

خطة تعلم الأمن السيبراني (للطلاب الجدد)

الأسبوع 1-2: المقدمة والأساسيات

الهدف

- وضع أساسيات مبادئ الأمن السيبراني وتطوره.

الأنشطة

- مقدمة في تاريخ الأمن السيبراني والمعايير والتشريعات والأطر العملية.
- استكشاف معاني ونطاق الأمن السيبراني.
- مناقشة كيفية تطور مجال الأمن السيبراني كما هو الآن.

الأسبوع 3-4: أمن الشبكات

الهدف

- التركيز على تأمين الشبكات وفهم الضعف فيها.

الأنشطة

- التعمق في مبادئ أمن الشبكات، بما في ذلك جدران الحماية، أنظمة كشف الاختراق، وتكوينات الشبكات الآمنة.
- تنفيذ تمارين عملية باستخدام محاكاة الشبكات أو إعدادات الشبكة الأساسية.

الأسبوع 5-6: أمن الويب وممارسات البرمجة الآمنة

الهدف

- التعرف على ثغرات أمن الويب وأفضل الممارسات في البرمجة الآمنة.

الأنشطة

- مناقشة الثغرات الشائعة في الويب مثل حقن SQL، هجمات XSS، و CSRF.
 - تقديم ممارسات البرمجة الآمنة في لغات مثل Python، Java، أو JavaScript.
 - مختبرات عملية لتحديد وإصلاح الثغرات الأمنية.
-

الأسبوع 7-8: التشفير

الهدف

- فهم مبادئ التشفير.

الأنشطة

- تقديم خوارزميات التشفير (التماثلية واللاتماثلية)، التوقيعات الرقمية، والتجزئة.
- تمارين عملية في تشفير وفك تشفير البيانات باستخدام مكتبات أو أدوات التشفير.

الأسبوع 9-10: التطبيقات العملية والمشاريع

الهدف

- تطبيق المفاهيم المتعلمة في سيناريوهات عملية وإكمال المشاريع النهائية.

الأنشطة

- كل طالب يعمل على مشروع فردي في مجال أمن السيبراني.
- اختيار موضوع مشروع يغطي مختلف الجوانب المتعلمة خلال الدورة، مثل إعداد أمن الشبكات، تنفيذ البرمجة الآمنة، وتطبيقات التشفير.
- تقديم وعرض المشروع النهائي لكل طالب، يتضمن شرحًا للتحديات والحلول التي تم التعامل معها خلال المشروع.