GIAC GSEC

OUR LEARNING EXCLUSIVE

- Custom exam prep software and materials
- Structured help building your **exam index** — the single biggest factor in passing an open-book GIAC exam
- A **98% success rate** on the exam
- Your exam attempt scheduled and activated for you — GIAC proctors its own exams, so this one is not sat in our classroom
- Course-specific thinQtank® Learning publications to keep the learning engaging
- Extended hours of training, including immersive hands-on exercises
- **We do not teach the test.** We always deliver valuable hands-on experience
- Every course taught by working security practitioners

TRAINING CAMP FORMAT

thinQtank® Learning delivers this course as an **instructor-led training camp**. Camps are scheduled by cohort rather than to a fixed calendar, and the balance of lecture and lab work is set to suit the group and the delivery method. Contact us for the schedule covering your dates.

PREREQUISITES

- A solid working understanding of information security concepts
- Practical familiarity with networking, and with both Linux and Windows
- Our Cybersecurity Foundations material is the recommended preparation if you are coming in without that grounding

TARGET AUDIENCE

- Security analysts, engineers and administrators
- Systems and network administrators taking on security responsibility
- IT staff whose role now requires demonstrable security knowledge
- Anyone in a DoD 8140 work role that accepts GSEC

EXAM

This exam is OPEN BOOK. GIAC allows all printed books, notes and study guides — and no digital material of any kind. Building your own indexed reference is what separates a pass from a fail, and we build it with you in class. GSEC is accredited to **ISO/IEC 17024** by ANAB and aligned to US Department of Defense **directive 8140**.

GSEC — GIAC Security Essentials

106 questions, four hours. Minimum passing score 72% for exam versions released on or after 6 April 2026. Twenty-six objective areas. Proctored and web delivered; 120 days from activation to sit your attempt.

COURSE OVERVIEW

thinQtank® Learning offers an industry-unique training camp in which students earn the **GIAC Security Essentials** certification.

GSEC is the broad defensive certification: networking and protocols, defensible network design, authentication and access control, Linux and Windows security, cryptography, risk and vulnerability management, malware, virtualization and cloud, wireless, VoIP and the physical layer everything else sits on. The emphasis throughout is on what actually stops an attack and what actually detects one.

It is a harder exam than its name suggests — 106 questions over four hours, at a 72% cut, across twenty-six objective areas. It is also **open book**, which changes how you prepare for it entirely. The **exam attempt is available** at $949 USD.

COURSE OBJECTIVES

Primary course objectives:

- Work confidently with networking fundamentals, protocols and real traffic
- Design a defensible network: segmentation, architecture, defense in depth
- Implement authentication, access control and password management
- Deploy network security devices, and know what each one can and cannot see
- Secure and harden Linux, using the command line as a security tool
- Secure and harden Windows: access controls, policy, services and the cloud
- Apply cryptography correctly, and know where it belongs in practice
- Run risk management in an operational setting, not a spreadsheet
- Secure virtualization and cloud workloads
- Run vulnerability scans, and know what a penetration test does not tell you
- Recognize malicious code and apply exploit mitigation on the endpoint
- Handle incidents, and use log management and SIEM to detect them
- Apply data loss prevention and mobile device security
- Secure wireless, VoIP and the physical layer
- Apply security frameworks and the CIS Controls

DELIVERY METHODS

- Instructor-led training
- Immersive live-online training
- On-site and custom delivery

WHAT YOU WILL BE ABLE TO DO

- Read a network the way a defender has to, not the way a diagram shows it
- Harden Linux and Windows to a standard you can evidence
- Detect an incident from logs rather than from a phone call
- Walk into an open-book exam with an index you built and can actually use

EXCLUSIVE LEARNING PACKAGE

- Guided exam index build — yours, not somebody else's
- Hands-on Linux and Windows hardening lab
- Packet capture and log analysis exercise set
- GSEC video course
- GSEC reading plan and review guide
- GSEC certification practice exam

COURSE MODULES

01 Information Security and the GSEC Certification
- Topic A: What the certification covers, and how it is examined
- Topic B: Security concepts and the history that shaped them

02 Networking Fundamentals
- Topic A: Protocols, addressing and the traffic a defender reads
- Topic B: Network services and where they are exposed

03 Network Design
- Topic A: Defensible architecture and segmentation
- Topic B: Defense in depth, applied rather than recited

04 Authentication and Access Control
- Topic A: Identification, authentication and authorization
- Topic B: Password management and its failure modes

05 Network Security
- Topic A: Firewalls, IDS/IPS and network security devices
- Topic B: Monitoring, log management and SIEM
- Topic C: Web communication security

06 Linux
- Topic A: Linux fundamentals for security work
- Topic B: Hardening, permissions and audit

07 Windows
- Topic A: Windows access controls and security policy
- Topic B: Windows services, automation and auditing
- Topic C: Windows security infrastructure and the Microsoft cloud

08 Encryption
- Topic A: Cryptography fundamentals
- Topic B: Applied cryptography and key handling

09 Risk Management
- Topic A: Identifying and assessing operational risk
- Topic B: Security frameworks and the CIS Controls

10 Virtual Machines
- Topic A: Virtualization security
- Topic B: Cloud and container security essentials

11 Vulnerability Control
- Topic A: Vulnerability scanning and interpreting the output
- Topic B: What a penetration test does and does not tell you

12 Malware
- Topic A: Malicious code and how it establishes itself
- Topic B: Exploit mitigation and endpoint security

13 Physical Security
- Topic A: Physical controls and the assumptions they protect
- Topic B: Data loss prevention and mobile device security

14 Wireless Technologies
- Topic A: Wireless protocols and their weaknesses
- Topic B: Securing a wireless network

15 VoIP
- Topic A: VoIP architecture and its attack surface
- Topic B: Securing voice on a data network