دورة معتمدة في القرصنة الأخلاقية واختبار الاختراق المتقدم

1 – 5 مارس 2027

دبي

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

دورة معتمدة في القرصنة الأخلاقية واختبار الاختراق المتقدم

المرجع: 32632_103600311 **التاريخ:** 1 – 5 مارس 2027 **المكان:** دبي **الرسوم:** Euro 6500

نظرة عامة على الدورة التدريبية

في المشهد الرقمي اليوم، تواجه المؤسسات تهديدات سيبرانية متزايدة يمكن أن تعرض البيانات الحساسة والأنظمة الحيوية للخطر. تعد القرصنة الأخلاقية واختبار الاختراق من استراتيجيات الأمن السيبراني الأساسية لتحديد الثغرات الأمنية وتخفيفها قبل أن يتمكن المخترقون الخبيثون من استغلالها. تم تصميم هذا التدريب في مجال الأمن السيبراني للمحترفين الذين يسعون للحصول على شهادة الهاكر الأخلاقي المعتمد وخبرة عملية في أمن الشبكات، واختبار أمن الويب، وتحليل التهديدات السيبرانية.

خلال هذا التدريب للحصول على شهادة القرصنة الأخلاقية، سيتقن المشاركون أحدث المنهجيات، بما في ذلك اختبار الاختراق وفقًا لمنهجية OSSTMM، وتقييم الأمان وفقًا لمعيار PTES، وتقنيات القرصنة باستخدام Kali Linux. تغطي الدورة أيضًا التدريب على اختبار الاختراق في الأمن السيبراني، واختبار أمن تطبيقات الويب، وتقييم ثغرات الشبكة، مما يجعلها واحدة من أفضل دورات القرصنة الأخلاقية عبر الإنترنت.

بحلول نهاية هذا البرنامج، سيتمكن المشاركون من إجراء اختبار الاختراق، ومحاكاة الهجمات الواقعية، وتطبيق الإجراءات الأمنية المضادة.

الجمهور المستهدف

- محترفو الأمن السيبراني
- مديرو أمن تكنولوجيا المعلومات
- مسؤولو الشبكات ومهندسو النظم
- مطوروالبرمجيات ومختبرو أمن الويب
- الهاكرز الأخلاقيون ومستشارو الأمن
- مسؤولو المخاطر والامتثال
- مسؤولو إنفاذ القانون وخبراء الأدلة الجنائية الرقمية

AGILE LEADERS
Training Center

الإدارات التنظيمية المستهدفة

- فرق الأمن السيبراني وأمن تكنولوجيا المعلومات
- إدارات المخاطر والامتثال
- فرق تطوير البرمجيات
- وحدات التدقيق والحوكمة
- فرق الاستجابة للحوادث والأدلة الجنائية الرقمية

القطاعات المستهدفة

- القطاع المالي والمصرفي
- الرعاية الصحية والصناعات الدوائية
- القطاع الحكومي والدفاعي
- التجارة الإلكترونية وتجارة التجزئة
- الاتصالات
- التكنولوجيا وتطوير البرمجيات

مخرجات الدورة التدريبية

عند إكمال دورة اختبار الاختراق المتقدمة هذه، سيتمكن المشاركون من:

- إجراء تقييمات القرصنة الأخلاقية باستخدام أدوات القرصنة في Kali Linux
- تنفيذ اختبار الاختراق وفقًا لمعايير تقييم الأمان OSSTMM و PTES
- تحديد واستغلال الثغرات الأمنية في اختبار أمن الويب
- تعلم تقنيات اختبار الاختراق الواقعية لتحليل التهديدات السيبرانية
- تطبيق تقييم ثغرات الشبكة وتحليل خروقات أمن تكنولوجيا المعلومات
- فهم كيفية إجراء اختبار الاختراق وتحليل النتائج بفعالية
- التحضير لامتحان الهاكر الأخلاقي المعتمد من خلال التدريب العملي

منهجية التدريب

تتبع هذه الدورة نهجًا عمليًا وتطبيقيًا لضمان اكتساب المشاركين خبرة واقعية. تشمل منهجيات التدريب ما يلي:

- محاضرات تفاعلية ودراسات حالة تغطي أطر عمل الأمن السيبراني ومنهجيات القرصنة
- عروض قرصنة حية باستخدام أدوات القرصنة في Kali Linux للمختبرات العملية للقرصنة الأخلاقية
- مختبرات عملية لاختبار الاختراق لإجراء تدريبات على اختبار الاختراق في الأمن السيبراني
- هجمات سيبرانية محاكاة تحاكي التهديدات السيبرانية الواقعية في بيئة خاضعة للرقابة

أدوات الدورة التدريبية

- كتب إلكترونية ومواد قراءة في الأمن السيبراني
- أدوات القرصنة في Kali Linux وأطر عمل اختبار الاختراق
- موارد معسكرات التدريب المكثفة للأمن السيبراني عبر الإنترنت
- مجموعات أدوات اختبار أمن تطبيقات الويب
- برامج فحص أمن الشبكات وتقييم الثغرات
- قوالب لتقارير تقييم مخاطر الأمن السيبراني
- قوائم تحقق لتنفيذ اختبار الاختراق

جدول أعمال الدورة التدريبية

اليوم الأول: أسس القرصنة الأخلاقية واختبار الاختراق

- **الموضوع 1:** مقدمة في القرصنة الأخلاقية ومبادئ الأمن السيبراني
- **الموضوع 2:** منهجيات وأطر عمل اختبار الاختراق OSSTMM و PTES
- **الموضوع 3:** أساسيات أمن الشبكات وتقنيات الاستطلاع
- **الموضوع 4:** أساسيات علم التشفير وتقنيات التشفير في الأمن السيبراني
- **الموضوع 5:** أساسيات Kali Linux وإعداد بيئة اختبار الاختراق
- **الموضوع 6:** الاعتبارات القانونية والأخلاقية في القرصنة الأخلاقية
- **تأمل ومراجعة:** النقاط الرئيسية المستفادة من أساسيات القرصنة الأخلاقية ومنهجيات اختبار الاختراق

AGILE LEADERS
Training Center

اليوم الثاني: جمع المعلومات وتقييم الثغرات

- **الموضوع 1:** الاستطلاع السلبي وذكاء المصادر المفتوحة OSINT
- **الموضوع 2:** الاستطلاع النشط وتقنيات فحص الشبكة
- **الموضوع 3:** تحديد ورسم خرائط الثغرات الأمنية في الشبكات والأنظمة
- **الموضوع 4:** اختبار أمن تطبيقات الويب والثغرات الشائعة
- **الموضوع 5:** نمذجة التهديدات السيبرانية واستراتيجيات تقييم المخاطر
- **الموضوع 6:** تطبيق إطار عمل اختبار الاختراق OSSTMM
- **تأمل ومراجعة:** تحليل تقنيات الاستطلاع وتقييم الثغرات

اليوم الثالث: الاستغلال واستراتيجيات الهجوم

- **الموضوع 1:** نمذجة التهديدات وتحليل سطح الهجوم
- **الموضوع 2:** التهرب من أنظمة كشف ومنع الاختراق
- **الموضوع 3:** تقنيات الاستغلال من جانب الخادم وتصعيد الامتيازات
- **الموضوع 4:** الهجمات من جانب العميل، والتصيد الاحتيالي، والهندسة الاجتماعية
- **الموضوع 5:** هجمات تطبيقات الويب، وحقن SQL، والبرمجة عبر المواقع XSS
- **الموضوع 6:** قرصنة الشبكات اللاسلكية واختبار اختراق شبكات WiFi الأخلاقي
- **تأمل ومراجعة:** مراجعة نتائج اختبار الاختراق واستراتيجيات الهجوم

اليوم الرابع: ما بعد الاستغلال، والحفاظ على الوصول، وإعداد التقارير

- **الموضوع 1:** إخفاء الآثار وإزالة مخلفات اختبار الاختراق
- **الموضوع 2:** إنشاء وصول دائم والحفاظ عليه
- **الموضوع 3:** تقنيات تصعيد الامتيازات والحركة الجانبية
- **الموضوع 4:** تقنيات نقل الملفات والتنقل عبر الأنظمة المخترقة
- **الموضوع 5:** إعداد تقارير اختبار الاختراق الاحترافية
- **الموضوع 6:** أفضل الممارسات لتخفيف الثغرات المكتشفة
- **تأمل ومراجعة:** إعداد تقارير اختبار الاختراق الفعالة وتخطيط المعالجة

اليوم الخامس: اختبار الاختراق العملي والتقييم النهائي

- **الموضوع 1:** تمارين ومختبرات عملية للقرصنة الأخلاقية ودراسات حالة
- **الموضوع 2:** تقنيات اختبار الاختراق الواقعية ومنهجيات القرصنة الأخلاقية
- **الموضوع 3:** تقييم مخاطر الأمن السيبراني وتطبيق السياسات الأمنية
- **الموضوع 4:** فهم متطلبات الشهادة وعملية الحصول على شهادة الهاكر الأخلاقي المعتمد
- **الموضوع 5:** التحضير لامتحان الهاكر الأخلاقي المعتمد وسيناريوهات تدريبية
- **الموضوع 6:** اتجاهات الصناعة والتطورات المستقبلية في القرصنة الأخلاقية
- **تأمل ومراجعة:** جلسة أسئلة وأجوبة نهائية، وموجز للمفاهيم الرئيسية، والخطوات التالية في مسار مهني في الأمن السيبراني

الأسئلة الشائعة

ما هي المؤهلات أو المتطلبات المسبقة المحددة اللازمة للمشاركين قبل التسجيل في الدورة؟

يُوصى بمعرفة أساسية بأمن الشبكات وأنظمة التشغيل والتدريب على أمن تكنولوجيا المعلومات. وتُعد الخبرة في القرصنة باستخدام Kali Linux أو التعرض المسبق لأساسيات القرصنة الأخلاقية أمرًا مفيدًا.

كم تبلغ مدة الجلسة اليومية، وهل هناك عدد إجمالي من الساعات المطلوبة للدورة بأكملها؟

تستمر كل جلسة يومية من 4 إلى 5 ساعات، بإجمالي 20-25 ساعة على مدى خمسة أيام، بما في ذلك المختبرات العملية والمناقشات.

ما هي الأدوات التي سيتم توفيرها لمختبرات اختبار الاختراق؟

على الرغم من عدم توفير أي برامج بشكل مباشر، سيتم توجيه المشاركين حول كيفية استخدام أدوات القرصنة في Kali Linux، وأطر عمل اختبار الاختراق OSSTMM، وأدوات اختبار أمن تطبيقات الويب.

كيف تختلف هذه الدورة عن دورات القرصنة الأخلاقية الأخرى

تتميز هذه الدورة بنهجها القائم على اختبار الاختراق في العالم الحقيقي، حيث تركز على المختبرات العملية للقرصنة الأخلاقية وأطر العمل المعترف بها في الصناعة مثل OSSTMM وتقييم الأمان PTES. على عكس العديد من أفضل دورات القرصنة الأخلاقية عبر الإنترنت، يقدم هذا التدريب محاكاة تفاعلية للهجمات السيبرانية، وتحليلاً معمقًا للثغرات الأمنية، والتحضير لامتحان الهاكر الأخلاقي المعتمد.

بحلول نهاية هذا البرنامج، لن يتعلم المشاركون القرصنة الأخلاقية عبر الإنترنت فحسب، بل سيطورون أيضًا المهارات العملية اللازمة للدفاع ضد التهديدات السيبرانية. هذا هو أفضل تدريب للحصول على شهادة الهاكر الأخلاقي المعتمد للمحترفين الذين يتطلعون إلى التقدم في التدريب على اختبار الاختراق في الأمن السيبراني وتحليل خروقات أمن تكنولوجيا المعلومات.