



# Lead Pen Test Professional Certification

## **Introduction**

La formation *Certified Lead Pen Test Professional* est à la fois théorique et pratique qui va permettre aux participants de connaître le déroulement d'une mission de pen test et de manipuler les outils de scan et de pen test (nmap, metasploit,...).

## **Résumé de la Formation**

Ce cours intensif de cinq jours permet aux participants de développer l'expertise nécessaire pour mener un test professionnel de pénétration en utilisant un mélange de techniques pratiques et de compétences en gestion.

Le cours a été conçu par des experts de l'industrie avec une expérience approfondie dans les domaines de test de pénétration. Contrairement à d'autres certifications, ce cours se concentre spécifiquement sur les connaissances et les compétences nécessaires pour un professionnel qui cherche à conduire ou à prendre part à un test de pénétration. Le cours présentera les dernières techniques des connaissances, des outils et des techniques dans des domaines clés, y compris l'infrastructure, les Applications Web et la sécurité mobile, ainsi que l'ingénierie sociale.

Des exercices pratiques vont aider les participants à comprendre les concepts de pen testing et à manipuler les outils.

En parallèle avec les techniques et les outils, nous enseignons à nos participants comment devenir des « pen testeurs » respectés en leur décrivant les compétences de gestion et les bonnes pratiques dont ils ont besoin pour mener une mission de pénétration (pen testing) en maîtrisant l'environnement des entreprises et en gérant les risques.

## **Objectifs de la Formation**

- Etre en mesure d'interpréter et d'illustrer les principaux concepts et principes Penetration Testing
- Comprendre les connaissances techniques de base nécessaires pour organiser et bien mener un ensemble efficace de tests
- Apprendre à planifier efficacement un test de pénétration et à identifier un champ d'application qui est convenable et approprié en fonction du risque
- Apprendre les bonnes pratiques sur les compétences et les outils pertinents et techniques pour procéder à un test de pénétration efficace
- Gérer efficacement le temps et les ressources nécessaires à l'échelle d'un test de pénétration spécifique

## **Public visé**

La formation s'adresse aux:

- Professionnels de la sécurité qui souhaitent acquérir des compétences formelles dans les tests de pénétration.
- Personnel IT qui désirent améliorer leurs compétences et connaissances techniques

- Auditeurs qui cherchent à comprendre les processus des tests de pénétration
- Gestionnaires des IT et des risques qui cherchent une compréhension plus détaillée de l'utilisation appropriée et bénéfique des tests de pénétration
- Professionnels de la continuité des activités et de la manipulation des incidents qui cherchent à utiliser des tests dans le cadre de leurs opérations de tests

### **Pré requis**

- Connaissances basiques dans le domaine de la sécurité de l'information
- Connaissance des environnements Windows et Linux
- Connaissances basiques dans le développement

### **Informations Générales sur la Formation**

- 4j et 1/2 avec examen
- Cette formation permet aux participants d'avoir la certification Lead Pent Test Professional
- La formation est donnée en français.
- Un support (cours, exercices, corrigés) en anglais sera remis à chaque participant.
- Chaque session est limitée à un maximum de 15 personnes

### **Travaux pratiques**

Par des exercices réalisés en séance et des discussions, les participants seront capables de comprendre comment mener une mission de tests de pénétration (pen testing)

### **Formateur**

L'animateur, Anis Fourati, certifié ISO27001 et CLPTP et certifié PECB Formateur est consultant sénior en sécurité des systèmes d'informations et a plusieurs références dans l'audit de la sécurité de l'information en Tunisie et à l'étranger.

### **Organisme de certification**

L'organisme certificateur est : «Professional Evaluation and Certification Board (PECB) », un organisme de certification canadien accrédité par « The American National Standards Institute (ANSI) » et certifié ISO 17024.

### **Examen de Certification**

- L'examen de certification sera en anglais et dure 3h sous forme d'un QCM de 150 Questions
- Il aura lieu le 22 Avril 2016 de 9h à 12h

# **Programme détaillé de la Formation**

## **Jour 1: Introduction to Penetration Testing, ethics, planning and scoping**

- Penetration testing principles
- Legal and ethical issues
- Fundamental principles of information security and risk management
- Penetration testing approaches
- Phases of penetration testing
- Management of a penetration test
- **Exercices**

## **Jour 2: Technical Foundation Knowledge and Techniques (with practical exercises in all areas)**

- Network and Infrastructure Security
- Web Application Security
- Mobile Application Security
- Social Engineering
- **Exercices**

## **Jour 3: Conducting a penetration test using tools and techniques and review of testing areas**

- Conducting a penetration test – Infrastructure testing
- Conducting a penetration test – Web application penetration testing
- Conducting a penetration test – Social engineering testing
- Conducting a penetration test – Physical security testing
- **Exercices**

## **Jour 4: Analyzing results from testing, reporting and follow up**

- Documentation of the test quality review and reporting
- Action plans and follow up
- Managing a test programme
- Practical Capture the flag exercises – A 3 hour in class penetration test to be carried out by the delegates
- **Exercices**

## **Jour 5 : Examen de certification**