الدورة التدريبية: اختبار الاختراق الأخلاقي - المهارات المتقدمة للمحترفين

مايو - ٠٤ يونيو ٢٠٢٦ ٣١

اسطنبول

(للشخص الواحد) € ٤٥٠٠

Ref: #CYB8974_58626

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

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

القطاعات والصناعات المستهدفة:

- قطاع تكنولوجيا المعلومات والاتصالات.
- المالية. القطاع المالي والمصرفي لاختبار اختراق الأنظمة
- البنية التحتية الحرجة. القطاع الحكومي والهيئات العامة وما في حكمها لأمن
- 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:

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

- فهم المنهجيات المتقدمة لاختبار الاختراق.
- والتطبيقات والأنظمة. القدرة على تحديد الثغرات الأمنية في الشبكات
- 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.
- الاختراق. فهم الجوانب القانونية والأخلاقية لاختبار

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

المتقدمة الوحدة الأولى: أساسيات اختبار الاختراق ومنهجياته

- مقدمة إلى اختبار الاختراق الأخلاقي.
- مراحل اختبار الاختراق: الاستطلاع، المسح، التعداد.
- المحمولة. أنواع اختبار الاختراق: الشبكات، الويب، الأجهزة
- 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 ١٠).
- 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 (Windows و Linux).
- هجمات التصعيد الامتيازي.
- تجاوز أنظمة الكشف عن التسلل (IDS/IPS).
- استخدام أطر عمل الاستغلال.

وتطبيقات الويب الوحدة الرابعة: اختبار اختراق الشبكات اللاسلكية

- أساسيات أمن الشبكات اللاسلكية.
- اختبار اختراق شبكات Wi-Fi (WEP, WPA/WPA٢).
- 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:

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

لا توجد شروط مسبقة.

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

المدة إلى ٢٠-٢٥ بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام،

ساعة تدريبية. راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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