CERTIFICATION CERTIFIED PENETRATION TESTING (CPENT)

Objectifs

Après avoir terminé ce cours, vous devriez être capable de :

- Surmontez certains des obstacles les plus avancés auxquels les praticiens du monde réel sont confrontés lors de la réalisation de tests d'intrusion. Vous ferez face aux défis suivants
- Attaques Windows avancées
- Attaquer les systèmes IOT
- Écriture d'exploits : exploitation avancée des binaires
- Contourner un réseau filtré
- Technologie opérationnelle Pentesting (OT)
- Accédez aux réseaux cachés avec le pivotement
- Double pivotement
- Augmentation des privilèges
- Éviter les mécanismes de défense
- Automatisation des attaques avec des scripts
- Construisez votre propre armurerie : armez vos exploits
- Rédiger des rapports professionnels

Prérequis

Les participants doivent avoir des connaissances avancées sur les hackers éthiques, testeurs d'intrusion, administrateurs de serveurs réseau, administrateurs de pare-feu, testeurs de sécurité, administrateurs système et professionnels de l'évaluation des risques,

Programme

Module 01 : Introduction aux tests d'intrusion

Module 02 : Portée et engagement des tests d'intrusion

Module 03 : Intelligence Open Source (OSINT)

Module 04 : Tests d'intrusion d'ingénierie sociale

Module 05 : Tests de pénétration du réseau – Externe

Module 06 : Tests de pénétration du réseau – Interne

Module 07 : Tests de pénétration du réseau – Appareils de périmètre

Module 08 : Tests de pénétration des applications Web

Module 09 : Tests de pénétration sans fil

Module 10 : Tests de pénétration IoT

Module 11 : Tests d'intrusion OT/SCADA

Module 12 : Tests de pénétration du cloud

Module 13 : Analyse et exploitation binaires

Module 14 : Rédaction de rapports et actions post-test