+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 11/10/2024

Sign up

GIAC GPEN© Certification Preparation Course

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

5 days (35 hours)

Presentation

Become a certified slope climber with GIAC's renowned GPEN© certification. Our GPEN© training will prepare you step by step with a comprehensive program covering all the skills assessed in the exam.

We'll start this course with an introduction to penetration testing from various angles: planning, scoping, recognition and scanning. You'll learn to master the tools that are indispensable to ethical hackers: Nmap, Netcat, PowerShell and Netgrok.

We'll teach you the intrusion methods present in the test, such as password attacks, privilege escalation and exploitation. Finally, you'll be able to write convincing pentesting reports assessing the business risk.

In addition, strategies and methods will be divulged to prepare you for the GPEN© certification. We also prepare the practical part: GX-PT©.

Objectives

- Understand the main vulnerabilities and intrusion techniques for systems and the web
- Be ready for GPEN© certification

Target audience

- Slater
- Ethical hackers
- Red team member
- Blue team member
- Auditor
- Cybersecurity Analyst
- Cybersecurity Consultant

Prerequisites

- TCP/IP protocol experience
- Fluency in technical English
- Basic knowledge of Linux and Windows command lines

Hardware requirements

- Machine :
  - Minimum 64-bit Intel i5/i7 processor or AMD equivalent with 2 GHz or more
  - A recent, up-to-date operating system
  - 8GB RAM minimum
  - 50GB of free storage or more
  - A good Internet connection
  - Local administrative rights
- Software :
  - Depending on your environment, install: VMware Workstation Pro, VMware Player, VMWare Fusion Pro or VMware Fusion Player.
  - Disable VM Ware Hyper V on Windows
  - 7-Zip or Keka installed
  - Firewalls and antivirus software must be deactivated

Note: Ambient IT is not the owner of GPEN©, this certification belongs to GIAC©.

GIAC GPEN© Certification Preparation Program

Planning, scoping, recognition and scanning

- The mindset of the professional slider
- Setting up a world-class penetration testing infrastructure
- Create effective scopes and rules of engagement for penetration testing
- Recognition of target organization, infrastructure and users
- Tips for efficient scanning
- Version analysis with Nmap
- Reduction of false positives
- Netcat for pentesting
- Getting the most out of Nmap
- Scan faster with Masscan
- Operating system fingerprinting, in-depth version analysis
- EyeWitness

- Nmap in depth: The Nmap scripting engine

Initial access, payloads and situational awareness

- Obtain initial access
- Guess passwords, destroy them and fill them with credentials
- Operations and operating categories
- Operating network services and using Meterpreter
- Command and control frameworks and choosing the right one for you
- Use of opposing emulation and the red team framework, Sliver
- Post-operation with PowerShell Empire
- Payload generation in Metasploit and Sliver
- Presumed post-operational intrusion test
- Familiarity with Linux and Windows
- Extract useful information from a compromised Windows host with Seatbelt

Privilege escalation, persistence and password attacks

- Privilege escalation methods and techniques under Windows and Linux
- Identifying attack paths with BloodHound
- Maintaining access
- Tips for password attacks
- Hash recovery and manipulation on Windows, Linux and other systems
- Extracting hashes and passwords from memory with Mimikatz
- Efficient password cracking with John the Ripper and Hashcat
- Poisoning multicast name resolution with Responder

Lateral movements and ratio

- Lateral movement
- Remote command execution
- Attacking network protocols with Impacket
- Anti-virus and bypassing defense tools
- Bypassing application control using Windows built-in functions
- Implementation of port forwarding relays via SSH for Merciless-free pivots
- Pivoting in target environments with C2
- Effective reporting and corporate communication

Domain domination and Azure annihilation

- Kerberos authentication protocol
- Kerberoasting for domain privilege escalation and credential compromise
- Permanent access to the administrative area
- Assessing and attacking AD CS
- Obtain NTDS.dit and extract domain hashes
- Gold and silver ticket attacks for persistence
- Other Kerberos attacks, including Skeleton Key, Over-Pass-the-Hash and Pass-the-Ticket
- Effective escalation of domain privileges

- Azure and Azure AD recognition
- Attacks and destruction of Azure passwords
- Understanding Azure permissions
- Executing commands on Azure hosts
- Tunnels with Ngrok
- Lateral movement in Azure

Penetration test and flag capture

- Application of penetration testing and ethical hacking practices
- Detailed end-to-end analysis to identify vulnerabilities and access paths
- Exploitation to take control of target systems
- Post-operation to determine commercial risk
- Merciless pivot
- Analyze results to understand business risk and design corrective measures

Strategy and methods for exam success

Additional module (+1 day) : Preparing for GX-PT©

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.