BLACKBIRD FOR TRAINING

الهاكر الأخلاقي

June 2027 25 – 21

لندن (المملكة المتحدة)



الهاكر الأخلاقي

المرجع: 342067_3255450 **التاريخ:** 21 – 25 June 2027 **المكان:** لندن (المملكة المتحدة) **الرسوم:** GBP 6100

مقدمة

يشهد العالم المعاصر توسعًا متسارعًا في الاعتماد على الأنظمة الرقمية، الأمر الذي جعل حماية المعلومات ضرورة أساسية لضمان استمرارية الأعمال والحفاظ على سمعة المؤسسات. ومع تطور الهجمات الإلكترونية وتعقيد أساليب الاختراق، لم يعد تأمين الأنظمة مجرد خيار إضافي، بل أصبح عنصرًا محوريًا في إدارة المخاطر. هنا يظهر دور الهاكر الأخلاقي باعتباره متخصصًا يمتلك المعرفة العميقة بأساليب الهجوم المختلفة، لكنه يوظف مهاراته في خدمة حماية الأنظمة وكشف الثغرات قبل استغلالها من جهات غير مصرح لها.

تستهدف هذه الدورة مجموعة واسعة من المهنيين، تشمل التنفيذيين، قادة الفرق، مسؤولي الأنظمة، محللي الأمن الرقمي، المتخصصين في إدارة الشبكات، ومديري المشاريع التقنية، إضافة إلى المهتمين بتطوير مسارهم في مجال الأمن السيبراني. ويبحث هؤلاء عن مهارات متقدمة، وأدوات عملية، ومعارف حديثة تساعدهم على حماية مؤسساتهم من المخاطر الرقمية المتزايدة. كما أن العديد من المؤسسات أصبحت تعتمد على هذه المهارات لتعزيز قدراتها الدفاعية وتحسين استراتيجياتها الأمنية، مما يجعل الحصول على خبرة في مجال الهاكر الأخلاقي خطوة استراتيجية مهمة.

تهدف الدورة إلى توفير محتوى شامل يجمع بين المعرفة النظرية والتطبيق العملي، من خلال استعراض أساليب الاختبار الأمني، تحليل الثغرات، التعامل مع الهجمات المحتملة، وإدارة الاستجابة للمخاطر. ويستند البرنامج إلى منهجية منظمة ترتكز على أفضل الممارسات العالمية، مما يتيح للمشاركين فرصة اكتساب خبرة تطبيقية تساعدهم في تقييم الأنظمة، تحديد نقاط الضعف، وتقديم التوصيات المناسبة لتعزيز الأمن الرقمي. ومع تعدد التهديدات الإلكترونية وتنوعها، تمنح هذه الدورة فرصة فريدة لفهم كيفية حماية البنية التحتية المعلوماتية بطريقة منهجية ومستدامة.



أهداف الدورة

- التعرف على المفاهيم الأساسية المتعلقة بالأمن السيبراني ودور الهاكر الأخلاقي.
- فهم أنواع الهجمات الشائعة وطرق تحليلها والتعامل معها.
- اكتساب القدرة على تقييم نقاط الضعف في الأنظمة والشبكات.
- استخدام الأدوات الأساسية للكشف عن الثغرات وتحليل المخاطر.
- تطوير مهارات اختبار الاختراق بشكل عملي وممنهج.
- إعداد تقارير احترافية حول الثغرات، تتضمن تقييمًا شاملاً وحلولاً مقترحة.
- تحليل السيناريوهات المحتملة للهجمات والاستجابة لها.
- تصميم خطط حماية تساهم في تقليل المخاطر وتعزيز الأمن المؤسسي.
- بناء مهارات تساعد على اتخاذ القرارات الأمنية المناسبة في البيئات التقنية الحرجة.
- توظيف التفكير النقدي وطرق التحقق الأمني لتحسين جودة الأنظمة الرقمية.

محاور الدورة

اليوم الأول: أساسيات الأمن السيبراني ومفهوم الهاكر الأخلاقي

- التعرف على مفهوم الهاكر الأخلاقي ودوره في حماية الأنظمة.
- مبادئ الأمن السيبراني وأهميته في المؤسسات.
- الفرق بين الاختراق الأخلاقي وغير الأخلاقي.
- أنواع التهديدات الرقمية وتأثيرها على الأعمال.
- المفاهيم الأساسية في حماية الشبكات والأنظمة.
- خطوات بناء قاعدة معرفية قوية لاحتراف المجال.

اليوم الثاني: أدوات التحليل والكشف عن الثغرات

- التعرف على أدوات الاختبار الأمني المستخدمة في تحليل الأنظمة.
- طريقة عمل أدوات فحص المنافذ ورصد الخدمات النشطة.
- تحليل مستويات التشفير والبحث عن نقاط ضعف التهيئة.
- آليات مسح الشبكات وتحديد مصادر المخاطر.
- فهم سجلات الأنظمة واستخدامها في التحقيقات الأمنية.
- تمارين تطبيقية حول فحص الأنظمة وتحليل النتائج.



اليوم الثالث: اختبار الاختراق وأساليب الهجوم

- دراسة مراحل اختبار الاختراق من الاستطلاع حتى التنفيذ.
- التمييز بين أنواع الهجمات الشائعة وطريقة اكتشاف آثارها.
- تحليل الثغرات التي تستهدف البنية التحتية الشبكية.
- فهم المبادئ الأساسية لهجمات الهندسة الاجتماعية.
- محاكاة سيناريوهات دخول غير مصرح به إلى الأنظمة.
- تطبيقات عملية على تقييم الأنظمة واختبار متانتها.

اليوم الرابع: إدارة المخاطر والاستجابة للحوادث

- منهجيات تحليل المخاطر وتقييم تأثير التهديدات.
- تصميم خطط استجابة فعالة للهجمات الرقمية.
- تقنيات تتبع الهجمات وتحديد مصدرها.
- كيفية إعداد خطط التعافي بعد الحوادث الرقمية.
- بناء آليات مراقبة مستمرة للأنظمة الحساسة.
- دراسة حالات عملية توضح كيفية التعامل مع الانتهاكات الأمنية.

اليوم الخامس: إعداد التقارير والتوصيات الأمنية

- كيفية صياغة تقارير احترافية بعد اختبار الاختراق.
- تحديد نقاط الضعف ووصفها بطريقة منهجية.
- وضع توصيات عملية تتناسب مع طبيعة المؤسسة.
- بناء استراتيجية حماية متكاملة تعتمد على نتائج الفحص.
- تقييم مستوى النضج الأمني واقتراح منهجيات التحسين.
- مراجعة شاملة لمحتوى الدورة واستخلاص الدروس النهائية.



لماذا يجب عليك حضور هذه الدورة؟ الإيجابيات والسلبيات!

- اكتساب معرفة متقدمة في مجال الهاكر الأخلاقي.
- تطوير مهارات عملية يمكن تطبيقها مباشرة في بيئات العمل.
- تحسين قدرتك على اكتشاف الثغرات قبل استغلالها.
- تعزيز مهاراتك في إدارة المخاطر والاستجابة للهجمات.
- دعم مسارك المهني بالحصول على خبرة تخصصية مطلوبة.
- اكتساب ثقة أكبر في التعامل مع الأنظمة المعقدة.
- تحسين جودة التقارير الأمنية واتخاذ القرارات.
- بناء أساس قوي لمتابعة المزيد من الشهادات المتقدمة.

الخاتمة

يمثل مجال الهاكر الأخلاقي أحد الأعمدة الأساسية لحماية الأنظمة في العصر الرقمي، حيث يوفر منهجًا متخصصًا يساعد على تحليل المخاطر والتعامل معها بطرق منهجية. وتُعد القدرة على تقييم الأنظمة، فهم نقاط الضعف، وتطبيق استراتيجيات الحماية المتقدمة عناصر أساسية لضمان أمن المعلومات واستمرارية الأعمال. ومن خلال هذه الدورة، يحصل المشاركون على محتوى شامل يجمع بين المعرفة العميقة والتطبيق العملي، مما يساعدهم على تطوير قدراتهم الأمنية وتعزيز جاهزيتهم للتعامل مع التهديدات المستقبلية.

إن اكتساب مهارات الهاكر الأخلاقي ليس مجرد تعلم لمجموعة من الأدوات أو التقنيات، بل هو تطوير لطريقة تفكير تعتمد على التحليل، الحذر، والانتباه للتفاصيل. وتساهم هذه الدورة في ترسيخ هذا النهج، من خلال توفير بيئة تعليمية تساعد المتدرب على فهم أساليب الهجوم والدفاع، وتمنحه القدرة على اتخاذ قرارات مدروسة في المواقف الحرجة. ومع تزايد أهمية الأمن الرقمي، توفر الدورة فرصة ثمينة للوصول إلى مستوى احترافي يمكن الاعتماد عليه في تعزيز حماية الأنظمة وتحسين الأداء المؤسسي.

