ainfct

المؤسسة العربية للاستشارات والتدريب وتطوير الأداء

AINFCT | info@ainfct.com | www.ainfct.com

Advanced Penetration Testing and Exploitation

فكرة الدورة

تحتاج المؤسسات الحديثة إلى قدرات اختبار أمني متقدمة تساعدها على كشف الثغرات العميقة، وفهم أساليب الخصوم، وتقييم قدرة الضوابط الحالية على الصمود أمام سيناريوهات هجوم معقدة. ومع توسع البيئات السحابية والتطبيقات المتصلة وسلاسل التوريد الرقمية، أصبح اختبار الاختراق المتقدم ممارسة ضرورية لدعم إدارة المخاطر والتحقق من فعالية الدفاعات.

يركز هذا البرنامج التدريبي من AINFCT على بناء فهم مهني متقدم لمنهجيات اختبار الاختراق، بدءاً من التخطيط وتحديد النطاق، مروراً بالاستطلاع والتحليل الفني، وصولاً إلى تقييم الاستغلال، ورفع الامتيازات، والحركة الجانبية، واختبار التطبيقات والشبكات والبيئات السحابية. ويتم تناول الموضوعات من منظور منضبط يوازن بين العمق التقني، والحوكمة، وأخلاقيات الاختبار، وسلامة بيئة العمل.

يوفر البرنامج قيمة تطبيقية واضحة من خلال تحويل نتائج الاختبار إلى توصيات قابلة للتنفيذ، وربط المخرجات الفنية بقرارات التحسين الأمني وإدارة المخاطر المؤسسية.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تخطيط اختبارات اختراق متقدمة وفق نطاق واضح.
- تحليل أسطح الهجوم في البيئات المعقدة.
- تقييم قابلية الاستغلال دون الإضرار بالأنظمة.
- تنفيذ تحقق أمني منضبط للتطبيقات والشبكات.
- صياغة تقارير فنية وتنفيذية عالية الجودة.
- ربط نتائج الاختبار بإدارة المخاطر.

منهجية الدورة

- عروض تفاعلية تركّز على المنهجية والقرار المهني.
- سيناريوهات تحليلية لاختبار بيئات مؤسسية افتراضية.
- تمارين توثيق نتائج وصياغة تقارير فنية.
- مناقشات موجهة حول إدارة المخاطر أثناء الاختبار.
- مراجعات معرفية قصيرة في نهاية المحاور الرئيسية.

أثر الدورة على المنظمة

يمكن رفع فاعلية الدفاعات السيبرانية المؤسسية من خلال:

- تحسين اكتشاف الثغرات عالية الأثر.
- دعم أولويات المعالجة بناءً على المخاطر.
- اختبار فعالية الضوابط في سيناريوهات واقعية.
- تعزيز جودة التقارير الأمنية للإدارة.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- تطبيق منهجيات اختبار متقدمة ومنضبطة.
- فهم تقنيات الخصوم ضمن سياق دفاعي.
- تحليل نتائج الاستغلال بمهنية عالية.
- تقديم توصيات معالجة عملية وواضحة.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المشاركين ذوي الخلفية التقنية في الأمن السيبراني أو الشبكات أو إدارة الأنظمة، ممن يحتاجون إلى تطوير قدراتهم في اختبار الاختراق المتقدم ضمن أطر مهنية ومنضبطة. كما يلائم الفرق المسؤولة عن التحقق الأمني وتحسين الضوابط الدفاعية.

- مختصو اختبار الاختراق والأمن الهجومي.
- محللو الأمن السيبراني ومراكز العمليات الأمنية.
- مسؤولو الشبكات والأنظمة والبنية التحتية.
- فرق إدارة الثغرات والتحقق الأمني.
- مستشارو أمن المعلومات وإدارة المخاطر التقنية.

موضوعات الدورة

اليوم الأول: الحوكمة المهنية لاختبار الاختراق المتقدم

- أهداف اختبار الاختراق المتقدم وحدوده المهنية.
- الأدوار والمسؤوليات بين الفريق والجهة المالكة للنظام.
- قواعد الاشتباك وتوثيق النطاق والصلاحيات.
- الاعتبارات القانونية والأخلاقية وسلامة بيئة الاختبار.
- إدارة المخاطر التشغيلية أثناء تنفيذ الاختبارات.

اليوم الثاني: التخطيط وتحديد النطاق وبناء المنهجية

- تحليل أهداف الاختبار وربطها بالمخاطر المؤسسية.
- اختيار نوع الاختبار المناسب للبيئة المستهدفة.
- تحديد الأصول الحرجة وحدود الاختبار والاستثناءات.
- بناء خطة اختبار متدرجة وقابلة للتدقيق.
- توثيق الافتراضات والقيود وقنوات التصعيد.

اليوم الثالث: الاستطلاع المتقدم وتحليل سطح الهجوم

- مصادر المعلومات المفتوحة وأساليب جمع المؤشرات.
- تحليل البصمة الرقمية للمؤسسة والأنظمة المكشوفة.
- تحديد التقنيات والخدمات ونقاط التعرض المحتملة.
- تحليل العلاقات بين الأصول والهويات والموردين.
- تنظيم نتائج الاستطلاع لدعم مراحل الاختبار اللاحقة.

اليوم الرابع: النمذجة الهجومية وربطها بذكاء التهديدات

- استخدام أطر التكتيكات والتقنيات لفهم سلوك الخصوم.
- بناء سيناريوهات اختبار مرتبطة بأهداف أعمال محددة.
- تحليل مسارات الهجوم المحتملة داخل البيئة.

- تحديد نقاط التحكم والمراقبة المتوقعة.
- تحويل معلومات التهديد إلى فرضيات اختبار عملية.

اليوم الخامس: اختبار الشبكات والبنية التحتية

- تقييم الخدمات والبروتوكولات المكشوفة داخل النطاق.
- تحليل أخطاء الإعدادات وضعف التقسيم الشبكي.
- اختبار الضوابط الحدودية وقواعد السماح والمنع.
- تقييم مخاطر الخدمات الإدارية والواجهات البعيدة.
- ربط نتائج الشبكات بمسارات التصعيد المحتملة.

اليوم السادس: اختبار أنظمة التشغيل والخدمات المؤسسية

- تحليل التكوينات الأمنية في الخوادم ومحطات العمل.
- تقييم التصحيحات والثغرات المرتبطة بالخدمات.
- اختبار التحكم في الصلاحيات والملفات الحساسة.
- تحديد نقاط الضعف في خدمات الدليل والهوية.
- توثيق النتائج بطريقة تدعم المعالجة الفنية.

اليوم السابع: تقنيات الاستغلال المنضبط والتحقق الآمن

- مبادئ التحقق من قابلية الاستغلال ضمن بيئات مصرح بها.
- تقدير أثر الثغرة دون تعطيل الخدمة.
- استخدام الأدلة الفنية لإثبات مستوى الخطر.
- ضبط حدود الاختبار لتجنب الأثر غير المقصود.
- تصنيف النتائج حسب الاحتمالية والأثر وسهولة المعالجة.

اليوم الثامن: رفع الامتيازات وإدارة الهويات المميزة

- تحليل مسارات التصعيد عبر الحسابات والصلاحيات.
- تقييم ضعف إعدادات الامتيازات المحلية والمركزية.
- اختبار ضوابط الوصول للحسابات الحساسة.

- رصد فرص إساءة استخدام الاعتمادات والهويات.
- تقديم توصيات لتقليل الامتيازات وتحسين المراقبة.

اليوم التاسع: الحركة الجانبية والتمركز داخل البيئة

- تحليل مسارات الانتقال بين الأنظمة ضمن النطاق.
- تقييم فعالية التقسيم الشبكي وحدود الثقة.
- اختبار الضوابط التي تمنع الانتشار الداخلي.
- فهم مؤشرات السلوك غير الطبيعي أثناء الاختبار.
- تحديد نقاط التحسين في الرصد والاستجابة.

اليوم العاشر: اختبار تطبيقات الويب وواجهات البرمجة

- تقييم المصادقة والتفويض وإدارة الجلسات.
- اختبار التحقق من المدخلات وأخطاء المعالجة.
- تحليل منطق الأعمال ومسارات إساءة الاستخدام.
- تقييم أمن واجهات البرمجة وتبادل البيانات.
- ترتيب ثغرات التطبيقات وفق أثرها التشغيلي.

اليوم الحادي عشر: اختبار البيئات السحابية والهجينة

- فهم نموذج المسؤولية المشتركة في الاختبار السحابي.
- تقييم إعدادات الهوية والصلاحيات السحابية.
- تحليل التخزين المكشوف وضوابط التشفير والمفاتيح.
- اختبار العزل بين الموارد والبيئات والحسابات.
- توثيق مخاطر السحابة بلغة قابلة للتنفيذ.

اليوم الثاني عشر: الاختبار المتقدم للرصد والكشف

- تقييم فعالية السجلات والتنبيهات أثناء الاختبار.
- ربط الأنشطة الفنية بمؤشرات قابلة للرصد.
- تحليل فجوات الكشف في مركز العمليات الأمنية.

- اختبار جودة إجراءات التصعيد والاستجابة.
- تقديم توصيات لتحسين قواعد الكشف والمراقبة.

اليوم الثالث عشر: إدارة الأدلة والتوثيق الفني

- توثيق خطوات الاختبار بطريقة قابلة للمراجعة.
- حفظ الأدلة الفنية دون تعريض البيانات للخطر.
- تمييز النتائج المؤكدة عن المؤشرات غير الحاسمة.
- صياغة وصف الثغرات وأثرها وسياقها.
- بناء سجل ملاحظات يدعم التقرير النهائي.

اليوم الرابع عشر: التقارير التنفيذية وخطط المعالجة

- بناء ملخص تنفيذي يوضح المخاطر والأولويات.
- كتابة نتائج فنية دقيقة وقابلة للتنفيذ.
- تحديد توصيات معالجة قصيرة ومتوسطة المدى.
- ربط النتائج بمالكي الأنظمة ومواعيد الإغلاق.
- تقديم مؤشرات قياس لمتابعة التحسين الأمني.

اليوم الخامس عشر: تطبيق تكاملي ومراجعة مهنية

- تحليل سيناريو اختبار اختراق متقدم من البداية للنهاية.
- تقييم قرارات النطاق والتحقق والتصعيد.
- مراجعة جودة الأدلة والتوصيات والتقارير.
- مناقشة أخطاء شائعة في الاختبارات المتقدمة.
- بناء خطة تطوير مهني بعد انتهاء 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 نقاش أو تمرين تطبيقي، وينتهي بخلاصة تربط نتائج اليوم بمخرجات الاختبار المهني. يتم توزيع الوقت بما يوازن بين الشرح، والتحليل، والتطبيق، ومراجعة المخرجات.

course_assessment

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

course_key_competencies

- تخطيط اختبار الاختراق.
- تحليل سطح الهجوم.
- الاستغلال الأمني المنضبط.
- تقييم تطبيقات الويب.
- اختبار البيئات السحابية.
- التقارير الأمنية المهنية.

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