SANS Technology Institute

Graduate Certificate Program
Penetration Testing & Ethical Hacking

The SANS Technology Institute's post-baccalaureate certificate program in **Penetration Testing & Ethical Hacking** is based entirely upon courses already available as an elective path through its graduate program leading to a Master of Science Degree in Information Security Engineering.

As an independent offering, the graduate certificate in **Penetration Testing & Ethical Hacking** is a highly technical, 13 credit hour program with a cohesive and progressive set of learning outcomes. A hands-on focus is emphasized throughout, including the requirement to unlock the upper levels of the NetWars Continuous internet-accessible cyber range as the capstone experience. These learning outcomes focus on the student's capability to discover, analyze, and understand the implications of information security vulnerabilities in systems/networks/applications in order to identify solutions before others exploit these flaws.

Course Number and Name	SANS Class and GIAC Exam	Credit Hours
ISE 5201 Hacking Techniques & Incident Response	SEC 504, GCIH	3
ISE 6315 Web Application Penetration Testing & Ethical Hacking	SEC 542, GWAPT	3
ISE 6320 Network Penetration Testing & Ethical Hacking	SEC 560, GPEN	3
ISE 6300 Core NetWars Continuous Capstone	Core NetWars	1
Students choose one of the following as their fourth course		
ISE 6325 Mobile Device Security	SEC 575, GMOB	3
ISE 6330 Wireless Networks Penetration Testing	SEC 617, GAWN	3
ISE 6350 Python for Penetration Testers	SEC 573, GPYC	3
ISE 6360 Advanced Network Penetration Testing	SEC 660, GXPN	3
	Total	**13**

The graduate certificate in **Penetration Testing & Ethical Hacking** provides a path for professionals to specialize in a sub-area of the information security field, and this progression of courses in penetration testing and ethical hacking is made available just as they would be to a candidate for the master's degree in Information Security Engineering. Armed with a deep understanding of the offensive techniques used by malicious agents seeking to breach information security defenses, the professional who earns the Penetration Testing & Ethical Hacking post-baccalaureate certificate will be empowered to identify and help remediate these vulnerabilities.

Graduates of the **Penetration Testing & Ethical Hacking** post-baccalaureate certificate program will be able to:

1. Conduct vulnerability scanning and exploitation of various systems and applications using a careful, documented methodology to provide explicit proof of the extent and nature of IT infrastructure risks, conducting these activities according to well-defined rules of engagement and a clear scope.

2. Provide documentation of activities performed during testing, including all exploited vulnerabilities and how those vulnerabilities were combined into attacks to demonstrate business or institutional risk.
3. Produce an estimated risk level for a given discovered flaw by using the amount of effort the team needed to expend in penetrating the information system as an indicator of the penetration resistance of the system.
4. Provide actionable results with information about possible remediation measures for the successful attacks performed.

The following assessment methods will be utilized to determine if students meet the program learning outcomes:

1. Standardized exams
    a. Required:
        i. GIAC Certified Incident Handler (GCIH) exam,
        ii. GIAC Web Application Penetration Testing (GWAPT) exam, and
        iii. GIAC Penetration Tester (GPEN) exam;
    b. Elective Choice of:
        i. GIAC Mobile Device Security Analyst (GMOB) exam,
        ii. GIAC Assessing and Auditing Wireless Networks (GAWN) exam,
        iii. GIAC Python Code (GPYC) exam,
        iv. GIAC Exploit Research and Advanced Penetration Tester (GXPN) exam.
2. Simulation Experience – NetWars Continuous

Course Descriptions

Individual course descriptions are provided below. For additional, detailed technical goals for each course, please link through to individual SANS class descriptions on the sans.org website.

Required Courses:

ISE 5201 Hacking Techniques & Incident Response

SANS class: SEC504 Hacker Techniques, Exploits & Incident Handling
Assessment: GIAC GCIH
3 Credit Hours | Tuition: $5,000

By adopting the viewpoint of a hacker, ISE 5201 provides an in-depth focus into the critical activity of incident handling. Students are taught how to manage intrusions by first looking at the techniques used by attackers to exploit a system. Students learn responses to those techniques, which can be adopted within the framework of the incident handling process to handle attacks in an organized way. The faculty instruction, lab exercises, and exam are coordinated to develop and test a student's ability to utilize the core capabilities required for incident handling.

ISE 6315: Web App Penetration Testing and Ethical Hacking

SANS class: SEC 542 Web App Penetration Testing and Ethical Hacking
Assessment: GIAC GWAPT
3 Credit Hours | Tuition: $5,000

ISE 6315 is a highly technical information security course in offensive strategies where students learn the art of exploiting Web applications so they can find flaws in enterprise Web apps before they are otherwise discovered and exploited. Through detailed, hands-on exercises students learn the four-step process for Web application penetration testing. Students will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. They then utilize cross-site scripting attacks to dominate a target infrastructure in a unique hands-on laboratory environment. Finally students explore various other Web app vulnerabilities in-depth with tried-and-true techniques for finding them using a structured testing regimen.

ISE 6320: Network Penetration Testing and Ethical Hacking

SANS class: SEC 560 Network Penetration Testing and Ethical Hacking
Assessment: GIAC GPEN
3 Credit Hours | Tuition: $5,000

ISE 6320 prepares students to conduct successful penetration testing and ethical hacking projects. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with detailed hands-on exercises and practical tips for doing the job safely and effectively. Students will participate in an intensive, hands-on Capture the Flag exercise, conducting a penetration test against a sample target organization.

ISE 6300 Core NetWars Continuous Capstone

1 Credit Hour | Tuition: $0.00

Elective courses allow students choose one of the following:

ISE 6325: Mobile Device Security

SANS class: SEC 575 Mobile Device Security and Ethical Hacking
Assessment: GIAC GMOB
3 Credit Hours | Tuition: $5,000

ISE 6325 helps students resolve their organization's struggles with mobile device security by equipping then with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course teaches students to build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in their organization.

ISE 6330: Wireless Penetration Testing

SANS class: SEC 617 Wireless Ethical Hacking, Penetration Testing, and Defenses
Assessment: GIAC GAWN
3 Credit Hours | Tuition: $5,000

ISE 6330 takes an in-depth look at the security challenges of many different wireless technologies, exposing students to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, students will navigate through the techniques attackers use to exploit WiFi networks, Bluetooth devices, and a variety of other wireless technologies. Using assessment and analysis techniques, this course will show students how to identify the threats that expose wireless

technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

ISE 6350: Python for Penetration Testers

SANS class: SEC 573 Python for Penetration Testers
Assessment: GIAC GPYC
3 Credit Hours | Tuition: $5,000

The ISE 6350 course teaches students in the pen testing specialization, and other students who want to use the Python programming language, how to enhance their overall effectiveness during information security engagements. Students will learn how to apply core programming concepts and techniques learned in other courses through the Python programming language. The course teaches skills and techniques that can enhance an information security professional in penetration tests, security operations, and special projects. Students will create simple Python-based tools to interact with network traffic, create custom executable, test and interact with databases and websites, and parse logs or sets of data.

ISE 6360: Advanced Network Penetration Testing

SANS class: SEC 660 Advanced Penetration Testing, Exploits, and Ethical Hacking
Assessment: GIAC GXPN
3 Credit Hours | Tuition: $5,000

ISE 6360 builds upon ISE 6320 – Network Penetration Testing and Ethical Hacking. This advanced course introduces students to the most prominent and powerful attack vectors, allowing students to perform these attacks in a variety of hands-on scenarios.

Enrollment Design

The **Penetration Testing & Ethical Hacking** graduate certificate program is designed to be completed in 18-24 months, allowing each student adequate time between courses to practice and implement their skills. Enrolled students must complete all courses within three months of their course start date. Grades for each course are assigned according to a student's performance on the assessments, with letter grades for GIAC exams established versus a pre-determined numerical curve. All courses taken for credit must be taught by faculty of the SANS Technology Institute, but otherwise may be taken either live at a SANS event, at an on-site hosted at your organization, or online from home or work. Credit is earned only when a student enrolls first in a given certificate program and then registers for the appropriate graduate courses. Certain waivers may be available for previous SANS Institute class or GIAC experiences, please inquire at admissions@sans.edu for more information.

Because the certificate program is based on the courses that may be chosen by a master's candidate during the normal course of studies, all credits earned while completing the Penetration Testing & Ethical Hacking certificate program may be applied directly in fulfillment of the master's degree requirements should the student matriculate later in the master's program.

Admissions

Applicants to the **Penetration Testing & Ethical Hacking** post-baccalaureate certificate program must hold a bachelor's degree from a regionally accredited US institution (or international equivalent), and have at least 12 months of professional work experience in information technology, information security, or audit. The admissions process requires the submission of our online application, a current resume, and delivery of official undergraduate transcripts.

For additional information on the admissions process, please inquire at admissions@sans.edu.