الجمهورية العربية السورية
المعهد العالي للعلوم التطبيقية والتكنولوجيا

وثيقة توصيف مقرّر درسي

عنوان المقرّر	أمن الشبكات (Networks Security)
عدد وحدات التعلّم	3.5 ECTS
غاية المقرّر	تزويد الطالب بالمعارف المتعلّقة بأمن شبكات المعطيات بمختلف أشكالها وتجهيزاتها (بما في ذلك التهديدات والمخاطر التي تتعرّض لها هذه الشبكات والتجهيزات) وبأهم طرائق حماية الشبكات ونظم المعلومات، بما يمكّنه من استخدام المعايير والإجراءات (بما في ذلك بروتوكولات أمن الشبكات وتطبيقاتها) والنظم البرمجيّة أو العتاديّة لحماية أمن الشبكات وكشف الاختراقات.

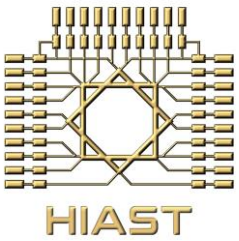
مخرجات التعلّم المستهدفة

سيكون الطالب الذي يكمل هذا المقرّر بنجاح قادراً على:

- تعرّف أهم أنواع التهديدات التي تتعرّض لها شبكات المعطيات مثل الهجومات الشبكيّة والبرامج الخبيثة وفهم آليّة عمل هذه التهديدات.
- فهم عمل أدوات حماية الشبكات مثل الجدار الناري وأنظمة كشف الاختراق: أنواعها، مبدأ عمل كل منها وطرائق استخدامها.
- تعرّف بروتوكولات أمن الشبكات المعياريّة وتطبيقاتها مثل TLS, SSL, IPSec.
- تعرّف المخاطر والتهديدات التي تتعرّض لها نظم التشغيل ومراكز المعلومات وطرائق حمايتها.
- تعرّف التهديدات والمخاطر الخاصّة بالشبكات اللاسلكيّة وطرائق حمايتها بشكل معياري.
- تعرّف التهديدات والمخاطر المتعلّقة ببعض الأنظمة الخاصّة مثل: إنترنت الأشياء والحوسبة السحابيّة.
- معالجة نقاط الضعف أو الثغرات الأمنيّة في نظم المعلومات.

محتوى المقرّر

- **الهجمات الشبكيّة المعروفة وطرائق منعها:** DOS attacks، Spoofing، Flooding، Distributed DOS، Reflector and implifier، Responding to DOS attack.
- **البرامج الخبيثة:** Advanced Persistent Threat، Viruses، Worms، Trojans – Spam، Social Engineering، Information theft: Keylogger, phishing, spyware، Information thift: backdoors, rootkits، الأنظمة المضادة للفيروسات.
- **أمن الشبكات الفيزيائي:** التهديدات الفيزيائيّة على البنية التحتيّة والتجهيزات (كابلات، مبدّلات، موجّهات)، أدوات منع والحد من



التهديدات الفيزيائيّة، استعادة النظام بعد حدوث الخرق الفيزيائي، تكامل الحماية الفيزيائي المنطقي.

- **نظم كشف الاختراق:** كشف الاختراق، طرق التحليل، كشف الاختراق على مستوى المحطّة HIDS، كشف الاختراق في الشبكة NIDS، كشف الاختراق الموزّع DIDS، جرار العسل، مثال: Snort.
- **الجدار الناري:** مبدأ عمل الجدار الناري، سياسة الوصول، أنواع الجدار الناري، تموضع وإعدادات الجدار الناري.
- **معايير وبرتوكولات أمن الشبكات وتطبيقاتها:** SSL, TLS، SSH، IPSec، VPN، TOR.
- **أمن مراكز المعلومات وشبكات المؤسسات enterprise networks:** الأمن على مستوى طبقة الربط المعطيات MAC layer، Ethenet, Learning Bridging , VLAN، الهجوم على الشبكات المحلّيّة الافتراضيّة VLAN attacks، Spanning tree protocol، Attack on spanning tree، Switch Learning attacks، DHCP attacks.
- **أمن نظم التشغيل:** أمن نظام التشغيل Windows، أمن نظام التشغيل Linux.
- **أمن برتوكولات التوجيه:** التهديدات على برتوكولات التوجيه، تقنيّات الأمن المطبّقة على البرتوكولات RIP, OSPF، هجوم شجرة الـ BGP، البرتوكولات SBGP, SOBGP.
- **أمن الشبكات اللاسلكيّة:** تهديدات االشبكات اللاسلكيّة، أمن الشبكات اللاسلكيّة وفق المعيار ٨٠٢,١١، i٨٠٢,١١، أمن الحوسبة السحابيّة، أنواع الحوسبة السحابيّة، التهديدات والمخاطر ونقاط الضعف في الحوسبة السحابيّة، الاعتبارات الأمنيّة في الحوسبة السحابيّة، الإجراءات الأمنيّة المفضّلة في الحوسبة السحابيّة.
- **أمن إنترنت الأشياء:** الواقع الحالي لإنترنت الأشياء وتطبيقاتها، أهميّة أمن إنترنت الأشياء، السرّية والخصوصيّة لإنترنت الأشياء المعرفة وفق ITU-T، التهديدات على شبكات إنترنت الأشياء، حماية إنترنت الأشياء.