FORTRA

GUIDE (Penetration Testing Services)

Certifications to Look for When Choosing a Pen Testing Team

You may know that building a penetration testing team or hiring pen testing services can help uncover security gaps putting your organization at risk, but getting started is sometimes difficult. What makes a good security tester? Is there a way to differentiate true security pros from the inexperienced and unprofessional? Actually, there is. Pen testers may have a variety of education and employment backgrounds, but one of the best measures of skill and dedication is industry certifications.

What Makes Pen Testing Certifications Important?

Pen testing certifications help verify that pen testers have spent time adequately training and possess the necessary skills required in order to successfully conduct a pen test. Reputable certifications are issued by institutions and organizations that are considered authorities in the field. There are a number of possible certifications that a pen tester can train and test for, with some covering broad pen testing concepts and others narrow in on specific topics for testers who want to further their expertise and specialize in a niche area. The following list has details on some of the most common certifications, including how long they are valid and what they focus on.

CEH

Certified Ethical Hacker

Granted by: International Council of E-Commerce Consultants (EC-Council), which was formed after 9/11 to prevent a similar attack on cyber infrastructure; recognized by the US National Security Agency (NSA) and the Committee on National Security Systems (CNSS) for meeting American National Standards Institute (ANSI) requirementse with Cisco solutions
Requirements: Two years IT security experience and completion of related course
Format: Four-hour exam with 125 questions and variable requirements for passing
Valid: Three years
Focuses on:

- Cloud computing
- Cryptography
- Denial of service
- Enumeration
- Evading IDS, firewalls, and honeypots
- Footprinting and reconnaissance
- Hacking IoT, mobile platforms, operational technology (OT), web applications and servers, and wireless networks
- Malware threats
- Scanning networks
- Session hijacking
- Sniffing
- Social engineering
- SQL injection
- System hacking
- Vulnerability analysis

CCNA

Cisco Certified Network Associate

Granted by: The Cisco Learning Network, the training and certifications arm of Cisco Systems, an international seller of switches, routers, networking, and cybersecurity products
Requirements: Recommended at least one year experience with Cisco solutions
Format: Two-hour exam with a varying number of questions and variable requirements for passing
Valid: Three years; can recertify with 30 continuing education credits
Focuses on:

- Automation and programmability 10%
- IP connectivity 25%
- IP services 10%
- Network access 20%
- Network fundamentals 20%
- Security fundamentals 15%

CEPT

Certified Expert Penetration Tester

Granted by: Infosec Institute, a non-profit that's accredited by the professional organization Information Systems Audit and Control Association (ISACA) and one of its two Elite+ Partners in the world
Requirements: Experience in ethical hacking
Format: Two-hour test with 50 questions and three hands-on pen testing challenges that requires 70% correct answers to pass
Valid: Four years
Focuses on:

- Exploit creation - Linux/Unix
- Exploit creation - Windows
- Linux and Unix shellcode
- Memory corruption/buffer overflow vulnerabilities
- Network attacks
- Network recon
- Pen testing methodologies
- Reverse engineering
- Windows shellcode

CMWAPT

Certified Mobile and Web Application Penetration Tester

Granted by: Infosec Institute, a non-profit that's accredited by the professional organization Information Systems Audit and Control Association (ISACA) and one of its two Elite+ Partners in the world
Requirements: Understanding of Windows and Linux/Unix OSs, information security, networking, and pen testing
Format: Two-hour test with 50 questions that requires 70% correct answers to pass
Valid: Four years
Focuses on:

- Android app attacks and components
- iOS app attacks and components
- Mobile and web app pen testing
- Secure coding principles
- Web app attacks and vulnerabilities

CISSP

Certified Information Systems Security Professional

Granted by: International Information System Security Certification Consortium (ISC2), a non-profit organization formed in 1989 to create internationally recognized information security certifications.
Requirements: Five years paid work experience in two or more of the eight exam focus areas. Education may count for one year of experience.
Format: Four-hour exam that requires 70% correct answers to pass
Valid: Three years; one continuing professional education (CPE) credit required in the interim
Focuses on:

- Security and risk management 15%
- Communications and network Security 13%
- Identity and access management 13%
- Security architecture and engineering 13%
- Security operations 13%
- Security assessment and testing 12%
- Software development security 11%
- Asset security 10%

CRTOP

Certified Red Team Operations Professional

Granted by: Infosec Institute, a non-profit that's accredited by the professional organization Information Systems Audit and Control Association (ISACA) and one of its two Elite+ Partners in the world
Requirements: Understanding of Windows and Linux/Unix OSs, information security, networking, and pen testing
Format: Two-hour test with 5 questions that requires 70% correct answers to pass
Valid: Four years
Focuses on:

- Assessment methodology and reporting
- Digital reconnaissance
- Physical reconnaissance
- Roles and responsibilities of red teams
- Social engineering
- Vulnerability identification and mapping

CRT

Council for Registered Ethical Security Testers (CREST) Registered Tester

Granted by: CREST, an international non-profit established in 2006 in the United Kingdom to help regulate cyber security professionals
Requirements: Three years relevant experience
Format: Two-and-a-half-hour test with 150 questions and a practical component that requires 60% correct answers to pass
Valid: Three years
Focuses on:

- Application fingerprinting and evaluating unknown services
- Cross-site scripting attacks
- Domain name server queries and responses, zone transfers, and analysis of records
- File system permissions
- Interpreting tool output
- Management protocols
- Microsoft Active Directory, domain reconnaissance, SQL server, and user enumeration
- Network mapping and target identification
- Networking protocols
- Oracle RDBMS
- OS fingerprinting
- Parameter manipulation
- RPC services
- SQL injection
- SSH
- Unix FTP, NFS, R* services, SMTP, user enumeration, vulnerabilities,
- Web/app/database connectivity
- Web application servers
- Web protocols
- Web server operation and flaws
- Website structure discovery
- Windows common applications and vulnerabilities
- X11

CySA+

CompTIA Cybersecurity Analyst

Granted by: The Computing Technology Industry Association (CompTIA), which offers training, certification, and market research to promote the industry
Requirements: Recommended knowledge of Network+, Security+, or equivalent and minimum of four years hands-on experience
Format: Two-hour exam with up to 85 questions that requires a score of 750 on a scale of 100-900 to pass
Valid: Three years; automatically renews with 60 CompTIA continuing education units (CEUs)
Focuses on:

- Compliance and assessment
- Incident response
- Security operations and monitoring
- Software and systems security
- Threat vulnerability management

eJPT

eLearnSecurity Junior Penetration Tester

Granted by: eLearn Security
Requirements: Recommended experience with information gathering, Metasploit, network vulnerability assessment, networking, pen testing, traffic protocol analysis, and web application security and exploitation
Format: Three-day exam with 20 questions in a hands-on lab environment
Valid: No expiration
Focuses on:

- Information gathering
- Networking basics and attacks
- Programming basics
- Scanning and footprinting
- System attacks
- Web vector attacks

GAWN

Global Information Assurance Certification (GIAC) Assessing and Auditing Wireless Networks

Granted by: Global Information Assurance Certification (GIAC), a for-profit professional certifications company formed by The Escal Institute of Advanced Technologies (SANS) in 1999 to quantify infosec security credentials
Requirements: None, though practical work experience or training is recommended
Format: Two-hour test with 75 questions that requires 70% correct answers to pass
Valid: Four years; renew with 36 CPEs or retake the exam
Focuses on:

- 802.11 fuzzing attacks
- Attacking weak encryption
- Bluetooth and Bluetooth low energy attacks
- Bridging the air gap
- Digital Enhanced Cordless Telecommunications (DECTTM)
- DoS on Wireless Networks
- Hotspots
- Near Field Communications (NFC) and how it uses consistent data protocols to exchange data bidirectionally for uses in payment systems, and generic data transfers.
- Practical SDR Attacks
- RFID attacks
- Rogue Networks
- Wireless basics, client attacks, and sniffing
- WPA2
- Zigbee

GCCC

Global Information Assurance Certification (GIAC) Critical Controls Certification

Granted by: Global Information Assurance Certification (GIAC), a for-profit professional certifications company formed by The Escal Institute of Advanced Technologies (SANS) in 1999 to quantify infosec security credentials
Requirements: None, though practical work experience or training is recommended
Format: Two-hour test with 75 questions that requires 71% correct answers to pass
Valid: Four years; renew with 36 CPEs or retake the exam
Focuses on:

- V8 -
  - Access control, account, audit log, incident response, network infrastructure, and service provider management
  - Application software security
  - Background on CIS controls, standards, and governance
  - Continuous vulnerability management
  - Data protection and recovery
  - Email and web browser protections
  - Inventory, control, and secure configuration of enterprise assets and software
  - Malware defenses
  - Network monitoring and defense
  - Pen testing
  - Security awareness and skills training

GCIH

Global Information Assurance Certification (GIAC) Certified Incident Handler

Granted by: Global Information Assurance Certification (GIAC), a for-profit professional certifications company formed by The Escal Institute of Advanced Technologies (SANS) in 1999 to quantify infosec security credentials
Requirements: None, though practical work experience or training is recommended
Format: Four-hour test with 106 questions that requires 70% correct answers to pass
Valid: Four years; renew with 36 CPEs or retake the exam
Focuses on:

- Cyber, incident-response, memory and malware, and network investigation
- Detecting cover communications, evasive techniques, and exploitation tools
- Drive-by, networked-environment, password, post-exploitation, and web app attacks
- Endpoint attack and pivoting
- Reconnaissance and open-source intelligence
- Scanning and mapping
- SMB scanning

GMOB

Global Information Assurance Certification (GIAC) Mobile Device Security Analyst

Granted by: Global Information Assurance Certification (GIAC), a for-profit professional certifications company formed by The Escal Institute of Advanced Technologies (SANS) in 1999 to quantify infosec security credentials
Requirements: None, though practical work experience or training is recommended
Format: Two-hour test with 75 questions that requires 71% correct answers to pass
Valid: Four years; renew with 36 CPEs or retake the exam
Focuses on:

- Analyzing applications and network activity
- Application analysis, manipulation, and security assessment
- Intercepting encrypted network traffic
- Jailbreaking, rooting, and managing Android and iOS devices and applications
- Mitigating against mobile malware and stolen devices
- Pen testing mobile devices

GPEN

Global Information Assurance Certification (GIAC) Penetration Tester

Granted by: Global Information Assurance Certification (GIAC), a for-profit professional certifications company formed by The Escal Institute of Advanced Technologies (SANS) in 1999 to quantify infosec security credentials
Requirements: None, though practical work experience or training is recommended
Format: Three-hour test with 60 questions that requires 67% correct answers to pass
Valid: Four years; renew with 36 CPEs or retake the exam
Focuses on:

- Attacking password hashes
- Azure applications, AD integration, and attack strategies
- Basic and advanced password attacks
- Domain escalation and persistence attacks
- Escalation and exploitation fundamentals
- Kerberos Attacks
- Metasploit
- Moving files with exploits
- Password formats and hashes
- Pen test planning
- Pen testing with PowerShell and the Windows command line
- Reconnaissance
- Scanning and host discovery
- Vulnerability scanning

GWAPT

Global Information Assurance Certification (GIAC) Web Application Penetration Tester

Granted by: Global Information Assurance Certification (GIAC), a for-profit professional certifications company formed by The Escal Institute of Advanced Technologies (SANS) in 1999 to quantify infosec security credentials
Requirements: None, though practical work experience or training is recommended
Format: Two-to-three-hour test with 82 to 115 questions that requires 71% correct answers to pass
Valid: Four years; renew with 36 CPEs or retake the exam
Focuses on:

- Cross-site request forgery, cross-site scripting, and client-side injection attack
- Reconnaissance and mapping
- Web application -
- Authentication attacks
- Configuration testing
- Overview
- Session Management
- SQL injection Attacks
- Testing Tools

GXPN

Global Information Assurance Certification (GIAC) Exploit Researcher and Advanced Penetration Tester

Granted by: Global Information Assurance Certification (GIAC), a for-profit professional certifications company formed by The Escal Institute of Advanced Technologies (SANS) in 1999 to quantify infosec security credentials
Requirements: None, though practical work experience or training is recommended
Format: Three-hour test with 60 questions that requires 67% correct answers to pass
Valid: Four years; renew with 36 CPEs or retake the exam
Focuses on:

- Accessing, exploiting, manipulating networks
- Introductory, practical, and advanced fuzzing
- Advanced stack smashing
- Client exploitation and escape
- Crypto for pen testers
- Introduction to memory and dynamic Linux memory
- Introduction to Windows exploitation
- Python and Scapy for pen testers
- Shellcode
- Smashing the stack
- Windows overflows

PCI ASV

Payment Card Industry (PCI) Approved Scanning Vendor

Granted by: OPCI Security Standards Council (PCI SSC), a global organization dedicated to account data security for the credit and debit card industry
Requirements: Documented business independence, insurance, and legitimacy as well as scanning experience and staff to support vulnerability scanning
Format: Remotely scan test infrastructure and report findings
Valid: One year
Focuses on:

- Scan administration
- Scan performance
- Scan report

Network+

CompTIA Network+

Granted by: The Computing Technology Industry Association (CompTIA), which offers training, certification, and market research to promote the industry
Requirements: Recommended CompTIA A+ and one year of networking experience
Format: 90-minute exam with a maximum of 90 questions and a hand-on portion that requires a score of 720 on a scale of 100-900 to pass
Valid: Three years; automatically renews with 30 CompTIA CEUs or CertMaster course
Focuses on:

- Network implementations
- Network operations
- Network security
- Network troubleshooting
- Networking fundamentals

Security+

CompTIA Security+

Granted by: The Computing Technology Industry Association (CompTIA), which offers training, certification, and market research to promote the industry
Requirements: Recommended CompTIA Network+ and two years experience in IT administration with a focus on security
Format: 90-minute exam with a maximum of 90 questions and a hands-on portion that requires a score of 750 on a scale of 100-900 to pass
Valid: Three years; automatically renews with 50 CompTIA CEUs or CertMaster course
Focuses on:

- Architecture and design
- Attacks, threats, and vulnerabilities
- Governance, risk, and compliance
- Implementation
- Operations and incident response

OSCP

Offensive Security Certified Professional

Granted by: Offensive Security, which aims to give students the tools, techniques, and critical thinking skills used by hackers in order to thwart intruders
Requirements: TCP/IP networking fundamentals, Windows and Linux administration and Active Directory experience as well as familiarity with Bash and Python programming languages. Completion of PEN-200 OSCP training course, included in exam fee.
Format: 24-hour exam with three targets and one Active Directory set. Proof files and a report documenting the exploitation process is required for each machine.
Valid: No expiration
Focuses on:

- Active and passive information gathering
- Active directory attacks
- Antivirus evasion
- Bash scripting
- Client-side attacks
- Command lines
- File transfers
- Fixing exploits
- Kali Linux
- Linux and Windows buffer overflows
- Locating public exploits
- Metasploit
- Password attacks
- Pen testing
- PowerShell Empire
- Port redirection and tunneling
- Privilege escalation
- Vulnerability scanning
- Web application attacks

OSWP

Offensive Security Wireless Professional

Granted by: Offensive Security, which aims to give students the tools, techniques, and critical thinking skills used by hackers in order to thwart intruders
Requirements: Understanding of TCP/IP, OSI, and Linux as well as completion of PEN-210 OSWP training course, included in exam fee
Format: Three-hour and 45-minute exam with three live, wireless network simulations where a proof.txt file must be obtained and the process documented. Requires success on two of the three scenarios to pass.
Valid: No expiration
Focuses on:

- Aircrack-ng essentials
- Attacking captive portals
- Attacking WPA Enterprise
- Attacking WPS Networks
- bettercap essentials
- Cracking authentication hashes
- Determining chipsets and drivers
- Frames and network interaction
- IEEE 802.11
- Kismet essentials
- Linux wireless tools, drivers, and stacks
- Manual network connections
- Rogue access points
- Wi-Fi encryption
- Wireless networks
- Wireshark essentials

Using Certifications to Inform Your Third-Party Team Selection

When shopping for a third-party cybersecurity vendor, due diligence is important. After all, you're trusting them with the security of your highly valued assets. But cybersecurity talent is scarce, so not all pen testing teams are on equal footing. Many focus on basic, routine tests that are performed with a vulnerability scanner and an automated pen testing tool, packaging it as a custom service. However, such tools can be used by your own security team, so it's important to find a partner with a team that can advise you on the different options, tailor their tests to suit your needs, and expertly probe your systems and exploit vulnerabilities.

Certifications are a key measure you can look for when evaluating whether a vendor has the experience needed to effectively assess your network. Though a minimum level of certification is important, a team with a variety of certifications among its members could be most capable at tackling an array of testing scenarios. At Fortra, our security testing teams have essential certifications and more so you can feel confident in their ability to uncover vulnerabilities before bad actors do.

Fortra offers a number of penetration testing services to meet the unique security objectives and challenges of any environment. Testing areas include network infrastructure, web applications, mobile applications, wireless networks, IoT, social engineering, and more. Our testing teams offer a fresh perspective on the state of your security and provide new ways to make improvements, including increasing user awareness, finding new vulnerabilities, circumventing access controls, and finding paths to compromise high-value assets that were not explored before. In addition to thorough testing procedures, Fortra provides detailed reports that present a clear path forward, with recommendations on remediation and other best practices.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.