

An **OPSA certified professional** is a security analyst who has the skills and knowledge to analyze a security posture of a company, network, or product and provide the insight on how to improve its security defenses.

Purpose

To be able to design an overall security strategy detailing specific defense tactics based on system information, network information, security scans, penetration test results, and usage.

Requirements

Linux Skill: Low

Windows Skill: Low

Networking Knowledge: Medium

Security Experience: Medium

Business Experience: Medium

Recommended: OPSE or CHA certifications

Training

Average Training Time Required: 32 hours

The exam requires mastering the application of the following security analysis skills:

- Comprehend network and security scans.
- Evaluate testing techniques and scope to assure results.
- Detect and properly act on anomalies, patterns, and vulnerabilities.
- Evaluate attack surface and determine appropriate controls.
- Calculate and measure the level of security.
- Techniques to analyze new or unknown systems or technologies.
- Assure proper reporting and create an OSSTMM Audit Report (STAR).

Exam

Exam time: 3 hours

Questions: 50 multiple choice, single answer, skills-based.

Passing: 60% or better for certification. Scores of 90% or better include a seal of excellence.

