الجمهورية العربية السورية
المعهد العالي للعلوم التطبيقية والتكنولوجيا

وثيقة توصيف مقرّر درسي

عنوان المقرّر	الاختراق الأخلاقي (Ethical Hacking)
عدد وحدات التعلّم	3 ECTS
غاية المقرّر	تعريف الطالب بالمبادئ الأساسيّة للاختراق الأخلاقي وطرائق تحليل نقاط الضعف وتقييمها والعمل على معالجتها، بما يمكّنه من استخدام الأساليب والأدوات الحديثة في عمليات واختبارات الاختراق لنظم المعلومات والاتصالات بما في ذلك مخدّمات الويب وتطبيقاته ونظم التشغيل والشبكات اللاسلكيّة.

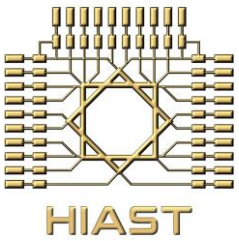
مخرجات التعلّم المستهدفة

سيكون الطالب الذي يكمل هذا المقرّر بنجاح قادراً على:

- تعرّف المفاهيم الأساسيّة لعمليّات تجميع المعلومات واختراق النظم.
- فهم مبادئ وطريقة القيام بتحليل نقاط الضعف لمنظومات معلوماتيّة.
- فهم مبادئ الاختراق على مستوى الشبكة وعلى مستوى تبادل المعطيات.
- تعرّف المبادئ الأساسيّة لاختراقات الويب وتطبيقاته.
- تعرّف على طرائق اختبار الشبكات اللاسلكيّة أمنيّاً وسد الثغرات الناتجة.
- تنفيذ اختبارات الاختراق للمنظومات الشبكية.
- تطبيق وتنفيذ تحليل نقاط الضعف واستخراج التقارير.
- اتخاذ التدابير اللازمة للحماية من الاختراق.

محتوى المقرّر

- **تجهيز المخبر والأدوات:** تجهيز حواسيب المخبر وحواسيب الطلاب بما يلزم للعمل في المنزل.
- **جمع المعلومات:** Footprinting من خلال محرّكات البحث، Footprinting من خلال خدمات الويب، Footprinting من خلال مواقع التواصل الاجتماعي، Footprinting مواقع الويب، إجراء المسح، إجراء التعداد.
- **تحليل نقاط الضعف:** آليّات التحليل وطرائق العمل، OpenVAS، Nessus، GFI LanGuard، Nikto.
- **اختراق الأنظمة:** الوصول إلى الأنظمة، تعديل الصلاحيّات، الوصول عن بعد وإخفاء البرامج الخبيثة، مسح السجلّات وإلغاء الأدلّة الرقميّة.



- **البرمجيّات الخبيثة:** استخدام أحصنة طروادة، استخدام الفيروسات، القيام بعمليّات تحليل البرامج الخبيثة.
- **الهندسة الاجتماعيّة:** الحصول على كلمات المرور، الاصطياد، كشف الاصطياد.
- **منع الخدمة:** SYN flooding، hping3، DDOS، كشف منع الخدمة.
- **الهجمات الشبكيّة:** Active Sniffing، Network sniffing، Detect Sniffing، Session Hijacking.
- **تجاوز الجدران الناريّة:** كشف الدخلاء، كشف حركة المرور الخبيثة، تجاوز الجدران النارية.
- **هجمات الويب:** تعداد ومسح مخدمات الويب، كسر كلمات مرور FTP، Brute-force attack، XSS، CSRF، SQL injection، كشف اختراقات الويب.
- **هجمات الشبكات اللاسلكيّة:** تحليل حركة مرور الشبكات اللاسلكيّة المحليّة، إيجاد الشبكات المخفيّة، كسر WEP، كسر WPA، اختراق نظم Android، حماية نظم Android.
- **تحليل التعمية:** حساب توابع البصمة، تعمية الملفّات والرسائل النصيّة، حماية البريد الإلكتروني، تعمية الأقراص، تحليل التعمية.