

## **GIAC Security Essentials...much more than the essentials**

Vendors have been offering information technology certifications in the areas of system and network administration for the last decade and a half or so. As a result, information technology certification became a booming field and anybody who wanted to further their information technology career took the opportunity to certify. Over the years it seemed that vendors such as Microsoft and Cisco were releasing new certifications on a weekly basis, but there was a core area that wasn't being focused on; namely information security.

This was partly due to the lack of attention that information security as a whole played in the corporate environment. It wasn't until the Internet grew to massive proportions, that organizations began to take information security seriously. As organizations began to buy and use security products, vendors such as Check Point and Cisco launched their own set of certifications in order to capitalize on the fast-growing certification market. Although information security certifications were now available, it wasn't until GIAC was created that we finally had the opportunity to obtain an information security certification that was vendor neutral. Global Information Assurance Certification, GIAC for short, came about and introduced different levels of certification that were developed by some of the best information security professionals in the world.

### **GSEC as a starting point...**

I personally obtained my GSEC certification in 2000. I was an information security consultant for a reseller of vendor security products and at the time I only considered obtaining certification in the security products that were being sold by the organization. I first saw this as a way to grow within the organization, but more importantly a way to become a security expert. As time went on I began to realize that learning a set of security products did not make me a security expert by any means. Upon this realization I became very uncomfortable with my current career path. It seemed like I was headed into a position that was more geared towards application specialization, rather than a security professional who truly knew how to effectively protect an organization's assets.

I voiced my concerns to a mentor of mine who, unbeknownst to me, had already obtained GIAC certification. He pointed me towards GIAC and provided a run-down as to what they were all about. I was pleasantly surprised at their approach to security certification and began asking other consultants their opinion in order to grasp the sort of reputation GIAC had earned. To my surprise every individual I spoke with who had certified with GIAC only had great things to say. I decided to sign up and soon after obtained GSEC, my first vendor neutral IT security certification.

GIAC introduced the GIAC Certified Security Essentials (GSEC) certification, which was a certification that covered the bare essential knowledge that an information security professional should hold in order to be able to protect their corporate systems. GSEC ensures that students become familiar with the following areas:

- Risk Assessment & Auditing
- Host & Network Based Intrusion Detection
- Honeypots, Firewalls & Perimeter Protection
- Security Policy
- Password Management
- Incident Handling
- Information Warfare
- Web Security
- Network Fundamentals & IP Concepts/Behavior
- Cisco Router Filters
- Four Primary Threats for Perimeter Protection
- Defense in Depth

- PGP & Steganography
- Anti-Viral Tools
- Windows (2000, XP, NT, 98) Security Administration & Auditing
- IIS Security
- UNIX Security Fundamentals

While other security certifications such as CompTIA's Security+ offer an entry/intermediate level of IT security certification, nobody has come close to covering GSEC's wide range of topics in the detail that is essential to understanding security, not only as a technical issue, but as a managerial issue. Since obtaining my GSEC certification I have acquired multiple GIAC certifications in the areas of intrusion detection, hacker exploits, etc, but GSEC was the starting point that assisted me in furthering my career in information security.

Almost a decade after GIAC was launched it's difficult to find an information security job posting without GIAC certification being required, or at least recommended. Organizations have begun to take notice of GIAC as the definitive security certification for information security professionals.

Before deciding on the next security certification you intend to acquire it is best to conduct an appropriate amount of research to ensure that you certify with an organization whose main purpose is to make the Internet a safer place for all of us.

**About the author**

Peter Giannoulis, [GSEC](#), [GCIH](#), [GCIA](#), [GCFA](#), [CISSP](#), is an information security consultant for Access 2 Networks, a Toronto, Ontario based security consulting firm. He also serves as a technical director for [GIAC](#).