BLACKBIRD FOR TRAINING

# دورة الاختراق الأخلاقي واختبار الاختراق المتقدم

October 2027 22 – 18

لندن (المملكة المتحدة)

UK Traininig

PARTNER



www.blackbird-training.com

# دورة الاختراق الأخلاقي واختبار الاختراق المتقدم

**المرجع:** 201633_3255277 **التاريخ:** 18 – 22 October 2027 **المكان:** لندن (المملكة المتحدة) **الرسوم:** GBP 6100

## مقدمة

في عالم يعتمد على التكنولوجيا في جميع جوانب الحياة اليومية، أصبحت الأمن السيبراني ضرورة استراتيجية لحماية الأنظمة والمعلومات من التهديدات المتزايدة. ومع التطور المستمر في تقنيات الهجوم الإلكتروني، برز مفهوم الاختراق الأخلاقي واختبار الاختراق المتقدم كأحد أهم الأساليب الاستباقية لتعزيز الحماية واكتشاف الثغرات قبل أن يستغلها المهاجمون.

تهدف دورة الاختراق الأخلاقي واختبار الاختراق المتقدم إلى تزويد المشاركين بفهم عميق لأساليب القراصنة الأخلاقيين وتقنيات اختبار الأنظمة والشبكات والتطبيقات لاكتشاف نقاط الضعف وتصحيحها. تجمع الدورة بين المعرفة النظرية والتطبيق العملي، مما يتيح للمشاركين تنفيذ اختبارات أمنية حقيقية باستخدام أدوات متقدمة وأساليب احترافية تُستخدم عالمياً في مجال الأمن السيبراني.

## أهداف الدورة

بنهاية الدورة، سيتمكن المشاركون من:

- فهم المفاهيم الأساسية للاختراق الأخلاقي وأهميته في حماية الأنظمة.
- تحليل البنية الأمنية للشبكات والأنظمة والتطبيقات.
- استخدام أدوات اختبار الاختراق لاكتشاف الثغرات الأمنية.
- تنفيذ اختبارات أمنية على بيئات حقيقية بشكل آمن ومنهجي.
- إعداد تقارير احترافية تتضمن نتائج الاختبارات والتوصيات الأمنية.
- التعامل مع الثغرات الأمنية وإغلاقها بطرق فعالة.
- تطبيق أفضل الممارسات في مجال الأمن الوقائي والاستجابة للحوادث.



## محاور الدورة

### اليوم الأول: مدخل إلى الاختراق الأخلاقي ومفاهيم الأمن السيبراني

- مقدمة في الاختراق الأخلاقي وأنواعه.
- الفرق بين القراصنة الأخلاقيين والمخترقين الخبيثين.
- مراحل عملية الاختراق الأخلاقي الاستطلاع، الفحص، الاستغلال، التقارير.
- المبادئ القانونية والأخلاقية لممارسة الاختراق الأخلاقي.
- بيئة العمل والأدوات المستخدمة في اختبار الاختراق.

### اليوم الثاني: جمع المعلومات والاستطلاع

- تقنيات جمع المعلومات العامة والمخفية عن الأنظمة المستهدفة.
- أدوات الاستطلاع النشط والسلبي.
- تحليل البنى الشبكية وتحديد نقاط الدخول المحتملة.
- استخدام أدوات متخصصة لاكتشاف المنافذ والخدمات المفتوحة.
- إعداد خرائط للشبكات وتحليل البنية التحتية الرقمية.

### اليوم الثالث: تحليل الثغرات والاستغلال

- أدوات فحص الثغرات واكتشاف نقاط الضعف.
- تحليل نتائج الفحص وتحديد المخاطر الأمنية.
- استغلال الثغرات للوصول إلى الأنظمة المستهدفة.
- تقنيات تجاوز أنظمة الحماية والجدران النارية.
- تطبيق عملي على اختراق بيئة تجريبية واستخلاص البيانات.

### اليوم الرابع: اختبار الاختراق لتطبيقات الويب والأنظمة

- تحليل أمن تطبيقات الويب وتحديد الثغرات الشائعة.
- ثغرات حقن الأوامر وحقن قواعد البيانات.
- استغلال ثغرات المصادقة والتحكم في الجلسات.
- تقييم أمان أنظمة التشغيل والخوادم.
- تقنيات رفع الصلاحيات والتحكم عن بُعد.



## اليوم الخامس: إعداد التقارير والمعالجة الأمنية

- توثيق نتائج الاختبارات بطريقة احترافية.
- إعداد تقارير توضح الخطورة والتوصيات الأمنية.
- استراتيجيات معالجة الثغرات وإغلاقها.
- تحسين بيئة الأمن السيبراني بناءً على نتائج التقييم.
- مراجعة شاملة وتقييم عملي نهائي.

## لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- تعلم أساليب القراصنة الأخلاقيين وفهم طرق عملهم بدقة.
- اكتساب مهارات عملية في استخدام أدوات اختبار الاختراق الاحترافية.
- تعزيز القدرة على اكتشاف الثغرات قبل استغلالها من قبل المهاجمين.
- تطوير مهارات إعداد التقارير والتحليل الأمني المتقدم.
- بناء خبرة واقعية من خلال تمارين عملية في بيئة آمنة.
- تحسين جاهزية المؤسسة في مواجهة الهجمات السيبرانية.
- فهم دورة حياة الهجمات الإلكترونية من البداية حتى الاستجابة.
- رفع الكفاءة التقنية في مجالات الأمن الرقمي والتقييم الوقائي.

## الخاتمة

تُعد دورة الاختراق الأخلاقي واختبار الاختراق المتقدم محطة أساسية لأي مختص يسعى إلى تعزيز قدراته في مجال الأمن السيبراني. فهي تدمج بين الجانب العلمي والعملي لتأهيل المشاركين لاكتشاف الثغرات والتعامل معها بشكل احترافي، مما يساهم في بناء بيئات رقمية أكثر أماناً.

تمكن هذه الدورة المؤسسات من الانتقال من النهج الدفاعي إلى الاستباقي في حماية أصولها الرقمية. كما تمنح المشاركين القدرة على فهم ديناميكيات الهجمات الإلكترونية والتفكير بنفس منطق القراصنة، لكن بهدف الحماية لا الاختراق.

**في عالم تتسارع فيه التهديدات الإلكترونية، يمثل الاختراق الأخلاقي أداة أساسية لضمان الأمن والاستقرار الرقمي للمؤسسات.**

