مقررات برنامج ماجيستر الأمن السيبراني

أمن :511يهدف هذا المقرر إلى تعريف الطلاب بإجراءات وعمليات تخطيط وإدارة الأمن السيبراني على المستويات التكتيكية والاستراتيجية والتشغيلية. يتناول المقرر مجموعة من الموضوعات التي تشمل دور المسؤولين التنفيذيين في الأمن السيبراني، حماية الملكية الفكرية، وإدارة تحديثات الأنظمة. كما سيتم تعريف الطلاب بإجراءات الاستجابة للحوادث واستمرارية الأعمال وإجراءات الاستعداد للكوارث.

أمن :512يهدف هذا المقرر إلى تعريف الطلاب بالمصطلحات الأساسية في ميدان الجرائم الإلكترونية، التحقيق الجنائي الرقمي، الاستجابة للحوادث الأمنية، التحقيق في الجرائم الإلكترونية والمحاكمة والملاحقة الجنائية. سيكتسب الطلاب المهارات المعرفية الخاصة بدور التكنولوجيا في التحقيق في الجرائم الإلكترونية وإجراءات التحليل الجنائي الرقمي. يمكن هذا المقرر الطلاب من اكتساب المعلومات اللازمة عن أدوات تصوير أنواع مختلفة من الوسائط الإلكترونية ومن ثم تحليل هذه الصور لاستخراج الأدلة منها. كما سيتعلمون كيف يمكن للمؤسسات إنشاء فريق استجابة للحوادث الأمنية، التحضير للحوادث الأمنية، و كيفية إدارتها.

أمن :513يغطي هذا المقرر معرفة الهندسة الأمنية المستخدمة لحماية أنظمة المعلومات. وسيتم عرض المواضيع المتعلقة بالدفاع العميق، المنطقة الوسيطة المنزوعة السلاح، الخوادم الوكيلة، المجموعات الفرعية لـTCB ، الهياكل الأمنية المؤسسية، والتصميم الآمن للشبكات. كما يركز المقرر على معايير ضمان المعلومات، حيث يتم تفصيل المعايير الوطنية واللوائح والمعايير الدولية)على سبيل المثال (NIST والمعايير التجارية) على سبيل المثال (PCI/DSS والمعايير المفتوحة) مثل (OWSAP المتعلقة بالأمن السيبراني.

أمن :514يهدف هذا المقرر إلى تزويد الطلاب بالمكتسبات والمعلومات اللازمة لفهم جيد لمنهجيات اختبار الاختراق الأخلاقي. يزود هدا المقرر الطلاب بكيفية استخدام أساليب استطلاع الأهداف، تعداد المضيفين والخدمات، تحديد الثغرات ونقاط لضعف واستغلالها، بالإضافة إلى كيفية استخدام المهاجمين والمخترقين لهذه التقنيات المختلفة من أجل توسيع نطاق تأثيرهم. يتم تعريف الطلاب بمختلف الأدوات اللازمة لتحديد الثغرات ونقاط الضعف، استغلالها، تقييم المخاطر الأمنية في الشبكات وأنظمة التشغيل والتطبيقات. يستخدم الطلاب في هذا المقرر عددا من الأدوات مفتوحة المصدر لاختبار الاختراق وإعداد تقارير عن النتائج.

أمن :515يهدف هذا المقرر إلى تزويد الطلاب بمقدمة عن المنهجيات والأدوات البرمجية المستخدمة في تقييم نقاط الضعف واكتشاف الثغرات. يركز المقرر على استخدام هذه المنهجيات لإثبات وتوثيق وتقديم تقارير تتضمن خريطة طريق واضحة لمعالجة هذه الثغرات ونقاط الضعف. سيتمكن الطلاب من استكشاف طرق استطلاع الهدف، الفحص العميق للحزم، المقارنة المتبادلة، وتحليل ملفات السجل. كما يتم تعريف الطلاب بخوارزميات التصفية المختلفة وأدوات مفتوحة المصدر للكشف عن الاختراق ومنعه على مستوى المضيف والشبكة.

أمن :516يوفّر هذا المقرر نظرة عامة وشاملة حول مواضيع التشفير المتقدّم. سيتعلّم الطلاب مبادئ نظرية الأعداد، مبادئ الاحتمالات والإحصاء، ومبادئ الجبر الخطي، والتشفير بالمنحنيات الإهليلجية، RSA، وAES، حزمة الخوارزميات غير العسكرية وغير السريةSuite B ، أنواع الهجمات التي يتعرض لها التشفير مثل: التحليل التفاضلي للتشفير، هجوم الرجل في الوسط، التحليل الخطي، تجزئة التوقيعات الرقمية، إدارة المفاتيح، التحليل التقليدي والكلاسيكي للتشفير، الهجمات الجانبية مثل هجمات التوقيت وهجمات استهلاك الطاقة، الهجمات عن طريق تحليل اختلاف الأخطاء، التشفير المستند إلى الهوية، التوقيع الرقمي، الشبكات الافتراضية الخاصة، والحوسبة الكمومية والتشفير.

أمن :530يتيح هذا المقرر للطلاب إتقان مجال معين ضمن مجال الأمن السيبراني من خلال القيام بعمل علمي بحثي ضمن مشروع تخرج. يجب توثيق نتائج البحث والدفاع عنها بنجاح خلال تقديم شفوي. في هذا الجزء من المشروع، سيتم تعريف الطلاب بمنهجيات البحث، كيفية تخطيط مقترحاتهم البحثية، تصميمها، وتوثيقها .**المتطلب: استكمال 12ساعة.**

أمن :531يتيح هذا المقرر للطلاب إتقان مجال معين ضمن مجال الأمن السيبراني من خلال القيام بعمل علمي بحثي ضمن مشروع تخرج. يجب توثيق نتائج البحث والدفاع عنها بنجاح خلال تقديم شفوي. في هذا الجزء من المشروع، سيواصل الطلاب

العمل على مقترحاتهم من خلال تطوير عمليات التنفيذ أو المحاكاة، وكذلك من خلال التقييمات التجريبية وتحليل النتائج المتوصل إليها .**المتطلب: أمن .530**