المملكة العربية السعودية

وزارة التعليم
Ministry of Education

قررت وزارة التعليم تدريس
هذا الكتاب وطبعه على نفقتها

الأمن السيبراني

التعليم الثانوي - نظام المسارات

السنة الثالثة

طبعة 1445-2023

يوزع مجاناً ولا يباع
وزارة التعليم
Ministry of Education
2023 - 1445

فهرسة مكتبة الملك فهد الوطنية أثناء النشر
وزارة التعليم
الأمن السيبراني - التعليم الثانوي - نظام المسارات - السنة الثالثة. /
وزارة التعليم .- الرياض، ١٤٤٥ هـ
١٤١ ص ؛ ٢١ x ٢٥,٥ سم
ردمك : ٩٧٨-٦٠٣-٥١١-٥٧٣-٥
١ - الحواسيب - تعليم - السعودية ٢- التعليم الثانوي - السعودية
كتب دراسية أ . العنوان
ديوي ٠٠٤,٠٧ ١٤٤٥ / ١٥٨٣

رقم الإيداع : ١٤٤٥ / ١٥٨٣
ردمك : ٩٧٨-٦٠٣-٥١١-٥٧٣-٥

مواد إثرائية وداعمة على "منصة عين الإثرائية"

ien.edu.sa

أعزاءنا المعلمين والمعلمات، والطلاب والطالبات، وأولياء الأمور، وكل مهتم بالتربية والتعليم:
يسعدنا تواصلكم؛ لتطوير الكتاب المدرسي، ومقترحاتكم محل اهتمامنا.

fb.ien.edu.sa

أخي المعلم/أختي المعلمة، أخي المشرف التربوي/أختي المشرفة التربوية:
نقدر لك مشاركتك التي ستسهم في تطوير الكتب المدرسية الجديدة، وسيكون لها الأثر الملموس في دعم العملية التعليمية، وتجويد ما يقدم لأبنائنا وبناتنا الطلبة.

fb.ien.edu.sa/BE

وزارة التعليم
Ministry of Education
2023 - 1445

الناشر: شركة تطوير للخدمات التعليمية

تم النشر بموجب اتفاقية خاصة بين شركة Binary Logic SA وشركة تطوير للخدمات التعليمية
(عقد رقم 2022/0003) للاستخدام في المملكة العربية السعودية

binarylogic

وزارة التعليم
Ministry of Education
2023 - 1445

مقدمة

إن تقدم الدول وتطورها يقاس بمدى قدرتها على الاستثمار في التعليم، ومدى استجابة نظامها التعليمي لمتطلبات العصر ومتغيراته. وحرصًا من وزارة التعليم على ديمومة تطوير أنظمتها التعليمية، واستجابة لرؤية المملكة العربية السعودية 2030 فقد بادرت الوزارة إلى اعتماد نظام «مسارات التعليم الثانوي» بهدف إحداث تغيير فاعل وشامل في المرحلة الثانوية.

إن نظام مسارات التعليم الثانوي يقدم أنموذجًا تعليميًا متميزًا وحديثًا للتعليم الثانوي بالمملكة العربية السعودية يسهم بكفاءة في:

- تعزيز قيم الانتماء لوطننا المملكة العربية السعودية، والولاء لقيادته الرشيدة حفظهم الله، انطلاقًا من عقيدة صافية مستندة على التعاليم الإسلامية السمحة.
- تعزيز قيم المواطنة من خلال التركيز عليها في المواد الدراسية والأنشطة، اتساقًا مع مطالب التنمية المستدامة، والخطط التنموية في المملكة العربية السعودية التي تؤكد على ترسيخ ثنائية القيم والهوية، والقائمة على تعاليم الإسلام والوسطية.
- تأهيل الطلبة بما يتوافق مع التخصصات المستقبلية في الجامعات والكليات أو المهن المطلوبة؛ لضمان اتساق مخرجات التعليم مع متطلبات سوق العمل.
- تمكين الطلبة من متابعة التعليم في المسار المفضل لديهم في مراحل مبكرة، وفق ميولهم وقدراتهم.
- تمكين الطلبة من الالتحاق بالتخصصات العلمية والإدارية النوعية المرتبطة بسوق العمل، ووظائف المستقبل.
- دمج الطلبة في بيئة تعليمية ممتعة ومحفزة داخل المدرسة قائمة على فلسفة بنائية، وممارسات تطبيقية ضمن مناخ تعليمي نشط.
- نقل الطلبة عبر رحلة تعليمية متكاملة بدءًا من المرحلة الابتدائية حتى نهاية المرحلة الثانوية، وتُسهِّل عملية انتقالهم إلى مرحلة ما بعد التعليم العام.
- تزويد الطلبة بالمهارات التقنية والشخصية التي تساعدهم على التعامل مع الحياة، والتجاوب مع متطلبات المرحلة.
- توسيع الفرص أمام الطلبة الخريجين عبر خيارات متنوعة إضافة إلى الجامعات مثل: الحصول على شهادات مهنية، والالتحاق بالكليات التطبيقية، والحصول على دبلومات وظيفية.

ويتكون نظام المسارات من تسعة فصول دراسية تُدرّس في ثلاث سنوات، تتضمن سنة أولى مشتركة يتلقى فيها الطلبة الدروس في مجالات علمية وإنسانية متنوعة، تليها سنتان تخصصيتان، يُسكّن الطلبة بها في مسار عام وأربعة مسارات تخصصية تتسق مع ميولهم وقدراتهم، وهي: المسار الشرعي، مسار إدارة الأعمال، مسار علوم الحاسب والهندسة، مسار الصحة والحياة، وهو ما يجعل هذا النظام هو الأفضل للطلبة من حيث:

- وجود مواد دراسية جديدة تتوافق مع متطلبات الثورة الصناعية الرابعة والخطط التنموية، ورؤية المملكة 2030، تهدف لتنمية مهارات التفكير العليا وحل المشكلات، والمهارات البحثية.
- برامج المجال الاختياري التي تتسق مع احتياجات سوق العمل وميول الطلبة، حيث يُمكّن الطلبة من الالتحاق بمجال اختياري محدد وفق مصفوفة مهارات وظيفية محددة.
- مقياس ميول يضمن تحقيق كفاءة الطلبة وفاعليتهم، ويساعدهم في تحديد اتجاهاتهم وميولهم، وكشف مكامن القوة لديهم، مما يعزز من فرص نجاحهم في المستقبل.
- العمل التطوعي المصمم للطلبة خصيصًا بما يتسق مع فلسفة النشاط في المدارس، ويعد أحد متطلبات التخرج؛ مما يساعد على تعزيز القيم الإنسانية، وبناء المجتمع وتنميته وتماسكه.
- التجسير الذي يمكن الطلبة من الانتقال من مسار إلى آخر وفق آليات محددة.
- حصص الإتقان التي يتم من خلالها تطوير المهارات وتحسين المستوى التحصيلي، من خلال تقديم حصص إتقان إثرائية وعلاجية.

- خيارات التعليم المدمج، والتعلم عن بعد، والذي بُني في نظام المسارات على أسس من المرونة، والملاءمة والتفاعل والفعالية.
- مشروع التخرج الذي يساعد الطلبة على دمج الخبرات النظرية مع الممارسات التطبيقية.
- شهادات مهنية ومهارية تمنح للطلبة بعد إنجازهم مهامَّ محددة، واختبارات معينة بالشراكة مع جهات تخصصية.

وبالتالي فإن مسار علوم الحاسب والهندسة كأحد المسارات المستحدثة في المرحلة الثانوية يسهم في تحقيق أفضل الممارسات عبر الاستثمار في رأس المال البشري، وتحويل الطالب إلى فرد مشارك ومنتج للعلوم والمعارف، مع إكسابه المهارات والخبرات اللازمة لاستكمال دراسته في تخصصات تتناسب مع ميوله وقدراته أو الالتحاق بسوق العمل.

وتُعدُّ مادة الأمن السيبراني أحد المواد الرئيسة في مسار علوم الحاسب والهندسة التي تقدم في كتاب شامل، حيث تسهم في توضيح مفاهيم الأمن السيبراني والتقنيات المرتبطة به، وذلك مع التركيز بشكل خاص على التهديدات السيبرانية واستراتيجيات الحد منها. وتهدف المادة إلى تعريف الطالب بأهمية الأمن السيبراني في مختلف الصناعات، والقطاعات المالية، ومؤسسات الرعاية الصحية، والهيئات الحكومية، كما تغطي أساسيات الأمن السيبراني بما في ذلك تقييم المخاطر، وأمن البرمجيات والشبكات، والاستجابة للحوادث، ويوفر الكتاب تمارين عملية لتعزيز فهم الطالب لمفهوم التشفير، كما يؤكد الكتاب على أهمية توعية المُستخدِم، والكشف الاستباقي عن التهديدات، واستخدام الأدوات الرقمية في حماية الأفراد والمنظمات.

ويتميز كتاب الأمن السيبراني بأساليب حديثة، تتوافر فيه عناصر الجذب والتشويق، والتي تجعل الطلبة يقبلون على تعلمه والتفاعل معه، من خلال ما يقدمه من تدريبات وأنشطة متنوعة، كما يؤكد هذا الكتاب على جوانب مهمة في تعليم الأمن السيبراني وتعلمه، تتمثل في:

- الترابط الوثيق بين المحتويات والتهديدات السيبرانية الواقعية.
- تنوع طرائق عرض المحتوى بصورة جذابة ومشوقة.
- إبراز دور المتعلم في عمليات التعليم والتعلم.
- الاهتمام بترابط محتوياته مما يجعل منه كلًّا متكاملًا.
- الاهتمام بتوظيف التقنيات المناسبة في المواقف المختلفة.
- الاهتمام بتوظيف أساليب متنوعة في تقويم الطلبة بما يتناسب مع الفروق الفردية بينهم.

ولمواكبة التطورات العالمية في هذا المجال، فإن كتاب مادة الأمن السيبراني سوف يوفر للمعلم مجموعة متكاملة من المواد التعليمية المتنوعة التي تراعي الفروق الفردية بين الطلبة، بالإضافة إلى البرمجيات والمواقع التعليمية، التي توفر للطلبة فرصة توظيف التقنيات الحديثة والتواصل المبني على الممارسة؛ مما يؤكد دوره في عملية التعليم والتعلم.

ونحن إذ نقدم هذا الكتاب لأعزائنا الطلبة، نأمل أن يستحوذ على اهتمامهم، ويُلبي متطلباتهم، ويجعل تعلّمهم لهذه المادة أكثر متعة وفائدة.

والله ولي التوفيق

بسم الله الرحمن الرحيم

وزارة التعليم
Ministry of Education
2023 - 1445

الفهرس

وزارة التعليم
Ministry of Education
2023 - 1445

1. أساسيات الأمن السيبراني

سيتعرف الطالب في هذه الوحدة على المفاهيم الأساسية للأمن السيبراني، وعلى مراحل تطوره والدور الذي يلعبه في العالَم المعاصر، كما سيتعرف على المخاطر والثغرات الأمنيّة الموجودة في الأنظمة التّقنية، وعلى استراتيجيات الاستجابة لتلك المخاطر ومواجهتها، وفي الختام سيتعرف على حماية البيانات في الأمن السيبراني، وكيفية تنفيذ التحكم بالوصول لحماية أنظمة المعلومات، وكذلك على دور القرصنة الأخلاقية في حماية المؤسسات والشركات.

أهداف التعلُّم

بنهاية هذه الوحدة سيكون الطالب قادرًا على أن:

- يوضِّح المقصود بمجال الأمن السيبراني وتاريخه.
- يُعدِّد المبادئ الأساسية للأمن السيبراني.
- يُحلِّل الأدوار الوظيفية الرئيسة في الأمن السيبراني.
- يتعرّف على النشأة الرّائدة للمملكة العربية السعودية في مجال الأمن السيبراني.
- يُعدِّد الفئات المختلفة للبرمجيات الضارة.
- يُوضِّح كيفية عمل الهجمات السيبرانية.
- يُقيِّم الاستراتيجيات المختلفة لتحديد المخاطر وكيفية الحدّ منها وإدارتها.
- يُحدِّد كيف تساعد تقنيات التحكم بالوصول في حماية أنظمة المعلومات.
- يشرح دور القرصنة الأخلاقية في مجال الأمن السيبراني.

رابط الدرس الرقمي

www.ien.edu.sa

الدرس الأول

مقدمة في الأمن السيبراني

ما المقصود بالأمن السيبراني؟ What is Cybersecurity

أضحى مجال الأمن السيبراني مهمًا بشكل متزايد في السنوات الأخيرة، خاصةً مع الاندماج الكبير للتقنية في الحياة اليومية؛ فمَع ظهور الإنترنت وانتشار أجهزة الحاسب والأجهزة المحمولة، أصبح الأمن السيبراني ضروريًا لحماية المعلومات الحساسة وضمان حماية الأنشطة عبر الإنترنت وأمنها، حيث يشمل مجال الأمن السيبراني مجموعة من الممارسات والتقنيات المصمَّمة للحماية من التهديدات والهجمات السيبرانية.

تأسست **الهيئة الوطنية للأمن السيبراني** (National Cybersecurity Authority – NCA) في المملكة العربية السعودية بموجب أمر ملكي، وذلك كجهة مختصة بالأمن السيبراني، والمرجع الوطني في شؤونه، حيث يتم تعريف الأمن السيبراني حسب تنظيم الهيئة الوطنية للأمن السيبراني كما يلي:

هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

تمثِّل الطبيعة المتطورة والمتغيِّرة للتهديدات السيبرانية التحدي الرئيس للأمن السيبراني، حيث يتغيَّر هذا المجال بشكل مستمر، ولذلك يحتاج المختصون إلى تطوير إجراءاتهم الأمنيّة باستمرار لمواكبة هذه التغييرات، ويتضمن الأمن السيبراني مجالات مختلفة مثل: أمن البيانات، وأمن الشبكات، والتشفير، وإدارة المخاطر السيبرانية. وبسبب طبيعة مجال الأمن السيبراني الذي يشمل عددًا من التخصصات البينية فإن العمل فيه يُعدُّ تحديًا مثيرًا لتقديمه العديد من فُرص التعلُّم والتقدم الوظيفي.

تُعدُّ حماية البيانات والمعلومات أمرًا ضروريًا، وكذلك تدابير الأمن السيبراني ضرورية للحماية من الهجمات السيبرانية، فقد تتعرض البيانات الشخصية والمعلومات المالية والملكية الفكرية للخطر بسبب هذه الهجمات، وقد تكون العواقب الناجمة عن أي هجوم سيبراني ناجح وخيمة للغاية، وبشكل خاص عند تسببها بخسائر مالية للأفراد، حيث تؤدي أغلب الهجمات السيبرانية الناجحة إلى سرقة الأموال أو الأصول

تهديدات الأمن السيبراني (Cybersecurity Threats):

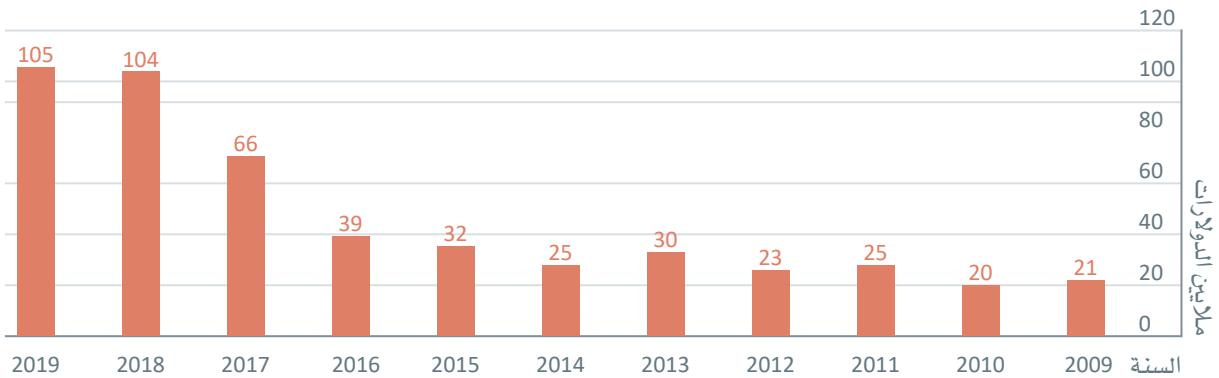
تتمثّل هذه التهديدات في أيّ ظرف أو حدث قد يؤثر سلبًا على العمليات، أو الأصول التنظيمية، أو الأفراد من خلال نظام معلومات عبر الوصول غير المُصرَّح به، أو التخريب والإفصاح عن المعلومات وتغييرها، أو حجب الخدمة.

الهجمات السيبرانية (Cybersecurity Attacks):

هي إجراء يقوم به طرف معيَّن ذو نوايا سيئة بهدف الإتلاف، أو التعطيل، أو الوصول غير المُصرَّح به إلى أنظمة الحاسب أو الشبكات أو البيانات.

القَيِّمة الأخرى، وبالنسبة للشركات، فالعواقب المالية لهذا الهجوم تكون أكثر خطورة، مع خسائر محتملة بملايين الدولارات. يُمكن أن يؤدي الهجوم السيبراني إلى الإضرار بالسمعة، وقد يصعب تجاوز ذلك الضرر بسهولة، حيث يفقد المستهلكون والعملاء الثقة في الأعمال التجارية التي تعرضت لهذا الهجوم، وقد تؤدّي هذه الهجمات أيضًا إلى مسؤوليات قانونية معقدة، فقد تتحمل الشركات المسؤولية عن أي أضرار إذا تم اختراق البيانات الحساسة لديها. ويمكن أن تشكّل هذه الهجمات تهديدًا للأمن القومي للدول، حيث تتعرض الحكومات والمؤسسات العسكرية والأمنيّة في الدول لخطر الهجمات السيبرانية التي يُمكنها تعطيل البنية التحتية الحيوية أو سرقة البيانات الحساسة، ويُمكن أن يؤدي الهجوم الناجح إلى فقدان أسرار الدولة أو استراتيجياتها العسكرية، مما قد يتسبب بعواقب وخيمة.

يُعدُّ الأمن السيبراني ضروريًا للأفراد أيضًا، فمع ظهور الخدمات المصرفية الرقمية، وتوسُّع التجارة الإلكترونية، أصبحت المعلومات المالية الشخصية معرضة لخطر السرقة، كما يُمكن أيضًا سرقة البيانات الشخصية مثل: **معلومات التعريف الشخصية** (Personal Identifiable Information – PII)، والعناوين، وأرقام الهواتف لاستخدامها في عمليات انتحال الهوية، ويمكن لتدابير الأمن السيبراني مثل: كلمات المرور القوية، والمصادقة الثنائية أن تساعد في حماية الأفراد من هذه التهديدات.



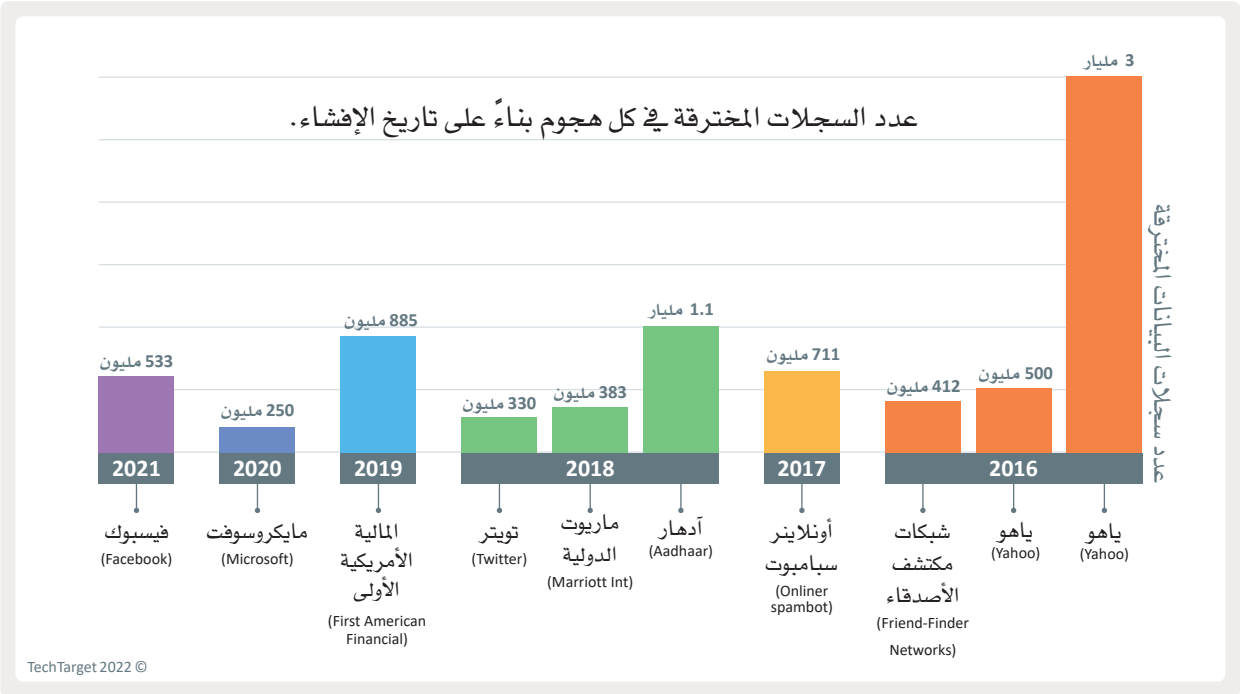
شكل 1.1: حوادث لهجمات سيبرانية مبلّغ عنها في العقد الماضي، تجاوزت خسائرها ملايين الدولارات حسب بيانات مركز الدراسات الاستراتيجية والدولية (Center for Strategic & International Studies – CSIS)

تاريخ الأمن السيبراني History of Cybersecurity

يرجع تاريخ الأمن السيبراني إلى السبعينيات من القرن العشرين، عندما تم تطوير شبكات الحوسبة، حيث ظهرت فيروسات الحاسب في العام 1986، وتسببت بتلف البيانات والأنظمة، ولذلك تم تطوير جُدران الحماية والتشفير لمكافحة الهجمات السيبرانية، حيث تتحكم جُدران الحماية في حركة البيانات ويحمي التشفير البيانات والمعلومات. وعلى الرغم من التطور المستمر في أنظمة الحماية الجديدة، إلا أن مُرتكبي الجرائم السيبرانية يجدون طرائقَ لتجاوزها.

لقد شهد القرن الحادي والعشرون زيادة كبيرة في الهجمات السيبرانية واسعة النطاق والتي عرَّضت الحكومات والشركات والأفراد للخطر، ومن أشهر أمثلة تلك الهجمات: خرق بيانات مؤسسة **إكويفاكس** (Equifax) عام 2017 الذي كشف البيانات الشخصية لأكثر من 140 مليون شخص، وهجوم **سولارويندز** (SolarWinds) عام 2020 الذي أثّر على العديد من الوكالات الحكومية الأمريكية والشركات الخاصة، ويوضِّح الشكل 1.2 بعض أكبر خروقات البيانات في التاريخ، ومع تقدُّم التقنية واندماجها المتزايد في الحياة، تتزايد الحاجة إلى الأمن السيبراني.

وفي السنوات الماضية، انتشر التعليم والتوعية بمجال الأمن السيبراني على نطاق واسع، وقد طوَّرت الحكومات والمؤسسات أُطُر عمل وإرشادات خاصة بهذا المجال لمساعدة الأفراد والشركات على حماية أنفسهم من التهديدات السيبرانية، وتزايد الطلب على متخصصي الأمن السيبراني، وتنوعت فرص العمل المتعلقة بهذا المجال، ومع ازدياد تعقيد الهجمات السيبرانية، تستمر الحاجة إلى المتخصصين المهرة الذين يُمكنهم مواجهة هذه الهجمات.



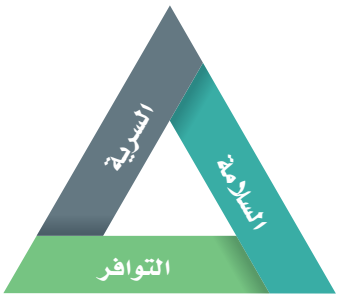
شكل 1.2: عشرة من أكبر خروقات البيانات في التاريخ بناءً على بحث تك تارجيت (TechTarget)

المبادئ الأساسية للأمن السيبراني Key Principles of Cybersecurity

تُعدُّ حماية أنظمة الحاسب والشبكات والبيانات من الوصول غير المُصرَّح به والأنشطة الضارة أمرًا بالغ الأهمية، فمن الضروري الالتزام بالمبادئ الأساسية للأمن السيبراني لإنشاء إطار أمني قوي وفعّال، كما يُعدُّ فهم هذه المبادئ وتنفيذها أمرًا حيويًا لحماية المعلومات الحساسة، وضمان دقة البيانات، والحفاظ على الوصول غير المنقطع إلى الموارد الهامة.

فيما يلي عرض لهذه المبادئ الأساسية:

السرية والسلامة والتوافر (مثلث أمن المعلومات)
Confidentiality, Integrity, and Availability (The CIA Triad)



شكل 1.3: مثلث أمن المعلومات

مثلث أمن المعلومات (The CIA Triad) هو نموذج مُستخدَم على نطاق واسع لتصميم سياسات وممارسات الأمن السيبراني وتنفيذها، حيث يشير الاختصار CIA إلى **السرية** (Confidentiality – C) و**السلامة** (Integrity – I) و**التوافر** (Availability – A)، وهي الأهداف الرئيسة الثلاثة لحماية المعلومات والأنظمة من الوصول غير المصرَّح به أو التغيير أو الانقطاع.

تشير **السرية** (Confidentiality) إلى الحفاظ على القيود المُصرَّح بها للوصول إلى المعلومات، أي عدم السماح بالوصول للبيانات لمن لا يحق لهم الوصول إليها، ويُمكن الحفاظ على السرية من خلال طرائق مختلفة مثل: التشفير، والتحكم في الوصول، وإخفاء البيانات. وتواجه السرية تهديدات محتملة مثل: هجمات التصيد الإلكتروني، حيث ينتحل المهاجمون شخصيات كيانات شرعية لخداع الأفراد والحصول على معلومات حساسة.

تشير **السلامة** (Integrity) إلى توكيد دقة البيانات وعدم التلاعب بها، حيث إن سلامة البيانات ضرورية للحفاظ على الثقة في أنظمة المعلومات، فبدونها لا يُمكن للمُستخدِمين الوثوق بدقة المعلومات التي يتلقونها، ويُمكن أن تساعد إجراءات

مثل: التشفير والتوقيعات الرقمية في ضمان سلامة البيانات، ويُعدُّ اعتراض البيانات بين طرفين من الأمثلة الشائعة على تهديدات سلامة البيانات، حيث يُمكن للمهاجِم من خلال اعتراض البيانات التسلل إلى شبكة **واي فاي** (Wi-Fi) اللاسلكية غير الآمنة والتلاعب بحزم البيانات التي يتم إرسالها، وتغيير المحتوى دون علم المُرسِل أو المُستلِم.

يشير **التوافر** (Availability) إلى ضمان إمكانية الوصول إلى المعلومات عند الحاجة، ويُعدُّ ضروريًا لضمان إتاحة الأنظمة والخدمات للمُستخدِمين عند الحاجة، كما يُمكن أن يساعد تخزين نُسخ متعددة من البيانات، وعمل النسخ الاحتياطية، ووضع خُطط استعادة القدرة على العمل بعد الكوارث في ضمان التوافر. تُعدُّ هجمات **حجب الخدمة** (Denial of Service – DoS) طريقة شائعة للمهاجِمين لعرقلة توافر البيانات؛ وذلك بإغراق الشبكة بحركة كميات كبيرة من البيانات مما يتسبب في توقف العمليات.

التوقيع الرقمي (Digital Signature):
التوقيع الرقمي هو أحد أنواع التوقيع الإلكتروني يستخدِم خوارزميات رياضية للتحقق من صحة رسالة أو مستند أو معاملة وسلامتها.

الأدوار الوظيفية في الأمن السيبراني Job Roles in Cybersecurity

يقدِّم مجال الأمن السيبراني مجموعة واسعة من فرص العمل للأفراد ذوي الخلفيات والمهارات المختلفة، حيث تتنوع هذه الفرص بين الأدوار التقنية مثل: محلِّلي الأمن السيبراني، وأخصائيي اختبار الاختراقات، والأدوار الإدارية مثل: **رئيس إدارة الأمن السيبراني** (Chief Information Security Officer – CISO)، وهناك مجموعة متنوعة من الأدوار الوظيفية في الأمن السيبراني تناسب الرغبات المختلفة والأهداف المهنية، بالإضافة إلى الأدوار الفنية والإدارية، هناك أيضًا فرص عمل خاصة بسياسات وحوكمة الأمن السيبراني مثل: مستشاري الأمن السيبراني وأخصائيي الالتزام في الأمن السيبراني، ويزداد تنوع الأدوار الوظيفية والمسارات المهنية في هذا المجال مع استمرار تزايد الطلب على متخصصي الأمن السيبراني، حيث أدى العجز الكبير في متخصصي الأمن السيبراني محليًا وعالميًا إلى جعل هذا المجال من أكثر المجالات الوظيفية المستقبلية المطلوبة وأهمها، وفيما يلي بيان للأدوار الوظيفية الرئيسة في الأمن السيبراني كما وردت في **الإطار السعودي لكوادر الأمن السيبراني (سيوف)** (Saudi Cybersecurity Workforce Framework – SCyWF).

تصنيف الإطار السعودي لكوادر الأمن السيبراني (سيوف) The SCyWF Taxonomy

الفئات الوظيفية	مجال التخصص	الأدوار الوظيفية
معمارية الأمن السيبراني والبحث والتطوير (CARD)	معمارية الأمن السيبراني (CA)	• مُصمِّم معمارية الأمن السيبراني. • أخصائي الحوسبة السحابية الآمنة.
	البحث والتطوير في الأمن السيبراني (CRD)	• أخصائي تطوير أمن النُظم. • مُطوِّر الأمن السيبراني. • مُقيِّم البرمجيات الآمنة. • باحث الأمن السيبراني. • أخصائي علم البيانات للأمن السيبراني. • أخصائي الذكاء الاصطناعي للأمن السيبراني.

الفئات الوظيفية	مجال التخصص	الأدوار الوظيفية
القيادة وتطوير الكوادر (LWD)	القيادة (L)	• رئيس إدارة الأمن السيبراني. • مدير الأمن السيبراني. • مستشار الأمن السيبراني.
	تطوير الكوادر (WD)	• مدير الموارد البشرية للأمن السيبراني. • مُطوِّر المناهج التعليمية للأمن السيبراني. • مُدرِّب الأمن السيبراني.
الحوكمة والمخاطر والالتزام والقوانين (GRCL)	الحوكمة والمخاطر والالتزام (GRC)	• أخصائي مخاطر الأمن السيبراني. • أخصائي الالتزام في الأمن السيبراني. • أخصائي سياسات الأمن السيبراني. • مُقيِّم ضوابط الأمن السيبراني. • مدقِّق الأمن السيبراني.
	القوانين وحماية البيانات (LDP)	• أخصائي قانون الأمن السيبراني. • أخصائي الخصوصية وحماية البيانات.
الحماية والدفاع (PD)	الدفاع (D)	• مُحلِّل دفاع الأمن السيبراني. • أخصائي البنية التحتية للأمن السيبراني. • أخصائي الأمن السيبراني.
	الحماية (P)	• أخصائي التشفير. • أخصائي إدارة الهوية والوصول. • مُحلِّل أمن النُظم.
	تقييم الثغرات (VA)	• أخصائي تقييم الثغرات. • أخصائي اختبار الاختراقات.
	الاستجابة للحوادث (IR)	• أخصائي استجابة للحوادث السيبرانية. • أخصائي التحليل الجنائي الرقمي. • أخصائي تحقيقات الجرائم السيبرانية. • أخصائي الهندسة العكسية للبرمجيات الضارة.
	إدارة التهديدات (TM)	• مُحلِّل معلومات التهديدات السيبرانية. • أخصائي اكتشاف التهديدات السيبرانية.

الفئات الوظيفية	مجال التخصص	الأدوار الوظيفية
أنظمة التحكم الصناعي والتقنيات التشغيلية (ICS / OT)	أنظمة التحكم الصناعي والتقنيات التشغيلية (ICS / OT)	• مُصمِّم معمارية الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية. • أخصائي البنية التحتية للأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية. • مُحلِّل دفاع الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية. • أخصائي مخاطر الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية. • أخصائي استجابة للحوادث السيبرانية لأنظمة التحكم الصناعي والتقنيات التشغيلية.

الأمن السيبراني في المملكة العربية السعودية Cybersecurity in Saudi Arabia

أصبحت المملكة العربية السعودية من أهم الدول الرائدة على مستوى العالم في مجال الأمن السيبراني، فهي تحتل المرتبة الثانية في **المؤشر العالمي للأمن السيبراني** (Global Cybersecurity Index – GCI) الذي يُعدُّ بمثابة مرجع دولي موثوق يقيس التزام الدول بالأمن السيبراني على المستوى العالمي، ويهتم بزيادة الوعي بأهمية الأمن السيبراني وأبعاده المختلفة. نظرًا للنطاق الواسع للتطبيقات المختلفة في الأمن السيبراني، والتي تشمل الصناعات والقطاعات المختلفة، يتم تقييم مستوى التنمية أو التطور لكل دولة بناءً على خمس ركائز أساسية : (1) التدابير القانونية، (2) التدابير التقنية، (3) التدابير التنظيمية، (4) تنمية القدرات، (5) التعاون، ثم تجميعها في نتيجة إجمالية، وقد احتلت المملكة العربية السعودية أيضًا المرتبة الثانية عالميًا في **الكتاب السنوي للتنافسية العالمية** (World Competitiveness Yearbook-WCY) لعام 2023 الصادر عن **المعهد الدولي للتنمية الإدارية** (International Institute for Management Development-IMD) ومقره سويسرا.

الهيئة الوطنية للأمن السيبراني National Cybersecurity Authority

الهيئة الوطنية للأمن السيبراني (NCA) هي الجهة المختصة بالأمن السيبراني في المملكة والمرجع الوطني في شؤونه، وتهدف إلى تعزيزه؛ حماية للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز SAFCSP

الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز هو مؤسسة وطنية تهدف إلى تمكين القوى العاملة المحلية وتعزيز قدراتها في مجالات الأمن السيبراني، وتطوير البرمجيات، والطائرات المُسيَّرة والتقنيات المتقدِّمة بناءً على أفضل الممارسات الدولية.

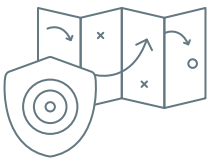
الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY, PROGRAMMING & DRONES

المبادرات المهنية للأمن السيبراني في المملكة العربية السعودية
Cybersecurity Career Initiatives in Saudi Arabia

تتخذ المملكة العربية السعودية خطوات مهمة لتلبية الحاجة إلى وظائف وخبرات الأمن السيبراني في البلاد، ونستعرض فيما يلي مبادرات المملكة في هذا المجال:

التعليم والتدريب

استثمرت الحكومة السعودية بشكل كبير في مجال برامج التعليم والتدريب في الأمن السيبراني لتطوير القدرات المحلية، حيث تقدِّم العديد من الجامعات والمعاهد في المملكة العربية السعودية برامج متخصصة للحصول على درجات علمية وشهادات في هذا المجال، كما أطلقت الحكومة مبادرات تدريبية لتطوير مهارات متخصصي تقنية المعلومات في مجال الأمن السيبراني، ومن الأمثلة على هذه البرامج: برامج الأكاديمية الوطنية للأمن السيبراني التي لها العديد من المسارات، وتهدف إلى تطوير وبناء القدرات الوطنية في هذا المجال، وتوطين محتوى التدريب في مجالات الأمن السيبراني، ويوفِّر **الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز** (SAFCSP) معسكرات تدريبية ومسابقات في مجال الأمن السيبراني، كما أصدرت **الهيئة الوطنية للأمن السيبراني** (NCA) **الإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم)** (Saudi Cybersecurity Higher Education Framework – SCyber_Edu) بهدف ضمان جودة التعليم العالي للأمن السيبراني في المملكة العربية السعودية، ويحدِّد هذا الإطار الحد الأدنى من المتطلبات لبرامج التعليم العالي في هذا المجال لضمان مواءمة نتائج التعلُّم مع الاحتياجات الوطنية للقوى العاملة في مجال الأمن السيبراني.

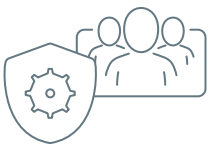


استراتيجية الأمن السيبراني

طوَّرت المملكة العربية السعودية استراتيجية وطنية شاملة للأمن السيبراني تحدِّد رؤية المملكة وأهدافها في هذا المجال، وتتضمن تلك الاستراتيجية خُططًا لتطوير القدرات الوطنية للأمن السيبراني داخل المملكة، بالإضافة إلى تدابير لحماية البنية التحتية الحيوية ولتعزيز التعاون الدولي في هذا المجال.

الشراكات الصناعية

تعمل الحكومة السعودية أيضًا بشكل وثيق مع شركات القطاع الخاص لتلبية الحاجة إلى الخبرات في مجال الأمن السيبراني، فعلى سبيل المثال: دخلت الحكومة في شراكة مع شركات دولية لتوفير برامج التدريب والتطوير لمتخصصي الأمن السيبراني.



تطوير قطاع الأمن السيبراني

لدى المملكة العربية السعودية العديد من المبادرات لتسريع تطوير قطاع الأمن السيبراني ونموه وبناء قدراته في المملكة، وتشمل هذه المبادرات البرنامج الوطني **سايبرك** (CyberIC) الذي يُعدُّ مظلة للعديد من المبادرات مثل: **التمارين الوطنية السيبرانية** (National Cyber Drills)، ومبادرات التدريب على الأمن السيبراني التي تستهدف فئات مختلفة من المجتمع، وتحديات الأمن السيبراني لتشجيع الابتكار وريادة الأعمال في هذا المجال، وكذلك تشجيع منظومة القدرات المحلية في الأمن السيبراني وربط الشركات الناشئة في تقنيات الأمن السيبراني بالمستثمرين.

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. تم تطوير جُدران الحماية والتشفير لمكافحة الهجمات السيبرانية المتزايدة.	○	○
2. تُعدُّ الوكالات الحكومية من الأهداف الرئيسة للهجمات السيبرانية.	○	○
3. جميع الجرائم الإلكترونية لها نفس المستوى من الخطورة والعواقب.	○	○
4. السرية والسلامة والمصادقة تُشكِّل مثلث أمن المعلومات.	○	○
5. الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز هو مؤسسة وطنية تهدف إلى تدريب المواهب المحلية في مجال الذكاء الاصطناعي.	○	○
6. تشير السلامة إلى التأكد من دقة البيانات وعدم التلاعب بها.	○	○
7. يُعدُّ التشفير والتحكم في الوصول وإخفاء البيانات من الطرائق المستخدَمة للحفاظ على سرية البيانات.	○	○
8. تضمن السرية أن البيانات دقيقة ولم يتم التلاعب بها.	○	○
9. يُعدُّ رئيس إدارة الأمن السيبراني (CISO) مسؤولًا تنفيذيًا يشرف على برنامج الأمن السيبراني لمؤسسة معيَّنة.	○	○
10. يؤدّي رئيس إدارة الأمن السيبراني دورًا وظيفيًا في الأمن السيبراني.	○	○

2 اكتب وصفًا موجزًا لمجال الأمن السيبراني حسب ما يتطابق مع تعريف الهيئة الوطنية للأمن السيبراني.

3 صِفْ ما يمثله مثلث أمن المعلومات (CIA Triad) في مجال الأمن السيبراني.

4 وضِّح كيف تساعد السرية في حماية المعلومات الحساسة.

5 اشرح سبب أهمية التوافر لضمان إمكانية وصول المُستخدِمين إلى الأنظمة والخدمات.

6 حلِّل المبادرات المهنية الرئيسة لمجال الأمن السيبراني في المملكة العربية السعودية.

7 اشرح كيف أصبحت المملكة العربية السعودية واحدة من الدول الرائدة في تطوير أنظمة الأمن السيبراني وتشريعاته.

رابط الدرس الرقمي

www.ien.edu.sa

الدرس الثاني

مخاطر الأمن السيبراني وثغراته

مُقدِّمة في المخاطر والثغرات

Introduction to Risks and Vulnerabilities

يطلق لفظ الثغرات في الأمن السيبراني على نقاط الضعف في أنظمة الحاسب والشبكات والأجهزة التي يُمكن لمُرتكبي الجرائم السيبرانية استغلالها لتنفيذ أنشطة ضارة، وقد تظهر الثغرات في الأمن السيبراني نتيجة أخطاء برمجية، أو قصور في إعدادات الأنظمة، أو بسبب أخطاء بشرية.

قد تنطوي هجمات الأمن السيبراني على عواقب وخيمة، بما فيها سرقة البيانات والخسارة المالية والإضرار بالسمعة، و لذلك يجب أن يكون الأفراد والمؤسسات على دراية تامة بالتهديدات المحتملة للأمن السيبراني، وتحديد الثغرات الموجودة، وتحديد المخاطر المحتملة، وتنفيذ تدابير أمن سيبراني قوية لحماية تلك الأنظمة.

الهجمات السيبرانية هي أنشطة ضارة يقوم بها مُرتكبي الجرائم السيبرانية من خلال استغلال الثغرات الأمنيّة في أنظمة الحاسب والشبكات والأجهزة، وتأتي الهجمات السيبرانية بأشكال متعددة، ويُمكن تصنيفها إلى فئات مختلفة بناءً على التقنيات التي يستخدمها المهاجِم لاختراق النظام.

قد تتنوع الجهات المسؤولة عن تهديدات الأمن السيبراني والهجمات السيبرانية، ويُمكن تصنيفها على نطاق واسع بناءً على قدراتها ومواردها وأساليبها ودوافعها، ويوضِّح الجدول 1.1 بعض هذه الأنواع.

أصول الأمن السيبراني (Cybersecurity Assets):

أصول الأمن السيبراني هي أي شيء ذو قيمة لفرد أو مؤسسة أو دولة يُمكنه أن يتأثر سلبًا بهجوم سيبراني ضار.

ثغرات الأمن السيبراني (Cybersecurity Vulnerabilities):

ثغرات الأمن السيبراني هي نقاط ضعف في نظام حاسب أو شبكة أو تطبيق يُمكن استغلالها من قبل الجهات الخبيثة لإحداث ضرر، أو الحصول على وصول غير مُصرَّح به إلى البيانات الحساسة.

مخاطر الأمن السيبراني (Cybersecurity Risks):

تتعلق مخاطر الأمن السيبراني بفقدان السرية أو السلامة، أو توافر المعلومات أو البيانات أو نُظم المعلومات (أو نُظم التحكم)، وتعكس الآثار السلبية المحتملة على ممتلكات وعمليات الأفراد والمؤسسات والمجتمع بأكمله.

جدول 1.1: أنواع الجهات المسؤولة عن الهجمات السيبرانية

النوع	الوصف
جهات على مستوى دولي	وهي مجموعات متطورة غالبًا ما تكون تابعةً لجيش أو جهاز مخابرات لدولة معيَّنة، وتنفّذ هجمات سيبرانية للحصول على ميزة استراتيجية، أو للتجسس، أو لتعطيل البنية التحتية الحيوية، أو لنشر معلومات مضللة، ويُمكن أن تكون دوافعها سياسية أو اقتصادية أو عسكرية.

النوع	الوصف
مجموعات الجريمة المنظمة	تتكون من مجرمين محترفين ينفذون هجمات سيبرانية لتحقيق مكاسب مالية، وغالبًا ما تستخدِم هذه الفئة تكتيكات مثل: برمجيات الفدية، وسرقة الهوية، وانتحال الشخصية، والاحتيال على بطاقات الائتمان، وأنواع أخرى من الجرائم الإلكترونية، ويكون دافعهم الأساسي ماليًّا.
النشطاء المخترقين (Hacktivists)	هم أفراد أو مجموعات يستخدِمون القرصنة للترويج لقضية سياسية أو اجتماعية، وغالبًا ما ينخرطون في أنشطة مثل: تشويه مواقع ويب معيَّنة، أو إجراء هجمات حجب الخدمة لجذب الانتباه لقضيتهم، وغالبًا ما تكون دوافعهم أيديولوجية أو سياسية.
التهديدات الداخلية	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.
هواة السيكربت (Script Kiddies)	يشير هذا المصطلح إلى متسللين هواة يستخدِمون أدوات القرصنة وبعض البرامج النصية الأخرى لتنفيذ هجمات، وذلك دون خبرة تقنية كبيرة؛ من أجل التسلية، أو لاكتساب الشهرة، أو لتحدي أنفسهم.
المنافسون	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، أو معلومات حساسة يُمكن استخدامها لصالحهم.

النوع الأكثر شيوعًا من الهجمات السيبرانية يتم ينفذه عن طريق زرع **برمجيات ضارة** (Malware)، وهي برامج صمِّمت لإلحاق الضرر بنظام الحاسب أو الشبكة، وتشمل الأنواع المختلفة من هذه البرامج **الفيروسات** (Viruses) و**الديدان** (Worms) و**أحصنة طروادة** (Trojans) و**برمجيات الفدية** (Ransomware). يُمكن التمييز بين أنواع البرمجيات الضارة بناءً على **آلية انتشارها** (Propagation Mechanism) و**الحمولة** (Payload)، فبالنسبة لآلية الانتشار يُمكن أن تنتشر البرمجيات الضارة باستخدام تقنيات مختلفة، كأن يقوم المُستخدِم بنشرها دون معرفته بمحتواها، أو من خلال البريد الإلكتروني، أو الويب، أو الشبكة، أو الوسائط المحمولة، أمّا حمولات البرمجية الضارة فهي تعليمات برمجية لها أهداف خبيثة وتشمل أنواعها: البيانات أو الملفات المشفرة، أو سرقة بيانات الاعتماد أو المعلومات السرية، أو الوصول عن بُعد، أو التشغيل الضار للنظام.

الفيروسات Viruses

الفيروس هو جزء من تعليمات برمجية ترتبط ببرنامج أو بملف آخر، ويتم تنفيذه عند تشغيل هذا البرنامج أو الملف، حيث يُمكن للفيروس إتلاف البيانات، أو حذفها، أو تعديل إعدادات النظام، أو الانتشار إلى ملفات أو أجهزة أخرى.

أحد الأمثلة الشهيرة لفيروسات الحاسب فيروس **تشيرنوبيل** (Chernobyl) أو CIH، وقد تم إصداره عام 1998، وتسبب بتعطيل أنظمة الحواسيب وخسارة الكثير من المعلومات، وقد تم احتواء الفيروس في وقت لاحق، وأدت قدرته التدميرية إلى بروز الحاجة إلى تدابير أمنية أكبر في أنظمة تشغيل **ويندوز** (Windows)، ويصيب الفيروس **قطاع بدء التشغيل** (Boot Sector) في محرك الأقراص الثابتة بجهاز الحاسب، وبالتحديد منطقة **قطاع بدء التشغيل** (Boot Sector) التي تحتوي على البرمجة اللازمة لبدء تشغيل الحاسب. يُمكن أن تجعل فيروسات قطاع بدء التشغيل جهاز الحاسب غير قابل للاستخدام أو تتسبب في تعطيله، كما تُنتقل الفيروسات عادةً إلى أجهزة الحاسب الأخرى من خلال محركات أقراص **يو إس بي** (USB) المصابة، أو عن طريق تنزيل البرامج الحاملة للفيروس من شبكة الإنترنت.

الديدان Worms

تشبه الديدان الفيروسات، ولكنها لا تحتاج إلى إرفاق نفسها ببرامج أو ملفات أخرى لمضاعفتها، وبدلًا من ذلك فإنها تنتشر بسرعة عبر الشبكات، وتستهلك موارد النظام وتسبب الضرر، ومن أمثلتها دودة **ماي دووم** (Mydoom) التي تسببت في أضرار جسيمة لأنظمة الحاسب في جميع أنحاء العالم عام 2004.

أحصنة طروادة Trojans

تطلق تسمية حصان طروادة على البرمجيات الضارة التي تظهر كبرنامج موثوق أو مفيد، ولكنها في الحقيقة تُنفِّذ إجراءات ضارة على جهاز الحاسب في الخلفية دون علم مُستخدِم الجهاز، ويُمكنها إنشاء أبواب خلفية للوصول عن بُعد، أو سرقة المعلومات الشخصية، أو تنزيل برمجيات ضارة أخرى، أو عرض إعلانات غير مرغوب فيها. على سبيل المثال، استهدف **حصان طروادة زيوس** (Zeus Trojan) المعلومات المصرفية لمُستخدِمي نظام **ويندوز** (Windows)، وقام بسرقة بيانات الدخول عبر الإنترنت لأنظمة المصارف، وأرقام بطاقات الائتمان، وغيرها من البيانات الحساسة.

برمجيات الفدية Ransomware

برمجيات الفدية هي أحد أنواع البرمجيات الضارة التي تقوم بتأمين أو تشفير ملفات المُستخدِم أو الجهاز، وتطالب بالدفع مقابل استعادتها. قد تهدد برمجيات الفدية أيضًا بحذف بيانات المُستخدِم أو كشفها إذا لم يتم دفع الفدية خلال فترة زمنية معيَّنة، ويُمكن أن ينتشر من خلال مرفقات البريد الإلكتروني، أو روابط التصيد الإلكتروني، أو ثغرات الشبكة. على سبيل المثال، كانت برمجيات فدية **واناكراي** (WannaCry) عبارة عن دودة استغلت ثغرة أمنية في نظام ويندوز وأصابت مئات آلاف أجهزة الحاسب في عام 2017، حيث تم تشفير ملفات المُستخدِمين، وعرض رسالة تطالب بدفع فدية **بالعملة الرقمية** (Bitcoin) لفك تشفير تلك الملفات، وتوفر برمجيات الفدية أيضًا مفتاحًا لإيقاف نشرها إذا تم تسجيل اسم مجال معيَّن.

البرمجيات الدعائية Adware

البرمجيات الدعائية هي برمجيات ضارة تعرض إعلانات غير مرغوب فيها على جهاز المُستخدِم أو متصفحه، ويُمكنها جمع المعلومات حول عادات تصفح المُستخدِم وتفضيلاته لتقديم إعلانات مستهدفة، وتتسم بكونها مزعجة وتطفلية، ولكنها ليست بالضرورة ضارة، ومع ذلك يُمكن لبعضها تثبيت برمجيات ضارة أخرى، أو توجيه متصفح المُستخدِم لمواقع ويب ضارة. قد يتم تثبيت هذه البرمجيات بموافقة المُستخدِم كجزء من برنامج مجاني يقوم بتثبيته، أو دون موافقته، وذلك من خلال روابط التصيد الإلكتروني أو **التحميل غير المقصود** (Drive-by Downloads). على سبيل المثال، أتاحت البرمجية الدعائية **قاتور** (Gator) حفظ كلمات المرور وملء النماذج للمُستخدِمين، ولكنها عرضت أيضًا الإعلانات المنبثقة وقامت بجمع المعلومات الشخصية التي تم إدخالها، كما يتم دمج البرمجيات الدعائية مع برامج مجانية أخرى، ويُطلب من المُستخدِمين قبول شروط وأحكام التثبيت الخاصة بها.

برامج التجسس Spyware

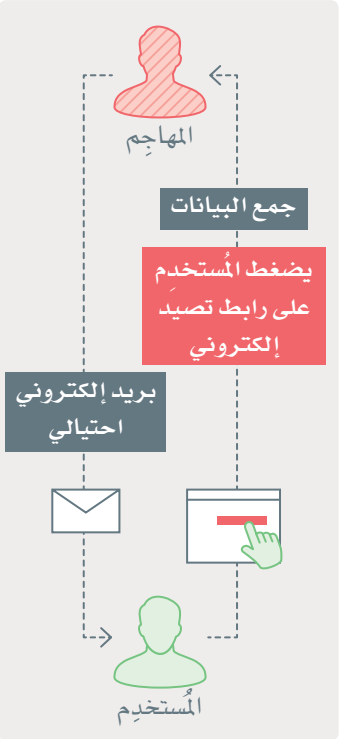
برامج التجسس هي إحدى أنواع البرمجيات الضارة التي تراقب وتجمع معلومات حول نشاط المُستخدِم عبر الإنترنت أو سجل التصفح، أو ضغطات لوحة المفاتيح، أو البيانات الشخصية، أو إعدادات النظام. يُمكن لبرامج التجسس تغيير إعدادات المتصفح أو إعادة توجيه صفحات الويب أو عرض الإعلانات المنبثقة (النوافذ الإعلانية)، كما يُمكن تثبيتها دون موافقة المُستخدِم أو معرفته من خلال البرمجيات المدمجة أو روابط التصيد الإلكتروني أو **التحميل غير المقصود** (Drive-by Downloads)، فعلى سبيل المثال: اعتُبر برنامج التجسس **كول ويب سيرش** (CoolWebSearch) برنامجًا خاصًّا باختراق المتصفح يعيد توجيه المُستخدِمين إلى مواقع ويب غير مرغوب فيها ويعرض إعلانات منبثقة، وتقوم برامج التجسس أيضًا بتغيير إعدادات المتصفح وتثبيت برمجيات ضارة إضافية. مثال آخر على مثل هذه البرامج هو برنامج التجسس **راصد لوحة مفاتيح** (Keylogger) الذي يسجل ضغطات لوحة المفاتيح لكل مُستخدِم ويرسلها إلى جهاز خادم مجهول، حيث يُمكن لبرامج التجسس التقاط كلمات المرور، وأرقام بطاقات الائتمان، ورسائل الدردشة، والمعلومات الحساسة.

أنواع الهجمات السيبرانية Types of Cyberattacks

بالإضافة إلى الهجمات التي تسببها البرمجيات الضارة، يُمكن استخدام العديد من أنواع الهجمات السيبرانية الأخرى لتعريض أنظمة الحاسب والشبكات والأجهزة للخطر، وفيما يلي بعض أكثر أنواع الهجمات السيبرانية شيوعًا:

هجمات الهندسة الاجتماعية Social Engineering Attacks

الهندسة الاجتماعية هي أحد أشكال التلاعب والخداع التي يستخدمها المهاجِمون للحصول على معلومات حساسة من أجل الوصول غير المُصرَّح به إلى الأنظمة المادية أو أنظمة الحاسب، حيث يحاول المهاجِمون خداع المُستخدِمين للكشف عن معلوماتهم الحساسة مثل: كلمات المرور، أو أرقام بطاقات الائتمان، أو غيرها من المعلومات الشخصية، وغالبًا ما تأتي هذه الهجمات على شكل رسائل بريد إلكتروني أو رسائل يبدو أنها من مصدر موثوق مثل: أحد البنوك أو أحد مواقع التواصل الاجتماعي الشهيرة، حيث تحتوي تلك الرسائل عادةً على رابط يوصل إلى موقع ويب مخادع أو مزيف مُصمَّم ليبدو كموقع رسمي، حيث يُطلب من المُستخدِم إدخال معلوماته، وفيما يلي بيان الأنواع الرئيسة لهجمات الهندسة الاجتماعية:



شكل 1.4: مثال على هجوم تصيد باستخدام الهندسة الاجتماعية

هجوم التصيد الإلكتروني (Phishing):
يتم خداع الضحايا من خلال الضغط على الروابط الاحتيالية المرسَلة عبر البريد الإلكتروني.

هجوم تصيد الرسائل القصيرة (Smishing):
يتشابه هذا النوع مع التصيد الإلكتروني، إلا أنه يتم بإرسال رسالة نصية (SMS) تحتوي على نص خادع على تطبيقات المراسلة، حيث يحتوي ذلك النص على رابط احتيالي.

هجوم التصيد الصوتي (Vishing):
يتصل مُرتكبو الجرائم السيبرانية بالضحايا المحتملين في هذا النوع من الهجوم، مدَّعين بأنهم شركة ما أو شخص معروف، وذلك بهدف الحصول على معلومات شخصية من الضحية.

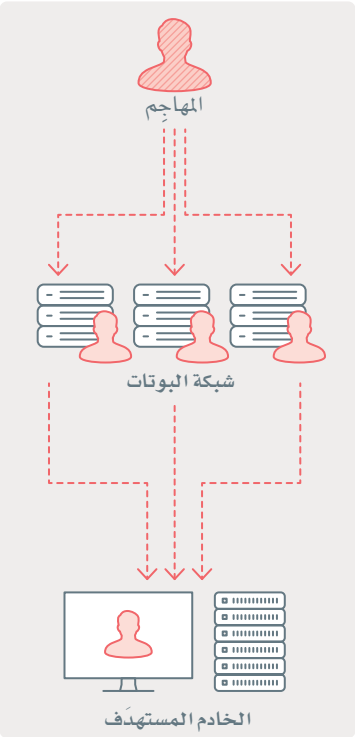
تثير رسائل البريد الإلكتروني التي تعتمد على التصيد الإلكتروني شعورًا بالقلق لدى المُستخدِم من فقدان القدرة على الوصول إلى حساباته أو خدماته، وفيما يلي توضيح للخصائص الأكثر شيوعًا لتلك الرسائل المشبوهة التي قد تكون هجوم تصيد إلكتروني:

شكل 1.5: مثال على الروابط الاحتيالية

- تشير رسالة البريد الإلكتروني إلى أن حسابك مُعلَّق بسبب مشكلة في الدفع.
- يحتوي البريد الإلكتروني على تحية عامة.
- يدعوك البريد الإلكتروني للضغط على رابط لتحديث تفاصيل الدفع الخاصة بك.

هجمات حجب الخدمة وحجب الخدمة الموزع
Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

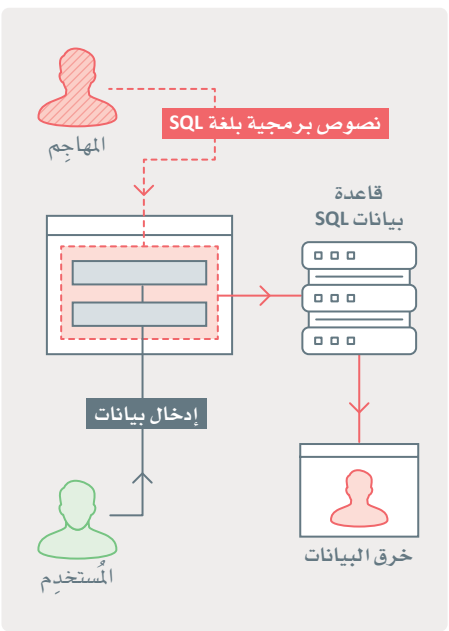
هجمات **حجب الخدمة** (DoS) وحجب **الخدمة الموزع** (DDoS) هي هجمات سيبرانية تعتمد على إغراق الشبكة أو الخادم بحركة بيانات ضخمة تجعل من الصعب أو حتى من المستحيل على المُستخدِمين الشرعيين الوصول إلى الخدمة، ويُمكن وصف هذا النوع من الهجمات بأنه هجوم على **التوافر** (Availability)، حيث يتم في هجوم **حجب الخدمة** (DoS) استخدام حاسب أو جهاز واحد لإغراق الشبكة، بينما يتم في هجوم **حجب الخدمة الموزع** (DDoS) استخدام أجهزة متعددة لمهاجمة الشبكة في وقت واحد، ويُمكن تنفيذ هذه الهجمات باستخدام مجموعة متنوعة من التقنيات مثل: إرسال كميات كبيرة من الطلبات إلى خادم، أو إغراق الشبكة بحركة بيانات من مصادر متعددة، كما يُمكن أن يكون لهذه الهجمات عواقب وخيمة مثل: إيقاف تشغيل الخدمات المهمة، وتعطيل العمليات التجارية. يُمكن للمؤسسات حماية نفسها ضد هذه الهجمات من خلال توظيف جُدران الحماية وأنظمة **كشف التسلل** (Intrusion Detection Systems – IDSs)، واستخدام **شبكات توزيع المحتوى** (Content Distribution Networks – CDNs) لتوزيع حركة البيانات عبر خوادم متعددة، وقد أدَّت جائحة **كوفيد 19** (COVID-19) في عام 2020 إلى زيادة هجمات **حجب الخدمة الموزع** (DDoS) ضد مؤسسات الرعاية الصحية، حيث استهدف المهاجِمون المستشفيات ومقدِّمي الرعاية الصحية، مما تسبب في تعطيل الخدمات الحيوية. من المعروف أن بعض الهجمات واسعة النطاق نتج عنها حركة بيانات ضخمة تعدّت **التيرابت في الثانية** (Terabits per second – Tbps)، مما أدى إلى إرباك الأنظمة المستهدَفة وتوقفها.



شكل 1.6: مثال على هجوم حجب الخدمة الموزع باستخدام شبكة بوتات (DDoS botnet)

حقن النصوص البرمجية بلغة SQL
SQL Injections

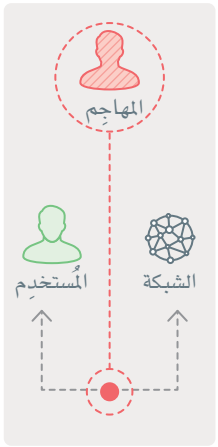
تستغل هجمات حقن النصوص البرمجية بلغة SQL الثغرات في قاعدة بيانات تطبيق الويب للوصول غير المُصرَّح به أو لإحداث تغييرات على البيانات، ويُمكن القيام بذلك من خلال إدخال تعليمات برمجية ضارة في حقول إدخال موقع الويب مثل: نماذج تسجيل الدخول، وذلك بهدف الوصول إلى قاعدة البيانات، كما يُمكن أن يكون لهذه الهجمات عواقب وخيمة مثل: سرقة البيانات الحساسة، أو تعديل سجلات قاعدة البيانات، ويُمكن للمؤسسات حماية نفسها من هجمات حقن نصوص SQL من خلال تنفيذ أفضل ممارسات **الترميز الآمن** (Secure Coding)، واستخدام **جُدران حماية تطبيقات الويب** (Web Application Firewalls – WAFs) لاكتشاف حركة البيانات الضارة وحظرها. من أمثلة هجوم حقن النصوص البرمجية بلغة SQL ما حدث عام 2019 عندما تعرضت ثغرة أمنية في نظام **ماجنتو** (Magento) للتجارة الإلكترونية التي تسمى الآن أدوبي **كوميرس** (Adobe Commerce) للمهاجِمين بالوصول إلى بيانات العملاء الشخصية ومعلومات بطاقات الائتمان.



شكل 1.7: مثال على حقن نصوص برمجية بلغة SQL

هجمات الوسيط Man-in-the-Middle (MitM) Attacks

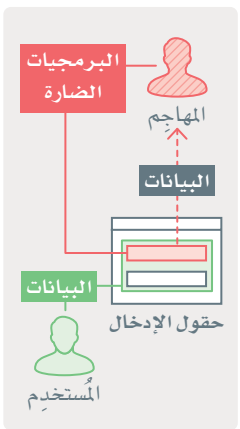
هجمات الوسيط (MitM) هي هجمات سيبرانية يَعترِض بها المهاجِم الاتصالات بين طرفين للتنصت أو للتلاعب بالمحادثة، ويُمكن تنفيذ ذلك بالدخول بين الطرفين واعتراض الرسائل ذهابًا وإيابًا، مما يسمح للمهاجِم بقراءة الرسائل أو تغييرها، ويُمكن تنفيذ هذه الهجمات باستخدام تقنيات مختلفة مثل: **التقاط حِزم البيانات** (Packet Sniffing)، أو **بتزوير معلومات الشبكة** (IP Spoofing) من خلال انتحال عنوان **بروتوكول الإنترنت** (IP). يُمكن أن يترتب على هذه الهجمات عواقب وخيمة مثل: سرقة المعلومات الحساسة، أو التلاعب في المُعامَلات المالية، كما يُمكن للمُستخدِمين حماية أنفسهم من هجمات الوسيط باستخدام تقنيات التشفير الآمنة مثل: **بروتوكول نقل النص التشعبي الآمن** (HTTPS) **والشبكة الخاصة الافتراضية** (VPN)، وتوخِّي الحذر عند استخدام شبكات **واي فاي** (Wi-Fi) اللاسلكية العامة. استغل المهاجِمون في عام 2020 ثغرة أمنية في تشفير برنامج زووم (Zoom)، وتمكنوا من القيام بهجوم وسيط واعتراض مكالمات الفيديو والتنصت عليها، كما تمكنوا من الوصول غير المُصرَّح به إلى معلومات حساسة مثل: خُطط الأعمال والبيانات المالية.



شكل 1.8: مثال على هجوم الوسيط (MitM)

هجمات البرمجة العابرة للمواقع Cross-Site Scripting (XSS) Attacks

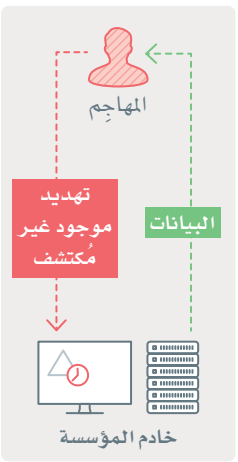
تقوم هجمات **البرمجة العابرة للمواقع** (XSS) بحقن نصوص برمجية ضارة في موقع ويب لسرقة معلومات المُستخدِم أو التلاعب بالمحتوى المعروض، ويُمكن القيام بذلك عن طريق إدخال نصوص برمجية في حقول إدخال موقع الويب مثل: مربعات البحث، أو أقسام التعليقات ومن ثمّ يتم تنفيذها عند تفاعل المُستخدِم مع الصفحة. يُمكن أن يكون لهجمات **البرمجة العابرة للمواقع** (XSS) عواقب كبيرة مثل: سرقة معلومات حساسة أو التلاعب بمحتوى موقع الويب، ويُمكن للمؤسسات حماية نفسها من هذه الهجمات من خلال تنفيذ ممارسات ترميز آمنة واستخدام **سياسات أمن المحتوى** (Content Security Policies – CSPs) لاكتشاف البرامج النصية الضارة وحظرها. استخدم المهاجِمون في عام 2018 هجوم **البرمجة العابرة للمواقع** (XSS) لسرقة معلومات حساسة من عملاء شركة كبيرة لبيع التذاكر، حيث قاموا بحقن نصوص برمجية ضارة في صفحة الدفع الخاصة بالشركة، مما سمح لهم بسرقة معلومات العملاء بما في ذلك الأسماء والعناوين ومعلومات بطاقات الدفع.



شكل 1.9: مثال على هجوم البرمجة العابرة للمواقع (XSS)

الهجمات بواسطة تهديد متقدِّم ومستمر Attacks by Advanced Persistent Threat (APT)

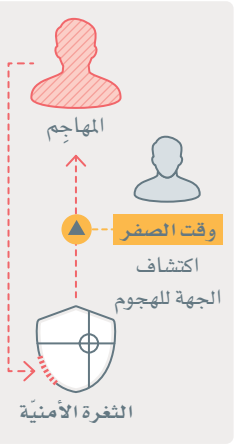
تستخدِم **هجمات التهديد المتقدِّم والمستمر** (APT) تقنيات متطورة للوصول غير المُصرَّح به إلى نظام معيَّن، مع مراعاة عدم اكتشافها لفترات طويلة، حيث تستخدِم هذه الهجمات مزيجًا من الهندسة الاجتماعية، والبرمجيات الضارة، وتقنيات أخرى للوصول إلى المعلومات أو الأنظمة الحساسة، كما يُمكن أن يكون لها عواقب وخيمة مثل: سرقة الملكية الفكرية أو بيانات العملاء الحساسة. يُمكن للمؤسسات حماية نفسها من هجمات **التهديد المتقدِّم والمستمر** (APT) من خلال تنفيذ نظام أمني شامل يتضمن تدريب الموظفين وإدارة الثغرات وتحليل معلومات التهديدات، وكمثال على هذه الهجمات، استغل المهاجِمون في عام 2015 اختراقًا سابقًا لإحدى المؤسسات الطبية لسرقة المعلومات الشخصية والطبية لثمانين مليون عميل، حيث تمكَّنوا من التواجد داخل الأنظمة والحصول على المعلومات لعدة شهور دون أن يتم اكتشافهم، مما يبرز الحاجة الماسة إلى برامج أمنية شاملة وتحليل معلومات التهديدات.



شكل 1.10: مثال على هجوم تهديد متقدِّم ومستمر (APT)

استغلال الثغرات الصفري Zero-Day Exploits

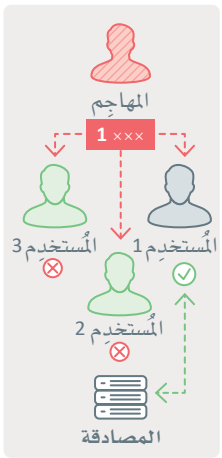
تعتمد عمليات استغلال الثغرات الصفري على استغلال نقاط الضعف في البرامج قبل اكتشافها وتصحيحها مما يكسبها خطورة عالية، بسبب عدم تمكّن المطوِّرين من تصحيح المشكلة قبل بدء الهجوم وفوات الأوان، ويُمكن استخدام استغلال الثغرات الصفري للوصول غير المُصرَّح به للنظام، أو لسرقة معلومات حساسة، أو لإلحاق الضرر بنظام معيَّن. عادة ما يكتشف المهاجمون هذه الثغرات لتنفيذ هجمات مستهدفة ضد المؤسسات، وتكمن صعوبة الحماية من استغلال الثغرات الصفري في كونها غير معروفة لمُستخدِم البرنامج وكذلك لمن قاموا بإنشائه، وبالتالي لا يُمكن تصحيحها إلا حين يتم اكتشافها. يُمكن للمؤسسات حماية نفسها من هذه العمليات من خلال تنفيذ أفضل ممارسات الترميز الآمن، واستخدام أدوات الحماية التي يُمكنها اكتشاف السلوك المشبوه للبرامج وحظره، وكمثال على هذه الثغرات، استخدَم المهاجمون في عام 2021 ثغرة أمنية في إصدار **مايكروسوفت** (Microsoft) الجديد من **الخادم التبادلي** (Exchange Server) لتثبيت **أبواب خلفية** (Backdoors) لاختراق الأنظمة المستهدَفة.



شكل 1.11: مثال على استغلال الثغرات الصفري

هجمات كلمة المرور Password Attacks

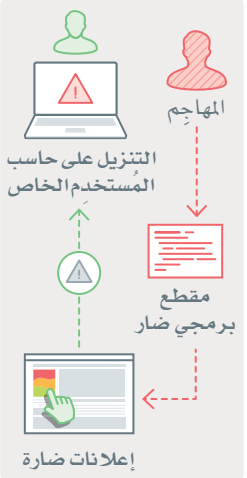
تستخدِم هجمات كلمة المرور تقنيات مثل: **هجوم القوة المُفرطة** (Brute Force Attack)، أو **التصيد الإلكتروني** (Phishing) لتخمين كلمات مرور المُستخدِمين أو لسرقتها والوصول غير المُصرَّح به إلى الأنظمة، حيث تستخدِم هجمات القوة المُفرطة أدوات آلية لتجربة آلاف أو ملايين كلمات المرور المحتملة حتى يتم العثور على الكلمة الصحيحة، وتستخدِم هجمات التصيد الإلكتروني تقنيات الهندسة الاجتماعية لخداع المُستخدِمين للكشف عن كلمات المرور الخاصة بهم. يُمكن أن يكون لهجمات كلمات المرور عواقب وخيمة مثل: سرقة البيانات الحساسة، أو تعريض الأنظمة المهمة للخطر، ويُمكن للمُستخدِمين حماية أنفسهم من تلك الهجمات باستخدام كلمات مرور قوية ومعقدة، وتفعيل **المصادقة متعددة العوامل** (Multi-Factor Authentication – MFA)، وذلك بالتحقق بواسطة الرسائل القصيرة مثلًا أو باستخدام نظام **نفاذ** (Nafath) السعودي، وذلك للحصول على طبقة إضافية من الأمان. استخدم المهاجمون في عام 2012 هجوم القوة المُفرطة للوصول إلى قاعدة بيانات شبكة **لينكد إن** (LinkedIn)، وتمكنوا من اختراق الملايين من كلمات مرور المُستخدِمين.



شكل 1.12: مثال على هجمات كلمة المرور

الإعلانات الضارة Malvertising

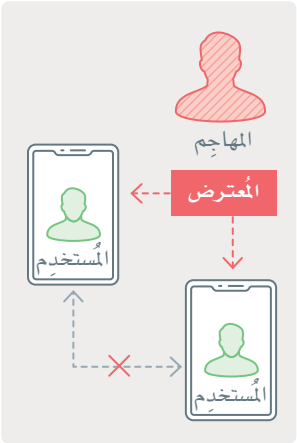
الإعلانات الضارة هي ممارسة تقوم على تضمين نصوص برمجية ضارة في الإعلانات الإلكترونية، بهدف إصابة أجهزة حاسب المُستخدِمين الخاصة ببرمجيات ضارة. قد يصعب اكتشاف الإعلانات الضارة، حيث تكون في الغالب جزءًا من الإعلانات الرسمية التي تقدمها الشركات المختلفة للمتصفحين، فبمجرد أن يضغط المُستخدِم على إعلان ضار، يتم تنزيل البرمجيات الضارة على حاسبه بحيث يُمكن استخدامها لسرقة معلوماته الحساسة أو تنفيذ هجمات أخرى. يُمكن للمُستخدِمين حماية أنفسهم من أخطار تلك الإعلانات الضارة باستخدام أدوات منع الإعلانات، وبتوخي الحذر عند الضغط على الإعلانات عبر الإنترنت. على سبيل المثال، تعرض المتصفحون في عام 2016 لمجموعة أدوات إعلانات ضارة استغلت فجوة **أنقلير** (Angler) الأمنيّة لتنزيل مقطع برمجي مشبوه قام بتحميل برمجيات فدية **لوكي** (Locky)، وقد تأثر بها الكثير من مواقع الويب المشهورة، بما فيها جريدة **نيويورك تايمز** (New York Times) و**هيئة الإذاعة البريطانية** (BBC)، وهذا يسلط الضوء على حاجة المُستخدِمين إلى استخدام أدوات حظر الإعلانات وأدوات الأمان الأخرى للحماية من مثل هذه الإعلانات الضارة.



شكل 1.13: مثال على ممارسة الإعلانات الضارة

التنصت Eavesdropping

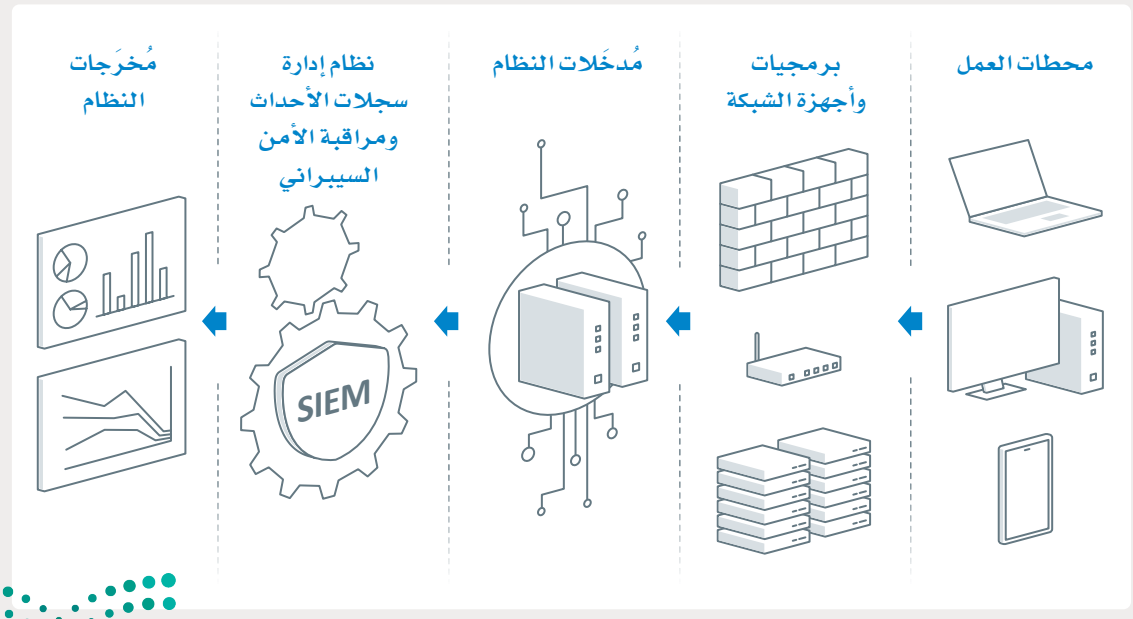
التنصت هو الاعتراض غير المُصرَّح به للاتصالات المختلفة مثل: رسائل البريد الإلكتروني، أو المكالمات الهاتفية، أو الرسائل الفورية، ويُمكن إجراؤه باستخدام تقنيات مختلفة مثل: التقاط حزم البيانات أو التنصت على الشبكة. يُمكن أن يكون للتنصت عواقب وخيمة مثل: سرقة معلومات حساسة أو اختراق أنظمة حيوية، ويُمكن للمُستخدِمين حماية أنفسهم من التنصت باستخدام تقنيات التشفير الآمنة مثل: **بروتوكول نقل النص التشعبي الآمن** (HTTPS)، و**الشبكة الخاصة الافتراضية** (VPN)، وكذلك توخي الحذر عند استخدام شبكات **واي فاي** (Wi-Fi) اللاسلكية العامة. من أمثلة التنصت ما حدث في عام 2020 عندما قام المهاجِمون باستغلال ثغرة أمنية في بروتوكول الاتصالات لإحدى شركات الاتصالات ونجحوا في اعتراض الرسائل النصية والتنصت على المكالمات الهاتفية، حيث أبرزت تلك الثغرة الأمنيّة التي كانت معروفة سابقًا منذ عدة سنوات حاجة شركات الاتصالات إلى اتخاذ تدابير أمنية أقوى للحماية من التنصت.



شكل 1.14: مثال على اعتراض التنصت

نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني
Security Information and Event Management (SIEM) System

نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) هو أدوات برمجية مصمَّمة لمساعدة المؤسسات والشركات على اكتشاف تهديدات الهجمات السيبرانية والاستجابة الفورية لها، حيث يقوم بجمع وتحليل البيانات من مصادر مختلفة مثل: أجهزة الشبكة، والخوادم، والتطبيقات لتحديد الحوادث الأمنيّة المحتملة، ويتم تحليل البيانات باستخدام خوارزميات التعلُّم الآلي والذكاء الاصطناعي، لاكتشاف الأحداث المثيرة للشك على مستوى الأنظمة، وتحليل البيانات والأنماط التي قد تشير إلى وجود تهديد أمني.



شكل 1.15: تمثيل نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM)

تحديد مخاطر الأمن السيبراني وتقليلها وإدارتها
Cybersecurity Risk Identification, Mitigation, and Management

يُعدُّ التعرف على مخاطر الأمن السيبراني وتقليلها وإدارتها من العمليات الأساسية للمؤسسات، وذلك لحماية أصولها الهامة، والمعلومات الحساسة، وضمان استمرارية عملياتها.

تحديد المخاطر Risk Identification

تتضمن الخطوة الأولى في إدارة مخاطر الأمن السيبراني تحديد التهديدات والثغرات المحتملة التي قد تؤثر على أصول المؤسسة الرقمية، وتشمل الأنشطة الرئيسة لتحديد المخاطر ما يلي:

مستودع الأصول

يشمل إنشاء قائمة شاملة بالأصول الرقمية للمؤسسة مثل: الأجهزة، والبرامج، والبيانات، والبنية التحتية للشبكة.

تقييم التهديدات

يشمل تحديد مصادر التهديد المحتملة مثل: مُرتكبي الجرائم السيبرانية، أو التهديدات الداخلية، أو الكوارث الطبيعية، والتي يُمكن من خلالها استغلال الثغرات في أنظمة المؤسسة.

تقييم الثغرات الأمنيّة

يشمل اكتشاف وتوثيق نقاط الضعف في الأصول الرقمية للمؤسسة باستخدام فحص الثغرات الأمنيّة، والقيام باختبارات الاختراق، وكذلك عمليات التقييم اليدوية الأخرى.

تحليل المخاطر

يتم تحديد أولويات المخاطر بناءً على عواقبها المحتملة من خلال تقييم احتمالية التهديدات والثغرات الأمنيّة التي تم تحديدها، وتأثيرها.

إدارة المخاطر Risk Management

فور الانتهاء من تحديد المخاطر، يجب على المؤسسات اتخاذ خطوات لتقليلها أو إدارتها. تتضمن إدارة المخاطر تنفيذ تدابير أمنية فعّالة لمعالجة الثغرات وتقليل احتمالية ظهورها، ومعالجة تأثير التهديدات، وتشمل استراتيجيات الحد من المخاطر الرئيسة ما يلي:

التوعية والتدريب بالأمن السيبراني

يشمل توعية الموظفين حول أفضل ممارسات الأمن السيبراني ومسؤولياتهم في حماية الأصول الرقمية للمؤسسة.

تخطيط الاستجابة للحوادث

يشمل وضع خطة لاكتشاف الحوادث الأمنيّة والاستجابة لها، والتعافي منها؛ بهدف الحدّ من تأثيرها على المؤسسة في حال وقوعها.

التحكم بالوصول

يشمل تنفيذ آليات للمصادقة والتفويض لتقييد الوصول إلى البيانات والأنظمة الحساسة وقصرها على المُستخدِمين المُصرَّح لهم بذلك.

التشفير

يحول التشفير النص غير المُشفَّر والبيانات إلى صيغة مشفرة لمنع الوصول غير المُصرَّح به، كما يحمي تشفير البيانات والمعلومات الحساسة من الوصول غير المُصرَّح به أو سرقتها، سواء أثناء تخزينها أو خلال نقلها عبر الأجهزة والشبكات.

إدارة التحديثات

تشمل تحديث البرامج والأجهزة بانتظام لمعالجة الثغرات الأمنيّة المعروفة وضمان بقاء الأنظمة آمنة ضد التهديدات الجديدة.

معالجة المخاطر

يشمل اختيار استراتيجيات الحدّ من المخاطر وتنفيذها بناءً على موارد المؤسسة وقدرتها على تحمل المخاطر، وعلى المراجعة المنظمة لفعالية هذه الاستراتيجيات.

الحوكمة والامتثال

تشمل ضمان توافق سياسات الأمن السيبراني وممارساته للمؤسسة مع القوانين واللوائح، ومع المعايير الصناعية ذات العلاقة.

الإبلاغ والتواصل

يشمل إطلاع أصحاب المصلحة بشكلٍ مستمر على خُطط المؤسسة للاستجابة لمخاطر الأمن السيبراني، وعلى أي تغييرات تطرأ على استراتيجيات إدارة المخاطر.

جدول 1.2: أدوات تحديد مخاطر الأمن السيبراني وتقليلها وإدارتها

التصنيف	الوصف
نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM)	تجمع هذه الأنظمة البيانات الأمنيّة من مصادر مختلفة وتُحللها.
أدوات اختبار الاختراق	تُحاكي الهجمات على الأنظمة أو الشبكات لتحديد الثغرات الأمنيّة وتختبر فعالية الضوابط الأمنيّة.
تقييم المخاطر الأمنيّة	تحدِّد المخاطر الأمنيّة في البنية التحتية للمؤسسة وتُقيمها، بما فيها الشبكات والأنظمة والتطبيقات.
منع فقدان البيانات	يُراقب تدفق البيانات الحساسة داخل المؤسسة ويضبطها للمساعدة في منع خروقات البيانات.
جدار الحماية ونظام الحماية من الاختراق	يُراقب حركة البيانات الواردة التي تم تحديدها على أنها ضارة ويحظرها.
حماية النقطة الطرفية	تحمي أجهزة الأفراد مثل: أجهزة الحاسب المحمولة، والهواتف الذكية من البرمجيات الضارة، والتهديدات الأخرى.
أدوات التحليلات الأمنيّة	تستخدِم التعلُّم الآلي والتقنيات المتقدِّمة الأخرى لتحليل البيانات الأمنيّة وتحديد التهديدات المحتملة.

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. الفيروس جزء من تعليمات برمجية يربط نفسه ببرنامج أو ملف آخر، ويتم تنفيذه عند تشغيل هذا البرنامج أو الملف.	○	○
2. تقوم برمجيات الفدية بتشفير ملفات المُستخدِم أو الجهاز، وتطالب بالدفع مقابل استعادتها.	○	○
3. حصان طروادة برنامج موثوق أو مفيد يُنفِّذ إجراءات مفيدة في الخلفية.	○	○
4. يُمكن أن تضيف المصادقة متعددة العوامل (MFA) طبقة حماية إضافية للحد من الهجمات التي تستهدف كلمات المرور.	○	○
5. برامج التجسس هي برمجيات ضارة تحمي خصوصية المُستخدِم وأمنه على الإنترنت.	○	○
6. هجمات التصيد الإلكتروني شكل من أشكال الهندسة الاجتماعية تحاول خداع المُستخدِمين للكشف عن معلومات حساسة.	○	○
7. تتضمن هجمات حجب الخدمة (DoS) التنسيق بين أجهزة متعددة لمهاجمة الشبكة في وقت واحد.	○	○
8. تستغل هجمات حقن النصوص البرمجية بلغة SQL الثغرات في قاعدة بيانات تطبيق الويب للوصول غير المُصرَّح به أو لإحداث تغييرات على البيانات.	○	○
9. تقوم هجمات البرمجة العابرة للمواقع (XSS) بحقن نصوص برمجية ضارة في موقع ويب لسرقة معلومات المُستخدِم أو التلاعب بالمحتوى المعروض.	○	○
10. لا تتعرض شبكات واي فاي (Wi-Fi) اللاسلكية العامة لهجمات التنصت.	○	○

2 وضِّح المقصود بالبرمجيات الضارة.

3 اشرح ماهية فيروس الحاسب وكيفية عمله.

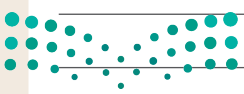
4 ميّز وقارن بين خصائص الفيروسات والديدان وأحصنة طروادة وبرمجيات الفدية.

5 عدِّد المخاطر والميزات المتعلقة بشبكات واي فاي (Wi-Fi) اللاسلكية العامة مع توضيح كيفية إمكانية حماية المُستخدِمين لأجهزتهم عند الاتصال بها.

6 وضِّح أهمية الوعي بهجمات الإعلانات الضارة.

7 قيِّم فعالية نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) في اكتشاف التهديدات الأمنيّة والاستجابة لها.

8 ميِّز وقارن بين هجمات حجب الخدمة (DoS) وحجب الخدمة الموزع (DDoS).



9 اذكر واشرح الخطوات التي يجب أن تتخذها أي مؤسسة للحماية من عمليات استغلال الثغرات الصفري.

10 وضِّح تأثير هجمات حقن النصوص البرمجية بلغة SQL على تطبيق الويب.

11 اذكر مثالين على الأنشطة التي تشكل جزءًا من تحديد المخاطر وتقليلها وإدارتها.

رابط الدرس الرقمي

www.ien.edu.sa

الدرس الثالث

تهديدات الأمن السيبراني وضوابطه

تهديدات الأمن السيبراني Cybersecurity Threats

أصبحت تهديدات الأمن السيبراني تُشكِّل خطرًا دائمًا في عالمنا الذي يعتمد على التقنية بشكل مطّرد، ومع ازدياد الأنشطة التي تتم عبر الإنترنت، أصبح الوصول إلى البيانات الشخصية أكثر سهولة، وأضحى فهم المخاطر المرتبطة بتحديات الأمن السيبراني أمرًا محتَّمًا، ومن أمثلة تلك المخاطر: تهديدات البيانات، وانتحال الشخصية، والتَتبُّع عبر الإنترنت.

تهديدات البيانات Data Threats

تُعدُّ حماية البيانات أمرًا بالغ الأهمية في ظل تخزين المزيد من المعلومات الشخصية والحساسة رقميًا، حيث يجب على المؤسسات التعامل مع البيانات الشخصية بشكل آمن ومسؤول، وحمايتها من الوصول غير المشروع، أو التغيير أو الكشف غير المُصرَّح به، وتشمل مخاوف حماية البيانات الرئيسة ما يلي:

خروقات البيانات (Data Breaches):
الوصول غير المُصرَّح به إلى البيانات الشخصية، أو الكشف عنها، وهذا غالبًا بسبب ضعف التدابير الأمنيّة أو خطأ بشري.

الاحتفاظ بالبيانات (Data Retention):
يُمكن أن تثير المدة والطريقة التي يتم بها تخزين البيانات الشخصية المخاوف خاصةً إذا كانت البيانات المخزَّنة غير محمية بشكل كافٍ.

سيادة البيانات (Data Sovereignty):
الآثار القانونية لتخزين البيانات في بلدان مختلفة مما قد يتسبب في تطبيق قوانين وأنظمة خصوصية مختلفة على هذه البيانات وفقًا لقوانين كل دولة.

انتحال الشخصية Identity Theft

يحدث انتحال الشخصية من خلال سرقة المعلومات الشخصية لفرد ما واستخدامها بطريقة احتيالية؛ لتحقيق مكاسب مالية غالبًا، وأتاح العصر الرقمي لمُرتكبي الجرائم الوصول إلى البيانات الشخصية واستغلالها، مما زاد من عمليات انتحال الشخصية، ومن الأمثلة عليها:

انتحال الهوية (Spoofing):
انتحال الهوية هو تكر المهاجم كمُستخدِم شرعي للنّظام من أجل الوصول إلى المعلومات.

هجوم التصيد المستهدف (Spear-Phishing):
يَتوجّه هجوم التصيد المستهدف إلى الأفراد أو المؤسسات برسائل مخصصة بهدف الحصول على معلوماتهم الحساسة والشخصية، حيث يستخدِم المهاجِم المعلومات الشخصية للضحية لجعل الرسالة تبدو من مصدر رسمي.

التَتبُّع الإلكتروني Online Tracking

يخضع الكثير من الأشخاص للتَتبُّع والمراقبة عند القيام بالأنشطة المختلفة عبر الإنترنت، مما يثير مخاوف بشأن الخصوصية والمراقبة، وتوجد بعض الممارسات المشروعة أو الإجتياحية (غير المشروعة) للتَتبُّع الإلكتروني مثل:

تَتبُّع السلوك (Behavioral Tracking):
مراقبة وتحليل أنشطة الفرد عبر الإنترنت لإنشاء ملف تعريف يحدِّد اهتماماته وعاداته وتفضيلاته، وغالبًا ما يُستخدَم للإعلانات المستهدفة.

ملفات تعريف الارتباط (Cookies):
ملفات نصية صغيرة يتم وضعها على جهاز المُستخدِم بواسطة مواقع الويب لتَتبُّع نشاط التصفح والتفضيلات لأغراض مشروعة، مثل تخصيص المحتوى، ولكن يُمكن أيضًا استخدامها لجمع البيانات دون موافقة المُستخدِم.

لمواجهة تهديدات الأمن السيبراني المختلفة، يجب أن تعمل الحكومات والمؤسسات والأفراد معًا لتطوير وتنفيذ السياسات واللوائح وأفضل الممارسات التي تخلق التوازن بين فوائد التقنيات الرقمية والحاجة إلى حماية البيانات الشخصية.

الأمن السيبراني والتحكم بالوصول Cybersecurity and Access Control

التحكم بالوصول إجراء دفاعي أساسي في الأمن السيبراني يهدف إلى حماية أنظمة المعلومات وخصوصية البيانات من الوصول غير المُصرَّح به ومن التغيير غير المشروع، ويُمكن أن يعتمد على نماذج مختلفة، مثل تلك التي تعتمد على الأدوار المخصصة أو السمات، كما يُمكن أن يساعد على تحقيق أهداف أمنية متنوعة مثل: المصادقة والتفويض وعدم الإنكار، وسيتم شرح هذه المفاهيم بمزيد من التفصيل أدناه.

التحكم في الوصول بناءً على الدور Role-Based Access Control (RBAC)

التحكم في الوصول بناءً على الدور هو نهج في الأمن السيبراني يحدِّد وصول المُستخدِمين المُصرَّح لهم إلى النظام بناءً على أدوارهم داخل المؤسسة، وفي هذا النموذج يتم تعيين أذونات لأداء عمليات معيَّنة لأدوار محدَّدة بحيث يتم تعيين الأدوار المناسبة للمُستخدِمين، وبالتالي الحصول على هذه الأذونات. على سبيل المثال، يُمكن للمطوِّرين في شركة برمجيات كتابة التعليمات البرمجية وتغييرها، بينما في المقابل يكون لمُختبِر ضمان الجودة حق الوصول فقط لعرض التعليمات البرمجية واختبارها دون إمكانية تعديلها. يجعل **التحكم في الوصول بناءً على الدور** (RBAC) من عملية إدارة صلاحيات المُستخدِم وتدقيقها أمرًا سهلًا، مما يُقلِّل من الأخطاء المحتملة عند تعيين الأذونات بشكل فردي.

التحكم في الوصول بناءً على السمات Attribute-Based Access Control (ABAC)

التحكم في الوصول بناءً على السمات هو طريقة أكثر مرونة ودقة للتحكم بالوصول من خلال منح أذونات بناءً على السمات المرتبطة بالمُستخدِم، والموارد التي يحاول الوصول إليها، والشروط التي يتم بموجبها طلب الوصول. قد تكون هذه سمات للمُستخدِم (مثل: الدور، أو الموقع الذي يعمل به)، وسمات للموارد (مثل: تصنيف البيانات، أو القسم)، وسمات بيئية (مثل: الوقت، وموقع الوصول). على سبيل المثال، يُمكن الوصول إلى مستند حسَّاس في شركة من قِبل المدير (سمة المُستخدِم) فقط إذا تم وضع إشارة على المستند توضح أنه ينتمي إلى قسم (سمة الموارد)، وذلك خلال ساعات العمل (السمة البيئية). يسمح **التحكم في الوصول بناءً على السمات** (ABAC) لنظام التحكم بالوصول الديناميكي والمناسب لطبيعة العمل بصورة ناجحة.

التعريف Identification

التعريف وسيلة للتحقق من هوية المُستخدِم أو العملية أو الجهاز بصفته شرطًا مُسبقًا لمنح الوصول إلى الموارد في النظام، وتتم خطوة التعريف عادة خارج النظام كخطوة مسبقة. على سبيل المثال، يتم منح موظف جديد اسم مُستخدِم وكلمة مرور بمجرد انضمامه إلى مؤسسة، والتأكد من هويته بشكلٍ شخصي أو عبر طريقة تحقق تعتمدها المؤسسة.

المصادقة Authentication

المصادقة هي عملية التحقق من هوية مُستخدِم أو جهاز أو نظام يحاول الوصول إلى الموارد داخل المؤسسة، وتساعد آليات المصادقة القوية على ضمان وصول المُستخدِمين الموثوقين فقط إلى موارد المؤسسة.

التفويض Authorization

بمجرد مصادقة مُستخدِم أو جهاز أو نظام، تحدِّد عملية التفويض مستوى الوصول الذي يجب منحه، ويتضمن ذلك تعيين الأذونات بناءً على سياسات الوصول المحدَّدة مسبقًا، أو وفق أدوار المُستخدِمين أو أعضاء المجموعة، كما يضمن التفويض المناسب أن المُستخدِمين المناسبين هم فقط من يُمكنهم الوصول إلى الموارد وتنفيذ الإجراءات المسموح لهم بها، مما يَحدُّ من إمكانية الوصول غير المُصرَّح به أو إساءة استخدام البيانات الحساسة.

عدم الإنكار Nonrepudiation

يُعدُّ عدم الإنكار جانبًا مهمًا من جوانب التحكم بالوصول والأمن السيبراني، حيث يضمن عدم تمكن المُستخدِمين من إنكار صحة أفعالهم أو مُعامَلاتهم داخل النظام، ويحمل هذا الأمر أهمية خاصة في الحالات التي يجب فيها الحفاظ على سلامة البيانات أو صحة المُعامَلات مثل: الخدمات المالية، والرعاية الصحية، والمُعامَلات القانونية، كما يُمكن أن يساعد تنفيذ آليات عدم الإنكار في منع النزاعات والاحتيال والأنشطة غير المُصرَّح بها من خلال تقديم أدلة دامغة على إجراءات المُستخدِمين.

مبدأ الحد الأدنى من الصلاحيات والامتيازات Principle of Least Privilege

من المهم أن تلتزم أنظمة التحكم بالوصول بمبدأ الحد الأدنى من الصلاحيات والامتيازات الذي ينص على أنه يجب منح المُستخدِمين الحد الأدنى من مستوى الوصول اللازم لأداء أدوارهم الوظيفية، ويَحدُّ هذا من إمكانية الوصول غير المُصرَّح به، أو إساءة استخدام البيانات الحساسة ويسهم في تقليل الضرر المحتمل الناجم عن اختراق حسابات المُستخدِمين أو التهديدات الداخلية.

الحاجة إلى المعرفة Need to Know

يجب أن يقتصر الوصول للمعلومات على أولئك الذين لديهم حاجة تشغيلية لمعرفة تلك المعلومات، ويُعدُّ هذا إجراءً هامًا للأمن والخصوصية لأنه يَحدُّ من كمية البيانات التي يُمكن الوصول إليها بشكل غير مناسب، كما يُستخدَم هذا المبدأ في المؤسسات العامة والخاصة على حد سواء لضمان سلامة الأصول الهامة.

تعدُّد الطبقات Layering

يُمكن للمُستخدِمين ضمان حماية البيانات والأنظمة المهمة من الوصول غير المُصرَّح به والتلاعب من خلال إضافة أشكال مختلفة من أشكال الأمن على مستويات متعددة، ويُعدُّ هذا المبدأ جزءًا أساسيًا من أنظمة أمن المعلومات، حيث يَحدُّ من مخاطر الحماية المبنية على إجراء أمني واحد فقط.

التنويع Diversification

يوصي هذا المبدأ بأنه يجب على المؤسسات تنفيذ مجموعة متنوعة من آليات الأمن لتقليل مخاطر الهجوم أو التهديدات الأخرى، فمن خلال وجود أشكال مختلفة من الأمن تكون المؤسسات قادرة على تحديد الثغرات الأمنيّة ونقاط الضعف التي قد تحدث، والاستجابة وفقًا لذلك، كما يُمكن للمؤسسات من خلال التنويع في الإجراءات الأمنيّة المطبقة تقليل مخاطر حدوث خلل يتسبب بحدوث خرق معيَّن للبيانات.

التعتيم Obscurity

يعتمد مبدأ التعتيم على توفير معلومات أو رؤية محدودة للغاية للبيانات أو الأنظمة الحساسة، ويُمكن للمؤسسات حماية بياناتها وأصولها من المهاجمين أو الدخلاء المحتملين من خلال جعل الوصول إليها أمرًا صعبًا أو بمنع الوصول المباشر إليها. يتضمن هذا المبدأ إخفاء بيانات المصادقة الضرورية عن الأنظار، ويُعدُّ بمثابة شكلٍ مهم من أشكال حماية التطبيقات لمنع الوصول غير المُصرَّح به إلى المعلومات والبيانات المهمة.

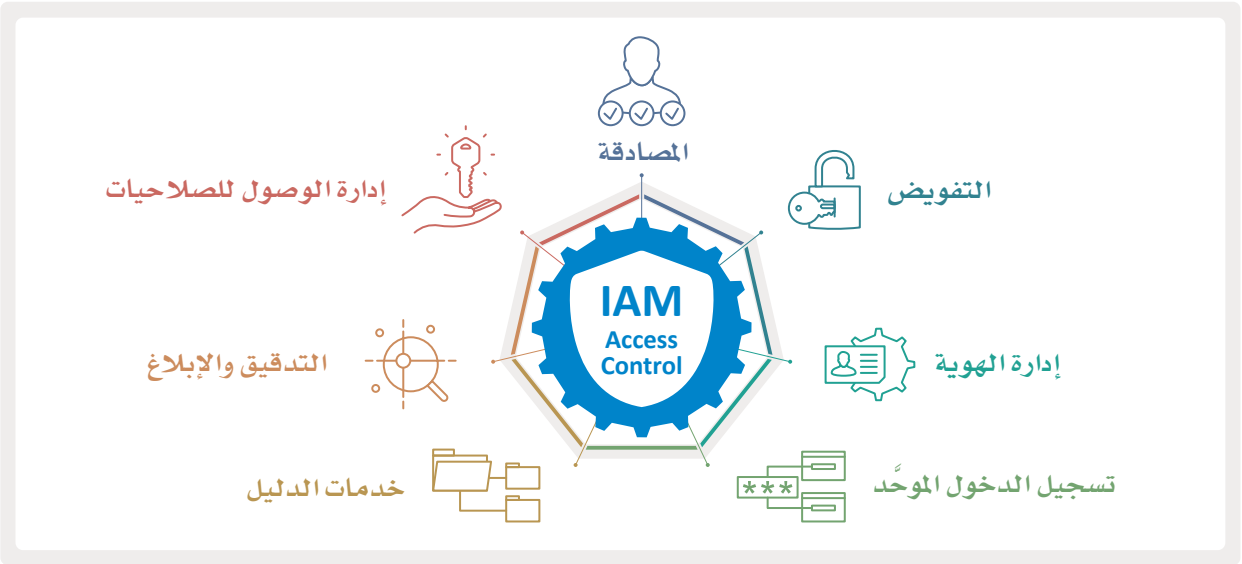
التدقيق والمراقبة Auditing and Monitoring

يجب أن تتضمن أنظمة التحكم بالوصول قدرات تدقيق ومراقبة لتَتبُّع أنشطة المُستخدِم ومحاولات الوصول، ومن خلال تسجيل ومراجعة محاولات وأحداث الوصول يُمكن للمؤسسات تحديد الأنشطة المشبوهة، واكتشاف الانتهاكات الأمنيّة المحتملة، وضمان الامتثال للسياسات الداخلية واللوائح الخارجية.

أدوات التحكم بالوصول للأمن السيبراني Cybersecurity Access Control Tools

التحكم في إدارة الهوية والوصول (IAM)

تُعدُّ عمليات **إدارة الهوية والوصول** (Identity and Access Management – IAM) مكوِّنًا أساسيًا في الأمن السيبراني يساعد المؤسسات على إدارة هويات المُستخدِمين وحمايتها والوصول إلى الموارد. يتم تصميم حلول **إدارة الهوية والوصول** (IAM) لتوفير تحكم مركزي في هويات المُستخدِمين وفي الوصول إلى الموارد، وكذلك لإتاحة أتمتة تعيين حسابات المُستخدمين وإلغائها، كما تشتمل هذه الحلول على مستوى المؤسسات ميزات إضافية متنوعة لمساعدتها على إدارة وحماية هويات المُستخدِمين والوصول إلى الموارد، وتشمل هذه الميزات:



شكل 1.16: ميزات التحكم في إدارة الهوية والوصول (IAM)

- **المصادقة** (Authentication):

تشمل إمكانات **المصادقة متعددة العوامل** (MFA) التي تساعد في الحماية من انتحال الشخصية والوصول غير المُصرَّح به، ويُمكن أن تسبق عمليات المصادقة من خارج النظام مثل: تعيين اسم مُستخدِم وكلمة مرور لموظف جديد بمجرد انضمامه إلى مؤسسة، بحيث يتم التأكد من الهوية بشكلٍ شخصي أو من خلال طرائق تحقق أوجدتها المؤسسة لهذا الغرض.

- **التفويض** (Authorization):

هو عملية السماح للمؤسسات بإدارة الوصول إلى الموارد استنادًا إلى **التحكم في الوصول بناءً على الدور** (RBAC) وعلى نماذج التحكم بالوصول الأخرى.

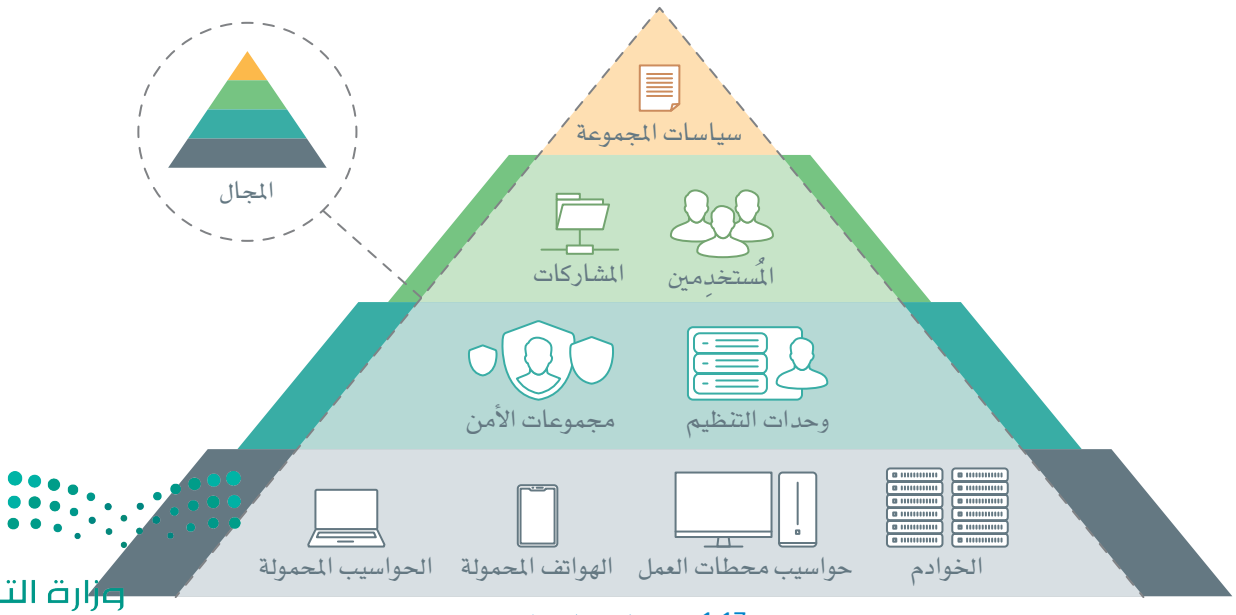
- **إدارة الهوية** (Identity Management):

تشمل إدارة هويات المُستخدِمين عبر العديد من الأنظمة الأساسية والتطبيقات، وأتمتة عملية تعيين حسابات المُستخدِمين وإلغاء تعيينها.

- **تسجيل الدخول الموحَّد** (Single Sign-On - SSO):
هو عملية الوصول إلى تطبيقات وموارد متعددة باستخدام مجموعة واحدة من بيانات الاعتماد مما يبسط عملية تسجيل الدخول، وتقليل مخاطر الحوادث الأمنيّة المتعلقة بكلمات المرور.
- **خدمات الدليل** (Directory Services):
توفر خدمات الدليل إدارة مركزية لهويات المُستخدِمين والوصول إلى الموارد.
- **التدقيق والإبلاغ** (Auditing and Reporting):
يتم توفير إمكانيات تدقيق وإبلاغ مُفصَّلة تسمح للمؤسسات بتَتبُّع نشاط المُستخدِم، واكتشاف النشاط المشبوه، وتلبية متطلبات الامتثال.
- **إدارة الوصول للصلاحيات** (Privileged Access Management - PAM):
تساعد إدارة الوصول للصلاحيات المؤسسات على تأمين الوصول لصلاحيات الأنظمة والبيانات الحساسة وإدارتها ومراقبتها.

مثال على الدليل النشط Active Directory Example

يسمح **الدليل النشط** (Active Directory) للمسؤولين بإنشاء حسابات المُستخدِمين والمجموعات وأجهزة الحاسب، وإدارتها، والتحكم بالوصول إلى الموارد، وذلك استنادًا إلى **التحكم في الوصول بناءً على الدور** (RBAC). يتضمن الدليل النشط أيضًا نظام مصادقة مدمج يوفِّر مصادقة آمنة للعملاء والخوادم المبنيَّة على نظام التشغيل ويندوز (Windows)، ويتم تنظيم الدليل النشط في بنية هرمية من المجالات والأشجار والغابات، **فالمجال** (Domain) هو مجموعة منطقية من موارد الشبكة مثل: حسابات المُستخدِمين وأجهزة الحاسب التي تشترك في مساحة اسم مشتركة، **والشجرة** (Tree) هي مجموعة مجالات تشترك في مساحة اسم متجاورة، **والغابة** (Forest) هي شجرة ذات مُخطَّط مشترك. يُمكن أيضًا استخدام الدليل النشط لتنفيذ الدخول الموحَّد بما يسمح للمُستخدِمين بالوصول إلى الموارد عبر مجالات أو تفرعات متعددة باستخدام مجموعة واحدة من بيانات الاعتماد، كما يُمكن أن يكون هذا مفيدًا للمؤسسات ذات الشركات الفرعية المتعددة أو التي تحتاج إلى مشاركة الموارد مع الشركاء أو العملاء.



شكل 1.17: هيكلية الدليل النشط

جدول 1.3: الميزات والمشكلات المحتملة لأنظمة التحكم في إدارة الهوية والوصول (IAM)

الميزات	المشكلات المحتملة
توفِّر حلول **إدارة الهوية والوصول** (IAM) تحكمًا مركزيًا في هويات المُستخدِمين والوصول إلى الموارد، ويسمح هذا للمؤسسات بفرض سياسات أمن سيبراني مختلفة مثل: المصادقة متعددة العوامل، وإدارة الوصول إلى الموارد، وذلك استنادًا إلى التحكم في الوصول بناءً على الدور.	يُمكن لحلول **إدارة الهوية والوصول** (IAM) أن تكون معقدة التنفيذ والصيانة، وتتطلب معرفة وموارد متخصصة.
يُمكن لحلول **إدارة الهوية والوصول** (IAM) أتمتة عملية تعيين وإلغاء تعيين حسابات المُستخدِمين، وتقليل الأخطاء وتحسين كفاءة العملية.	قد تتطلب حلول **إدارة الهوية والوصول** (IAM) التكامل مع الأنظمة والتطبيقات الحالية، وقد يتسم ذلك بالصعوبة، وقد يستغرق وقتًا طويلًا لإنجازه.
يُمكن أن توفِّر حلول **إدارة الهوية والوصول** (IAM) إمكانات تدقيق وإبلاغ مُفصَّلة ليسمح للمؤسسات بتَتبُّع نشاط المُستخدِمين واكتشاف النشاط المشبوه، مما يساعد على تلبية متطلبات الامتثال.	عادةً ما تكون حلول **إدارة الهوية والوصول** (IAM) أهدافًا للمهاجِمين، مما يُحتِّم تحديثها ومراقبتها باستمرار للحماية من التهديدات الجديدة.
يُمكن أن توفِّر حلول **إدارة الهوية والوصول** (IAM) أيضًا إمكانات **تسجيل الدخول الموحَّد** (SSO)، مما يُبسِّط عملية تسجيل الدخول، ويقلل من مخاطر الحوادث الأمنيّة المتعلقة بكلمة المرور.	تعتمد حلول **إدارة الهوية والوصول** (IAM) بشكل كبير على البيانات الدقيقة والحديثة التي قد يكون من الصعب الحفاظ عليها خاصة في البيئات الكبيرة والمعقدة.

مهاجمة إدارة الهوية والوصول Attacking an IAM

هناك طرائق عدّة يُمكن للمهاجِم من خلالها محاولة مهاجمة نظام **إدارة الهوية والوصول** (**IAM**):

الهندسة الاجتماعية (Social Engineering):
يُمكن للمهاجِم استخدام تقنيات الهندسة الاجتماعية مثل: التصيد الإلكتروني والتحجج الاحتيالي لخداع المُستخدِمين للكشف عن بيانات اعتمادهم أو إقناعهم بتنفيذ إجراءات تهدد الأمن السيبراني.

هجوم القوة المُفرطة (Brute-Force):
يُمكن للمهاجِم استخدام الأدوات الآلية لتجربة مجموعات مختلفة من أسماء المُستخدِمين وكلمات المرور لتخمين بيانات اعتماد تسجيل الدخول الصحيحة.

رفع مستوى الصلاحيات (Privilege Escalation):
يُمكن للمهاجِم محاولة استغلال الثغرات الأمنيّة في نظام **إدارة الهوية والوصول** (IAM) أو في الأنظمة الأخرى للحصول على إمكانيات وصول عالية والوصول إلى الموارد الحساسة.

التهديدات الداخلية (Insider Threats):
يُمكن أن يكون المهاجِم شخصًا تمت مصادقة معلوماته بالفعل ويمتلك حق الوصول إلى النظام، حيث يُمكنه استخدام إمكانية وصوله لسرقة البيانات الحساسة، أو تعطيل النظام، أو استخدام النظام لإطلاق هجمات على الموارد الأخرى.

هجمات الوسيط (MitM):
يُمكن للمهاجِم اعتراض اتصالات الشبكة واستخدامها لاعتراض أو سرقة المعلومات الحساسة مثل: بيانات اعتماد تسجيل الدخول.

هجمات حجب الخدمة الموزع (DDoS):

يُمكن للمهاجِم استخدام هجوم **حجب الخدمة الموزع** (DDoS) للتغلب على نظام **إدارة الهوية والوصول** (IAM) وتعطيل عملياته، مما يجعله غير قادر على معالجة الطلبات ومصادقة بيانات المُستخدِمين.

تسجيل الدخول الموحَّد (SSO)

تسجيل الدخول الموحَّد (SSO) هي طريقة مصادقة تتيح للمُستخدِمين الوصول إلى تطبيقات وموارد متعددة بمجموعة واحدة من بيانات الاعتماد بدلًا من الحاجة إلى تذكر معلومات تسجيل دخول منفصلة لكل تطبيق وإدخالها، ويُمكن لهذا الأمر تبسيط عملية تسجيل دخول المُستخدِمين والتقليل من مخاطر الحوادث الأمنيّة المتعلقة بكلمة المرور. تُعدُّ بوابة **نفاذ** (Nafath) السعودية مثالًا على التحكم **بتسجيل الدخول الموحَّد** (SSO).

شكل 1.18: وصول المُستخدِم إلى تطبيقات متعددة عبر تسجيل الدخول الموحَّد (SSO)

جدول 1.4: الميزات والمشكلات المحتملة المتعلقة بمصادقة تسجيل الدخول الموحَّد (SSO)

الميزات	المشكلات المحتملة
يُمكن أن يُسهِّل **تسجيل الدخول الموحَّد** (SSO) وصول المُستخدِمين إلى الموارد المطلوبة باستخدام مجموعة واحدة من بيانات اعتماد تسجيل الدخول.	يعتمد **تسجيل الدخول الموحَّد** (SSO) على خادم مصادقة مركزي، وإذا أصبح هذا الخادم غير متاح، فلن يتمكن المُستخدِمون من الوصول إلى الموارد الضرورية.
يُمكن أن يقلِّل **تسجيل الدخول الموحَّد** (SSO) من مخاطر الحوادث الأمنيّة المتعلقة بكلمة المرور مثل: إعادة استخدام كلمة المرور، وهجمات التصيد الإلكتروني، حيث يحتاج المُستخدِمون تذكُّر كلمة مرور واحدة فقط.	يُمكن أن يكون **تسجيل الدخول الموحَّد** (SSO) معقدًا من حيث التنفيذ والصيانة، ويتطلب معرفة وموارد متخصصة.
يُمكن أن يساعد **تسجيل الدخول الموحَّد** (SSO) المؤسسات على الامتثال للمتطلبات التنظيمية لإدارة كلمات المرور، حيث يحتاج المُستخدِمون تذكُّر كلمة مرور واحدة فقط.	يُمكن أن يؤدي **تسجيل الدخول الموحَّد** (SSO) إلى مخاطر أمنية أكبر، حيث يُمكن للمهاجِم الذي يحصل على بيانات اعتماد المُستخدِم الوصول إلى موارد متعددة.

تقييم وتحديد الثغرات الأمنيّة للأنظمة
Assessing and Identifying Vulnerabilities of Systems

هناك العديد من استراتيجيات الأمن السيبراني وتقنياته لتقييم وتحديد الثغرات الأمنيّة ونقاط ضعف أنظمة المعلومات، ومن أبرزها **تقييم الثغرات الأمنيّة** (Vulnerability Assessment – VA) و**اختبار الاختراق** (Penetration Testing – PT)، وهما من الممارسات الأساسية للأمن السيبراني التي تساعد المؤسسات على تقييم وتحديد الثغرات الأمنيّة ونقاط الضعف في أنظمتها، حيث تسمح هذه الإجراءات الاستباقية للمؤسسات بمعالجة المخاطر الأمنيّة المحتملة قبل تَمكُّن الجهات الخبيثة من استغلالها، وفيما يلي شرح لهذه الاستراتيجيات:

تقييم الثغرات الأمنيّة (VA) Vulnerability Assessment

يعمل تقييم الثغرات الأمنيّة بشكل منهجي على تحديد الثغرات الأمنيّة وتحليلها وتحديد أولوياتها في أنظمة المؤسسة أو تطبيقاتها أو شبكاتها، حيث يهدف هذا التقييم إلى اكتشاف نقاط الضعف التي يُمكن للمهاجِمين استغلالها، وتقديم الأفكار حول عوامل الهجوم المحتملة، ويشمل تقييم الثغرات الأمنيّة الجوانب التالية:

المسح (Scanning):
يتم مسح الثغرات الأمنيّة بفحص الأنظمة والتطبيقات بحثًا عن نقاط الضعف المعروفة أو الإعدادات الخاطئة باستخدام أدوات آلية أو تقنيات يدوية.

الإبلاغ (Reporting):
بعد عملية المسح، يتم إنشاء تقرير مُفصَّل يسرد نقاط الضعف التي تم تحديدها، ومدى خطورتها، وتأثيرها المحتمل على المؤسسة.

تحديد الأولويات (Prioritization):
يتم تصنيف الثغرات الأمنيّة بناءً على خطورتها وتأثيرها المحتمل، مما يساعد المؤسسات على تحديد أولويات جهود تصحيحها.

التصحيح (Remediation):
تستخدم المؤسسات النتائج المستخلصة من تقييم الثغرات الأمنيّة لمعالجة الثغرات الأمنيّة المحدَّدة وإصلاحها غالبًا من خلال التصحيح أو تغيير الإعدادات أو تحسينات الأمن الأخرى.

اختبار الاختراق (Penetration Testing - PT):
اختبار الاختراق أو **القرصنة الأخلاقية** (Ethical Hacking) هو تقييم أكثر عمقًا واستهدافًا للوضع الأمني للمؤسسة، حيث يتضمن محاكاة لهجمات حقيقية؛ لاختبار فعالية الضوابط الأمنيّة وتحديد الثغرات الأمنيّة التي يُمكن استغلالها بالنظام. يهدف **اختبار الاختراق** (PT) إلى الكشف عن نقاط الضعف التي قد لا تكشفها عمليات المسح الآلي للثغرات الأمنيّة، وتقييم القدرات الدفاعية الشاملة للمؤسسة، وتشمل الجوانب الرئيسة للاختبار ما يلي:

التخطيط والنطاق (Planning and Scope):
يتم وضع خطة لاختبار الاختراق وتحديد نطاقه بما في ذلك أهدافه، والأنظمة المستهدفة، وحدود الاختبار.

الاستطلاع (Reconnaissance):
يجمَع اختبار الاختراق معلومات حول الأنظمة والبيئة المستهدفة لتحديد الثغرات الأمنيّة المحتملة واتجاهات الهجوم.

الاستغلال (Exploitation):
يحاول المُختبِر استغلال الثغرات الأمنيّة التي تم تحديدها ومحاكاة تصرفات هجوم حقيقي للوصول غير المُصرَّح به، أو الحصول على الامتيازات، أو اختراق البيانات الحساسة.

الإبلاغ (Reporting):
بعد الاختبار، يتم إنشاء تقرير مُفصَّل يُحدِّد الثغرات الأمنيّة التي تم اكتشافها، والاستغلالات الناجحة، وتوصيات المعالجة.

الأمن السيبراني والقرصنة الأخلاقية Cybersecurity and Ethical Hacking

يُطلق لقب **القراصنة الأخلاقيون** (Ethical Hackers) أو **القراصنة ذوي القبعات البيضاء** (White-Hat Hackers) على القراصنة الذين يستخدمون التقنيات والأدوات لتحديد الثغرات الأمنيّة ونقاط ضعف أنظمة المؤسسة، أو شبكاتها، أو تطبيقاتها. يتمثل الاختلاف الأساسي بين القرصنة الأخلاقية والقرصنة الخبيثة في الإجراءات المُستخدَمة والأذونات الممنوحة من المؤسسة المستهدَفة، حيث يعمل القراصنة الأخلاقيون ضمن الحدود القانونية والأخلاقية لمساعدة المؤسسات على تحسين وضعها الأمني، بينما يهدف القراصنة الخبثاء إلى استغلال الثغرات الأمنيّة لأغراض خبيثة أو لتحقيق مكاسب شخصية. من المهم النظر بموضوعية عند مناقشة القرصنة الأخلاقية، حيث يُمكن إساءة فهم المصطلح أو إساءة استخدامه، حيث تؤدّي القرصنة الأخلاقية بلا شك دورًا مهمًا في تحديد الثغرات الأمنيّة، ولكن لا يجب تشجيعها كهواية يقوم بها الجميع، ولا يجب الخلط بينها وبين الممارسات غير القانونية للقراصنة التقليديين. تركز النقاط التالية على الجوانب الحاسمة للحفاظ على التوازن والموضوعية فيما يتعلق بالقرصنة الأخلاقية:

الإذن والتفويض
يجب العمل بإذن صريح من المؤسسة التي يتم اختبارها، مع وجود اتفاقٍ واضحٍ يُحدِّد نطاق أنشطتهم وأهدافها وحدودها.

الامتثال القانوني والتنظيمي
يضمن الامتثال للقوانين واللوائح والمعايير ذات الصلة؛ لضمان أن الأنشطة تقع ضمن الحدود القانونية والأخلاقية، ويساعد على تجنب المشكلات القانونية المحتملة أو العواقب غير المقصودة.

الاحترافية والمسؤولية
الالتزام بقواعد السلوك الصارمة وإثبات الاحترافية، بحيث يتحمل القراصنة الأخلاقيون مسؤولية أفعالهم ويحرصون على عدم التسبب في أي ضرر للأنظمة التي يختبرونها.

الإفصاح والمعالجة
عند اكتشاف الثغرات الأمنيّة المحتملة، يجب على القراصنة الأخلاقيين إبلاغ المؤسسة المستهدَفة فورًا، وتقديم توصيات للمعالجة، ويساعد هذا النهج التعاوني في معالجة مشكلات الأمن بشكل فعَّال مع الحفاظ على الثقة بين القرصان الأخلاقي والمؤسسة.

التعليم والشهادات
يساعد التشجيع على التدريب وتعلُّم القرصنة الأخلاقية على تكوين فهم واضح للمعايير الأخلاقية والمهنية التي يجب الحفاظ عليها.

يؤدّي المتخصِّصون في مجال الأمن دورًا حيويًا في تحديد الثغرات الأمنيّة السيبرانية ومساعدة المؤسسات على تحسين وضعها الأمني، ومع ذلك، فمن الضروري الحفاظ على رؤية متوازنة حول هذه الممارسة لضمان بقائها ضمن الحدود الأخلاقية والقانونية وتثبيط أي إساءة استخدام محتملة للمصطلح أو المهارات المعنية.

جدول 1.5: الأنشطة الرئيسة التي يؤديها متخصصو الأمن السيبراني

النشاط	الوصف
 اختبار الاختراق	تنفيذ اختبارات الاختراق لمحاكاة الهجمات على أنظمة المؤسسة أو شبكاتها أو تطبيقاتها، ويساعد هذا في تحديد الثغرات الأمنيّة القابلة للاستغلال وتقييم فعالية الضوابط الأمنيّة الحالية.
 تقييمات الثغرات الأمنيّة	إجراء تقييمات للثغرات الأمنيّة عن طريق فحص الأنظمة والتطبيقات بحثًا عن الثغرات الأمنيّة أو الإعدادات الخاطئة أو نقاط الضعف المعروفة، ثم يتم تقديم تقرير مُفصَّل عن النتائج التي تم التوصل إليها وترتيب أولوية الثغرات الأمنيّة حسب خطورتها من أجل علاجها.
 تدقيقات الأمن	إجراء عمليات تدقيق أمنية شاملة للبنية التحتية للمؤسسة وسياساتها وإجراءاتها لتقييم وضعها الأمني العام وتحديد مجالات التحسين والتطوير.
 تقييمات الهندسة الاجتماعية	إجراء تقييمات الهندسة الاجتماعية لتقييم قابلية المؤسسة للتعرض للهجمات على العنصر البشري مثل: التصيد الإلكتروني، أو الخداع، أو الاختراق الأمني، كما يُمكن أيضًا تقديم التوصيات لتحسين الوعي والتدريب الأمني للموظفين.
 تقييمات الشبكة اللاسلكية	تقييم أمن الشبكات اللاسلكية للمؤسسة، بما في ذلك شبكات **الواي فاي** (Wi-Fi) و**البلوتوث** (Bluetooth) لتحديد الثغرات الأمنيّة، أو التشفير الضعيف، أو الإعدادات الخاطئة التي قد يستغلها المهاجِمون.
 اختبار تطبيق الويب	اختبار تطبيقات الويب بحثًا عن أي ثغرات أمنية محتملة مثل: حقن النصوص البرمجية بلغة SQL، أو الهجوم البرمجي العابر للمواقع، أو تجاوز عمليات المصادقة، مما يساعد المؤسسات على تأمين خدماتها عبر الإنترنت وحماية بياناتها الحساسة.
 ممارسات فريق الأمن الأحمر	المشاركة في أنشطة فريق الأمن الأحمر، والتصرف كمهاجِمي أنظمة ضمن سيناريو محاكاة يختبر قدرة استجابة المؤسسة للحوادث، واستعداداتها الأمنيّة، ومرونتها الشاملة.
 مراجعة التعليمات البرمجية الآمنة	مراجعة التعليمات البرمجية الخاصة بالمؤسسة بحثًا عن الثغرات الأمنيّة، أو نقاط الضعف المحتملة، ثم تقديم التوصيات لتحسين أمن التعليمات البرمجية وتقليل مخاطر الاستغلال.
 التدريب والتوعية الأمنيّة	مساعدة المؤسسات على تطوير وتقديم برامج التدريب الأمني ومشاركة الخبرات والمعرفة لتثقيف الموظفين حول أفضل ممارسات الأمن السيبراني وتقنيات الهجوم الشائعة.

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. هجمات التصيد المستهدف هي هجمات موزعة ذات مصادر متعددة تستهدف مجموعة كبيرة من الأشخاص.	○	○
2. ملفات تعريف الارتباط هي ملفات نصية صغيرة يتم وضعها على جهاز المُستخدِم بواسطة مواقع الويب لتَتبُّع نشاط التصفح.	○	○
3. يتم استخدام تَتبُّع السلوك حصريًا للأغراض الأمنيّة وليس للإعلانات المستهدفة.	○	○
4. لا يُعدُّ التحكم بالوصول هامًا لحماية أنظمة المعلومات وخصوصية البيانات من الوصول غير المُصرَّح به والتعديل.	○	○
5. ينص مبدأ الحد الأدنى من الصلاحيات والامتيازات على أنه يجب منح المُستخدِمين الحد الأقصى من مستوى الوصول اللازم لأداء أدوارهم الوظيفية.	○	○
6. تُعدُّ نماذج التحكم بالوصول مثل التحكم في الوصول بناءً على السمات (ABAC) والتحكم في الوصول بناءً على الدور (RBAC) مسؤولة عن فرض سياسات الأمن وإدارة وصول المُستخدِم داخل المؤسسة.	○	○
7. تتماثل القرصنة الأخلاقية مع القرصنة الخبيثة من حيث النوايا والسماح.	○	○
8. يجب أن يعمل القراصنة الأخلاقيون دائمًا بإذن صريح من المؤسسة التي يختبرونها.	○	○
9. الإفصاح والمعالجة من الجوانب الأساسية للقرصنة الأخلاقية للحفاظ على الثقة ومعالجة القضايا الأمنيّة بشكل فعَّال.	○	○
10. يقوم فريق قراصنة القبعات البيضاء بعمل تقييمات الهندسة الاجتماعية لمعرفة مدى قدرة المؤسسة الأمنيّة على مواجهة الهجمات على العنصر البشري.	○	○

2 **حلِّل دور حماية البيانات في معالجة قضايا التهديدات التي تواجهها البيانات في العصر الرقمي، وما مخاوف حماية البيانات الرئيسة؟**

3 قيِّم استخدام ملفات تعريف الارتباط في التَتبُّع عبر الإنترنت، وكيف يُمكنها تحسين تجربة المُستخدِم أو إثارة مخاوفه بشأن الخصوصية؟

4 حلِّل أهمية عدم الإنكار في التحكم بالوصول والأمن السيبراني.

5 قيِّم مبدأ الحد الأدنى من الصلاحيات والامتيازات وتأثيره على التحكم بالوصول، وكيف يؤدي الالتزام بهذا المبدأ إلى تقليل المخاطر الأمنيّة داخل المؤسسة؟

6 صِفْ دور القرصنة الأخلاقية في الحفاظ على وضع قوي للأمن السيبراني، وكيف تساهم تلك القرصنة في الأمن العام للمؤسسة؟

7 وضِّح دور الاحترافية والمسؤولية في القرصنة الأخلاقية.

8 قيِّم دور القراصنة ذوي القبعات البيضاء في إجراء عمليات تدقيق الأمن وممارسات فريق الأمن الأحمر.

المشروع

خلال عملك كموظف في شركة مالية كبيرة، تم تكليفك بإنشاء تحليل أمني شامل لمجلس إدارة الشركة، حيث ستعرِض التهديدات من البرمجيات الضارة والهجمات السيبرانية المتقدِّمة وكيف يُمكن لاستراتيجيات إدارة المخاطر مساعدة الشركة في التخفيف من تأثيرها، وستقوم بتحليل التهديدات التي تواجهها الشركات مثل شركتك، والخطوات التي يُمكن اتخاذها لتأمين أنظمة المعلومات الخاصة بها.

1. عرِّف البرمجيات الضارة والهجمات السيبرانية المتقدِّمة واعرِض أمثلة عليها، ثم اشرح عواقب الهجمات الضارة على نظام معلومات الشركة.

2. حدِّد عمليات تحديد المخاطر وقيّمها، ثم صِفْ الاستراتيجيات المختلفة التي يُمكن استخدامها لتقليل المخاطر المرتبطة بالبرمجيات الضارة والهجمات السيبرانية المتقدِّمة.

3. ركِّز على أهمية إدارة المخاطر المستمرة والمراقبة في مجال الأمن السيبراني، واعرض دراسات حالة لمؤسسات تمكنت بشكل فعَّال من إدارة المخاطر التي تشكلها البرمجيات الضارة والهجمات السيبرانية المتقدِّمة.

4. أنشئ عرضًا تقديميًا باستخدام **باوربوينت** (PowerPoint) من أجل تقديمه لمجلس إدارة الشركة، بحيث يتضمن الملاحظات المذكورة أعلاه، ويوجز ضرورة استراتيجيات الأمن السيبراني الفعَّالة وأهميتها في العصر الرقمي.

ماذا تعلّمت

- تعريف الأمن السيبراني.
- تحديد المبادئ الأساسية للأمن السيبراني.
- سرد المسارات الوظيفية الرئيسة في مجال الأمن السيبراني.
- استعراض كيف أصبحت المملكة العربية السعودية دولة رائدة في مجال الأمن السيبراني.
- تحليل الأنواع المختلفة من البرمجيات الضارة.
- تحديد كيفية استخدام مُرتكبي الجرائم السيبرانية للهجمات السيبرانية المتقدِّمة.
- التمييز بين العمليات والأنشطة المختلفة لتحديد المخاطر وتقليلها وإدارتها.
- تحديد مشكلات تهديد البيانات التي يتم تكليف أنظمة الأمن السيبراني بتأمينها.
- تلخيص تقنيات التحكم بالوصول لتأمين أنظمة المعلومات.
- وصف كيفية مساعدة القرصنة الأخلاقية في حماية المؤسسات والشركات.

المصطلحات الرئيسة

Integrity	السلامة
Malware	البرمجيات الضارة
Nonrepudiation	عدم الإنكار
Penetration Testing (PT)	اختبار الاختراق
Risk Identification	تحديد المخاطر
Risk Management	إدارة التهديد
Risk Mitigation	تخفيف المخاطر
Single Sign-On (SSO)	تسجيل الدخول الموحَّد
Vulnerability Assessment (VA)	تقييم الثغرات الأمنيّة
White-Hat Hackers	قراصنة القبعات البيضاء

Access Control	التحكم بالوصول
Authentication	المصادقة
Authorization	التفويض
Availability	التوافر
CIA Triad	مثلث أمن المعلومات
Chief Information Security Officer (CISO)	رئيس إدارة الأمن السيبراني
Confidentiality	السرية
Data Threat	تهديد البيانات
Data Protection	حماية البيانات
Ethical Hacking	القرصنة الأخلاقية
Identity and Access Management (IAM)	إدارة الهوية والوصول

2. الحماية والاستجابة في الأمن السيبراني

سيتعرف الطالب في هذه الوحدة على التهديدات التي تؤثر على أمن العتاد والبرمجيات ونظام التشغيل وكيفية الحماية منها، ثم سيتعرف على الوسائل المستخدَمة لمهاجمة أنظمة الشبكة وكيفية تحليلها ومواجهتها، وطرائق الحماية منها باستخدام بروتوكولات وتقنيات آمنة، وفي الختام سيتعرف على طرائق مختلفة لكيفية استخدام التحليل الجنائي الرقمي والاستجابة للحوادث لحماية الأنظمة واسعة النطاق من الهجمات السيبرانية.

أهداف التعلُّم

بنهاية هذه الوحدة سيكون الطالب قادرًا على أن:

- يُحدِّد التهديدات والثغرات الأمنيّة التي تؤثر على أمن العتاد ونظام التشغيل والبرمجيات.
- يُحلِّل تقنيات تصميم النظام الآمن.
- يُطبِّق إجراءات الأمن الأساسية لحماية الأجهزة والبيانات في ويندوز.
- يَصِف كيفية تأثير هياكل الشبكات وتقنيات الويب على أنظمة الأمن السيبراني.
- يُوضِّح بروتوكولات أمن الشبكة وتقنياتها.
- يُحلِّل حركة بيانات الشبكة باستخدام برنامج واير شارك (Wireshark).
- يَستخدِم خدمة الشبكة الافتراضية الخاصة في ويندوز (Windows VPN).
- يُحلِّل كيفية استخدام التحليل الجنائي الرقمي والاستجابة للحوادث في حماية الأنظمة الرقمية.

الأدوات

- برنامج واير شارك (Wireshark)
- جدار حماية ويندوز ديفندر (Windows Defender Firewall)
- متصفح دي بي إس كيو لايت (DB Browser for SQLite)

رابط الدرس الرقمي

www.ien.edu.sa

الدرس الأول

أمن العتاد والبرمجيات ونظام التشغيل

مقدمة في أمن العتاد والبرمجيات ونظام التشغيل

Introduction to Hardware, Operating and Software System Security

أصبح أمن العتاد والبرمجيات وأنظمة التشغيل من التهديدات المحتملة مطلبًا ضروريًا في الأمن السيبراني، حيث تُشكِّل هذه المُكوِّنات الثلاثة بالإضافة إلى المعلومات والشبكات أساس أي نظام رقمي، ولذا فإن أمنها ضروري لضمان سلامة المُستخدِمين وخصوصيتهم. سيناقش هذا الدرس طرائق أمن العتاد والبرمجيات ونظام التشغيل، ثم سيتم تناول أمن الشبكة في الدرس التالي.

أمن العتاد Hardware Security

يتضمَّن أمن العتاد العناية بالمكوِّنات المادية لنظام الحاسب مثل: المعالجات، والذاكرة، وأجهزة التخزين، كما يتضمَّن اتِّخاذ تدابير معيَّنة لمنع الوصول غير المُصرَّح به أو التخريب المتعمد، وحماية الأجهزة من التَّلف الناتج عن العوامل البيئية، أو اختلالات التيار الكهربائي، وغير ذلك من المخاطر المحتملة. تتضمَّن بعض تقنيات أمن العتاد الشائعة: استخدام **عمليات بدء تشغيل آمنة** (Secure Boot Processes)، واستخدام **وحدات المنصَّة الموثوقة** (Trusted Platform Modules – TPMs) للتشفير، والاستعانة **بمفاتيح أمن عتادية** (Hardware Security Keys) لعمليات المصادقة.

التهديدات الرئيسة لأنظمة العتاد:

- **الهجمات المادية** (Physical Attacks): تشمل الوصول غير المُصرَّح به إلى مكوِّنات الأجهزة أو تغييرها أو سرقتها.
- **المُكوِّنات المزيفة** (Counterfeit Components): تشمل إدخال مُكوِّنات أجهزة زائفة أو مقلدة، أو أجهزة ذات أداء دون المستوى المطلوب في سلسلة توريد الأجهزة، مما قد يُعرِّض الأمن للخطر.
- **أحْصنة طروادة العتادية** (Hardware Trojans): هي دوائر إلكترونية أو مُكوِّنات ضارة مخفيَّة داخل العتاد لديهَا القدرة على اختراق النظام أو تسريب البيانات الحساسة.
- **هجمات القنوات الجانبية** (Side-Channel Attacks): هي الهجمات التي تعتمد على المعلومات التي يُمكن الحصول عليها من العتاد مثل: استهلاك الطاقة، أو الإشعاع الكهرومغناطيسي، أو التوقيت.

ممارسات الأمان لحماية أنظمة العتاد:

- **عملية بدء التشغيل الآمنة** (Secure Boot Process): التأكد من أن عملية بدء التشغيل تستخدِم توقيعًا رقميًا للتحقق من موثوقية نظام التشغيل.
- **وحدات المنصَّة الموثوقة** (TPMs): تضمين هذه الوحدات لتفعيل التشفير المَبني على العتاد، والتخزين الآمن لمفاتيح التشفير.
- **مفاتيح أمن عتادية** (Hardware Security Keys): يتم فيها استخدام **رموز العتاد** (Hardware Tokens)، أو الأجهزة المبنيَّة على الخصائص الحيوية **للمصادقة متعددة العوامل** (MFA).

- **أمن البرامج الثابتة** (Firmware Security): هو ضمان تشفير توقيع تحديثات البرامج الثابتة وإتاحتها للأجهزة بشكلٍ آمن.
- **البيئة الإفتراضية المبنية على العتاد** (Hardware-Based Virtualization): استخدام خصائص العتاد لفرز البيئات الافتراضية وتأمينها.
- **فجوة الشبكة** (Network Air Gap): هي إجراء أمني يقوم بِفَصل العتاد ماديًا عن الشبكات الأخرى لمنع القرصنة.

جدول 2.1: أمثلة على تهديدات أمن العتاد وأفضل ممارسات الأمان

مثال على التهديد	أفضل ممارسات الأمان
حصول شخص غير مُصرَّح له على حق الوصول إلى غرفة الخادم ليتلاعب بالعتاد.	تنفيذ عملية بدأ تشغيل تعتمد التوقيعات الرقمية للتحقُّق من موثوقية نظام التشغيل.
إدخال شريحة ذاكرة وصول عشوائي مزيَّفة في الحاسب، مما يُقوِّض أداء النظام وأمنه.	تضمين وحدة المنصَّة الموثوقة (TPM) في النظام لتوفير تشفير مبني على العتاد وموقع تخزين آمن لمفاتيح التشفير.

أمن نظام التشغيل Operating System Security

يُعدُّ **نظام التشغيل** (Operating System-OS) البرنامج الأساسي الذي يدير عتاد الحاسب وبرمجياته ويعمل كوسيط بين المُستخدِم ومُكوِّنات النظام، ويُعدُّ تأمينه أمرًا حيويًا للحفاظ على أمن النظام بشكل عام. تحتوي أنظمة التشغيل الحديثة على ميزات أمن مدمجة تساعد في الحماية من التهديدات الشائعة، وقد تتضمَّن هذه الميزات: مصادقة المُستخدِم، وأُذونات الملفات والمجلدات، والتشفير، وكذلك جدار الحماية. إن تحديث نظام التشغيل بانتظام باستخدام **حِزم التحديثات والإصلاحات الأمنيّة** (Security Patches)، واستخدام كلمات مرور قوية وفريدة لحسابات المُستخدِمين يُعدُّ من أفضل الممارسات الأساسية للحفاظ على أمن نظام التشغيل.

التهديدات الرئيسة لأنظمة التشغيل:

- **الوصول غير المُصرَّح به** (Unauthorized Access): يتسبب الوصول غير المُصرَّح به إلى نظام التشغيل إلى سرقة البيانات، أو اختراق النظام، أو تعطيله.
- **هجمات رفع مستوى الصلاحيات** (Privilege Escalation): من خلال استغلال الثغرات الأمنيّة للحصول على مستويات وصول أعلى في النظام، أو التحكم بنظام التشغيل.
- **هجمات الجذور المخفية** (Rootkits): هي برامج ضارة يتم إنشاؤها للوصول إلى نظام تشغيل الحاسب دون علم صاحبه والتحكم به.
- **هجمات قطاع بدء التشغيل** (Boot Sector): هي هجمات تستهدف قطاع بدء التشغيل في النظام، مما قد يمنع نظام التشغيل من التحميل أو أداء وظائفه.

ممارسات الأمان لحماية أنظمة التشغيل:

- **مصادقة المُستخدِم:** تتطلب استخدام اسم مُستخدِم فريد، وكلمة مرور قوية ومُعقَّدة لكل حساب مُستخدِم.
- **أُذونات الملفات والمجلدات:** هي إعداد ضوابط وصول مناسبة لتقييد الوصول إلى الملفات والمجلدات الحساسة.
- **التشفير:** يكون باستخدام أدوات تشفير مضمنة في نظام التشغيل لحماية البيانات الحساسة على أجهزة التخزين.
- **جدار الحماية:** تفعيل وإعداد جدار حماية لنظام التشغيل لمراقبة حركة بيانات الشبكة الواردة والصادرة من أو إلى نظام التشغيل والتحكم فيها.
- **تحديثات نظام التشغيل العادية:** من خلال تثبيت حِزم إصلاحات نظام التشغيل والتحديثات الأمنيّة لمعالجة الثغرات الأمنيّة.
- **الإعدادات الأمنيّة الأساسية والتحصين:** عن طريق تطبيق أفضل الممارسات والإعدادات الأمنيّة لنظام التشغيل للحدِّ من تأثير الهجمات المختلفة.

جدول 2.2: أمثلة على تهديدات أمن نظام التشغيل وأفضل ممارسات الأمان

مثال على التهديد	أفضل ممارسات الأمان
تثبيت البرمجيات الضارة بشكلٍ خفي في نظام التشغيل، مما يمنح المهاجِم وصولًا غير مقيد إليه.	استخدام أدوات التشفير المضمنة في نظام التشغيل لحماية البيانات الحسَّاسة على أجهزة التخزين.
استخدام المهاجِم برمجيات ضارة لتغيير قطاع بدء التشغيل في نظام التشغيل، مما يمنع النظام من العمل بشكل صحيح.	تفعيل جدار حماية نظام التشغيل وإعداده لمراقبة حركة بيانات الشبكة الواردة والصادرة والتحكم بها.

أمن البرمجيات Software Security

يتضمَّن أمن البرمجيات حماية البرامج والتطبيقات التي تعمل على نظام الحاسب من الثغرات الأمنيّة والأخطاء البرمجية ونقاط الضعف المحتملة، كما يتضمَّن تطوير ممارسات الترميز الآمن، وتحديث البرمجيات بانتظام باستخدام حِزم التحديثات والإصلاحات الأمنيّة، واستخدام برامج مكافحة الفيروسات لاكتشاف البرامج الضارة وإزالتها، بالإضافة إلى ذلك يضمن أمن البرمجيات تثبيت التطبيقات الموثوقة التي تم التحقق منها فقط على النظام، وتطبيق معايير وصول مناسبة لمنع الاستخدام أو التغيير غير المُصرَّح به.

التهديدات الأساسية لأنظمة البرمجيات:

- **استغلال الثغرات الأمنيّة (Exploitation of Vulnerabilities):** يَستغِّل المهاجِمون الثغرات الأمنيّة للبرمجيات لاختراق الأنظمة، أو للحصول على وصول غير مُصرَّح به.

- **البرمجيات الضارة** (Malware): يُمكن للبرامج الضارة مثل الفيروسات، والديدان، وبرمجيات الفدية وبرامج التجسس المختلفة التسبب بضرر أو سرقة البيانات الحساسة.
- **هجمات حقن النصوص البرمجية** (Injection Attacks): يتم في هذه الهجمات إدخال نصوص أو أوامر برمجية ضارة في النظام البرمجي بما يسمح بالوصول أو التحكم غير المُصرَّح به.
- **الباب الخلفي** (Backdoor): هو خلل أمني في البرمجيات يسمح بإيجاد طريقة للوصول إلى نظام أو جهاز بتجاوز إجراءات المصادقة العادية.
- **تجاوزات سعة المخزن المؤقت** (Buffer Overflows): إذا لم يكن البرنامج معدًّا للتعامل مع كميات كبيرة من البيانات، فمن الممكن أن يتسبب إدخال كمية كبيرة من البيانات في تعطُّل النظام أو إحداث خلل في تنفيذ التعليمات البرمجية، مما قد يسمح بتشغيل التعليمات البرمجية الضارة.

ممارسات الأمان لحماية أنظمة البرمجيات:

- **ممارسات الترميز الآمنة** (Secure Coding Practices): تكون من خلال اعتماد ممارسات مثل: التحقُّق من صِحَّة الإدخال، ومعالجة الأخطاء بشكل مناسب أثناء تطوير البرمجيات.
- **التحديث الدوري للبرمجيات** (Regular Software Updates): تطبيق حِزم التحديثات والإصلاحات الأمنيّة بمجرد صدورها من قِبَل مُصنِّعي البرمجيات.
- **برامج مكافحة الفيروسات** (Antivirus Programs): تثبيت برامج مكافحة الفيروسات وتحديثها لاكتشاف البرمجيات الضارة وإزالتها.
- **البيئة المعزولة لاختبار التطبيق** (Application Sandboxing): من خلال عزل التطبيقات في بيئة مُقيَّدة لتقليل الضرر المحتمل.
- **كَشْف أو منع التسلُّل** (Intrusion Detection/Prevention): يستخدِم المتسلِّلون بوابات الشبكة لإصابة برمجيات النظام، ولذلك يقوم **نظام كَشف التسلُّل** (Intrusion Detection System – IDS) بمراقبة الشبكات بحثًا عن أي نشاط ضار محتمل ومن ثَمّ يتخذ الإجراء المناسب بناءً على ذلك.

جدول 2.3: أمثلة على تهديدات أمن البرمجيات وأفضل ممارسات الأمان

مثال على التهديد	أفضل ممارسات الأمان
استخدام المهاجِم ثغرة أمنية معروفة في تطبيق ويب للوصول غير المُصرَّح به إلى بيانات المُستخدِم.	استخدام التحقق من صحة الإدخال، والتعامل الصحيح مع الأخطاء أثناء تطوير البرمجيات لتقليل احتمالية الاستغلال.
قيام مُطوِّر البرمجيات دون معرفة مسبقة بتضمين مقطع برمجي يسمح بالوصول عن بُعد دون مصادقة في تحديث البرنامج.	تشغيل التطبيقات التي يحتمل أن تكون غير آمنة في بيئة مقيدة لتقليل احتمالية حدوث ضرر.

ترتبط التهديدات وأفضل الممارسات الموضحة سابقًا لأمن العتاد والبرمجيات وأنظمة التشغيل بالعديد من التحديات التي يجب مواجهتها عند حماية أنظمة تقنية المعلومات، ويُوضِّح الجدول 2.4 أهم هذه التحديات.

جدول 2.4: التحديات الرئيسة لحماية العتاد والبرمجيات وأنظمة التشغيل

التحدي	الوصف
أمن نظام العتاد	
العَبَث المادي بالأجهزة	حماية العتاد من الوصول المادي غير المُصرَّح به أو التغيير أو السرقة.
أمن سلسلة التوريد	ضمان أمن وسلامة مُكوِّنات العتاد في جميع مراحل سلسلة التوريد بدءًا من التصنيع إلى التشغيل.
الثغرات الأمنيّة للبرامج الثابتة	تحديد الثغرات الأمنيّة في البرامج الثابتة التي يُمكن للمهاجِمين استخدامها لاختراق العتاد، ومعالجتها بشكل صحيح.
تَقادُم العتاد	التعامل مع مخاطر الأمن المرتبطة بمكوِّنات الأجهزة القديمة أو غير المدعومة.
أمن أنظمة البرمجيات	
تهديدات الثغرات الأمنيّة الصفرية	تحديد الثغرات الأمنيّة للبرامج التي لم تَكُن معروفة سابقًا، ومعالجتها قبل استغلالها من قِبَل المهاجِمين.
تعقيدات البرمجيات	إدارة الحاجة المتزايدة لأنظمة برمجية أكثر تعقيدًا، والتي يُمكن أن تؤدي إلى ثغرات جديدة تجعل من الصعب تحقيق الأمن.
هجمات سلسلة توريد البرمجيات	تأمين سلسلة توريد البرمجيات ومكوِّناتها ضد الاختراقات التي تؤدي إلى إدخال نصوص برمجية ضارة أو إيجاد ثغرات أمنية في تلك البرمجيات.
أمن أنظمة التشغيل	
الثغرات الأمنيّة لنظام التشغيل	تحديد الثغرات الأمنيّة ومعالجتها في نظام التشغيل التي يُمكن للمهاجِمين استغلالها.
رفع مستوى الصلاحيات	منع المهاجِمين من الحصول على مستويات وصول أعلى أو التحكم في نظام التشغيل.
تحصين نظام التشغيل	التنفيذ والصيانة الدورية للإعدادات الأمنيّة اللازمة، وتَبَنِّي أفضل الممارسات لحماية نظام التشغيل.
مشكلات التوافق	التأكد من عدم تأثير الإجراءات الأمنيّة سلبًا على أداء أو توافق التطبيقات التي تعمل على نظام التشغيل.

تقنيات تصميم النظام الآمن Secure System Design Techniques

يُعدُّ التصميم الآمن للنظام نهجًا أساسيًا في الأمن السيبراني لضمان أمن الأنظمة بجميع مكوِّناتها، ويتضمن أخذ التهديدات المحتملة والثغرات الأمنيّة أثناء عملية التطوير في الاعتبار، وتنفيذ تدابير للحَدِّ من المخاطر بشكلٍ استباقي، وفيما يلي بعض الممارسات الأكثر شيوعًا لتصميم نظام آمن:

الأمن من خلال التصميم Security by Design

يدعو مبدأ الأمن من خلال التصميم إلى التكامل بين التدابير الأمنيّة والاعتبارات الأخرى المتعلقة بتطوير النظام أو البرنامج، وبدلًا من إضافة تلك التدابير في وقتٍ لاحق، يتم تضمين بروتوكولات الأمن والإجراءات الأمنيّة الأخرى في المُنتَج منذ البداية. يؤكِّد هذا النهج الاستباقي على إنشاء الأنظمة والتطبيقات بطريقة تكون آمنة بطبيعتها، ويشمل هذا تحديد السياسات والأدوار والمسؤوليات، وضمان سلامة البيانات والخصوصية، وتنفيذ معايير وصول المُستخدِم وممارسات التشفير الآمن، كما يهدف الأمن من خلال التصميم إلى تقليل الثغرات الأمنيّة والحَدّ من تأثير الخروقات الأمنيّة المحتملة.

الدفاع متعدد الطبقات Defense in Depth

الدفاع متعدد الطبقات هو نهجٌ شاملٌ في الأمن السيبراني، يتم من خلاله إضافة طبقات متعددة من الضوابط والتدابير الأمنيّة في كافة مناحي نظام تقنية المعلومات، ويعتمد هذا النهج على المبدأ العسكري القائل بأنه من الصعب على العدو اختراق نظام دفاعي مُعقَّد ومتعدد الطبقات بعكس اختراق حاجز واحد فقط، حيث تهدف هذه الاستراتيجية إلى حماية سلامة المعلومات وتوافُرها وسرِّيتها من خلال استخدام سلسلة من الآليات الدفاعية، بما فيها جُدران الحماية، وأنظمة كشف التسلُّل، وتشفير البيانات، وبرمجيات مكافحة الفيروسات، وإجراءات الأمن المادية. يعتمد هذا المفهوم على مبدأ أنه في حال كانت إحدى طبقات الدفاع غير فعَّالة أو تم اختراقها، فيجب أن تكون الطبقة التالية قادرة على منع الهجوم؛ مما يمنح المؤسسة فرصًا متعددةً للحَدِّ من التهديدات المحتملة.

هناك بعض أوجه التشابه بين نهج الأمن من خلال التصميم ونهج الدفاع متعدد الطبقات، ولكن هناك اختلافات في تطبيقهما، وتوضِّح الأمثلة التالية أوجه الاختلاف في سيناريوهات مختلفة:

تطوير موقع الويب مع الأمن من خلال التصميم (Website Development with Security by Design):
عند تطوير موقع جديد للتجارة الإلكترونية، يقتضي الأمن من خلال التصميم استخدام ممارسات الترميز الآمنة، والتحقق من صِحّة إدخال البيانات لمنع حقن النصوص البرمجية بلغة SQL أو هجمات البرمجة العابرة للمواقع، وتنفيذ مصادقة قوية للمُستخدِم وضوابط للوصول من البداية.

إعداد البنية التحتية للشبكة مع دفاع متعدد الطبقات (Network Infrastructure Setup with Defense in-Depth):
يتم نشر جُدران الحماية في الشبكة، وتنفيذ **أنظمة كشف أو منع التسلُّل** (Intrusion Detection/Prevention Systems-IDS/IPS)، واستخدام برامج حماية قوية للنقاط الطرفية، ووضع خطة استجابة متينة للحوادث، كما تُشكِّل عمليات التدقيق المنتظمة واختبار الاختراق جزءًا أساسيًا من هذه الاستراتيجية.

تطوير الخدمات السحابية مع الأمن من خلال التصميم (Cloud-Based Service Development with Security by Design):
عند تطوير الخدمات السحابية، قد تتضمَّن أفضل الممارسات استخدام واجهات برمجة التطبيقات الآمنة، وآليات مصادقة قوية، والتحكم بالوصول، وتقنيات تشفير البيانات المدمجة.

أمن مركز البيانات المادي مع دفاع متعدد الطبقات (Physical Data Center Security with Defense in-Depth):
لحماية الأمن المادي لمركز البيانات، يستخدِم نهج الدفاع متعدد الطبقات عملية التجزئة لتقسيم الشبكة إلى أقسام فرعية أصغر ومعزولة، ويتم تقسيم الشبكة على مستويات متعددة عادةً بواسطة جُدران الحماية، والشبكات **المحلية الافتراضية** (Virtual LANs – VLANs)، بحيث يجب أن يكون لكل جزء ضوابط أمنية خاصة به مثل: المصادقة، وفحص حركة المرور، وبروتوكولات المراقبة، وذلك لتقليل مخاطر الهجمات.

البرمجة الآمنة Secure Programming

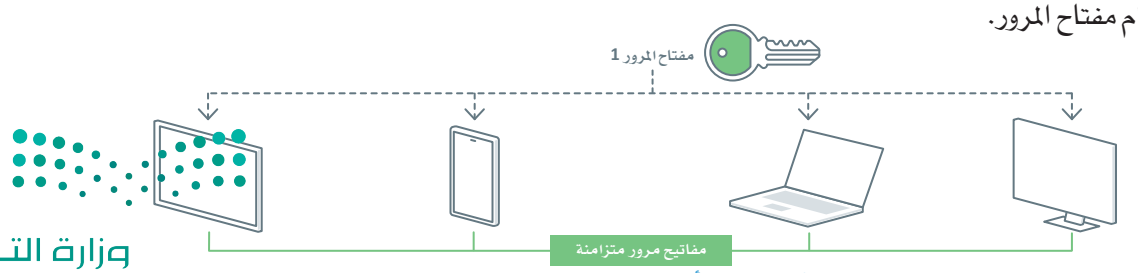
تتضمَّن البرمجة الآمنة كتابة تعليمات برمجية خالية من الثغرات الأمنيّة وغَيرَ قابلةٍ للاستغلال، وتتضمَّن استخدام تقنيات الترميز الآمن وأفضل الممارسات ومنهجيات التطوير لتقليل مخاطر وجود عيوب أمنية في البرمجيات، ويوضِّح الجدول 2.5 السيناريوهات التي يتم فيها تطبيق تقنية البرمجة الآمنة.

جدول 2.5: تطبيقات الأمن بواسطة تقنية البرمجة الآمنة

السيناريو	التطبيق
تطوير تطبيق الويب	يقوم المُطوِّرون بإنشاء تطبيق ويب جديد لنظام مصرفي، و في هذا السياق قد تتضمَّن البرمجة الآمنة التحقق من صحة الإدخال، واستخدام اتصالات آمنة ومشفرة باستخدام **بروتوكول نقل النص التشعبي الآمن** (HTTPS)، و تنفيذ إدارة دخول مناسبة إلى النظام.
تطوير تطبيق الهاتف الذكي	تُوجِب البرمجة الآمنة على المُطوِّرين العاملين في تطوير تطبيق جديد للهاتف الذكي خاص بالرعاية الصحية التأكد من عدم تخزين التطبيق للبيانات الحساسة بشكلٍ غير آمن على الجهاز، وتنفيذ ضوابط وصول قوية، وتشفير جميع البيانات المنقولة بين التطبيق والخادم.

مفاتيح المرور وأمن الأجهزة Passkeys and Device Security

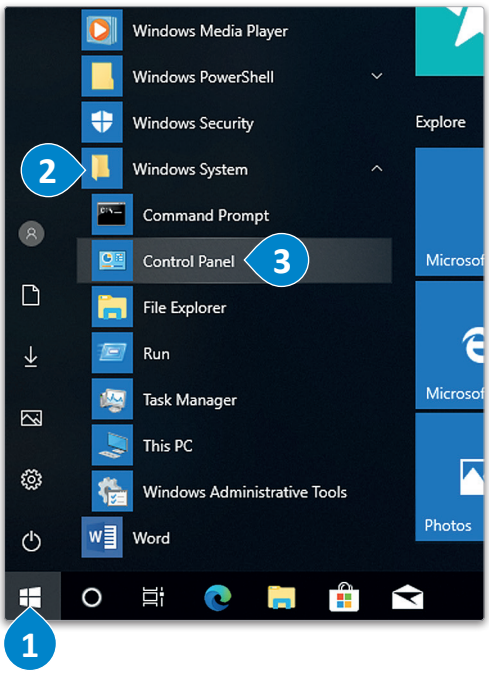
هناك العديد من الأدوات والتقنيات المُستخدَمة لحماية الأجهزة وبياناتها، وقد أثبتت أبسط تدابير الأمن فعاليتها ضد الثغرات الأمنيّة، و**مفاتيح المرور** (Passkeys) أحد الأمثلة الحديثة على هذه التدابير. مفتاح المرور هو بيانات اعتماد رقمية تَحِلُّ مَحَلَّ كلمات المرور التقليدية، وتسمح للمُستخدِمين بتسجيل الدخول إلى التطبيقات ومواقع الويب باستخدام مستشعرات البيانات الحيوية، أو **رقم التعريف الشخصي** (Personal Identification Number-PIN)، أو **أنماط القفل** (Patterns)، حيث تُوفِّر مفاتيح المرور حماية قوية ضد هجمات التصيد الإلكتروني، وتعمل بالطريقة نفسها سواء عند استخدام المتصفح أو أنظمة التشغيل، وعند رغبة المُستخدِمين في تسجيل الدخول بخدمة مفتاح المرور، يساعدهم المتصفح أو نظام التشغيل في اختيار واستخدام مفتاح المرور الصحيح. سيطلب النظام من المُستخدِمين إلغاء قَفل أجهزتهم باستخدام مستشعر البيانات الحيوية، أو **رقم التعريف الشخصي** (PIN) أو نمط القفل، ويتيح ذلك التأكد من أن المُستخدِم الشرعي هو مَنْ يُمكنه استخدام مفتاح المرور حصرًا. تستخدِم مفاتيح المرور **تشفير المفتاح العام** (Public Key Cryptography)، مما يُقلِّل من التهديدات المحتملة لخُروقات البيانات، فعندما ينشئ المُستخدِم مفتاح مرور لموقع أو لتطبيق، يتم إنشاء زوج مفاتيح، مفتاح عام وآخر خاص على جهازه. يُخزِّن الموقع أو التطبيق المفتاح العام فقط الذي يُعدُّ وحده عديم الفائدة للمهاجِم، حيث لا يُمكن اشتقاق المفتاح الخاص بالمُستخدِم من البيانات المخزنة على الخادم، وهو أمرٌ مطلوبٌ لإكمال المصادقة. ترتبط مفاتيح المرور بهُوية موقع الويب أو التطبيق، ولذلك فهي في مأمن من هجمات التصيد الإلكتروني، كما يضمن المتصفح ونظام التشغيل بأنه لا يُمكن استخدام مفتاح المرور إلا في موقع الويب أو التطبيق اللذان أنشئ لهما، ويحمي هذا الإجراء المُستخدِمين من إمكانية تسجيل الدخول إلى موقع ويب مُخادع أو تطبيق مزيف. أحد الأمثلة هو **الهوية السريعة على الإنترنت** (Fast Identity Online – FIDO2)، وهو معيار مصادقة مفتوح يدعم المصادقة دون كلمة مرور باستخدام البيانات الحيوية ومفاتيح الأمن الخارجية، ويوضِّح الشكل 2.1 استخدام مفتاح المرور.



شكل 2.1: مصادقة الأجهزة المحمولة باستخدام مفتاح مرور

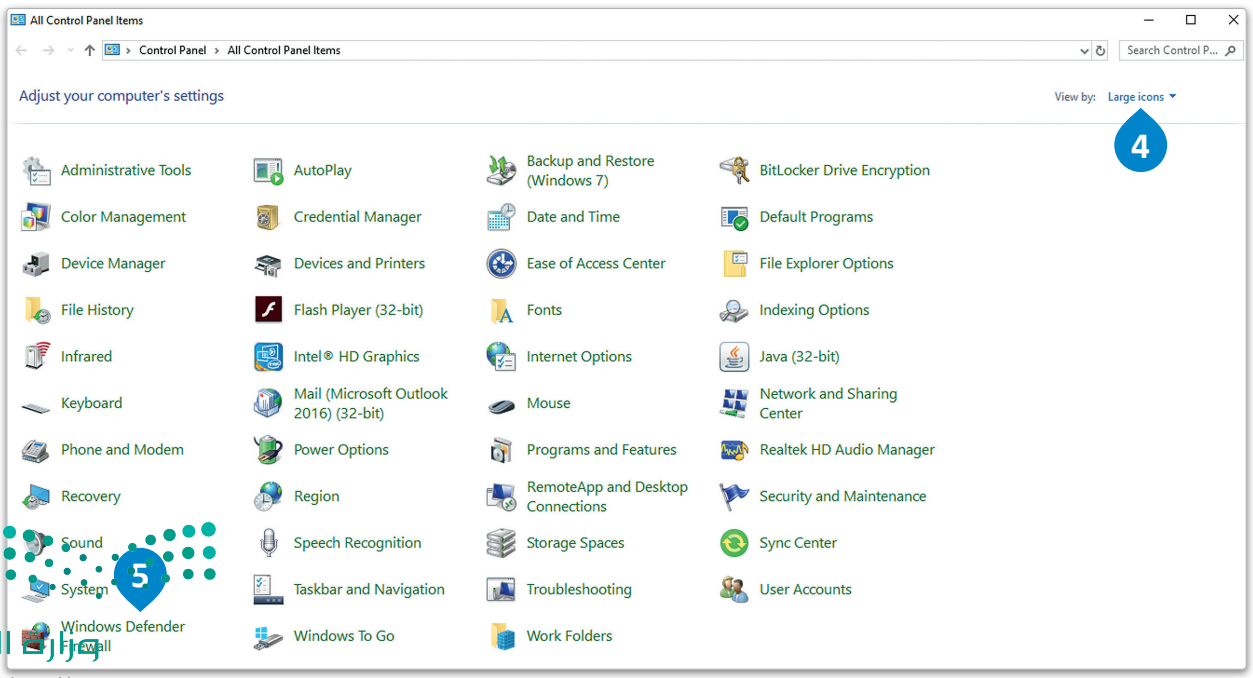
جدار حماية ويندوز Windows Firewall

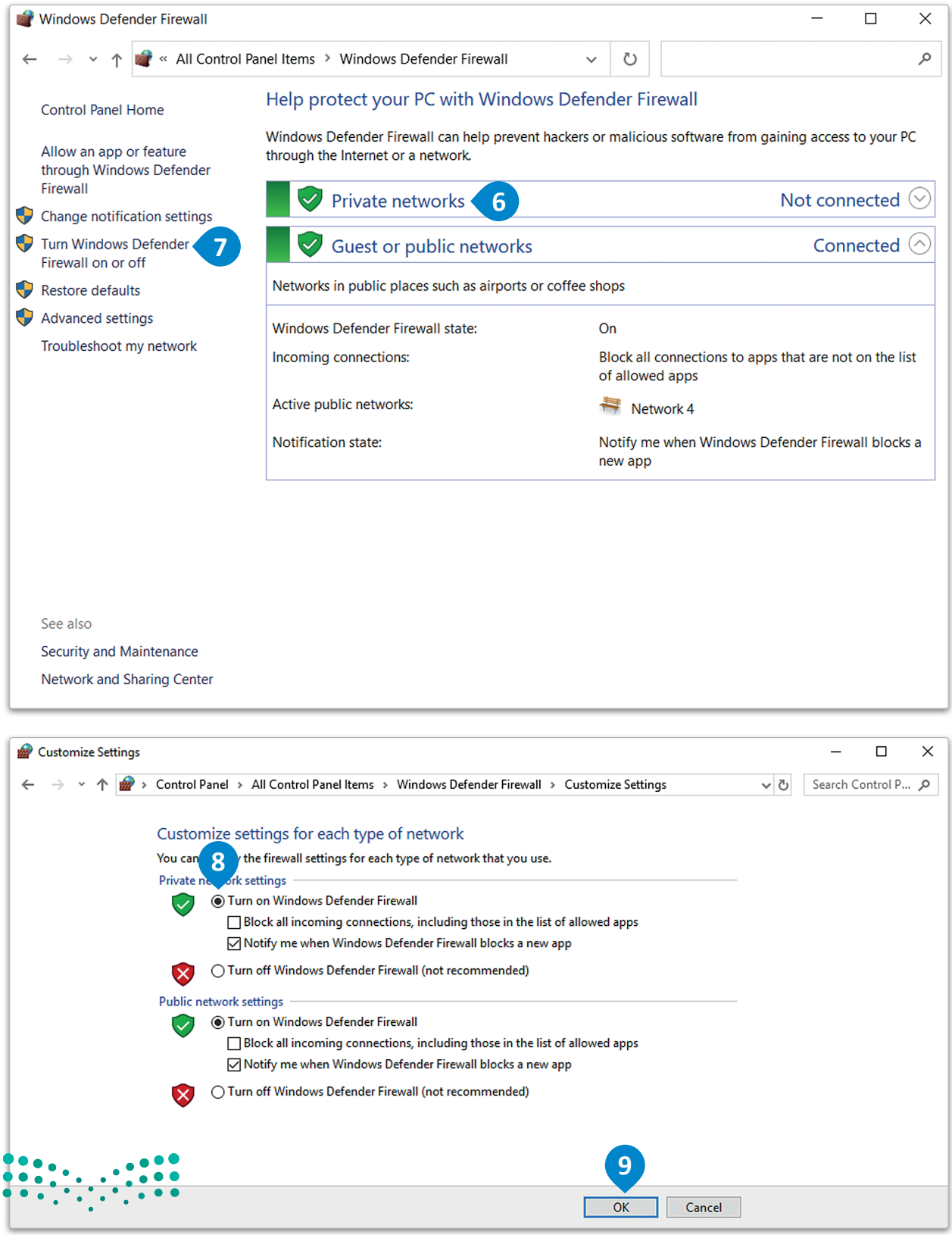
جدار حماية ويندوز المُضمَّن هو تطبيق برمجي يساعد في حماية نظام تشغيل حاسبك بمراقبة حركة بيانات الشبكة الواردة والصادرة، فيسمح لها أو يحظرها بناءً على مجموعة من القواعد، حيث يُشكِّل جدار الحماية حاجزًا بين حاسبك وشبكة الإنترنت أو الشبكات الأخرى، مما يمنع الوصول غير المُصرَّح به إلى نظامك. نَفِّذ الخطوات التالية لمعرفة كيفية تنشيط جدار حماية ويندوز على حاسبك، مع ملاحظة أن هذه الخطوات قد تختلف بصورة طفيفة اعتمادًا على إصدار نظام تشغيل ويندوز المُستخدَم، وفي هذا المثال سيتم استخدام ويندوز **10** (Windows 10):



لتنشيط جدار حماية ويندوز:

- اضغط على زرّ Start (بدء) في نظام تشغيل ويندوز. 1
- اضغط على Windows System (نظام ويندوز)، 2 ثم اضغط على تطبيق Control Panel (لوحة التحكم). 3
- غَيِّر إعدادات العرض إلى Large icons (أيقونات كبيرة). 4
- اضغط على خيار Windows Defender Firewall (جدار حماية ويندوز). 5
- تَحقَّق من لون الدرع الأخضر الذي يشير إلى تمكين جدار الحماية. 6
- اضغط على خيار Turn Windows Defender Firewall on or off (تشغيل جدار حماية ويندوز ديفندر أو إيقاف تشغيله). 7
- اضغط على أزرار الاختيار لتنشيط جدار الحماية أو إلغاء تنشيطه. 8
- اضغط على OK (موافق). 9





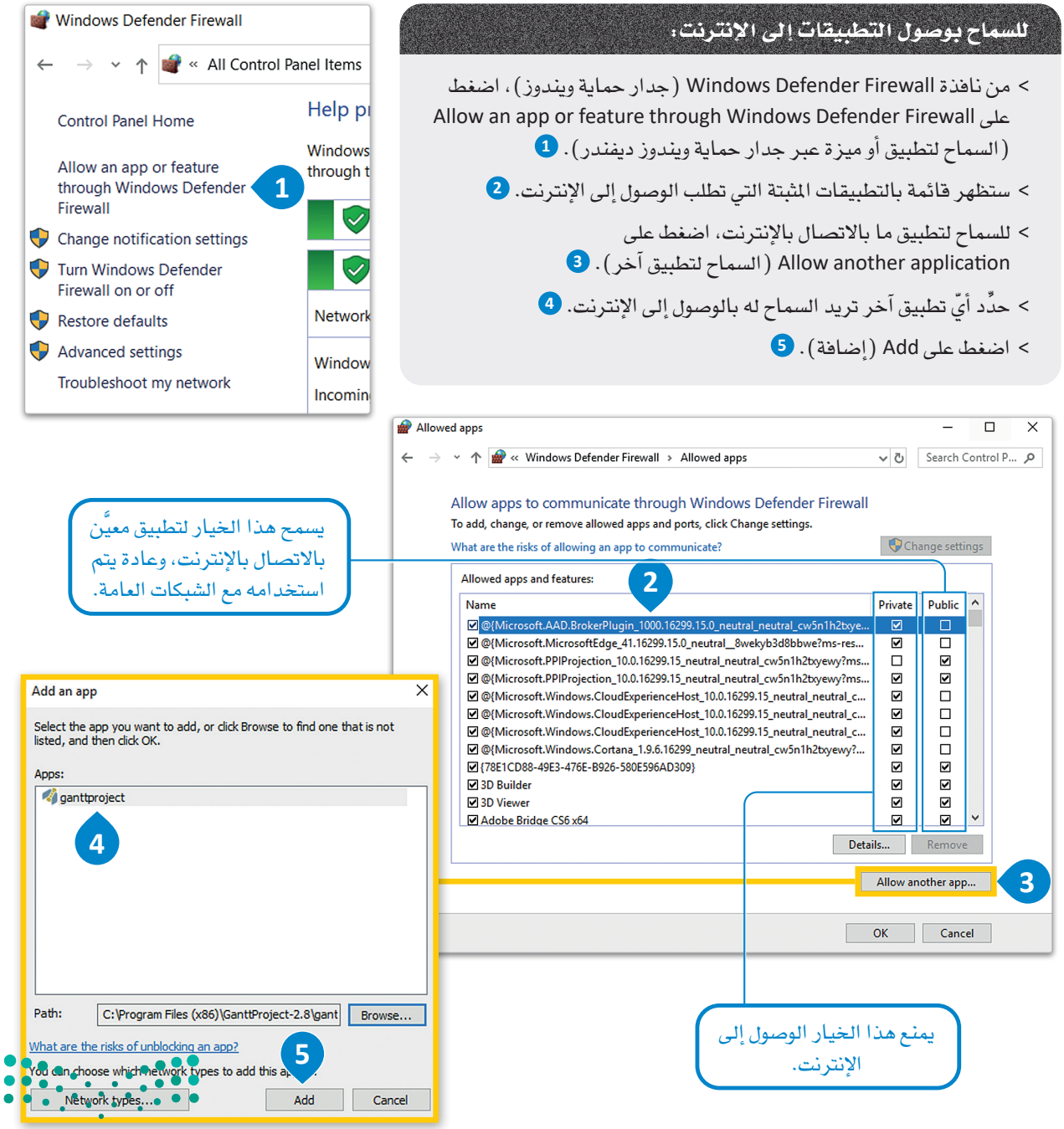
شكل 2.2: تشغيل جدار حماية ويندوز

السماح للتطبيقات الموجودة على حاسبك بالوصول إلى الإنترنت
Allowing Internet Access to Applications on your PC

يُوفِّر ويندوز العديد من ميزات الأمن لحماية حاسبك وبياناتك من الوصول غير المُصرَّح به، ومن البرمجيات الضارة والهجمات الأخرى. على الرغم من أن جدار الحماية يعمل بصورة جيدة في إدارة التطبيقات وتقييد اتصالات الشبكة، إلا أنه قد يتطلب منك عمل بعض الإجراءات الأمنيّة يدويًا للسماح للتطبيقات أو حظرها.

للسماح بوصول التطبيقات إلى الإنترنت:

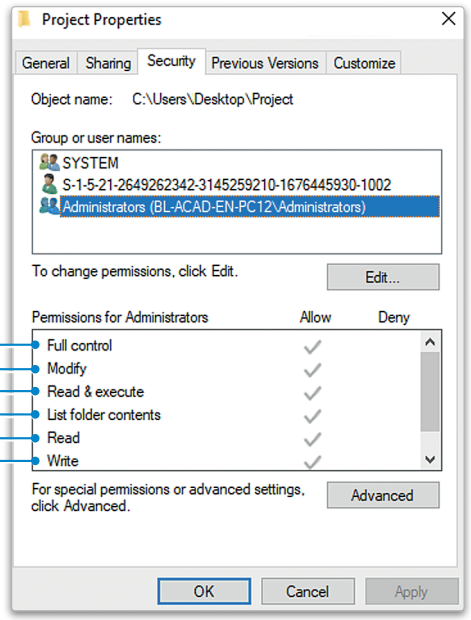
- من نافذة Windows Defender Firewall (جدار حماية ويندوز)، اضغط على Allow an app or feature through Windows Defender Firewall (السماح لتطبيق أو ميزة عبر جدار حماية ويندوز ديفندر). 1
- ستظهر قائمة بالتطبيقات المثبتة التي تطلب الوصول إلى الإنترنت. 2
- للسماح لتطبيق ما بالاتصال بالإنترنت، اضغط على Allow another application (السماح لتطبيق آخر). 3
- حدِّد أيّ تطبيق آخر تريد السماح له بالوصول إلى الإنترنت. 4
- اضغط على Add (إضافة). 5



شكل 2.3: السماح بوصول التطبيقات إلى الإنترنت

تعديل أذونات الملفات والمجلدات على حاسبك
Modifying File and Folder Permissions on your PC

يُعدُّ التحكم في الوصول إلى الملفات والمجلدات أحد الإجراءات الأساسية لتأمين أنظمة المعلومات. يُوفِّر ويندوز واجهة لتعيين الأذونات والوصول إلى المجلدات والملفات المختلفة الموجودة على النظام، وسيؤدي هذا إلى منع المُستخدِمين غير المرغوبين من الوصول إلى البيانات الحساسة. تستخدم أنظمة ويندوز أذونات **نظام ملفات التقنية الجديدة** (New Technology File System – NTFS)، وهي مجموعة عناصر تحكم في الوصول تُستخدَم لتقييد أو منح أذونات وصول المُستخدِمين والمجموعات إلى الملفات والمجلدات، وتُمكِّن أذونات **نظام ملفات التقنية الجديدة** (NTFS) المسؤولين من تعيين أذونات دقيقة للمُستخدِمين والمجموعات على مستوى الملفات والمجلدات، مما يسمح بالتحكم الدقيق في من يُمكنه الوصول إلى ملفات ومجلدات معيَّنة أو تعديلها أو حذفها. من أكثر أذونات **نظام ملفات التقنية الجديدة** (NTFS) شيوعًا ما يلي:

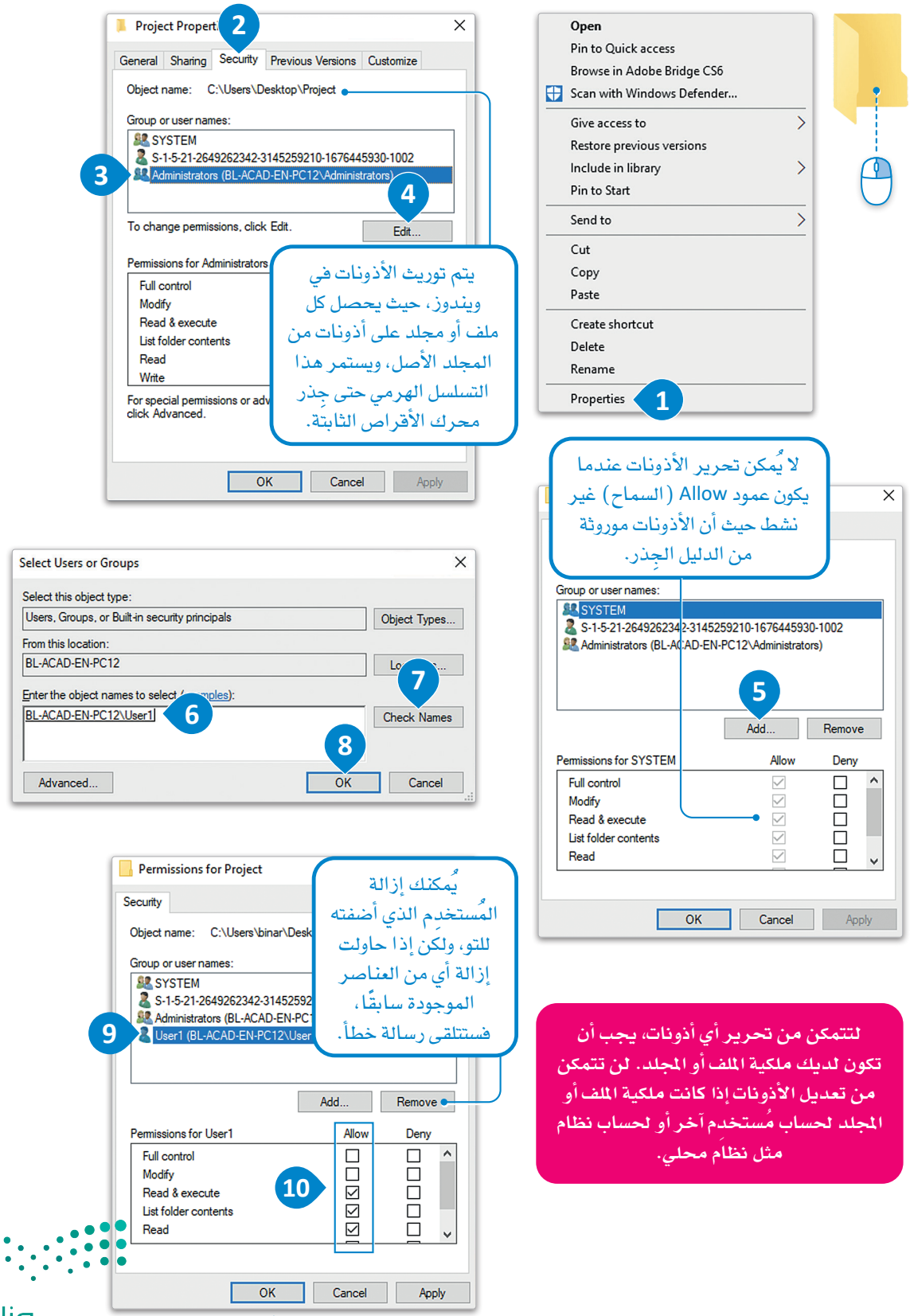


- **Full Control** (تحكم كامل): يُوفِّر للمُستخدِم أو المجموعة تحكمًا كاملًا في الملف أو المجلد، بما في ذلك القدرة على تعديل الأذونات ذاتها، والحذف، والحصول على الملكية للملف أو المجلد.
- **Modify** (تعديل): يسمح للمُستخدِمين بتعديل الملفات أو المجلدات، بما في ذلك إنشاء ملفات ومجلدات فرعية جديدة.
- **Read Execute** (قراءة وتنفيذ): يسمح للمُستخدِمين بقراءة وعرض الملفات والمجلدات، وتنفيذها.
- **List Folder Contents** (سرد محتويات المجلد): يسمح للمُستخدِمين بعرض محتويات المجلد، ولكن لا يسمح بقراءة الملفات الموجودة داخله أو تعديلها أو تنفيذها.
- **Read** (قراءة): يسمح للمُستخدِمين بعرض الملفات والمجلدات.
- **Write** (كتابة): يسمح للمُستخدِمين بإنشاء ملفات ومجلدات جديدة.

تُوضِّح الإرشادات التالية كيفية تعديل الأذونات والوصول إلى مجلد لمُستخدِم أو لمجموعة معيَّنة.

لتعديل أذونات الملفات والمجلدات لمُستخدِم معيَّن:

> اضغط بزرّ الفأرة الأيمن على الملف أو المجلد المطلوب، ثم اضغط على Properties (خصائص). 1
> اضغط على علامة تبويب Security (الأمان). 2
> يُمكنك عرض قائمة جميع المُستخدِمين ممن لديهم أذونات. 3
> اضغط على زرّ Edit (تحرير) لتعديل أذونات مُستخدِم أو مجموعة. 4
> اضغط على زرّ Add (إضافة) لإضافة مُستخدِم أو مجموعة جديدة. 5
> إذا كنت بحاجة إلى تغيير أذونات مُستخدِم أو مجموعة، فاكتب اسمها. 6
> اضغط على زرّ Check Names (التحقق من الأسماء) للتحقُّق من صحة النص المُدخَل. 7
> اضغط على OK (موافق). 8
> يُمكنك عرض المُستخدِم الجديد أو المجموعة الجديدة في القائمة المُحدَّثة. 9
> استخدِم صناديق التحديد لتعيين الأذونات التي تريدها. 10



لتتمكن من تحرير أي أذونات، يجب أن تكون لديك ملكية الملف أو المجلد. لن تتمكن من تعديل الأذونات إذا كانت ملكية الملف أو المجلد لحساب مُستخدِم آخر أو لحساب نظام مثل نظام محلي.

شكل 2.4: تعديل أذونات الملفات والمجلدات لمُستخدِم معيَّن

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. يتضمَّن أمن العتاد العناية بالمكوِّنات المادية لنظام الحاسب.	○	○
2. البرمجيات الضارة هي تعليمات برمجية ضارة يتم تشغيلها بحالةٍ أو حدث معيَّن.	○	○
3. تُستخدم تقنية البيئة المعزولة (Sandboxing) لعزل التطبيقات عن نظام التشغيل الرئيس.	○	○
4. يشمل أمن البرمجيات تثبيت برامج مكافحة الفيروسات لاكتشاف البرامج الضارة وإزالتها.	○	○
5. يتم استخدام عمليات بدء التشغيل الآمنة للتحقق من أصالة نظام التشغيل قبل بدء تشغيله.	○	○
6. لا تعتمد مفاتيح المرور على استخدام البيانات الحيوية لمصادقة المُستخدِم.	○	○
7. يتضمن أمن البرامج الثابتة التأكد من توقيع تحديثات البرامج الثابتة بشكل مشفر وإتاحتها للأجهزة بشكلٍ آمن.	○	○
8. يُستخدم التشفير لحماية البيانات الحساسة على أجهزة التخزين.	○	○
9. يجب تثبيت تحديثات نظام التشغيل بصورة منتظمة لمعالجة أي ثغرات أمنية.	○	○
10. الأمن من خلال التصميم نهج استباقي لتطوير أنظمة وتطبيقات آمنة من خلال دمج التدابير والاعتبارات الأمنيّة بعد إتمام عملية التطوير.	○	○

2 قيِّم المخاطر المرتبطة بمكوِّنات العتاد القديم أو غير المدعومة.

3 قارِن بين التحديات التي تواجه ضمان أمن العتاد وأمن أنظمة البرمجيات.

4 حلِّل أفضل الممارسات الرئيسة لحماية أنظمة التشغيل.

5 قيِّم فعالية تقنيات تصميم النظام الآمن المُستخدَمة لحماية الأنظمة الرقمية.

6 اسرُد بعض الأمثلة على تطبيقات عملية الأمن من خلال التصميم.

7 صِف كيف تُستخدَم مفاتيح المرور كطريقة مصادقة حديثة.

رابط الدرس الرقمي

www.ien.edu.sa

هياكل الشبكات وتقنيات الويب في الأمن السيبراني

Network Structures and Web Technologies in Cybersecurity

يُعدُّ فهم هيكلية الشبكات وتقنيات الويب أمرًا بالغ الأهمية في الأمن السيبراني، حيث ترتبط هذه العناصر بطبيعة التهديدات، وبالتدابير الوقائية التي يُمكن اتخاذها للحدِّ منها، وتتكوَّن الشبكات من أجهزة مترابطة تتبادل المعلومات مع بعضها البعض، بينما تتيح تقنيات الويب إنشاء ومشاركة المحتوى والتطبيقات عبر الإنترنت. يُمكن وصف الإنترنت بأنه شبكة مكوَّنة من مجموعة من الشبكات، ومع ازدياد عدد الأجهزة والخدمات المقدَّمة عبر الويب، فإن هذه الأنظمة تزداد تعقيدًا، وكذلك تزداد نقاط ضعفها. تؤثر هيكلية الشبكات وتقنيات الويب بشكل مباشر على أنواع التهديدات التي يُمكن مواجهتها في مجال الأمن السيبراني، فعلى سبيل المثال: قد تواجه الشبكات هجمات **رفض الخدمة الموزع** (DDoS) التي بدورها تؤثر على الخدمات وتعطلها عن طريق إغراقها بحركة بيانات ضخمة، وقد تتعرض تقنيات الويب كذلك للتهديدات مثل هجمات **البرمجة العابرة للمواقع** (XSS) وهجمات **حقن النصوص البرمجية بلغة SQL** (SQL injection)، حيث يستغل المتسلِّلون ثغرات تطبيقات الويب للوصول غير المُصرَّح به إلى البيانات الحساسة. تُحدِّد هيكلية الشبكات وتقنيات الويب المُستخدَمة طبيعة التدابير الوقائية التي يُمكن استخدامها لحمايتها، فعلى سبيل المثال: يُمكن لتجزئة الشبكة عزل الأنظمة الهامة وتقليل نطاق الهجوم المحتمل، وفي المقابل يُمكن **لأنظمة كشف التسلُّل** (IDSs) وجُدران الحماية المساهمة في مراقبة تدفق حركة البيانات داخل الشبكة وخارجها والتحكم بها. يُمكن أن تساعد ممارسات البرمجة الآمنة والمناسبة في تقنيات الويب مثل: التحقق من صحة الإدخال، ومعالجة الأخطاء المناسبة في منع استغلال الثغرات الأمنيّة. فيما يلي عرض لأهم المفاهيم الأساسية الخاصة بالشبكات وتقنية الويب المؤثرة على تهديدات الأمن السيبراني وتدابير الحماية.

مفاهيم الشبكات الأساسية Fundamental Networking Concepts

مُخطَّطات الشبكة (Network Topologies):

هي الترتيب المادي أو المنطقي للأجهزة في الشبكة، وتشمل الهياكل الشائعة للشبكات: الهيكل النجمي والحلقي والخطي والشبكي والهجين.

أجهزة الشبكة (Network Devices):

هي مُكوِّنات الأجهزة الأساسية التي تُسهِّل الاتصال داخل الشبكات مثل: **المحوِّلات** (Switches) و**الموجِّهات** (Routers) و**جُدران الحماية** (Firewalls) و**نقاط الوصول** (Access Points).

وسائط النقل (Transmission Media):

هي الوسائل المادية أو اللاسلكية التي يتم من خلالها نقل البيانات بين الأجهزة في الشبكة، وتشمل كابلات **الشبكة المحلية** (Ethernet) مثل: الكابلات المزدوجة أو الكابلات المحورية أو الألياف الضوئية، والتقنيات اللاسلكية مثل: **الواي فاي** (Wi-Fi) أو **البلوتوث** (Bluetooth) أو **الشبكات الخلوية** (Cellular Networks).

بروتوكولات الشبكة (Network Protocols):

هي مجموعة قواعد وتعريفات تحدِّد كيفية اتصال الأجهزة وتبادل المعلومات داخل الشبكة، وتعمل البروتوكولات في طبقات مختلفة من **نموذج الربط البيني للأنظمة المفتوحة** (Open Systems Interconnection – OSI) أو نماذج بروتوكول TCP / IP، وتتضمَّن الأمثلة بروتوكولات HTTP/S وFTP وTCP وUDP وIP.

مُكوِّنات الشبكات الأساسية Fundamental Networking Components

المحوِّلات (Switches):
هي أجهزة الشبكة المسؤولة عن توجيه حركة البيانات داخل **شبكة محلية** (Local Area Network – LAN)، وتوصيل الأجهزة، والتأكد من وصول حزم البيانات إلى وجهاتها المقصودة.

الموجِّهات (Routers):
هي الأجهزة التي تعيد توجيه حزم البيانات بين الشبكات المختلفة، وتُحدِّد المسار الأكثر كفاءة لنقل البيانات.

جُدران الحماية (Firewalls):
هي أجهزة حماية تراقب وتتحكم في حركة بيانات الشبكة الواردة والصادرة بناءً على قواعد أمن محدَّدة مسبقًا، وتحمي الشبكات الداخلية من الوصول غير المُصرَّح به والهجمات السيبرانية المحتملة.

نقاط الوصول (Access Points):
هي أجهزة الشبكة التي تُوفِّر اتصالًا لاسلكيًا بالأجهزة الأخرى، وتُمكِّنها من الاتصال بالشبكة والتواصل مع الأجهزة أو الأنظمة الأخرى.

بروتوكولات الشبكات الأساسية Fundamental Networking Protocols

بروتوكول الإنترنت (Internet Protocol – IP):
مسؤول عن عنونة حزم البيانات وتوجيهها عبر الشبكات بما يضمن وصولها إلى الوجهات المقصودة.

بروتوكول الإنترنت الآمن (Internet Protocol Security – IPSec):
يشير إلى مجموعة بروتوكولات مُستخدَمة لتأمين اتصالات **بروتوكول الإنترنت** (IP) من خلال مصادقة وتشفير كل حزمة IP في تدفق البيانات، ويعمل في طبقة الشبكة الخاصة **بحزمة بروتوكولات الإنترنت** (Internet Protocol Suite) مما يساعد في حماية أي حركة بيانات للتطبيق عبر شبكة **بروتوكول الإنترنت** (IP).

بروتوكول التحكم بالنقل (Transmission Control Protocol – TCP):
يضمن نقل البيانات بشكل موثوق من خلال إنشاء اتصال بين الأجهزة وتسلسل حزم البيانات وإدارة تدفق المعلومات.

بروتوكول أمن طبقة النقل/ بروتوكول طبقة المنافذ الآمنة
(Secure Sockets Layer / Transport Layer Security – SSL/TLS):
بروتوكولات تشفير تُوفِّر اتصالًا آمنًا عبر الشبكة عن طريق تشفير البيانات المتبادلة بين عميل وخادم، وتُستخدم بشكل واسع في تصفح الويب والبريد الإلكتروني والتطبيقات الأخرى التي تتطلب نقل بيانات آمن.

بروتوكول حِزم بيانات المُستخدم (User Datagram Protocol – UDP):
بروتوكول غير موثوق به يُستخَدم مع التطبيقات التي تتطلب تسليمًا سريعًا للبيانات، ولكنها لا تتطلب الميزات المعقدة **لبروتوكول التحكم بالنقل** (TCP).

بروتوكول نقل النص التشعبي (Hypertext Transfer Protocol – HTTP):
يستخدم لنقل المحتوى المبني على الويب بين عميل (على سبيل المثال متصفح الويب) وخادم باستخدام اتصال بواسطة **بروتوكول التحكم بالنقل** (TCP)، مما يتيح تبادل النصوص والصور وعناصر الوسائط المتعددة الأخرى.

بروتوكول نقل النص التشعبي الآمن (Hypertext Transfer Protocol Secure – HTTPS):
إصدار مشفر من **بروتوكول نقل النص التشعبي** (HTTP) يستخدِم **بروتوكول أمن طبقة النقل/ بروتوكول طبقة المنافذ الآمنة** (SSL / TLS) بدلًا من استخدام **بروتوكول التحكم بالنقل** (TCP) مباشرة، ويتم استخدامه حاليًا في غالبية خدمات الإنترنت.

بروتوكول نقل الملفات (File Transfer Protocol – FTP):
بروتوكول قياسي لنقل الملفات بين عميل وخادم عبر الشبكة، مما يسمح للمُستخدِمين بتحميل الملفات وتنزيلها وإدارتها على نظام بعيد.

بروتوكول نقل الملفات الآمن (Secure File Transfer Protocol – SFTP):
إصدار آمن من **بروتوكول نقل الملفات** (FTP) حيث يستخدِم **بروتوكول النقل الآمن** (Secure Shell – SSH) لتشفير البيانات أثناء الإرسال، مما يُوفِّر طبقة إضافية من الأمن لعمليات نقل الملفات.

نظام أسماء النطاقات (Domain Name System–DNS):
بروتوكول يقوم بترجمة تسميات النطاقات التي يُمكن قراءتها (على سبيل المثال www.example.com) إلى عناوين **بروتوكول الإنترنت** (IP)، مما يسمح للمُستخدِمين بالوصول إلى مواقع الويب وموارد الشبكة الأخرى باستخدام تسميات يسهل فهمها كعناوين **مُحدِّد موقع الموارد المُوحَّد** (Unified Resource Locator –URL).

بروتوكول التهيئة/الإعداد الديناميكي للمضيف (Dynamic Host Configuration Protocol– DHCP):
بروتوكول إدارة الشبكة ويقوم تلقائيًا بتعيين عناوين **بروتوكول الإنترنت** (IP) ومعلومات تهيئة/إعداد الشبكة الأخرى للأجهزة الموجودة على الشبكة، مما يسهِّل من عملية إدارة الشبكة ويقلِّل من مخاطر التعارض بين عناوين **بروتوكول الإنترنت** (IP).

بروتوكول إدارة الشبكة البسيط (Simple Network Management Protocol –SNMP):
بروتوكول لمراقبة وإدارة أجهزة الشبكة مثل: الموجِّهات، والمحوِّلات، والخوادم من خلال جمع وتنظيم المعلومات حول أدائها واستخدامها وحالتها.

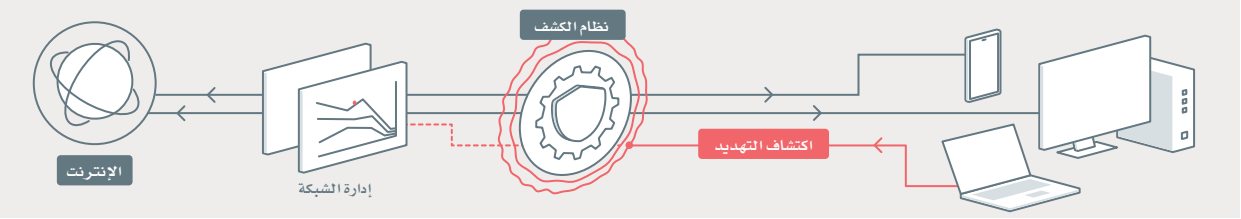
تقنيات أمن الشبكات والويب Network and Web Security Technologies

من المهم في الأمن السيبراني فهم واستخدام بروتوكولات وتقنيات أمن الشبكة المختلفة لحماية سلامة البيانات والأنظمة وضمان سريتها وتوافرها، وفيما يلي أكثر إجراءات أمن الشبكة شيوعًا وضرورة.

أنظمة كشف التسلُّل Intrusion Detection Systems (IDSs)

نظام كشف التسلُّل (IDS) هو تقنية أمنية تراقب حركة البيانات في الشبكة بحثًا عن أي مؤشرات أو دلائل على وجود نشاط ضار أو اختراق أمني في الشبكة وأجهزتها. يُمكن لأنظمة كشف التسلُّل إصدار تنبيهات عند اكتشاف تهديدات محتملة، مما يسمح لمسؤولي الشبكة بالاستجابة بشكلٍ سريع، والعمل على إيقاف الهجوم أو الحد من تأثيره، وهناك نوعان من **أنظمة كشف التسلُّل** (IDSs):

- **نظام كشف التسلُّل المُستند إلى الشبكة** (Network-based IDS - NIDS):
يُحلِّل هذا النوع من الأنظمة حركة بيانات الشبكة، ويبحث عن الأنماط المشبوهة أو أي مؤشرات للوصول غير المُصرَّح به.
- **نظام كشف التسلُّل المُستند إلى المُضيف** (Host-based IDS - HIDS):
يتم تثبيت هذا النوع من **نظام كشف التسلُّل** (IDS) على أجهزة مستقلة مثل: الخوادم أو حاسبات محطات العمل، ويراقب هذا النظام نشاط النظام المحلي بحثًا عن أي مؤشرات اختراق أو وصول غير مُصرَّح به.

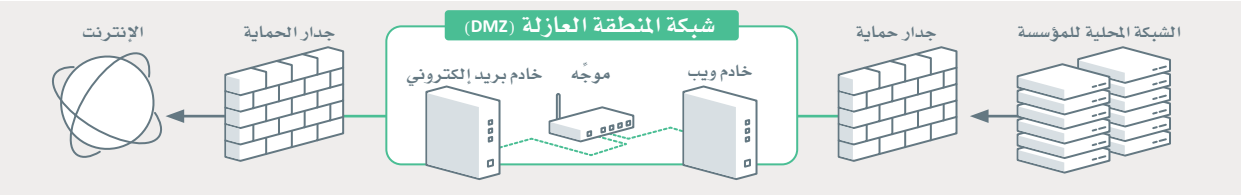


شكل 2.5: تمثيل نظام كشف التسلُّل

المناطق العازلة Demilitarized Zones (DMZs)

تُطلَق تسمية **منطقة عازلة** (DMZ) على جزء من الشبكة يقع بين شبكة المؤسسة الداخلية والشبكة الخارجية غير الموثوق بها، مثل الإنترنت، وتم تصميم هذه المنطقة لتوفير طبقة إضافية من الحماية، وذلك بعَزل الخدمات التي يجب الوصول إليها عبر الإنترنت مثل: خوادم الويب أو خوادم البريد الإلكتروني عن الشبكة الداخلية للمؤسسة، ومن خلال وضع

التي يتم الوصول إليها عبر الإنترنت في **منطقة عازلة** (DMZ)، يتم احتواء نطاق أي هجمات أو ثغرات محتملة داخل تلك المنطقة والحَدِّ من احتمالات تأثيرها على الشبكة الداخلية، ويسمح هذا التكوين للمؤسسات بالحفاظ على مستوى أعلى من الأمن لأنظمتها وبياناتها الهامة.

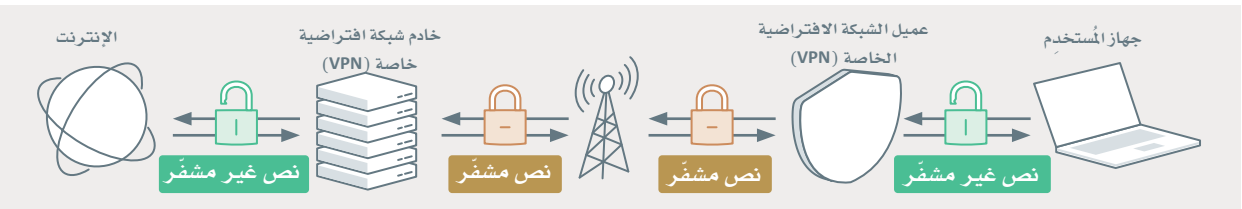


شكل 2.6: هيكلية شبكة المنطقة العازلة (DMZ)

الشبكات الافتراضية الخاصة Virtual Private Networks (VPNs)

الشبكة الافتراضية الخاصة (VPN) هي تقنية تُنشئ اتصالًا آمنًا ومشفّرًا بين جهاز المُستخدِم وشبكة أخرى بعيدة غالبًا عبر الإنترنت، وتحمي الشبكات الافتراضية الخاصة سرية البيانات المنقولة وسلامتها بين جهاز المُستخدِم والشبكة البعيدة، مما يضمن بقاء المعلومات الحساسة مُؤمَّنة حتى عند إرسالها عبر شبكات غير آمنة.

توفِّر **الشبكات الافتراضية الخاصة** (VPNs) ميزات إضافية مثل: تجاوز القيود الجغرافية، وحماية خصوصية المُستخدِم، والسماح بالوصول عن بُعد إلى الشبكات الآمنة. يتم استخدام هذه التقنيات بشكل شائع من قِبل الشركات والأفراد على حدٍّ سواء للحفاظ على الأمن والخصوصية أثناء استخدام الإنترنت.



شكل 2.7: تمثيل الشبكة الافتراضية الخاصة (VPN)

حماية أجهزتك على شبكة الواي فاي اللاسلكية العامة
Protecting your Devices on a Public Wi-Fi Network

يُعدُّ استخدام شبكات **الواي فاي** (WiFi) اللاسلكية العامة أمرًا شائعًا للوصول إلى الخدمات المختلفة عبر الإنترنت، ولكن استخدامها دون الاحتياطات المناسبة قد ينتج عنه مخاطر أمنية متنوعة تُهدِّد أجهزتك وبياناتك. فيما يلي أفضل الممارسات لحماية أجهزتك عند استخدام شبكة الواي فاي اللاسلكية العامة.

- استخدِم بيانات هاتفك المحمول كنقطة **اتصال محمولة** (Mobile Hotspot).
- أوقِف تشغيل الاتصال بشبكات **الواي فاي** (WiFi) اللاسلكية عند عدم رغبتك في الاتصال بها.
- لا تُنفِّذ مهامًا تتطلب نقل معلومات حساسة كالبيانات المالية أو الطبية عبر شبكة الواي فاي العامة.
- لا تَقُمْ بإعادة تعيين كلمات المرور لحساباتك عبر شبكة الواي فاي العامة.
- استخدِم خدمة **الشبكة الافتراضية الخاصة** (VPN).
- تَجنَّب صفحات الويب التي تستخدم بروتوكول HTTP عوضًا عن بروتوكول HTTPS الأكثر أمنًا.
- أوقِف خدمة مشاركة الموارد على أجهزتك.

مراقبة الشبكة والتقاط حِزم البيانات
Network Monitoring and Packet Sniffing

تُوجد أدوات عديدة تُستخدم لمراقبة حركة بيانات الشبكة، ولتَتَبُّع وتحليل الحِزم التي يتم إرسالها عبرها، حيث يتم تنفيذ هذه الإجراءات بواسطة أدوات تسمى **مُحلِّلات حِزم البيانات** (Packet Analyzers)، ويُعدُّ برنامج **وايرشارك** (Wireshark) أحد أكثر أدوات تحليل حِزم البيانات شيوعًا.

وايرشارك (Wireshark) هو مُحلِّل حِزم بيانات مفتوح المَصدر يُستخدم لفحص تفاصيل حركة البيانات على عدة مستويات، بدءًا من مستوى معلومات الاتصال وحتى مستوى معلومات الحزم الفردية، كما يتيح لمسؤول الشبكة الحصول على معلومات تتعلق بالحزم الفردية مثل: وقت الإرسال، والمَصدر، والوجهة، ونوع البروتوكول، وبيانات رأس الحزمة التي يُمكن أن تكون مهمة جدًا لتقييم مشكلات الأمن وتشخيصها. يُمكنك تنزيل البرنامج وتثبيته من الرابط التالي:
https://www.wireshark.org/download.html

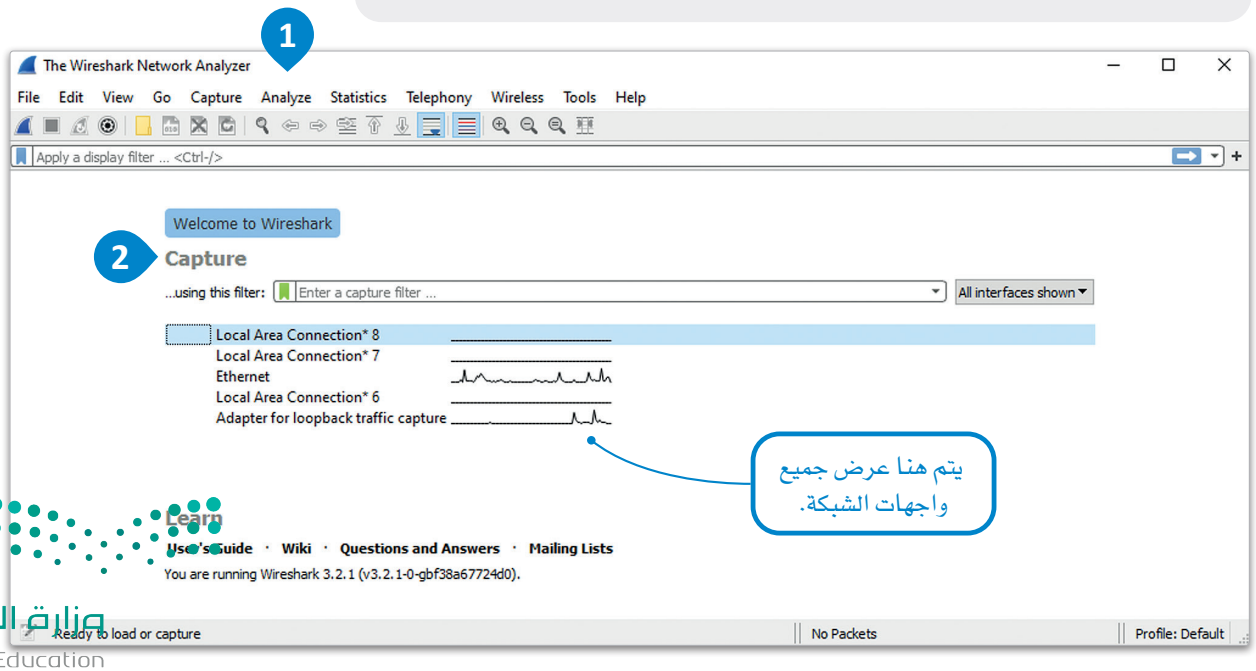
شكل 2.8: رمز الاستجابة السريعة (QR) لتنزيل برنامج وايرشارك

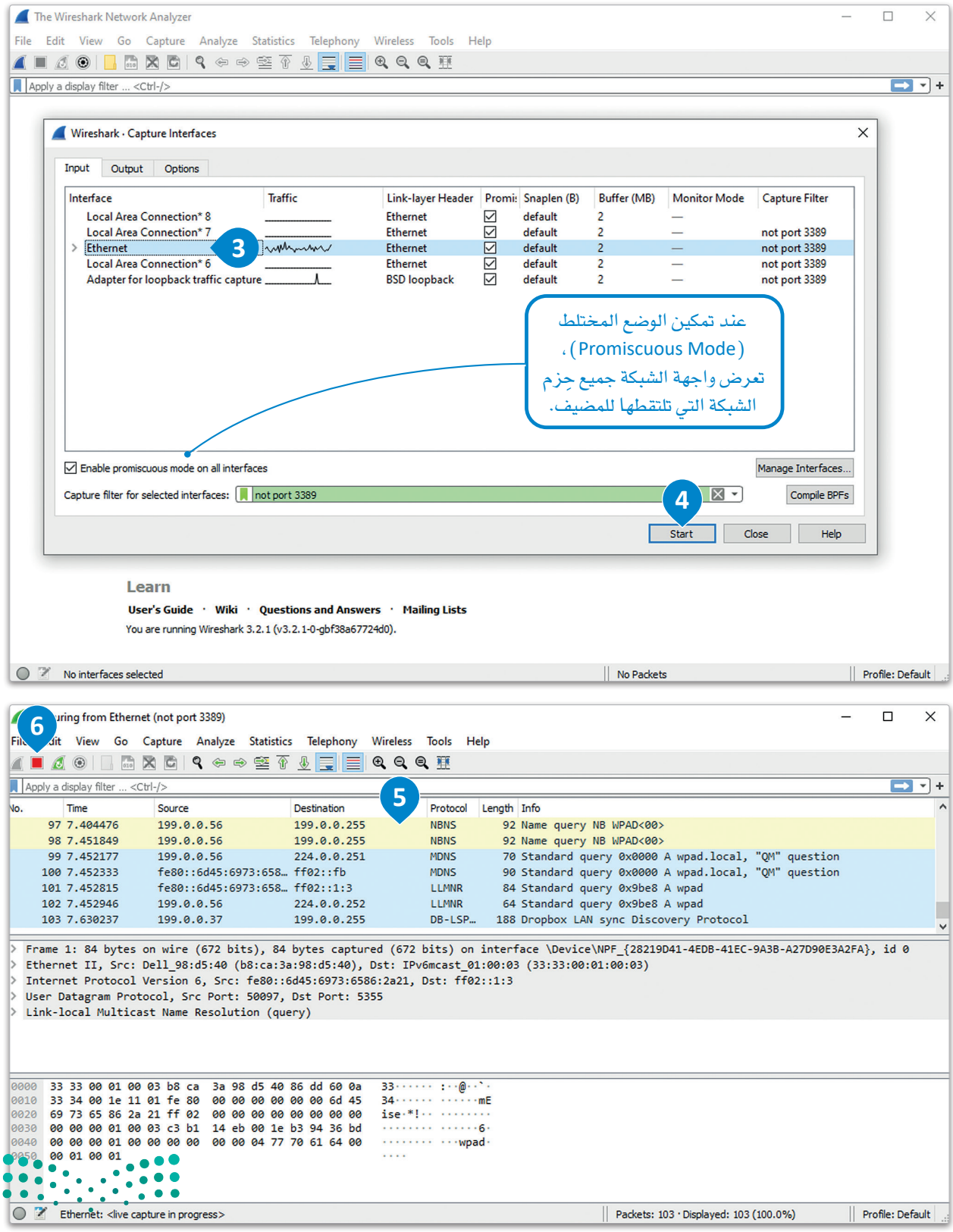
مراقبة الشبكة باستخدام وايرشارك Monitoring a Network with Wireshark

ستتعرف الآن على واجهة مُحلِّل الشبكة **وايرشارك** (Wireshark).

لمراقبة الشبكة باستخدام وايرشارك:

> افتح تطبيق وايرشارك واعرض قائمة Available Networks (الشبكات المتاحة). 1
> اضغط على أمر Capture (الالتقاط). 2
> من نافذة Capture (الالتقاط)، اضغط على الشبكة التي تريد مراقبتها. 3
> اضغط على زرّ Start (بدء). 4
> راقب تدفق حزم البيانات في الشبكة. 5
> اضغط على زرّ Stop (إيقاف) لإنهاء مراقبة الشبكة. 6





شكل 2.9: مراقبة الشبكة باستخدام واير شارك

تحليل مُخرَجات واير شارك Analyzing the Wireshark Output

يعرض مُحلِّل الشبكة واير شارك الكثير من البيانات حول تدفق حِزم البيانات عبر الشبكة مُجمَّعة في ثلاثة لوحات مختلفة وهي: **لوحة قائمة الحِزمة** (Packet List Pane)، و**لوحة تفاصيل الحِزمة** (Packet Details Pane)، و**لوحة بيانات الحِزمة** (Packet Byte Pane).

لوحة قائمة الحِزمة The Packet List Pane

الوقت (**Time**): يشير عمود الوقت إلى وقت استلام الحزمة أو إرسالها، ويُقاس بالثواني منذ بداية الالتقاط.

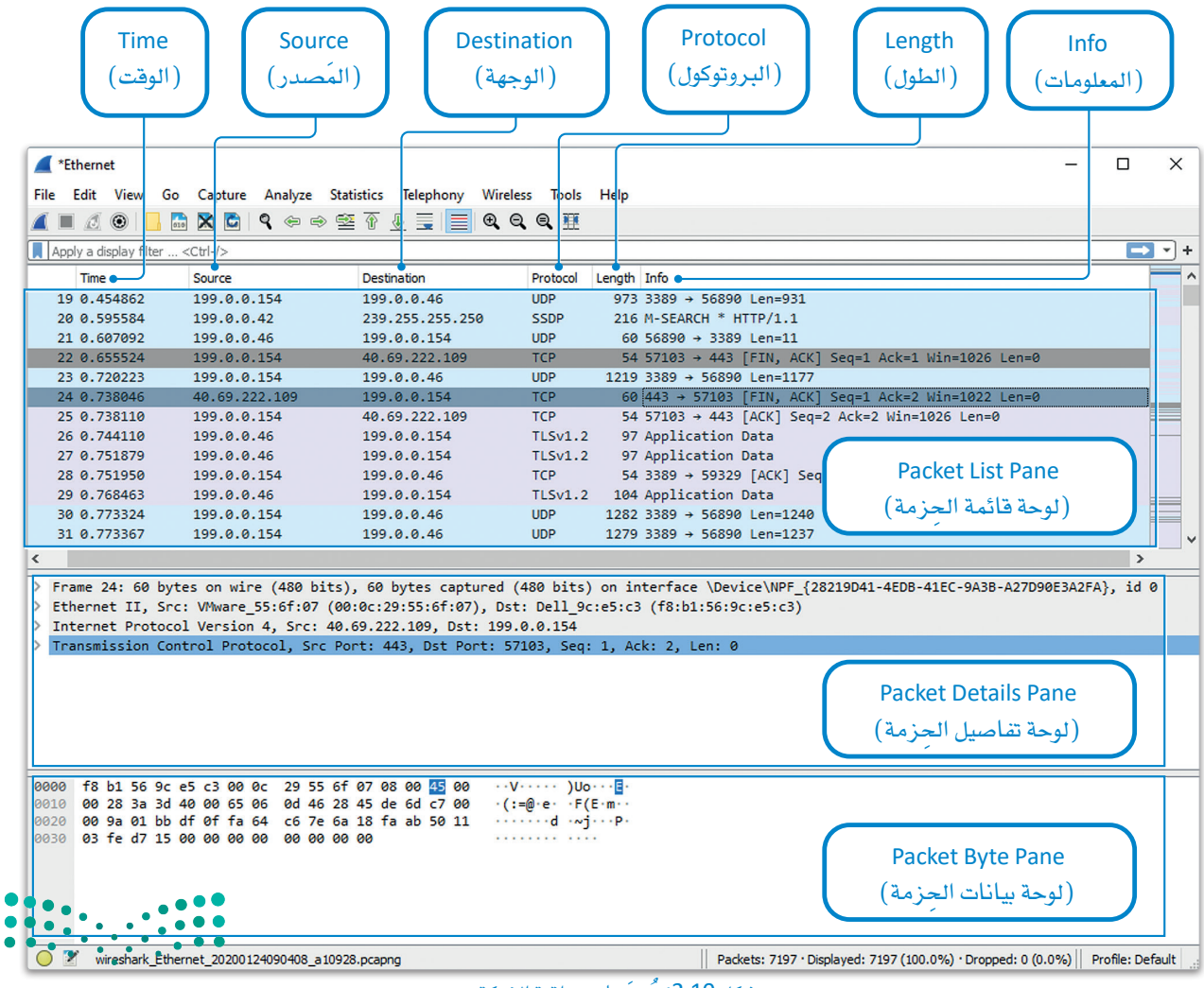
المَصدر (**Source**): يشير عمود المَصدر إلى عنوان IP الخاص بالمَصدر.

الوِجهة (**Destination**): يشير عمود الوِجهة إلى عنوان IP الوِجهة.

البروتوكول (**Protocol**): يشير عمود البروتوكول إلى بروتوكول الاتصال المُستخدَم.

الطول (**Length**): يشير عمود الطول إلى طول الحزمة.

المعلومات (**Info**): يتضمن العمود المختص معلومات إضافية حول الحزمة.



شكل 2.10: مُخرَجات مراقبة الشبكة

لوحة تفاصيل الحِزمة The Packet Details Pane

```
> Frame 24: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{28219D41-4EDB-41EC-9A3B-A27D90E3A2FA}, id 0
> Ethernet II, Src: VMware_55:6f:07 (00:0c:29:55:6f:07), Dst: Dell_9c:e5:c3 (f8:b1:56:9c:e5:c3)
v Internet Protocol Version 4, Src: 40.69.222.109, Dst: 199.0.0.154
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x3a3d (14909)
  > Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 101
    Protocol: TCP (6)
    Header checksum: 0x0d46 [validation disabled]
    [Header checksum status: Unverified]
    Source: 40.69.222.109
    Destination: 199.0.0.154
> Transmission Control Protocol, Src Port: 443, Dst Port: 57103, Seq: 1, Ack: 2, Len: 0
```

شكل 2.11: لوحة تفاصيل الحزمة

تعرض القائمة المنسدلة الأولى بيانات وصفية حول الحِزمة.

تعرض القائمة المنسدلة الثانية معلومات الشبكة التي تم تحليلها.

تعرض القائمة المنسدلة الثالثة معلومات بروتوكول IP المُستخدَم.

```
> Frame 24: 60 bytes on wire
> Ethernet II, Src: VMware_55
v Internet Protocol Version 4
```

لوحة بيانات الحِزمة The Packet Byte Pane

تعرض صندوق لوحة **بيانات الحِزمة** (Packet Byte) بيانات الحِزمة المحدَّدة بالتنسيق **السداسي العشري** (Hexadecimal).

```
0000  f8 b1 56 9c e5 c3 00 0c  29 55 6f 07 08 00 45 00   ··V·····)Uo···E·
0010  00 28 3a 3d 40 00 65 06  0d 46 28 45 de 6d c7 00   ·(:=@·e· ·F(E·m··
0020  00 9a 01 bb df 0f fa 64  c6 7e 6a 18 fa ab 50 11   ·······d ·~j···P·
0030  03 fe d7 15 00 00 00 00  00 00 00 00               ···· ···· ····

wireshark_Ethernet_20200124090408_a10928.pcapng | Packets: 7197 · Displayed: 7197 (100.0%) · Dropped: 0 (0.0%) | Profile: Default
```

شكل 2.12: لوحة بيانات الحِزمة

معلومة

يعرض واير شارك (Wireshark) لوحة بيانات الحِزمة بالتنسيق السداسي العشري؛ لأنه يُوفِّر تمثيلًا أكثر وصفًا وقابلية للقراءة للبيانات المنقولة على الشبكة، حيث يتم في هذا النظام تمثيل كل بايت من البيانات بخانتين من مجموعتي الأرقام والحروف (0-9 وA-F)، مما يُوفِّر طريقة مُختصرة لعرض وتحليل محتويات الحِزم. يشيع استخدام التنسيق السداسي العشري في بروتوكولات ومعايير الشبكات، مما يسمح بمقارنة البيانات وتحليلها بسهولة عبر الأنظمة والمنصات الأساسية المختلفة.

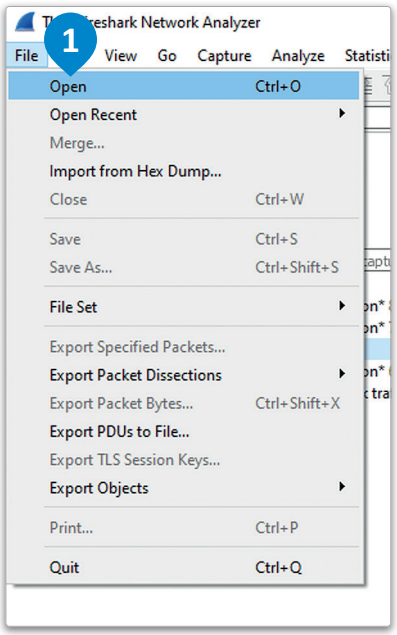
تحليل فحص وايرشارك Analyzing a Wireshark Scan

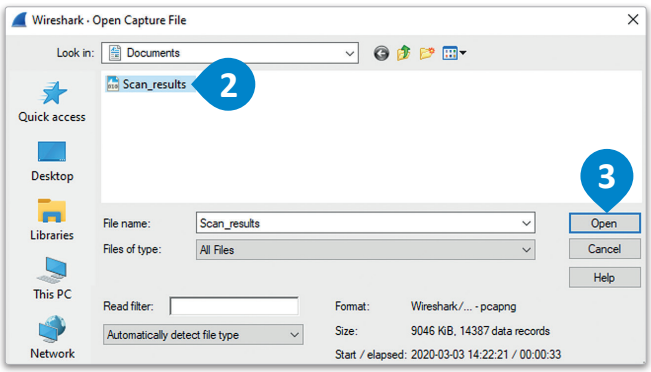
يُمكن استخدام وايرشارك لتحليل تَدفُّق بيانات الشبكة من عمليات فحص تم إجراؤها سابقًا ثم حفظها، حيث ستستخدم ملف فحص محفوظ للعثور على نشاط مشبوه على الشبكة، ويُمكنك تنزيل هذا الملف من الرابط التالي:

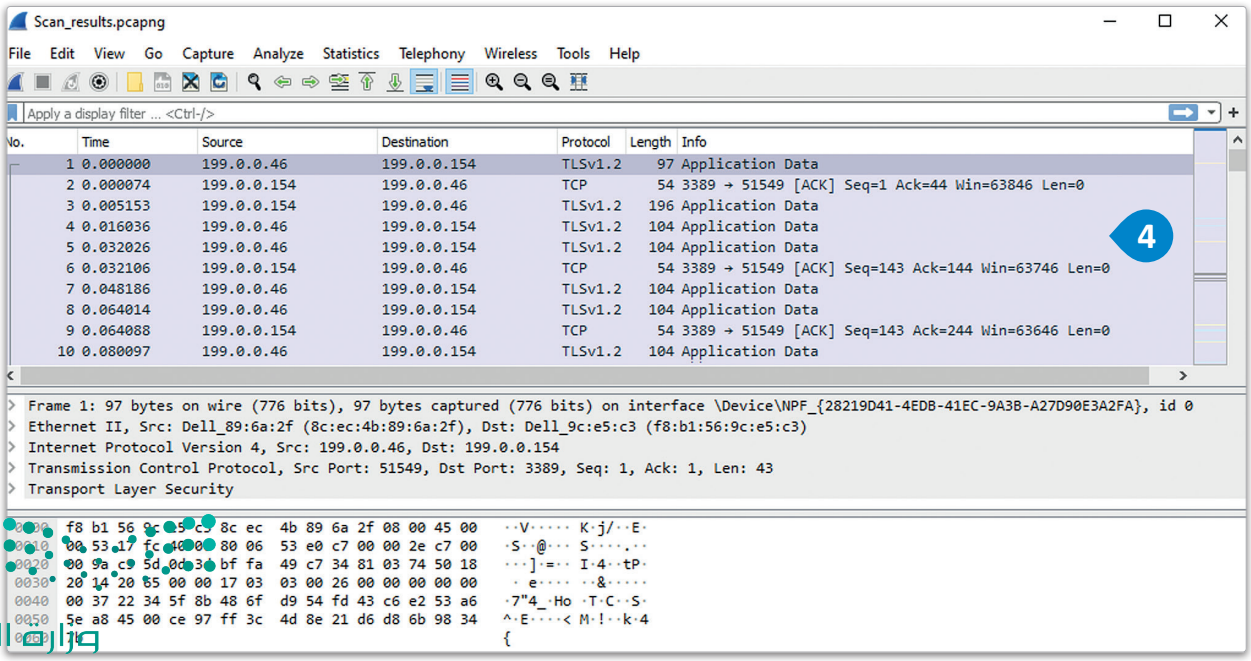
https://bl-xtrransfer.s3.amazonaws.com/KSA/G12/CYB/U2/L2/Scan_results.pcapng

لفتح ملف وايرشارك:

- من علامة تبويب File (ملف)، اضغط على خيار Open (فتح). 1
- من نافذة Open Capture File (فتح ملف الالتقاط)، اختر ملف Scan_results.pcapng (فحص النتائج). 2
- اضغط على Open (فتح). 3
- سيقوم ملف الفحص بإخراج كافة حركة البيانات المُسجلة للشبكة. 4

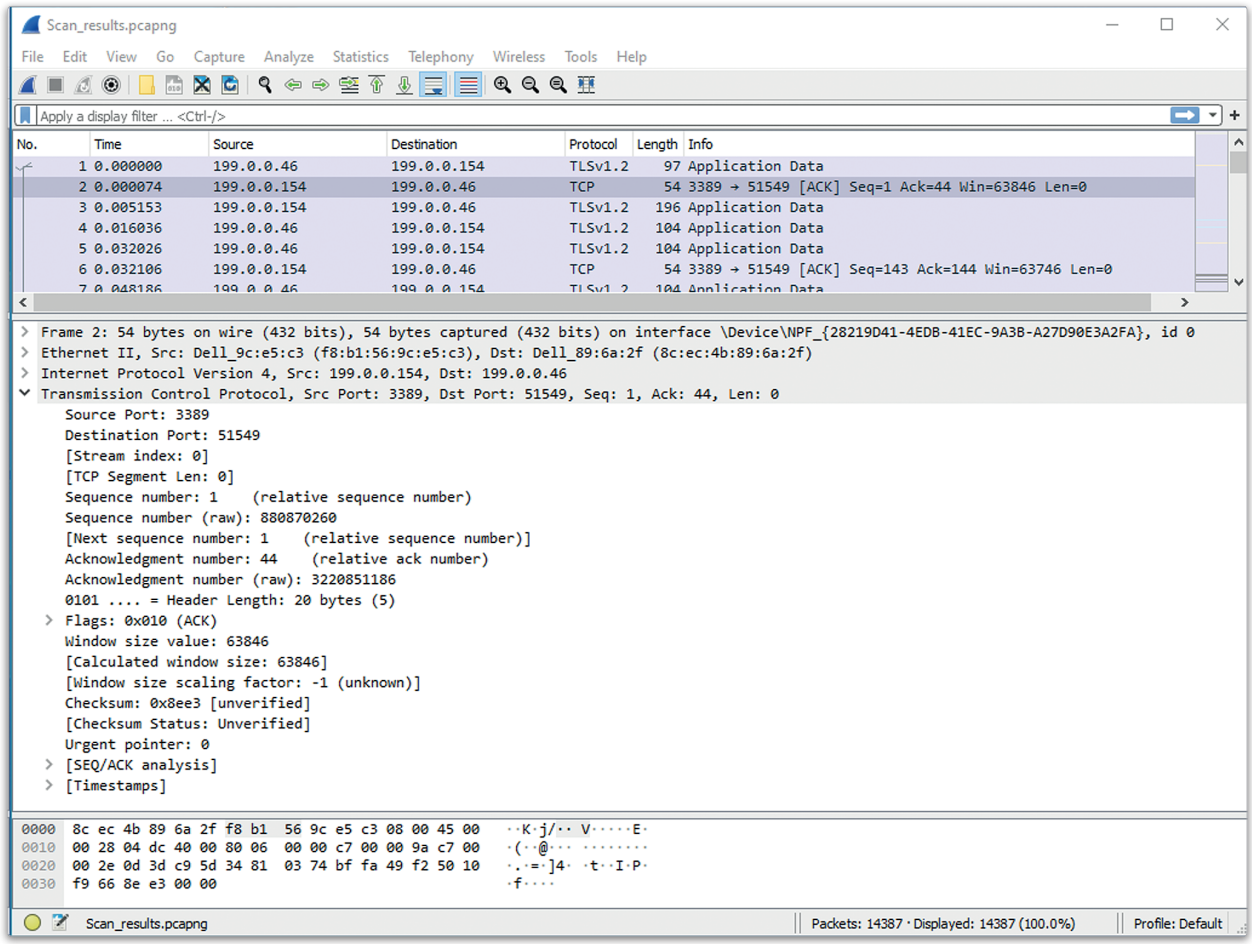






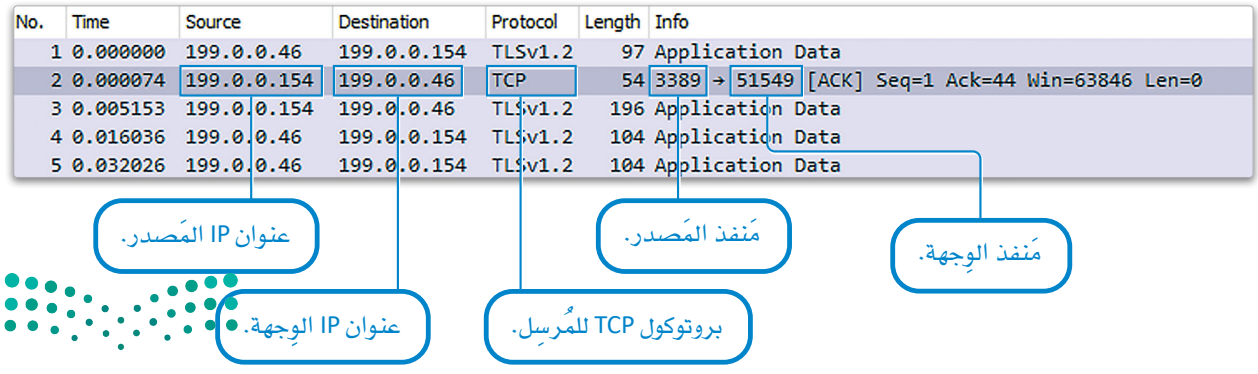
شكل 2.13: فتح ملف وايرشارك

تَمَعَّن في لوحة قائمة الحِزمة التي تعرض نتائج الفحص، وسيُمكنك ملاحظة أن ملف الفحص يحتوي على حِزم تصف مراسلات بين أجهزة المُستخدِمين (العملاء) والخوادم المركزية.

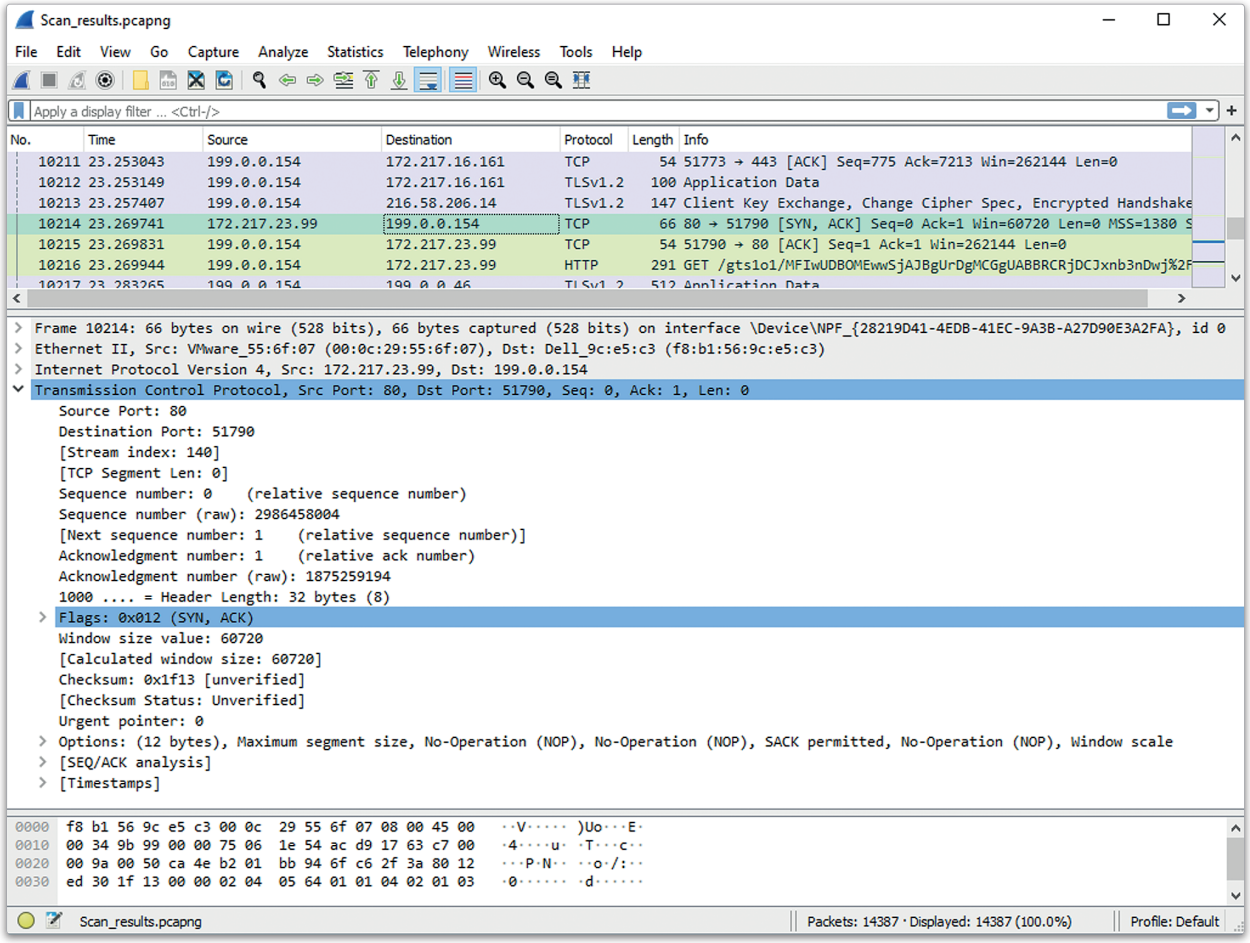


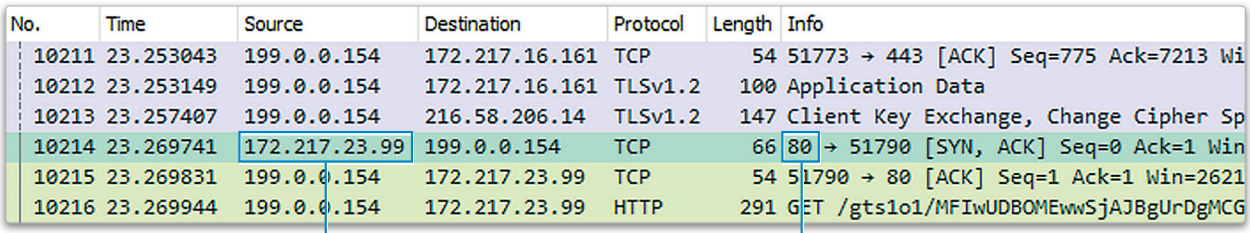
شكل 2.14: المُخرَجات التفصيلية للوحة تفاصيل الحِزمة

في الحِزمة رقم 2، يكون عنوان **بروتوكول الإنترنت للمَصدر** (Source IP) 199.0.0.154، وعنوان **بروتوكول الإنترنت للوجهة** (Destination IP) 199.0.0.46، ويُرسِل جهاز المُستقبِل حزمة باستخدام **بروتوكول التحكم بالنقل** (TCP) الخَاص بالمُرسِل عبر المَنفذ 3389 كمَنفذ المَصدر (مَنفذ المُرسِل)، والمَنفذ 51549 كمَنفذ الوِجهة (مَنفذ المُتلقِّي).



في مثال آخر للحزمة رقم 10214، يُمكنك ملاحظة أن عنوان **بروتوكول الإنترنت للمَصدر** (Source IP) هو 172.217.23.99، وعنوان **بروتوكول الإنترنت للوجهة** (Destination IP) هو 199.0.0.154، وتُوضِّح معلومات الحزمة أيضًا أن بروتوكول الإرسال المُستخدَم هو **بروتوكول التحكم بالنقل** (TCP) ورقم المَنفذ هو 80، مما يُشير إلى استخدام **بروتوكول نقل النص التشعبي** (HTTP)، وهذا يعني أن المُستخدِم يزور صفحة ويب بعنوان بروتوكول إنترنت 172.217.23.99 من صفحة محرك بحث **قوقل** (Google)، مما يعني تَلقي حِزمة بيانات من قوقل.





شكل 2.15: تحليل عناوين بروتوكول الإنترنت (IP)

صفحة محرك بحث قوقل (Google).

يتم استخدام بروتوكول نقل النص التشعبي (HTTP).

كشف نشاط مريب على الشبكة Detecting Suspicious Activity on a Network

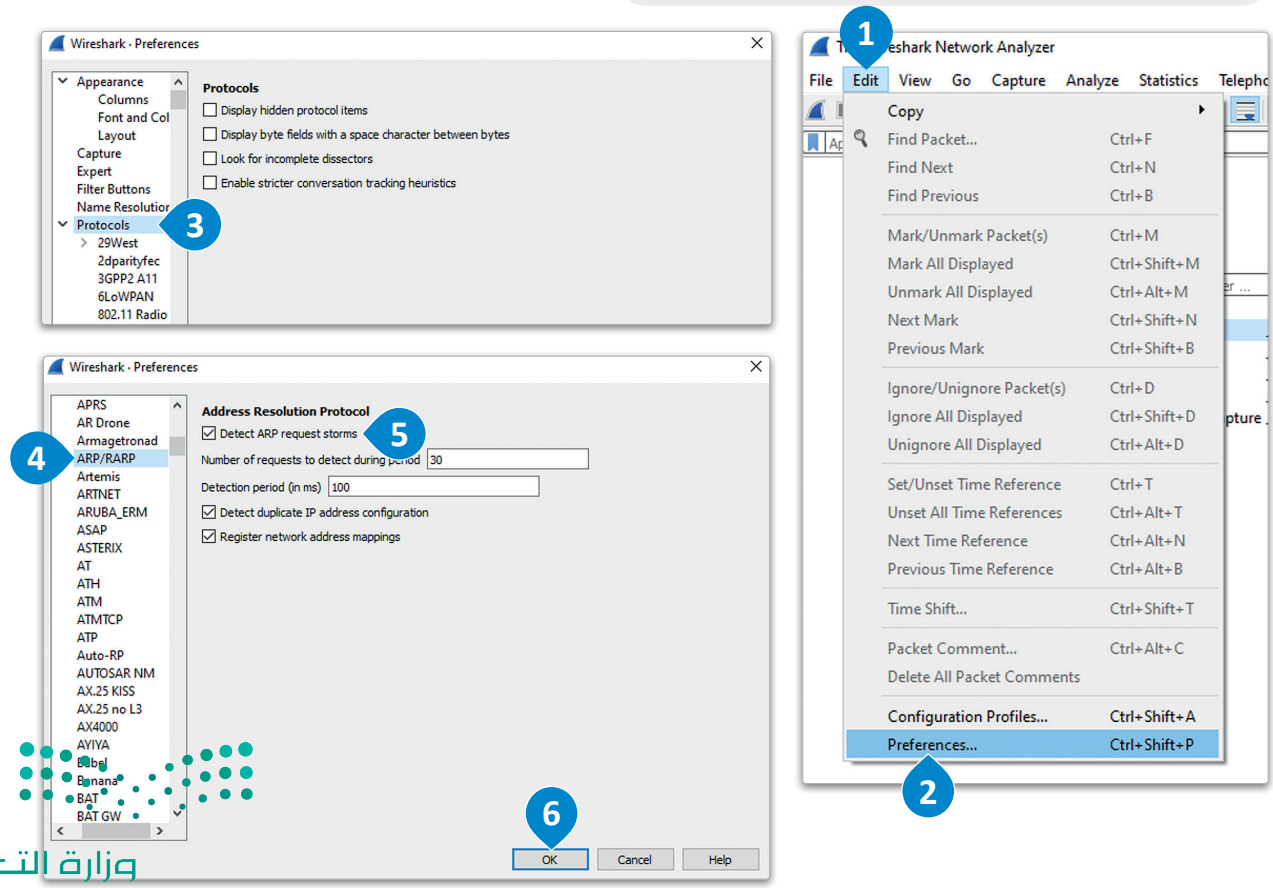
يُستخدم واير شارك للكشف عن الأنشطة المريبة على الشبكة، وعليك التحقق من رسائل وحِزم **بروتوكول اقتران العناوين** (Address Resolution Protocol – ARP) التي تستخدِم هذا البروتوكول لاكتشاف الأجهزة التي تحاول إجراء عمليات مريبة.

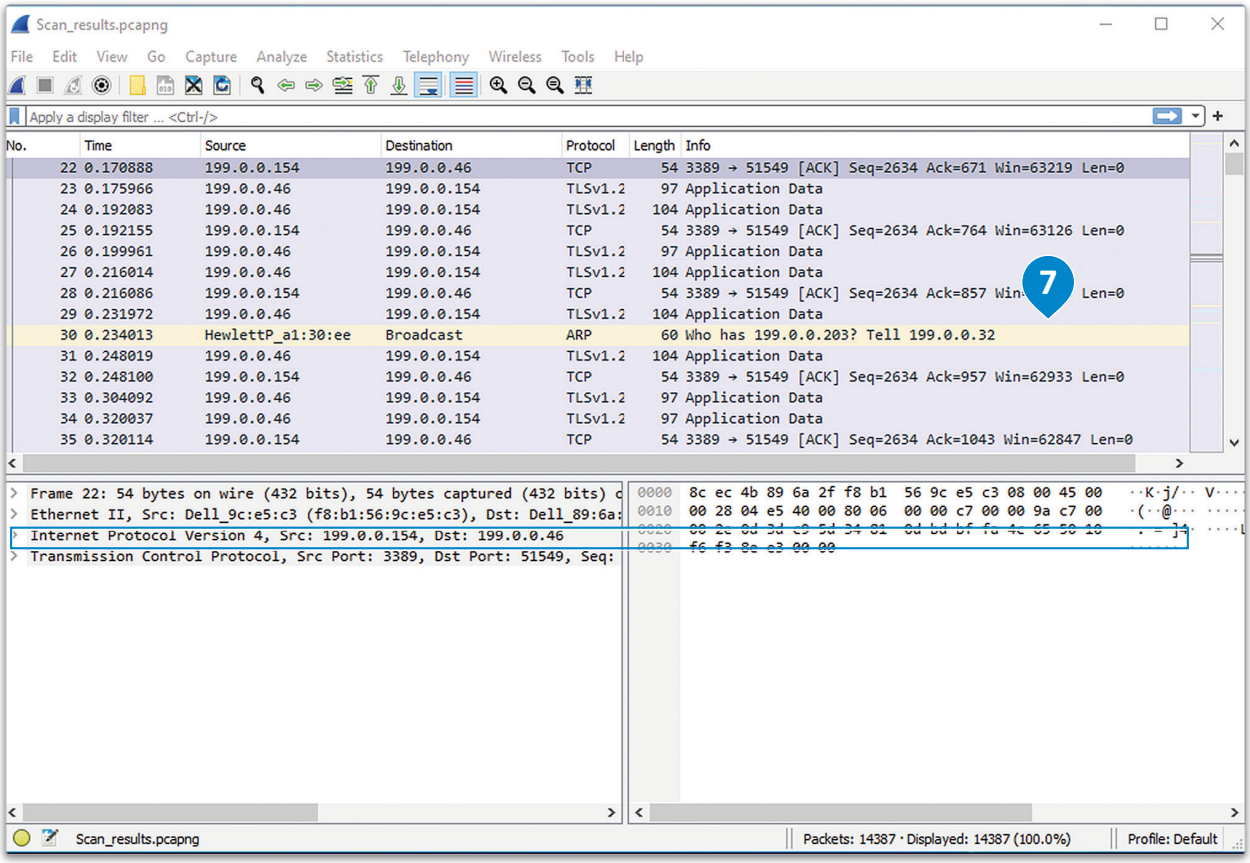
لكشف طلبات بروتوكول اقتران العناوين (ARP):

- من علامة تبويب Edit (تحرير)، 1 اضغط على Preferences (التفضيلات). 2
- من نافذة Preferences (التفضيلات)، اختر خيار Protocols (البروتوكولات). 3
- اختر بروتوكول ARP/RARP (بروتوكول اقتران العناوين/ بروتوكول اقتران العناوين العكسي). 4
- حدِّد صندوق Detect ARP request storms (اكتشاف طلبات بروتوكول اقتران العناوين). 5
- اضغط على OK (موافق). 6
- يُمكنك من لوحة Packet List (قائمة الحِزمة) التَحقُّق من وجود نشاط مريب. 7

بروتوكول اقتران العناوين (Address Resolution Protocol - ARP):

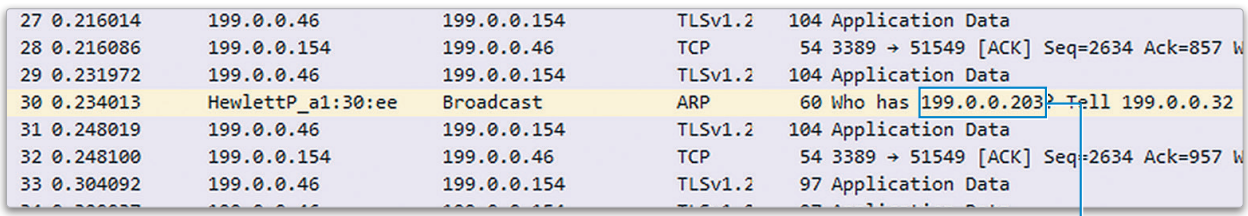
هو بروتوكول اتصال يُستخدم للربط بين عناوين طبقة الشبكة (عناوين IPv4) لجهاز ما وعنوان طبقة ربط البيانات المقابلة (عنوان MAC) على شبكة محلية، ويُعدُّ هذا البروتوكول ضروريًا لتمكين الأجهزة من الاتصال ببعضها في الشبكة المحلية عن طريق تعيين عناوين **بروتوكول الإنترنت** (IP) لعناوين **التحكم بالنفاذ للوسط** (MAC).





شكل 2.16: كشف طلبات بروتوكول اقتران العناوين (ARP)

في لوحة قائمة الحِزمة، تُظهر نتائج الالتقاط أنه تم اكتشاف نشاط مريب في الشبكة، وبشكلٍ أكثر تحديدًا هناك جهاز يُرسِل البيانات دون عرض الوِجهة التي يتم الإرسال إليها، وأنه يتنصت على الأجهزة الأخرى على الشبكة. يقوم هذا الجهاز بالتحقق مما إذا كان عنوان بروتوكول الإنترنت 199.0.0.203 قيد الاستخدام، ويتم إرجاع استجابة إلى عنوان بروتوكول الإنترنت 199.0.0.32، كما يُمكنك أن تستنتج من هذه المعلومات أن شخصًا ما قد يحاول اكتشاف ما إذا كان عنوان بروتوكول الإنترنت 199.0.0.203 قيد الاستخدام كما يظهر لنا في الشكل 2.17، وإذا لم يتم اكتشاف الأمر، فيُمكن للمتسلِّل المحتمل استخدام عنوان بروتوكول الإنترنت هذا للاتصال بالشبكة.



شكل 2.17: مُستخدِم مجهول يحاول اكتشاف ما إذا كان عنوان بروتوكول الإنترنت 199.0.0.203 قيد الاستخدام

تحليل تَدفُّق البيانات بخيار معلومات الخبير

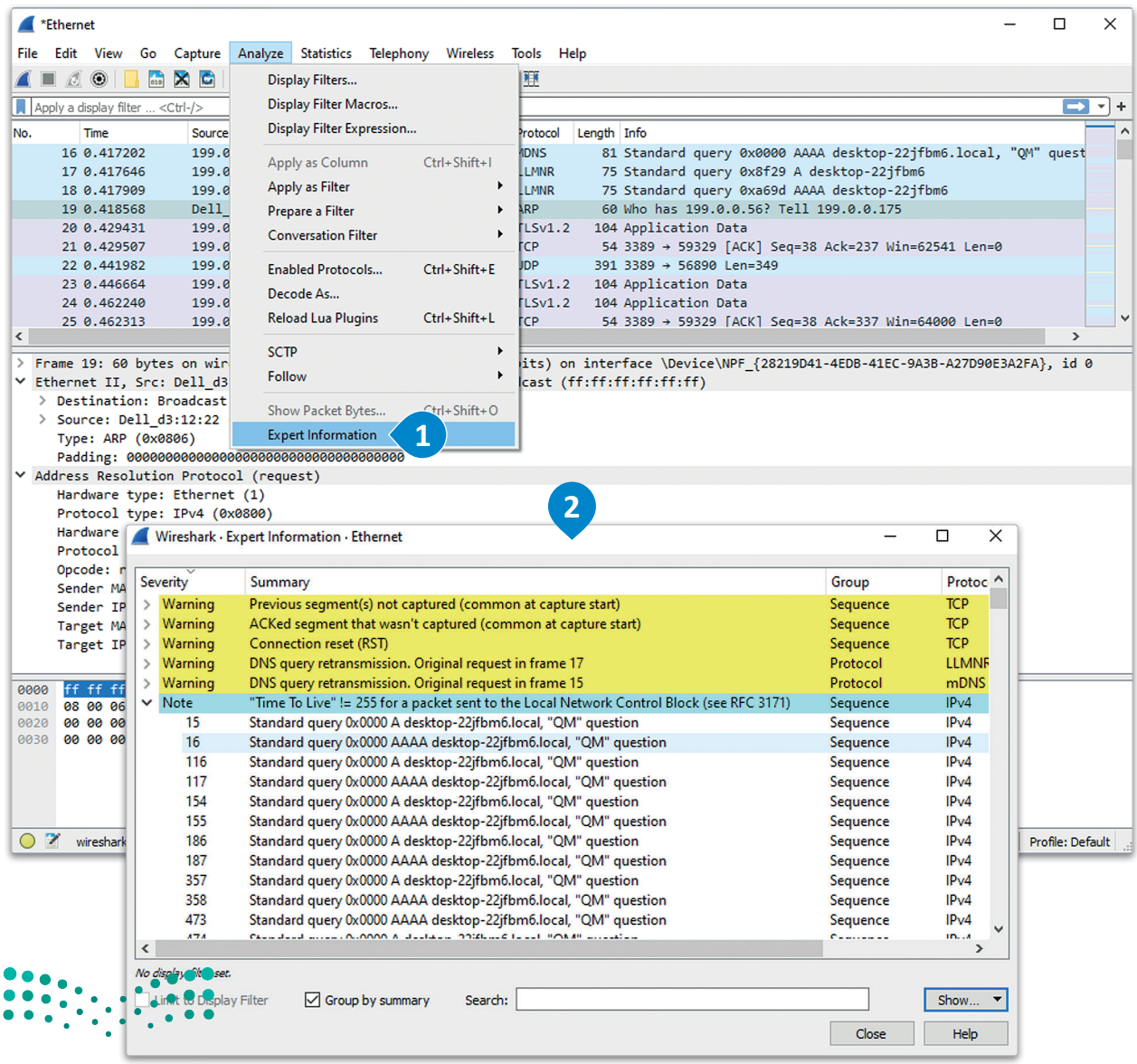
Analyzing Data Flow with Expert Information

يُقدِّم وايـر شـارك خيـار **معلومـات الخبـير** (Expert Information) لتحديـد مشـكلات الشـبكة، وأي سـلوك أو نشـاط مشبوه، بما يساعد غير المتخصِّصين في تحديد هذه الأنشطة.

لتفعيل خيار معلومات الخبير (Expert Information):

> من علامة تبويب Analyze (تحليل)، اضغط على خيار Expert Information (معلومات الخبير). 1

> سيتم التعرف على النشاط المشبوه بواسطة نظام معلومات الخبير. 2

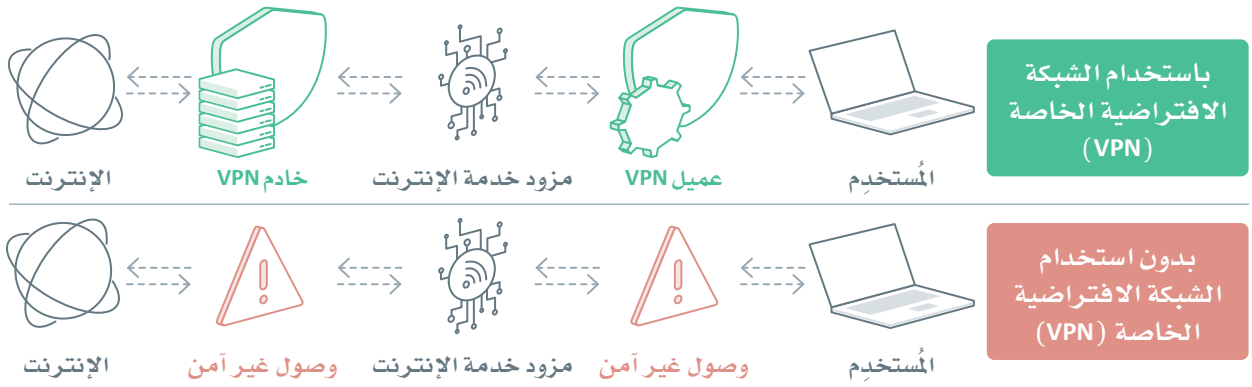


شكل 2.18: تفعيل خيار معلومات الخبير (Expert Information)

الاتصال بخدمة الشبكة الافتراضية الخاصة من نظام تشغيل ويندوز
Connecting to a VPN Service on your Windows Machine الخاص بك

يحتوي نظام تشغيل ويندوز على أداة مُتضمِّنة للاتصال **بالشبكة الافتراضية الخاصة** (VPN)، ويُمكنك استخدامها لحماية جهازك. تُستخدم هذه الطريقة على نطاقٍ واسعٍ لتتيح للمُستخدِمين الوصول الآمن إلى الأجهزة والخوادم عن بُعد، ولقد لجأت الشركات والمؤسسات إلى توفير الوصول الآمن لموظفيها بسبب الحاجة المتزايدة للعمل عن بُعد أو بعيدًا عن مقرات المؤسسات.

يُمكن للموظف الاتصال بشكل آمن بخوادم المؤسسة من خلال خدمة **الشبكة الافتراضية الخاصة** (VPN) دون القلق بشأن اعتراض بيانات تسجيل دخوله أو غيرها من البيانات الحساسة عند الاتصال من المنزل أو من أي مكان خارج مبنى المؤسسة.

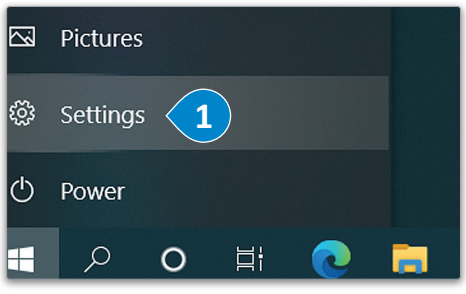


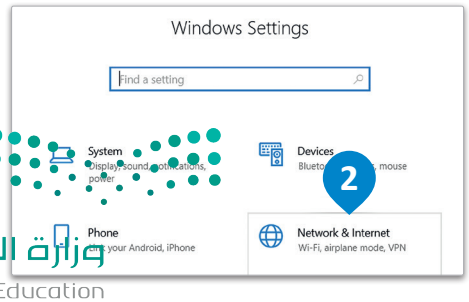
شكل 2.19: خدمة الشبكة الافتراضية الخاصة كطريقة آمنة لاتصال موظف يعمل عن بُعد

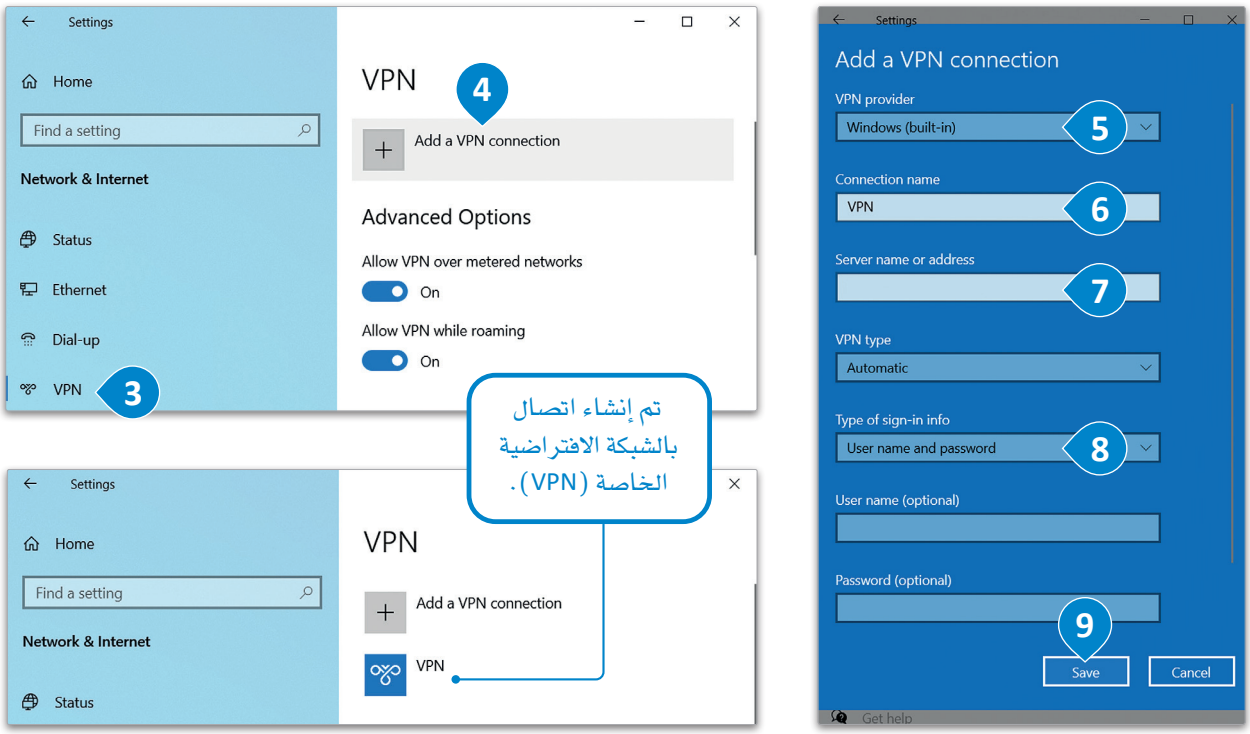
يُمكن للحاسب الذي يعمل بنظام ويندوز الاتصال **بالشبكة الافتراضية الخاصة** (VPN) للعمل أو للاستخدام الشخصي، حيث يوفِّر الاتصال بواسطة **الشبكة الافتراضية الخاصة** (VPN) المزيد من الأمن في الوصول إلى شبكة شركتك والإنترنت في الأماكن العامة، أو للشبكات غير الآمنة مثل المطاعم والمطارات. افترض وجود خدمة **الشبكة الافتراضية الخاصة** (VPN) مُثبتة سابقًا على حاسبك باسم my-vpn-server وتريد الاتصال بها.

للاتصال بخدمة الشبكة الافتراضية الخاصة (VPN):

- من قائمة Start (بدء) في ويندوز، اضغط على Settings (الإعدادات). 1
- من نافذة Settings (إعدادات)، اضغط على Network & Internet (الشبكة والإنترنت). 2
- اضغط على علامة تبويب VPN (الشبكة الافتراضية الخاصة). 3
- اضغط على زرّ Add a VPN connection (إضافة اتصال VPN). 4
- من القائمة المنسدلة لخيار VPN provider (موفر VPN)، اختر خيار Windows (built in) (مضمن ويندوز). 5
- اكتب "VPN" في حقل Connection name (اسم الاتصال). 6
- اكتب "my-vpn-server" في حقل Server name or address (اسم الخادم أو عنوانه). 7
- في حقل Type of sign-in info (نوع معلومات تسجيل الدخول)، اختر User name and password (اسم المستخدم وكلمة المرور). 8
- اضغط على Save (حفظ). 9







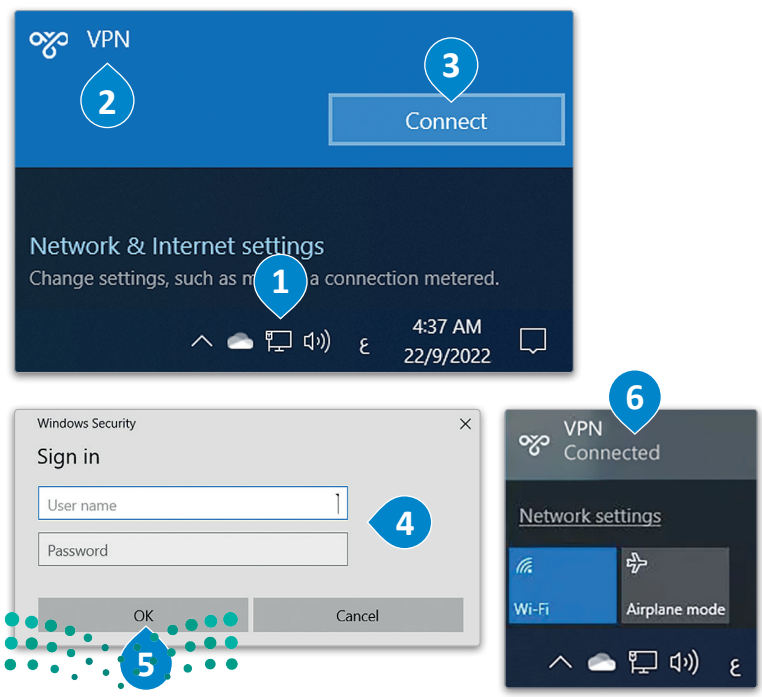
شكل 2.20: الاتصال بخدمة الشبكة الافتراضية الخاصة (VPN)

تفعيل خدمة الشبكة الافتراضية الخاصة Activating the VPN Service

بعد تكوين خدمة الشبكة الافتراضية الخاصة (VPN)، عليك الاتصال بها لتفعيل ميزاتها.

لتفعيل خدمة الشبكة الافتراضية الخاصة (VPN):

- في منطقة إشعارات ويندوز، اضغط على زرّ Network (الشبكة). 1
- اختر اتصال VPN الذي تريد استخدامه وهو في هذه الحالة: VPN. 2
- اضغط على Connect (اتصال). 3
- أدخل User name (اسم المستخدم) و Password (كلمة المرور). 4
- اضغط على OK (موافق). 5
- عند إنشاء الاتصال ستظهر كلمة Connected (متصل) أسفل اسم شبكة VPN. 6



شكل 2.21: تفعيل خدمة الشبكة الافتراضية الخاصة (VPN)

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. تتضمَّن وسائط نقل الشبكة الكابلات المزدوجة والمحورية وكابلات الألياف الضوئية.	○	○
2. المُوجِّهات هي المسؤولة عن توجيه حركة البيانات داخل الشبكة المحلية (LAN).	○	○
3. الهجوم البرمجي العابر للمواقع (XSS) نوعٌ من الهجمات المبنية على مواقع الويب.	○	○
4. بروتوكول الإنترنت الآمن (IPSec) هو بروتوكول شبكة شائع الاستخدام.	○	○
5. تَتوفَّر جُدران الحماية (Firewalls) على شكل برامج أو على شكل عتاد.	○	○
6. تُراقِب أنظمة كشف التسلُّل (IDS) عمليات نقل الملفات.	○	○
7. بروتوكول طبقة المنافذ الآمنة (SSL) هو بروتوكول لتشفير البيانات أثناء نقلها.	○	○
8. يقوم نظام أسماء النطاقات (DNS) بترجمة عناوين بروتوكول الإنترنت (IP) إلى أسماء نطاقات يُمكن قراءتها.	○	○
9. يُستخدم واير شارك (Wireshark) في عمليات التقاط حِزم البيانات.	○	○

2 **اذكر أهم فروقات الأمان بين بروتوكول نقل النص التشعبي (HTTP) وبروتوكول نقل النص التشعبي الآمن (HTTPS).**

3 اشرح كيفية استخدام المناطق العازلة (DMZs) لحماية الشبكات الداخلية من التهديدات الخارجية.

4 قيِّم فعالية الشبكات الافتراضية الخاصة (VPNs) في الحفاظ على خصوصية المُستخدِم.

5 وضِّح كيفية استخدام جُدران الحماية وأنظمة كشف التسلُّل (IDSs) لحماية الشبكات من الهجمات.

6 اشرح الفرق بين نظام كشف التسلُّل المُستند إلى الشبكة (NIDS)، ونظام كشف التسلُّل المُستند إلى المُضيف (HIDS).

7 التقاط وتحليل حركة بيانات الشبكة:

- افتح واير شارك (Wireshark) وحدِّد واجهة الشبكة الخاصة بك، وابدأ بالتقاط الحِزَمْ.
- تصفَّح الإنترنت لبضع دقائق، عن طريق فتح بعض مواقع الويب، ومشاهدة مقطع فيديو، وما إلى ذلك.
- تَوقَّف عن التقاط الحِزم واحفظ البيانات.
- حَلِّل حركة البيانات، واستخرج بعض المعلومات مثل المَصدر IP/Port (بروتوكول الإنترنت / المَنفذ)، والوِجهة IP/Port (بروتوكول الإنترنت / المَنفذ) و Capture time (وقت الالتقاط).

8 تحليل طلب بروتوكول اقتران العناوين (ARP):

- التقط صورة جديدة للشبكة المحلية (Ethernet) الخاصة بك.
- قُم بتصفية نتائج بروتوكول اقتران العناوين (ARP) بكتابة "arp" في شريط filter (التصفية).
- حَلِّل النتائج. كم عدد طلبات بروتوكول اقتران العناوين (ARP) الموجودة؟ وهل يُمكنك تحديد عناوين التحكم بالنفاذ للوسط (MAC) للمَصدر وللوِجهة؟

9 الكشف عن نشاط غير طبيعي في الشبكة بواسطة واير شارك (Wireshark)

- حمِّل ملف Scan_results.pcapng الذي سيمنحه لك معلّمك.
- استخدم علامة تبويب Expert Information (معلومات الخبير) للعثور على أي مشكلات محتملة أو نشاطات غير اعتيادية في الشبكة.
- ابحث عن أي ملاحظات غير طبيعية وحاول تحديد سببها، وهل توجد إشارة على وجود تهديد أمني محتمل؟

رابط الدرس الرقمي

www.ien.edu.sa

الدرس الثالث

التحليل الجنائي الرقمي والاستجابة للحوادث

مُقدِّمة في التحليل الجنائي الرقمي والاستجابة للحوادث

Introduction to Digital Forensics (DF) and Incident Response (IR)

يُعدُّ **التحليل الجنائي الرقمي والاستجابة للحوادث** (DFIR) أحد فروع الأمن السيبراني المهمة المرتكزة على تحديد الهجمات السيبرانية، والتحقيق فيها، واحتوائها، وتجاوزها، وتوفير المعلومات للقضايا القانونية أو التحقيقات الرقمية الأخرى، وتتكوَّن هذه الخدمات من مُكوِّنين رئيسين:

التحليل الجنائي الرقمي (Digital Forensics):
بصفته حقلًا استقصائيًا في علم التحليل الجنائي، يتضمَّن التحليل الجنائي الرقمي عمليات جمع الأدلة الرقمية وتحليلها وتقديمها على أنظمة الحاسب، أو أجهزة الشبكة، أو الهواتف المحمولة، أو الأجهزة اللوحية، ويُمكن أن تساعد هذه الأدلة في الكشف عن حقيقة الأحداث التي حدثت على هذه الأجهزة. يتم اللجوء للتحليل الجنائي الرقمي على نطاقٍ واسع في الإجراءات القانونية، والاستقصاءات التنظيمية، وفي التحقيقات الداخلية للشركات، وفي قضايا النشاط الإجرامي، وكذلك أنواع أخرى من التحقيقات الرقمية.

الاستجابة للحوادث (Incident Response):
تغطي الاستجابة للحوادث أيضًا قضايا التحقيق، ولكنها تُركِّز بشكل خاص على معالجة الحوادث الأمنيّة، وفي هذه الحالات يقوم المُحقِّقون بإجراءات مختلفة، يتعلَّق بعضها بالاحتواء والتعافي للاستجابة بشكل فعَّال للوضع القائم.

يؤدّي كل من التحليل الجنائي الرقمي والاستجابة للحوادث أدوارًا حاسمة في الكشف عن الحقائق المحيطة بالأحداث الرقمية ومعالجة الحوادث الأمنيّة المحتملة لضمان أمن الأنظمة والبيانات الرقمية وسلامتها.

سلسلة الهجوم السيبراني (Cyber Kill Chain):
تُستخدم منهجية سلسلة الهجوم السيبراني لفهم وتحليل الهجمات السيبرانية الضارة، وتُحدِّد المراحل التي تُمكِّن المهاجمين من التحكم بهدفهم وتنفيذ أغراضهم بالنهاية، ويُعدُّ فهم سلسلة الهجوم السيبراني جزءًا أساسيًا من عملية **التحليل الجنائي الرقمي والاستجابة للحوادث** (DFIR)، فمن خلال فهم تلك السلسلة يُمكن للمسؤولين عن حماية الشبكات وأمنها تحديد أنماط الهجوم، والتعرف على التقنيات المعروفة التي يستخدِمها المهاجِمون والاستجابة وفقًا لذلك، وتتكون مراحل سلسلة الهجوم السيبراني من التالي:

المرحلة الأولى: الاستطلاع (Reconnaissance)
يُحدِّد المهاجِمون الأهداف ويستكشفون نقاط الضعف لاستغلالها أثناء الاستطلاع، وقد تتضمن هذه العملية جمع بيانات الاعتماد والوصول، وجمع المعلومات مثل: عناوين البريد الإلكتروني، ومُعرِّفات المُستخدِمين، والمواقع، ومعلومات التطبيقات، والبرامج، ونظام التشغيل. وبالطبع كلما ازداد كَمُّ المعلومات التي يتم جمعها كلما أدى إلى المزيد من الهجمات الناجحة.

المرحلة الثانية: التسليح (Weaponization)
يُنشئ المهاجِم ناقلًا للهجوم أثناء التسليح (على سبيل المثال: البرمجيات الضارة، وبرمجيات الفدية، والفيروسات، والديدان) لاستغلال ثغرة معروفة، وقد يقوم المهاجِم أيضًا بإعداد أبواب خلفية للوصول المستمر في حالة تعذَّرت عملية الدخول بالشكل المخطط له.

المرحلة الثالثة: التسليم (Delivery)

قد يُرسِل المهاجِمون مرفقات أو روابط ضارة إلى المُستخدِمين لمحاولة فتح ثغرة في مرحلة التسليم، وقد يستخدمون تقنيات الهندسة الاجتماعية لزيادة فعالية هجومهم.

المرحلة الرابعة: الاستغلال (Exploitation)

يتم تشغيل التعليمات البرمجية الضارة على نظام الفرد المستهدَف أثناء مرحلة الاستغلال.

المرحلة الخامسة: التثبيت (Installation)

بعد مرحلة الاستغلال مباشرة يتم تثبيت ناقل الهجوم على نظام الضحية، مما يسمح للجهة المهاجِمة بالتحكم في النظام أو الشبكة.

المرحلة السادسة: القيادة والتحكم (Command and Control)

يستطيع فيها المهاجِم التحكم عن بُعد بجهاز أو هوية داخل الشبكة ويتحرك ليتوسع داخل النظام أو الشبكة ويزيد مدى الوصول وينشئ نقاط دخول جديدة.

المرحلة السابعة: تحقيق الأهداف (Actions on Objective)

يمضي المهاجِم خلال هذه المرحلة في تحقيق أهدافه المرجوة التي قد تشمل سرقة البيانات أو إتلافها، أو تشفير المعلومات أو استخراج البيانات.

عمليات التحليل الجنائي الرقمي والاستجابة للحوادث DFIR Processes

فِرَق الاستجابة لحوادث أمن الحاسب (Computer Security Incident Response Teams - CSIRTs):
هي مجموعات متخصصة من المهنيين التقنيين الذين يقومون بالتحقيق في حوادث الأمن الرقمي وتحليلها والاستجابة لها، وتؤدّي تلك الفِرَق دورًا مهمًا في حماية شبكات الحاسب وصيانتها واستعادتها بعد تحديد المشكلات الأمنيّة.

يرتبط التحليل الجنائي الرقمي والاستجابة للحوادث ارتباطًا وثيقًا رغم اختلاف وظائفهما، وغالبًا ما يتم دمجهما في الممارسة العملية، حيث يُعدان مكوِّنان أساسيان للأمن السيبراني. يرتكز التحليل الجنائي الرقمي على جمع أدلة الحادث الأمني وتحليلها، أما الاستجابة للحوادث فتتضمَّن التحقيق في حوادث أمن الحاسب والحدّ من تأثيرها أو احتواءها، والتعامل معها، والتعافي منها. يتم استخدام هذه التقنيات معًا بشكل متكرر من قِبَل **فِرَق الاستجابة لحوادث أمن الحاسب** (CSIRTs) في التعامل مع الهجمات السيبرانية والتحقيقات الرقمية المختلفة، وكذلك في القضايا القانونية والمحاكم.

تشمل عمليات **التحليل الجنائي الرقمي والاستجابة للحوادث** (DFIR) ما يلي:

جَمع الأدلة الجنائية (Forensic Collection):
يتضمن ذلك عملية جمع البيانات وفحصها وتحليلها من مصادر مختلفة مثل: الشبكات، والتطبيقات، ومخازن البيانات، والنقاط الطرفية سواء في مراكز البيانات داخل الشركات أو الخدمات السحابية.

سلسلة الحيازة (Chain of Custody):
إجراء يتم به الاستمرار في جمع الأدلة الجنائية من خلال تَتَبُّع رحلة الأدلة من الجمع إلى التحليل، كما يتضمن توثيق تفاعل كل فرد مع الأدلة، وتاريخ الجمع أو النقل ووقته، وسبب النقل.

التحقيق في السبب الجذري (Root Cause Investigation):
يتم في هذه الخطوة تحديد ما إذا كانت المؤسسة هدفًا أساسيًا للخَرق، وتحديد السبب الجذري للحادث، ونطاقه، والجدول الزمني لحدوثه وتأثيره.

الإخطار والإبلاغ (Notification and Reporting):
تقوم المؤسسات بإخطار السلطات المختصة بخصوص الانتهاكات أو التهديدات الأمنيّة اعتمادًا على التزامات الامتثال الخاصة بها.

مراجعة ما بعد الحادث (Post-Incident Review):
قد تتطلب هذه المرحلة من المؤسسة التفاوض مع المهاجِمين، والتواصل مع أصحاب المصلحة والعملاء والصحافة، وتنفيذ تغييرات على الأنظمة والعمليات لمعالجة الثغرات الأمنيّة اعتمادًا على طبيعة الحادث.

عملية التحليل الجنائي الرقمي Digital Forensics Process

تَمُرُّ عملية التحليل الجنائي الرقمي النموذجية بالخطوات التالية:

التعريف (Identification):
يشمل تحديد الأدلة الرقمية المحتملة المتعلقة بالحادثة أو بالتحقيق وتوثيقها، ويتضمَّن ذلك تحديد مصادر البيانات ذات العلاقة مثل: أجهزة الحاسب، أو الأجهزة المحمولة، أو الخوادم، أو سجلات الشبكة وتحديد نطاق التحقيق.

المحافظة (Preservation):
يتم حماية الأدلة الرقمية المُحدَّدة لمنع تغييرها أو تلفها أو ضياعها، ويشمل ذلك إنشاء نُسخ من بيانات التحقيق الجنائي، وعزل الأنظمة المتأثرة عن الشبكات، والحفاظ على كافة البيانات والمعلومات واستخدامها بطريقة مناسبة لضمان سلامة الأدلة.

التحليل (Analysis):
يتم فحص الأدلة التي تم جمعها للكشف عن المعلومات ذات العلاقة وتحديد الأنماط أو الروابط، وقد يتضمن ذلك استخدام أدوات وتقنيات متخصصة في التحليل الجنائي لاستعادة الملفات المحذوفة، أو فك تشفير البيانات المُشفَّرة أو تحليل سجلات النظام. يجب على المحلِّلين أيضًا تفسير النتائج، مع مراعاة سياق التحقيق والتفسيرات البديلة المحتملة، ويتضمَّن التحليل الطرائق التالية:

- **التحليل الجنائي لنظام الملفات:** هو التحقيق في أنظمة ملفات النقطة الطرفية لتحديد مؤشرات الاختراق الأمني أو استغلال الثغرات.
- **التحليل الجنائي للذاكرة:** هو فحص ذاكرة النظام للكشف عن أي مؤشرات لوجود الثغرات التي قد لا تكون موجودة في أنظمة الملفات.
- **التحليل الجنائي للشبكة:** هو تحليل نشاط الشبكة مثل: رسائل البريد الإلكتروني، والرسائل، وسجل التصفح للتعرُّف على الهجوم وفَهم أساليبه وتحديد نطاق الحادث.
- **تحليل السجلات:** مراجعة وتفسير سجلات النشاط لاكتشاف الأحداث غير العادية أو السلوك المشبوه الذي قد يشير إلى وقوع حادث أمني.

التوثيق (Documentation):
يجب توثيق عملية التحليل الجنائي الرقمي بأكملها، بما في ذلك الخطوات المتخذة والأدوات المُستخدَمة والاستنتاجات التي تم التوصل إليها، ويضمن التوثيق التفصيلي إمكانية مراجعة التحليل الجنائي وتكراره ونقضه إذا لزم الأمر حسب التزام المُحقِّق بأفضل الممارسات والمعايير الصناعية.

الإبلاغ (Reporting):
بَعد عملية التحليل الجنائي الرقمي، تُقدِّم الفِرَق الأدلة والنتائج التي تم التوصل إليها، وعادةً ما تُوضِّح هذه الخطوة الأخيرة منهجية التحليل والإجراءات المتبعة أثناء التحقيق، مما يضمن تقديم المعلومات بوضوح ودقة للمزيد من المراجعة أو الإجراءات القانونية المحتملة.

عملية الاستجابة للحوادث Incident Response (IR) Process

تَمُرُّ عملية الاستجابة للحوادث النموذجية بالخطوات التالية:

تحديد النطاق (Scoping):
يكون الهدف في هذه المرحلة تقييم شدة الحادث ونطاقه واتساعه وتحديد جميع **مؤشرات الاختراق** (Indicators of Compromise – IoC)، كما تساعد هذه الخطوة في تحديد نطاق الهجوم وتحديد أولويات إجراءات الاستجابة وفقًا لذلك.

التحقيق(Investigation):
يتضمَّن ذلك استخدام أنظمة متقدمة والمعلومات الاستباقية لاكتشاف التهديدات وجمع الأدلة وتوفير معلومات متعمِّقة حول الحادث، وهي خطوة حاسمة في فهم طبيعة الهجوم وجمع البيانات الأساسية للمزيد من التحليل.

التأمين (Securing):
تبقى المؤسسات بحاجة إلى مراقبة صحة أنظمتها الإلكترونية باستمرار حتى بعد معالجة التهديدات، وغالبًا ما تتضمَّن هذه المرحلة احتواء التهديدات النشطة التي تم تحديدها أثناء التحقيق واستئصالها، وغلق أي ثغرات أمنية محدَّدة لمنع الهجمات المستقبلية.

الدعم والإبلاغ (Support and Reporting):
تختتم مرحلة الدعم والإبلاغ كل حادث أمني بتقديم خطة مفصَّلة للدعم المستمر، وبتقديم التقارير المخصصة، وقد يقوم مزود خدمة **التحليل الجنائي الرقمي والاستجابة للحوادث** (DFIR) بفحص المُنشأة وتقديم نصيحة اختصاصية بشأن الخطوات التالية لتعزيز التدابير الأمنيّة وضمان الاستعداد للحوادث المستقبلية المحتملة.

التَحوُّل (Transformation):
أخيرًا، تتضمَّن مرحلة التَحوُّل من فِرَق **التحليل الجنائي الرقمي والاستجابة للحوادث** (DFIR) تحديد الثغرات في الوضع الأمني للمؤسسة، وتقديم المشورة بشأن تعزيز نقاط ضعف النظام والحدّ منها، كما تهدف هذه المرحلة إلى تحسين الوضع الأمني للمؤسسة وزيادة صمودها ضد التهديدات السيبرانية المستقبلية.

تحديات التحليل الجنائي الرقمي والاستجابة للحوادث
Digital Forensics and Incident Response Challenges

تزداد التحديات التي يواجهها **التحليل الجنائي الرقمي والاستجابة للحوادث** (DFIR) مع تقدُّم أنظمة الحاسب، وتزداد العقبات أمام الخبراء في هذا المجال، ويوضِّح الجدول 2.6 التحديات الرئيسة التي تواجه **التحليل الجنائي الرقمي والاستجابة للحوادث** (DFIR).

جدول 2.6: التحديات الرئيسة للتحليل الجنائي الرقمي والاستجابة للحوادث

التحدي	الوصف
التحليل الجنائي الرقمي	
تعدد مصادر الأدلة	لم تَعُدْ إمكانية إعادة إنشاء الأدلة الرقمية تعتمد على موقع أو خادم أو شبكة واحدة؛ بل أصبحت تنتشر خلال العديد من المواقع المادية والافتراضية، ونتيجة لذلك تتطلب التحاليل الجنائية الرقمية مزيدًا من الخبرة والأدوات والوقت لجمع التهديدات والتحقيق فيها بدقة وكفاءة.
الوتيرة المتسارعة للتقنية	تتطوَّر الأجهزة الرقمية وتطبيقات البرمجيات وأنظمة التشغيل وتتوسع باستمرار، ونظرًا لمعدل التغيير السريع يتعين على خبراء التحليل الجنائي الرقمي أن يكونوا قادرين على إدارة الأدلة الرقمية في مجموعة متنوعة من إصدارات التطبيقات وتنسيقات الملفات.
الاستجابة للحوادث	
تزايد البيانات ونُدْرَة الدعم	تواجه المؤسسات عددًا متزايدًا من التنبيهات الأمنيّة، ومع ذلك، فهي على الأغلب لا تمتلك الخبرة الكافية في مجال الأمن السيبراني اللازمة لمعالجة حجم المعلومات وحجم التهديدات، حيث تعتمد المؤسسات على الخبراء الخارجيين في **التحليل الجنائي الرقمي والاستجابة للحوادث** (DFIR) لسد فجوة المهارات، والحصول على الدعم أثناء التهديدات الحرجة.
تَوسُّع نطاق الهجوم	يجعل تَوسُّع نطاق الهجوم لأنظمة الحوسبة والبرمجيات الحديثة عملية الحصول على ملخص دقيق للشبكة أكثر صعوبة، ويزيد من مخاطر التهيئة الخاطئة وأخطاء المُستخدِمين.

أفضل ممارسات التحليل الجنائي الرقمي والاستجابة للحوادث
Digital Forensics and Incident Response Best Practices

أفضل ممارسات التحليل الجنائي الرقمي (DF):
تعتمد فعالية **التحليل الجنائي الرقمي والاستجابة للحوادث** (DFIR) على الاستجابة السريعة والشاملة، ومن الضروري أن تتمتع فِرَق التحاليل الجنائية الرقمية بالخبرة الواسعة، والأدوات المناسبة، والخطوات الصحيحة لتوفير استجابة عملية وسريعة لأي مشكلة.

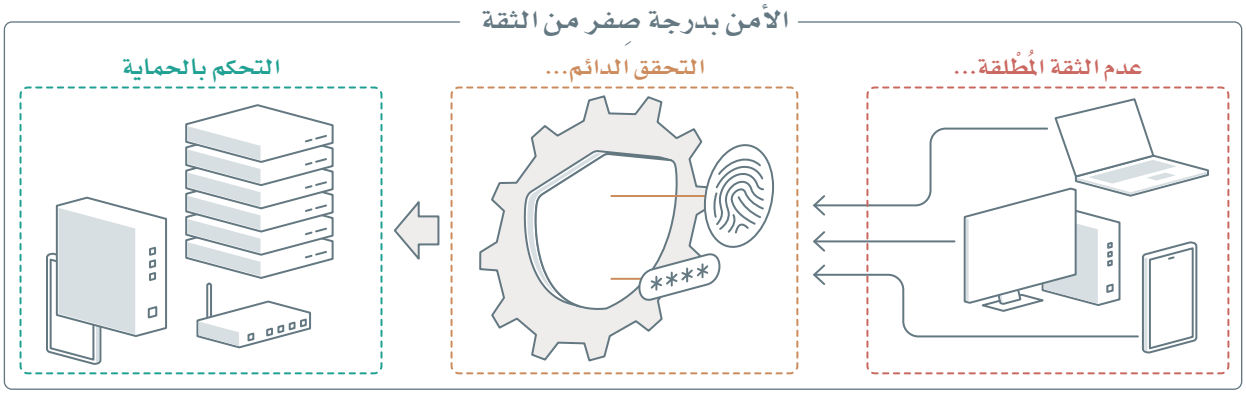
تتمتع الخبرة في التحليل الجنائي الرقمي بعدد من المزايا، بما فيها القدرة على تحديد السبب الجذري للحادث وتحديد نطاقه وتأثيره بدقة، وسيؤدي استخدام أدوات التحقيق المناسبة إلى تحسين تحديد الثغرات الأمنيّة التي أدت إلى الهجوم المستهدَف أو غير ذلك.

أفضل ممارسات الاستجابة للحوادث (IR):
يتم تخصيص خدمات الاستجابة للحوادث الفورية لإدارة الحوادث لتقليل الضرر الذي يلحق بالسُمعة، والخسارة المالية، وتعطيل الأعمال، كما تشمل أفضل الممارسات الخاصة بالاستجابة للحوادث: التحضير، والجاهزية، والتخطيط، بالإضافة إلى الحدِّ من أثر الحوادث، والاستِجابة الدقيقة والسليمة في الوقت المناسب.

تشمل أفضل ممارسات التحليل الجنائي الرقمي والاستجابة للحوادث التعرف على السبب الأساسي للمشكلات، وتحديد جميع الأدلة والبيانات المتاحة ومعرفة موقعها بشكل صحيح، وتقديم الدعم المستمر لضمان تعزيز الدفاع الأمني للمؤسسة في المستقبل.

الأمن بدرجة صِفر من الثقة Zero-Trust Security

تَهدِف **الاستجابة للحوادث** (IR) أيضًا إلى منع الهجمات الضارة للنظام، ولقد طَوَّرت الشركات نماذج أمنية حديثة يُطلق عليها نماذج **الأمن بدرجة صِفر من الثقة** (Zero-Trust Security) لمواجهة المخاطر الأمنيّة المتزايدة. أصبح نموذج الأمن بدرجة صفر شائع التطبيق في الآونة الأخيرة، فعلى العكس من الأساليب التقليدية التي تعتمد على الدفاعات المحيطة لحماية الشبكة الداخلية مثل جُدران الحماية، يَفتَرِضُ هذا النموذج انعدام الثقة بأي جهاز أو مُستخدِم، ويعني هذا بأنه حتى إذا كان بإمكان المُستخدِم الوصول إلى النظام من حساب فعَّال وجهاز داخل الشبكة، فإنه لا يزال يحتاج إلى المصادقة والتصريح، ولا يتم منح المصادقة في هذا النموذج بشكل افتراضي كما هو الحال في الأنظمة القديمة، بل تُمنح عند وجود الحاجة لها. أصبح هذا النموذج أكثر شيوعًا لعدة عوامل أهمها التغيُّرات الكبيرة في التقنية والمجتمع، وطبيعة الأعمال مثل العمل عن بُعد، وبسبب تزايد الهجمات السيبرانية التي تجعل جميع الدفاعات المحيطة بالنظام أقل فعالية.



شكل 2.22: تمثيل الأمن بدرجة صِفر من الثقة

جدول 2.7: المبادئ الرئيسة لتنفيذ نموذج الأمن بدرجة صفر من الثقة

المبدأ	الوصف
التحقق من الهوية	يجب مصادقة جميع المُستخدِمين والأجهزة والتطبيقات وترخيصهم قبل منح الوصول إلى الموارد، وغالبًا ما تُستخدم **المصادقة متعددة العوامل** (MFA) لتوفير طبقة حماية إضافية تتجاوز استخدام أسماء المُستخدِمين وكلمات المرور.
الحد الأدنى من الصلاحيات والامتيازات	يجب منح الوصول إلى الموارد على أساس الحاجة إلى الاستخدام أو المعلومات، وذلك بالحدِّ الأدنى من الوقت المطلوب لإكمال مهمة محدَّدة.
تجزئة الشبكة	يجب تجزئة الشبكة للحدِّ من تحركات المهاجِمين، ويتم تحقيق ذلك غالبًا من خلال التجزئة الدقيقة التي تُقسِّم الشبكة إلى مناطق صغيرة ومعزولة يُمكن تأمينها بشكل فردي.
المراقبة المستمرة	يتطلب الأمن بدرجة صِفر من الثقة مراقبة مستمرة لسلوك المُستخدِم والأجهزة، وحركة بيانات الشبكة، وأحداث الأمن لاكتشاف التهديدات والاستجابة الفورية لها.
حماية البيانات	يجب حماية البيانات باستخدام التشفير والتدابير الأمنيّة الأخرى، وذلك سواء في حالة نقل البيانات أو تخزينها.
تطبيق السياسات الأمنيّة	يجب تحديد السياسات الأمنيّة لضمان امتثال جميع المُستخدِمين والأجهزة والتطبيقات لمتطلبات الأمن.

تحليل أنشطة الويب على الجهاز Analyzing the Web Activity of a Device

تنشأ العديد من الهجمات السيبرانية من خلال اختراق أمني يحدُثُ بسبب نشاط المُستخدِم عبر الويب، وتتم عملية التحليل الجنائي الرقمي بَعد وقوع حدث أمني معيَّن في النظام، كما تتمثل إحدى المهام الرئيسة بالتحقيق في نشاط الويب الخاص بالجهاز المتأثر بالحادث وتحليله.

تقوم متصفحات الويب بتخزين **ملفات السجل** (Log Files) التي تحتوي على بيانات ومعلومات حول الأنشطة التي تم إجراؤها باستخدام المتصفح، ويتم تنظيم هذه الملفات بطريقة يُمكن الوصول إليها وقراءتها بواسطة أدوات تحليل البيانات.

ستحّلل في السيناريو التالي نشاط الويب لجهازك في متصفح ويب **كروم** (Chrome)، حيث ستستخدم **متصفح دي بي إس كيو لايت** (DB Browser for SQLite) وهو أداة نظام إدارة قواعد البيانات، وسيتم استخدام هذه الأداة للوصول إلى ملفات السجل وقراءة بيانات النشاط. يُمكنك تنزيل **متصفح دي بي** (Browser DB) وتثبيته من الرابط التالي:

https://download.sqlitebrowser.org/DB.Browser.for.SQLite-3.12.2-win64.msi

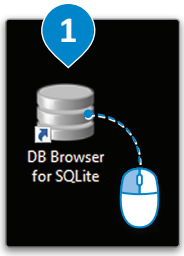
شكل 2.23: رمز الاستجابة السريعة (QR) لتنزيل متصفح دي بي إس كيو لايت

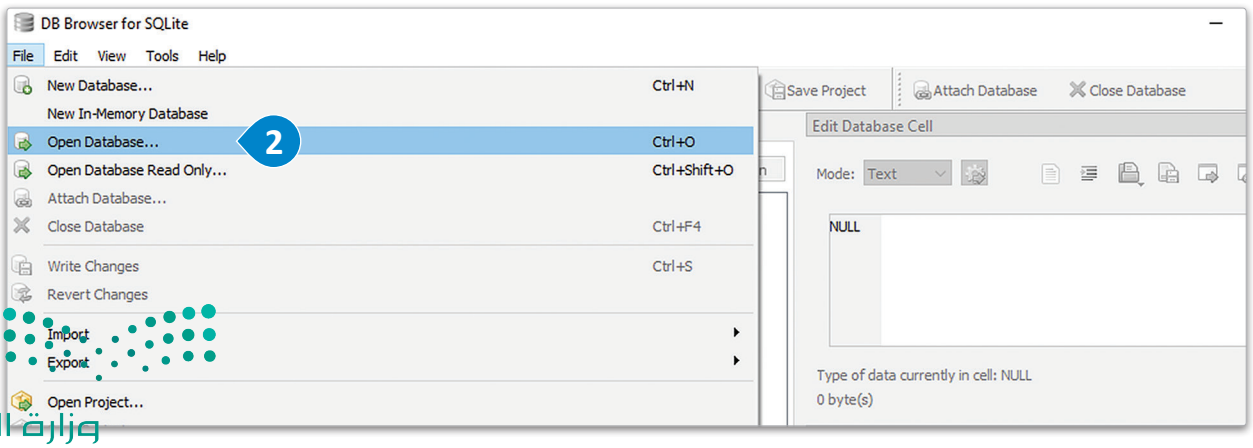
بدء العمل مع متصفح دي بي Getting Started with DB Browser

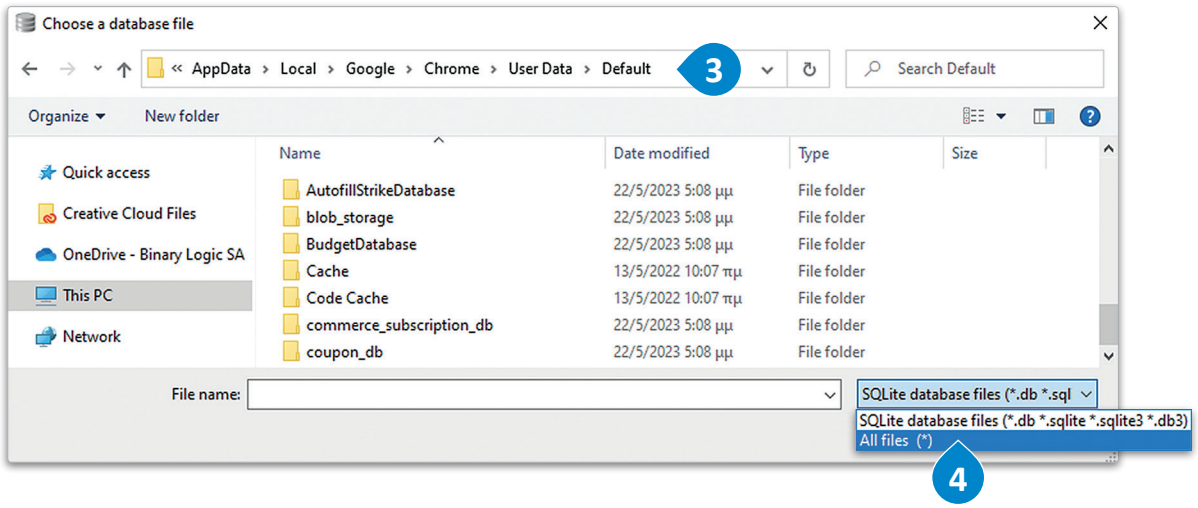
لعرض نشاط متصفحك يتعين عليك في البداية البحث عن ملفات سجل متصفح كروم وفتحها. **ملفات السجل** (Log Files) هي قواعد بيانات تحتوي على جداول متعددة، حيث يحتوي كل جدول على معلومات حول نشاطك مثل: مواقع الويب التي زُرتها والملفات التي قمت بتنزيلها. تأكَّد دائمًا من اتباعك أفضل ممارسات الأمن والحماية لحاسبك عند التصفح على الإنترنت.

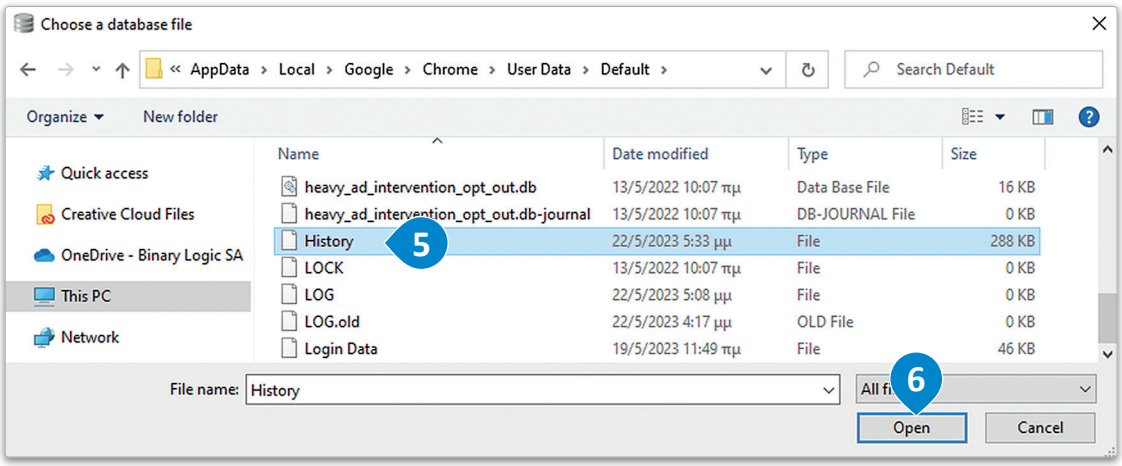
لفتح متصفح دي بي وتحميل ملف السجل:

- اضغط ضغطةً مزدوجةً على اختصار DB Browser (متصفح دي بي) من سطح المكتب. 1
- اضغط على File (ملف) > Open Database... (فتح قاعدة بيانات...). 2
- أدخل: "C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default" في مسار الموقع، وفي حقل [username] (اسم المُستخدِم) أدخل اسم مُستخدِم الحاسب. 3
- اختر All files (*) (كافة الملفات) من القائمة المنسدِلة. 4
- اضغط على History (المحفوظات)، 5 لاختيار ملف سجل المحفوظات،ثم اضغط على Open (فتح). 6

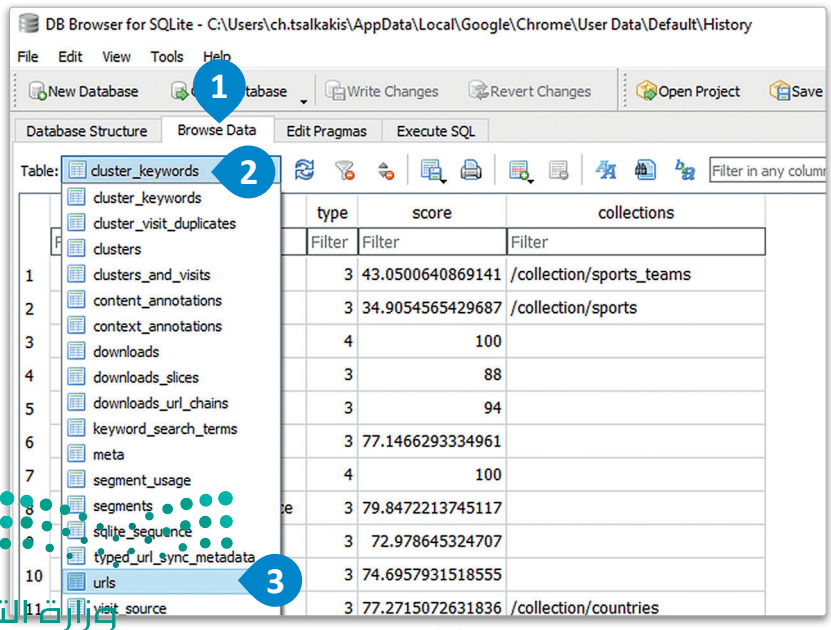








شكل 2.24: فتح متصفح دي بي وتحميل ملف السجل



شكل 2.25: عرض الجدول

لعرض جدول:

- اضغط على علامة تبويب Browse Data (تَصفُّح البيانات). 1
- اضغط على القائمة المنسدلة، 2 ثم اختر urls (مُحدِّدات موقع الموارد المُوحَّد) لعرض جدول عناوين urls. 3

جدول مُحدِّدات موقع الموارد المُوحَّد The Uniform Resource Locators (URLs) Table

يؤدي جدول عناوين **مُحدِّدات موقع الموارد المُوحَّد** (URLs) دورًا مهمًا في التحقيق في أنشطة تصفح المُستخدِم وتحليلها عند إجراء التحليل الجنائي للأمن السيبراني، ويحتوي هذا الجدول الموجود في سجل متصفح كروم على معلومات قيِّمة حول عناوين الويب التي زارها المُستخدِم أثناء جلسات التصفح، حيث يُمكن للمُحقِّقين معرفة مواقع الويب التي تم الوصول إليها بدقة، وتَتَبُّع سلوك المُستخدِم، والكشف عن الأدلة الحاسمة المتعلقة بالجرائم الإلكترونية من خلال فحص البيانات المُخزنة في جدول العناوين.

يتكون جدول عناوين **مُحدِّدات موقع الموارد المُوحَّد** (URLs) من عدة أعمدة رئيسة توفِّر تفاصيل محدَّدة حول كل عنوان URL تمت زيارته. فيما يلي، ستستكشف هذه الأعمدة وتتعرف على أهميتها في مجال التحليل الجنائي للأمن السيبراني:

مُحدِّد موقع الموارد المُوحَّد (url):

يُخزِّن عمود مُحدِّد موقع الموارد المُوحَّد (url) عناوين الويب المحدَّدة لمواقع الويب التي تمت زيارتها، حيث يسمح تحليل هذه العناوين للمُحقِّقين بتحديد صفحات الويب التي تم الوصول إليها، واسترداد المعلومات الهامة المتعلقة بنشاط معيَّن عبر الإنترنت.

العنوان (title):

يحتوي عمود **العنوان** (title) على عناوين أو أسماء صفحات الويب التي تمت زيارتها، وتُقدِّم هذه المعلومات سياقًا إضافيًا وتساعد المُحقِّقين على فهم محتوى المواقع التي تم الوصول إليها والغرض منها، كما يُمكن أن يوفِّر تحليل العناوين معلومات مهمة حول اهتمامات المُستخدِم وعادات التصفح والمجالات التي يجب تركيز التحقيق حولها.

عداد الزيارة (visit_count):

يُسجِّل عمود **عداد الزيارة** (visit_count) عدد المرات التي زار فيها المُستخدِم عنوان URL محدَّد، ويسمح هذا العداد للمُحقِّقين بتحديد وتيرة ومستوى استخدام المُستخدِم لموقع ويب معيَّن، كما يساعد هذا التحليل في تحديد الموارد التي تم الوصول إليها بشكل متكرر، وتحديد أولويات جهود التحقيق، وتحديد أنماط أو اتجاهات سلوك المُستخدِم.

وقت آخر زيارة (last_visit_time):

يُوفِّر عمود **وقت آخر زيارة** (last_visit_time) ختم الوقت أو تاريخ أحدث زيارة لعنوان URL محدَّد ووقتها، وتُمكِّن هذه المعلومات المُحقِّقين من إنشاء جداول زمنية وتَتَبُّع التسلسل الزمني لأنشطة المُستخدِم، وربما ربط زيارات موقع الويب بأحداث أو إجراءات أخرى.

Table: urls

Filter in any column

	id	url	title	visit_count	last_visit_time
	Filter	Filter	Filter	Filter	Filter
1	1	https://www.google.com/search?...	ksa ministry of education - ...	2	13331026045492522
2	2	https://moe.gov.sa/en	Ministry of Education	1	13331026047091166
3	3	https://moe.gov.sa/en/Pages/...	Ministry of Education	1	13331026047091166
4	4	https://nca.gov.sa/en	National Cybersecurity ...	2	13331026071307456
5	5	https://sdaia.gov.sa/en/default.aspx	Saudi Authority for Data and...	1	13331026134530124

قراءة ختم الوقت Reading a Timestamp

ختم الوقت (Timestamp) هو قيمة رقمية تمثِّل نقطة زمنية محدَّدة، ويُستخدم بشكل شائع في قواعد البيانات وأنظمة الحاسب لتسجيل وتَتَبُّع الأحداث أو إنشاء البيانات وتعديلها، وغالبًا ما يتم تخزين أختام الوقت على هيئة رقم يمثِّل الثواني أو الملّي ثانية منذ نقطة مرجعية محدَّدة تُعرف باسم **الحُقبة** (Epoch).

يُمكنك استخدام البرنامج النصي التالي في علامة تبويب تنفيذ SQL (Execute SQL) في **متصفح دي بي** (DB Browser) لعرض تاريخ الإدخال عن طريق استبدال **ختم الوقت** (Timestamp) بالقيمة التي تريد عرضها:

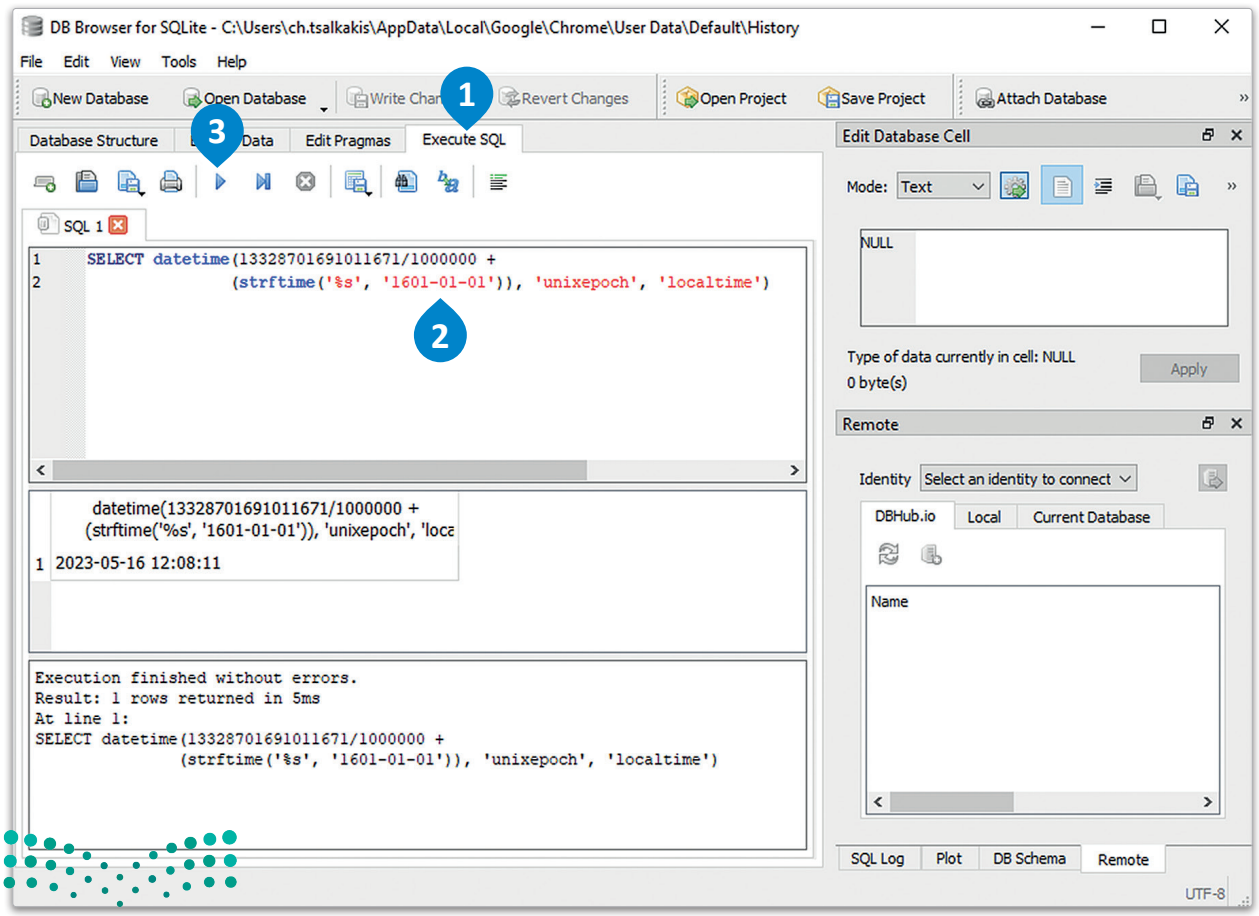
```
SELECT datetime (timestamp/1000000 +
                (strftime('%s', '1601-01-01')), 'unixepoch', 'localtime')
```

لقراءة ختم الوقت (Timestamp):

> اضغط على علامة تبويب Execute SQL (تنفيذ SQL). 1

> أدخل البرنامج النصي مع ختم الوقت الذي ترغب في عرضه في الحقل أدناه. 2

> اضغط على زرّ Run (تشغيل) لتشغيل البرنامج النصي. 3



شكل 2.26: قراءة ختم الوقت (Timestamp)

جدول مصطلحات البحث عن الكلمات الرئيسة The Keyword_search_terms Table

يُعدُّ جدول **مصطلحات البحث عن الكلمات الرئيسة** (keyword_search_terms) مُكوِّنًا مُهمًا في تحقيقات التحليل الجنائي للأمن السيبراني، حيث أنه يحتوي على معلومات مهمة حول مصطلحات البحث، أو الكلمات الرئيسة المُستخدَمة أثناء أنشطة التصفح على الويب، كما يلتقط عمود **المصطلح** (Term) في هذا الجدول استعلامات البحث الفردية التي أدخلها المُستخدِمون. يُوفِّر عمود **المصطلح** (Term) معلومات قيِّمة حول اهتمامات المُستخدِمين واحتياجاتهم المعلوماتية وسلوكهم عبر الإنترنت، ويسمح تحليل مثل هذه المعلومات للمُحقِّقين بفهم الكلمات الرئيسة أو العبارات المحدَّدة المُستخدَمة عند البحث عن المعلومات. يُمكن أن تتراوح مصطلحات البحث هذه من مجرد كلمات رئيسة بسيطة إلى استعلامات أكثر تعقيدًا، مما يُوفِّر أدلة قيِّمة حول نوايا المُستخدِمين ونوع المعلومات التي كانوا يبحثون عنها.

جدول التنزيلات Downloads Table

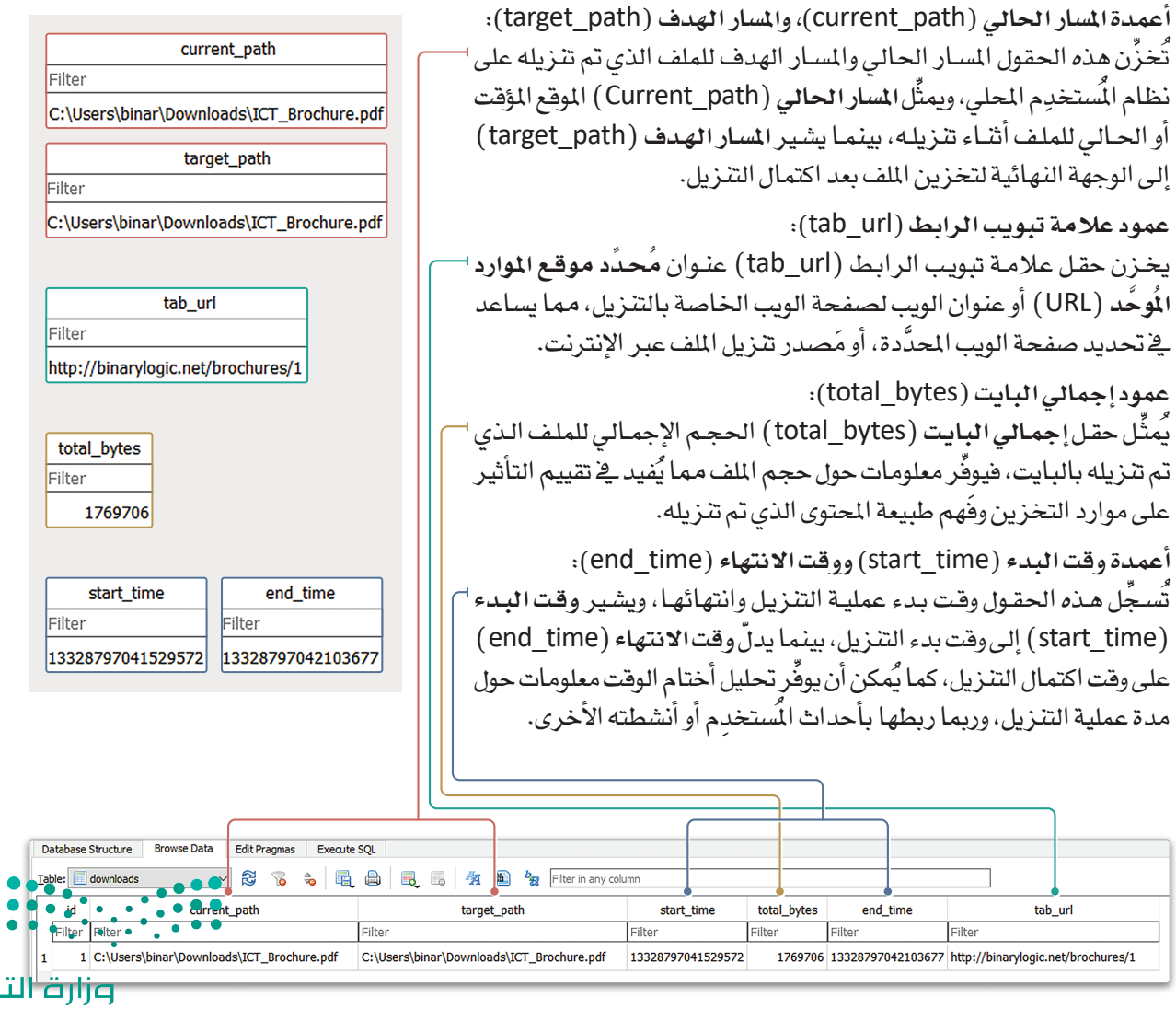
هناك جدول آخر يحتوي على معلومات مهمة في التحليل الجنائي باسم جدول **التنزيلات** (Downloads)، ويحتوي هذا الجدول على معلومات حول الملفات التي تم تنزيلها، وحول البيانات الوصفية المرتبطة بها، وكذلك يؤدّي دورًا مُهمًا في إدارة المحتوى الذي تم تنزيله وتَتَبُّعه، كما يتضمن الجدول عدة حقول مهمة توفر معلومات حول الملفات التي تم تنزيلها والتفاصيل المتعلقة بها:

أعمدة المسار الحالي (current_path)، **والمسار الهدف** (target_path):
تُخزِّن هذه الحقول المسار الحالي والمسار الهدف للملف الذي تم تنزيله على نظام المُستخدِم المحلي، ويمثِّل **المسار الحالي** (Current_path) الموقع المؤقت أو الحالي للملف أثناء تنزيله، بينما يشير **المسار الهدف** (target_path) إلى الوجهة النهائية لتخزين الملف بعد اكتمال التنزيل.

عمود علامة تبويب الرابط (tab_url):
يخزن حقل علامة تبويب الرابط (tab_url) عنوان **مُحدِّد موقع الموارد المُوحَّد** (URL) أو عنوان الويب لصفحة الويب الخاصة بالتنزيل، مما يساعد في تحديد صفحة الويب المحدَّدة، أو مَصدر تنزيل الملف عبر الإنترنت.

عمود إجمالي البايت (total_bytes):
يُمثِّل حقل **إجمالي البايت** (total_bytes) الحجم الإجمالي للملف الذي تم تنزيله بالبايت، فيوفِّر معلومات حول حجم الملف مما يُفيد في تقييم التأثير على موارد التخزين وفَهم طبيعة المحتوى الذي تم تنزيله.

أعمدة وقت البدء (start_time) **ووقت الانتهاء** (end_time):
تُسجِّل هذه الحقول وقت بدء عملية التنزيل وانتهائها، ويشير **وقت البدء** (start_time) إلى وقت بدء التنزيل، بينما يدلّ **وقت الانتهاء** (end_time) على وقت اكتمال التنزيل، كما يُمكن أن يوفِّر تحليل أختام الوقت معلومات حول مدة عملية التنزيل، وربما ربطها بأحداث المُستخدِم أو أنشطته الأخرى.



جدول تسجيلات الدخول Logins Table

يُمكنك في ملف سجل بيانات **تسجيل الدخول** (Login) العثور على جدول تسجيلات الدخول الذي يحتوي على معلومات متعلقة بعمليات تسجيل دخول المُستخدِم وبيانات الاعتماد المخزنة، وتوجد هذه البيانات بشكل شائع في قواعد بيانات متصفحات الويب وتؤدّي دورًا مهمًا في إدارة تفاصيل تسجيل الدخول وتعبئتها تلقائيًا، كما يتضمَّن جدول تسجيلات الدخول العديد من الحقول المهمة التي توفر رُؤى حول بيانات اعتماد المُستخدِم والبيانات الوصفية المرتبطة بها:

عمود عنوان URL الأصل (origin_url):

يُخزِّن حقل **عنوان URL الأصل** (origin_url) عنوان **مُحدِّد موقع الموارد المُوحَّد** (URL) أو عنوان موقع الويب حيث تم استخدام بيانات اعتماد تسجيل الدخول أو حفظها، ويساعد هذا في تحديد موقع الويب أو الخدمة عبر الإنترنت المرتبطين بمعلومات تسجيل الدخول المخزَّنة.

أعمدة عنصر اسم المُستخدم (username_element) **وقيمة اسم المُستخدم** (username_value):

تلتقط هذه الحقول اسم عنصر **لغة ترميز النص التشعبي** (HTML) والقيمة المقابلة لاسم المُستخدِم أو مُعرِّفه أثناء تسجيله الدخول، وتوفِّر معلومات حول قيم حقول اسم المُستخدِم في نموذج الويب.

أعمدة عنصر كلمة المرور (password_element) **وقيمة كلمة المرور** (password_value):

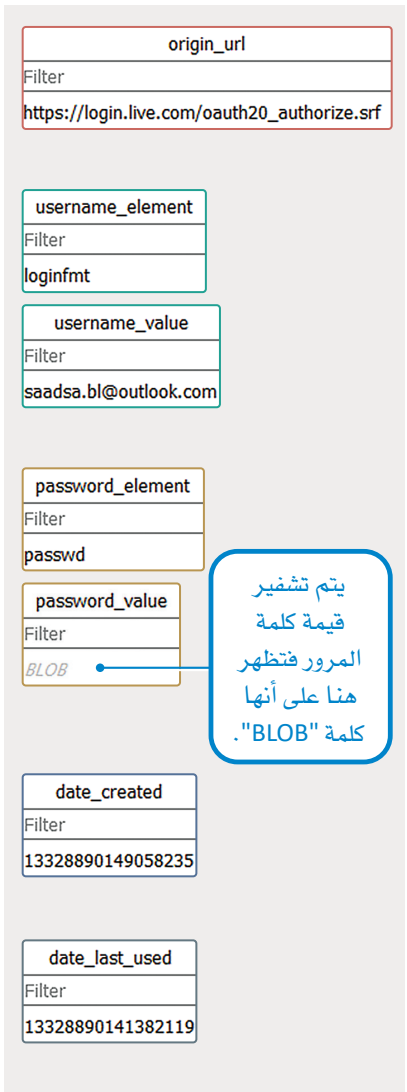
على غِرار حقول اسم المُستخدِم، تلتقط هذه الحقول اسم عنصر **لغة ترميز النص التشعبي** (HTML) والقيمة المقابلة لكلمة المرور المُستخدَمة أثناء تسجيل الدخول، وتوفِّر معلومات حول قيم حقول كلمة المرور في نموذج الويب.

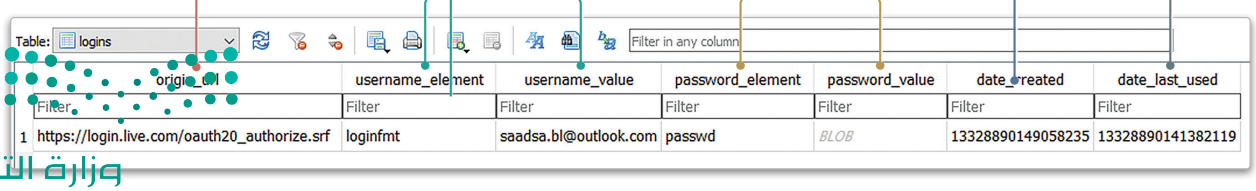
عمود تاريخ الإنشاء (date_created):

يشير حقل **تاريخ الإنشاء** (date_created) إلى التاريخ والوقت اللذين تم فيهما إنشاء بيانات اعتماد تسجيل الدخول أو حفظها، ويساعد في تحديد **ختم الوقت** (Timestamp) الذي تم فيه تخزين بيانات الاعتماد من البداية في قاعدة بيانات المتصفح.

عمود تاريخ آخر استخدام (date_last_used):

يُسجِّل حقل **تاريخ آخر استخدام** (date_last_used) أحدث تاريخ ووقت تم فيه استخدام بيانات اعتماد تسجيل الدخول للمصادقة، ويوفِّر معلومات حول آخر مرة تم فيها استخدام بيانات الاعتماد لتسجيل الدخول إلى الموقع المرتبط.





تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. يُركِّز التحليل الجنائي الرقمي على استعادة الملفات المحذوفة وفَك تشفير البيانات.	○	○
2. التحليل الجنائي الرقمي والاستجابة للحوادث عمليات مختلفة.	○	○
3. يُستخدم التحليل الجنائي الرقمي في الإجراءات القانونية فقط.	○	○
4. تتضمن الاستِجابة للحوادث جَمع البيانات وتحليلها لتحديد تفاصيل أي حادث أمن سيبراني.	○	○
5. تؤدّي فِرَق الاستجابة لحوادث أمن الحاسب (CSIRTs) دورًا أساسيًا في الأمن السيبراني.	○	○
6. لا تُعدُّ مراجعة ما بعد الحادث ضرورية لعملية التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR).	○	○
7. يَشمل جَمع الأدلة الجنائية تجميع البيانات من مَصدر واحد فقط.	○	○
8. يتطابق التَحليل الجنائي للذاكرة مع التَحليل الجنائي لنظام الملفات.	○	○

2 حَدِّد مصادر الأدلة التي يجب تحديدها عند إجراء تحقيق التحليل الجنائي الرقمي.

3 حلِّل دور فِرَق الاستجابة لحوادث أمن الحاسب (CSIRTs) في حماية شبكات الأجهزة.

4 صِف خطوات عملية التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR) النموذجية.

5 صِف التحديات الرئيسة المرتبطة بالتحليل الجنائي الرقمي والاستجابة للحوادث.

6 باستخدام متصفح الويب الذي يحتوي على كَمٍ كبيرٍ من بيانات الأنشطة، حلِّل النتائج من جدول عناوين URL، وحاوِل تحديد ما إذا كانت هناك أنماط معيَّنة يتبعها المُستخدِم في نشاط تصفح الويب الخاص به.

7 باستخدام طبيعة البيانات نفسها من التمارين السابقة، قَيِّم البيانات من جدول تسجيلات الدخول (Logins) واسرد المواقع التي أدخل فيها المُستخدِم بيانات اعتماده، ثم صنِّف هذه المواقع على أنها آمنة أو غير آمنة.

المشروع

افترض أنك متخصص أمن سيبراني في مؤسسة كبيرة وتتعامل مع تَفشّي فيروس على شكل دودة برمجية ضارة جديدة، وينتشر هذا الفيروس المتنقل عبر الوسائط القابلة للإزالة ويُصيب الأجهزة المُضيفة، حيث يعمل على تثبيت برنامج يقوم بهجوم **حجب الخدمة الموزع** (DDoS) عليها، وهكذا تكون المؤسسة قد تعرَّضت فِعليًا إلى هجمات واسعة النطاق قبل توافر تحديثات برامج مكافحةالفيروسات. عليك وضع استراتيجيات لتحديد هذا الفيروس واحتوائه وحماية البيانات الحساسة.

1 حَدِّد الطرائق التي يُمكن لفريق الاستجابة للحوادث استخدامها للعثور على جميع الأجهزة المصابة، وناقش كيف يُمكن للمؤسسة محاولة منع هذا الفيروس من دخول أجهزتها قبل إصدار تحديثات مكافحة الفيروسات الخاصة بهذا الفيروس.

2 اشرح الخطوات التي يُمكن أن تتخذها المؤسسة لمنع انتشار هذا الفيروس عَبر الأجهزة المصابة قبل إصدار تحديثات مكافحة الفيروسات الخاصة بهذا الفيروس، ثم ناقش كيف سيتغير التعامل مع هذا الحادث إذا تم إعداد الأجهزة المصابة ببرنامج هجوم **حجب الخدمة الموزع** (DDoS) لمهاجمة موقع الويب الخاص بمؤسسة أخرى في صباح اليوم التالي.

3 قَدِّم تحليلًا للكيفية التي ستتعامل بها مع هذا الحادث إذا احتوى جهاز أو أكثر من الأجهزة المصابة على معلومات حساسة ومُحدِّدة للهويات الشخصية لموظفي المؤسسة، وما الاحتياطات والإجراءات الإضافية الضرورية لحماية هذه البيانات الحساسة؟

4 صِف التدابير التي سيحتاج فريق الاستجابة للحوادث إلى تنفيذها مع الأجهزة غير المتصلة حاليًا بالشبكة وذلك للتأكد من أنها غير مصابة، أو بأنها لن تنشر الفيروس عند اتصالها.

5 اجمع الملاحظات التي كتبتها وأنشئ عرضًا تقديميًا باستخدام **باوربوينت** (PowerPoint) يوضِّح تحليلًا للسيناريو السابق واستجابة **التحليل الجنائي الرقمي والاستجابة للحوادث** (DFIR).

ماذا تعلّمت

- تحديد نقاط ضعف العتاد وأنظمة التشغيل والبرمجيات.
- وَصف تقنيات التصميم الآمن للأنظمة.
- حماية نظام ويندوز بتقنيات أمنية مختلفة.
- تحديد العلاقة بين هياكل الشبكات وتقنيات الويب وأنظمة الأمن السيبراني.
- التعرف على كيفية تأمين أنظمة الشبكة من خلال البروتوكولات وأفضل الممارسات.
- تحليل تدفق البيانات عبر الشبكة باستخدام وايرشارك (Wireshark).
- تنشيط خدمة الشبكة الافتراضية الخاصة في ويندوز (Windows VPN).
- تحليل كيفية استخدام التحليل الجنائي الرقمي والاستجابة للحوادث (DFIR) في التعامل مع الهجمات السيبرانية المعقدة والدفاع عنها.
- تقييم نشاط الويب للمتصفح باستخدام متصفح دي بي إس كيو لايت (DB Browser for SQLite).

المصطلحات الرئيسة

Intrusion Detection Systems (IDSs)	أنظمة كشف التسلُّل
Packet Analyzers	مُحلِّلات حِزم البيانات
Passkeys	مفاتيح المرور
Secure Programming	البرمجة الآمنة
Security by Design	الأمن من خلال التصميم
Virtual Private Networks (VPNs)	الشبكات الخاصة الافتراضية
Zero Trust Security	الأمن بدرجة صِفر من الثقة

Address Resolution Protocol (ARP)	بروتوكول اقتران العناوين
Computer Security Incident Response Teams (CSIRTs)	فِرَق الاستجابة لحوادث أمن الحاسب
Defense In-Depth	الدفاع متعدد الطبقات
Demilitarized Zones (DMZs)	المناطق العازلة
Digital Forensics (DF)	التحليل الجنائي الرقمي
Firewalls	جُدران الحماية
Incident Response (IR)	الاستجابة للحوادث

3. مواضيع متقدِّمة في الأمن السيبراني

سيتعرَّف الطالب في هذه الوحدة على تأثير التشريعات المتعلقة بالأمن السيبراني على المشهد التّقني الحديث في المملكة العربية السعودية وعلى الصعيد الدولي كذلك، ثُمَّ سيَستعرِض مفاهيم عِلم التشفير الأساسية، ويُنفِّذ خوارزميات التشفير باستخدام لغة برمجة البايثون، وفي الختام سيتعرَّف على أهميَّة أنظمة الأمن السيبراني الحديثة والمتقدِّمة بالنسبة للتطبيقات المُنشأة باستخدام التقنيات الناشئة.

أهداف التعلُّم

بنهاية هذه الوحدة سيكون الطالب قادرًا على أن:

- يُحدِّد النقاط الرئيسة للتشريعات الموحدة للأمن السيبراني.
- يُصنِّف قوانين الأمن السيبراني الرئيسة وضوابطه في المملكة العربية السعودية والدول الأخرى.
- يُفسِّر المقصود بالتشفير واستخداماته.
- يُميِّز بين أنواع التشفير وأنواع التهديدات المحتملة من المُتسلِّلين.
- يُنفِّذ خوارزميات التشفير باستخدام لغة البايثون.
- يُحلِّل كيفية حماية أنظمة الأمن السيبراني للتطبيقات المُنشأة باستخدام التقنيات الناشئة.

الأدوات

- البايثون (Python)

رابط الدرس الرقمي

www.ien.edu.sa

الدرس الأول

تشريعات وقوانين الأمن السيبراني

أهمية تشريعات الأمن السيبراني وقوانينه

The Importance of Laws and Regulations in Cybersecurity

تزداد الحاجة إلى ضمان أمن الأفراد والمنشآت عبر الإنترنت مع التَقدُّم المتسارع لأنظمة التقنيات الحديثة، ولقد تمَّ تطوير التشريعات والقوانين الخاصَّة بالأمن السيبراني لتُؤكِّد على تَحمُّل الأفراد والشركات مسؤولية الحوادث والاختراقات الأمنيّة التي قد تحدث، وتبعاتها، ويُمكن للمؤسسات والجهات الحكومية حماية البيانات بشكلٍ أكثر فعالية بالامتثال لتلك التشريعات والقوانين، إضافةً إلى اللوائح والقوانين الأخرى المتعلقة بالأعمال، ويُساعد فهم التشريعات والقوانين الأفراد والمنشآت في تَبنِّي دور نشط للحفاظ على الأمن عبر الإنترنت، كما تُسهم هذه المعرفة في تعزيز ممارسات الأمن، وإنشاء مُنتَجات أكثر أمنًا، وزيادة ثقة العملاء في المُنتَجات والخدمات المُقدَّمة من الأفراد والمؤسسات.

فيما يلي أهم اعتبارات الاستخدام الصحيح للتشريعات والقوانين المُنظِّمة لمجال الأمن السيبراني:

خصوصية البيانات وحمايتها (Data Privacy and Protection):

مع وجود كميّات ضخمة للغاية من البيانات الحسَّاسة والشخصية التي يتم جمعُها وتخزينها ونَقلها عبر الشبكات رقميًا، فإن القوانين والتشريعات تُساعد في ضمان التعامل مع هذه المعلومات بشكل آمن ومسؤول، مما يحمي حقوق خصوصية الأفراد، ويَمنع الوصول غير المُصرَّح به أو إساءة استخدام تلك البيانات.

المعايير القياسية (Standardization):

تُوفِّر تشريعات الأمن السيبراني وقوانينه مجموعةً قياسيةً من المعايير وأفضل الممارسات التي يجب على المنشآت اتِّباعُها، مما يُعزِّز مستويات الأمن على مستوى المؤسسات والصناعات المختلفة، كما يُسهِّل وجود المعايير القياسية عملية التعاون بين المؤسسات، ويُوفِّر استراتيجيات استجابة موحَّدة أكثر فعالية للتهديدات السيبرانية.

الامتثال والمساءلة (Compliance and Accountability):

تُحمِّل الأُطُر القانونية المُنشآت المسؤولية وضع أمنها السيبراني من خلال مطالبتها بتنفيذ تدابير أمن سيبراني مُحدَّدة، والإبلاغ عن الانتهاكات والاختراقات عند حدوثها، كما يُعزِّز وجود هذه الأُطُر ثقافة الامتثال ويُشجِّع المنشآت على تقييم ممارسات الأمن السيبراني وتحسينها باستمرار.

الرَدع والملاحقة القضائية (Deterrence and Prosecution):

تُحدِّد قوانين الأمن السيبراني مختلف الجرائم الإلكترونية وتُصنِّفها حَسب طبيعتها، مما يسمح لجهات تنفيذ القانون بملاحقة الجُناة ومقاضاتهم، كما تعمل هذه القوانين كرادعٍ ضد الأنشطة السيبرانية الضارة، وتضمن محاسبة مُرتكبي الجرائم السيبرانية على أفعالهم.

التعاون الدولي (International Cooperation):

تَبرُز الحاجة إلى التعاون الدولي لمكافحة الجرائم الإلكترونية نظرًا للنطاق الواسع والعالمي للتهديدات والهجمات السيبرانية، وتُسهِم تشريعات الأمن السيبراني وقوانينه في تعزيز التعاون بين الدول، مما يتيح تبادل المعلومات الاستخباراتية والموارد وأفضل الممارسات في مجال معالجة التهديدات السيبرانية العالمية.

قوانين الأمن السيبراني وتشريعاته في المملكة العربية السعودية
Cybersecurity Laws and Regulations in KSA

ضوابط الأمن السيبراني Cybersecurity Controls

نشرت **الهيئة الوطنية للأمن السيبراني** (NCA) في المملكة العربية السعودية العديد من ضوابط الأمن السيبراني التي يجب على الكيانات العامة والخاصة العامِلة في المملكة العربية السعودية الالتزام بها، وتلك الضوابط هي تدابير تقنية وغير تقنية مُصمَّمة لحماية أنظمة الحاسب والشبكات والبيانات من الوصول غير المُصرَّح به، أو سوء الاستخدام، أو التعديل، أو الإتلاف، أو تعطيل الوصول للبيانات والأنظمة، وفيما يلي نظرة عامة على هذه الضوابط:

الضوابط الأساسية للأمن السيبراني (Essential Cybersecurity Controls – ECC):

يُعدُّ توفير الحد الأدنى من المتطلبات الأساسية للأمن السيبراني الهدف الرئيس لهذه المتطلبات التي صُمِّمت بناءً على أفضل الممارسات والمعايير لحماية الأصول المعلوماتية للجهات من التهديدات الداخلية والخارجية وتقليل المخاطر السيبرانية، كما تتناول هذه الضوابط جوانب مختلفة من الأمن السيبراني، بما في ذلك إدارة الأصول وهويات الدخول والصلاحيات، وإدارة حوادث وتهديدات الأمن السيبراني، والتوعية والتدريب بالأمن السيبراني. وتُعدُّ هذه الضوابط ملزمة على جميع الجهات الحكومية في المملكة العربية السعودية، بما في ذلك الوزارات والهيئات والمؤسسات وغيرها، والجهات والشركات التابعة لها، وجهات القطاع الخاص التي لديها **بُنى تحتية وطنية حسَّاسة** (Critical National Infrastructures - CNIs) أو تعمل على تشغيلها أو استضافتها؛ وذلك لضمان حماية أنظمة المعلومات الخاصة بها.

شكل 3.1: المكونات الأساسية للضوابط (ECC – 1: 2018)

ضوابط الأمن السيبراني للبيانات (Data Cybersecurity Controls – DCC):
أصدرت **الهيئة الوطنية للأمن السيبراني** (NCA) ضوابط الأمن السيبراني للبيانات لتحسين تنظيم الفضاء السيبراني وأمنه في المملكة، وتهدف تلك الضوابط إلى رفع مستوى الأمن السيبراني لحماية البيانات الوطنية، وتعزيز الأمن السيبراني للجهات خلال مراحل دورة حياة البيانات وذلك لضمان حماية بياناتها والأصول المعلوماتية من التهديدات والمخاطر السيبرانية.

1. حوكمة الأمن السيبراني Cybersecurity Governance	1-1	المراجعة والتدقيق الدوري للأمن السيبراني	1-2	الأمن السيبراني المتعلق بالموارد البشرية
	1-3	برنامج التوعية والتدريب بالأمن السيبراني		
2. تعزيز الأمن السيبراني Cybersecurity Defense	2-1	إدارة هويات الدخول والصلاحيات	2-2	حماية الأنظمة وأجهزة معالجة المعلومات
	2-3	أمن الأجهزة المحمولة	2-4	حماية البيانات والمعلومات
	2-5	التشفير	2-6	الإتلاف الآمن للبيانات
	2-7	الأمن السيبراني للطابعات والماسحات الضوئية وآلات التصوير		
3. الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	31	الأمن السيبراني المتعلق بالأطراف الخارجية		

شكل 3.2: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للبيانات (DCC)

ضوابط الأمن السيبراني للحوسبة السحابية (Cloud Cybersecurity Controls):
طوَّرت **الهيئة الوطنية للأمن السيبراني** (NCA) ضوابط الأمن السيبراني للحوسبة السحابية كامتداد **الضوابط الأساسية للأمن السيبراني** (ECC)، وذلك بهدف تقليل المخاطر السيبرانية على **مقدمي الخدمات السحابية** (Cloud Service Providers – CSOs) و**مشتركي الخدمات السحابية** (Cloud Service Tenants – CSTs).

ضوابط الأمن السيبراني للعمل عن بُعد (Telework Cybersecurity Controls):
الغرض من هذه الوثيقة هو رفع جاهزية الجهات للعمل عن بُعد بشكل آمن والتكيّف مع تغيرات بيئات وأنظمة العمل عن بُعد، بالإضافة لتعزيز قدرات الأمن السيبراني للجهات للصمود ضد التهديدات السيبرانية عند العمل عن بُعد.

ضوابط الأمن السيبراني للأنظمة الحسَّاسة (Critical Systems Cybersecurity Controls):
تَهدف هذه الضوابط إلى تطوير قدرات الحماية والصمود ضد الهجمات السيبرانية، وذلك لتمكين الجهات ذات الأنظمة الحساسة من المحافظة على أصولها المعلوماتية والتقنية لتلبية الاحتياجات الأمنية الحالية وتعزيز جاهزية الجهات حيال المخاطر السيبرانية المتزايدة والتي قد ينجم عنها تأثيرات ضارة على المستوى الوطني.

ضوابط الأمن السيبراني للأنظمة التشغيلية (Operational Technology Cybersecurity Controls):
تَهدف هذه الضوابط إلى رفع جاهزية الجهات حتى تتمكن من حماية أنظمتها التشغيلية، كما تحدِّد الوثيقة الحد الأدنى من متطلبات الأمن السيبراني للأنظمة التشغيلية في المرافق الصناعية الحساسة لدى الجهات الحكومية والخاصة لمنع الوصول غير المُصرَّح به لهذه الأنظمة.

أنظمة الجرائم الإلكترونية Cybercrime Regulation

تم تشريع العديد من القوانين والضوابط في المملكة العربية السعودية لمكافحة الجرائم الإلكترونية وحماية خصوصية وأمن الأفراد والمنشآت، وفيما يلي لمحة عامة حول أبرزها:

قانون حماية البيانات الشخصية (Personal Data Protection Law – PDPL):
تم تشريع **قانون حماية البيانات الشخصية** (PDPL) ولوائحه التنفيذية لحماية خصوصية الأفراد في المملكة العربية السعودية، حيث يضع الأساس القانوني لحماية حقوق الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قِبَل جميع الكيانات في المملكة وخارجها لجميع الأفراد في المملكة باستخدام أي وسيلة، بما في ذلك معالجة البيانات الشخصية عبر الإنترنت.

قانون مكافحة جرائم المعلوماتية (Anti-Cyber Crime Law):
قانون مكافحة جرائم المعلوماتية في المملكة العربية السعودية هو مجموعة من القوانين والضوابط التي تُجرِّم مجموعة واسعة من أنشطة الجرائم الإلكترونية، ولقد تم سَنُّ القانون لحماية الأمن القومي للبلاد ومصالحها الاقتصادية من التهديدات السيبرانية، وضمان سلامة المواطنين والمقيمين من الجرائم الإلكترونية.

يُجرِّم قانون مكافحة جرائم المعلوماتية كافة أنشطة الجرائم الإلكترونية مثل: القرصنة، والاحتيال عبر الإنترنت، وانتحال الشخصية، وانتهاك الخصوصية، كما يتضمن أحكامًا لحماية البيانات الشخصية والتحقيق في الجرائم الإلكترونية والملاحقة القضائية لمُرتكبيها.

بموجب قانون مكافحة جرائم المعلوماتية تُعدُّ الجريمة الإلكترونية جريمة خطيرة يُعاقب عليها بالغرامة والسجن وعقوبات أخرى، كما يُخوّل القانون الحكومة باتخاذ تدابير لمنع الوصول إلى مواقع الويب التي تُعدُّ مُتورِّطةً في الجرائم الإلكترونية.

القوانين والضوابط الدولية للأمن السيبراني
International Cybersecurity Laws and Regulations

أصبحت القوانين والضوابط الدولية للأمن السيبراني ذات أهمية متزايدة في حماية البيانات والمعلومات على المستوى العالمي، وذلك بالإضافة إلى القوانين والضوابط المعمول بها فعليًا في المملكة العربية السعودية، وفيما يلي بعض أبرز القوانين والضوابط الدولية للأمن السيبراني:

الولايات المتحدة الأمريكية USA

قانون الاحتيال والانتهاك الحاسوبي (Computer Fraud and Abuse Act – CFAA):
هو قانون اتحادي خاص بجرائم الحاسب وخصوصية البيانات، حيث يَحظُر القانون الوصول غير المُصرَّح به إلى أجهزة الحاسب، وكافة أشكال التخريب أو الضرر المتعمد لأي نظام حاسب، وهو أحد القوانين الفيدرالية الأولى التي تُجرِّم إساءة استخدام الحاسب وتُركِّز على حماية البيانات.

قانون نقل التأمين الصحي والمساءلة (Health Insurance Portability and Accountability Act – HIPAA):
هو قانون اتحادي يَضعُ معايير وطنية لحماية المعلومات الصحِّية الحسَّاسة للمرضى، ويحميها من المشاركة أو النشر دون موافقة المريض أو عِلمه، ولقد تم وضعه في عام 1996.

قانون حماية خصوصية الأطفال على الإنترنت (Children's Online Privacy Protection Act – COPPA):
هو قانون في الولايات المتحدة يُحدِّد قواعد جَمع البيانات الشخصية من الأطفال الذين تقِلُّ أعمارهم عن 13 عامًا واستخدامها، ويتطلب من مواقع الويب وتطبيقات الهاتف الذكي والخدمات الإلكترونية الأخرى الحصول على موافقة الوالدين قبل جَمع تلك البيانات، أو استخدام معلوماتهم الشخصية ومشاركتها.

الاتحاد الأوروبي EU

قانون الاتحاد الأوروبي للأمن السيبراني (EU Cybersecurity Act):
يُعزِّز قانون الاتحاد الأوروبي للأمن السيبراني صلاحيات **وكالة الاتحاد الأوروبي للأمن السيبراني** (EU Agency for Cybersecurity-ENISA)، ويُنشئ إطارًا للمصادقة على الأمن السيبراني للمُنتَجات والخدمات، حيث تقوم تلك الوكالة بإعداد الأُسُس التّقنية لخُطط الاعتماد، ويُؤسِّس القانون إطار الاعتماد على مستوى الاتحاد الأوروبي لمُنتَجات تقنية المعلومات والاتصالات، وخدماتها، وعملياتها، كما يعني هذا أنّ الشركات العاملة في الاتحاد الأوروبي يجب أن تحصل على المصادقة على مُنتَجاتها وعملياتها وخدماتها في مجال تقنية المعلومات والاتصالات مرة واحدة كي يتم تعميم الاعتراف بتلك المُصادَقات في جميع أنحاء الاتحاد الأوروبي.

النظام الأوروبي العام لحماية البيانات (General Data Protection Regulation - GDPR):
هو لائحة قانونيّة تَختصُّ بحماية البيانات والخصوصية في الاتحاد الأوروبي والمنطقة الاقتصادية الأوروبية، وينطبق قانون **النظام الأوروبي العام لحماية البيانات** (GDPR) على معالجة البيانات الشخصية كليًا أو جزئيًا بالوسائل المؤتمتة، ومعالجتها بغيرها من تلك الوسائل التي تشكل أو ستشكل جزءًا من نظام الملفات.

المملكة المتحدة UK

لوائح أمن الشبكات وأنظمة المعلومات (Network & Information Systems Regulations – NIS):
هي قوانين تَهدف إلى زيادة أمن الشبكات الرقمية والمادية وأنظمة المعلومات، ولقد تم تَشريعها لحماية الخدمات الأساسية والرقمية من الهجمات السيبرانية، ولحماية المواطنين والشركات والخدمات العامة، وتنطبق هذه اللوائح على الشركات التي تُقدِّم الخدمات الأساسية مثل: النقل، والطاقة، والمياه، والصحة، والبنيَة التحتيَّة الرقمية، إضافة إلى مُقدِّمي الخدمات الرقمية، بما في ذلك المتاجر الإلكترونية، ومحركات البحث، وخدمات الحوسبة السحابية.

تمرينات

1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. يَقتصر تطبيق القوانين والضوابط الخاصة بالأمن السيبراني على حماية المنشآت من التهديدات السيبرانية.	○	○
2. يَعمل وجود المعايير القياسية لقوانين الأمن السيبراني وضوابطه على تعزيز مستويات الأمن.	○	○
3. لا تتحمَّل الحكومات والمؤسسات أي مسؤولية حول أي اختراقات أمن سيبراني.	○	○
4. لا يُعدُّ التعاون الدولي أساسيًا في مكافحة الجريمة الإلكترونية.	○	○
5. لا تؤثِّر قوانين الأمن السيبراني وضوابطه على ثِقة العملاء في المُنتَجات والخدمات.	○	○
6. تَهدف الهيئة الوطنية للأمن السيبراني (NCA) إلى حماية مصالح المملكة من خلال تعزيز البنيَة التحتيَّة للأمن السيبراني.	○	○
7. تتناول الضوابط الأساسية للأمن السيبراني (ECC) إدارة هويات الدخول والصلاحيات فقط.	○	○
8. يُوفِّر قانون حماية البيانات الشخصية (PDPL) تَدابير لإدارة الأمن السيبراني السحابي.	○	○
9. يُنظِّم قانون نقل التأمين الصحي والمساءلة (HIPPA) عملية الوصول غير المُصرَّح به للبيانات المالية الرقمية.	○	○
10. يُغطِّي قانون مكافحة جرائم المعلوماتية السعودي كلًا من أمن الأفراد وأمن المؤسسات.	○	○

2 اشرح فوائد المعايير القياسية لقوانين الأمن السيبراني في الشركات والمؤسسات.

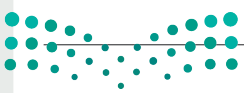
3 حلِّل فئتين فرعيتين من ضوابط الأمن السيبراني للبيانات.

4 قَيِّم الآثار المترتبة على عدم الامتثال لقوانين الأمن السيبراني وأنظمته.

5 عَرِّف قانون مكافحة جرائم المعلوماتية في المملكة العربية السعودية.

6 ابحث في الإنترنت عن الضوابط الأساسية للأمن السيبراني (ECC)، وأذكر الضوابط الرئيسة لبرنامج التوعية بالأمن السيبراني، والتدريب عليه.

7 قَيِّم الآثار المترتبة على النظام الأوروبي العام لحماية البيانات (GDPR) على الشركات العاملة عبر الحدود.



رابط الدرس الرقمي

www.ien.edu.sa

الدرس الثاني

التشفير في الأمن السيبراني

مقدمة في علم التشفير Introduction to Cryptography

أهمية علم التَشفير The Importance of Cryptography

علم التشفير هو العِلم الذي يختصُّ بالكتابة السرِّية بهدف إخفاء المعنى الحقيقي للرسالة، ويَهدفُ هذا العِلم إلى الحفاظ على المعلومات آمنةً وسريةً باستخدام الترميز والخوارزميات والشفرات. لعِلم التشفير تاريخ طويل، حيث تطوَّرت أشكاله على مدى التاريخ بِدءًا بالشّفرات البسيطة المَبنيَّة على استبدال الحروف التي استخدمتها الحضارات القديمة، إلى خوارزميات التشفير المتطورة المُستخدَمة في الاتصالات الرقمية الحديثة، ويَعكس تطوره عبر التاريخ الابتكار المستمر والجهود المبذولة لتطوير تقنيات التشفير للاستجابة للاحتياجات المُتغيِّرة والتقدُّم التقني.

يَعتمدُ عِلم التشفير في جوهره على مفهومين أساسيين هما: **التشفير** (Encryption) و**فكُّ التشفير** (Decryption)، حيث يُحوِّل التشفير النص غير المُشفَّر والمعلومات القابلة للقراءة إلى نص مُشفَّر ومعلومات غيرَ قابلة للقراءة وذلك باستخدام مفتاح سرِّي وخوارزمية محدَّدة، بينما يعمل فكُّ التشفير عكس ذلك، فهو ببساطة عملية تحويل النص المُشفَّر مرة أخرى إلى نص غير مشفّر.

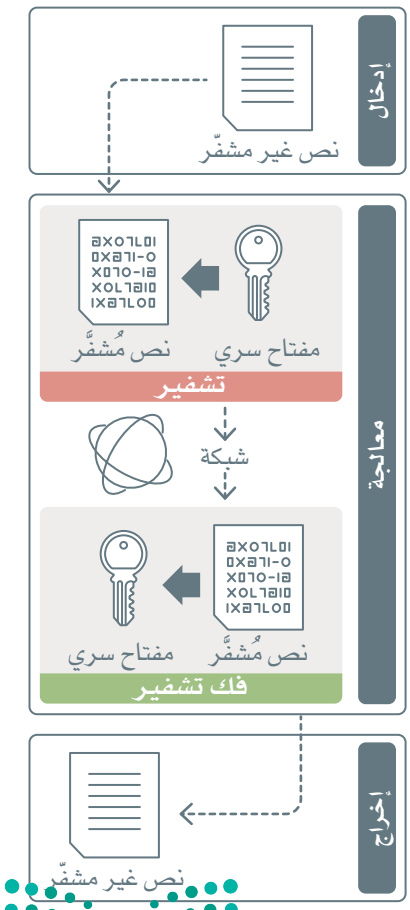
يُعدُّ عِلم التشفير أمرًا حيويًا لتأمين الاتصالات وحماية البيانات في عالم يعتمد على الاتصالات بشكلٍ متزايد، وتوضِّح النقاط التالية أهمية هذا العِلم:

سرِّية البيانات (Data Confidentiality):
يقوم التشفير بحماية البيانات الحسَّاسة والمعلومات الشخصية والمالية والسرية بحيث لا يتمكَّن من الوصول إليها إلا أولئك المُصرَّح لهم بذلك باستخدام المفاتيح الصحيحة لفك التشفير، ويُعدُّ هذا ضروريًا للقطاعات الحيوية في الدولة مثل: القطاعات المالية، ومؤسسات الرعاية الصحية، والهيئات الحكومية.

المصادقة (Authentication):
يُتيح التشفير استخدام التَّوقيعات الرقمية للتحقُّق من صحَّة الرسائل، وإنشاء هوية المُرسِل، ومنع العَبَث بالمحتوى أثناء الإرسال.

السلامة (Integrity):
يُساعد التشفير على ضمان سلامة البيانات باستخدام تقنيات متقدِّمة للتحقق واكتشاف أي تغيير.

عدم الإنكار (Non-repudiation):
تُوفِّر تقنيات التشفير خاصية عدم الإنكار، مما يضمن عدم تَمكُّن الأطراف التي تملك إمكانية الوصول إلى البيانات من إنكار مُعامَلاتهم أو تداولهم للبيانات، ويُعدُّ هذا الأمر مهمًا في الأغراض القانونية والمالية وغيرها، حيث يكون الحفاظ على سلامة البيانات والمُعامَلات أمرًا ضروريًا.



شكل 3.3: تمثيل عملية تشفير وفك تشفير قياسية

تطبيقات التشفير Applications of Cryptography

تطبيقات التشفير واسعة ومتنوعة، وتؤدّي دورًا حاسمًا في تأمين الاتصالات وحماية البيانات الحسَّاسة وتعزيز الثقة في التقنيات الرقمية للاستخدامات المختلفة، ويُوضِّح الجدول 3.1 أكثر تطبيقات التشفير شيوعًا.

جدول 3.1: تطبيقات التشفير الشائعة

التطبيق	الوصف
 المراسلة الآمنة	يُعدُّ التشفير ضروريًا لتأمين قنوات الاتصال بين المُستخدِمين مما يضمن سرِّية المحادثات وسلامتها، فعلى سبيل المثال: تستخدِم تطبيقات مثل **سيجنال** (Signal) وواتس آب (WhatsApp) طريقة تشفير تدعى **التشفير التام بين الطرفين** (End-to-End Encryption – E2EE) لحماية الرسائل من الوصول غير المُصرَّح به أو من التَنصُّت عليها، وباستخدام تلك الطريقة يُمكن للمُستلِمين المستهدَفين فقط فكُّ تشفير الرسائل وقراءتها، مما يُوفِّر مستوى عالٍ من الأمن والخصوصية.
 أمن البريد الإلكتروني	تُعدُّ بعض تقنيات التشفير مثل **تقنية الخصوصية الجيدة** (Pretty Good Privacy – PGP) مفيدةً في تأمين اتصالات البريد الإلكتروني، وتقوم هذه التقنية بتشفير الرسائل والمرفقات، مما يضمن سرِّية المحتوى وسلامته، فهي تسمح للمُستلِم المستهدَف فقط بالوصول إلى المعلومات وفك تشفيرها، مما يوفِّر أمنًا قويًا للبريد الإلكتروني كوسيلة اتصالات. وتوفِّر هذه التّقنية التوقيعات الرقميّة التي تسهم في التحقُّق من شخصية المُرسِل، مما يؤدي إلى بناء الثقة في عمليات تبادل البريد الإلكتروني.
 تصفُّح الويب الآمن	يُعدُّ التشفير الآمن باستخدام **بروتوكول نقل النص التشعبي الآمن** (HTTPS) ضروريًا لتأمين عملية تَصفُّح الويب، حيث يتم تشفير الاتصال بين متصفح المُستخدِم وخادم الويب، مما يوفِّر سرِّية البيانات الحسَّاسة التي يتم تبادلها أثناء التصفح وسلامتها.
 أمن التجارة الإلكترونية	يحمي التشفير البيانات الحسَّاسة في التجارة الإلكترونية، حيث يتم تشفير المعلومات المالية المهمة مثل تفاصيل بطاقات الائتمان، مما يضمن السرِّية وعدم الإنكار، كما يُتيح التشفير التحقُّق من موثوقية موقع الويب باستخدام تقنيات مثل **كيربيروس** (Kerberos)، و**البنيَة التحتيَّة للمفاتيح العامة** (Public Key Infrastructure – PKI) لتقديم تجربة تسوق آمنة للعملاء.
 الشبكة الافتراضية الخاصة	يُستخدم التشفير إلى جانب **بروتوكول الإنترنت الآمن** (IPsec) في **الشبكات الافتراضية الخاصة** (VPNs) لإنشاء اتصالات آمنة ومُشفَّرة بين الأجهزة البعيدة والشبكة الخاصة. **بروتوكول الإنترنت الآمن** (IPsec) هو مجموعة بروتوكولات تُوفِّر المصادقة والتشفير والتحقق من تكامل الاتصالات بين عناوين **بروتوكول الإنترنت** (IP)، ومع التشفير يضمن هذا البروتوكول سرية البيانات المنقولة عبر الشبكة الافتراضية الخاصة وسلامتها.
 أمن إنترنت الأشياء	يؤدّي التشفير دورًا مهمًا في ضمان الاتصال الآمن وحماية البيانات مع النمو السريع لأجهزة إنترنت الأشياء، حيث تقوم تقنيات التشفير الخفيفة بتشفير البيانات المنقولة بين أجهزة إنترنت الأشياء و**الخوادم الخلفية** (Backend Servers).

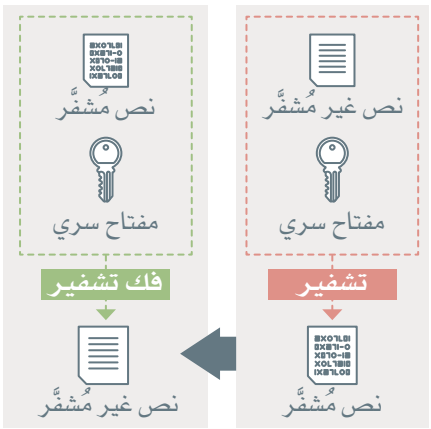
التطبيق	الوصف
 سلسلة الكُتل والعملات الرقمية	يُعدُّ التشفير عُنصرًا أساسيًا في تقنية **سلسلة الكُتل** (Blockchain) و**العملات الرقمية** (Digital Currencies)، حيث يُستخدم لحماية المُعامَلات والحفاظ على **السِجل الموزع** (Distributed Ledger)، وضمان موثوقية المشتركين.

أنواع التشفير Types of Cryptography

يَشمل التشفير مجموعة متنوعة من التقنيات يُمكن تصنيفها على نطاق واسع إلى ثلاثة أنواع رئيسة هي: **تشفير المفتاح المتماثل** (Symmetric Key Cryptography)، و**تشفير المفتاح غير المتماثل** (Asymmetric Key Cryptography)، و**دوال الاختزال** (Hash Functions)، بحيث يخدم كل نوع غرضًا مختلفًا، ويتمتع بمزايا وقيود اعتمادًا على متطلبات الأمن وحالات الاستخدام المحدَّدة، وفيما يلي نبذة عن كل نوع من هذه الأنواع:

تشفير المفتاح المتماثل Symmetric Key Cryptography

يَستخدِم تشفير المفتاح المتماثل أو تشفير المفتاح السريّ مفتاحًا واحدًا لعمليات التشفير وفك التشفير، وتتمثل وظيفته الرئيسة في التحويل والتبديل. إذا أراد المُرسِل إرسال بيانات مُشفَّرة، فإنه يَستخدِم المفتاح السريّ المشترك لتشفير النص العادي وتحويله إلى نص مُشفَّر، ثم يقوم المُستلِم الذي يمتلك المفتاح السريّ نفسه أيضًا بفك تشفير النص المُشفَّر مرة أخرى إلى نص غير مُشفَّر. يُعدُّ طول المفتاح مهمًا جدًا في تشفير المفتاح المتماثل، ومن أمثلة خوارزميات المفاتيح المتماثلة الشائعة خوارزمية **معيار التشفير المتقدِّم** (Advanced Encryption Standard – AES).



شكل 3.4: عملية التشفير باستخدام المفتاح المتماثل

تشفير المفتاح غير المتماثل Asymmetric Key Cryptography

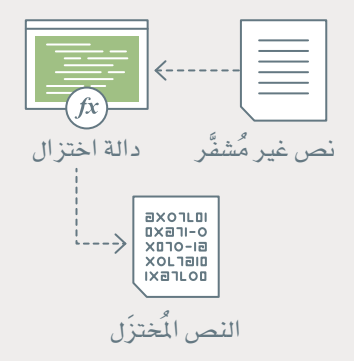
يتضمَّن تشفير المفتاح غير المتماثل، أو تشفير المفتاح العام، استخدام مفتاحين مُختلفين يرتبطان حسابيًا وهُما: **المفتاح العام** (Public Key) و**المفتاح الخاص** (Private Key). يتم توزيع المفتاح العام ومشاركته بطريقة عَلنية، بينما يبقى المفتاح الخاص سرِّيًا بحَوزَة المالك، ولا يُمكن الوصول إلى المفتاح الخاص من خلال المفتاح العام، ويجب أن تحظى الجهة التي تُزوِّد المُستخدِم بالمفتاح العام بالثقة لكي يعمل تشفير المفتاح غير المُتماثل بشكل صحيح. إذا أراد المُرسِل تشفير البيانات، فإنه يَستخدِم المفتاح العام للمُستلِم، وعند استلام البيانات المُشفَّرة يَستخدِم المُستلِم مفتاحه الخاص لفك تشفير الرسالة. على العكس من ذلك، يُمكن استخدام المفتاح الخاص لتواقيع البيانات لأغراض المصادقة، ويُمكن التحقُّق من التَّوقيع بواسطة المفتاح العام. تَتضمَّن بعض خوارزميات المفاتيح غير المتماثلة المُستخدَمة على نطاق واسع خوارزمية آر إس إيه (RSA)، وخوارزمية **ديفي-هيلمان** (Diffie-Hellman)، وخوارزمية **التشفير بالمنحنيات الإهليلجية** (Elliptic Curve Cryptography – ECC)، فمن المهمِّ ملاحظة أن طول المفتاح بوحدة **البت** (Bits) يؤثِّر بشكلٍ مباشرٍ على أمن التشفير، حيث تُوفِّر المفاتيح الأطول حماية أقوى ضد الهجمات.

شكل 3.5: عملية التشفير باستخدام المفتاح غير المتماثل

دوال الاختزال Hash Functions

دوال الاختزال هي تقنية تشفير تقوم بتحويل مُدخَلات ذات طول عشوائي إلى مُخرَجات بطول ثابت، وتَكون هذه الدوال أُحادية الاتجاه، وبالتالي يستحيل حسابيًا الهندسة العكسية للنصّ المُختزل بهدف الحصول على المُدخَل الأصلي، حيث يؤدي التغيير في المُدخَلات على الأرجح إلى تغيير في المُخرَجات. تُعدُّ دالة الاختزال مفيدة بشكلٍ خاصٍ لضمان سلامة البيانات والمصادقة عليها.

عندما يتم نقل البيانات أو تخزينها، يُمكن إنشاء دالة الاختزال وإرسالها مع البيانات، ويُمكن للمُستلِم بعد ذلك حساب اختزال جديد للبيانات المستلَمة ومقارنتها بالاختزال الأَصلي، وإذا تطابقت الاختزالات، فهذا يعني أنه لم يتم العبث بالبيانات أو تغييرها. تتضمَّن بعض خوارزميات الاختزال الشائعة **خوارزمية الاختزال الآمنة** (Secure Hash Algorithm 3 – SHA3)، و**خوارزمية ملخص الرسائل 5** (Message Digest 5 – MD5)، ودوال **رمز مصادقة الرسالة المستند إلى الاختزال** (Hash based Message Authentication Code – HMAC).



شكل 3.6: عملية التشفير باستخدام دوال الاختزال

جدول 3.2: مزايا أنواع التشفير وعيوبه

النوع	المزايا	العيوب
تشفير المفتاح المتماثل	• أسرع وأكثر كفاءة من الناحية الحسابية. • مناسب لتشفير البيانات واسعة النطاق.	• تحدِّيات في توزيع المفاتيح وإدارتها. • لا يستخدِم توقيع رقمي، ولايضمن صحَّة هوية المُستخدِم.
تشفير المفتاح غير المتماثل	• التوزيع المبسط للمفاتيح (مشاركة المفتاح العام). • تمكين التَّوقيعات الرقمية والمصادَقة.	• أبطأ وأكثر صعوبة من الناحية الحسابية. • أقل ملاءمة لتشفير البيانات واسعة النطاق.
الاختزال	• يتميز بالسرعة. • من الصعب عمل الهندسة العكسية للعملية. • المُخرَجات بطولٍ ثابتٍ بغَضِّ النظر عن طول المُدخَلات.	• عُرضَة للتصادم في الخوارزميات الضعيفة، حيث يُمكن لمُدخَلين مختلفين إنتاج المخرَج نفسه.

التحقُّق من صحَّة المفاتيح العامة Validation of Public Keys

يُمثِّل التحقُّق من صحَّة المفتاح العام المُستخدَم لتشفير الرسالة وفك تشفيرها أحد تحدِّيات تشفير المفتاح غير المتماثل، ويتم استخدام الطريقتين التاليتين من أجل التحقق من صحَّة المفتاح العام وضمان مصدره:

شبكات الثِّقة (Webs of Trust):

شبكات الثِّقة هي نهج لامركزي يُستخدَم في التشفير للتحقُّق من صحَّة المفاتيح العامة، ويُمكِن تفسير هذا النهج بالمثال التالي:

لنفترض أنّ خالدًا أراد التحقّق من أمان المفتاح العام لأحمد بطريقة لا تعتمد على هيئة شهادات مركزية، وهي فحص شبكة الثقة، ومن خلال ذلك وجد أن فهد – وهو كيان موثوق به على الويب – قد وَقَّع على المفتاح العام لأحمد ليؤكِّد على صحَّته، وبما أن خالدًا يَعرِف فهد ويثقُ به، فيُمكنه الآن الوثوق في أصالة المفتاح العام الذي يخصُّ أحمد، كما لاحظ خالد أن مُستخدِمين آخرين على الويب قد أكَّدوا على مفتاح أحمد، مما زاد من درجة موثوقية الشبكة، وهذا يعني أنه كلما ازداد عدد المُستخدِمين الذين يؤكِّدون صحَّة مفتاح عام، فإنه يصبح أكثر جدارةً بالثقة داخل الشبكة. يساعد هذا النهج اللامركزي في منع الجهات الضارة من استخدام مفاتيح عامة مزيفة أو غير مُصرَّح بها للوصول إلى البيانات المُشفَّرة، ومن خلال الاعتماد على شبكة من الكيانات الموثوقة يعمل التشفير على تعزيز شبكات الثقة للتحقُّق من صحَّة المفاتيح العامة وضمان أمن وسلامة الاتصالات.

هيئات الشهادات (Certificate Authorities):

هيئة الشهادات (Certificate Authority – CA) هي كيان موثوق به يتحقق من صحَّة المفاتيح العامة في التشفير، كما تؤدّي الهيئة دورًا مركزيًا في مُصادَقة الشهادات الرقمية مثل: شهادات **طبقة المآخذ الآمنة** (Secure Sockets Layer - SSL) التي تُنشئ اتصالات آمنة بين المواقع والمُستخدِمين. على سبيل المثال: عندما يريد موقع ويب الحصول على شهادة **طبقة المآخذ الآمنة** (SSL) الرقمية، يُرسل مَالِك موقع الويب طلبًا إلى مرجعٍ مُصدَّق موثوق به، حيث يتحقَّق هذا المرجِع من هوية المَالِك باستخدام طرائق المصادقة المختلفة، بما في ذلك التحقق من ملكية **النطاق** (Domain)، وبمجرد التحقُّق من هوية المَالِك والمفتاح العام المرتبط تصدر هيئة الشهادات شهادة **طبقة المآخذ الآمنة** (SSL) الرقمية لموقع الويب المرتبط بالنطاق، وتربط هذه الشهادة هوية موقع الويب بمفتاحه العام، مما يتيح الاتصال الآمن والتشفير بين موقع الويب ومُستخدِميه.

هجمات التشفير Cryptography Attacks

هناك العديد من الأساليب والتقنيات التي يستخدمها المتسلِّلون للوصول إلى البيانات المُشفَّرة بواسطة خوارزميات التشفير، وفيما يلي طريقتان من أكثر الطرائق المُستخدَمة شيوعًا:

هجمات القوة المُفرطة (Brute Force Attacks):

تُستخدَم هجمات القوة المُفرطة في هجمات التشفير كطريقة تعتمد على المحاولة والخطأ لاختراق البيانات المُشفَّرة، وفيها يقوم المهاجِم بتجربة كافة التراكيب الممكنة لمفتاح التشفير حتى يعثر على التركيبة الصحيحة التي يستطيع باستخدامها فك تشفير البيانات.على سبيل المثال، يحاول المهاجِم في هجوم القوة المُفرطة الكشف عن كلمة مرور مُشفَّرة باستخدام مجموعات مختلفة من الأحرف حتى يكتشف المفتاح الذي يقوم بفك تشفير كلمة المرور، ويُمكن أن تستغرق هذه الطريقة وقتًا طويلًا وتستهلك الكثير من الموارد، خاصةً إذا كانت خوارزمية التشفير تستخدم مفاتيح قوية وطويلة. يوصي **المعهد الوطني للمعايير والتقنية** (National Institute of Standards and Technology – NIST) أن يكون الحدُّ الأدنى لطول المفتاح 2048 بت للتشفير المبني على خوارزمية آر إس إيه (RSA)، وبطول 224 بت للتشفير المبني على **خوارزمية التشفير بالمنحنيات الإهليلجية** (ECC)، وذلك للحماية من هجمات القوة المُفرطة.

تحليل الشفرات (Cryptanalysis):

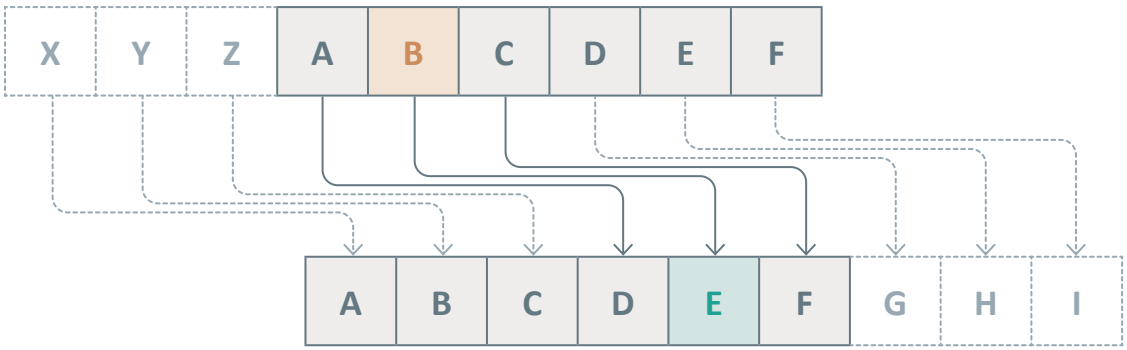
يُستخدَم تحليل الشفرات لمعالجة تشفير البيانات للوصول إلى نقاط الضعف في مُخطَّط التشفير التي يُمكن استغلالها لاستخراج البيانات أو تغييرها، حيث يَستخدِم المتسلِّلون هذا التحليل للوصول إلى البيانات المُشفَّرة مثل: كلمات المرور، وأرقام بطاقات الائتمان والمستندات السرية، وغالبًا ما يستخدمون تقنيات لكسر مُخطَّطات التشفير، بما في ذلك الهجمات التحليلية، والقوة المُفرطة، وهجمات القناة الجانبية. تتضمَّن **الهجمات التحليلية** (Analytical Attacks) خوارزميات لتحديد المفاتيح المحتملة لتشفير البيانات، بينما تقوم هجمات **القوة المُفرطة** (Brute-Force) بالتحقق من جميع المفاتيح الممكنة حتى يتم العثور على المفتاح الصحيح، في حين تستغِل هجمات **القنوات الجانبية** (Side-Channel) العيوب المعروفة في العتاد أو البرمجيات لتجاوز إجراءات الأمن.

تنفيذ خوارزميات التشفير Implementing Cryptographic Algorithms

ستقوم الآن بتنفيذ بعض خوارزميات التشفير باستخدام لغة برمجة **البايثون** (Python).

خوارزمية تشفير قيصر Caesar Cipher

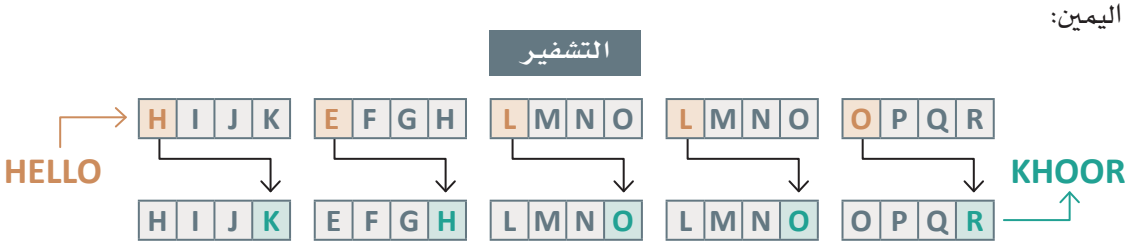
يتم في هذه الخوارزمية استبدال بسيط للحروف، حيث يتم استبدال كل حرف بحرف آخر اعتمادًا على مفتاح التشفير، وهي خوارزمية تشفير بسيطة للغاية لا تُستخدَم في أنظمة الإنتاج.



شكل 3.7: تمثيل خوارزمية تشفير قيصر باستخدام مفتاح = 3

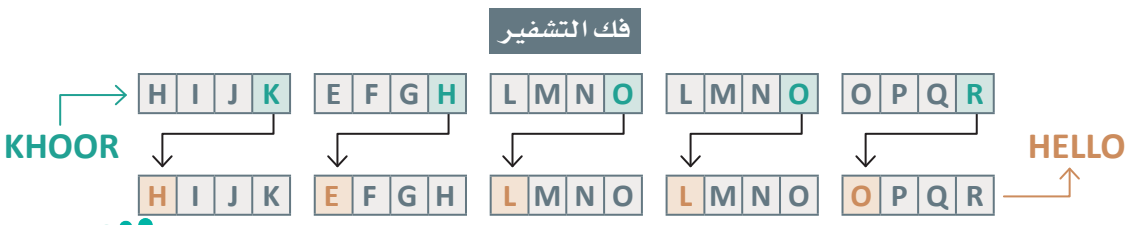
مثال:

ستستخدم هنا إزاحة لليمين لـ 3 (المعروف أيضًا باسم مفتاح 3) في خوارزمية تشفير قيصر. النص غير المشفّر (الرسالة الأصلية) هو HELLO (مرحبًا)، وهنا سيتم إزاحة كل حرف من كلمة "HELLO" ثلاثة مواضع إلى اليمين:



تَمَّ في هذه الحالة تشفير كلمة "HELLO" بخوارزمية تشفير قيصر بإزاحة 3 لتصبح"KHOOR".

لفك تشفير الرسالة يتم الأمر بعكس العملية فقط ليتم إزاحة كل حرف 3 مواضع إلى اليسار، أو 23 موضعًا إلى اليمين، حيث يُمكن الحصول على الناتج نفسه، لأن اللغة الإنجليزية تتكون من 26 حرفًا أبجديًا.



استرجاع الرسالة الأصلية "HELLO".

تشفير الرسالة (Encrypting the Message):

```
def caesar_encrypt(message, key):
    # Create a list of alphabet characters
    alphabet_lower = "abcdefghijklmnopqrstuvwxyz"
    alphabet_upper = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    # Create an empty string to store the encrypted message
    encrypted_message = ""
    # Iterate through each character in the message
    for char in message:
        # Check if character is a lowercase letter
        if char in alphabet_lower:
            # Find index of the character in alphabet list
            char_index = alphabet_lower.find(char)
            # Move the character to the right by the key
            new_char_index = (char_index + key) % 26
            # Add the replaced character to the encrypted message
            encrypted_message += alphabet_lower[new_char_index]
        # Check if character is an uppercase letter
        elif char in alphabet_upper:
            char_index = alphabet_upper.find(char)
            new_char_index = (char_index + key) % 26
            encrypted_message += alphabet_upper[new_char_index]
        else:
            # Add the character to the encrypted message as it is
            encrypted_message += char
    # Return the encrypted message
    return encrypted_message
```

فك تشفير الرسالة (Decrypting the Message):

```
def caesar_decrypt(encrypted_message, key):
    # Create a list of lowercase alphabet characters
    alphabet_lower = "abcdefghijklmnopqrstuvwxyz"
    # Create a list of uppercase alphabet characters
    alphabet_upper = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    # Create an empty string to store the decrypted message
    decrypted_message = ""
```

```
    # Iterate through each character in the encrypted message
    for char in encrypted_message:
        # Check if character is a lowercase letter
        if char in alphabet_lower:
            # Find the index of the character in the lowercase alphabet list
            char_index = alphabet_lower.find(char)
            # Move the character to the left by the key
            new_char_index = (char_index - key) % 26
            # Add the replaced character to the decrypted message
            decrypted_message += alphabet_lower[new_char_index]
        # Check if character is an uppercase letter
        elif char in alphabet_upper:
            # Find the index of the character in the uppercase alphabet list
            char_index = alphabet_upper.find(char)
            # Move the character to the left by the key
            new_char_index = (char_index - key) % 26
            # Add the replaced character to the decrypted message
            decrypted_message += alphabet_upper[new_char_index]
        else:
            # If the character is not a letter, add it to the decrypted message as it is
            decrypted_message += char
    # Return the decrypted message
    return decrypted_message
```

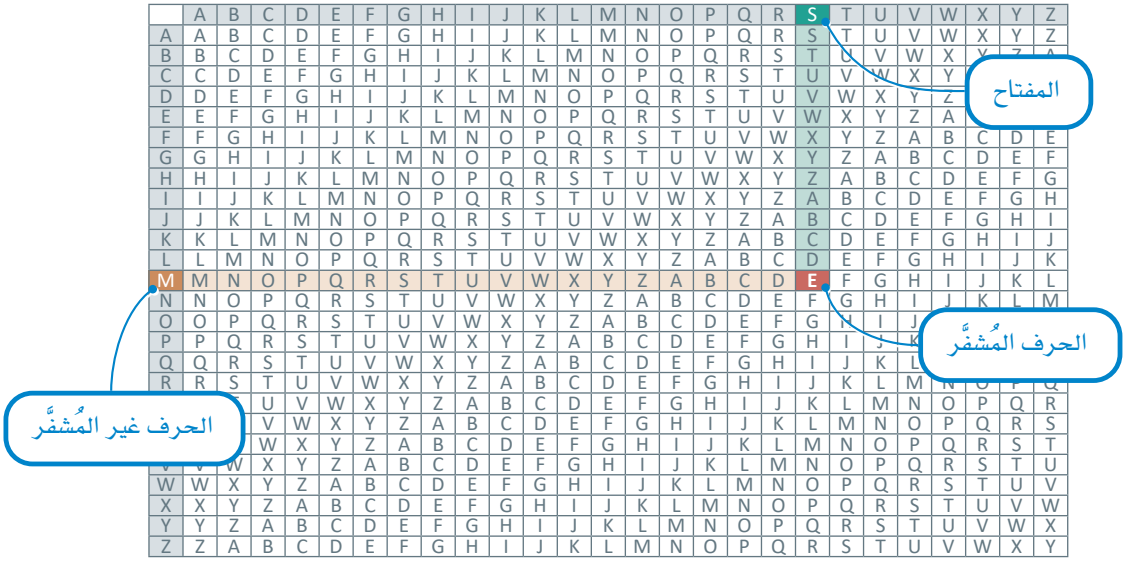
اختبار التشفير (Testing the Cipher):

```
# Testing the Caesar cipher
message = "There are twenty three items in the inventory."
key = 5

encrypted_message = caesar_encrypt(message, key)
decrypted_message = caesar_decrypt(encrypted_message, key)

print(encrypted_message)
print(decrypted_message)
```

```
Ymjwj fwj ybjsyd ymwjj nyjrx ns ymj nsajsytwd.
There are twenty three items in the inventory.
```

خوارزمية تشفير فيجنر Vigenère Cipher

يُعدُّ هذا التشيفر امتدادًا لخوارزمية تشفير قيصر، حيث يتم إزاحة كل حرف بناءً على كلمة مفتاحية لتشفير الرسائل، وهي مثل خوارزمية تشفير قيصر ولكنها أكثر تعقيدًا منها، ورغم ذلك لا يُعدُّ هذا التعقيد كافيًا للاستخدام في أنظمة الإنتاج.



شكل 3.8: تمثيل خوارزمية تشفير فيجنر

مثال:

افترض أن النصَّ غير المشفّر (الرسالة الأصلية) هو "HELLO"، وسيتم استخدام الكلمة الأساسية "KEY". أولًا، ستقوم بمحاذاة الكلمة الأساسية مع النص الغير مشفّر الخاص بك، وتكرِّر الكلمة الأساسية حسب الضرورة:

نص غير مشفّر
HELLO
KEYKE
الكلمة المفتاحية

لذلك، بالنسبة إلى كلمتك الأساسية "KEY"، ستكون الإزاحات Y = 24 ، E = 4 ، K = 10.

يؤدي تطبيق هذه الإزاحات على كل حرف في "HELLO" إلى تحقيق ما يلي:

"H" (تم إزاحتها بمقدار 10 مواضع) لتصبح "R".

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

"E" (تم إزاحتها بمقدار 4 مواضع) لتصبح "I".

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

"L" (تم إزاحتها بمقدار 24 موضعًا) لتصبح "J".

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

"L" (تم إزاحتها بمقدار 10 مواضع) لتصبح "V".

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

"O" (تم إزاحتها بمقدار 4 مواضع) لتصبح "S".

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N

وفي هذه الحالة فإن كلمة "HELLO" المُشفَّرة بواسطة خوارزمية تشفير فيجنر وباستخدام الكلمة المفتاحية "KEY" تُصبح "RIJVS".

لفك تشفير الرسالة، يتم إجراء العملية العكسية ليتم إزاحة كل حرف في "RIJVS" إلى الخلف بالمقدار المحدَّد للحرف المقابل في الكلمة الأساسية "KEY".

تشفير الرسالة (Encrypting the Message):

```
def vigenere_encrypt(plaintext, keyword):
    # Calculate the length of the keyword
    keyword_length = len(keyword)
    # Convert each character in the keyword to its ASCII value
    keyword_as_int = [ord(i) for i in keyword]
    # Convert each character in the plaintext to its ASCII value
```

يمثِّل نظام آسكي (ASCII) نظام ترميز يتكون من مجموعة رموز قياسية تمثِّل جميع الأحرف الأبجدية الرقمية الإنجليزية.

```
    plaintext_int = [ord(i) for i in plaintext]
    ciphertext = ''
    # Loop over each character in the plaintext
    for i in range(len(plaintext_int)):
        # Calculate the new character by adding the ASCII value of the plaintext
        # character and the corresponding keyword character (modulo 26)
        value = (plaintext_int[i] + keyword_as_int[i % keyword_length]) % 26
        # Convert the new character back to a string and append it to the ciphertext
        # Adding 65 converts the value to its ASCII representation as an uppercase letter
        ciphertext += chr(value + 65)
    return ciphertext
```

فك تشفير الرسالة (Decrypting the Message):

```
def vigenere_decrypt(ciphertext, keyword):
    # Calculate the length of the keyword
    keyword_length = len(keyword)
    # Convert each character in the keyword to its ASCII value
    keyword_as_int = [ord(i) for i in keyword]
    # Convert each character in the ciphertext to its ASCII value
    ciphertext_int = [ord(i) for i in ciphertext]
    plaintext = ''
    # Loop over each character in the ciphertext
    for i in range(len(ciphertext_int)):
        # Calculate the original character by subtracting the ASCII value of the
        # corresponding keyword character from the ciphertext character (modulo 26)
        value = (ciphertext_int[i] - keyword_as_int[i % keyword_length]) % 26
        # Convert the original character back to a string and append it to the plaintext
        # Adding 65 converts the decrypted value back to its ASCII representation as an uppercase letter
        plaintext += chr(value + 65)
    return plaintext
```

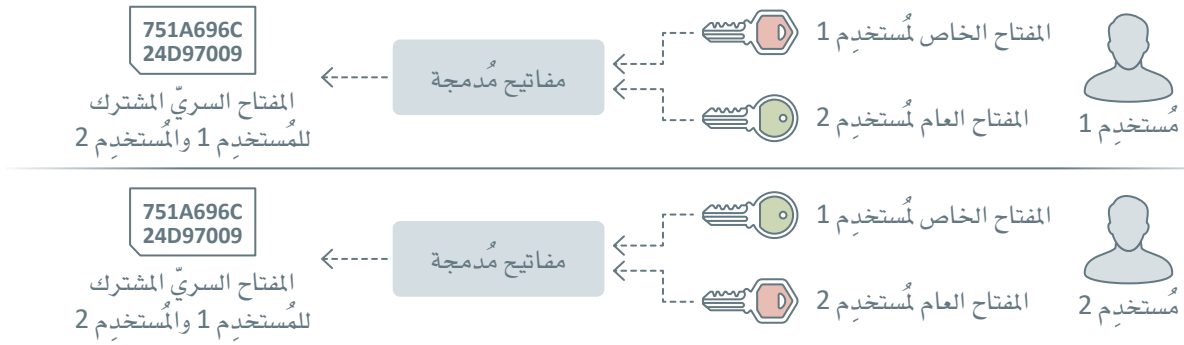
اختبار التشفير (Testing the Cipher):

```
encrypted_message = vigenere_encrypt("THERE ARE TWENTY THREE ITEMS IN THE INVENTORY", "LEMON")
print(encrypted_message)
decrypted_message = vigenere_decrypt(encrypted_message, "LEMON")
print(decrypted_message)
```

```
ELQFREEDSGEAQBGJXFVEPIFWGPQEHVYXFVREMZJRYXAFL
THERETARETTWENTYTTHREETITEMSTINTTHETINVENTORY
```

خوارزمية ديفي-هيلمان لتبادل المفاتيح
The Diffie–Hellman (DH) Key Exchange Algorithm

خوارزمية ديفي – هيلمان لتبادل المفاتيح هي بروتوكول تشفير للاتصال الآمن عبر شبكة غير آمنة، حيث تسمح هذه الخوارزمية لطرفين بإنشاء مفتاح سري مشترك يُمكن استخدامه لتشفير الرسائل المتبادلة بينهما وفك تشفيرها.



شكل 3.9: تمثيل خوارزمية ديفي–هيلمان لتبادل المفاتيح

مثال:

لاستعراض كيفية القيام بعملية التشفير بشكل مبسَّط، سنستعرض مثالًا باستخدام أرقام صغيرة، مع العلم أنّه في التطبيق الواقعي يتم استعمال أرقام أكبر بكثير لتوفير أمن كاف.

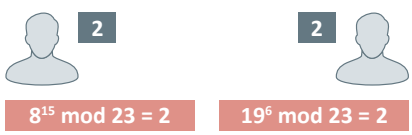
1. يتفق الطرفان في البداية على عددين أوليين كبيرين، على سبيل المثال: 5 (مُعامِل جذر أولي) و23 (مُعامِل باقي القسمة)، كما يُمكن أن تكون هذه الأرقام عامة.

2. يختار بعد ذلك كل طرف رقمًا سريًا، بحيث يختار علي الرقم 6، ويختار أحمد الرقم 15، مع العلم بأن هذه الأرقام خاصة ولا يجب مشاركتها.

3. يتشارك الطرفان القيمة العامة مع بعضهما، بحيث يحسب علي باقي قسمة (Mod) 5^6 على 23 فتكون النتيجة 8، ويحسب أحمد باقي قسمة 5^{15} على 23 فتكون النتيجة 19.

4. يتبادل علي وأحمد هذه القيم العامة.

5. يحسب الآن كل طرف السر المشترك، بحيث يحسب علي باقي قسمة 19^6 على 23 ويحصل على 2، ويحسب أحمد باقي قسمة 8^{15} على 23 ويحصل أيضًا على 2.



هكذا يكون علي وأحمد قد اتفقا على مفتاح سري مشترك، وهو (2 في هذه الحالة) عبر قناة غير آمنة دون إرسال المفتاح السرّي نفسه. سيحتاج المُتنصّت إلى حلّ مسألة لوغاريتمية منفصلة مُعقَّدة لمعرفة المفتاح السريّ، وهو أمر حسابي صعب ويستغرق وقتًا طويلًا خاصةً عند استخدام أعداد أكبر.

إعداد الخوارزمية (Preparing the Algorithm):

```
import random
import hashlib

# Modular exponentiation: (base^exponent) % modulus
def mod_exp(base, exponent, modulus):
    return pow(base, exponent, modulus)

# Generate a large prime number
def generate_large_prime(bits=2048):
    return random.getrandbits(bits) | 1 # Command to create a prime number
```

تنفيذ عملية تبادل المفاتيح (Implementing the Key Exchange):

```
def dh_key_exchange():
    # Agree on large prime numbers p and g
    p = generate_large_prime()
    g = generate_large_prime()

    # Each party selects a private key
    ali_private_key = generate_large_prime()
    ahmed_private_key = generate_large_prime()

    # Each party computes their public key
    ali_public_key = mod_exp(g, ali_private_key, p)
    ahmed_public_key = mod_exp(g, ahmed_private_key, p)

    # Each party exchanges their public key and computes the shared secret
    ali_shared_secret = mod_exp(ahmed_public_key, ali_private_key, p)
    ahmed_shared_secret = mod_exp(ali_public_key, ahmed_private_key, p)

    # Verify that the shared secrets match
    assert ali_shared_secret == ahmed_shared_secret

    # Optionally, hash the shared secret to derive a symmetric key
    shared_secret_hash = hashlib.sha256(str(ali_shared_secret).encode())for bothhexdigest()

    return shared_secret_hash
```

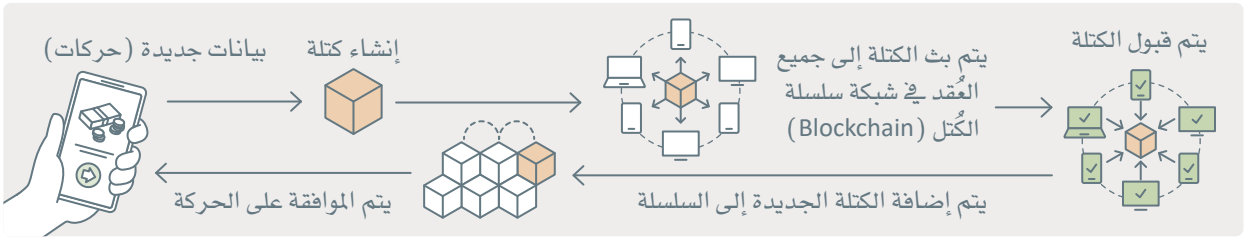
توليد المفتاح السريّ المشترك (Generating the Secret Shared Key):

```
# Produce the shared secret key
shared_secret = dh_key_exchange()
print("Shared secret:", shared_secret)
```

```
Shared secret: 74b40ad75c4d76edcef424bcb1e27be104c60c22072e0aad65b5a29b60d1ddab
```

الأمن السيبراني والتشفير وسلسلة الكُتل Cybersecurity, Cryptography and Blockchain

لقد اكتسبت تقنية **سلسلة الكُتل** (Blockchain) في السنوات الأخيرة اهتمامًا خاصًا في أنظمة الأمن السيبراني، فهي سجل لامركزي مفتوح يُستخدَم لتسجيل المُعامَلات بشكل آمن، ومع ذلك لا تُعدُّ هذه التقنية محصَّنة ضدَّ الثغرات الأمنيّة والهجمات السيبرانية. أحد المجالات المثيرة للقلق في هذه التقنية هو **العقود الذكية** (Smart Contracts)، وهي عقود ذاتية التنفيذ مكتوبة برمجيًا، ويتم تنفيذها باستخدام تقنية **سلسلة الكُتل** (Blockchain). على سبيل المثال، تخيَّل عَقدًا ذكيًا مصمَّمًا لإدارة مُعامَلات سلسلة التوريد، ففي حالة وجود خطأ في البرمجة أو ثغرة أمنية في هذا العقد الذكي، يُمكن للمهاجِم استغلالها للتحايُل أو لتعطيل عملية سلسلة التوريد، وقد يؤدي هذا إلى أنشطة احتيالية أو إلى وصول غير مُصرَّح به إلى المعلومات الحسَّاسة، ويوضِّح الشكل 3.10 تمثيلًا مرئيًا للعمليات التي تستخدمها تقنية **سلسلة الكُتل** (Blockchain).



شكل 3.10: تمثيل تقنية سلسلة الكُتل

ومع ذلك يُمكن أن تساعد تقنية **سلسلة الكُتل** (Blockchain) في تحقيق الأمن السيبراني بطرائق عدّة، بما في ذلك:

إدارة الهوية (Identity Management):
يُمكن **لسلسلة الكُتل** (Blockchain) إنشاء نظام إدارة هوية آمن لامركزي يمكّن المُستخدِمين من التحكُّم ببياناتهم ومشاركتها مع الآخرين حسب الحاجة، فعلى سبيل المثال: يُمكن لأنظمة الهوية المُستنِدة إلى سلسلة الكُتل تخزين هويات المُستخدِمين والتحقُّق منها، مما يصعّب سرقة بياناتهم على المهاجمين، أو تغييرها.

إدارة سلسلة التوريدات (Supply Chain Management):
يُمكن **لسلسلة الكُتل** (Blockchain) إنشاء نظام إدارة سلسلة توريد آمن ومفتوح يسجل جميع المُعامَلات في سجل غير قابل للتلاعب، فعلى سبيل المثال: يُمكن لأنظمة سلسلة التوريد المُستنِدة إلى سلسلة الكُتل تَتَبُّع حركة البضائع والتأكد من عدم العبث بها أو تزويرها.

العقود الذكية (Smart Contracts):
يُمكن **لسلسلة الكُتل** (Blockchain) إنشاء عقود ذكية آمنة ومؤتمتة، والتي بدورها تُساعد في تقليل مخاطر الاحتيال والتأكد من تنفيذ المُعامَلات على النحو المطلوب، فعلى سبيل المثال: يُمكن للعقود الذكية القائمة على **سلسلة الكُتل** (Blockchain) أتمتة عمليات معالجة الدفع، مما يُقلِّل من مخاطر الاحتيال في الدفع.

الشبكات الموزعة (Distributed Networks):
يُمكن **لسلسلة الكُتل** (Blockchain) إنشاء شبكات آمنة غير مركزية، والتي يُمكنها المساعدة في تقليل مخاطر **نقطة الفشل المفردة** (Single Points of Failure)، والتأكد من توزيع البيانات عبر عُقَد متعددة، فعلى سبيل المثال: يُمكن للشبكات القائمة على سلسلة الكُتل إنشاء أنظمة مشاركة الملفات من نقطة إلى نقطة بشكلٍ أكثر أمنًا وفعالية.

تخزين البيانات (Data Storage):
يُمكن استخدام **سلسلة الكُتل** (Blockchain) لإنشاء أنظمة تخزين بيانات آمنة وغير مركزية، والتي يُمكن أن تساعد في تقليل مخاطر خروقات البيانات، والتأكد من أن البيانات المُخزَّنة غير قابلة للعبث، فعلى سبيل المثال: يُمكن لأنظمة تخزين البيانات المُستنِدة إلى سلسلة الكُتل تخزين البيانات الحسَّاسة مثل: السجلات الطبية، أو المعلومات المالية.

تمرينات

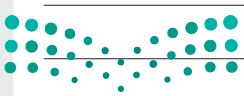
1

حدِّد الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. يُحوِّل التشفير النص غير المُشفَّر إلى معلومات يُمكن قراءتها.	○	○
2. تُستخدم المصادقة للتحقق من سلامة الرسائل.	○	○
3. تُعدُّ سرية البيانات أمرًا ضروريًا للاتصالات داخل المؤسسات المالية.	○	○
4. يؤدّي التشفير دورًا حيويًا في تأمين تصفُّح الويب.	○	○
5. لا تَستخدم الشبكات الافتراضية الخاصة (VPNs) التشفير لإجراء الاتصالات الآمنة.	○	○
6. يُعدُّ تشفير المفتاح المتماثل أسرع وأكثر كفاءة حسابيًا من تشفير المفتاح غير المتماثل.	○	○
7. يُستخدم الاختزال بشكل أساسي لتشفير البيانات.	○	○
8. يَستخدِم المتسلِّلون أسلوب تحليل الشفرات للوصول إلى البيانات المُشفَّرة.	○	○
9. تتكون شبكة الثقة من المُستخدِمين الذين وافقوا على التَّوقيع على المفاتيح العامة لبعضهم البعض.	○	○
10. تُصدِر هيئة الشهادات (CA) شهادة رقمية تربط مفتاحًا عامًا بهوية لكيان محدَّد.	○	○

2 صِف المبادئ الأساسية للتشفير وكيفية عمله.

3 حَدِّد التطبيقات المختلفة للتشفير في العالم الرقمي الحديث.

4 اذكر الأنواع الثلاثة الرئيسة لخوارزميات التشفير.



5 صَمِّم تمثيلًا للتشفير بواسطة المفتاح غير المتماثل.

6 اذكر مزايا الأنواع الرئيسة الثلاثة لخوارزميات التشفير وعيوبها.

7 حَلِّل كيفية استخدام شبكات الثقة للتحقُّق من صحَّة المفاتيح العامة في التشفير.

8 اشرح كيف يُمكن للمتسلِّلين استخدام تحليل الشفرات للوصول إلى البيانات المُشفَّرة.

رابط الدرس الرقمي

www.ien.edu.sa

الدرس الثالث

الأمن السيبراني والتقنيات الناشئة

أنظمة الأمن السيبراني في التقنيات الناشئة

Cybersecurity Systems in Emerging Technologies

تُسهِم التقنيات الناشئة في التحوُّل والتطوُّر الكبير والسريع لكثيرٍ من مناحي الحياة حول العالم، كما تُشكِّل هذه التقنيات أيضًا تحديات ومخاطر كبيرة على أمن وخصوصية الأفراد والمؤسسات والدول.

تُعدُّ أنظمة الأمن السيبراني ضرورية لحماية البيانات والأنظمة والشبكات التي تستعين بهذه الأنظمة من الهجمات الضارة والحدِّ من إمكانيات الوصول غير المُصرَّح به، وفيما يلي مُقدِّمة لبعض الثغرات الأمنيّة المعروفة في التقنيات الناشئة المُستخدَمة على نطاقٍ واسعٍ، وسبب أهمية أنظمة الأمن السيبراني في حمايتها:

أجهزة إنترنت الأشياء IoT Devices

إنترنت الأشياء (Internet of Things – IoT) هو شبكة من الأجهزة المترابطة والمستشعرات تجمع البيانات وتنقلها وتتبادلها مع بعضها، وتشمل هذه الأجهزة أنواعاً مختلفة تمتد من الأجهزة المنزلية الذكية مثل: مُنظِّمات الحرارة وأنظمة الحماية، إلى الآلات الصناعية، وأجهزة المراقبة الصحية، والأجهزة القابلة للارتداء. تزداد مساحة الهجمات المحتملة لمُرتكبي الجرائم السيبرانية مع تزايد عدد أجهزة إنترنت الأشياء، فعلى سبيل المثال: تمتلك الكثير من هذه الأجهزة في بيئات الحوسبة المتطورة موارد محدودة، مما يَحدُّ من قدرتها على تنفيذ إجراءات أمن قوية، ويجعلها أكثر عُرضة للهجمات. يجب أن تتبنى المؤسسات التي تستخدِم الحوسبة المتطورة ممارسات أمن سيبراني قوية مثل: التشفير، والإدارة الآمنة للأجهزة، وتجزئة الشبكة لحماية بياناتها وأنظمتها من التهديدات المحتملة، وتتضمَّن بعض المخاطر المرتبطة بإنترنت الأشياء ما يلي:

ضعف المصادقة والتفويض (Weak Authentication and Authorization):
غالبًا ما تفتقر أجهزة إنترنت الأشياء إلى آليات مصادقة وتفويض قوية، مما يجعلها أهدافًا سهلة للمهاجِمين، ولذلك يجب استخدام كلمات مرور قوية و**المصادقة متعددة العوامل** (MFA) لحماية أجهزة إنترنت الأشياء من الوصول غير المُصرَّح به.

ضعف التشفير (Lack of Encryption):
تفتقر العديد من أجهزة إنترنت الأشياء إلى إمكانات التشفير القوية، مما قد يُتيح اعتراض البيانات من قِبَل المهاجِمين، ولذلك يجب تنفيذ إجراءات تشفير متقدِّمة.

ثغرات البرامج الثابتة (Firmware Vulnerabilities):
البرامج الثابتة (Firmware) هي شكل من أشكال البرامج المُصغَّرة أو المُضمَّنة في الأجهزة لتعمل بفعالية، وغالبًا ما تحتوي أجهزة إنترنت الأشياء على برامج ثابتة يُمكن اختراقها بسهولة، مما يسمح للمهاجِمين بالتحكُّم في الجهاز.

البرمجيات غير المحدَّثة (Outdated Software):
لم يكن من الشائع وضع عوامل الأمن بالاعتبار عند تصميم أجهزة إنترنت الأشياء، وما زالت الكثير منها تعمل ببرمجيات تشغيل غير محدَّثة تحتوي على ثغرات أمنية معروفة، ولذلك يضمن التحديث المنتظم للبرامج الثابتة والبرمجيات الخاصة بأجهزة إنترنت الأشياء تصحيح الثغرات الأمنيّة المعروفة.

مخاوف الخصوصية (Privacy Concerns):
غالبًا ما تجمع أجهزة إنترنت الأشياء بيانات شخصية حسّاسة مثل: معلومات الموقع، والبيانات الحيوية التي يُمكن استخدامها لأغراض ضارة إذا وقعت في الأيدي الخطأ، ولذلك يجب أن تحدّ المؤسسات من كمية البيانات الشخصية التي يتم جمعها وتخزينها بواسطة أجهزة إنترنت الأشياء لتقليل المخاوف المتعلقة بالخصوصية.

المُدُن الذكية Smart Cities

تستخدِم المُدُن الذكية التقنيات المترابطة **وإنترنت الأشياء** (IoT) لتعزيز جودة الحياة الحضرية وتحسين استهلاك الموارد وتحسين الخدمات العامة، حيث يتم الاعتماد على البيانات المُجمَّعة من المستشعرات والأجهزة والأنظمة لتمكين اتخاذ القرارات الفورية وأتمتة العمليات. ومع ذلك، فإن زيادة الاتصال بين المرافق المختلفة، والاعتماد على التقنيات تجعل المُدُن الذكية عُرضة للهجمات السيبرانية، مما قد يتسبب بتعطيل الخدمات، أو سرقة البيانات، أو تعريض البنيَة التحتيَّة للخطر.

على سبيل المثال: يُمكن للمهاجِم تهديد نظام إدارة حركة المرور في المدينة الذكية، مما يتسبب في حدوث اختناق أو وقوع حوادث سير، أو يُمكنه السيطرة على نظام إمدادات المياه في المدينة، أو تلويث المياه أو تعطيل توزيعها. من الضروري تنفيذ تدابير قوية للأمن السيبراني لضمان أمن المُدُن الذكية، وتشمل تلك التدابير تجزئة الشبكة، واستخدام بروتوكولات الاتصال الآمن، والمراقبة المستمرة لحماية البنيَة التحتيَّة للمدينة والبيانات المُجمَّعة. تتضمن بعض المخاطر الأمنيّة المرتبطة بالمُدُن الذكية ما يلي:

قابلية الأجهزة للاختراق (Vulnerable Devices):
غالبًا ما يتم تصميم أجهزة إنترنت الأشياء دون اعتبارات متطلبات الأمن السيبراني وبالتالي يُمكن اختراقها بسهولة، ولهذا يُمكن استخدام هذه الأجهزة لشن هجمات على أجهزة أخرى أو الوصول إلى البيانات الحساسة.

خصوصية البيانات (Data Privacy):
تجمع أنظمة المُدُن الذكية الكثير من البيانات عن الأفراد مثل: بيانات الموقع، والمعلومات الشخصية الأخرى، وتُعدُّ هذه البيانات قيِّمة للجهات الإعلانية والأطراف الخارجية الأخرى، ولكنها تثير أيضًا مخاوف بشأن الخصوصية وأمن البيانات.

الهجمات السيبرانية (Cyber Attacks):
قد تتعرض أنظمة المُدُن الذكية للهجمات السيبرانية التي يُمكن أن تُعطِّل الخدمات أو تُلحق الضرر بالبنيَة التحتيَّة، فعلى سبيل المثال: يُمكن للمهاجِمين إغلاق إشارات المرور مما يتسبب في حدوث فوضى مرورية وحوادث.

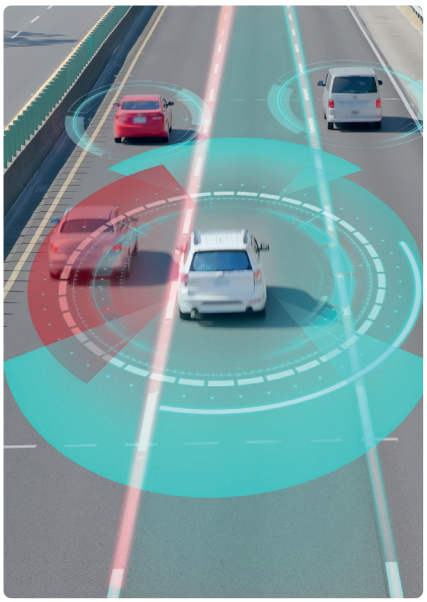
عدم وجود المعايير القياسية (Lack of Standardization):
غالبًا ما يتم تطوير أنظمة المُدُن الذكية بواسطة جهات متعددة وباستخدام تقنيات وبروتوكولات مختلفة، ويساهم عدم وجود المعايير القياسية في صعوبة دمج الأنظمة، ويُمكن أن يُنشئ ثغرات أمن سيبراني.

للتخفيف من هذه المخاطر، من المُهم تنفيذ أفضل الممارسات لدعم أمن المُدُن الذكية، منها على سبيل المثال:

- تحديث جميع الأجهزة والأنظمة وتصحيحها بانتظام لضمان أمنها وعملها بشكل صحيح.
- تنفيذ مصادقة قوية والتحكم بالوصول لمنع الوصول غير المُصرَّح به إلى الأجهزة والأنظمة.
- إجراء تقييمات أمن سيبراني منتظمة لتحديد ثغرات الأمن السيبراني ومعالجتها.
- وضع خطط شاملة للاستجابة للحوادث والتخفيف منها بسرعة.
- التأكد من تطبيق السياسات السليمة للحفاظ على خصوصية البيانات، وأن البيانات يتم جمعها وتخزينها واستخدامها وفقًا للضوابط المحدَّدة لذلك.
- تطوير المعايير القياسية النموذجية لضمان توافق الأنظمة المختلفة وأمنها.

المركبات ذاتية القيادة Autonomous Vehicles

تعتمد المركبات أو السيارات ذاتية القيادة على تقنيات ومستشعرات متقدِّمة للعمل دون التحكُّم البشري في قيادتها. نظرًا لأن المركبات أصبحت أكثر اتصالًا وأتمتة، فقد أصبحت أكثر عُرضة للهجمات السيبرانية التي قد تؤدي إلى سرقة المركبات، وانتهاك الخصوصية، أو حدوث أضرار جسدية بالركاب والمشاة. تجمع المركبات ذاتية القيادة الكثير من البيانات حول الركاب والمناطق المحيطة بالمركبة أثناء وقوفها وحركتها، وتُعدُّ هذه البيانات قيِّمة لجهات مُعيَّنة، كالجهات الإعلانية والأطراف الخارجية الأخرى، ولكنها تثير أيضًا مخاوف بشأن الخصوصية وأمن البيانات.



شكل 3.11: حماية المركبات ذاتية القيادة أمر بالغ الأهمية لسلامة الركاب

على سبيل المثال: يُمكن لمُرتكبي الجرائم السيبرانية استغلال ثغرة أمنية في نظام اتصالات مركبة ذاتية القيادة للتحكم بها، مما قد يتسبب في تدميرها أو تعريض ركابها للخطر. يتطلب ضمان أمن المركبات ذاتية القيادة تنفيذ تدابير أمنية متعددة مثل: التشفير القوي للاتصالات، وتطبيق ممارسات تطوير البرمجيات الآمنة، والمراقبة المنتظمة للتهديدات المحتملة، كما تُعدُّ حماية هذه المركبات من التهديدات السيبرانية أمرًا بالغ الأهمية في عملية دمجها بأنظمة النقل بأمان ونجاح.

للتخفيف من المخاطر المحتملة على أمن المركبات ذاتية القيادة، من المُهم تنفيذ أفضل الممارسات التالية:

- تشفير كافة البيانات المتبادلة بين المركبة والأنظمة الخارجية.
- تحديث برمجيات المركبة وأجهزتها بانتظام للتأكد من أنها آمنة وتعمل بشكل صحيح.
- إجراء تقييمات أمن سيبراني منتظمة لتحديد ثغرات الأمن السيبراني ومعالجتها.

إجراء اختبارات صارمة والتحقق من صحَّة جميع المكوِّنات لتحديد ثغرات الأمن السيبراني وإصلاحها.

تنفيذ مصادقة قوية والتحكم بالوصول لمنع الوصول غير المُصرَّح به إلى الأنظمة المركبة.

وضع خطط شاملة للاستجابة للحوادث والتخفيف منها بسرعة.

التأكد من تطبيق السياسات السليمة للحفاظ على خصوصية البيانات، وأن البيانات يتم جمعها وتخزينها واستخدامها وفقًا للضوابط المحدَّدة لذلك.

شبكات الجيل الخامس 5G Networks

تتميز شبكات الجيل الخامس بتوفير خدمات الاتصالات والإنترنت بسُرعات عالية، وزمن وصول أقل، وسعة أكبر لتحميل وتبادل البيانات، مما يتيح ظهور تقنيات حديثة مثل: المركبات ذاتية القيادة، والمُدُن الذكية، وتطبيقات إنترنت الأشياء. ومع ذلك، فإن نشر شبكات الجيل الخامس يمثِّل تحديات جديدة للأمن السيبراني، حيث أصبحت هناك حاجة ماسة إلى اتخاذ تدابير قوية للأمن السيبراني لحماية البنيَة التحتيَّة أمام زيادة نطاق الهجمات، والمخاطر المُحدِقة بسلاسل التوريد، والاستغلال المحتمل لمُكوِّنات الشبكة.

أضِفْ إلى ذلك أن تعقيد شبكات الجيل الخامس والعدد الهائل من الأجهزة المترابطة يتيح الفرصة لمُرتكبي الجرائم السيبرانية في استغلال نقاط الضعف، مما قد يؤدي إلى تعطيل الخدمات المهمة أو سرقة البيانات الحساسة.

الحوسبة السحابية Cloud Computing

تُمكّن الحوسبة السحابية الشركات والأفراد من تخزين بياناتهم ومعالجتها وإدارتها على الخوادم البعيدة، مما يوفر قابلية التوسع وتوفير التكاليف والمرونة، ولكن يتطلب الاعتماد على الخدمات والبنيَة التحتيَّة السحابية تطبيق تدابير أمن سيبراني قوية لحماية البيانات والتطبيقات المستضافة سحابيًا. تشمل مخاطر الأمن السيبراني السحابية خروقات البيانات، والوصول غير المُصرَّح به، وسرقة الحسابات، فعلى سبيل المثال: يُمكن لخدمات التخزين السحابية التي تمت تهيئتها بشكل غير صحيح عرض معلومات حساسة للجمهور، مما يؤدي إلى تَسرُّب البيانات وما يتبع ذلك من العواقب القانونية المحتملة، كما يُمكن أن تُشكّل التهديدات الداخلية خطرًا كبيرًا على البيئات السحابية، حيث يُمكن للمُستخدمين ذوي الصلاحيات الواسعة في الأنظمة السحابية إساءة استخدام صلاحيات الوصول لسرقة البيانات أو تعطيل الخدمات. تُعدُّ المسؤولية المشتركة لإدارة الحوسبة السحابية مصدرًا للقلق، حيث يكون مزود الخدمة السحابية مسؤولًا عن تأمين البنيَة التحتيَّة الأساسية، بينما يكون العميل مسؤولًا عن حماية بياناته وتطبيقاته المُستضافة سحابيًا، ويؤدي تقسيم المسؤولية هذا أحيانًا إلى حدوث ارتباك أو ثغرات أمنية، مما يزيد من احتمالية نجاح الهجمات، ولذلك يجب على المؤسسات فهم مسؤولياتها وتنفيذ إجراءات الأمن المناسبة لحماية أصولها السحابية.

الحوسبة الكَميَّة Quantum Computing

تستفيد الحوسبة الكَميَّة من مبادئ ميكانيكا الكَم لأداء العمليات الحسابية بشكل أسرع من أجهزة الحاسب التقليدية، وتُعدُّ هذه التقنية المتطورة ذات إمكانات هائلة لمختلف الصناعات، بما في ذلك مجالات التشفير، وتطوير الأدوية، والخدمات المالية، ولكن قد تُشكِّل أجهزة الحاسب الكَميَّة مخاطر كبيرة تتعلق بالأمن السيبراني، لا سيما في مجال التشفير، حيث يُمكن للتطوير السريع والكبير لأجهزة الحاسب الكَميَّة أن يُتيح لها إمكانية كسر العديد من خوارزميات التشفير الحالية، مما يجعل البيانات المُشفَّرة عُرضة للاعتراض وفك التشفير. يقوم الباحثون بتطوير خوارزميات جديدة مقاومة لقدرات الحوسبة الكَميَّة على فك التشفير للاستعداد لمواجهة المخاطر المتعلقة بالتشفير في ظل تطور الحوسبة الكَميَّة، حيث يُساعد تطبيق هذه الخوارزميات مسبقًا على ضمان سرية البيانات الحساسة وسلامتها.

أنظمة الذكاء الاصطناعي وتعلُّم الآلة
Artificial Intelligence (AI) and Machine Learning (ML) Systems

أحدثت أنظمة الذكاء الاصطناعي وتعلُّم الآلة نَقلة نوعية في الصناعات المختلفة من خلال تمكين الآلات للتعلُّم من البيانات، وقيامها بالتنبؤ وتحسين أدائها بمرور الوقت. يوجد لهذه الأنظمة تطبيقات في قطاعات متنوعة، بما فيها المجالات المالية، والرعاية الصحية، والتصنيع، والنقل، كما يُمكن للتقنيات القائمة على الذكاء الاصطناعي مساعدة متخصصي الأمن السيبراني في تحليل كميات كبيرة من البيانات، وتحديد الأنماط التي قد تمر فيها دون أن يلاحظها أحد، وهذا يُمكن أن يُتيح للمؤسسات الاستجابة بسرعة وفعالية أكبر للحوادث الأمنيّة.

يمثِّل تعلُّم الآلة إحدى طرائق استخدام الذكاء الاصطناعي في الأمن السيبراني، حيث يُمكن لخوارزميات تعلُّم الآلة تحليل بيانات الأمن السيبراني مثل: حركة بيانات الشبكة أو سلوك المُستخدِمين، وتحديد الأنماط أو الحالات الشاذة التي قد تشير إلى وجود تهديد أمني، ويُمكن أن يساعد ذلك فِرَق الأمن السيبرانِي في اكتشاف الهجمات والاستجابة الفورية لها.

يُمكن أيضًا الاستعانة بالذكاء الاصطناعي في الأمن السيبراني من خلال التحليلات التنبؤية، حيث يُمكن أن تُساعد هذه التحليلات المؤسسات على تحديد تهديدات الأمن السيبراني المحتملة قبل حدوثها، وتتيح لفِرَق الأمن توقُّع الهجمات ومنعها من خلال تحليل سجلات البيانات وتحديد الأنماط.

فيما يلي بعض الأمثلة العملية لتطبيقات الذكاء الاصطناعي وتعلُّم الآلة في الأمن السيبراني:

الكشف عن البرمجيات الضارة (Malware Detection):
يُمكن للذكاء الاصطناعي اكتشاف البرمجيات الضارة من خلال تحليل أنماط السلوك وتحديد النشاط الشَّاذ في الأنظمة والشبكات، فعلى سبيل المثال: قد يقوم النظام القائم على الذكاء الاصطناعي بتمييز برنامج يصل إلى العديد من الملفات، أو يتصل بخوادم غير معروفة على أنه برمجية ضارة محتملة.

كشف اختراق الشبكة (Network Intrusion Detection):
يُمكن للذكاء الاصطناعي اكتشاف عمليات اختراق الشبكة عن طريق تحليل حركة البيانات، وتحديد الأنماط التي قد تشير إلى وقوع هجوم، فعلى سبيل المثال: قد يشير النظام القائم على الذكاء الاصطناعي إلى محاولات اختراق محتملة للشبكة من خلال وجود عدد غير اعتيادي لمحاولات تسجيل الدخول الفاشلة.

تحليل سلوك المُستخدِم (User Behavior Analysis):
يُمكن استخدام الذكاءَ الاصطناعي لتحليل سلوك المُستخدِم، وتحديد مخاطر الأمن السيبراني المحتملة، فعلى سبيل المثال: قد يشير النظام القائم على الذكاء الاصطناعي إلى وصول الموظف إلى البيانات الحسَّاسة خارج ساعات عمله الاعتيادية باعتباره تهديدًا محتملًا.

تحليل المعلومات الاستباقية (Threat Intelligence Analysis):
يُمكن للذكاء الاصطناعي القيام بعمليات تحليل المعلومات الاستباقية للبيانات وتحديد التهديدات الناشئة، فعلى سبيل المثال: قد يُميِّز النظام القائم على الذكاء الاصطناعي وجود برمجية ضارة تنتشر بسرعة عبر الإنترنت ويشير إليها باعتبارها تهديدًا ناشئًا محتملًا.

كشف الاحتيال (Fraud Detection):
يُمكن للذكاء الاصطناعي اكتشاف الأنشطة الاحتيالية مثل: الاحتيال على بطاقات الائتمان أو انتحال الشخصية. على سبيل المثال: قد يشير النظام القائم على الذكاء الاصطناعي إلى مُعامَلة لبطاقة ائتمان تتم من موقع غير عادي أو خارجَ نَمط الإنفاق الاعتيادي للمُستخدِم على أنها احتيال محتمل.

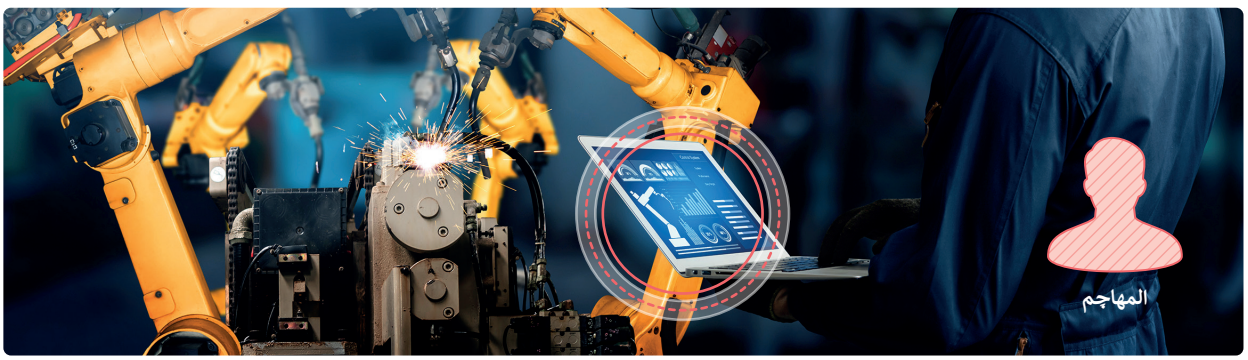
يُثير الاعتماد المتزايد على أنظمة الذكاء الاصطناعي وتعلُّم الآلة مخاوف أمنية إضافية، حيث يُمكن لمُرتكبي الجرائم السيبرانية استهداف هذه الأنظمة ومحاولة التحايل عليها، أو اختراقها لأغراض ضارة، كما يُمكن للمتسلِّلين استخدام تعلُّم الآلة والتقنيات الأخرى القائمة على الذكاء الاصطناعي لتحديد الثغرات الأمنيّة للأنظمة وشن هجمات أكثر تعقيدًا. على سبيل المثال: يُمكن للمهاجمين استخدام خوارزميات تعلُّم الآلة لإنشاء رسائل بريد إلكتروني احتيالية ذات محتوى احترافي مُقنِع، أو تجاوز ضوابط الأمن بانتحال شخصية مُستخدِمين موثوقين.

إحدى المخاطر المحتملة الأخرى المرتبطة بأنظمة الذكاء الاصطناعي وتعلُّم الآلة هي الهجمات العدائية، حيث يُنشئ مُرتكبي الجرائم السيبرانية مُدخَلات ضارة مُصمَّمة لخداع أو استغلال الثغرات الأمنيّة في نماذج الذكاء الاصطناعي. على سبيل المثال: قد يُضيف المهاجِم تشويشًا خفيفًا إلى صورة، مما قد يتسبب في إخفاق نظام معالجة الصور في التعرف على المُستخدِمين، والمثال الآخر هو التحايل على الخوارزميات الخاصة بمنصَّات التواصل الاجتماعي، حيث يُمكن للمهاجِم نشر معلومات خاطئة، أو إنشاء ملفات شخصية مزيفة، وذلك بهدف التأثير على سلوك المُستخدِمين.

أصبح من المُهم تطوير تدابير قوية للأمن السيبراني وتنفيذها للحَدِّ من المخاطر المرتبطة بالهجمات التي تعمل بالذكاء الاصطناعي،ويُمكن أن يشمل ذلك استخدام تقنيات مدعومة بالذكاء الاصطناعي لاكتشاف التهديدات الفورية والاستجابة لها، وتنفيذ تدابير أمن سيبراني إضافية مثل **المُصادقة متعددة العوامل** (MFA)، وتطبيق ضوابط الوصول الأخرى لمنع الوصول غير المُصرَّح به.

الروبوتات والأنظمة المستقلة ذاتيًا Robotics and Autonomous Systems

يتم دمج تقنيات الروبوتات والأنظمة المستقلة ذاتيًا بشكل متزايد في مختلف الصناعات كالزراعة والنقل والتصنيع، ولقد أصبحت هذه التقنيات أكثر تعقيدًا وترابطًا مما جعلها أكثر عُرضة للهجمات السيبرانية. تشمل مخاطر الأمن السيبراني المرتبطة بالروبوتات والأنظمة المستقلة ذاتيًا عمليات الوصول غير المُصرَّح به، وسرقة البيانات، والتلاعب بالأنظمة لإحداث ضرر مادي أو تعطيل العمليات، فعلى سبيل المثال: يُمكن للمهاجِم اختراق نظام التحكُّم في روبوت صناعي، مما يتسبب في تعريض العمال للخطر أو إلحاق الضرر بهم. يتطلب ضمان أمن الروبوتات والأنظمة المستقلة ذاتيًا ضوابط قوية للتحكم بالوصول، ووجود بروتوكولات اتصال آمنة، ومراقبة منتظمة للتهديدات المحتملة، كما تُعدُّ معالجة تحديات الأمن السيبراني أمرًا بالغ الأهمية لدمج الروبوتات والأنظمة المستقلة ذاتيًا بأمان ونجاح في مختلف القطاعات.



شكل 3.12: تلاعب مُرتكبي الجرائم السيبرانية بنظام محدَّد لإحداث ضرر مادي أو تعطيل عملياته

تقنيات الواقع المعزز والواقع الافتراضي والميتافيرس
Augmented Reality (AR), Virtual Reality (VR) and the Metaverse

تطوَّرت تقنيات **الواقع المعزز** (AR) **والواقع الافتراضي** (VR) **والميتافيرس** (Metaverse) بسرعة، وتوسَّع نطاق تطبيقاتها من الألعاب إلى مختلف الصناعات مثل: الرعاية الصحية، والتعليم، والتصنيع، وكذلك البيئات الافتراضية الناشئة كما في الميتافيرس.

يُمكن لهذه التقنيات جمع كميات هائلة من البيانات الشخصية والحسَّاسة، مما يجعلها أهدافًا رئيسةً لمُرتكبي الجرائم السيبرانية، ولذلك يُعدُّ ضمان خُصوصيَّة البيانات وأمنها في بيئات الواقع المعزز والواقع الافتراضي والميتافيرس أمرًا بالغ الأهمية لحماية معلومات المُستخدِمين من الوصول غير المُصرَّح به أو إساءة الاستخدام.

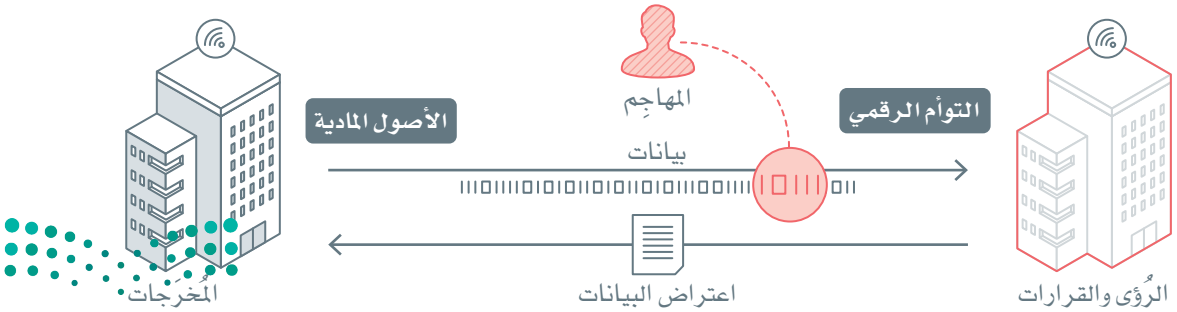
من أمثلة المخاطر الأمنيّة المحتملة في هذه البيئات ضرورة استخدام البيانات الحيوية للمصادقة مثل: التعرُّف على الوجه، أو تتبُّع العين، ففي حين أن هذه التقنيات تُعزِّز تجربة المُستخدِم، إلا أنها تضيف ثغرات أمن سيبراني جديدة وتثير مخاوف حول الخصوصية، ولذلك يجب على المؤسسات التي تُطبِّق تقنيات الواقع الافتراضي والواقع المعزز والميتافيرس استخدام تدابير أمنية قوية لحماية بيانات المُستخدِم، والحفاظ على الثقة في هذه التقنيات البديلة.

أصبح الاهتمام بالأمن السيبراني أولويّة هامّة وذلك مع استمرار تطور الميتافيرس وظهور البيئات الافتراضية المترابطة، وإمكانيات التفاعل في بيئات مختلفة للمُستخدِم، وتُنشئ الطبيعة المترابطة للميتافيرس مشهدًا معقدًا، حيث تتطلب حماية بيانات المُستخدِم، ومنع الوصول غير المُصرَّح به، وتقليل التهديدات المحتملة، وتطبيق تدابير أمن سيبراني شاملة.

شكل 3.13: استهداف البيانات الحيوية في بيئات الواقع المعزز والواقع الافتراضي من خلال الهجمات السيبرانية

التوائم الرقمية Digital Twins

التوائم الرقمية هي نُسخ افتراضية متماثلة للأصول المادية أو الأنظمة أو العمليات التي يُمكن استخدامها للمحاكاة والتحليل والتحسين، ولهذه النماذج الرقمية تطبيقات مختلفة، بما فيها المُدُن الذكية والتصنيع والرعاية الصحية، ونظرًا لأن التوائم الرقمية أصبحت أكثر ترابطًا، وأكثر قدرةً على تخزين كميات هائلة من البيانات الحسَّاسة، فقد أصبحت أهدافًا رئيسة لمُرتكبي الجرائم السيبرانية. تشمل مخاطر الأمن السيبراني المحتملة للتوأم الرقمي عمليات الوصول غير المُصرَّح به، والتلاعب بالبيانات، والهجمات على البنيَة التحتيَّة الأساسية الداعمة له. على سبيل المثال، يُمكن للمهاجِم التلاعب ببيانات التوأم الرقمي لإحداث اضطرابات تشغيلية أو خِداع مُتَّخِذي القرار، ولحماية التوائم الرقمية من التهديدات السيبرانية يجب على المؤسسات تنفيذ ضوابط وصول قوية، وتشفير البيانات، والمراقبة المستمرة لضمان أمن أصولهم الرقمية وسلامتها.



شكل 3.14: تخزين التوائم الرقمية لكميات هائلة من البيانات الحساسة مما يجعلها أهدافًا رئيسة لمُرتكبي الجرائم السيبرانية

تمرينات

1

حدِّدْ الجملة الصحيحة والجملة الخاطئة فيما يلي:	صحيحة	خاطئة
1. الأمن السيبراني مهم لحماية البيانات والأنظمة والشبكات من الهجمات الضارة ومن الوصول غير المُصرَّح به.	○	○
2. تعتمد المُدُن الذكية على البيانات المُجمَّعة من المستشعرات والأجهزة لإتاحة اتخاذ القرارات الفورية.	○	○
3. قد تتأثر المركبات ذاتية القيادة سلبًا بالهجمات السيبرانية.	○	○
4. يُمكن للحوسبة الكَمِّية كسر خوارزميات التشفير الحالية.	○	○
5. لا تقدِّم الحوسبة السحابية تحديات جديدة للأمن السيبراني.	○	○
6. تُنشئ شبكات الجيل الخامس نطاق هجوم أوسع لمُرتكبي الجرائم السيبرانية.	○	○
7. لا تتعرضُ أنظمة الذكاء الاصطناعي وتعلُّم الآلة للهجمات العدائية.	○	○
8. لا تُشكِّل الروبوتات والأنظمة المستقلة ذاتيًا أي مخاطر أمن سيبراني.	○	○
9. تُعدُّ العقود الذكية آمنةً من أي هجمات مُحتملة.	○	○
10. لا تَجمع تطبيقات الواقع المعزز والواقع الافتراضي البيانات الشخصية.	○	○

2 صِف ثغرات الأمن السيبراني الفريدة التي تواجهها أجهزة إنترنت الأشياء (IoT).

3 قَيِّم التدابير الأمنيّة اللازمة لحماية شبكات الجيل الخامس (5G) من التهديدات السيبرانية.

4 قَدِّم أمثلة على مخاطر الأمن السيبراني المرتبطة بأنظمة الذكاء الاصطناعي وتعلُّم الآلة.

5 قَيِّم نموذج المسؤولية المشتركة الموجود بين مزود الخدمة السحابية وعملائه.

6 صِف الحاجة إلى تطوير خوارزميات مقاومة للحوسبة الكَمِّية.

7 اشرح نوع المعلومات المُخزَّنة في التوأم الرقمي ومخاطر استخدامها.

المشروع

ساهمت المُدُن الذكية في إحداث ثورة في حياة البشر، وأعمالهم، وتفاعلهم مع بيئتهم من خلال الاستفادة من التقنيات المتطورة لإنشاء مساحات حضرية أكثر كفاءة واستدامة وترابطًا. ومع ذلك، فإن هذا الاعتماد على التقنية يَجلِب عددًا لا يحصى من تحدِّيات الأمن السيبراني التي يجب معالجتها لضمان سلامة المواطنين وخصوصيتهم ورفاهيتهم.

1 اعرِض لَمحةً عامةً عن مدينة ذكية ومكوِّناتها وفوائدها للحكومات وللمواطنين.

2 حدِّد التحديات الرئيسة للأمن السيبراني للمدن الذكية ثم قم بوصفها، بما في ذلك التهديدات المحتملة للبنيَّة التحتيَّة الحيوية، وخصوصية البيانات، وشبكات الاتصال.

3 حَلِّل المُكوِّنات المختلفة للمُدُن الذكية مثل: أنظمة إدارة الطاقة، وأنظمة النقل، والسلامة العامة، والرعاية الصحية، ثم ناقش تدابير الأمن السيبراني المطلوبة لحماية هذه المُكوِّنات.

4 ابحث عن التقنيات والأدوات والاستراتيجيات الناشئة التي يُمكن أن تُعزِّز وضع الأمن السيبراني للمُدُن الذكية مثل: الذكاء الاصطناعي أو سلسلة الكُتل أو أنظمة كشف التسلُّل، ثم قم بعرضها.

5 لَخِّص النتائج والتوصيات الرئيسة الخاصة بحماية المُدُن الذكية، واستخدم ملاحظاتك لإنشاء عرض باوربوينت تقديمي.

ماذا تعلّمت

- تحديد أهمية التشريعات المُوحدَّة للأمن السيبراني.
- تَحليل الضوابط الرئيسة الخاصة بالأمن السيبراني محليًا ودوليًا.
- وَصف التشفير وحالات استخدامه.
- تصنيف أنواع التشفير والطرائق التي يستخدمها المتسلِّلون للوصول إلى البيانات المُشفَّرة.
- تنفيذ خوارزميات التشفير باستخدام لغة البايثون.
- وَصف أهمية أنظمة الأمن السيبراني في حماية التطبيقات المبنية باستخدام التقنيات الناشئة.

المصطلحات الرئيسة

Machine Learning (ML)	تعلُّم الآلة
Private Key	مفتاح خاص
Public Key	مفتاح عام
Quantum Computing	الحوسبة الكَميَّة
Robotics and Autonomous Systems	الروبوتات والأنظمة المستقلة ذاتيًا
Smart Cities	المُدُن الذكية
Symmetric Key Cryptography	تشفير المفتاح المتماثل
Threat Intelligence Analysis	تحليل المعلومات الاستباقية
User Behavior Analysis	تحليل سلوك المُستخدِم

5G Networks	شبكات الجيل الخامس
Artificial Intelligence (AI)	الذكاء الاصطناعي
Asymmetric Key Cryptography	تشفير المفتاح غير المتماثل
Cloud Computing	الحوسبة السحابية
Cryptography	علم التشفير
Cybercrime Regulation	أَنظمة الجرائم الإلكترونية
Digital Twins	التوائم الرقمية
Hashing	الاختزال
Internet of Things (IoT)	إنترنت الأشياء