Security Certification: GSEC

GIAC Security Essentials (GSEC)

View Professionals →

Target

Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks. Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts.

No Specific training is required for any GIAC certification. There are many sources of information available regarding the certification objectives' knowledge areas. Practical experience is an option; there are also numerous books on the market covering Computer Information Security. Another option is any relevant courses from training providers, including SANS.

Requirements

- 1 proctored exam
- 180 questions
- Time limit of 5 hours
- Minimum Passing Score of 74%

Note: GIAC reserves the right to change the specifications for each certification without notice. Based on a scientific passing point study, the passing point for the GSEC exam has been determined to be 74% for all candidates receiving access to their certification attempts on or after August 28th, 2015. To verify the format of your current certification attempt, please read the Certification Information found in your portal account at https://exams.giac.org/pages/attempt.

Renew

Certifications must be renewed every 4 years. Click here for details.

Delivery

NOTE: All GIAC exams are delivered through proctored test centers and must be scheduled in advance.
GIAC certification attempts will be activated in your GIAC account after your application has been approved and according to the terms of your purchase. Details on delivery will be provided along with your registration confirmation upon payment. You will receive an email notification when your certification attempt has been activated in your account. You will have 120 days from the date of activation to complete your certification attempt. GIAC exams must be proctored through Pearson VUE. Please click the following link for instructions on How to Schedule Your GIAC Proctored Exam http://www.giac.org/information/schedule_proctored_exam.pdf. GIAC exams are delivered online through a standard web browser.

Links

- Certified Professionals (GSEC)
- Recertification
- Exam Feedback Procedure
- Feedback Procedure
- Proctored exam procedure
- SANS Information Security Reading Room

Bulletin (Part 2 of Candidate Handbook)

Exam Certification Objectives & Outcome Statements

The topic areas for each exam part follow:

802.11 attacks & countermeasures
The candidate will demonstrate an understanding of the different 802.11 protocols, as well as an understanding of common wireless attacks and how to prevent them.

Access Control Theory
The candidate will demonstrate an understanding of the fundamental theory of access control.

Alternate Network Mapping Techniques
The candidate will demonstrate a fundamental understanding of network mapping techniques an attacker might use to examine wireless networks, and public switched telephony networks. The candidate will also demonstrate an understanding of how to identify the basic penetration techniques at a high level.

Authentication and Password Management
The candidate will demonstrate understanding of the role of authentication controls, how they are managed, and the methods used to control access to systems.

Common Types of Attacks
The candidate will demonstrate the ability to identify the most common attack methods, as well as the basic strategies used to mitigate those threats.

Contingency Planning
The candidate will demonstrate an understanding of the critical aspect of contingency planning with a Business Continuity Plan (BCP) and Disaster Recover Plan (DRP).

Critical Security Controls
The candidate will be familiar with the background, history and purpose of the Critical Security Controls.

Crypto Concepts
The candidate will demonstrate a high-level understanding of the mathematical concepts which contribute to modern cryptography.

Crypto Fundamentals
The candidate will demonstrate an understanding of the core concepts of cryptography and the three main algorithms.

Defense-in-Depth
The candidate will demonstrate an introductory understanding of the terminology and concepts of *Risk* and Defense-in-Depth, including threats and vulnerabilities.

DNS
The candidate will demonstrate a high-level understanding of the Domain Name System architecture.

Firewalls
The candidate will demonstrate a fundamental understanding of firewalling technologies and techniques.

Honeypots
The candidate will demonstrate understanding of basic honeypot techniques and common tools used to set up honeypots.

ICMP
The candidate will demonstrate an understanding of the structure and purpose of ICMP, as well as the fields in a ICMP datagram header.

Incident Handling Fundamentals
The candidate will demonstrate an understanding of the concepts of incident handling and the six-step incident handling process.

Information Warfare
The candidate will demonstrate an understanding of information warfare methods and defense.

Intrusion Detection Overview
The candidate will demonstrate an understanding of the overall concepts of Intrusion Detection.

IP Packets
The candidate will demonstrate a fundamental understanding of how the IP protocol works.

IPS Overview
The candidate will demonstrate a high-level understanding of how IPS systems operate.

IPv6
The candidate will demonstrate a high-level understanding of the IPv6 protocol.

Legal Aspects of Incident Handling
The candidate will demonstrate an understanding of the basic legal issues in incident and evidence handling.

Linux/Unix Configuration Fundamentals
The candidate will demonstrate an understanding of Linux/Unix fundamental configuration settings, including file permissions, user accounts, groups, and passwords, and commands used to display information and run backups.

Linux/Unix Logging and Log Management
The candidate will demonstrate an understanding of the various logging capabilities and log file locations common to Linux operating systems.

Linux/Unix OS Security Tools and Utilities
The candidate will demonstrate an understanding of how to use key security utilities and tools that are available for Linux/Unix systems, including file integrity, host firewalls, and applications such as SELinux.

Linux/Unix Overview
The candidate will demonstrate familiarity with the different variants of Linux/Unix, the Linux file system, and important commands.

Linux/Unix Patch Management
The candidate will demonstrate an understanding of the process of patch management, best practices, and common patch management tools and techniques for Linux/Unix systems.

Linux/Unix Process and Service Management
The candidate will demonstrate an understanding of how to manage Linux/Unix processes, run levels, and services, and best practices for common processes and services.

Mitnick-Shimomura
The candidate will demonstrate an understanding of the details of the famous Mitnick-Shimomura attack, as well as what we can learn from this attack to appropriately protect our networks today against these vulnerabilities. The candidate will also demonstrate an understanding of the strategies that would have prevented the Mitnick attack.

Network Addressing
The candidate will demonstrate an understanding of the essentials of IP addressing, subnets, CIDR and netmasks.

Network Fundamentals
The candidate will demonstrate an understanding of basic network hardware, topologies, architectures.

Network Mapping and Scanning
The candidate will demonstrate a fundamental understanding of the common tools attackers use to scan systems and the techniques used to create a network map.

Network Protocol
The candidate will demonstrate an understanding of the properties and functions of network protocols and network protocol stacks.

Policy Framework
The candidate will demonstrate an understanding of the purpose and components of policy.

Protecting Data at Rest
The candidate will demonstrate an understanding of the functionality of PGP cryptosystems and how they operate.

Public Key Infrastructure PKI
The candidate will demonstrate an understanding of how PKI works and the key components for managing keys.

Reading Packets
The candidate will demonstrate an understanding of how to decode a packet from hexadecimal output.

Risk Management
The candidate will demonstrate an understanding of the terminology and basic approaches to Risk Management.

Securing Windows Server Services
The candidate will demonstrate an understanding of the basic measures in securing Windows IIS, SQL, and Terminal Servers.

Steganography Overview
The candidate will demonstrate an understanding of the different methods of steganography, as well as some of the common tools used to hide data with steganography.

TCP
The candidate will demonstrate an understanding of the structure and purpose of TCP, as well as the fields in a TCP datagram header.

UDP
The candidate will demonstrate an understanding of the structure and purpose of UDP, as well as the fields in a UDP datagram header.

Virtual Private Networks VPNs
The candidate will demonstrate a high-level understanding of VPNs and be able to identify IPSec and non-IPSec protocols used for VPN communications.

Viruses and Malicious Code
The candidate will demonstrate an understanding of what malicious code is, how it propagates and why it is such an expensive problem. Additionally, the candidate will demonstrate an understanding of the attack vectors leveraged by recent malicious code attacks.

Vulnerability Management Overview
The candidate will demonstrate the ability to perform reconnaissance and resource protection to manage vulnerabilities, and address threats and vectors.

Vulnerability Scanning
The candidate will demonstrate an understanding of how data generated from a port scanner like nmap, and vulnerability assessment tools like nessus can be used to examine systems, ports and applications in more depth to secure an environment.

Web Application Security
The candidate will demonstrate an understanding of web application security and common vulnerabilities including CGI, cookies, SSL and active content.

Windows Auditing
The candidate will demonstrate an understanding of the techniques and technologies used to audit Windows hosts.

Windows Automation and Configuration
The candidate will demonstrate an understanding of the techniques and technologies used to automate configuration.

Windows Network Security Overview
The candidate will demonstrate an understanding of the basic measures in securing a Windows host, including managing services and VPNs.

Windows Permissions & User Rights
The candidate will demonstrate an understanding of how permissions are applied in the Windows NT File System, Shared-Folder, Encrypting File System, Printer, Registry Key, Active Directory, and how User Rights are applied.

Windows Security Templates & Group Policy
The candidate will demonstrate a high-level understanding of the features and functionality of Group Policy and best practices for locking down systems.

Windows Service Packs, Hotfixes and Backups
The candidate will demonstrate an understanding of how to manage Windows Service Packs and Hotfixes, as well as backups and restoration for a network of Windows hosts.

Windows Workgroups, Active Directory and Group Policy Overview
The candidate will demonstrate an understanding of the basic security infrastructure of local accounts, workgroups, Active Directory and Group Policy.

Wireless Overview
The candidate will demonstrate a fundamental understanding of wireless technologies including Bluetooth and Zigbee.

Where to Get Help

Training is available from a variety of resources including on line, course attendance at a live conference, and self study.

Practical experience is another way to ensure that you have mastered the skills necessary for certification. Many professionals have the experience to meet the certification objectives identified.

Finally, college level courses or study through another program may meet the needs for mastery.

The procedure to contest exam results can be found at http://www.giac.org/about/procedures/grievance.

GIAC Certified

Security Administration
GSEC
GCIH
GCIA
GPEN
GWAPT
GPPA
GCWN
GISF
GCED
GAWN
GICSP
GCUX
GXPN
GMOB
GCCC
GMON
GPYC