Certifications Part Two: Security Certifications

By Shawn Conaway

Information security spans many different roles and responsibilities. Growth in the available number of security certifications now provides enough variety for IT professionals to choose a certification that best meets their career goals. Why not get a security certification to validate your skills? This article provides details on the many different security certifications available today.

REMEMBER that dream? The one where you are at school and you realize you aren't wearing any pants? Or the other dream where you are running and running as hard as you can, but you can't seem to get anywhere? Sometimes managing security can be a lot like a bad dream. You don't want the private parts of your network exposed to the public. You don't want to get caught with your pants down when unsecured and un-patched systems allow your network to be compromised. Remember W32.Blaster.Worm? Cleaning up that mess was like running in place—once one system was cleaned and patched, two more computers got infected.

Protection from virus attacks, distributed denial of service attacks and hackers is a necessary evil. Private networked systems are increasingly being exposed to the world through Internet-enabled technologies like Web services, B2B portals, customer portals, and remote access technologies. Odds of attack are increased when these varied pathways onto your network are combined corporate policies that allow for weak passwords and non-removal of stale user accounts.

Mediating security risk is achieved by adopting a security posture that enforces organizational security policies and procedures. Security by obscurity can't match the good physical security, auditing and monitoring, and a secure infrastructure.

Given the diversity of potential security exploits, there are now more information security roles than Baskin Robbins has flavors. Confucius was right when he said, "He who wishes to secure the good of others, has already secured his own." Said another way, computer security is job security.

Security officers with an eye on their own job security can close security holes by securing wireless networks with firewalls and private keys, auditing and monitoring systems for performance or intrusion, implementing password strength and length policies, maintaining security patch levels, disabling unneeded system services, and using computer forensics techniques to identify attempted and successful hacker attacks. Certifications that specialize in these areas are listed below. Becoming certified will validate that you have the skills for which the certification was designed.

CIW

CIW got their name from the first certification they offered—the Certified Internet Webmaster. Later, they expanded their technical certification offerings and shortened their name to CIW. One of their newer certifications is the CIW Security Analyst.

The target audience for the CIW Security Analyst certification is technical professionals who are already skilled in networking administration. These professionals already hold a premium certification from Microsoft, Novell Cisco or a Linux certification from LPI or SAIR. The one-certification track allows them to validate their security skills or to develop their skills quickly.

Candidates are tested on their knowledge of network security, firewalls, operating system security, security auditing principles, threat analysis and identification, encryption, system permissions, and identification of penetration strategies.

COMPTIA

The Computing Technology Industry Association offers the Security+ certification as well as many other entry-level and mid-level vendor-neutral certifications. The target audience for the Security+ certification is IT professionals with two years of networking experience.

The test covers five areas:

- General Security Concepts such as authentication methods, recognizing and reacting to an attack, social engineering and auditing.
- Communication Security including e-mail and Internet security, SSL and HTTPS.

- Infrastructure Security covering hardware such as firewalls, routers and switches, as well as physical security.
- Basics of Cryptography
- Operational and Organizational Security, which covers physical security, biometrics, disaster recovery plans, and business continuity.

The Security+ also qualifies as an elective for the Microsoft Certified Systems Engineer (MCSE).

TRUSECURE

TruSecure offers the vendor-neutral TruSecure ICSA Security Practitioner Certification (TICSA). TruSecure says the TICSA was designed to 'validate and improve foundation-level IT security skills.' The target audience for this certification is network administrators, systems administrators and other IT personnel.

Certification requirements:

- Two years of network security administration experience or attendance of at least 48 hours of approved computer security training or coursework.
- Accept the code of ethics
- Complete an online profile
- Pass the test

The TICSA certification is good for two years. The testing criteria for the certification are based on the TruSecure Essential Body of Knowledge (EBK) and the TruSecure ICSA Six Categories of Risk. The EBK includes:

- Security Practices and Procedures
- Security Fundamentals
- Firewall Management Fundamentals
- Detection, Response and Recovery
- Design and Configuration Basics
- Malicious Code Fundamentals
- Authentication
- Cryptography
- Host-Based vs. Network-Based Security
- PKI

(ISC)^2

The International Information Systems Security Certification Consortium offers a number of vendor-neutral certifications. They offer two main certifications—the Certified Information Systems Security Professional (CISSP) and the Systems Security Certified Practitioner (SSCP). They also have three 'concentrations,' which are additional certifications that can be added on to the CISSP. The concentrations are: the Information Systems Security Engineering Professional (ISSEP), the Information Systems Security Architecture Professional (ISSAP), and the Information Systems Security Management Professional (ISSMP). Finally, they offer the (ISC)2 Associate designation—not certification—for security novices who intend to become a SSCP or CISSP certified.

The (ISC)^2 has identified security information areas which they refer to as the 'Common Body of Knowledge' or CBK. A candidate for the six-hour long CISSP exam has to demonstrate his 'working knowledge' of the CBK by answering 250 questions in all 10 areas of the CBK which include:

- Security Management Practices
- Security Architecture and Models
- Access Control Systems and Methodology
- Application Development Security
- Operations Security
- Physical Security
- Cryptography
- Telecommunications, Network and Internet Security
- Business Continuity Planning
- Law, Investigations and Ethics

The SSCP exam is three hours long and consists of 125 multiple-choice questions. The SSCP has to prove he is knowledgeable in these seven areas of the CBK.

You are eligible to take the SSPC or CISSP exams if you:

- Pay the application fee ($499 for CISSP, $369 for SSCP)
- CISSP candidates must have four years of professional experience. A Bachelor's degree can substitute for one year. A Master's degree in information security from a National Center of Excellence can substitute for another year.
- SSCP candidates need one year of professional experience.
- Accept the code of ethics
- CISSPs: Answer four questions regarding criminal history and related background successfully.

The SSPC and CISSP require a passing the exam with a score of 700 points. The CISSP also requires that a qualified third party affirm the candidate's professional experience and good standing in the information security industry.

Concentrations:

The ISSEP was developed with the US National Security Agency to ensure CISSPs have the knowledge to perform as Information Systems Security Engineers and to provide a method to demonstrate their competency in information security engineering. The competencies measured by the ISSEP exam are:

- Systems Security Engineering
- Certification and Accreditation
- Technical Management
- U.S. Government Information Assurance Regulations

The ISSMP provides a method for security professionals to demonstrate their knowledge of security management. The ISSMP exam focuses on:

- Enterprise Security Management Practices
- Enterprise-Wide System Development Security
- Overseeing Compliance of Operations Security
- Understanding BCP, DRP and COOP
- Law, Investigations, Forensics and Ethics

The ISSAP provides CISSPs with a way to prove their expertise in Security Architecture. The ISSAP exam covers:

- Access Control Systems and Methodologies
- Telecommunications and Network Security
- Cryptography
- Requirements Analysis and Security Standards, Guidelines, Criteria
- Technology-Related BCP and DRP

The concentration exam fee is $349. The ISSMP and ISSAP exam consists of 125 questions (100 exam and 25 pre-test). The ISSEP exam is 150 questions long (125 exam questions and 25 pretest). The exams are all three hours long.

Alternative path:

The CCSP and CISSP certifications require some degree of security experience. Candidates with little or no security experience can sign up for the (ISC)^2 Associate Program. The designation is achieved by passing the CISSP or SSCP exam without having the security experience. The (ISC)^2 Associate for SSCP designation is valid for two years. The (ISC)^2 Associate for CISSP designation is valid for five years. The SSCP certification is achieved when the candidate acquires the necessary experience. The CISSP certification is achieved by both gaining the appropriate experience and submitting the required endorsement.

The catch

Cancellations: You have to pay $100 to cancel or reschedule with less than 22 days notice. You get no refund if you cancel with less than five days notice.

Maintaining your certification: A CISSP must complete 120 continuing professional education (CPE) credits every three years and pay an annual $85 maintenance fee. A $35 annual fee per concentration is also required. An SSCP must complete 60 CPEs every three years and pay a $65 annual fee. (ISC)^2 Associates are not required to complete CPEs but must pay a $35 annual fee.

THE SANS INSTITUTE

The SANS (**S**ysAdmin, **A**udit, **N**etwork, **S**ecurity) Institute offers an array of training covering entry-level topics such as Security Essentials to advanced topics like intrusion detections, forensics and hacking techniques. SANS founded the Global Information Assurance Certification (GIAC) program to provide certifications that complement SANS training.

GIAC candidates must complete a written "practical assignment." Once completed, the candidates must also pass a technical exam to achieve a certification. SANS offers a plethora of GIAC certifications which include:

- GIAC Security Essentials Certification (GSEC) - An entry-level certification that tests essential security knowledge and skills.
- GIAC Information Security Fundamentals (GISF) - The GISF certification track helps security novices learn best practices that will help them identify and communicate information resource threats to management.
- GIAC Systems and Network Auditor (GSNA) - The GSNA is for auditors who want to learn basic risk analysis techniques so they perform technical audits on their systems.
- GIAC Certified Forensic Analyst (GCFA) - Security experts can become GCFA certified to demonstrate their skill in forensic investigation, analysis or formal incident investigation.
- GIAC IT Security Audit Essentials (GSAE) - This certification is geared for entry-level individuals who audit organizational policy, risk and procedures for compliance with established best practices.
- GIAC Certified ISO-17799 Specialist (G7799) - Take this course if you are a security officer or manager who wants to know how to implement the ISO-17799 standard.

The following five certifications are in the GIAC Security Engineer (GSE) Track. Any candidate who completes the practical assignment and passes one of the exams will be certified in that area. The candidate can sit for the GSE exam if all five of these exams are passed and honors (90%+ or better) are received on at least one. An oral presentation, written exam, multiple-choice test, hands-on practical exercise, and supervised on-site security evaluation are required to become GSE certified. Achieving GSE status is a difficult task. SANS considers the GSE exam 'absolutely the toughest exam in the Information Security arena.' As of December 2003, the GIAC site showed only two people with current GSE certifications.

- GIAC Certified Firewall Analyst (GCFW) - An intermediate certification that validates an individual's ability to design, configure and monitor routers, firewalls and perimeter defense systems.
- GIAC Certified Intrusion Analyst (GCIA) - This intermediate certification examines a networking professional's skill with configuring and monitoring intrusion detection systems as well as analyzing and interpreting network traffic.
- GIAC Certified Incident Handler (GCIH) - Individuals responsible for responding to security incidents can use the GHIC as a validation of their ability to manage security incidents, to understand common attack techniques, and to create countermeasures to defend against such attacks.
- GIAC Certified Windows Security Administrator (GCWN) - Systems administrators can use the GCWN as a confirmation that they are skilled in auditing Windows systems and identifying/securing unneeded systems services.
- GIAC Certified UNIX Security Administrator (GCUX) - Administrators who install, configure and monitor Linux and Unix systems can prove their ability to secure and audit those systems by earning the GCUX certification.

MICROSOFT

Microsoft does not offer an individual security certification. Instead, they offer a 'specialization' as part of the Microsoft Certified Systems Engineer (MCSE) and Microsoft Certified Systems Administrator (MCSA) tracks. These specializations are available for both Windows 2000 and Windows 2003.

Aspiring Windows 2000 MCSAs must pass a matrix of tests which includes two security specialization exams. The first security exam covers implementing and administering security. The second exam is on Internet Security and Acceleration (ISA) server. CompTIA's Security+ certification can substitute for the ISA exam. One additional security design exam is required as part of the MCSE track.

The Windows 2003 MCSA and MCSE tracks are similar to the 2000 MCSA and MCSE tracks. The MCSA on Windows 2003 track also requires the candidate to pass two security exams to receive the security specialization designation. The requirements are the same, except that the implementing and administering security exam is for Windows 2003 server. The MCSE on 2003 security specialization also requires an exam on designing security on a Windows 2003 network.

CISCO

Cisco has multiple certification tracks including two specifically on network security. These tracks are targeted at network professionals who design, build and implement networks. The two tracks are the Cisco Certified Security Professional (CCSP) and the Cisco Certified Internetwork Expert (CCIE).

The CCSP is a premium certification that validates a networking professional's network design and implementations skills. CCSPs are tasked with integrating security devices like firewalls, intrusion detection systems and VPNs. Candidates must pass five exams before they are CCSP certified. A Cisco

Certified Network Associate (CCNA) or Cisco Certified Internetwork Professional (CCIP) certification is also a prerequisite. Once certified, the CCSP will last for three years. After three years, a recertification exam is required to maintain certified status.

CCIE Security is an expert-level certification focusing on security-related technologies as well as IP routing and switching. A written exam and lab exam are required to secure the certification. The two-hour long multiple-choice written exam covers networking concepts and equipment commands. The exam addresses topics such as security protocols, operating systems and general networking. An eight-hour long hands-on lab exam must be scheduled within 18 months of passing the written exam. Candidates taking the lab exam are required to build secure networks according to a set of specifications. An 80% score is required to pass the lab exam.

CHECK POINT

The Check Point Certified Professional Program includes six certifications designed for networking professionals who want to secure their networks with Check Point products. The certifications are grouped into two general groups—security and management.

Security Certifications

Check Point Certified Security Principles Associate (CCSPA) - The entry-level CCSPA certification covers security fundamentals, recognizing security threats and best practices.

Check Point Certified Security Administrator (CCSA) - The CCSA focus is on implementing the FireWall-1 product to provide secure network access, to monitor network security activity, and to block intruders.

Check Point Certified Security Expert (CCSE) - The CCSE builds on the skills developed for the CCSA. A CCSE is able to configure the VPN-1 and FireWall-1 products to provide a secure, encrypted connection to the network.

Check Point Certified Security Expert Plus (CCSE Plus) - Product experts with this certification have developed the same skills as a CCSA and CCSE. The CCSE Plus validates their ability to plan and implement complex Check Point solutions.

Management Certifications

Check Point Certified Managed Security Expert (CCMSE) - The CCMSE is designed for product experts who implement the VPN-1, FireWall-1, and Provider-1 products. The CCSA and CCSE are prerequisites for this certification.

Check Point Certified Managed Security Expert Plus VSX (CCMSE Plus VSX) - Network security professionals with this certification are skilled in implementing Check Point's VSX as an enterprise security solution and managing VSX with Provider-1. The CCSA, CCSE, and CCMSE are prerequisites for this certification.

PLANET3 WIRELESS

Planet3 created the four-tiered Certified Wireless Network Professional certification program as a building-block method to learning wireless networking. The four tiers of the program span beginner to expert. The certifications are:

Certified Wireless Network Administrator (CWNA) - Training for this entry-level certification provides the basics of wireless LANs. Some of the topics include radio frequency (RF), wireless LANs, site surveys, wireless security, and industry standards.

Certified Wireless Security Professional (CWSP) - A CWSP is skilled in securing wireless LANs from common attacks. The focus of the CWSP is to learn how to identify security threats and intruders. Design techniques to reduce wireless risk are discussed with an emphasis on hardware, software and protocols solutions.

Certified Wireless Network Integrator (CWNI) - The CWNI is focused on the secure and seamless installation of multiple wireless networks into existing network infrastructures. Particularly emphasis is placed on site surveys, wireless integration, network design analysis, and design considerations.

Certified Wireless Networking Expert (CWNE) – The CWNE is the top tier of Planet3's certification program. The exam validates a networking specialist's skills with packet and protocol analysis, intrusion detection, and network performance analysis. Receiving the CWNE certification also proves the individual is an expert at wireless administration, installation, troubleshooting, and design.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA)

The ISACA formed in 1967 due to systems auditors' desire for guidance in the growing auditing and controls field. In 1978 The Certified Information Systems Auditor (CISA) certification was created as a way to validate an individual's skills in auditing, control and security. ISACA states that the CISA covers the following areas:

- IS management, planning and organization
- Technical infrastructure and operational practices
- Protection of information assets
- Disaster recovery and business continuity
- Business application system development, acquisition, implementation and maintenance
- Business process evaluation and risk management
- The IS audit process

Certified Information Security Manager (CISM) - The CISM is developed for experienced IT managers who are responsible for managing corporate information security. The CISM specifically addresses information risk management, security design and technical security. IT professionals who are responsible for making an overall assessment of corporate security should consider getting the CISM.

SUN

Sun has targeted the Sun Certified Security Administrator for the Solaris Operating System certification at professionals with six to twelve months' experience administering Solaris OS security. Sun has provided a practice exam for this certification on their Web site. A score of only 60% is required to pass.

The exam covers a number of topics including:

- General security concepts such as security policies and procedures, network security and application security
- Intrusion detection through auditing
- Identifying types of security attacks and preventing attacks
- Protecting file and system resources by managing accounts, permissions and policies
- Securing hosts and the network security by using firewalls, implementing IPsec, restricting services, and detecting network intruders
- Managing network access, authentication and encryption

CONCLUSION

As you have seen, information security spans many different roles and responsibilities. Growth in the available number of security certifications now provides enough variety for IT professionals to choose a certification that best meets their career goals.

Qualified security professionals are always in demand. Pick a field that interests you and learn as much as you can. Then, get a certification to validate your skills. The combination of experience, skills and a security certification should help you command a good salary. According to PayScale.com, the median salary for information security professionals is $70,000. As the wise man Jack Handy once said, “I’d rather be rich than stupid.” A security certification probably won’t get you rich, but with the security skills you develop, at least you won’t get caught with your pants down.

Go to www.naspa.com, click on *Technical Support* and go to the general information section to see a table of the certifications described in this article. The specific number of tests and a description and costs of the tests are provided. Link to the URL under ‘Additional Information’ to get the most up-to-date information on the certification you are interested in.

NaSPA member Shawn Conaway is a Systems Administrator for a Fortune 100 retailer. He currently holds the Microsoft Certified Systems Engineer, Citrix Certified Administrator, and A+ certifications. Send questions or comments to s.conaway@naspa.com.