the Weak Points in the Structure of the Internet |
| | 5.2 Define Web Site Attack Techniques |
| | 5.3 Define Attack Techniques of Web Users |
| | 5.4 Hardening Web Servers |
| | 5.5 Hardening DNS Servers |
| 6. Cryptography | 6.1 Historical Cryptography |
| | 6.2 Cryptographic Algorithms |
| | 6.3 Private Key Exchange |
| | 6.4 Public Key Exchange |
| | 6.5 Message Authentication |

7. Hardening Linux Computers

- 7.1 Linux File system and Navigation
- 7.2 Secure System Management
- 7.3 User and File system Security Administration
- 7.4 Secure Network Communications
- 7.5 Security Scripting
- 7.6 Linux Security Tools

8. Hardening Windows Server 2003

- 8.1 Windows Server 2003 Infrastructure Security
- 8.2 Examine Windows Server 2003 Authentication
- 8.3 Implement Windows Server 2003 Security Configuration Tools
- 8.4 Configure Windows Server 2003 Resource Security
- 8.5 Configure Windows Server 2003 Auditing and Logging
- 8.6 Configure Windows Server 2003 Network Security

List of basic concepts

This section contains the terms with which candidates should be familiar. Terms are listed in alphabetical order.

- A and PTR Records
- Active Directory Integrated Zone
- Algorithm
- Apache Web Server
- Cryptography
- Denial of Service
- Data Encryption Standard (DES)
- Diffie-Hellman
- DNS Server
- Escalation
- IIS (Internet Information Services) Security
- Incident Handling
- IP Spoofing
- Linux
 - Bastille
 - Export Permission
 - John the Ripper
 - Pluggable Authentication Module (PAM)
 - Runlevels
 - Samba Server
 - Secure Copy (SCP)
 - Sshd_config File
 - TCP Wrappers
 - Tripwire
 - Umask
 - Vi and emacs
 - Webmin
 - Xinetd
 - YaST
 - Yast Online Update (YOU)

- Microsoft Baseline Security Analyzer (MBSA)
- Message Authentication
- Network Reconnaissance
- Packet Signature
 - Abnormal Traffic Signature
 - Normal Traffic Signature
- Pollution
- Polybius Cryptography
- Primary Forward Lookup Zone
- Primary Reverse Lookup Zones
- Private Key Exchange
- Public Key Exchange
- Recursion
- Risk Assessment
- RSA Encryption
- Secondary Zone
- Security Policies
- Social Engineering
- Stub Zone
- Sweeping the network
- Trojan Horse
- Windows 2003 EFS
 - Group Policy (GPO)
 - Microsoft Management Console (MMC)
 - NT LAN Manager (NTLMv2)
 - Port filtering
 - Protocol filtering
 - Security Accounts Manager (SAM)
- Zone Transfers

Literature

A.

SC

Strategic Infrastructure Security

SCP Authorized Courseware for the Security Certified Network Professional

www.securitycertified.net



| Exam requirement | Literature |
|------------------|---------------------|
| 1 | A: Chapter 8 |
| 2 | A: Chapter 7 |
| 3 | A: Chapter 6 |

| Exam requirement | Literature |
|-------------------------|---------------------|
| 4 | A: Chapter 4 |
| 5 | A: Chapter 5 |
| 6 | A: Chapter 1 |
| 7 | A: Chapter 2 |
| 8 | A: Chapter 3 |

EXIN, Examination Institute for Information Science, is the certification organization that independently develops and delivers the certifications for the Security Certified Program.

Copyright © 2009 EXIN

All rights reserved. No part of this publication may be published, reproduced, copied or stored in a data processing system or circulated in any form by print, photo print, microfilm or any other means without written permission by EXIN.

EXIN, Examination Institute for Information Science, is the certification organization that independently develops and delivers the certifications for the Security Certified Program.