المؤسسة العربية للاستشارات والتدريب وتطوير الأداء
AINFCT I info@ainfct.com I www.ainfct.com

Ethical Hacker-CEH

فكرة الدورة

أصبحت الهجمات السيبرانية أكثر تنوعاً وتعقيداً مع توسع الخدمات الرقمية، وتزايد الاعتماد على الشبكات السحابية، والتطبيقات المتصلة، والأنظمة التي تتعامل مع بيانات حساسة. وفي هذا السياق، لم يعد اختبار الأمن نشاطاً تقنياً منفصلاً، بل أصبح جزءاً مهماً من إدارة المخاطر، وتحسين الضوابط، ورفع قدرة المؤسسة على اكتشاف نقاط الضعف قبل استغلالها.

يركز هذا البرنامج التدريبي من AINFCT على بناء فهم عملي ومنضبط لمبادئ الاختبار الأخلاقي، بدءاً من الأساسيات القانونية والأخلاقية، مروراً بجمع المعلومات، والفحص، وتحليل الثغرات، وانتهاءً بتقييم أمن الشبكات والتطبيقات والبيئات السحابية واللاسلكية. كما يوضح البرنامج كيفية تحويل نتائج الاختبار إلى توصيات دفاعية قابلة للتنفيذ.

يوفر البرنامج قيمة مهنية واضحة من خلال الجمع بين التفكير التحليلي والمنهجية الأخلاقية، بما يساعد المشاركين على دعم فرق الأمن في تحسين الوضع الأمني وتقليل التعرض للمخاطر.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تفسير مبادئ الاختبار الأخلاقي والالتزام القانوني.
- تنفيذ جمع معلومات ضمن نطاق مصرح.
- تحليل نتائج الفحص وتحديد مؤشرات المخاطر.
- تقييم أمن الشبكات والتطبيقات والأنظمة.
- توثيق الثغرات وفق منهجية مهنية واضحة.
- اقتراح معالجات أمنية قابلة للتنفيذ.

منهجية الدورة

- عروض تفاعلية تشرح المفاهيم والمنهجيات الأساسية.
- تمارين تحليل نتائج ضمن سيناريوهات مصرح بها.
- دراسات حالة حول إدارة الثغرات والتقارير.
- مناقشات موجهة حول أخلاقيات الاختبار وحدوده.
- مراجعات معرفية قصيرة بعد المحاور الرئيسية.

أثر الدورة على المنظمة

يمكن تعزيز قدرة المؤسسة على إدارة الثغرات من خلال:

- تحسين اكتشاف نقاط الضعف قبل استغلالها.
- رفع جودة تقارير الاختبار الأمني.
- دعم قرارات المعالجة حسب مستوى المخاطر.
- تعزيز التكامل بين الاختبار والدفاع.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- فهم مراحل الاختبار الأخلاقي باحترافية.
- استخدام أدوات الفحص ضمن نطاق مصرح.
- تحليل الثغرات بمنهجية منظمة.
- صياغة توصيات أمنية عملية.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المختصين الراغبين في فهم الاختبار الأخلاقي ضمن إطار مهني وقانوني منضبط. كما يفيد العاملين الذين يشاركون في حماية الأنظمة، وتحليل الثغرات، ودعم فرق الأمن السيبراني.

- مختصو الأمن السيبراني وأمن المعلومات.
- مسؤولو الشبكات والأنظمة والبنية التحتية.
- محللو الثغرات والمخاطر التقنية.
- أعضاء فرق العمليات الأمنية والاستجابة.
- المرشحون لتطوير مسار مهني مرتبط بـ CEH.

موضوعات الدورة

اليوم الأول: مدخل إلى الهاكر الأخلاقي والمسؤولية المهنية

- مفهوم الاختبار الأخلاقي ودوره في الأمن السيبراني.
- الفرق بين الاختبار المصرح والهجوم غير المشروع.
- القواعد القانونية والأخلاقية ونطاق التفويض.
- دورة حياة الاختبار الأمني ومخرجات كل مرحلة.
- مبادئ السلامة التشغيلية أثناء الاختبار.

اليوم الثاني: أساسيات أمن المعلومات والشبكات

- مفاهيم السرية والسلامة والتوافر في الاختبار.
- مكونات الشبكات والبروتوكولات الأساسية.
- نماذج الاتصال وطبقات الشبكة من منظور أمني.
- التهديدات الشائعة ضد الأنظمة والخدمات.
- الربط بين الثغرات والضوابط الدفاعية.

اليوم الثالث: جمع المعلومات والاستطلاع

- أنواع الاستطلاع السلبي والنشط.
- مصادر المعلومات المفتوحة وحدود استخدامها.
- تحليل أسماء النطاقات والبنية الظاهرة.
- جمع مؤشرات تقنية دون تجاوز نطاق التفويض.
- توثيق نتائج الاستطلاع بصورة قابلة للمراجعة.

اليوم الرابع: الفحص والتعداد الأمني

- أهداف الفحص الأمني وتحديد الأصول النشطة.
- فحص المنافذ والخدمات وتفسير النتائج.
- التعداد المرتبط بالحسابات والخدمات والبروتوكولات.

- مؤشرات التهيئة الضعيفة والخدمات المكشوفة.
- تقليل الأثر التشغيلي لعمليات الفحص.

اليوم الخامس: تحليل الثغرات وإدارة النتائج

- مفهوم الثغرة ومصادر معلوماتها المهنية.
- تقييم الخطورة باستخدام الاحتمالية والأثر.
- ترتيب الثغرات حسب الأولوية التشغيلية.
- التحقق الآمن من النتائج وتقليل الإيجابيات الكاذبة.
- ربط النتائج بخطط المعالجة والمتابعة.

اليوم السادس: أمن الأنظمة وتقنيات الوصول غير المصرح

- أنماط الهجمات على أنظمة التشغيل والخدمات.
- نقاط الضعف المرتبطة بكلمات المرور والصلاحيات.
- مفاهيم التصعيد والتحرك الجانبي على مستوى عالٍ.
- آثار التكوينات غير الآمنة على الأنظمة.
- ضوابط الحماية والتقوية ومراقبة السلوك.

اليوم السابع: البرمجيات الخبيثة والتهديدات المتقدمة

- أنواع البرمجيات الخبيثة ومؤشرات وجودها.
- أساليب الانتشار والتأثير على الأنظمة.
- مبادئ التحليل الآمن داخل بيئات معزولة.
- مؤشرات الاختراق وربطها بالمراقبة الدفاعية.
- الضوابط الوقائية والاستجابة الأولية.

اليوم الثامن: الهندسة الاجتماعية وأمن المستخدم

- مفهوم الهندسة الاجتماعية وعوامل نجاحها.
- أساليب التصيد والاحتيال الرقمي الشائعة.
- اختبار الوعي الأمني ضمن ضوابط مصرح بها.

- حماية المستخدمين والعمليات من الخداع.
- إعداد توصيات توعوية قائمة على المخاطر.

اليوم التاسع: أمن الشبكات المحيطية والبنية الدفاعية

- تقييم الجدران النارية وأنظمة الحماية المحيطية.
- تحليل التقسيم الشبكي وحدود الثقة.
- مخاطر الخدمات المكشوفة والوصول البعيد.
- اختبار الضوابط دون تعطيل الخدمات.
- توصيات تقوية الشبكات وتحسين المراقبة.

اليوم العاشر: أمن الويب والتطبيقات

- مدخل إلى بنية تطبيقات الويب الحديثة.
- الثغرات الشائعة في المدخلات والجلسات.
- أخطاء التحكم في الوصول داخل التطبيقات.
- اختبار التطبيقات وفق نطاق مصرح وآمن.
- ربط نتائج الاختبار بإجراءات تطوير آمنة.

اليوم الحادي عشر: أمن قواعد البيانات والبيانات

- مخاطر قواعد البيانات والتكوينات الضعيفة.
- حماية الاستعلامات والواجهات المرتبطة بالبيانات.
- إدارة الصلاحيات والحسابات عالية الامتياز.
- مراقبة الوصول إلى البيانات الحساسة.
- توصيات حماية البيانات وتقليل التعرض.

اليوم الثاني عشر: أمن الشبكات اللاسلكية والأجهزة المتصلة

- مخاطر الشبكات اللاسلكية وآليات الحماية.
- تقييم إعدادات التشفير والمصادقة اللاسلكية.
- الاعتبارات الأمنية للأجهزة المحمولة والمتصلة.

- تهديدات إنترنت الأشياء والبيئات التشغيلية.
- ضوابط الفصل والمراقبة والتحديث الآمن.

اليوم الثالث عشر: أمن الحوسبة السحابية والخدمات الحديثة

- نماذج الخدمة السحابية ومسؤولية الحماية المشتركة.
- مخاطر الهوية والتخزين والتكوين السحابي.
- تقييم الضوابط السحابية من منظور الاختبار.
- اعتبارات الحاويات وواجهات البرمجة.
- توصيات تقليل التعرض في البيئات السحابية.

اليوم الرابع عشر: التقارير المهنية والتواصل مع أصحاب المصلحة

- بنية تقرير الاختبار الأمني ومكوناته.
- صياغة الملخص التنفيذي بلغة واضحة.
- توثيق الأدلة دون كشف تفاصيل حساسة.
- ترتيب المعالجات حسب المخاطر والأولوية.
- عرض النتائج بصورة تدعم القرار الأمني.

اليوم الخامس عشر: مراجعة تطبيقية وتكامل المنهجية

- مراجعة مراحل الاختبار الأخلاقي كاملة.
- تحليل سيناريو تطبيقي متعدد المجالات.
- ربط نتائج الفحص بالتحسين الدفاعي.
- مناقشة الأخطاء الشائعة في الاختبارات.
- إعداد خطة تطوير مهني بعد البرنامج.

course_daily_schedule

يمتد البرنامج لمدة 15 يوماً تدريبياً، بواقع 4 ساعات تدريبية يومياً. يبدأ كل يوم بمراجعة موجزة للمفاهيم السابقة، ثم عرض للمحور الرئيسي، يتبعه نشاط تطبيقي أو نقاش موجه، وينتهي اليوم بخلاصة تربط الموضوعات بمخرجات عملية قابلة للاستخدام داخل بيئة العمل. يتم توزيع الوقت بما يوازن بين الشرح، والتحليل، والتطبيق، والمراجعة.

course_assessment

يعتمد التقييم على المشاركة الفعالة، والتمارين التطبيقية، وتحليل السيناريوهات، والمراجعات القصيرة المرتبطة بمحاور البرنامج. يحصل المشاركون في نهاية البرنامج على شهادة حضور/إتمام من AINFCT وفق متطلبات الحضور والمشاركة المعتمدة.

course_key_competencies

- الاختبار الأخلاقي.
- جمع المعلومات الأمني.
- تحليل الثغرات.
- تقييم أمن الشبكات.
- أمن التطبيقات.
- التقارير الأمنية.

مكتب القاهرة الرئيسي
القاهرة، جمهورية مصر العربية
7 شارع وهران، الطيران، مدينة نصر
+201152466358
info@ainfct.com
ainfct.com
رقم التسجيل الضريبي: 472920235
مكتب مدريد الفرعي
مدريد، إسبانيا

شارع الصحة 3، وسط المدينة، 28013 مدريد
training@ainfct.com
ainfct.com