الدورة التدريبية: اختبار الاختراق الأخلاقي - المهارات المتقدمة للمحترفين



14 - 18 ديسمبر 2026
بوسطن
7500 € (للشخص الواحد)
Ref: #CYB8974_326796

مقدمة الدورة التدريبية / لمحة عامة:

يُعد اختبار الاختراق الأخلاقي حجر الزاوية في أمن الشبكات وحماية الأنظمة من التهديدات السيبرانية المتطورة. هذه الدورة التدريبية المتقدمة مصممة خصيصًا للمحترفين الذين يسعون إلى صقل مهاراتهم في الأمن السيبراني واكتساب خبرة عملية في اكتشاف الثغرات الأمنية واستغلالها بطرق أخلاقية لتحسين دفاعات الشركات. سنتناول في هذه الدورة تقنيات اختبار الاختراق المتقدمة، تحليل الثغرات، والتعامل مع الهجمات المعقدة. سيكتسب المشاركون القدرة على التفكير كمخترق أخلاقي، مما يمكنهم من تحديد نقاط الضعف قبل أن يستغلها المهاجمون الخبثاء. سنغطي أدوات ومنهجيات مثل اختبار الاختراق للشبكات اللاسلكية، اختبار اختراق تطبيقات الويب، والهندسة العكسية للبرمجيات الخبيثة. تهدف الدورة إلى إعداد المشاركين لمواجهة التحديات الأمنية المعاصرة وبناء أنظمة أمنية قوية. يستند المحتوى إلى أحدث الأبحاث والمعايير الدولية في مجال الأمن الهجومي والدفاعي، مع الاستفادة من إسهامات أكاديميين وخبراء بارزين مثل البروفيسور مات بيشوب (Matt Bishop)، مؤلف العديد من الكتب المرجعية في أمن الكمبيوتر. يقدم BIG BEN Training Center هذه الدورة لتمكين المتخصصين من أن يصبحوا روادًا في مجال الأمن السيبراني الهجومي.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- متخصصو الأمن السيبراني ذوو الخبرة.
- مهندسي الاختراق ومحللو الثغرات.
- مهندسو أمن الشبكات والأنظمة.
- محللو البرمجيات الخبيثة.
- المستشارون الأمنيون.
- أي مهندس أو مطور برمجيات مهتم بأمن التطبيقات والأنظمة.

القطاعات والصناعات المستهدفة:

- قطاع تكنولوجيا المعلومات والاتصالات.
- القطاع المالي والمصرفي لاختبار اختراق الأنظمة المالية.
- القطاع الحكومي والهيئات العامة وما في حكمها لأمن البنية التحتية الحرجة.
- شركات تطوير البرمجيات والتطبيقات.
- شركات الأمن السيبراني وخدمات الاستشارات الأمنية.
- الرعاية الصحية لحماية بيانات المرضى.

الأقسام المؤسسية المستهدفة:

- فريق الأمن السيبراني.
- إدارة تقنية المعلومات.
- قسم تطوير البرمجيات والأنظمة.
- إدارة المخاطر والامتثال.
- فرق عمليات الأمن (SecOps).

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم المنهجيات المتقدمة لاختبار الاختراق.
- القدرة على تحديد الثغرات الأمنية في الشبكات والتطبيقات والأنظمة.
- تطبيق تقنيات الاستغلال المتقدمة بأسلوب أخلاقي.
- إجراء اختبار اختراق شامل لتطبيقات الويب والشبكات.
- تحليل البرمجيات الخبيثة والهندسة العكسية.
- إعداد تقارير اختبار اختراق مفصلة وتوصيات أمنية.
- فهم الجوانب القانونية والأخلاقية لاختبار الاختراق.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية مكثفة وعملية للغاية، تركز على التطبيق العملي لتقنيات اختبار الاختراق الأخلاقي. سيتمكن المشاركون من خلال ورش عمل عملية ومعامل افتراضية من محاكاة سيناريوهات اختراق حقيقية. تتضمن المنهجية تدريبات مكثفة على أدوات اختبار الاختراق، مثل Metasploit Nmap Burp Suite. سيتم تحليل دراسات حالة متقدمة للهجمات السيبرانية المعقدة، وكيفية اكتشاف الثغرات واستغلالها بشكل أخلاقي. يتم تشجيع المشاركة النشطة في تحديات القرصنة الأخلاقية لتعزيز المهارات العملية. يلتزم BIG BEN Training Center بتقديم بيئة تعليمية محفزة، تمكن المتدربين من تطوير قدراتهم في الأمن الهجومي والدفاعي. سيتم توفير تغذية راجعة فردية لضمان فهم عميق لكل مفهوم وتطبيق فعال للتقنيات المكتسبة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات اختبار الاختراق ومنهجياته المتقدمة

- مقدمة إلى اختبار الاختراق الأخلاقي.
- مراحل اختبار الاختراق: الاستطلاع، المسح، التعداد.
- أنواع اختبار الاختراق: الشبكات، الويب، الأجهزة المحمولة.
- التخطيط لاختبار الاختراق ووضع النطاق.
- التحضير للعمليات الهجومية.
- الأدوات المستخدمة في الاستطلاع.
- الامتثال للمعايير الأخلاقية.

الوحدة الثانية: اكتشاف الثغرات الأمنية وتحليلها

- تقنيات اكتشاف الثغرات الآلية واليدوية.
- تحليل نقاط الضعف في الشبكات.
- تقييم الثغرات في تطبيقات الويب (OWASP Top 10).
- فحص الخوادم وقواعد البيانات بحثًا عن الثغرات.
- اختبار اختراق الأنظمة المستندة إلى السحابة.
- تحليل الشفرة المصدرية للثغرات.
- إدارة الثغرات الأمنية.

الوحدة الثالثة: تقنيات الاستغلال المتقدمة

- هجمات تجاوز المصادقة.
- حقن SQL والبرمجة عبر المواقع (XSS).
- استغلال الثغرات في البروتوكولات الشبكية.
- اختراق أنظمة التشغيل (Linuxg Windows).
- هجمات التصعيد الامتيازي.
- تجاوز أنظمة الكشف عن التسلل (IDS/IPS).
- استخدام أطر عمل الاستغلال.

الوحدة الرابعة: اختبار اختراق الشبكات اللاسلكية وتطبيقات الويب

- أساسيات أمن الشبكات اللاسلكية.
- اختبار اختراق شبكات Wi-Fi (WEP, WPA/WPA2).
- هجمات رفض الخدمة على الشبكات اللاسلكية.
- تقنيات اختبار اختراق تطبيقات الويب المتقدمة.
- أتمتة اختبار اختراق الويب.
- استغلال ثغرات Logic Flaws في تطبيقات الويب.
- حماية تطبيقات الويب.

الوحدة الخامسة: الهندسة العكسية وتقارير الاختراق

- مقدمة إلى الهندسة العكسية للبرمجيات.
- تحليل البرمجيات الخبيثة (Malware Analysis).
- أدوات الهندسة العكسية.
- كتابة تقارير اختبار الاختراق الاحترافية.
- التوصيات الأمنية وخطط المعالجة.
- التعامل مع العملاء بعد الاختبار.
- التطور المستمر في مجال اختبار الاختراق.

الأسئلة المتكررة:

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

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.

سؤال للتأمل:

في ظل المشهد السيبراني المتغير باستمرار، حيث تظهر تهديدات جديدة كل يوم، كيف يمكن للمخترق الأخلاقي أن يظل في طليعة هذا التطور، ليس فقط باكتشاف الثغرات الحالية، ولكن بتوقع نقاط الضعف المستقبلية وبناء أنظمة دفاعية استباقية؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها العميق والمتقدم على المهارات العملية لاختبار الاختراق الأخلاقي، مما يميزها عن الدورات التي تكتفي بالمفاهيم الأساسية. نحن نقدم محتوى تفاعليًا ومكثفًا يغطي تقنيات الاستغلال المعقدة وتحليل الثغرات الأمنية على مستوى احترافي. بدلاً من مجرد عرض الأدوات، نركز على كيفية استخدام هذه الأدوات بذكاء وتطبيق منهجيات التفكير النقدي لحل المشكلات الأمنية. تتضمن الدورة تحديات عملية مكثفة تُحاكي بيئات حقيقية، مما يمنح المشاركين خبرة عملية لا تقدر بثمن. هذه الدورة ليست مجرد تعلم للتقنيات، بل هي بناء لعقلية المخترق الأخلاقي الذي يستطيع ليس فقط اكتشاف نقاط الضعف، بل فهم كيفية تأمين الأنظمة بشكل شامل وفعال.