

دورة الاختراق الأخلاقي المتقدم واختبار الاختراق

AGILE LEADERS
Training Center

3 – 7 أكتوبر 2027

عمان

AGILE LEADERS
Training Center

دورة الاختراق الأخلاقي المتقدم واختبار الاختراق

المرجع: 99510_103600311 **التاريخ:** 3 – 7 أكتوبر 2027 **المكان:** عمان **الرسوم:** Euro 6000

نظرة عامة

تواجه المنشآت تهديدات رقمية متواصلة تستهدف البنية التحتية المؤسسية والبيانات الحساسة ومنصات الويب. تمكن ممارسات الاختراق الأخلاقي واختبار الاختراق فرق الأمان من اكتشاف نقاط الضعف التقنية وتحليلها ومعالجتها قبل استغلالها من جهات غير مصرح لها. يهدف هذا البرنامج إلى بناء الكفاءات المهنية في تقييم ثغرات الشبكات، وإجراء اختبار أمان تطبيقات الويب، وضبط تدفق عمليات اختبار الاختراق، وتنفيذ تحليل مساحات الهجوم. يتدرب المشاركون على تحليل الموقف الدفاعي باستخدام أدوات Kali Linux، ومنهجية OSSTMM، ومعيار PTES لتنفيذ اختبارات الاختراق. تقدم هذه الدورة بواسطة أجايل للتدريب.

الفئة المستهدفة

- محللو الأمن السيبراني ومهندسو الأنظمة المسؤولون عن التقييم التقني للثغرات.
- مدراء أمن تقنية المعلومات المشرفون على البنى الدفاعية للمؤسسات والمراجعات التدقيقية.
- مسؤولو الشبكات ومهندسو النظم المكلفون بتحصين البنية التحتية ومحيط الشبكة.
- مطورو البرمجيات ومختبرو تطبيقات الويب الساعون إلى تقنيات فحص الشيفرات البرمجية الآمنة.
- مستشارو ومدققو أمن المعلومات القائمون على تنفيذ تقييمات الاختراق المنهجية.

الإدارات والقطاعات المستهدفة

تناسب هذه الدورة الفرق التقنية المسؤولة عن إدارة الثغرات، والدفاع عن البنية التحتية، وتدقيق الأنظمة عبر مختلف القطاعات المعتمدة على التكنولوجيا.

- فرق الأمن السيبراني وعمليات أمن تقنية المعلومات
- وحدات إدارة المخاطر والامتثال وحوكمة المعلومات
- مجموعات هندسة البرمجيات وأمان التطبيقات
- أقسام البنية التحتية للأنظمة وهندسة الشبكات
- قطاع المصارف والخدمات المالية والتأمين
- قطاعات الرعاية الصحية والاتصالات ومؤسسات التكنولوجيا

AGILE LEADERS
Training Center

أهداف التعلم

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- تنفيذ تدفق عمليات اختبار الاختراق المنظم المتوافق مع معايير OSSTMM و PTES.
- استخدام أدوات Kali Linux الأمنية لاكتشاف الأجهزة النشطة والخدمات العاملة وثغرات المحيط.
- اكتشاف ثغرات تطبيقات الويب الشائعة واستغلالها بما في ذلك هجمات حقن SQL والبرمجة عبر المواقع XSS.
- تنفيذ نمذجة التهديدات وإجراء تحليل مساحات الهجوم عبر طبقات بنيات الشبكات المؤسسية.
- تطبيق أساليب تصعيد الصلاحيات والتحرك الجانبي داخل بيئات معملية مضبوطة ومحكمة.
- إعداد تقارير اختبار الاختراق المهنية وتوثيق خطط المعالجة القابلة للتنفيذ.

جدول الدورة

اليوم 1: الأسس ومنهجيات التقييم

- مبادئ الأمن السيبراني وتحديد نطاق اختبار الاختراق
- مواءمة أطر العمل الأمنية وفق معايير OSSTMM و PTES
- أساسيات أمان الشبكات واستطلاع الأجهزة المضيفة
- المكونات التشفيرية الأساسية والتحقق من النقل الآمن
- تهيئة بيئة Kali Linux وإعداد حزمة الأدوات التقنية
- الأطر القانونية وقواعد الاشتباك ونطاقات التفويض

اليوم 2: الاستطلاع وتحديد الثغرات

- جمع المعلومات غير المباشر عبر مصادر الاستخبارات مفتوحة المصدر
- تقنيات الفحص النشط للشبكات واستكشاف المنافذ
- تقييم ثغرات الشبكات واكتشاف نقاط ضعف الخدمات
- رسم مساحات الهجوم على تطبيقات الويب واكتشاف المتغيرات البرمجية
- بروتوكولات نمذجة التهديدات ومصفوفات تحديد أولويات المخاطر
- مقاييس الأمان التشغيلي والتدقيق المرجعي وفق معيار OSSTMM

اليوم 3: الاستغلال واختراق الأنظمة

- اختيار مسارات الهجوم وأساليب تجاوز دفاعات المحيط
- تنفيذ هجمات خوادم الأنظمة وتحليل التنفيذ البرمجي عن بعد
- استغلال أجهزة المستخدمين وهجمات الصيد الموجه واختبار الهندسة الاجتماعية
- استغلال ثغرات الويب: حقن SQL وهجمات البرمجة عبر المواقع XSS
- تدقيق الشبكات اللاسلكية وتقييم تشفير اتصالات WiFi
- التحقق من قابلية الاستغلال وبناء أدلة الإثبات المضبوطة

اليوم 4: ما بعد الاستغلال وخطط المعالجة

- تثبيت نقاط الوجود وترسيخ الوصول بعد الاختراق
- تصعيد الصلاحيات والتحرك الجانبي في بيئات Windows و Linux
- منهجيات التوجيه الداخلي والانتقال عبر الشبكات
- إدارة الآثار الرقمية وإزالة بقايا ومخلفات الاختبار
- تطبيق الإجراءات الدفاعية المضادة واستراتيجيات إدارة التحديثات
- كتابة التقارير الفنية لاختبار الاختراق وتقديم الإيجاز التنفيذي

اليوم 5: التمارين التطبيقية وأطر الأمان

- تنفيذ سيناريوهات مختبرات اختبار الاختراق متعددة المراحل
- محاكاة الهجمات المؤسسية وتحليل مسارات الاستهداف الفعلية
- دمج تقييم المخاطر وتطوير السياسات التقنية
- معايير الشهادات الأمنية ومراجعة مجالات المعرفة التخصصية
- مسارات الهجوم الناشئة والاعتبارات السحابية والاتجاهات الدفاعية
- مراجعة نتائج التقييم وجلسة الأسئلة التقنية وخطط المعالجة

التمارين التطبيقية

ينفذ المشاركون أنشطة تطبيقية لمعالجة التحديات التشغيلية وبناء خطط التنفيذ الفنية.

- نشاط مقترح: تهيئة واستخدام أدوات Kali Linux لرسم خريطة الأجهزة النشطة والمنافذ المفتوحة عبر الشبكة الفرعية.
- نشاط مقترح: تنفيذ اختبار تطبيقي لمحاكاة هجوم على تطبيق ويب لتحديد ثغرات حقن SQL وطرق معالجتها.
- نشاط مقترح: تطبيق أساليب تصعيد الصلاحيات على جهاز تدريبي بالاعتماد على أخطاء التكوين والأذونات غير المحمية.
- نشاط مقترح: إعداد مسودة تقرير تنفيذي لنتائج اختبار الاختراق مع تقييم درجات المخاطر وجداول المعالجة الزمنية.

الأسئلة الشائعة

ما المؤهلات المحددة أو المتطلبات المسبقة المطلوبة من المشاركين قبل التسجيل في الدورة؟

يتطلب من المشاركين الإلمام بأساسيات بروتوكولات الشبكات، وأوامر أنظمة التشغيل، والمفاهيم الجوهرية لأمن المعلومات، وتعتبر الخبرة العملية في التعامل مع سطر أوامر Linux ميزة إضافية مفيدة.

ما مدة الجلسة التدريبية في كل يوم، وما إجمالي الساعات المطلوبة للدورة كاملة؟

تستمر جلسة التدريب اليومية لنحو 4 إلى 5 ساعات، بإجمالي يتراوح بين 20 و 25 ساعة تدريبية وتطبيقية على مدار الأيام الخمسة للدورة.

ما الأدوات التي سيتم توفيرها لمختبرات اختبار الاختراق؟

تركز التمارين على توجيه المشاركين لاستخدام الأدوات الأمنية مفتوحة المصدر وحزم التوزيعات القياسية، مع التركيز على أدوات Kali Linux، وخوادم الوكيل لفحص تطبيقات الويب، وقوائم التقييم المتوافقة مع معيار OSSTMM.

الخاتمة

يكتسب المشاركون بنهاية هذا البرنامج مهارات عملية ومنهجية في اكتشاف الثغرات الأمنية والتحقق منها وتوثيقها عبر بيئات الشبكات وتطبيقات الويب. ويسهم تطبيق معايير OSSTMM و PTES في رفع الجاهزية الدفاعية للمؤسسات والحد من التعرض للمخاطر التقنية وحماية الأصول الحيوية من التهديدات السيبرانية المتجددة.