وزارة التعليم
Ministry of Education

أوراق عمل

مقرر الأمن السيبراني

للصف الثالث ثانوي - مسار الحاسب والهندسة

الفصل الدراسي الأول

مدرسة بكة الثانوية للموهوبين

اسم الطالب:

الشعبـــــة:

معلم المـادة: حسام مساعد الثقفي

مدرسة بكة الثانوية للموهوبين
١٤٣٨هـ

جدول متابعة الطالب

الوحدة	أوراق العمل	الدرجة	توقيع المعلم
الوحدة الأولى	الدرس الأول		
	الدرس الثاني		
	الدرس الثالث		
الوحدة الثانية	الدرس الأول		
	الدرس الثاني		
	الدرس الثالث		
الوحدة الثالثة	الدرس الأول		
	الدرس الثاني		
	الدرس الثالث		
المجموع			

معلم المـادة: حسام مساعد الثقفي

محتوى مقرر مادة الأمن السيبراني

الوحدة الأولى

أساسيات الأمن السيبراني

الوحدة الثانية

الحماية والاستجابة في الأمن السيبراني

الوحدة الثالثة

مواضيع متقدمة في الأمن السيبراني

تدريب (١): أكمل الجدول التالي بما يناسبه من السطر الأول :

الهجمات السيبرانية	السرية	السلامة	التوافر	التوقيع الرقمي

م	النوع	الوصف
١		يستخدم خوارزميات رياضية للتحقق من صحة رسالة أو مستند أو معاملة وسلامتها
٢		يشير إلى ضمان إمكانية الوصول إلى المعلومات عند الحاجة
٣		تشير إلى توكيد دقة البيانات وعدم التلاعب بها
٤		إجراء يقوم به طرف معين ذو نوايا سيئة بهدف الإتلاف أو التعطيل أو الوصول غير المصرح به إلى أنظمة الحاسب أو الشبكات أو البيانات :
٥		تشير إلى الحفاظ على القيود المصرح بها للوصول إلى المعلومات

تدريب (٢): ضع علامة (✓) أمام العبارة الصحيحة وعلامة (✗) أمام العبارة الخاطئة:

١. السرية والسلامة والمصادقة تشكل مثلث أمن المعلومات .	
٢. جميع الجرائم الإلكترونية لها نفس المستوى من الخطورة والعواقب .	
٣. يعد التشفير والتحكم في الوصول وإخفاء البيانات من الطرائق المستخدمة للحفاظ على سرية البيانات.	
٤. يؤدي رئيس إدارة الأمن السيبراني دوراً وظيفياً في الأمن السيبراني .	
٥. سايبرك هي طريقة شائعة للمهاجمين لعرقلة توافر البيانات.	
٦. تعتبر وظيفة رئيس إدارة الأمن السيبراني من مجال تخصص القيادة .	
٧. يمكن الحفاظ على التوافر من خلال تخزين نسخ متعددة من البيانات.	
٨. يمكن الحفاظ على السلامة من خلال استخدام التوقيعات الرقمية .	
٩. تعتبر وظيفة محلل دفاع الأمن السيبراني من مجال تخصص الدفاع .	

تدريب (١): اختر الإجابة الصحيحة فيما يلي:

١	أي شيء ذو قيمة لفرد أو مؤسسة أو دولة يمكنه أن يتأثر سلباً بهجوم سيبراني ضار :						
أ	أصول الأمن السيبراني	ب	ثغرات الأمن السيبراني	ج	مخاطر الأمن السيبراني		
٢	تظهر كبرنامج موثوق أو مفيد ولكنها في الحقيقة تنفذ إجراءات ضارة على جهاز الحاسب في الخلفية دون علم مستخدم الجهاز :						
أ	الديدان	ب	أحصنة طروادة	ج	برمجيات الفدية		
٣	هجمات تعتمد على إغراق الشبكة أو الخادم بحركة بيانات ضخمة تجعل من الصعب على المستخدمين الشرعيين الوصول إلى الخدمة :						
أ	هجمات الهندسة الاجتماعية	ب	هجمات حجب الخدمة	ج	هجمات الوسيط		
٤	تعتمد على استغلال نقاط الضعف في البرامج قبل اكتشافها وتصحيحها مما يكسبها خطورة عالية :						
أ	هجمات البرمجة العابرة للمواقع	ب	هجمات كلمات المرور	ج	استغلال الثغرات الصفري		
٥	تحاكي الهجمات على الأنظمة أو الشبكات لتحديد الثغرات الأمنية وتختبر فعالية الضوابط الأمنية :						
أ	جدار الحماية ونظام الحماية	ب	تقييم المخاطر الأمنية	ج	أدوات اختبار الاختراق		

تدريب (٢): أكمل الجدول التالي بما يناسبه :

جهات على مستوى دولي	مجموعات الجريمة المنظمة	النشطاء المخترقين
التهديدات الداخلية	هواة السيكربت	المنافسون

م	المفهوم	الوصف
١		هم متسللين هواة يستخدمون أدوات القرصنة وبعض البرامج النصية الأخرى لتنفيذ هجمات وذلك من أجل التسلية، أو لاكتساب الشهرة أو لتحدي أنفسهم.
٢		هم أفراد أو مجموعات يستخدمون القرصنة للترويج لقضية سياسية أو اجتماعية مثل: تشويه مواقع ويب معينة، أو إجراء هجمات حجب الخدمة وجذب الانتباه لقضيتهم .
٣		تتكون من مجرمين محترفين ينفذون هجمات سيبرانية لتحقيق مكاسب مالية مثل : برمجيات الفدية، وسرقة الهوية، وانتحال الشخصية.
٤		هي مجموعات متطورة غالبا ما تكون تابعة لجيش أو جهاز مخابرات لدولة معينة وتكون دوافعها سياسية أو اقتصادية أو عسكرية.
٥		هم أفراد من داخل المؤسسة لديهم إمكانية الوصول ولكنهم يستخدمونها بشكل ضار أو غير مسؤول، وتتنوع الدوافع وراء ذلك مثل: تحقيق المكسب المالي، أو الانتقام، أو الإكراه.
٦		قد تنخرط بعض الشركات في عمليات تجسس على شركات أخرى بغرض الحصول على ميزة تنافسية، أو الحصول على أسرار تجارية أو منتجات أو استراتيجيات غير معلنة

تدريب (١): أكمل الجدول التالي بما يناسبه :

التعريف	المصادقة	التفويض
عدم الإنكار	مبدأ الحد الأدنى من الصلاحيات والامتيازات	الحاجة إلى المعرفة
تعدد الطبقات	التنويع	التعتيم
التدقيق والمراقبة		

م	المفهوم	الوصف
١		يتضمن هذا المبدأ إخفاء بيانات المصادقة الضرورية عن الأنظار، ويُعد بمثابة شكل مهم من أشكال حماية التطبيقات لمنع الوصول غير المصرح به إلى المعلومات والبيانات المهمة.
٢		يجب أن يقتصر الوصول للمعلومات على أولئك الذين لديهم حاجة تشغيلية لمعرفة تلك المعلومات، ويُعد هذا إجراء هاما للأمن والخصوصية.
٣		يضمن أن المستخدمين المناسبين هم فقط من يمكنهم الوصول إلى الموارد وتنفيذ الإجراءات المسموح لهم بها، مما يحد من إمكانية الوصول غير المصرح به أو إساءة استخدام البيانات الحساسة.
٤		يضمن عدم تمكن المستخدمين من إنكار صحة أفعالهم أو معاملاتهم داخل النظام، ويحمل هذا الأمر أهمية خاصة في الحالات التي يجب فيها الحفاظ على سلامة البيانات أو صحة المعاملات.
٥		يوصي هذا المبدأ بأنه يجب على المؤسسات تنفيذ مجموعة متنوعة من آليات الأمن لتقليل مخاطر الهجوم أو التهديدات الأخرى.
٦		هي عملية التحقق من هوية مستخدم أو جهاز أو نظام يحاول الوصول إلى الموارد داخل المؤسسة
٧		ويُعد هذا المبدأ جزءًا أساسيًا من أنظمة أمن المعلومات، حيث يحد من مخاطر الحماية المبنية على إجراء أمني واحد فقط.
٨		يجب أن تتضمن أنظمة التحكم بالوصول قدرات تدقيق ومراقبة لتتبع أنشطة المستخدم ومحاولات الوصول، ومن خلال تسجيل ومراجعة محاولات وأحداث الوصول.
٩		وسيلة للتحقق من هوية المستخدم أو العملية أو الجهاز بصفته شرطًا مسبقًا لمنح الوصول إلى الموارد في النظام.
١٠		يجب منح المستخدمين الحد الأدنى من مستوى الوصول اللازم لأداء أدوارهم الوظيفية، ويحدُّ هذا من إمكانية الوصول غير المصرح به، أو إساءة استخدام البيانات الحساسة.

تدريب (١): أكمل الفراغات التالية:

- ..... **يتضمن العناية بالمكونات المادية لنظام الحاسب واتخاذ تدابير معينة لمنع الوصول غير المصرح به أو التخريب المتعمد وحماية الأجهزة من التلف الناتج عن العوامل البيئية**
- ..... **هي دوائر إلكترونية أو مكونات ضارة مخفية داخل العتاد لديها القدرة على اختراق النظام أو تسريب البيانات الحساسة.**
- ..... **هي هجمات تستهدف قطاع بدء التشغيل في النظام مما قد يمنع نظام التشغيل من التحميل أو أداء وظائفه.**
- ..... **هو نهج شامل في الأمن السيبراني يهدف إلى حماية سلامة المعلومات وتوافرها وسريتها من خلال استخدام سلسلة من الآليات الدفاعية.**

تدريب (٢): ضع علامة (✓) أمام العبارة الصحيحة وعلامة (✗) أمام العبارة الخاطئة:

١. يعد التصميم الآمن للنظام نهجاً أساسياً في الأمن السيبراني لضمان أمن الأنظمة بجميع مكوناتها.	
٢. جدار حماية ويندوز هو تطبيق برمجي يساعد في حماية نظام تشغيل حاسبك بمراقبة حركة بيانات الشبكة.	
٣. فجوة الشبكة هي إجراء غير أمني يقوم بفصل العتاد مادياً عن الشبكات الأخرى لمنع القرصنة.	
٤. لا تعتمد مفاتيح المرور على استخدام البيانات الحيوية لمصادقة المستخدم.	
٥. يجب تثبيت تحديثات نظام التشغيل بصورة منتظمة لمعالجة أي ثغرات أمنية.	
٦. يُستخدم التشفير لحماية البيانات الحساسة على أجهزة التخزين.	
٧. يتضمن أمن العتاد العناية بالمكونات البرمجية لنظام الحاسب .	
٨. يعتمد مفهوم الدفاع متعدد الطبقات على مبدأ أنه في حال كانت إحدى طبقات الدفاع غير فعالة أو تم اختراقها فيجب أن تكون الطبقة التالية قادرة على منع الهجوم.	
٩. يعد التحكم في الوصول إلى الملفات والمجلدات أحد الإجراءات الأساسية لتأمين أنظمة المعلومات.	

تدريب (١): أكمل الجدول التالي :

م	البروتوكول	الإجابة	التعريف
١	DHCP		يضمن نقل البيانات بشكل موثوق من خلال إنشاء اتصال بين الأجهزة وتسلسل حزم البيانات
٢	FTP		بروتوكول إدارة الشبكة ويقوم تلقائيا بتعيين عناوين بروتوكول الإنترنت IP
٣	SSL/TLS		بروتوكول غير موثوق به يُستخدم مع التطبيقات التي تتطلب تسليما سريعًا للبيانات
٤	DNS		بروتوكولات تشفير توفر اتصالا آمنا عبر الشبكة عن طريق تشفير البيانات المتبادلة بين عميل وخادم
٥	TCP		بروتوكول يقوم بترجمة تسميات النطاقات التي يمكن قراءته إلى عناوين بروتوكول الإنترنت IP
٦	UDP		بروتوكول قياسي لنقل الملفات بين عميل وخادم عبر الشبكة.

تدريب (٢): اختر الإجابة الصحيحة فيما يلي:

١	**هي الترتيب المادي أو المنطقي للأجهزة في الشبكة، وتشمل الهياكل الشائعة للشبكات وهي الهيكل النجمي والحلقي والخطي والهجين :**					
أ	مخططات الشبكة	ب	أجهزة الشبكة	ج	بروتوكولات الشبكة	
٢	**هي الأجهزة التي تعيد توجيه حزم البيانات بين الشبكات المختلفة، وتُحدد المسار الأكثر كفاءة لنقل البيانات :**					
أ	نقاط الوصول	ب	المحولات	ج	الموجهات	
٣	**هي تقنية تُنشئ اتصالاً آمنا ومشفّرًا بين جهاز المستخدم وشبكة أخرى بعيدة غالباً عبر الإنترنت :**					
أ	أنظمة كشف التسلل	ب	الشبكات الافتراضية الخاصة	ج	المناطق العازلة	
٤	**أحد أكثر أدوات تحليل حزم البيانات شيوعا وهو محلل حزم بيانات مفتوح المصدر يُستخدم لفحص تفاصيل حركة البيانات :**					
أ	Wireshark	ب	VPN	ج	DB Browser	
٥	**هي مكونات الأجهزة الأساسية التي تُسهل الاتصال داخل الشبكات مثل: المحولات والموجهات وجدران الحماية ونقاط الوصول :**					
أ	مخططات الشبكة	ب	أجهزة الشبكة	ج	بروتوكولات الشبكة	

تدريب (١): اختر الإجابة الصحيحة فيما يلي:

١	من مراحل سلسلة الهجوم السيبراني وفيها يحدد المهاجمون الأهداف ويكتشفون نقاط الضعف لاستغلالها :				
أ	الاستطلاع	ب	التسليح	ج	الاستغلال
٢	من خطوات التحليل الجنائي الرقمي تشمل تحديد الأدلة الرقمية المحتملة المتعلقة بالحادثة أو بالتحقيق وتوثيقها:				
أ	التوثيق	ب	التعريف	ج	المحافظة
٣	هو التحقيق في أنظمة ملفات النقطة الطرفية لتحديد مؤشرات الاختراق الأمني أو استغلال الثغرات :				
أ	التحليل الجنائي للشبكة	ب	التحليل الجنائي للذاكرة	ج	التحليل الجنائي لنظام الملفات
٤	من خطوات عملية الاستجابة للحوادث وتساعد هذه الخطوة في فهم طبيعة الهجوم وجمع البيانات الأساسية للمزيد من التحليل :				
أ	تحديد النطاق	ب	التامين	ج	التحقيق
٥	من مراحل سلسلة الهجوم السيبراني وفيها يستطيع المهاجم التحكم عن بعد بجهاز أو هوية داخل الشبكة :				
أ	التثبيت	ب	القيادة والتحكم	ج	تحقيق الأهداف
٦	تركز بشكل خاص علي معالجة الحوادث الامنية وفي هذه الحالات يقوم المحققون بإجراءات مختلفة يتعلق بعضها بالتعافي من المشكلة :				
أ	الاستجابة للحوادث	ب	التحليل الجنائي الرقمي	ج	الأمن بدرجة صفة من الثقة
٧	من التحديات الرئيسية للتحليل الجنائي الرقمي :				
أ	تعدد مصادر الأدلة	ب	التحضير والجاهزية	ج	الحد من أثر الحوادث
٨	من خطوات التحليل الجنائي الرقمي فيها يتم فحص الأدلة التي جمعها للكشف عن المعلومات ذات العلاقة :				
أ	التحليل	ب	التعريف	ج	المحافظة
٩	من مراحل سلسلة الهجوم السيبراني وفيها ينشئ المهاجم ناقلاً للهجوم لاستغلال ثغرة معروفة :				
أ	الاستغلال	ب	التسليح	ج	التسليم

تدريب (٢): ضع علامة (✓) أمام العبارة الصحيحة وعلامة (✗) أمام العبارة الخاطئة:

١. تغطي الاستجابة للحوادث قضايا التحقيق ولكنها تركز بشكل خاص على معالجة الحوادث الأمنية.	
٢. فرق الاستجابة لحوادث أمن الحاسب هي مجموعات متخصصة من المهنيين التقنيين وتؤدي دوراً مهماً في حماية شبكات الحاسب وصيانتها واستعادتها بعد تحديد المشكلات الأمنية .	
٣. المرحلة الخامسة من مراحل سلسلة الهجوم السيبراني هي القيادة والتحكم.	
٤. التحليل الجنائي للذاكرة هو التحقيق في أنظمة ملفات النقطة الطرفية .	
٥. تستخدم منهجية سلسلة الهجوم السيبراني لفهم وتحليل الهجمات السيبرانية الضارة.	

معلم المادة: حسام مساعد الثقفي

تدريب (١): ضع علامة (✓) أمام العبارة الصحيحة وعلامة (✗) أمام العبارة الخاطئة:

١. يساعد فهم التشريعات والقوانين الأفراد والمنشآت في تبني دور نشط للحفاظ على الأمن عبر الإنترنت.	
٢. تهدف ضوابط الأمن السيبراني للبيانات إلى رفع مستوى الأمن السيبراني لحماية البيانات الوطنية.	
٣. لا تؤثر قوانين الأمن السيبراني وضوابطه على ثقة العملاء في المنتجات والخدمات.	
٤. يقتصر تطبيق القوانين والضوابط الخاصة بالأمن السيبراني على حماية المنشآت من التهديدات السيبرانية.	
٥. قانون حماية البيانات الشخصية يضع حرج الأساس القانوي لحماية حقوق الأفراد فيما يتعلق بمعالجة البيانات الشخصية.	
٦. يغطي قانون مكافحة جرائم المعلوماتية السعودي كلا من أمن الأفراد وأمن المؤسسات.	

تدريب (٢): اختر الإجابة الصحيحة فيما يلي:

١	يستخدم مفتاحاً واحداً لعمليات التشفير وفك التشفير وتتمثل وظيفته الرئيسة في التحويل والتبديل :						
أ	تشفير المفتاح المتماثل	ب	تشفير المفتاح غير المتماثل	ج	دوال الاختزال		
٢	يتم في هذه الخوارزمية استبدال بسيط للحروف حيث يتم استبدال كل حرف بحرف آخر اعتماداً على مفتاح التشفير :						
أ	خوارزمية تشفير ديفي – هيلمان	ب	خوارزمية تشفير فينجر	ج	خوارزمية تشفير قيصر		
٣	تقنية تشفير تقوم مدخلات ذات طول عشوائي إلى مخرجات بطول ثابت وتكون هذه الدوال أحادية الاتجاه :						
أ	هيئة الشهادات	ب	دوال الاختزال	ج	شبكات الثقة		
٤	هي عقود ذاتية التنفيذ مكتوبة برمجيا، ويتم تنفيذها باستخدام تقنية سلسلة الكتل :						
أ	العقود الذكية	ب	سلسة الكتل	ج	شبكات الثقة		
٥	يتضمن استخدام مفتاحين مختلفين يرتبطان حسابياً وهما المفتاح العام والمفتاح الخاص :						
أ	تشفير المفتاح المتماثل	ب	تشفير المفتاح غير المتماثل	ج	دوال الاختزال		
٦	هي نهج لامركزي يُستخدم في التشفير للتحقق من صحة المفاتيح العامة :						
أ	هيئة الشهادات	ب	دوال الاختزال	ج	شبكات الثقة		
٧	من أمثلة خوارزميات المفاتيح المتماثلة الشائعة :						
أ	خوارزمية معيار التشفير المتقدم	ب	خوارزمية آر إس إيه	ج	خوارزمية ديفي– هيلمان		

تدريب (١): اختر الإجابة الصحيحة فيما يلي:

١	شبكة من الأجهزة المترابطة والمستشعرات تجمع البيانات وتنقلها وتتبادلها مع بعضها :					
أ	أجهزة انترنت الأشياء	ب	المدن الذكية	ج	المركبات ذاتية القيادة	
٢	تتميز بتوفير خدمات الاتصالات والإنترنت بسرعات عالية وزمن وصول أقل وسعة أكبر لتحميل وتبادل البيانات :					
أ	المدن الذكية	ب	شبكات الجيل الخامس	ج	أجهزة إنترنت الأشياء	
٣	تعتمد على تقنيات ومستشعرات متقدمة للعمل دون التحكم البشري في قيادتها :					
أ	أجهزة أنترنت الأشياء	ب	المدن الذكية	ج	المركبات ذاتية القيادة	
٤	هي نسخ افتراضية متماثلة للأصول المادية أو الأنظمة أو العمليات التي يمكن استخدامها للمحاكاة والتحليل والتحسين :					
أ	الميتافيرس	ب	العقود الذكية	ج	التوائم الرقمية	

تدريب (٢): ضع علامة (✓) أمام العبارة الصحيحة وعلامة (✗) أمام العبارة الخاطئة:

١. يمثل تعلم الآلة إحدى طرائق استخدام الذكاء الاصطناعي في الأمن السيبراني.	
٢. يمكن الاستعانة بالذكاء الاصطناعي في الأمن السيبراني من خلال التحليلات التنبؤية.	
٣. لا تقدم الحوسبة السحابية تحديات جديدة للأمن السيبراني.	
٤. لا تتعرض أنظمة الذكاء الاصطناعي وتعلم الآلة للهجمات العدائية .	
٥. تعد العقود الذكية آمنه من أي هجمات محتملة .	
٦. تجمع تطبيقات الواقع المعزز والواقع الافتراضي البيانات الشخصية .	
٧. يمكن للحوسبة الكمية كسر خوارزميات التشفير الحالية	
٨. قد تتأثر المركبات ذاتية القيادة سلباً بالهجمات السيبرانية	