2023
TP-153

توصيف المقرر الدراسي

اسم المقرر: الاختراق الاخلاقي
رمز المقرر: 25262 سبر
البرنامج: الامن السيبراني
القسم العلمي: الحاسب الآلي ونظم المعلومات
الكلية: التطبيقية
المؤسسة: جامعة بيشة
نسخة التوصيف: 1
تاريخ آخر مراجعة:

جدول المحتويات

أ. معلومات عامة عن المقرر الدراسي: 4
ب. نواتج التعلم للمقرر واستراتيجيات تدريسها وطرق تقييمها: 6
ج. موضوعات المقرر 9
د. أنشطة تقييم الطلبة 9

ه. مصادر التعلم والمرافق: 10

و. تقويم جودة المقرر: 12

ز. اعتماد التوصيف: 12

أ. معلومات عامة عن المقرر الدراسي:

1. التعريف بالمقرر الدراسي

1. الساعات المعتمدة: (3)					
2. نوع المقرر					
أ -	☐ متطلب جامعة	☐ متطلب كلية	✔ متطلب تخصص	☐ متطلب مسار	☐ أخرى
ب -	✔ إجباري	☐ اختياري			
3. السنة / المستوى الذي يقدم فيه المقرر: (الاولى/الأول)					
4. الوصف العام للمقرر					
يقدم هذا المقرر محتوي يساعد الطالب على إتقان نفس الأساليب التي يستخدمها المتسللون لاختراق أنظمة الشبكات والاستفادة منها أخلاقياً لحماية البنية التحتية الخاصة للمؤسسات والافراد. يركز المقرر على أكثر المجالات الأمنية شيوعًا لتوفير نهج عملي لأنظمة الأمان الأساسية. سوف يتعلم الطالب تقييم أمان نظام الحاسب باستخدام تقنيات اختبار الاختراق؛ فحص الأنظمة والتطبيقات والاختبار والتسلل الآمن والحصول على خبرة عملية في تكتيكات الاستنشاق والتصيد الاحتيالي والاستغلال.					
5- المتطلبات السابقة لهذا المقرر (إن وجدت)					
تقنيات الاستجابة والتحليل الجنائي (25232سبر)					
6- المتطلبات المتزامنة مع هذا المقرر (إن وجدت)					
7. الهدف الرئيس للمقرر					

يقدم هذا المقرر المعرفة بمختلف تقنيات الاختراق والاختراق الأخلاقي والمهارات العملية المطلوبة لإجراء اختبار الاختراق، وزيادة مستوي التأمين في انظمة الحاسب مثل التي تستخدم في البنوك، الدواوين الحكومية، انظمة الدفع الالكتروني والشركات.

2. نمط التعليم (اختر كل ما ينطبق)

م	نمط التعليم	عدد الساعات التدريسية	النسبة
1	تعليم التقليدي	45	%75
2	التعليم الإلكتروني	15	%25
3	التعليم المدمج • التعليم التقليدي • التعليم الإلكتروني		
4	التعليم عن بعد		

3. الساعات التدريسية (على مستوى الفصل الدراسي)

م	النشاط	ساعات التعلم	النسبة
1	محاضرات	30	50%
2	معمل أو إستوديو	30	50%
3	ميداني		
4	دروس إضافية		
5	أخرى		
	الإجمالي	60	100%

ب. نواتج التعلم للمقرر واستراتيجيات تدريسها وطرق تقييمها:

الرمز	نواتج التعلم	رمز ناتج التعلم المرتبط بالبرنامج	استراتيجيات التدريس	طرق التقييم
1.0	المعرفة والفهم			
1.1	التعرف على اساسيات الاختراق الأخلاقي	ع1	محاضرة في القاعات الدراسية، مجموعات النقاش	الاختبارات الفصلية الواجبات الاختبار النهائي
1.2	التعرف على الأثار القانونية للاختراق الاخلاقي	ع2	محاضرة في القاعات الدراسية، مجموعات النقاش	الاختبارات الفصلية الواجبات الاختبار النهائي
1.3	معرفة ضوابط امن نظم المعلومات	ع3	محاضرة في القاعات الدراسية، مجموعات النقاش	الاختبارات الفصلية الواجبات الاختبار النهائي
2.0	المهارات			
2.1	تطبيق تقنيات اختبار الاختراق للكشف عن نقاط الضعف في أنظمة التشغيل والتطبيقات والشبكات.	م1	محاضرة في القاعات الدراسية، مجموعات النقاش	الاختبارات الفصلية الواجبات الاختبار النهائي
2.2	مهارات تحمل مسؤولية البحث عن معلومات جديدة في مجال البرمجة والامن السيبراني.	م2	محاضرة في القاعات الدراسية، مجموعات النقاش	الاختبارات الفصلية الواجبات الاختبار النهائي
2.3	مهارات التعامل مع الأشخاص وتحمل المسؤولية، ونقل المهارات المكتسبة الى التطبيق العملي.	م3	محاضرة في القاعات الدراسية، مجموعات النقاش	الاختبارات الفصلية الواجبات الاختبار النهائي
3.0	القيم والاستقلالية والمسؤولية			

الرمز	نواتج التعلم	رمز ناتج التعلم المرتبط بالبرنامج	استراتيجيات التدريس	طرق التقييم
3.1	تنفيذ اجراءات مضادة فعالة للدفاع عن الهجمات على نظام التشغيل والشبكات على أساس العمل الجماعي.	ق 1	محاضرة في القاعات الدراسية، مجموعات النقاش	الاختبارات الفصلية الواجبات الاختبار النهائي
3.2	القدرة على علاج اختراقات الأنظمة.	ق2	محاضرة في القاعات الدراسية، مجموعات النقاش	الاختبارات الفصلية الواجبات الاختبار النهائي

ج. موضوعات المقرر

م	قائمة الموضوعات	الساعات التدريسية المتوقعة
1	مقدمة للاختراق الاخلاقي: المصطلحات الاساسية، عناصر امن المعلومات، مثلث: الأمان، الوظيفية، والاستخدام	**4**
2	المخاطر التي تعترض امن المعلومات ومتجهات الهجوم: الدوافع وأهداف هجمات أمن المعلومات، التعرف على مخاطر امن المعلومات الاكثر شيوعا، تصنيف مهددات امن المعلومات، انواع الهجوم علي الأنظمة، حرب نظم المعلومات.	**4**
3	مفاهيم اختبار الاختراقات: لماذا اختبار الاختراقات، مقارنة طرق التدقيق الأمني وتقييم الضـــعف واختبار الاختراق، فرق العمل الزرقاء، فرق العمل الحمراء، انواع اختبارات الاختراق، مراحل اختبارات الاختراق، طرق اختبار امن الانظمة.	**6**
4	مفاهيم الاختراق: اختراق القبعة السوداء، اختراق القبعة الرمادية، اختراق القبعة البيضاء.	**4**
5	مفاهيم الاختراق الأخلاقي: تعريف الاختراق الاخلاقي، اهمية الاختراق الاخلاقي، مدي ومحددات الاختراق الاخلاقي، مهارات المخترق الاخلاقي.	**4**

6	ضوابط امن المعلومات: ضمان المعلومات، برنامج ادارة امن المعلومات، هندسة امن معلومات المشاريع، طرق تطويق (**Zoning**) امن الشبكات، نظرية الدفاع العميق، سياسات امن المعلومات، الأمن الفيزيائي، تعريف المخاطر، نمذجة المخاطر، ادارة الحوادث(**incident**)، تحليل سلوك المستخدم، تسرب البيانات، النسخ الاحترازية للبيانات، استرجاع البيانات، دور الذكاء الصناعي وتعلم الآلة في الأمن السيبراني.	4
7	اختبار نظري-1	2
8	قوانين امن نظم المعلومات: الطرق القياسية للدفع عبر البطاقات، قوانين امن نظم المعلومات في الدول المختلفة.	4
9	الشبكات واختراق الشبكات: طرق مسح الشبكات: مفاهيم مسح الشبكات، بروتوكول **TCP/IP**، تحليل الثغرات، مفاهيم التعداد (**Enumeration Concepts**)، تكنيكات التعداد، بورتات التعداد.	4
10	اختراق الانظمة: مفاهيم اختراق الانظمة، تحليل الثغرات: تصنيف الثغرات، اهداف اختراق الانظمة. حقن **SQL**.	4
11	كسر كلمات المرور: طرق الهجوم على كلمات المرور، طرق استعادة كلمات المرور، انظمة التحقق في انظمة التشغيل المختلفة.	4
12	اختراق الاجهزة الذكية وانترنت الاشياء: الثغرات في انظمة تشغيل الاجهزة الذكية، تشريح الهجوم علي الموبايل، كيف يحقق المخترق الربح من اختراق نظام الموبايل، اقتران اجهزة الموبايل عبر البلوتوث. تعريف انترنت الاشياء، المخاطر في انترنت الاشياء في مقابل الفرص التي تتيحها. اختراقات انترنت الاشياء،	6
13	الحوسبة السحابية: مقدمة للحوسبة السحابية، طرق النشر في الحوسبة السحابية، مهددات الحوسبة السحابية، هجومات الحوسبة السحابية.	4
14	اختبار نظري -2	2
15	اختراق سيرفرات الويب: اشغال سيرفرات الويب، معمارية سيرفرات الويب، طرق الهجوم علي سيرفرات الويب، ادوات الهجوم علي سيرفرات الويب، ادوات حماية سيرفرات الويب.	4
المجموع		60

د. أنشطة تقييم الطلبة

م	أنشطة التقييم	توقيت التقييم (بالأسبوع)	النسبة من إجمالي درجة التقييم
1	اختبار نظري - 1	7	10%
2	اختبار نظري - 2	14	10%
3	واجبات واختبارات قصيرة وأنشطة	طوال الفصل	10%
4	عملي	طوال الفصل	20%
5	اختبار نهائي	نهاية الفصل	50%

أنشطة التقييم (اختبار تحريري، شفهي، عرض تقديمي، مشروع جماعي، ورقة عمل وغيره)

ه. مصادر التعلم والمرافق:

1. قائمة المراجع ومصادر التعلم:

المرجع الرئيس للمقرر	Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition 5 th Edition, ISBN-13: 978-1260108415

المراجع المساندة	1- Zaid Sabih,"Learn Ethical Hacking from Scratch", Packt Publishing Ltd, 2018, ISBN 978-1-78862-205-9 2- The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy 2nd Edition ISBN-13: 978-0124116443 3- Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Branko Spasojevic, Ryan Linn, Stephen Sims, "Gray Hat Hacking_The Ethical Hacker's Handbook", McGraw-Hill Osborne Media, 2015 4. Patrick Engebretson, "The Basics of Hacking and Penetration Testing_Ethical Hacking and Penetration Testing Made Easy", Syngress, 2011
المصادر الإلكترونية	https://www.hackersonlineclub.com/online-ethical-hacking-training/
أخرى	

2. المرافق والتجهيزات المطلوبة:

العناصر	متطلبات المقرر
المرافق النوعية (القاعات الدراسية، المختبرات، قاعات العرض، قاعات المحاكاة ... إلخ)	قاعة دراسية سعة 50 طالب
التجهيزات التقنية (جهاز عرض البيانات، السبورة الذكية، البرمجيات)	سبورة ذكية، جهاز عرض البيانات، جهاز حاسب آلي
تجهيزات أخرى (تبعاً لطبيعة التخصص)	أقلام واوراق

و. تقويم جودة المقرر:

مجالات التقويم	المقيمون	طرق التقييم
فاعلية التدريس	الطلبة + رئيس القسم + والتقييم الذاتي	مباشر عن طريق الاستبيانات – وغير مباشر عن طريق تحليل الاداء والنتائج
فاعلية طرق تقييم الطلاب	المراجع النظير– استاذ المقرر – الطلاب	مباشر عن طريق المقارنات المرجعية – وتحديث المراجع
مصادر التعلم	استاذ المقرر – رئيس القسم	غير مباشر عن طريق تحليل الاداء والنتائج
مدى تحصيل مخرجات التعلم للمقرر	استاذ المقرر – رئيس القسم	غير مباشر عن طريق تحليل الاداء والنتائج
أخرى		

المقيمون (الطلبة، أعضاء هيئة التدريس، قيادات البرنامج، المراجع النظير، أخرى (يتم تحديدها).
طرق التقييم (مباشر وغير مباشر).

ز. اعتماد التوصيف:

جهة الاعتماد	
رقم الجلسة	
تاريخ الجلسة	