مستقبلك بين يديك

أساسيات الأمن السيبراني

تقسيم للمفاهيم الأساسية في الأمن السيبراني التي يجب أن تركز عليها لتصبح محلل أمن سيبراني

فاضل يونس
أكادمية برمج

April 4, 2024

DISCLAIMER

إخلاء المسؤولية

الغرض:

المعلومات الواردة في دليل "خارطة طريق لتصبح محلل بيانات" هي لأغراض إعلامية وتعليمية عامة فقط. يتم توزيعها مجانًا ولا يجوز بيعها. وبينما نسعى جاهدين للحفاظ على تحديث المعلومات ودقتها ، فإننا لا نقدم أي إقرارات أو ضمانات من أي نوع ، صريحة أو ضمنية ، حول اكتمال أو دقة أو موثوقية أو ملاءمة أو توفر المعلومات الواردة في الدليل أو المعلومات أو المنتجات أو الخدمات أو الرسومات ذات الصلة الواردة في الدليل لأي غرض. وبالتالي ، فإن أي اعتماد تضعوه على مثل هذه المعلومات يكون على مسؤوليتك الخاصة تمامًا.

إخلاء مسؤولية:

يُقدم هذا الدليل كمورد مجاني ولا يُقصد به أن يكون بديلاً عن الاستشارة المهنية. قبل اتخاذ أي إجراءات بناءً على هذه المعلومات ، نشجعك على استشارة المهنيين المختصين. استخدام هذا الدليل يتم وفقًا لتقديرك الخاص وعلى مسؤوليتك.

حدود المسئولية:

في أي حال من الأحوال ، لن نتحمل مسؤولية عن أي خسارة أو ضرر ، بما في ذلك على سبيل المثال لا الحصر ، الخسارة غير المباشرة أو التبعية ، أو أي خسارة أو ضرر ناشئ عن فقدان البيانات أو الأرباح الناشئة عن أو فيما يتعلق باستخدام هذا الدليل.

روابط خارجية:

من خلال هذا الدليل ، قد تتمكن من الوصول إلى مواقع ويب أخرى خارج سيطرة أكاديمية برمج أو أعضائها. ليس لدينا سيطرة على طبيعة ومحتوى وتوفر تلك المواقع. إن تضمين أي روابط لا يعني بالضرورة التوصية أو تأييد الآراء الواردة فيها.

إخلاء مسؤولية عن الأعطال الفنية:

يتم بذل كل جهد لإبقاء الدليل محدثًا. ومع ذلك ، لا تتحمل أكاديمية برمج وأعضاؤها أي مسؤولية عن تعطل الدليل مؤقتًا بسبب مشكلات فنية خارجة عن سيطرتنا.

أكاديمية برمج

https://barmij.academy
@younes.fadill

TABLE OF CONTENTS

أساسيات الأمن السيبراني

الأمن السيبراني يعتبر بالغ الأهمية في عالم اليوم الرقمي. بينما تزداد اعتمادنا على الأنظمة المترابطة، تزداد أيضًا إمكانية حدوث هجمات سيبرانية يمكن أن تعطل البنية التحتية الحيوية، وتسرق البيانات الحساسة، وتسبب الفوضى المالية. بينما تحمل الذكاء الاصطناعي (AI) وعدًا بتعزيز الأمن السيبراني من خلال كشف التهديدات المتقدمة والدفاعات الآلية، إلا أنه سلاح ذو حدين. يمكن للفاعلين الخبيثين أيضًا استخدام الذكاء الاصطناعي لتطوير هجمات أكثر تعقيدًا، مما قد يضع الأمن السيبراني في سباق مستمر من الهجوم والدفاع ضد التهديدات المدعومة بالذكاء الاصطناعي المتطورة باستمرار.

تطوير مهارات الأمن السيبراني

الأساسيات:

أمن الشبكات: فهم كيفية عمل الشبكات، أنواع توبولوجيا الشبكة المختلفة، بروتوكولات الشبكة (TCP/IP)، والثغرات الشبكية الشائعة. تعلم عن أجهزة أمن الشبكات مثل جدران الحماية، أنظمة الكشف/الوقاية من التسلل (IDS/IPS)، وكيف تحمي محيط شبكتك.

فهم الشبكات: https://edge.edx.org/courses/course-v1:BU+EC441+2018_fall/about (مجاني)

أجهزة أمن الشبكات: https://www.fortinet.com/training/cybersecurity-professionals

إدارة النظام: اكتساب معرفة بأنظمة التشغيل (Windows, Linux, macOS)، إدارة المستخدمين، أنظمة التحكم في الوصول، وتقنيات تصليب النظام. هذا سيساعدك على فهم كيفية تكوين الأنظمة وتأمينها.

أنظمة التشغيل:

أساسيات Linux للمبتدئين على edX: https://www.edx.org/learn/linux/the-linux-foundation-introduction-to-linux (مجاني)

Windows Server: https://learn.microsoft.com/en-us/windows-server/ (تعلم ذاتي)

الجدران النارية: تعمل كخط دفاع أول، تصفية حركة المرور الواردة والصادرة بناءً على قواعد أمان محددة مسبقًا. فهم كيف تعمل الجدران النارية، أنواع الجدران النارية المختلفة (الحالية، غير الحالية)، وكيفية تكوينها بفعالية.

المواد التدريبية:

الجدران النارية: كيف تعمل ولماذا هي مهمة | بواسطة NetworkChuck: https://www.youtube.com/watch?v=tRhRnLWSn8U (فيديو)

أكاديمية Fortinet لأمن الشبكات - أساسيات الجدران النارية: https://training.fortinet.com/login/index.php (مجاني)

الكشف عن التسلل والوقاية منه: تعلم عن أنظمة الكشف عن التسلل (IDS) وأنظمة الوقاية من التسلل (IPS). تراقب IDS حركة الشبكة بحثًا عن النشاط المشبوه وترفع التنبيهات، بينما تقوم IPS بحظر حركة المرور الخبيثة بنشاط. فهم أنواع الهجمات المختلفة (البرمجيات الخبيثة، الاحتيال الإلكتروني، رفض الخدمة) وكيف يمكن لـ IDS/IPS المساعدة في منعها.

المواد التدريبية:

Security Onion: مراقبة أمن الشبكات مجانية ومفتوحة المصدر: https://securityonionsolutions.com/ (تعلم عملي بأداة أمان مجانية)

التشفير: هو فن حماية المعلومات من خلال التشفير وفك التشفير. استكشاف المفاهيم الأساسية للتشفير مثل التشفير المتماثل وغير المتماثل، خوارزميات الهاش، والتواقيع الرقمية. فهم التشفير ضروري لتأمين البيانات أثناء الراحة وأثناء النقل.

المواد التدريبية:

أكاديمية خان: علوم الحاسب - مقدمة في التشفير: https://www.khanacademy.org/computing/computer-science/cryptography (دروس فيديو مجانية)

احصل على شهادات الأمن السيبراني

تعد شهادات الأمن السيبراني بمثابة أوراق اعتماد قيمة تثبت معرفتك ومهاراتك في المجال للموظفين المحتملين. يمكن أن تعزز سيرتك الذاتية بشكل كبير، تزيد من إمكانية الكسب، وتفتح أبوابًا لفرص مهنية جديدة. إليك تقسيمًا لسبب أهمية الشهادات وبعض الخيارات الشعبية للمبتدئين التي يجب النظر فيها:

لماذا تسعى للحصول على شهادات الأمن السيبراني؟

التحقق من المعرفة: تؤكد الشهادات على فهمك للمفاهيم الأساسية للأمن السيبراني، الأدوات، وأفضل الممارسات. إنها تظهر لأرباب العمل أنك قد استثمرت الوقت والجهد في تطوير خبرتك في الأمن السيبراني.

زيادة المصداقية: الحصول على شهادة أمن سيبراني معترف بها يُظهر التزامك بالمجال ويميزك عن المرشحين الآخرين.

التقدم المهني: تتطلب العديد من الوظائف في مجال الأمن السيبراني أو تفضل بشدة المرشحين الحاصلين على شهادات محددة. يمكن للشهادات أن تساعدك في التأهل للوظائف ذات المستوى الأعلى والترقيات.

البقاء على اطلاع: يتطور مشهد الأمن السيبراني باستمرار. غالبًا ما تتطلب الشهادات التجديد، مما يشجعك على البقاء محدثًا مع أحدث التهديدات والتقنيات.

شهادات الأمن السيبراني الشعبية للمبتدئين:

• **CompTIA Security+:** هذه الشهادة المحايدة بالنسبة للموردين هي اعتماد أساسي لأي شخص يسعى لمهنة في الأمن السيبراني. تغطي مجموعة واسعة من المواضيع، بما في ذلك أمان الشبكات، إدارة النظام، التشفير، وضوابط الأمان. Security+ هي شهادة معترف بها عالميًا ونقطة انطلاق للعديد من مسارات الأمن السيبراني الأخرى.

<u>الموارد:</u>

صفحة شهادة CompTIA Security+: https://www.comptia.org/certifications/security

الدليل الرسمي لدراسة CompTIA Security+: https://www.amazon.com/CompTIA-Security-Study-Guide-SY0-601/dp/1119736250 (كتاب)

سلسلة فيديوهات Professor Messer's Security+: https://m.youtube.com/watch?v=y0kxvVbAc1A

• **(ISC)² Certified Secure Incident Analyst (CySA+)**: تركز هذه الشهادة على المهارات المطلوبة لتحديد، تحليل، والاستجابة للحوادث الأمنية. تغطي إجراءات التعامل مع الحوادث، كشف التهديدات، وأدوات الأمان. CySA+ تثبت قدرتك على الاستجابة بفعالية للتهديدات السيبرانية والحفاظ على أمان المنظمات.

<u>الموارد:</u>

صفحة شهادة (ISC)² CySA+: https://www.isc2.org/certifications/associate

الدليل الرسمي لدراسة CISSP $(ISC)^2$ (CySA+) يغطي مجموعة فرعية من مواضيع CISSP):
https://www.amazon.com/Practical-Cybersecurity-Architecture-implementing-cybersecurity/dp/1837637164 (كتاب)

دورة CySA+ على Cybrary: https://www.cybrary.it/course/introduction-to-it-and-cybersecurity

• **GIAC Security Essentials (GSEC)**: توفر هذه الشهادة المحايدة بالنسبة للموردين أساسًا واسعًا في أمن المعلومات. تغطي المفاهيم الأساسية للأمان مثل أمان الشبكات، التشفير، وإدارة الأمان. GSEC هي اعتماد محترم ونقطة انطلاق جيدة للجدد في الأمن السيبراني.

<u>الموارد:</u>

صفحة شهادة GIAC GSEC: https://www.giac.org/

معسكر تدريبي GSEC من SANS: https://www.sans.org/ (تدريب مدفوع)

• **Certified Ethical Hacker (CEH):** تركز هذه الشهادة على اختبار الاختراق ومنهجيات القرصنة الأخلاقية. تزودك بالمهارات لتحديد واستغلال الثغرات في الأنظمة الحاسوبية، بطريقة مشابهة لما قد يفعله الفاعلون الخبيثون. CEH هي شهادة شائعة لأولئك المهتمين بالأدوار الأمنية الهجومية.

<u>الموارد:</u>

صفحة شهادة EC-Council CEH: https://www.eccouncil.org/train-certify/ethical-hacking/

الامتحانات التدريبية الرسمية لـ CEH: https://passemall.com/free-ceh-v11-practice-test