الدورة التدريبية: أمن الشبكات اللاسلكية والواي فاي: تهديدات، دفاعات، وأفضل الممارسات

#NO2515

الدورة التدريبية: أمن الشبكات اللاسلكية والواي فاي: تهديدات، دفاعات، وأفضل الممارسات

مقدمة الدورة التدريبية / لمحة عامة:

أصبح أمن الشبكات اللاسلكية والواي فاي تحديًا حاسمًا في عالمنا المتصل، حيث تتزايد التهديدات السيبرانية باستمرار، مما يتطلب فهمًا عميقًا لنقاط الضعف وطرق الحماية. تقدم هذه الدورة التدريبية الشاملة منهجًا متعمقًا في تهديدات أمن الشبكات اللاسلكية، تقنيات الدفاع ضد الاختراقات، وتطبيق أفضل ممارسات الأمن في بيئات الواي فاي المتنوعة، بدءًا من أساسيات التشفير اللاسلكي وصولًا إلى التطبيقات المتقدمة في تأمين الشبكات المعقدة. يركز التدريب على تزويد المشاركين بالمهارات العملية والنظرية اللازمة لتحديد المخاطر الأمنية، تطبيق الإجراءات الوقائية، والاستجابة للحوادث الأمنية اللاسلكية. يستعرض BIG BEN Training Center هذه المفاهيم بعمق، مستنيرًا بأعمال رواد المجال مثل البروفيسور ويليام ستالينغز (William Stallings)، الذي تُعد كتبه مراجع أساسية في مجال أمن الشبكات والشبكات اللاسلكية، مما يضمن تقديم محتوى أكاديمي وعملي رفيع المستوى. ستُمكن الدورة المتدربين من فهم كيفية تكوين شبكات الواي فاي الآمنة، حماية البيانات عبر الهواء، واستكشاف نقاط الضعف في بيئات الاتصال اللاسلكي، مما يؤهلهم لأن يكونوا خبراء في التعامل مع تحديات أمن الفضاء السيبراني اللاسلكي.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسي أمن الشبكات.
- مسؤولي تكنولوجيا المعلومات.
- خبراء الأمن السيبراني.
- مديري الشبكات.
- المتخصصين في البنية التحتية.
- مدققي الأمن.
- أي شخص مسؤول عن أمن الشبكات اللاسلكية في مؤسسته.

القطاعات والصناعات المستهدفة:

- تكنولوجيا المعلومات والاتصالات.
- القطاع المصرفي والمالي.
- الجهات الحكومية والدفاع.
- قطاع الرعاية الصحية.
- التصنيع والخدمات اللوجستية.
- التعليم والبحث العلمي.
- شركات استشارات الأمن السيبراني.

الأقسام المؤسسية المستهدفة:

- قسم الأمن السيبراني.
- إدارة تكنولوجيا المعلومات.
- قسم الشبكات.
- إدارة المخاطر.
- قسم التدقيق الداخلي.
- إدارة البنية التحتية.
- قسم الامتثال.

أهداف الدورة التدريبية:

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

- فهم معمق لتهديدات أمن الشبكات اللاسلكية ونقاط الضعف.
- تصميم وتنفيذ شبكات واي فاي آمنة.
- تطبيق بروتوكولات التشفير والمصادقة اللاسلكية (WPA3, 802.1X).
- حماية الشبكات اللاسلكية من الهجمات الشائعة.
- إدارة أجهزة الأمن اللاسلكي (Wireless Intrusion Detection/Prevention Systems).
- الاستجابة للحوادث الأمنية اللاسلكية.
- إجراء تقييمات الضعف واختبارات الاختراق للشبكات اللاسلكية.
- تطبيق أفضل ممارسات الأمن للشبكات اللاسلكية.
- تكوين جدران الحماية اللاسلكية.
- ضمان امتثال الشبكة اللاسلكية للمعايير الأمنية.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية عملية وتطبيقية مكثفة، مصممة لتمكين المشاركين من اكتساب خبرة مباشرة في أمن الشبكات اللاسلكية والواي فاي. تشمل الدورة مزيجًا من المحاضرات النظرية المتعمقة، وورش العمل العملية التي تركز على تطبيقات الأمن اللاسلكي في بيئات الأعمال الحقيقية. سيقوم المشاركون بتطبيق المفاهيم المكتسبة من خلال تمارين تكوين الشبكات اللاسلكية الآمنة، محاكاة الهجمات اللاسلكية، واستخدام أدوات تحليل الأمن اللاسلكي في بيئة معملية افتراضية. يتم تشجيع العمل الجماعي والمناقشات التفاعلية لتبادل الخبرات وحلول المشكلات. يقدم المدربون في BIG BEN Training Center، وهم خبراء في مجال أمن الشبكات والشبكات اللاسلكية، تغذية راجعة فورية ودقيقة لضمان فهم عميق للمفاهيم وتطوير المهارات. تهدف المنهجية إلى إعداد المتدربين ليصبحوا قادرين على تأمين شبكاتهم اللاسلكية بفعالية واحترافية عالية، مما يحمي مؤسساتهم من المخاطر السيبرانية المتزايدة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الشبكات اللاسلكية وتهديداتها

- مراجعة لأساسيات تقنيات الواي فاي (802.11).
- مكونات الشبكة اللاسلكية وأنواعها.
- نقاط الضعف الشائعة في الشبكات اللاسلكية.
- أنواع الهجمات اللاسلكية (DE authentication, Evil Twin, WEP/WPA Cracking).
- المخاطر الأمنية المرتبطة بالشبكات اللاسلكية.
- أهمية أمن الواي فاي للمؤسسات.
- نظرة عامة على البروتوكولات الأمنية اللاسلكية.

الوحدة الثانية: بروتوكولات الأمن اللاسلكي والتشفير

- بروتوكولات التشفير اللاسلكي (WPA2, WPA3).
- المصادقة الشبكية (X802.1) وخوادم RADIUS.
- إدارة مفاتيح التشفير اللاسلكية.
- تكوين الشبكات اللاسلكية الآمنة على نقاط الوصول.
- فصل الشبكات اللاسلكية (VLANs) لأغراض الأمن.
- تطبيق سياسات كلمة المرور القوية.
- استخدام الشهادات الرقمية في المصادقة اللاسلكية.

الوحدة الثالثة: دفاعات الشبكات اللاسلكية المتقدمة

- أنظمة كشف ومنع التسلل اللاسلكي (WIDS/WIPS).
- جدران الحماية اللاسلكية المتقدمة.
- الشبكات الافتراضية الخاصة (VPN) عبر Wi-Fi.
- أمن الأجهزة الطرفية المتصلة بالشبكة اللاسلكية.
- مراقبة حركة المرور اللاسلكية للنشاط المشبوه.
- تقنيات حماية Wi-Fi Protected Setup (WPS).
- إدارة الثغرات الأمنية في أجهزة الواي فاي.

الوحدة الرابعة: إدارة أمن الشبكات اللاسلكية والاستجابة للحوادث

- أدوات إدارة أمن الشبكات اللاسلكية.
- مراجعة سجلات الأمن اللاسلكي وتحليلها.
- إجراء تقييمات الضعف واختبارات الاختراق اللاسلكية.
- وضع خطط الاستجابة للحوادث الأمنية اللاسلكية.
- إجراء التدريبات الأمنية للموظفين.
- تطبيق التحديثات الأمنية الدورية لأجهزة الواي فاي.
- الامتثال للمعايير الأمنية للشبكات اللاسلكية.

الوحدة الخامسة: تقنيات الواي فاي الناشئة والمستقبل الأمني

- أمن Wi-Fi 6 (802.11ax) و Wi-Fi 7 (802.11be).
- أمن شبكات G5 الخاصة (Private 5G).
- الإنترنت اللاسلكي للأشياء (IoT) وأمنه.
- الذكاء الاصطناعي في أمن الشبكات اللاسلكية.
- تقنيات المصادقة المتقدمة (Biometrics, Multi-factor Authentication).
- تحديات الأمن اللاسلكي في البيئات السحابية.
- مستقبل أمن الشبكات اللاسلكية وتطورها.

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 التطور المتسارع للتهديدات السيبرانية وازدياد اعتمادنا على الاتصال اللاسلكي في كل جانب من جوانب حياتنا، كيف يمكن للمتخصصين في أمن الشبكات تحقيق التوازن بين توفير الوصول السهل والمرونة للمستخدمين، وبين فرض أعلى مستويات الحماية والأمان للبيانات الحساسة عبر شبكات الواي فاي؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها الشامل على أمن الشبكات اللاسلكية والواي فاي من منظور متعمق وعملي، مما يجعلها مختلفة عن الدورات التي تقتصر على المفاهيم الأساسية. يقدم BIG BEN Training Center منهجًا فريدًا يجمع بين فهم التهديدات السيبرانية المتقدمة والتطبيق العملي المكثف لتقنيات الدفاع، مع التركيز على التحديات الأمنية الفريدة للبيئات اللاسلكية. ما يميز هذه الدورة هو التركيز على تأمين بروتوكولات الواي فاي الحديثة، حماية البيانات عبر الهواء، والاستجابة الفعالة للحوادث الأمنية اللاسلكية. يتم تزويد المشاركين بأدوات تحليل الأمن اللاسلكي والممارسات الصناعية الرائدة، مما يؤهلهم لتصميم، تأمين، وإدارة شبكات لاسلكية فعالة وموثوقة. هذه الدورة ليست مجرد تدريب، بل هي تجربة تعليمية تحويلية تهدف إلى بناء خبراء قادرين على حماية البنية التحتية اللاسلكية الحيوية، مما يجعلهم قيمة مضافة حقيقية لأي مؤسسة تسعى لتعزيز دفاعاتها السيبرانية.