جمهورية العراق
وزارة التربية
المديرية العامة للتعليم المهني

امن الشبكات والحوسبة السحابية

فرع الحاسوب وتقنية المعلومات

اختصاص الأمن السيبراني

الصف الثاني

المؤلفون

أ.م.د عامر عبد الحميد عبد الرحمن
أ.م.د أسماعيل خليل علي
م.م فرهاد حسين شاه مراد
م.م ايهاب عبد الكريم فيروز

الطبعة الاولى
1447هـ - 2025م

تنضيد وتصميم الفـــني

شـــذى صبحـــي محمـــــد

مقـدمـــة

في ظل التحولات الاقتصادية والتقنية المتسارعة التي يشهدها العالم، تبرز الحاجة الماسّة إلى أنماط تعليمية تواكب متطلبات سوق العمل، وتزوّد الأجيال القادمة بالمهارات العلمية والعملية والمعرفة التطبيقية اللازمة لبناء مستقبل واعد. ويأتي التعليم المهني في صدارة هذه الأنماط، باعتباره مسارًا حيويًا يربط بين التعليم والإنتاج، ويمنح المتعلم القدرة على الإسهام الفعّال في التنمية الشاملة.

لقد أدركت وزارة التربية في العراق أهمية هذا النوع من التعليم، فانطلقت بخطى واثقة نحو دعمه وتطويره، ليس فقط من خلال تحديث مناهجه وبنيته التحتية، بل أيضًا عبر فتح اختصاصات جديدة تواكب احتياجات القطاعات المختلفة، وتنسجم مع الرؤية الوطنية للنمو المستدام. وتمثل هذه المبادرات استجابة عملية لتحديات البطالة، ونقلة نوعية نحو تمكين الشباب من اكتساب المهارات التي تؤهلهم للمنافسة والإبداع.

ومع توسّع الاعتماد على الإنترنت، وتقنيات الاتصال، والحوسبة السحابية شرعت المديرية العامة للتعليم المهني في العراق بافتتاح اختصاص الامن السيبراني أحد اختصاصات فرع الحاسوب وتقنية المعلومات . وتبرز أمن الشبكات كأحد أهم المجالات في هذا الميدان ، بل هي خط الدفاع الأول في مواجهة الهجمات الإلكترونية ومحاولات الاختراق.

لذا جاء هذا الكتاب ليسلط الضوء على المفاهيم الأساسية والحديثة في أمن الشبكات، وفي خمسة فصول , بدءًا من المبادئ العامة، مرورًا بالأنظمة والبروتوكولات، وصولاً إلى التهديدات الشائعة وآليات الحماية المتقدمة. ويتناول الكتاب أدوات التحليل، واختبار الاختراق، والجدران النارية، وأنظمة كشف التسلل، وغيرها من الحلول الأمنية التي تشكل منظومة متكاملة لحماية بيئة الشبكات. ومن هنا، يسعى هذا الكتاب إلى عرض بعض المفاهيم الشاملة التي تُمكّن الطلبة والمهنيين والمهتمين بمجال الأمن السيبراني من فهم بنية الشبكات، والتحديات الأمنية المحيطة بها، وكيفية التعامل معها بفعالية واحترافية , باسلوب سهل وميسر .

ونسأل الله أن يحقق هذا الكتاب الأهداف المرجوة منه , ويوفق طلبتنا ومدرسينا لما فيه خير الوطن وتقدمة.

..... ومن الله التوفيق

المؤلفون

المحتويــات

رقم الصفحة

المحتويـــات

رقم الصفحة

المحتويــات

رقم الصفحة

المحتويـــات

رقم الصفحة

الفصل الرابع

عنوان الفصل : تهديدات الامان في بيئة الحوسبة السحابية

المحتويـــات

رقم الصفحة

الفصل الأول

المبادئ الأساسية للشبكات

الهدف العام

تعليم الطلبة المبادئ الاساسية للشبكات

الاهداف الخاصة

أن يكون الطالب قادرا على:-

- استيعاب مفهوم الشبكة واهميتها
- التعرف على انواع شبكات الحاسوب وفق النطاق الجغرافي
- التعرف على مكونات الشبكات
- التعرف على انواع الشبكات
- التعرف على هيكلية الشبكات وطوبوغرافيتها

..... مفردات الفصل .....

مفهوم الشبكة وأهميتها

أنواع شبكات الحاسوب وفق النطاق الجغرافي (LAN,MAN,WAN)

مكونات الشبكات:

الأجهزة (مثل الحواسيب، الأجهزة الشبكية : Router, Switch , HUB)

الوسائط (مثل كابلات Ethernet، الألياف الضوئية، الاتصال اللاسلكي)

البرمجيات (مثل أنظمة التشغيل، برمجيات إدارة الشبكة)

أنواع الشبكات:

الشبكات السلكية (Wired)

الشبكات اللاسلكية (Wireless)

هيكلية الشبكات وطوبوغرافيتها:

الشبكة الخطية (Bus Network)

الشبكة النجمية (Star Network)

الشبكة الحلقية (Ring Network)

الشبكة المتداخلة (Mesh Network)

التمارين العملية:

تمرين :1 التدريب على ربط كيبل من نوع UTP

تمرين :2 تعريف نوع الشبكة التي تستخدمها في منزلك أو مكتبك (LAN , WLAN , ...الخ) وشرح المكونات المستخدمة فيها .

تمرين : 3 تصميم شبكة محلية (LAN) من خلال توصيل جهازين عبر كبل (Ethernet) .

تمرين :4 استخدام أداة Wireshark لمراقبة حركة البيانات في الشبكة المحلية

تمرين :5 تنفيذ مخطط شبكي يوضح اتصال الأجهزة في شبكة نجمية (Star Network) .

الفصل الأول

المبادئ الأساسية للشبكات

1-1 مفهوم الشبكة واهميتها

تعد الشبكات ومنها شبكات الحواسيب من أهم البنى التحتية التقنية التي يقوم عليها العالم اليوم، إذ تمثل النواة الأساسية لنقل المعلومات والبيانات وتبادلها بين الأفراد والمؤسسات في مختلف أنحاء العالم. لا يمكن تصور أي نشاط اقتصادي أو بحثي أو صناعي أو حتى اجتماعي في العصر الرقمي دون الاعتماد بشكل أو بآخر على نوع من أنواع الشبكات. فمن خلال هذه الشبكات، تتصل الأنظمة بعضها ببعض، وتتشارك الموارد الحوسبية، وتتفاعل الأجهزة الذكية، وتتدفق البيانات بسرعة مذهلة عبر العالم. إن التطور الحاصل في مجال شبكات الحواسيب لم يكن وليد اللحظة، بل هو نتاج عقود من الأبحاث والابتكارات المستمرة التي ما زالت تتطور بشكل متسارع لمواكبةً الحاجة البشرية المتزايدة للاتصال الفعال ونقل المعرفة.

1-1-1 مفهوم الشبكة

الشبكة هي مجموعة من الأجهزة (مثل الحواسيب، الهواتف الذكية، الخوادم، الطابعات، وغيرها) المتصل بعضها ببعض لتبادل البيانات والموارد، تعتمد الشبكات على بروتوكولات محددة لضمان انتقال البيانات بشكل صحيح وآمن بين الأجهزة المختلفة ويمكن أن تكون الشبكات محلية تغطي مساحة صغيرة مثل المنازل أو المكاتب، أو اقليمية بين المدن أو واسعة تمتد عبر الدول.

شكل (1– 1) يوضح نموذجا عاما للشبكة

2-1-1 أهمية الشبكات

تعد الشبكات أداة أساسية في عالم التكنولوجيا، أذ تُمكّننا من التواصل والتعاون وتبادل المعلومات على نطاق واسع وإتقانها يساعدنا على تحسين حياتنا وإنجاز أعمالنا بشكل أكثر فعالية وكفاءة. وتوجد الكثير من الفوائد التي تُقدمها لنا الشبكات، مثل:

1- **التواصل العالمي:** تتيح لنا الشبكات التواصل مع الأشخاص في جميع أنحاء العالم، مثل التواصل عبر البريد الإلكتروني أو مكالمات الفيديو. فمن خلال شبكات الإنترنت، يمكننا التواصل مع الأشخاص في أي مكان وزمان. فمثلاً، يمكن لشركة في العراق التواصل مع شركاء أعمالها في دول العالم المختلفة بمُكالمات الفيديو وتبادل البيانات والمعلومات بينهم.

2- **مشاركة المعلومات وتبادلها:** تتيح لنا الشبكات مشاركة المعلومات وتبادلها والملفات مع الآخرين، مثل مشاركة و تبادل ملفات الدراسة أوالعمل أو الصور ومقاطع الفيديو مع الأصدقاء والعائلة فمن خلال الشبكات، يمكننا نقل البيانات والوصول بسهولة وسرعة الى كم هائل من المعلومات فمثلاً، يمكن للمدرس مشاركة ملخصات الدروس وملفات التمارين مع طلابه من خلال منصات التعليم الالكترونية المرتبطة بشكل كامل بالشبكات او استخدام محركات البحث على الإنترنت للوصول الى المعلومات في المجالات المتنوعة مثل العلم والرياضة والثقافة والأخبار.
3- **الخدمات الإلكترونية:** تتيح لنا الشبكات استخدام الكثير من الخدمات الإلكترونية، مثل التسوق عبر الإنترنت أو الدفع الإلكتروني أو الحجز الإلكتروني. فمن خلال الشبكات، يمكننا إجراء الكثير من المعاملات والنشاطات بشكل سريع ومريح. فمثلاً، يمكن للمستخدم شراء المنتجات من خلال متاجر الكترونية ومتابعة طلباته وإجراء الدفع الإلكتروني بشكل آمن وسهل.
4- **التعليم عن بعد:** تتيح لنا الشبكات الحصول على التعليم عن بعد، مثل حضور الدروس عبر الإنترنت أو الحصول على شهادات عبر الإنترنت. فمن خلال الشبكات، يمكننا تعلم مهارات جديدة أو الحصول على شهادات دون الحاجة إلى حضور الدروس بشكل شخصي فمثلاً، يمكن للطالب الحصول على تعليم جامعي من خلال منصات التعليم الالكترونية ودون الحاجة إلى السفر إلى الجامعة.
5- **التعاون والعمل الجماعي:** تمكن الشبكات من التعاون بين الأفراد في مشاريع مشتركة من خلال منصات العمل الجماعي مثل **Google Docs** و **Microsoft Teams**، حيث يمكن للمشاركين في المشروع التعديل على الوثائق ومشاركة الأفكار والتواصل بعضهم مع بعض بشكل سريع ومُباشر.
6- **في المجال الطبي:** تمكن الشبكات من تقديم الخدمات الطبية عن بعد، حيث يمكن للمرضى التواصل مع الأطباء بمُكالمات الفيديو ومشاركة بياناتهم الطبية، كما يمكن للطبيب متابعة حالة المريض من خلال مراقبة البيانات الطبية المُرسلة من أجهزة المريض.
7- **المُشاركة المجتمعية والترفيهية:** تتيح الشبكات للأشخاص المشاركة في النشاطات المجتمعية والمشاركة في الحملات التوعوية، وتمكن من التواصل بين أفراد المجتمع ومشاركة الآراء والأفكار، مثل مشاركة البيانات والصور حول الأنشطة المجتمعية أو تقديم التبرعات للجمعيات الخيرية من خلال منصات التبرع الالكترونية وتتيح الشبكات الوصول إلى محتوى ترفيهي واسع مثل الأفلام والمسلسلات والموسيقى والمباريات الرياضية.

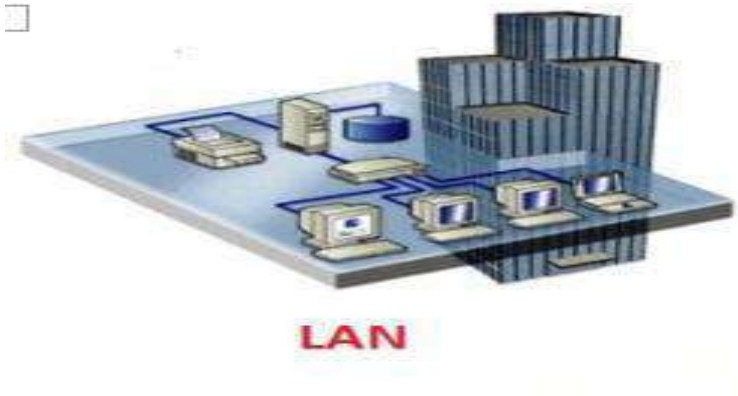
8- **ربط الأجهزة الذكية في إنترنت الأشياء(IoT):** تسهم الشبكات في ربط الأجهزة الذكية وتمكين التشغيل الآلي في مختلف المجالات و يوفر تمكين الأجهزة من العمل تلقائيًا دون تدخل بشري مثل الإضاءة الذكية التي تعمل بالحركة لمراقبة استهلاك الطاقة وتقليل الهدر و كذلك إدارة المرور وتخفيف الازدحام باستخدام إشارات المرور الذكية التي ترسل إشعارات عند ازدحام الطرق بالمركبات.

2-1 أنواع شبكات الحاسوب وفق النطاق الجغرافي (LAN, MAN, WAN)

تصنَّف الشبكات الحاسوبية بناءً على عدة معايير، أبرزها النطاق الجغرافي وطريقة التوصيل, وفيما يأتي تصنيف الشبكات حسب النطاق الجغرافي :

1. الشبكة المحلية (LAN) (Local Area Network) :

هي شبكة حاسوبية تربط مجموعة من الأجهزة ضمن نطاق جغرافي محدود، مثل المنازل أو المكاتب أو المدارس أو المباني. تهدف الشبكة المحلية إلى تمكين الأجهزة المتصلة من تبادل البيانات والمشاركة في الموارد، مثل الطابعات والملفات واتصال الإنترنت .



شكل (1– 2) يوضح نموذج لشبكة محلية (LAN)

2. الشبكة الاقليمية (Metropolitan Area Network MAN) :

هي نوع من الشبكات التي تغطي منطقة جغرافية أوسع من الشبكة المحلية و عادةً ما تربط الشبكة الإقليمية عدة شبكات محلية في مدينة أو منطقة حضرية، مما يسهل نقل البيانات وتحسين الاتصال بين الأفراد والشركات داخل المنطقة، وتوفر حلولاً متكاملة للأعمال والخدمات العامة، مثل المؤسسات التعليمية والمستشفيات والمراكز الحكومية.

شكل (1– 3) يوضح نموذج لشبكة محلية (MAN)

3. الشبكة الواسعة (Wide Area Network WAN) :

تُستخدم هذه الشبكات لتوصيل شبكات محلية متعددة في مناطق جغرافية مختلفة، مثل الدول أو القارات وتُستخدم عادةً لنقل البيانات والمعلومات وتستخدم الشركات الكبيرة الشبكات الواسعة لربط فروعها في مختلف البلدان ومشاركة البيانات والملفات بينها. تعتمد هذه الشبكات على تقنيات الاتصالات المختلفة مثل الأقمار الصناعية لضمان انتقال البيانات بسرعات وموثوقية عالية.

شكل (1 – 4) يوضح نموذج لشبكة محلية (WAN)

جدول (1-1) يوضح المقارنة بين الشبكة المحلية (LAN) و الشبكة الواسعة (WAN)

الخاصية	الشبكة المحلية (Local Area Network) (LAN)	الشبكة الواسعة (Wide Area Network) (WAN)
المساحة الجغرافية	تغطي مساحة صغيرة (المنزل، المدرسة، بناية مكتب)	تغطي منطقة جغرافية كبيرة (المدن، الدول)
السرعة	أسرع من WAN	أبطأ من LAN
طريقة الاتصال	كابلات إيثرنت، Wi-Fi	الأقمار الصناعية،الألياف الضوئية، الإنترنت
معدل نقل البيانات	مرتفع (يصل إلى 1000 ميجابت في الثانية)	أقل (يصل إلى 150 ميجابت في الثانية)
التكلفة	منخفضة نسبيًا	عالية جدًا
تحمل الأخطاء	مرتفع	منخفض
نوع الاتصال	كابلات إيثرنت، Wi-Fi	الأقمار الصناعية، الألياف الضوئية، الإنترنت
مثال	شبكة مكتب أو مدرسة	شبكة الإنترنت

3-1 مكونات الشبكات

وتشمل جميع الاجهزة والمعدات الفيزيائية المستخدمة لإنشاء الشبكة مثل الحواسيب و أجهزة الشبكة و المجمعات والموجهات والمبدلات ..... الخ ووسائل الاتصال التي تربط هذه الأجهزة بعضها ببعض . وفي الفقرات اللاحقة سنتعرف عزيزي الطالب على هذه المكونات .

1-3-1 الحواسيب (Computers) :

الحاسوب هو جهاز إلكتروني قادر على معالجة البيانات وفقًا لمجموعة من التعليمات المخزنة (البرامج) ويقوم الحاسوب بتنفيذ العمليات الحسابية والمنطقية ، وتخزين المعلومات ، وعرض النتائج. يعتمد الحاسوب على المعالج (CPU) والذاكرة و وحدات الإدخال والإخراج والبرامج لتشغيله. ويستخدم الحاسوب في مجالات متعددة منها (التعليم ، الطب ، الأعمال والإدارة المالية ، الهندسة والتصميم ، الأمن والدفاع ، ... الخ). وتختلف الحواسيب حسب (الحجم ، الأداء ، والاستخدام) . ومن أهم أنواعها الحاسوب الشخصي (PC) (Perseonal Computer) ، الحاسوب المحمول (Laptop) , الحاسوب اللوحي (Tablet) . ويمكن تلخيص أهمية الحاسوب فيما يلي :-

1- **تسريع العمليات** : تنفيذ المهام بسرعة ودقة عالية مقارنة بالإنسان.
2- **تخزين البيانات** : يمكنه حفظ كميات ضخمة من البيانات الرقمية واسترجاعها بسهولة.
3- **توفير الاتصال والتواصل** : من خلال الإنترنت، البريد الإلكتروني، وتطبيقات الدردشة.
4- **تحسين الإنتاج :** يساعد الشركات والمؤسسات على إدارة المهام بكفاءة عالية.
5- **الأتمتة** : يستخدم في الأتمتة الصناعية والروبوتات الذكية.

شكل (1– 5) يوضح انواع الحواسيب

2-3-1 الاجهزة الشبكية:

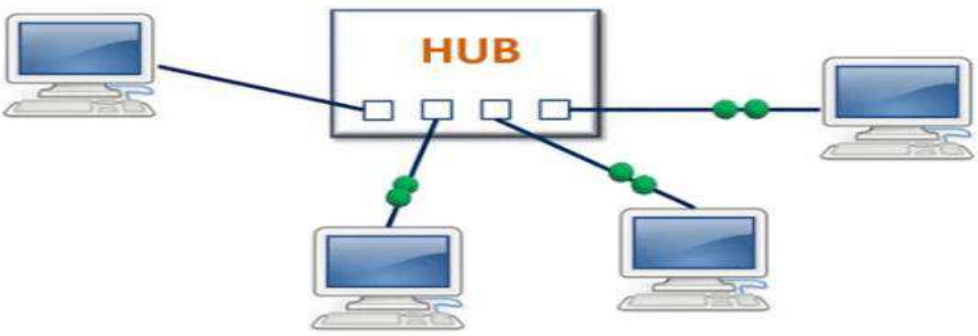
1- المجمع (Hub) في شبكات الحاسوب:

المجمع هو جهاز شبكي بسيط يستخدم لربط أجهزة متعددة في شبكة محلية (LAN) يعمل على نقل البيانات من الجهاز إلى جميع الأجهزة الأخرى المتصلة به دون تمييز بينها. لا يقوم بتحليل البيانات أو تحديد وجهتها، بل يرسلها إلى المنافذ المتاحة كلها.

شكل (1– 6) يوضح نموذج للمجمع (Hub)

وفيما يلي اهم الخصائص التي يتمتع بها المجمع (**Hub**):

1- **إرسال البيانات إلى جميع الأجهزة :** عندما يستقبل المجمع بيانات، يرسلها إلى جميع المنافذ بغض النظر عن وجهتها.
2- **لا يحتوي على ذاكرة تخزين مؤقتة** : لا يقوم بحفظ البيانات أو تصفيتها قبل إرسالها.
3- **عرض النطاق الترددي المشترك** : جميع الأجهزة المتصلة به تشارك عرض النطاق الترددي نفسه، مما قد يؤدي إلى بطء الأداء في حالة زيادة عدد الأجهزة.
4- **سهولة التركيب والاستخدام :** لا يحتاج إلى إعدادات معقدة، وإنما يتم توصيل الأجهزة به.
5- **أداء أقل مقارنةً بالمبدل (Switch) :** بسبب إرساله البيانات إلى جميع الأجهزة، قد يحدث ازدحام في الشبكة.



شكل (1 – 7) يوضح استخدام المجمع (Hub) في الربط الشبكي

ويمكن تلخيص أهمية المجمع (**Hub**) فيما يلي :-

1. ربط عدة أجهزة داخل شبكة محلية (**LAN**) صغيرة مثل المكاتب أو المنازل.
2. زيادة عدد الأجهزة المتصلة بالشبكة عندما تكون المنافذ المتاحة محدودة.
3. توصيل أجهزة متعددة بشبكة واحدة عند عدم الحاجة إلى إدارة متقدمة لحركة البيانات.
4. استخدامه في بعض البيئات التعليمية والتدريبية وسهولة استخدامه لفهم كيفية عمل الشبكات الأساسية.
5. يعد أداة فعالة في الشبكات الصغيرة التي لا تحتاج إلى إدارة معقدة لحركة البيانات.
6. تكلفة منخفضة مقارنة بالمبدّلات (**Switches**) .

2- المبدل (Switch) في شبكات الحاسوب:

المبدل هو جهاز شبكي يعمل على الطبقة الثانية من نموذج **OSI** ، ويستخدم لربط الأجهزة داخل الشبكة المحلية (**LAN**) يقوم بتوجيه البيانات بناءً على عناوين **MAC** ، مما يسمح بتوصيل الأجهزة بطريقة أكثر كفاءة مقارنة بالمجمع (**HUB**). في بعض الأحيان، تعمل بعض المبدلات الذكية على الطبقة الثالثة (**Layer 3**) لدعم وظائف التوجيه بين الشبكات.

وفيما يلي اهم الخصائص التي يتمتع بها المبدل (Switch)

1. يعمل على الطبقة الثانية (**Layer 2**) باستخدام عناوين **MAC** لتوجيه البيانات.
2. يدعم الاتصال المزدوج الكامل (**Full Duplex**) مما يسمح بالإرسال والاستقبال في وقت واحد.
3. دعم الأمان من خلال تقسيم الشبكة إلى شبكات فرعية (**VLANs**), وعزل الأجهزة لتنظيم الوصول إلى الشبكة.
4. يدعم جودة الخدمة لتحديد أولويات حركة المرور المهمة مثل الصوت والفيديو.
5. إدارة حركة البيانات بشكل ذكي و عرض النطاق الترددي (**Bandwidth**) بفعالية، مما يقلل من التصادمات وزيادة سرعة الاتصال.
6. يمكن أن يحتوي على منافذ متعددة بسرعات مختلفة (**10 / 100 / 1000 Mbps**).

ويمكن تلخيص أهمية المبدل (**Switch**) فيما يلي :-

1. إنشاء شبكات محلية (**LAN**) لربط أجهزة الحواسيب والطابعات والخوادم.
2. تحسين سرعة أداء الشبكة عبر توجيه البيانات فقط إلى الجهاز المستهدف بدلاً من إرسالها للجميع كما يفعل المجمع (**HUB**) .
3. استخدامه في مراكز البيانات (**Data Centers**) لربط الخوادم وتحقيق اتصال عالي السرعة.

شكل (1– 8) يوضح نموذج للمبدل (Switch)

3- الموجه (Router) في شبكات الحاسوب:

الموجه هو جهاز شبكة يستخدم لتوجيه البيانات بين الشبكات المختلفة. يقوم بتحديد أفضل مسار لنقل البيانات باستخدام بروتوكولات التوجيه، ويعمل الموجه بشكل أساسي على الطبقة الثالثة (**Layer 3**) من نموذج **OSI**.

وفيما يلي اهم الخصائص التي يتمتع بها الموجّه (**Router**) :-

1- **الاتصال بالإنترنت :** يقوم بربط الشبكة المحلية (**LAN**) بشبكة الإنترنت.

2- **توجيه البيانات بين الشبكات : يستخدم في المؤسسات والمنازل لإرسال البيانات بين الشبكات المختلفة.**

3- **إنشاء شبكات واسعة (WANs) :** يربط الفروع البعيدة لمؤسسة واحدة بشبكة موحدة.
4- **الحماية والأمان** : يوفر جدار حماية (**Firewall**) لمنع الوصول غير المصرح به.
5- **إدارة حركة المرور في الشبكة** : يساعد على توزيع البيانات بشكل فعال عبر الشبكة.

شكل (1– 8) يوضح نموذج للموجه (Router)

ويمكن تلخيص أهمية الموجّه (**Router**) فيما يلي :-

1. تحسين سرعة الشبكة من خلال توجيه البيانات بكفاءة.
2. الاتصال بين الشبكات المختلفة، مثل ربط شبكة منزلية بالإنترنت.
3. إدارة الشبكة من خلال تعيين عناوين (**Internet Protocol**) **IP** وتكوين الشبكات الفرعية (**Sub netting**).
4. يدعم تقنيات الأمان مثل التشفير، **VPN**، وجدران الحماية.

الشكل (1 – 9) يوضح نماذج لأجهزة الشبكة

جدول (1-2) يوضح الاختلافات الرئيسية بين المجمع ،المبدل ، و الموجه

الخاصية	المجمع (Hub)	المبدل (Switch)	الموجه (Router)
التعريف	جهاز يربط الأجهزة داخل الشبكة نفسها ولكنه يرسل البيانات إلى جميع الأجهزة المتصلة.	جهاز يقوم بتوصيل الأجهزة داخل الشبكة نفسها المحلية ويوجه البيانات إلى الجهاز المستهدف.	جهاز يوجه البيانات بين شبكات مختلفة أو بين أجهزة داخل الشبكة نفسها.
الوظيفة الأساسية	توزيع البيانات إلى جميع الأجهزة في الشبكة المحلية (LAN) دون تحديد الجهاز المستهدف.	توجيه البيانات داخل الشبكة المحلية (LAN) بين الأجهزة المختلفة.	توجيه البيانات بين الشبكات المختلفة، مثل شبكة الإنترنت والشبكة المحلية (LAN)
طريقة العمل	يرسل البيانات إلى جميع الأجهزة المتصلة، ولا يحدد الجهاز المستهدف.	يقوم بتوجيه البيانات إلى الجهاز المستهدف باستخدام عنوان الـ MAC	يقوم بتوجيه البيانات بين الشبكات باستخدام عنوان الـIP .
الطبقة في نموذجOSI	طبقة (Layer 1) الطبقة الفيزيائية.	طبقة (Layer 2) طبقة ربط البيانات.	طبقة (Layer 3) طبقة الشبكة.
الأداء	أقل كفاءة من الراوتر والمبدل؛ يسبب ازدحامًا في الشبكة بسبب إرسال البيانات لجميع الأجهزة.	أكثر كفاءة من الـ Hub لأنه يوجه البيانات إلى الجهاز المستهدف فقط.	يمكن أن يكون بطيئًا بسبب الحاجة إلى تحليل البيانات بين الشبكات.
الأمان	لا يوفر أمانًا؛ البيانات ترسل لجميع الأجهزة في الشبكة.	لا يوفر أمانًا، لكنه يحدد الجهاز المستهدف باستخدام عنوان MAC	يوفر أمانًا أعلى، يمكنه استخدام جدران نارية وأنظمةNAT
التوصيل بين الشبكات	يربط بين أجهزة في الشبكة المحلية (LAN) نفسها	يربط بين أجهزة في الشبكة المحلية (LAN) نفسها	يربط بين شبكات مختلفة (مثل الشبكة المحلية والإنترنت).
التكلفة	أقل تكلفة بين الثلاثة.	أقل تكلفة من الراوتر ولكن أغلى من الـ(Hub)	عادة أغلى من الـ Switch والـ(Hub) بسبب الميزات المتقدمة.

3-3-1 الإيثرنت (Ethernet) :

الإيثرنت هو مجموعة من تقنيات الشبكات المستخدمة في توصيل الأجهزة داخل الشبكات المحلية (LAN) يعتمد على بروتوكولات الاتصالات التي تحدد كيفية إرسال البيانات واستقبالها بين الأجهزة

المتصلة عبر كابلات أو شبكات لاسلكية. ويستخدم في شبكات المنازل والمكاتب و مراكز البيانات والخوادم والمؤسسات الكبيرة والبنوك وتشغيل الكاميرات الأمنية وأجهزة إنترنت الأشياء (**IoT**). ويعمل الايثرنت وفق معيار **IEEE** 802.3 لتنظيم إرسال البيانات. ويوفر الايثرنت سرعة واستقرارا و إمكانية في التوسع مما يجعله الخيار المثالي للشبكات الحديثة. تتكون أجهزة Ethernet من ثلاثة مكونات رئيسة:

1- **بطاقات الايثرنت:** تمكن بطاقات الايثرنت أجهزة الحاسوب من نقل البيانات واستقبالها عبر الشبكة.

2- **المحاور أو أجهزة التوجيه:** تقوم محاور الايثرنت بتوجيه البيانات بين أجهزة الحاسوب داخل الشبكة ويمكنها أيضا الاتصال بالإنترنت.

3- **الكابلات :** تسهل كابلات الايثرنت لنقل البيانات ثنائية الاتجاه و تنقسم كابلات الإيثرنت إلى عدة فئات بناءً على سرعتها وجودتها في نقل البيانات وكما موضح في الجدول الآتي :

جدول (1-3) يوضح الاختلافات الرئيسية بين الكيبلات

الفئة	السرعة القصوى	التردد (MHz)	المسافة (متر)
Cat 5	Mbps 100	MHz 100	100م
Cat 5e	Gbps1	MHz 100	100م
Cat 6	Gbps 10	MHz 250	100م
Cat 6 a	Gbps 10	MHz 500	100م
Cat 7	Gbps 10	MHz 600	100م
Cat 8	Gbps 25-40	MHz 2000	30م

1-3-4 البرمجيات (Software):

تشمل المكونات البرمجية على كل من أنظمة التشغيل والبروتوكولات والبرامج التطبيقية الأخرى ويمكن إدراجها في ما يأتي:

نظم تشغيل الشبكة Network Operating Systems:

نظم تشغيل الشبكات القديمة كانت تقدم خدمات بسيطة وبعضا من وسائل التأمين ولكن نظراً لازدياد طلبات المستخدم صممت أنظمة التشغيل الشبكات الحديثة لتلبي هذه الطلبات و فيما يأتي بعض هذه الخصائص الضرورية الموجودة في أنظمة التشغيل الخاصة بالشبكات الحديثة وهي (خدمات الملفات ، درجة إحتمال أخطاء النظام ، برامج حماية الشبكات).

بروتوكولات الشبكة Network Protocols:

البروتوكولات هي عبارة عن مجموعة من القواعد والقوانين والإجراءات اللازمة لإجراء عملية الاتصالات في الشبكات . فهي تحدد الاسس والمعايير التي تتحكم بالاتصال والتفاعل بين الأجهزة والحاسوب المختلفة المربوطة على الشبكة . وهناك انواع كثيرة من البروتوكولات تختلف في وظائفها ومهامها . ومن أهم هذه البروتوكولات (**TCP / IP ، FTP ، HTTP** , ...الخ).

برامج إدارة الشبكات:

هي برامج تقوم بإدارة الشبكة, وتعطي المستخدمين الصلاحيات التي تمكنهم من العمل على الشبكة وتقوم بتنظيم العمل بينهم وتنظيم مشاركة موارد الشبكة من برمجيات ومكونات مادية فيما بينها. ومن أهم هذه البرامج (**Easy Cafe**) وبرنامج (**Microsoft LAN Manager**).

برامج التطبيقات:

وهي البرامج التي تمكن المستخدمين من الإفادة من برمجيات الشبكة المختلفة مثل تصفح صفحات الويب وهذه الخدمة تتطلب برامج مستعرضات الويب مثل (**Firefox** ، **Mozilla** ، **Microsoft Edeg**) , وكذلك خدمة البريد الالكتروني التي تستلزم برامج خاصة مثل (**Express Outlook**) وخدمة المحادثات ومن امثلة برامجها (**Net Meeting**) .

4-1 انواع الشبكات

تعرف وسائط الربط والاتصال الشبكي بأنها تلك الوسائل التي تقوم بإرسال المعلومات ونقلها بين الأجهزة المختلفة في الشبكات مهما كان نطاق عمل هذه الشبكات، ومن الأمور الفنية الرئيسة الواجب توافرها في وسيلة الاتصال هو المحافظة على إيصال الإشارات المعلوماتية دون حدوث ضعف فيها خلال عملية النقل، بالإضافة إلى المحافظة على سرية المعلومات المنقولة، وبصورة عامة. ويمكن تصنيف الشبكات حسب طريقة التوصيل ووسائط الربط والاتصال الشبكي الى ما يأتي :

- **الشبكات السلكية (Wired Networks)**
- **الشبكات اللاسلكية (Wireless Networks)**

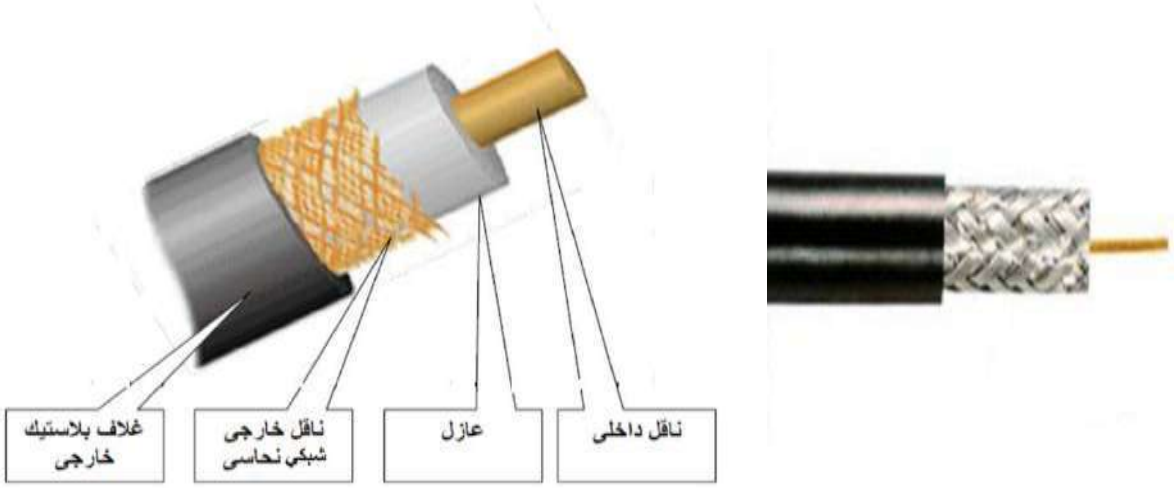
1-4-1 الشبكات السلكية (Wired Networks)

يقصد بوسائط الربط والاتصال السلكية جميع الموصلات (الكيبلات) التي تسهم في الربط الشبكي وإيصال المعلومات وتشاركها بين الأجهزة المختلفة في الشبكة، وتقسم هذه الوسائط إلى أنواع متعددة أهمها:

- ❖ الموصلات المحورية (**Coaxial Cables**).
- ❖ الموصلات المجدولة (**Twisted Pair Cables**): ويمكن أن تقسم بدورها إلى ثلاثة أقسام هي:
  - ✓ الموصلات المجدولة غير المعزولة (**Unshielded Twisted Pair (UTP**).
  - ✓ الموصلات المجدولة المعزولة (**Shielded Twisted Pair (STP**).
  - ✓ الموصلات المجدولة الملفوفة (**Folded Twisted Pair (FTP**).
- ❖ موصلات الألياف الضوئية (**Fiber Optic Cables**).

الموصلات المحورية Coaxial Cables:

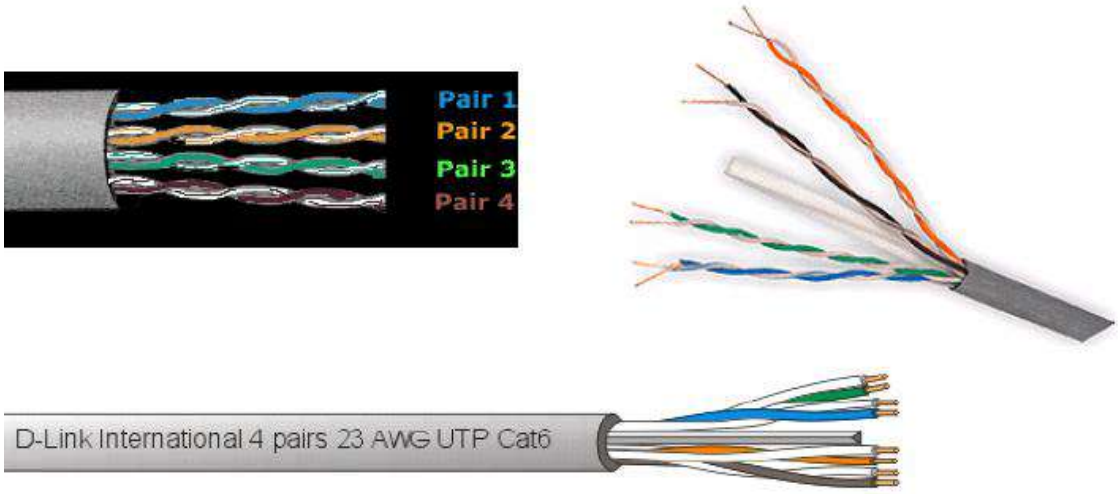
هذا النوع من الموصلات يتكون من سلك نحاسي محوري مسؤول عن نقل الإشارة الكهربائية مغطى بمادة عازلة ومحاط بشبكة سلكية ملفوفة بشكل ضفائر حول هذا العازل تمثل القطب الأرضي للسلك، تقوم الضفائر (الشبكة) المعدنية بحماية المحور من تأثير التداخل الكهرومغناطيسي والإشارات التي تتسرب من الأسلاك المجاورة التي تسمى (**Crosstalk**)، تحاط هذه الشبكة بغطاء خارجي مصنوع من المطاط أو البلاستيك أو التفلون (**Teflon**)، زيادة على ذلك تستخدم بعض الموصلات المحورية طبقة أو طبقتين من القصدير حماية إضافية.



الشكل (1 – 10) يوضح الموصلات المحورية المستخدمة في الربط الشبكي

الموصلات المجدولة Twisted Pair Cables:

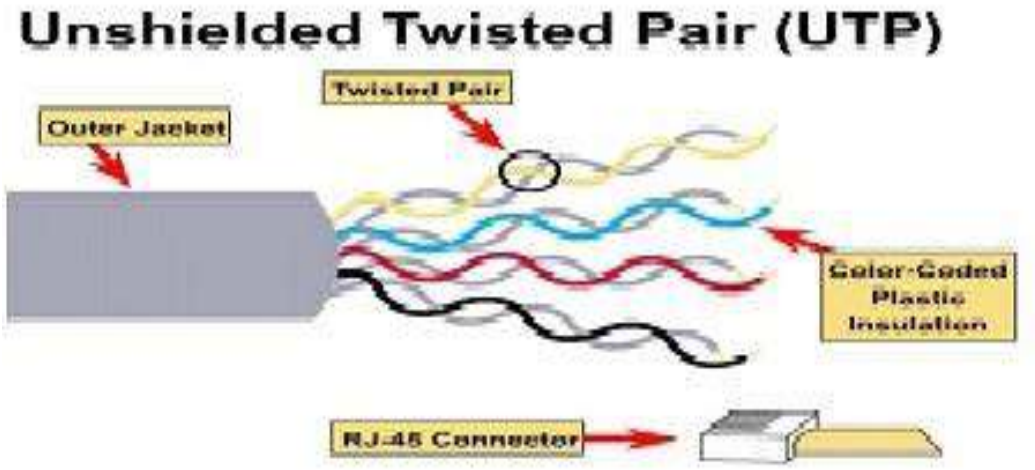
هي عبارة عن أسلاك مجدولة من سلكين نحاسيين احدهما ملفوف على الآخر، يستخدم هذا النوع من الموصلات بشكل أكثر من الموصلات المحورية وذلك لتميزها بسهولة التركيب والصيانة وقابلية التوسع وهو الأكثر استخداما في الشبكات المحلية. يشبه هذا النوع من الموصلات سلك الهاتف إلا أنه يحتوي على أربعة أزواج (ثمانية أسلاك) من الأسلاك النحاسية، حيث يتكون كل زوج من هذه الأزواج من سلكين نحاسيين معزولين وملفوفين بشكل حلزوني احدهما على الآخر ، حيث يستعمل أحد السلكين في نقل البيانات والآخر في استقبال البيانات وتتراوح سرعة نقل البيانات في هذه الأسلاك تقريبا مئة ميجابت في الثانية (100 **Mbps**), وتختلف احيانا بحسب نوع الكابل ، ويمكن تقسيم هذا النوع من الموصلات إلى ثلاثة أنواع اعتمادا على نوع وطبقة تغليف الأسلاك الداخلية المجدولة وعلى ما يأتي:



الشكل (1-11) يمثل المقطع الطولي للموصل المجدول غير المعزول

1- الموصلات المجدولة غير المعزولة Unshielded Twisted Pair (UTP):

يتكون الكيبل المجدول غير المعزول من ثمانية أسلاك نحاسية رفيعة موضوعة داخل عازل خارجي ويتم جدل كل زوج من هذه الأسلاك لحماية البيانات من التداخل والضوضاء، تستخدم الموصلات المجدولة هذه في الشبكات المحلية من النوع **Star**، وتنقل البيانات بسرعة فعلية تصل إلى 100 **Mbps** بحد أقصى لطول الموصل 100 **m** ، تستخدم الموصلات المجدولة وصله نوع **RJ** 45.



الشكل (1-12) يمثل حالة الجدل في السلك المجدول غير المعزول

مميزات هذا الموصل:

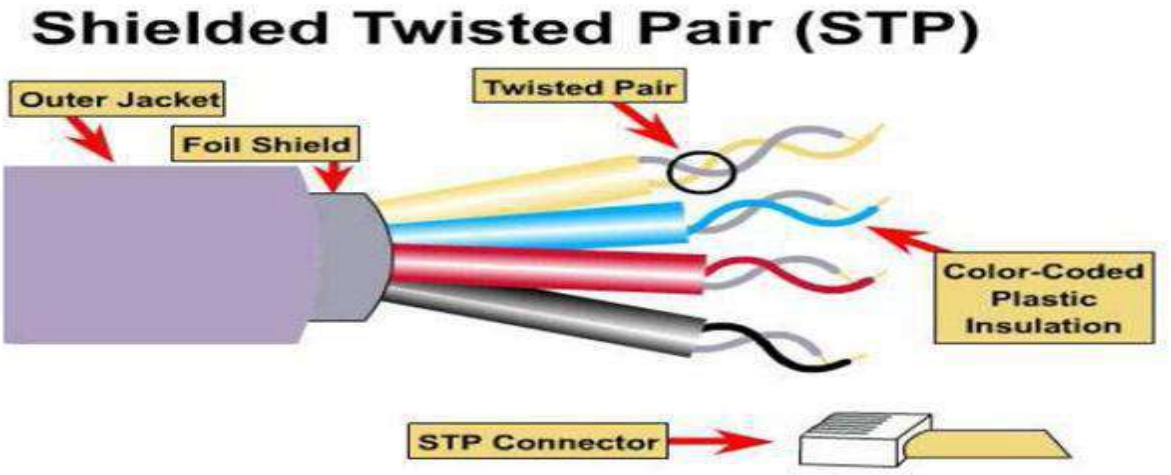
- أرخص أنواع الموصلات سعراً.
- أكثر أنواع الموصلات مرونة و أكثرها قابلية للثني.
- سهولة التركيب والاستخدام .
- أكثر الأنواع استخداما.

مساوئ هذا الموصل:

- المدى المسموح به لنقل البيانات قليل.
- سرعة نقل البيانات بطيئة.
- أكثر عرضة للتداخل لأنه قليل العزل

2- الموصلات المجدولة المعزولة Shielded Twisted Pair (STP):

الموصلات المجدولة المعزولة تشبه غير المعزولة ولكن تحاط أسلاك النحاسية الثمانية فيها بطبقة عازلة من الألومنيوم ويوجد طرف أرضي للتخلص من التداخلات غير المرغوب فيها. يستخدم كيبل **STP** في شبكات الـ **STAR** و شبكات **Token Ring** ، تصل سرعة نقل البيانات من الناحية العملية إلى 1000 **Mbps** بحد أقصى لطول الموصل 100**m** .



الشكل (1-13) يمثل الموصل المجدول المعزول STP

مميزات هذا الموصل:

- أسرع أنواع الموصلات النحاسية في نقل البيانات بعد الألياف الضوئية.
- أقل عرضة للتداخلات والموجات الكهرومغناطيسية.
- العزل الجيد.
- أقل عرضة للتجسس وسرقة المعلومات.

مساوئ هذا الموصل:

- صعوبة تركيب الموصل.
- أقل مرونة من الموصل **UTP**.
- غالي الثمن.

تتفوق الموصلات المجدولة من النوع **STP** على الموصلات من النوع **UTP** بعدة مزايا مهمة يمكن إجمالها بما يأتي:

1. أن الموصلات من النوع **STP** أقل عرضة للتداخل الكهرومغناطيسي.
2. أن الموصلات من النوع **STP** تستطيع دعم الإرسال لمسافات أبعد من النوع **UTP**.
3. أن الموصلات من النوع **STP** تستطيع في بعض الظروف توفير سرعات بتّ أكبر من النوع الثاني.

3- الموصلات المجدولة الملفوفة Folded Twisted Pair (FTP):

يكون تركيب هذا الموصل بطريقة تركيب موصل **UTP** نفسها, مع إضافة طبقة عازلة من الألومنيوم حول الأسلاك المجدولة لمنع الضوضاء و التداخلات الخارجية و تقليلها, لكن لا يوجد به طرف أرضي.

الشكل (1-14) يمثل الموصل المجدول المعزول الملفوف FTP

مميزات هذا الموصل:

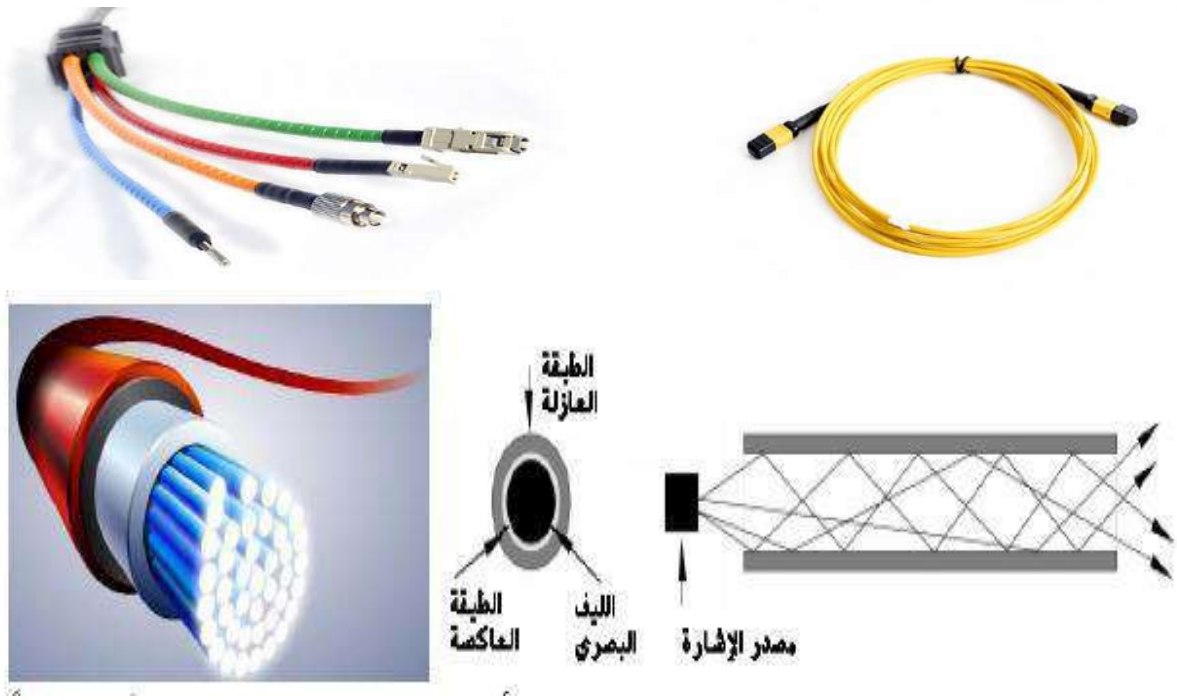
- العزل الجيد و ذلك لوجود طبقة من الألومنيوم.
- سهولة التركيب والاستخدام.
- أكثر مرونة من الموصل STP وأقل من **UTP**.
- أقل تكلفة من الموصل **STP**.

مساوئ هذا الموصل:

- ❖ قليل الاستخدام نظراً لأنه غير تام العزل كونه يحاط بطبقة عازلة من الالمنيوم حول الاسلاك المجدولة ولا يحاط بطبقة عازله حول الاسلاك نحاسية الثمانية, اضافة الى أنه لايوجد به طرف ارضي كما في الكيبل **STP** .
- ❖ سرعة نقل البيانات محدودة.

موصلات الألياف البصرية Fiber Optic Cables:

يستخدم هذا النوع من الموصلات كمصدر لنقل المعلومات بدرجة عالية من الدقة، حيث يتألف هذا الموصل من جدائل طويلة مصنوعة من الزجاج سمك الواحدة منها لا يتعدى سمك الشعرة وهذه الجدائل توضع بهيئة حزمة تسمى **Fiber Optic Cable**، أي أن الليف الضوئي يكون محاطاً بجزء عاكس وذلك لضمان عدم تشتت الضوء ومن ثم يغلف بمادة واقية من البلاستك، ويتراوح قطر الموصل ما بين (2 إلى 125) مايكرومتر، ويوجد منه نوعان أحدهما أحادي يستخدم للمسافات الطويلة والآخر متعدد يستخدم للشبكات المحلية، والشكل الآتي يوضح مقاطع مختلفة لهذا النوع من الموصل مع شكل مقابس الربط الخاصة به.



الشكل (1-15) يوضح مقاطع مختلفة من موصلات الألياف البصرية

خصائص الألياف الضوئية:

نقل البيانات بسرعة عالية: توفر الألياف الضوئية سرعات نقل بيانات تصل إلى جيجابايتات في الثانية، مما يجعلها مثالية للتطبيقات التي تتطلب نقل بيانات كثيف وسريع.

1- **مسافات طويلة:** يمكن للألياف الضوئية نقل الإشارات لمسافات طويلة (على سبيل المثال، عبر المدن أو بين البلدان) دون الحاجة إلى تعزيز الإشارة أو تقويتها.
2- **عدم التأثر بالتداخل الكهرومغناطيسي**: لا تتأثر الألياف الضوئية بالمجالات الكهرومغناطيسية أو التداخلات الناتجة عن الأجهزة الكهربائية الأخرى، مما يوفر اتصالًا أكثر استقرارًا.
3- **أداء أفضل في الظروف البيئية الصعبة:** فيمكن استخدام الألياف الضوئية في بيئات صعبة مثل تلك التي تحتوي على رطوبة أو درجات حرارة شديدة.
4- **صغر الحجم وخفة الوزن:** الألياف الضوئية أخف وأصغر مقارنة بالكابلات النحاسية، مما يجعلها أسهل في التركيب والنقل.
5- **الأمان:** يصعب اختراق الألياف الضوئية لأنها لا تنقل إشارات كهربائية يمكن اعتراضها بسهولة.

أما مساوئ موصلات الألياف الضوئية يمكن حصرها بأن تركيبها وصيانتها أمر في غاية الصعوبة.

2-4-1 الشبكات اللاسلكية (Wireless Networks)

الشبكات اللاسلكية هي شبكات تتيح تبادل البيانات بين الأجهزة دون الحاجة إلى كابلات أو أسلاك، وتعتمد على تقنيات مثل الموجات الراديوية أو الأشعة تحت الحمراء لنقل البيانات. تُستخدم هذه الشبكات في الكثير من التطبيقات، مثل شبكات الإنترنت المنزلية، والاتصالات بين الأجهزة الذكية، وشبكات الشركات، وغيرها ومن أهم أنواع الاتصالات اللاسلكية :

تقنية الواي فاي Wi-Fi (Wireless Fidelity)

- ✓ يُستخدم بشكل شائع في الشبكات المحلية (**LAN**) .
- ✓ يتيح الاتصال بالإنترنت للأجهزة عبر الموجهات اللاسلكية في المنازل والمكاتب.
- ✓ يدعم سرعات نقل بيانات تتراوح من 11 ميجابت في الثانية **Wi-Fi** 4 إلى 9.6 جيجابت في الثانية **Wi-Fi** 6.

تقنية البلوتوث Bluetooth

- ✓ يُستخدم للاتصال بين الأجهزة في نطاق قصير (عادة لا يتجاوز 100 متر).
- ✓ يتيح الاتصال بين الأجهزة مثل الهواتف المحمولة، السماعات، الساعات الذكية، والأجهزة القابلة للارتداء.
- ✓ مثالي لاستهلاك الطاقة المنخفض وملاءمة الاتصال في المسافات القريبة.

شبكات الجيل الرابع والخامس (4G / 5G)

- ✓ **4G** توفر سرعات عالية جدًا للإنترنت عبر الشبكات الخلوية.
- ✓ **5G** تقدم سرعات أعلى بكثير وتدعم تقنيات مثل الإنترنت للأشياء (**IoT**) والاتصال في الزمن الحقيقي.
- ✓ تستخدم في الهواتف الذكية، الأجهزة المحمولة، والسيارات المتصلة.

NFC (Near Field Communication)

- ✓ يستخدم في الاتصال بين الأجهزة على مسافة قصيرة جدًا (عادة أقل من 10 سنتيمترات).
- ✓ يُستخدم في الدفع الإلكتروني عبر الهواتف الذكية (مثل Apple Pay، **Google Pay**).

WIMAX (Worldwide Interoperability for Microwave Access)

- ✓ تقنية لاسلكية لتوفير الإنترنت عالي السرعة في المناطق الكبيرة أو عبر نطاقات واسعة.
- ✓ يُستخدم في بعض المناطق الريفية أو في تغطية المناطق التي يصعب وصول الكابلات إليها.

Zigbee

- ✓ تقنية منخفضة الطاقة تُستخدم في تطبيقات الإنترنت للأشياء.(**IoT**)
- ✓ يُستخدم في أجهزة التحكم الذكية في المنازل مثل الأضواء الذكية والمقابس الذكية.

جدول (4-1) يوضح الاختلافات الرئيسية بين الشبكات السلكية و الشبكات اللاسلكية

الخاصية	الشبكات السلكية (Wired)	الشبكات اللاسلكية (Wireless)
التوصيل	**يتم التوصيل باستخدام أسلاك وكابلات مثل Ethernet أو كابلات الألياف البصرية.**	**يتم التوصيل عبر إشارات راديوية أو أمواج لاسلكية مثل Wi-Fi أو (Bluetooth)**
الأداء	**عادةً ما تكون أسرع وأكثر استقرارًا مقارنة بالشبكات اللاسلكية.**	**قد تتأثر بالمسافة والتداخل، ولكن مع التقنيات الحديثة مثل Wi-Fi 6 ، يمكن أن تكون سريعة جدًا.**
التكلفة	**تحتاج إلى أسلاك وكابلات، مما قد يزيد من التكلفة، خصوصًا في المساحات الكبيرة.**	**تكاليف أقل من حيث التركيب، ولكن قد تحتاج إلى أجهزة موجهة أو نقاط وصول (Access Points).**
التغطية	**محدودة بالمسافة التي تصل إليها الكابلات.**	**التغطية يمكن أن تكون واسعة جدًا، ولكنها تتأثر بالعوائق مثل الجدران.**
التنقل	**لا يمكن التنقل بسهولة لأن الأجهزة مرتبطة بالكابلات.**	**يمكن التنقل بحرية لأن الاتصال لا يعتمد على الأسلاك.**
الأمان	**أكثر أمانًا بشكل عام لأن الاتصال يعتمد على الأسلاك الفعلية.**	**قد تكون أقل أمانًا، لأن الإشارات يمكن اعتراضها إذا لم تكن الشبكة مشفرة.**
الاستهلاك الكهربائي	**قد تستهلك الأجهزة التي تعمل بالشبكات السلكية طاقة أقل بسبب الاعتماد على الكابلات.**	**قد تستهلك المزيد من الطاقة في بعض الأحيان، خصوصًا في الأجهزة المحمولة.**
الموثوقية	**أكثر موثوقية لأن الإشارة تكون ثابتة وغير عرضة للتداخل.**	**قد تتأثر بالإشارات الشبكية من أجهزة أخرى أو المسافة عن نقطة الوصول.**
الصيانة	**تتطلب صيانة أسلاك وكابلات، وقد تكون أكثر تعقيدًا إذا كان هناك تلف في الكابلات.**	**أسهل من حيث الصيانة، ولكن قد تحتاج إلى تحديثات أو تغييرات في الأجهزة اللاسلكية بشكل متكرر.**

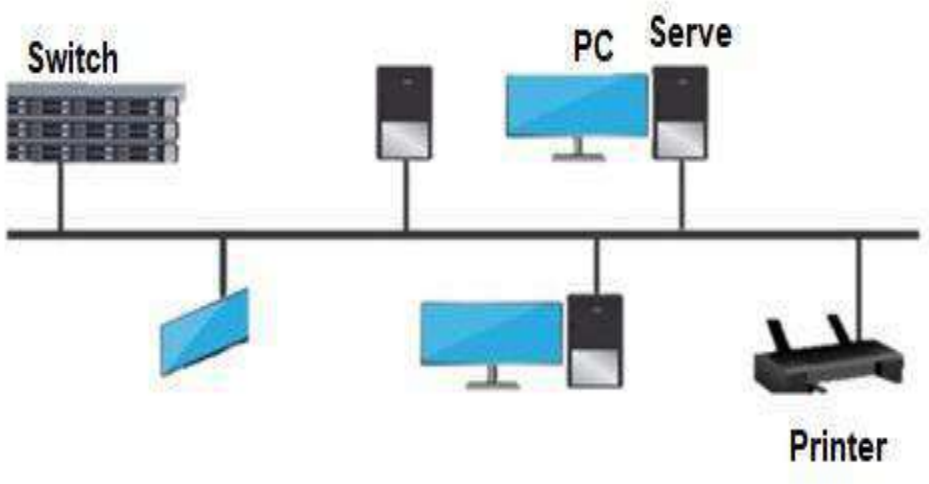
5-1 هيكلية الشبكات وطوبوغرافيتها

في علوم الحاسوب يشير بطوبوغرافية الشبكات إلى هيكل وترتيب الأجهزة المتصلة داخل الشبكة ومن أشهر انواعها:

1. الشبكة الخطية (Bus Network)
2. الشبكة النجمية (Star Network)
3. الشبكة الحلقية (Ring Network)
4. الشبكة المتداخلة (Mesh Network)

1-5-1 الشبكة الخطية (Bus Network) :

تعد الشبكة الخطية من أقدم وأبسط أنواع الشبكات أذ إن جميع الأجهزة المتصلة بالشبكة تتشارك في نفس الناقل أو الكابل بينها في خط مستقيم. ويستطيع أي جهاز أن يرسل الرسائل إلي أي عقدة وتنتقل هذه الرسائل إلي العقد الموجودة علي الشبكة كافة, ولكن لا يستطيع قراءتها إلا المرسلة له ويكون المرسل في هذه اللحظة هو المسيطر علي الشبكة حتى ينتهي من عملية الإرسال. ولا يوجد في هذه الشبكة أجهزة تبديل أو رادارات فجميع المحطات مربوطة فيما بينها عبر وسيط بث خطي مباشر، وبامكان جميع المحطات الاخرى في الشبكة استقبال أي بث يرد من محطة معينة. وفي سبيل السيطرة على الترتيب المنظم بين المحطات، فانه يتم تطبيق أسلوب التحكم بالوصول الذي لا يجيز بث البيانات إلا لجهاز واحد في وقت معين.



الشكل (1– 16) يوضح نموذجا للشبكة الخطية

أهمية الشبكة الخطية:

1- **البساطة** : الشبكة الخطية تصميم بسيط وسهل الفهم، مما يجعلها مناسبة للتطبيقات التي لا تتطلب هيكلًا معقدًا.
2- **التكلفة المنخفضة** : تحتاج إلى أقل كمية من الأسلاك مقارنة بالشبكات الأخرى.
3- **سهولة الاتصال** : الأجهزة يمكن أن تتصل بسهولة عبر الكابل المشترك.
4- **التوسع المحدود** : يمكن إضافة أجهزة بسهولة دون الحاجة إلى إعادة تصميم الشبكة بشكل كامل.

مزايا الشبكة الخطية:

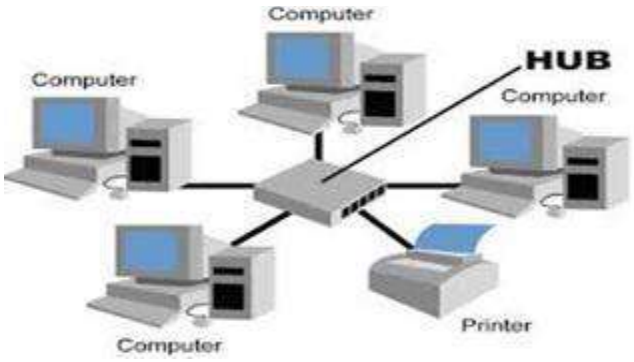
1- **التكلفة المنخفضة**: يتطلب بناء الشبكة الخطية عددًا أقل من الكابلات والأجهزة.
2- **السهولة في الإعداد**: يتم إعداد الشبكة بسهولة دون الحاجة إلى الكثير من المعدات.
3- **التوسع السهل**: من السهل إضافة أجهزة جديدة إلى الشبكة.
4- **البساطة**: تعد الشبكة الخطية بسيطة من حيث التصميم والهيكل.

عيوب الشبكة الخطية:

1- **التأثير عند انقطاع الكابل** : إذا حدث انقطاع في الكابل، تتوقف جميع الأجهزة عن العمل.
2- **ازدحام الشبكة** : إذا كان هناك عدد كبير من الأجهزة، قد يؤدي ذلك إلى بطء في نقل البيانات بسبب التداخل في الإشارات, والنقل باتجاه واحد.
3- **المشاكلات في الأداء** : مع زيادة عدد الأجهزة، يقل أداء الشبكة بسبب تزايد عدد الرسائل على الناقل
4- **صعوبة في الصيانة :** تتطلب المشاكلات التي تحدث في الكابل أو الأجهزة الى تتبعا دقيقا، وهذا قد يكون صعبًا في شبكات كبيرة.
5- **التحديات في التوسع** : التوسع في الشبكة قد يؤدي إلى تدهور في الأداء بسبب ازدحام الناقل

2-5-1 الشبكة النجمية (Star Network) :

الشبكة النجمية هي نوع من شبكات الحاسوب, تكون الأجهزة المتصلة بالشبكة مرتبطة جميعها بجهاز مركزي يُسمى المجمع (**Hub**) أو المبدل (**Switch**) في هذا النوع من الشبكات، يتم تبادل البيانات بين الأجهزة من خلال المحور أو المفتاح الذي يقوم بتوجيه البيانات بين الأجهزة المتصلة ومن أنواعها الشبكة النجمية التقليدية حيث يتم فيها ربط جميع الأجهزة بالمحور أو المفتاح باستخدام أسلاك والشبكة النجمية اللاسلكية :(**Wireless Star Network**) حيث يتم فيها ربط الأجهزة عبر الشبكة اللاسلكية (**Wi-Fi**) بموجه أو نقطة وصول (**Access Point**) .



الشكل (1 – 17) يوضح نموذجا للشبكة النجمية

أهمية الشبكة النجمية:

سهولة التركيب : الشبكة النجمية سهل إعدادها لأنها تعتمد على جهاز مركزي.
إدارة مركزية : من السهل إدارة الشبكة ومعرفة الجهاز الذي يواجه مشكلة لوجود نقطة مركزية.
المرونة في التوسع : يمكن إضافة أجهزة جديدة بسهولة إلى الشبكة بتوصيلها مباشرة بالمحور.
الأداء العالي : نقل البيانات بين الأجهزة يتم عبر المحور أو المفتاح، مما يضمن سرعة في التواصل.

مزايا الشبكة النجمية:

سهولة التركيب والصيانة : عملية التركيب والصيانة أسهل مقارنة بأنواع الشبكات الأخرى، إذ يمكن تشخيص المشكلات بسهولة بسبب وجود نقطة مركزية.
تقليل التأثير في حالة فشل جهاز : إذا فشل أحد الأجهزة المتصلة بالشبكة، فإن باقي الأجهزة لا تتأثر.
الأداء المحسن : المحور أو المفتاح يمكن أن يدير البيانات بكفاءة عالية ويسهم في تحسين الأداء.
التوسع السهل : يمكن إضافة المزيد من الأجهزة إلى الشبكة بسهولة.

عيوب الشبكة النجمية:

اعتماد كامل على الجهاز المركزي : في حالة فشل المحور أو المفتاح، فإن جميع الأجهزة المتصلة بالشبكة تتوقف عن العمل.
زيادة التكلفة : تحتاج إلى جهاز مركزي **(Hub)** أو **(Switch)** الذي قد يزيد من تكلفة الشبكة.
عدد الأسلاك : يتطلب عددا كبيرا من الأسلاك لتوصيل الأجهزة بالجهاز المركزي.
تأثير الحجم : كلما زاد عدد الأجهزة في الشبكة، زاد العبء على المحور أو المفتاح، مما قد يؤثر في الأداء إذا كان غير مناسب.

3-5-1 الشبكة الحلقية :(Ring Network)

الشكل (1 – 18) يوضح نموذجا للشبكة الحلقية

الشبكة الحلقية هي نوع من شبكات الحاسوب تكون الأجهزة فيها متصلة بشكل دائري، أي أن كل جهاز في الشبكة متصل بالجهازين السابق واللاحق له، ويشكل بذلك حلقة مغلقة. يتم إرسال البيانات في هذه الشبكة عبر حلقة (دائرة) بين الأجهزة، حيث يتم تمرير البيانات من جهاز إلى آخر حتى تصل إلى الجهاز المقصود ومن انواعها شبكة **Token Ring** التي كانت واحدة من أشهر أنواع الشبكات الحلقية في الماضي، حيث يتم إرسال "رمز **(Token)** "بين الأجهزة لإعطائها الحق في إرسال البيانات في الشبكة الحلقية البسيطة , حيث يتم إرسال البيانات من جهاز إلى آخر بشكل مستمر في دائرة مغلقة

أهمية الشبكة الحلقية

سهولة الهيكلة: يمكن تصميمها بسهولة مقارنة بأنواع الشبكات الأخرى.

التنظيم والتدفق المنظم للبيانات: تدفق البيانات في الشبكة الحلقية يتم بطريقة منظمة، مما يقلل من ازدحام الشبكة.

الأداء المتوازن : يمكن توزيع الضغط على الشبكة بشكل متوازن بين جميع الأجهزة المتصلة.

مزايا الشبكة الحلقية:

عدم وجود تصادمات: لوجود تدفق موجه للبيانات عبر حلقة، لا توجد تصادمات بين الأجهزة كما في الشبكات الأخرى.

التحكم في حركة البيانات : يتم التحكم في حركة البيانات بشكل جيد من خلال استخدام الرمز(**Token**) أو ما شابه.

التنظيم الجيد : الشبكة الحلقية قادرة على توفير تدفق منظم وفعال للبيانات بين الأجهزة.

سهولة في إضافة أجهزة : تعتبر عملية إضافة جهاز جديد إلى الشبكة سهلة نسبيا, على الرغم انها تؤدي الى توقف الشبكة لحين اضافة الجهاز.

عيوب الشبكة الحلقية:

التعطل عند انقطاع أي جهاز أو الكابل : إذا حدث انقطاع في أي جزء من الشبكة (مثل الكابل أو جهاز)، يمكن أن يؤدي ذلك إلى توقف الشبكة بالكامل.

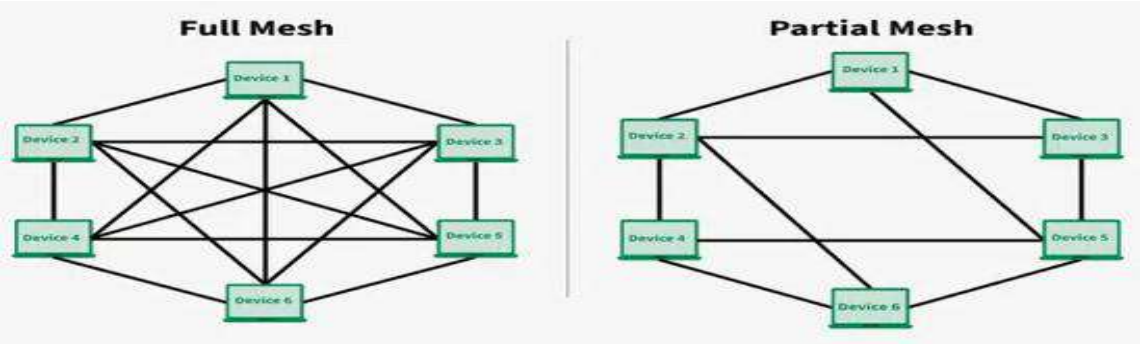
زيادة التأخير مع عدد الأجهزة : كلما زاد عدد الأجهزة في الشبكة، زاد الزمن الذي يستغرقه إرسال البيانات عبر الشبكة.

الصيانة المعقدة : في حالة حدوث مشكلة في الشبكة، قد يكون من الصعب تحديد مكان العطل، خاصة في الشبكات الكبيرة.

تكاليف إضافية : تتطلب الشبكة الحلقية بعض الأجهزة الخاصة مثل **Token Ring** ، مما قد يزيد من التكلفة.

4-5-1 الشبكة المتداخلة (Mesh Network) :

هي نوع من شبكات الحاسوب حيث يتم ربط كل جهاز في الشبكة مع الاجهزة الاخرى بشكل مباشر، مما يعني أن كل جهاز لديه اتصال مع الأجهزة الأخرى في الشبكة بكيبل خاص به. في هذا النوع من الشبكات، تكون البيانات قادرة على التنقل عبر أكثر من مسار، مما يسهم في تحسين استقرار الشبكة وتوفير خيارات متعددة لتوجيه البيانات. ومن انواعها الشبكة المتداخلة الكاملة (**Full Mesh**) في هذا النوع، كل جهاز متصل بكل جهاز آخر في الشبكة. والشبكة المتداخلة الجزئية (**Partial Mesh**) في هذا النوع، يتم ربط بعض الأجهزة ببعض، وليس جميع الأجهزة مرتبطة بكل الأجهزة الأخرى.



الشكل (1 – 19) يوضح نموذج الشبكة المتداخلة الكاملة و الجزئية

أهمية الشبكة المتداخلة :

التوافر المستمر : الشبكة المتداخلة تضمن اتصالاً موثوقًا حتى في حالة تعطل بعض الأجزاء، مما يجعلها مثالية للأنظمة الحساسة.
إعادة التوجيه التلقائي : توفر الشبكة مسارات بديلة تلقائيًا في حالة تعطل أحد المسارات، مما يحسن استقرار الشبكة.
المرونة : يمكن توسيع الشبكة بسهولة, وذلك بإضافة أجهزة جديدة دون التأثير الكبير في الشبكة الرئيسة

مزايا الشبكة المتداخلة

التوافر العالي : توفر مسارات متعددة لنقل البيانات، مما يضمن عدم توقف الشبكة حتى في حال حدوث مشكلة في جزء منها.
تحمل الأعطال : في حال تعطل أحد المسارات أو الأجهزة، يمكن للبيانات أن تستمر في الحركة عبر المسارات الأخرى.
الأداء العالي : لأنها تعتمد على نقل البيانات عبر مسارات متعددة، وتوفر أداءً جيدًا في الشبكات التي تحتوي على حركة مرور كثيفة.
الأمن العالي : نظرًا لتعدد المسارات، يصعب على المهاجمين أو المخترقين تعطيل الشبكة بسهولة.

عيوب الشبكة المتداخلة

التكلفة العالية : تركيب الشبكة المتداخلة يتطلب الكثير من الأسلاك أو الأجهزة الخاصة مثل أجهزة التوجيه (**Routers**) أو نقاط الاتصال، مما يجعل تكلفتها مرتفعة.
التعقيد في الإعداد والإدارة : بسبب العدد الكبير من التوصيلات والمسارات، يمكن أن تكون إدارة الشبكة المتداخلة معقدة.
استهلاك الطاقة والموارد : الشبكة المتداخلة تتطلب استهلاك طاقة أكبر مقارنة بالشبكات الأخرى بسبب الحاجة إلى مسارات متعددة.
التكلفة الباهظة في الشبكات الكاملة : في الشبكة المتداخلة الكاملة، حيث يتعين ربط كل جهاز مع كل جهاز آخر، قد يكون التنفيذ صعبًا ومكلفًا للغاية في الشبكات الكبيرة.

تمرين رقم 1 : التدريب على ربط كيبل من نوع (UTP)

الهدف من التمرين:

التدريب الطلاب على ربط كيبل من نوع (**UTP**)

المتطلبات الأساسية:

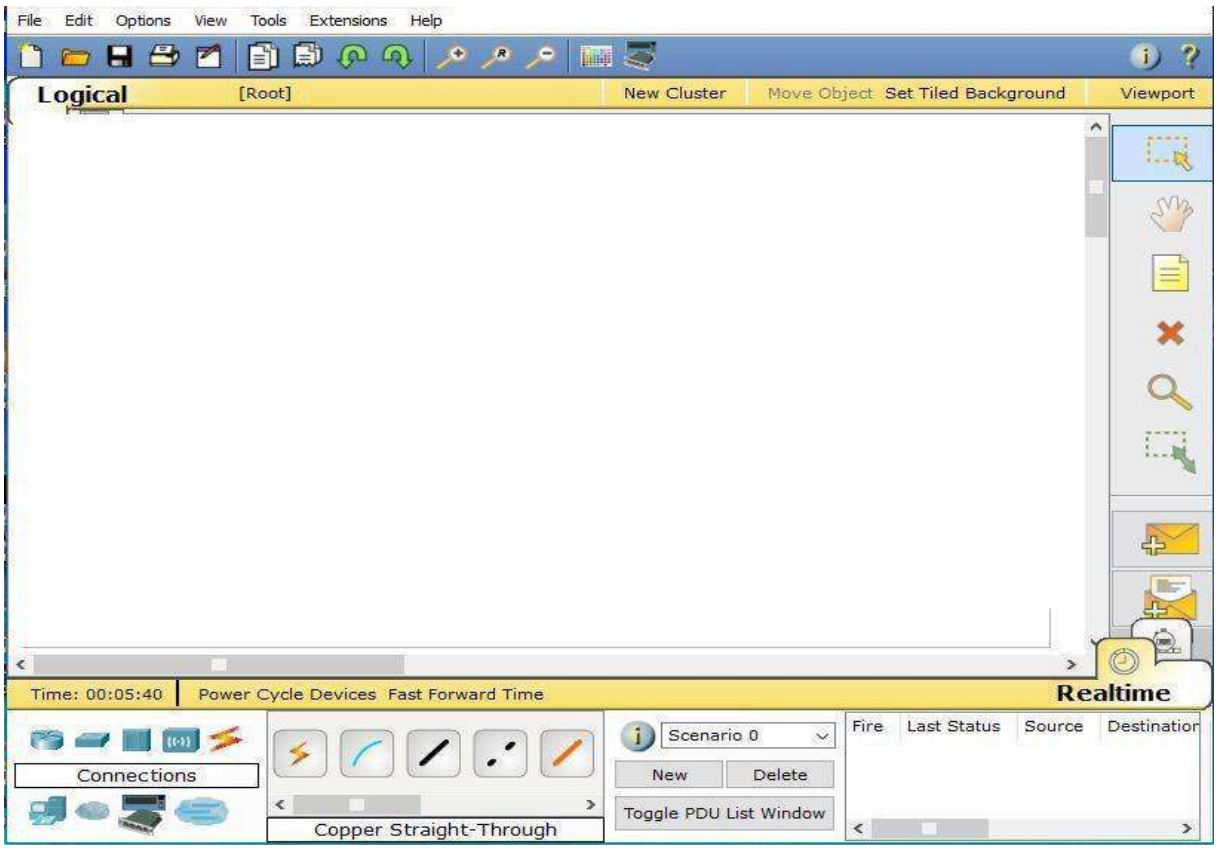
استخدام برنامج (**Cisco Packet Tracer**)

الخطوات العملية:

عزيزي الطالب اتبع الخطوات الآتية :

الخطوة 1: افتح **Cisco Packet Tracer**

قم بتشغيل برنامج .**Cisco Packet Tracer** , كما في الشكل (1-20).



الشكل (1-20)

الخطوة 2: اختيار الأجهزة المناسبة

من قائمة الأجهزة (**End Devices**)، قم بسحب جهازي حاسوب (**PC-0**) و (**PC-1**) إلى مساحة العمل.

من قائمة الشبكات (**Network Devices**) ، اختر مبدل (**Switch**) مثل 2960 .

اختيار نوع الكابل (**UTP - Straight Through**)

انقر على رمز الكابلات في أسفل الواجهة.

اختر كابل (**Copper Straight-Through**) يُستخدم للربط بين جهازين مختلفين، مثل **PC** إلى (**Switch**) .

الخطوة 3: توصيل الكابل بين الأجهزة

انقر على **PC-0** ثم اختر المنفذ **FastEthernet0** .

انقر على **Switch 2960** ثم اختر أي منفذ متاح مثل **FastEthernet** 0/1.

كرر العملية نفسها مع **PC-1** وقم بتوصيله بمنفذ آخر على الـ (**Switch**) مثل **FastEthernet** (0/2).

الخطوة 4: قم بتعيين عنوان **IP** لكل جهاز باستخدام الأمر:

PC-0: 192.168.1.1

PC-1: 192.168.1.2

الخطوة 5: اختبار الاتصال باستخدام الأمر **Ping**

انقر على **PC-0** ثم **Desktop** > **Command Prompt** .

الخطوة 6: عبر الذهاب إلى **IP Configuration** في كل جهاز.

اختبر الاتصال من **PC-0** إلى **PC-1** عبر تنفيذ الأمر الآتي في الـ **Command Prompt**:

ping 192.168.1.2

إذا كان الاتصال ناجحًا، سترى ردود (**Reply**) ، مما يعني أن الكابل **UTP** تم توصيله بنجاح.

النتيجة المتوقعة

بعد تنفيذ هذا التمرين سيكون الطلبة قادرين على ربط كيبل من نوع (**UTP**)

استمارة الفحص تمرين رقم (1)				
الجهة الفاحصة:				
اسم الطالب :	**المرحلة الثالثة**	**التخصص : الامن السيبراني**		
اسم التمرين : التدريب على ربط كيبل من نوع (UTP)				
ت	**الخطوات**	**الدرجة القياسية % 50**	**درجة الاداء %50**	**الملاحظات**
1	الدخول الى برنامج Cisco Packet Tracer	%5		
2	اختيار الأجهزة المناسبة	%5		
3	توصيل الكابل بين الأجهزة	%5		
4	تعيين عنوان IP لكل جهاز	%5		
5	اختبار الاتصال باستخدام الأمر Ping	%5		
6	اختبار الاتصال عبر تنفيذ الأمر Command Prompt	%5		
7	المناقشة	%10		
8	الزمن المخصص	%10		
المجموع				
اسم الفاحص		**التوقيع**		

تمرين رقم 2 : تعريف نوع الشبكة التي تستخدمها في منزلك أو مكتبك (LAN ، WLAN، ..... إلخ) وشرح المكونات المستخدمة فيها.

الهدف من التمرين:

تدريب الطلاب على تنفيذ محاكاة شبكة منزلية وتحديد نوع الشبكة سواء كانت شبكة محلية سلكية (**LAN**) او شبكة لاسلكية (**WLAN**) , مع شرح المكونات المستخدمة فيها وكما يأتي :-

- محاكاة شبكة **LAN** في **Packet Tracer**
- تحديد نوع الشبكة
  - **LAN (Local Area Network)** شبكة سلكية تعتمد على كابلات **UTP** للاتصال بين الأجهزة عبر **Switch** أو **Router** .
  - **WLAN (Wireless Local Area Network)** شبكة لاسلكية تعتمد على موجه لاسلكي (**Wireless Router**) بدلاً من الكابلات.

المتطلبات الاساسية:

استخدام برنامج (**Cisco Packet Tracer**)

الخطوات العملية:

عزيزي الطالب اتبع الخطوات الآتية :

خطوات تنفيذ الشبكة السلكية في **Packet Tracer**

الخطوة 1: افتح برنامج **Packet Tracer**.

اسحب من **End Devices** ثلاثة أجهزة حاسوب (**PC-0, PC-1, PC-2**) .

من **Network Devices**، اسحب **Switch** 2960 و **Router** 1941 .

اختر كابل **Straight-Through** وقم بتوصيل الأجهزة كما يأتي:

PC-0 → Switch (Fa0/1)

PC-1 → Switch (Fa0/2)

PC-2 → Switch (Fa0/3)

Switch → Router (Fa0/0)

الخطوة 2: اضبط عناوين **IP** للأجهزة عبر **IP Configuration** داخل كل **PC** .

اختبر الاتصال باستخدام **Ping** بين الأجهزة.

الخطوة 3: محاكاة شبكة **WLAN** في **Packet Tracer** :

المكونات المستخدمة في الشبكة اللاسلكية (**WLAN**)

- جهاز توجيه لاسلكي – (**Wireless Router - Linksys**) يوفر اتصال **Wi-Fi**.
- أجهزة لاسلكية – (**Laptop, Smartphone, Tablet**) تتصل عبر **Wi-Fi**.
- (خادم - **Server**) اختياري – يستخدم للمشاركة عبر الشبكة.

خطوات تنفيذ الشبكة اللاسلكية في **Packet Tracer** :

الخطوة 1: افتح **Packet Tracer**.

اسحب من **Network Devices** جهاز **Wireless Router (Linksys)**.

اسحب من **End Devices Laptop, Smartphone, Tablet**.

انقر على **PC Wireless** → **Desktop** → **Laptop**، ثم اختر الشبكة اللاسلكية الخاصة بالموجه.

ملاحظة: في حالة **Laptop** فان **Packet Tracer** عادة لا تتضمن **Wireless NIC** وانما فقط **Wired NIC** لذا من اجل ضمان الربط المباشر من ال(**Wireless Router**) تتطلب اضافة كارد واير ليس بدل الواير الى جهاز **Laptop**

الخطوة 2: تحقق من الاتصال الصحيح وضبط عناوين.**IP**

استخدم **Ping** لاختبار الاتصال بين الأجهزة المتصلة بالشبكة اللاسلكية.

النتيجة المتوقعة

بعد تنفيذ هذا التمرين سيكون الطلبة قادرين على تنفيذ محاكاة شبكة منزلية وتحديد نوع الشبكة سواء كانت شبكة محلية سلكية (**LAN**) او شبكة لاسلكية (**WLAN**) , بالاضافة الى التعرف على المكونات المستخدمة فيها .

استمارة الفحص تمرين رقم (2)				
الجهة الفاحصة:				
اسم الطالب :	**المرحلة الثالثة**		**التخصص : الامن السيبراني**	
اسم التمرين : تعريف نوع الشبكة التي تستخدمها في منزلك أو مكتبك (LAN ، WLAN، ..... إلخ) وشرح المكونات المستخدمة فيها.				
ت	**الخطوات**	**الدرجة القياسية % 50**	**درجة الاداء %50**	**الملاحظات**
خطوات تنفيذ الشبكة السلكية في برنامج Packet Tracer				
1	**الدخول الى برنامج Cisco Packet Tracer**	**%6**		
2	**ضبط عناوين IP للأجهزة**	**%6**		
3	**محاكاة شبكة WLAN في Packet Tracer**	**%6**		
خطوات تنفيذ الشبكة اللاسلكية في برنامج Packet Tracer				
5	**الدخول الى برنامج Cisco Packet Tracer**	**%6**		
6	**التأكد من الاتصال الصحيح وضبط عناوين IP**	**%6**		
7	**المناقشة**	**%10**		
8	**الزمن المخصص**	**%10**		
المجموع				
اسم الفاحص		**التوقيع**		

تمرين رقم 3 : تصميم شبكة محلية (LAN) من خلال توصيل جهازين عبر كبل (Ethernet)

الهدف من التمرين:

تدريب الطلاب على تصميم شبكة محلية (**LAN**) عبر توصيل جهازين باستخدام كابل (**Ethernet**) داخل برنامج (**Cisco Packet Tracer**) ، ثم التحقق من الاتصال بينهما باستخدام الأمر (**ping**) .

المتطلبات الأساسية:

- استخدام برنامج (**Cisco Packet Tracer**)
- جهازا كمبيوتر – (**PC-0, PC-1**) يمثلان الأجهزة في الشبكة.
- كابل (**Ethernet Copper Cross-Over**) أو (**Straight-Through**) لتوصيل الأجهزة.
- عنوان **IP** لكل جهاز لضمان الاتصال عبر الشبكة.

الخطوات العملية:

عزيزي الطالب اتبع الخطوات الآتية لتنفيذ التمرين في **Packet Tracer**

الخطوة 1: فتح **Packet Tracer** وإضافة الأجهزة .

افتح برنامج **Cisco Packet Tracer.**

من قائمة **End Devices**، اسحب جهازي كمبيوتر (**PC-0**) و (**PC-1**) إلى مساحة العمل.

الخطوة 2: توصيل الأجهزة باستخدام كابل **Ethernet**

اضغط على رمز الكابلات أسفل الواجهة.

اختر كابل (**Copper Cross-Over**) لأننا نربط جهازين مباشرة، وإذا استخدمنا (**Switch**) ، سنستخدم (**Straight-Through**) .

قم بتوصيل الكابل بين :

PC-0 منفذ (**FastEthernet0**) → **PC-1** منفذ (**FastEthernet0**)

الخطوة 3: ضبط عناوين **IP** لكل جهاز

انقر على **PC-0** ، ثم انتقل إلى **Desktop → IP Configuration.**

اضبط عنوان **IP** كما يأتي :

PC-0 :

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

PC-1 :

IP Address : 192.168.1.2

Subnet Mask : 55.255.255.0

أغلق النافذة بعد ضبط الإعدادات.

الخطوة 4: اختبار الاتصال بين الجهازين

انقر على **PC-0** ، ثم **Desktop → Command Prompt.**

أدخل الأمر الآتي لاختبار الاتصال مع **PC-1**:

Ping 192.168.1.2

إذا تم التوصيل بنجاح، سترى رسائل Reply، مما يعني أن الجهازين متصلان بشكل صحيح عبر كابل **Ethernet**.

ملاحظات مهمة:

- ✓ تحقق من استخدام كابل **Cross-Over** عند توصيل جهازين بدون Switch .
- ✓ استخدم كابل **Straight-Through** عند التوصيل عبر **Switch**.
- ✓ تحقق من أن **Subnet Mask** موحد بين الجهازين لتجنب مشاكل الاتصال.

نشاط

حاول توسيع الشبكة بإضافة **Switch** أو **Router** لاحقًا لربط مزيد من الأجهزة.

النتيجة المتوقعة

بعد تنفيذ هذا التمرين سيكون الطلبة قادرين على تصميم شبكة محلية (**LAN**) عبر توصيل جهازين باستخدام كابل (**Ethernet**) داخل برنامج (**Cisco Packet Tracer**) ، ثم التحقق من الاتصال بينهما باستخدام الأمر (**ping**) .

استمارة الفحص تمرين رقم (3)			
الجهة الفاحصة:			
اسم الطالب :	**المرحلة الثالثة**	**التخصص : الامن السيبراني**	
اسم التمرين : تصميم شبكة محلية (LAN) من خلال توصيل جهازين عبر كبل (Ethernet)			
ت	**الخطوات**	**الدرجة القياسية % 50**	**درجة الاداء %50**	**الملاحظات**
1	الدخول الى برنامج Cisco Packet Tracer	%5		
2	توصيل الأجهزة باستخدام كابل Ethernet	%10		
3	ضبط عناوين IP لكل جهاز	%5		
4	اختبار الاتصال بين الجهازين	%10		
7	المناقشة	%10		
8	الزمن المخصص	%10		
المجموع				
اسم الفاحص		**التوقيع**		

تمرين رقم 4 : استخدام اداة مثل (Wireshark) لمرقبة حركة البيانات في الشبكة المحلية

الهدف من التمرين:

تدريب الطلبة على القيام بمحاكاة بيئة شبكة **LAN** داخل **Cisco Packet Tracer**، وباستخدام أداة تحليل الحزم **(Wireshark)** أو ما يُعادلها داخل **(Packet Tracer)** لمراقبة حركة البيانات بين الأجهزة.

المتطلبات الأساسية:

- برنامج **(Cisco Packet Tracer)**
- جهازا كمبيوتر **(PC-0, PC-1)** لتمثيل الأجهزة المتصلة بالشبكة.
- مبدل **(Switch-2960)** لتوصيل الأجهزة داخل الشبكة.
- كابل **Ethernet (Straight-Through)** لربط الأجهزة بالمبدل.
- أداة **Simulation Mode** بديل **Wireshark** في **(Packet Tracer)** لمراقبة الحزم داخل الشبكة.

الخطوات العملية:

عزيزي الطالب اتبع الخطوات الآتية لتنفيذ التمرين في **Packet Tracer**

الخطوة 1: إنشاء الشبكة في **Packet Tracer**

افتح **Packet Tracer**.

اسحب جهازي كمبيوتر **(PC-0)** و **(PC-1)** من قائمة **End Devices** إلى مساحة العمل.

اسحب **Switch 2960** من قائمة **Network Devices** .

اختر كابل **Copper Straight-Through** وقم بتوصيل الأجهزة كما يأتي :

PC-0 → Switch (Fa0/1)

PC-1 → Switch (Fa0/2)

الخطوة 2: ضبط عناوين **IP** لكل جهاز

انقر على **PC-0** ، ثم انتقل إلى **Desktop → IP Configuration**.

اضبط عنوان **IP** كما يأتي:

PC-0:

IP Address: 192.168.1.1

Subnet Mask : 255.255.255.0

PC-1:

IP Address : 192.168.1.2

Subnet Mask : 255.255.255.0

الخطوة 3: تفعيل مراقبة الشبكة **(Packet Sniffing)**

انتقل إلى **Simulation Mode** اضغط على زر **Simulation** في أسفل **(Packet Tracer)** .

في نافذة المحاكاة، انقر على **Edit Filters** واختر **ICMP** فقط لرؤية حزم اختبار الاتصال **(Ping)** . انقر على **Capture/Forward** لبدء مراقبة الحزم.

الخطوة 4: تنفيذ اختبار الاتصال ورؤية الحزم

انتقل إلى **PC-1→ Desktop → Command Prompt**

اكتب الأمر الآتي لاختبار الاتصال مع **PC-1**:

Ping 192.168.1.2

في **Simulation Mode**، ستلاحظ تدفق الحزم بين الجهازين.

انقر على أي حزمة في جدول المحاكاة لرؤية تفاصيلها (المصدر، الوجهة، نوع البروتوكول).

ملاحظات مهمة:

- ✓ ان **Wireshark** غير مدمج داخل **Packet Tracer** ، لذا يمكن ان نستخدام **Mode Simulation** بديلا لرؤية الحزم.
- ✓ يمكنك إضافة جهاز **Router** لتوسيع التمرين وتحليل بروتوكولات أخرى مثل **TCP** و **HTTP** .

النتيجة المتوقعة

بعد تنفيذ هذا التمرين سيكون الطلبة قادرين على القيام بمحاكاة بيئة شبكة **LAN** داخل **Cisco Packet Tracer** ، باستخدام أداة تحليل الحزم **(Simulation Mode)** داخل **(Packet Tracer)** لمراقبة حركة البيانات بين الأجهزة.

استمارة الفحص تمرين رقم (4)			
الجهة الفاحصة:			
اسم الطالب :	**المرحلة الثالثة**	**التخصص : الامن السيبراني**	
اسم التمرين : استخدام اداة مثل (Wireshark) لمرقبة حركة البيانات في الشبكة			
ت	**الخطوات**	**الدرجة القياسية % 50**	**درجة الاداء %50**	**الملاحظات**
1	الدخول الى برنامج Cisco Packet Tracer وإنشاء الشبكة في Packet Tracer	%10		
2	ضبط عناوين IP لكل جهاز	%10		
3	تفعيل مراقبة الشبكة (Packet Sniffing)	%5		
4	تنفيذ اختبار الاتصال ورؤية الحزم	%5		
7	المناقشة	%10		
8	الزمن المخصص	%10		
المجموع				
اسم الفاحص		**التوقيع**		

تمرين رقم 5 : تنفيذ مخطط شبكي يوضح اتصال الأجهزة في شبكة نجمية (Star Network)

الهدف من التمرين:

تدريب الطلبة على القيام بتصميم شبكة نجمية (**Star Network**) داخل **Cisco Packet Tracer**، حيث تكون جميع الأجهزة متصلة بمبدل (**Switch**) يعد المركز الرئيسي للاتصال.

المتطلبات الأساسية:

- برنامج (**Cisco Packet Tracer**)
- جهاز مبدل (**Switch-2960**) ليكون نقطة الاتصال المركزية.
- أجهزة كمبيوتر (**PC-0**) , (PC-1) , (PC-2) , (PC-3) , (PC-4) , تمثل الأجهزة المتصلة بالشبكة.
- كابلات **Ethernet (Copper Straight-Through)** لربط الأجهزة بالمبدل.
- عناوين **IP** لكل جهاز لضمان الاتصال داخل الشبكة.

الخطوات العملية:

عزيزي الطالب اتبع الخطوات الآتية لتنفيذ التمرين في **Packet Tracer**

الخطوة 1: إنشاء الشبكة النجمية في **Packet Tracer**

افتح **Packet Tracer**.

من قائمة **End Devices**، اسحب خمسة أجهزة كمبيوتر (**PC-0**) إلى (**PC-4**) إلى مساحة العمل.

من قائمة **Network Devices**، اسحب **Switch** 2960 وضعه في المنتصف.

الخطوة 2: توصيل الأجهزة بالمبدل (**Switch**)

اختر أداة الكابلات في الأسفل.

حدد كابل **Copper Straight-Through**

قم بتوصيل الأجهزة كما يأتي:-

PC-0 → **Switch** (**Fa0**/1)

PC-1 → **Switch** (**Fa0**/2)

PC-2 → **Switch** (**Fa0**/3)

PC-3 → **Switch** (**Fa0**/4)

PC-4 → **Switch** (**Fa0**/5)

الآن ، جميع الأجهزة متصلة بالمبدل، مما يشكل هيكل الشبكة النجمية.

الخطوة 3: ضبط عناوين **IP** لكل جهاز

انقر على **PC**-0، ثم انتقل إلى **Desktop** → **IP Configuration**.

اضبط عنوان **IP** كما يأتي لكل جهاز:

PC-0:

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

PC-1:

IP Address : 192.168.1.2

: 255.255.255.0 **Subnet Mask**

PC-2:

: 192.168.1.3 **IP Address**

: 255.255.255.0 **Subnet Mask**

PC-3:

: 192.168.1.4 **IP Address**

: 255.255.255.0 **Subnet Mask**

PC-4:

: 192.168.1.5 **IP Address**

: 255.255.255.0 **Subnet Mask**

الخطوة 4: اختبار الاتصال بين الأجهزة

انتقل إلى **PC-0 → Desktop → Command Prompt**.

استخدم الأمر الآتي لاختبار الاتصال مع **PC**-3:

Ping 192.168.1.4

إذا كان الإعداد صحيحًا، ستظهر رسائل **Reply** ، مما يؤكد نجاح الاتصال.

كرر الاختبار مع بقية الأجهزة للتحقق من أن الشبكة تعمل بشكل سليم .

ملاحظات مهمة:

- ✓ الشبكة النجمية تتميز بوجود نقطة مركزية المبدل **(Switch)** ، مما يسهل إدارة الشبكة وزيادة الكفاءة.
- ✓ في حالة فشل أحد الأجهزة، لا تتأثر باقي الأجهزة بالشبكة.
- ✓ إذا تعطل **Switch** ، تتوقف الشبكة عن العمل بالكامل.

استنتاج

في هذا التمرين، قمنا بتنفيذ تصميم شبكة نجمية **(Star Network)** باستخدام **Packet Tracer** .
جميع الأجهزة متصلة بمبدل **(Switch)** يعد المركز الرئيسي، مما يضمن اتصالًا فعالًا وسهل الإدارة.

النتيجة المتوقعة

بعد تنفيذ هذا التمرين سكون الطلبة قادرون على القيام بتصميم شبكة نجمية **(Star Network)** داخل **Cisco Packet Tracer** ، حيث تكون جميع الأجهزة متصلة بمبدل **(Switch)** هو المركز الرئيسي للاتصال.

استمارة الفحص تمرين رقم (5)			
الجهة الفاحصة:			
اسم الطالب : المرحلة الثانية التخصص : الامن السيبراني			
اسم التمرين : تنفيذ مخطط شبكي يوضح اتصال الأجهزة في شبكة نجمية (Star Network)			
ت	الخطوات	الدرجة القياسية % 50	درجة الاداء %50	الملاحظات
1	الدخول الى برنامج Cisco Packet Tracer و إنشاء الشبكة النجمية في Packet Tracer	%10		
2	توصيل الأجهزة بالمبدل (Switch)	%5		
3	ضبط عناوين IP لكل جهاز	%10		
4	اختبار الاتصال بين الأجهزة	%5		
7	المناقشة	%10		
8	الزمن المخصص	%10		
المجموع				
اسم الفاحص		التوقيع		

أسئلة الفصل الأول

س1: اختر العبارة الصحيحة:

1. أي من الأجهزة الآتية يُستخدم لتوجيه البيانات بين الشبكات المختلفة؟
Repeater (D) Router (C) Switch (B) Hub (A)

2. أي من الأجهزة الآتية يعمل على توزيع البيانات إلى جميع الأجهزة المتصلة به دون تمييز؟
Firewall (D) Hub (C) Switch (B) Router (A)

3. أي من الوسائط الآتية يوفر أسرع نقل للبيانات؟
Bluetooth (D) Wi-Fi (C) الألياف الضوئية (B) Ethernet كابلات (A)

4. أي من التقنيات الآتية تُستخدم في الشبكات اللاسلكية؟
Coaxial Cable (D) Wi-Fi (C) الألياف الضوئية (B) Ethernet كابلات (A)

5. أي نوع من الشبكات يُستخدم عادة داخل مبنى واحد؟
VPN (D) WAN (C) MAN (B) LAN (A)

6. أي نوع من الشبكات يُغطي مدينة أو منطقة جغرافية واسعة؟
VPN (D) WAN (C) MAN (B) LAN (A)

7. أي من الطوبوغرافيات الآتية تعتمد على جهاز مركزي لإدارة الاتصال بين الأجهزة؟
Mesh (D) Star (C) Ring (B) Bus (A)

8. أي من الطوبوغرافيات تكون تكلفتها منخفضة؟
Mesh (D) Star (C) Ring (B) Bus (A)

9. أي من الطوبوغرافيات توفر أكثر من مسار واحد للبيانات، مما يجعلها الأكثر موثوقية؟
Mesh (D) Star (C) Ring (B) Bus (A)

10. أي من الطوبوغرافيات الآتية يُستخدم في شبكات الإنترنت لتوفير اتصال متعدد المسارات؟
Mesh (D) Star (C) Ring (B) Bus (A)

س2: كيف يمكن أن تؤثر شبكات الحاسوب في بيئة العمل داخل المؤسسات؟ وهل هناك سلبيات محتملة؟

س3: في ظل تطور تقنيات الاتصال، هل تعتقد أن الشبكات السلكية ستختفي مستقبلاً بسبب الشبكات اللاسلكية؟ ولماذا؟

س4: إذا كنت مسؤولًا عن تصميم شبكة لمؤسسة تحتوي على (500) موظف، فهل ستعتمد على أجهزة **Switch** أم **Router** بشكل أساسي؟ ولماذا؟

س5: لماذا قد تفضل استخدام الألياف الضوئية بدلاً من الكابلات النحاسية في بعض أنواع الشبكات، على الرغم من أن تكلفتها أعلى؟

س6: ما العوامل التي يجب أخذها في الاعتبار عند اختيار نظام تشغيل لشبكة مؤسسة كبيرة؟

س7: كيف يمكن لبرمجيات إدارة الشبكة أن تساعد على تحسين أمان البيانات؟

س8: ما العوامل التي تحدد اختيار نوع الشبكة (**LAN, MAN, WAN**) عند إنشاء شبكة جديدة؟

س9: في رأيك، هل يمكن أن تحل شبكات **WAN** محل أنواع أخرى من الشبكات مستقبلاً؟ ولماذا؟

س10: إذا كنت تخطط لإنشاء شبكة منزلية ذكية، فهل تعتمد على شبكة سلكية أم لاسلكية؟ ولماذا؟

س11: لماذا قد تختار شبكة نجمية (**Star Network**) بدلاً من شبكة خطية (**Bus Network**) في مؤسسة تجارية؟

س12: إذا كنت تصمم شبكة لإنترنت الأشياء (**IoT**) في مدينة ذكية، فهل تعتمد على شبكة متداخلة (**Mesh**) أو شبكة نجمية (**Star**) ؟ ولماذا؟

الفصل الثاني
اساسيات امن الشبكات

الهدف العام

تعليم الطالب أساسيات امن الشبكات

الأهداف الخاصة

ان يكون الطالب قادرا على:-

- ❖ استيعاب مفهوم أمن الشبكات وأهداف الأمان
- ❖ التعرف على مفهوم التهديدات الامنية
- ❖ التعرف على الفيروسات الالكترونية وانواعها
- ❖ التعرف على مفهوم الهجمات السيبرانية
- ❖ التعرف على بعض تقنيات الامان الاساسية
- ❖ التعرف على اهم انواع بروتوكولات الامان الاساسية
- ❖ التعرف على بعض أساليب الهجوم والوقاية

..::: مفردات الفصل :::..

1-2 مفهوم أمن الشبكات
- أهداف الأمان: السرية، النزاهة، التوفر

2-2 التهديدات الأمنية

3-2 الفيروسات ، الهجمات السيبرانية
- تقنيات الأمان الأساسية
- الجدران النارية (Firewall)
- التشفير
- تحديد الهوية والمصادقة والتفويض

4-2 بروتوكولات الأمان الأساسية
- TLS / SSL
- IPsec
- HTTPs
- WPA2 / WPA / WEP

5-2 أساليب الهجوم والوقاية
- الهجمات DDoS ، الهجمات الخفية
- الوقاية : IPS / IDS ، VPN

التمارين العملية:
- ➢ تمرين :1 إعداد جدار ناري بسيط باستخدام جهازك
- ➢ تمرين :2 تجربة تقنيات التشفير باستخدام أداة مثل OpenSSL لتشفير وفك تشفير الملفات .
- ➢ تمرين : 3 تكوين شبكة خاصة افتراضية VPN
- ➢ تمرين :4 استخدام أداة Wireshark لاكتشاف حركة البيانات المشبوهة في الشبكة

الفصل الثاني
اساسيات امن الشبكات

1-2 مفهوم أمن الشبكات (Network Security)

تعرفنا عزيزي الطالب في الفصل السابق على المبادئ الاساسية لشبكات الحاسوب , والتي تضمنت مفهوم شبكات الحاسوب ومكوناتها وانواعها وطبوغرافياتها , وتعرفنا ايضا على ان شبكات الحاسوب تتنوع وتختلف تبعا للمسافات التي تخطيها , ومن الجدير بالذكر ان ننوه هنا بأن هنالك جملة من المخاطر الامنية التي تترافق مع هذه شبكات , هذه المخاطر تتنوع وتتزايد باستمرار مع زيادة استخدام والاعتماد عليها خصوصا في التعاملات الالكترونية التي تجري عبرها ، مما يجعل من الضروري تطبيق حلول أمنية رصينة للحفاظ عليها . سنتعرف في هذا الفصل على بعض المفاهيم والممارسات الخاصة بأساسيات امن الشبكات . و احدى اهم هذه المفاهيم الاساسية في هذا المجال هو امن الشبكات **(Network Security)** .

ان امن الشبكات هي مجموعة من التدابير الوقائية اللازمة لحماية البيانات المتداولة عبر الشبكات وسلامتها واستمرارية تدفقها سواء كانت (شبكات محلية **(LAN)** أو شبكات واسعة **(WAN)** او حتى شبكة الإنترنت) من التهديدات الداخلية والخارجية , وذلك من خلال استخدام مجموعة من الأدوات والتقنيات المختلفة والمصممة لحماية البنى التحتية للشبكات وسلامتها وقابليتها للاستخدام , بحيث تضمن إنشاء بنية أساسية آمنة للأجهزة والتطبيقات والمستخدمين والبرامج لأداء وظائفهم الحيوية المسموح بها في بيئة آمنة ,ان المبادئ الأساسية لأمن الشبكة تتلخص فيما يأتي :-

1- **الوقاية :** هي عملية تنفيذ مجموعة من التدابير اللازمة لمنع الهجمات الإلكترونية والوصول غير المصرح به للشبكة . مثل استخدام جدران الحماية وبرامج مكافحة الفيروسات وآليات التحكم في الوصول.
2- **الكشف :** هي عملية مراقبة حركة مرور الشبكة لاكتشاف الأنشطة المشبوهة والتهديدات المحتملة فيها , ويتم ذلك من خلال استخدم أنظمة مصممة لهذا الغرض مثل نظام الكشف عن التسلل **(IDS Intrusion Detection System)** وأدوات التحليلات السلوكية .
3- **الاستجابة :** هي عملية اتخاذ الإجراءات المناسبة للتخفيف من تأثير التهديدات المكتشفة . ويتم ذلك بحظر حركة المرور الضارة وعزل الأجهزة المخترقة وتطبيق التصحيحات أو التحديثات.

و يشمل امن الشبكة نطاقا واسعا لكثير من الموضوعات , مثل التشفير والتوثيق ومختلف السياسات الأمنية الاخرى التي تعد نقطة البداية لتحقيق بنية تحتية قوية وآمنة تساهم في التقليل من مخاطر فقدان البيانات والسرقة والتخريب , ويمكن تصنيف أمان الشبكة الى ثلاثة عناصر تحكم مختلفة :

1- **أمان الشبكة المادية** : صممت ضوابط الأمن المادي لمنع الأفراد غير المصرح لهم من الوصول المادي إلى مكونات الشبكة مثل أجهزة التوجيه وخزائن الكابلات وما إلى ذلك.
2- **أمن الشبكة التقنية** : تحمي ضوابط الأمان الفنية البيانات المخزنة على الشبكة أو التي يتم نقلها عبر الشبكة أو داخلها أو خارجها.

3- أمن الشبكة الإدارية : تتكون ضوابط الأمان الإدارية من سياسات وعمليات الأمان التي تتحكم في سلوك المستخدم ، بما في ذلك كيفية مصادقة المستخدمين ، ومستوى وصولهم.

أهداف الأمان : السرية ، النزاهة ، التوفر

تتلخص أهداف الأمان في ثلاثة مفاهيم أساسية هي (السرية والنزاهة والتوافر) , حيث تعمل هذه المبادئ كإطار عمل لحماية البيانات والتأكد من معالجتها بشكل صحيح . وترتبط هذه المفاهيم بعضها ببعض بطرق متعددة ، وتعمل معًا لتحقيق الإطار الشامل لأمان الشبكات. ولذا يجب ان نميز بينها , وفيما يأتي وصفا مختصرا لما تعنيه هذه المفاهيم :

السرية (Confidentiality) : وتعني حماية البيانات من السرقة والمحافظة على سريتها وخصوصيتها وضمان الوصول إليها للأفراد أو الأجهزة المصرح لهم فقط.

النزاهة (Integrity) : وتعني الحفاظ على سلامة البيانات بشكلها الاصلي وحمايتها, وعدم تغييرها أو العبث بها بأي شكل من الأشكال مثل التعديل أو الحذف أو التلاعب غير المصرح به.

التوفر (Availability) : وتعني ضمان إمكانية الوصول إلى البيانات وبقائها متاحة وجاهزة للاستخدام دون انقطاع أو رفض عند الحاجة إليها في الوقت المناسب وبطريقة موثوق بها .

2-2 التهديدات الأمنية

ويقصد بالتهديدات الأمنية للشبكات المحاولات أو الافعال التي يمكن أن تلحق ضررا بالاجهزة والمكونات المادية للشبكات أو بالمعلومات المخزونة عليها , مثل محاولات تعطيل الأجهزة وإيقافها عن العمل أو محاولات سرقة المعلومات والعبث بها . وهذه التهديدات تنتج عادة عن هجمات البرامج الضارة أو الأخطاء البشرية التي يستغلها مجموعة من الأشخاص السيئين يطلق عليهم (القراصنة او الهكر) , وذلك لغرض السرقة أو التخريب أو الابتزاز .

في الفضاء الرقمي تعتبر الفيروسات والهجمات السيبرانية من اهم التهديدات الأمنية التي تصيب الشبكات والانترنت ، مما يتطلب استخدام تدابير أمنية معينة للتخفيف والوقاية منها اومنعها .

1-2-2 الفيروسات (Viruses)

تعتبر الفيروسات من التهديدات الرئيسية التي تشكل خطراً على أمن الشبكات , إذ تستطيع هذه الفيروسات من تدمير البرامج وأنظمة شبكات الحاسوب بشكل كامل . والفيروسات هي عبارة عن كائنات برمجيّة ضارةٌ يتم تحميلها على اجهزة الحاسوب دون علم المستخدم ، الغرض منها إصابة الأنظمة الحاسوبية ، والتحكُّم فيها . تقوم هذه الكائنات بتنفيذ إجراءات ضارة مثل التكرار الذاتي بنسخ نفسه وبشكل متكرر , وتقوم الفيروسات بتنفيذ عملية النسخ الذاتي بطريقتين الأولى بمجرد وصولها إلى جهاز حاسوب جديد يبدأ في عملية نسخ نفسه. والطريقة الثانية يبقى الفيروس ساكناً حتى يقوم المستخدم بتشغيل البرنامج المصاب عندها يبدأ بالعمل . وهنالك عدة طرق لانتشارها, مثلا عن طريق فتح الملفات المرفقة لرسائل البريد الإلكتروني ، أوعند زيارة موقع ويب مصاب بهذه الفيروسات ، أو عند مشاهدة إعلانات غير موثوقة المصدر، أوعند استخدام أدوات التخزين القابلة للإزالة التي تكون مصابة بالفيروس مثل الأقراص المدمجة او الفلاش , وغيرها من الطرق . هذا وقد تكون الفيروسات قابله للاكتشاف من خلال الشعور او التحسس ببعض العلامات الشائعة لفقدان الأداء ، وفيما يأتي بعض الحالات التي تدل على وجود الفيروسات :-

1. البطء في سرعة نظام الحاسوب
2. ظهور النوافذ المنبثقة غير المرغوب فيها .

3. انغلاق برامج الحاسوب بشكل غير متوقع من تلقاء نفسها
4. عمل جهاز الحاسوب بعدة طرق غريبة ، والتي قد تشمل فتح الملفات من تلقاء نفسها .
5. عرض رسائل خاطئة غير عادية .
6. النقر فوق المفاتيح بشكل عشوائي .

وفيما يأتي اهم الانواع الشائعة من الفيروسات التي تصنف بحسب الوظيفة المصمَّمة للقيام بها :-

1. الفيروس المقيم :(**Resident Virus**)
2. الفيروس متعدد الأطراف :(**Multipartite Virus**)
3. فيروس التنفيذ المباشر :(**Direct Action Virus**)
4. فيروس اختطاف المتصفح :(**Browser Hijacker**)
5. فيروس الكتابة :(**Overwrite Virus**)
6. فيروس أكواد الويب البرمجية : (**Web Scripting Virus**)
7. الفيروس المرافق :(**Companion Virus**)
8. فيروس الشبكة :(**Network Virus**)

وهنالك مجموعة اخرى من البرامج الضارة التي لا تُسمَّى بالفيروسات، ولكن لها نفس التأثيرات الضَّارة للفيروسات، ويشمل ذلك البرامج الدودية ، والبرامج الدعائية ، وبرامج الفدية . وهنالك مجموعة من البرامج التي تستخدم لمنع هذه الفيروسات من التأثير في جهاز الحاسوب والشبكات ، تسمى برامج مكافحة الفيروسات التي يمكنها اكتشاف جميع أنواع هذه الفيروسات وحظرها والقضاء عليها.

2-2-2 الهجمات السيبرانية

في عصر التطور التكنولوجي أصبحت التهديدات السيبرانية والهجمات الإلكترونية الموجهة ضد للأفراد والمؤسسات تمثل التحديً الأكثر تعقيدًا على المستويين الدولي والإقليمي . والهجمات السيبرانية هي مجموعة من الأنشطة التي تنطوي على مخاطر وأضرار يواجهها مستخدمو الشبكات والإنترنت بشكل عام , وهذه المخاطر عادة ما تستهدف تعطيل الانظمة والشبكات الحاسوبية أو الوصول غير المصرح به إلى البيانات والمعلومات المسجلة عليها , وتتلخص اسباب الهجمات السيبرانية فيما يلي:-

1. السرقة المالية
2. التجسس الصناعي
3. التخريب والتدمير
4. الابتزاز
5. الدوافع السياسية
6. الانتقام الشخصي

تتم هذه الهجمات عادةً عبر الإنترنت باستخدام وسائل متعددة مثل البريد الإلكتروني الضار، والمواقع الوهمية ، والبرامج الضارة. ويمكن أن تستهدف الهجمات السيبرانية الأفراد ، والشركات ، والمؤسسات الحكومية ، مما يؤدي إلى خسائر مالية كبيرة ، وتسريب معلومات حساسة ، وانتهاك الخصوصية ، وتعطيل الخدمات العامة وإحداث حالة من الفوضى الأمنية. و تتنوع هذه الهجمات في أشكالها وأهدافها، وتشمل فيروسات الكمبيوتر ، والبرمجيات الخبيثة (مثل برمجيات الفدية والتجسس)، وهجمات الحرمان من الخدمة (**DDoS**) التي تهدف إلى تعطيل الخدمات عبر الإنترنت ، وهجمات التصيد الاحتيالي التي تستهدف الحصول على معلومات حساسة مثل كلمات المرور وبيانات البطاقات الائتمانية ، والتي يترتب عليها بمختلف أنواعها آثار سلبية للمستخدمين حول العالم.

3-2 تقنيات الأمان الأساسية

لاحظ عزيزي الطالب ان هناك استخداما متزايدا للانترنت وشبكات الحاسوب في المؤسسات العامة والخاصة ، ومما لاشك فيه ان هذه الزيادة ترافقها زيادة وتنوع في الهجمات الالكترونية . لذا صار من الضروري استحداث وتطوير تقنيات الامان من أجل حماية المؤسسات من هذه الهجمات . وهنالك عدة تقنيات تستخدم في هذا المجال , وفيما يأتي عرض لأهم هذه التقنيات .

1-3-2 الجدران النارية (Firewalls)

تعتبر الجدران النارية او (جدران الحماية) الطبقة الأولية لحماية الانظمة وشبكات الحاسوب . وتستخدم لمراقبة حركة مرور البيانات الواردة والصادرة الى الشبكة وتصفيتها والتحكم فيها بناء على مجموعة من قواعد الأمان المحددة سلفا , الغرض الأساسي منها هو بناء حاجز بين الشبكة الداخلية الموثوقة سلفا والشبكات الخارجية غير الموثوق بها . ومن خلال هذه المراقبة لحركة المرور وتطبيق قواعد الأمان المحددة تستطيع هذه الجدران اكتشاف البيانات الضارة وحظرها ومنعها من الدخول إلى الشبكة . وتأتي جدران الحماية إما على شكل أجهزة أو برامج , ويتم وضع اجهزة جدران الحماية على حافة الشبكة ، وهذا ما يسمح لها بحماية أجهزة متعددة في وقت واحد .

بينما يتم تثبيت جدران الحماية البرمجية على الأجهزة الفردية مثل أجهزة الحاسوب أو الهواتف الذكية. إ ن وضع جدران الحماية على حافة الشبكة أو في مركز البيانات يسمح لها بمراقبة أي شيء يحاول العبور عن كثب , وتتيح لها هذه الرؤية فحص حزم البيانات ومصادقتها بدقة في الوقت الفعلي .

ويتلخص آلية عملها في التحقق من حزمة البيانات مقابل معايير محددة سلفا لتحديد ما إذا كانت تشكل تهديدا أم لا . فإذا فشلت الحزمة في تلبية المعايير ، فإن جدار الحماية تمنعها من الدخول إلى الشبكة أو مغادرتها . وهذه آلية في تنظم حركة المرور الواردة والصادرة تحمي الشبكة من التهديدات الخارجية مثل الفيروسات ورسائل البريد الإلكتروني للتصيد الاحتيالي وهجمات رفض الخدمة (DoS) ....الخ .

حيث تقوم جدران الحماية بتصفية تدفقات حركة المرور الواردة ، مما يمنع الوصول غير المصرح به إلى البيانات الحساسة ويحبط الإصابات المحتملة بالبرامج الضارة . بالاضافة الى انها تقوم بحماية الشبكة من التهديدات الداخلية مثل الجهات الفاعلة السيئة أو التطبيقات المحفوفة بالمخاطر . حيث تقوم جدران الحماية بفرض القواعد والسياسات لتقييد أنواع معينة من حركة المرور الصادرة، مما يساعد على تحديد النشاط المشبوه والتخفيف من استخراج البيانات .

هذا ويتم تصنيف الأنواع المختلفة من جدران الحماية بناء على وظيفتها. فمن أجل حماية الإنترنت يتم استخدام جدران حماية الشبكة ، ومن أجل حماية تطبيق الويب ، يتم استخدام جدران حماية لتطبيقات الويب. وينبغي تحديث قواعد جدران الحماية بصفة دورية ، وضبطها بدقة لتجنب إعطاء امتيازات كبيرة دون مبرر، مع مراعاة موازنة العبء الذي تضعه على أداء الشبكة.

2-3-2 التشفير (Encryption)

يتم استخدام التشفير لحماية البيانات المهمة والحساسة أثناء نقلها عبر الشبكات ، ويجعلها قابلة للقراءة فقط للأشخاص المصرح لهم الذين لديهم مفتاح فك تشفير الرمز للوصول إلى معلومات النص الأصلية. وبعبارة أبسط ، يعد التشفير طريقة لجعل البيانات غير قابلة للقراءة للطرف غير المصرح له . وهو شكل من أشكال أمان البيانات يعمل على إحباط مجرمي الإنترنت الذين ربما يستخدمون وسائل متطورة للوصول إلى الشبكة , ثم يكتشفون أن البيانات غير قابلة للقراءة وعديمة الفائدة . ان التشفير لا يضمن سرية البيانات أو الرسائل فحسب ، بل يوفر أيضا المصادقة والتكامل ، مما يثبت أن البيانات أو الرسائل

الأساسية لم يتم تغييرها بأي شكل من الأشكال عن حالتها الأصلية. ان عملية التشفير يمكن ان تجري على البيانات عندما تكون في حالة سكون عند تخزينها ، كما هو الحال في قاعدة بيانات , او عندما تكون البيانات في حالة حركة أثناء النقل ، كما هو الحال عنده تناقلها عبر الشبكات بين الأطراف.

ويعد التشفير من تقنيات الأمان الاساسية في الشبكات المعاصرة . وتعتمد هذه التقنية على تحويل البيانات باستخدام خوارزمية معينة تسمى (خوارزمية التشفير) وهي صيغة رياضية تستخدم لتحويل نص البيانات العادي إلى نص مشفر غير مقروءة إلا من الأطراف المخوّلة بامتلاك مفاتيح فك التشفير .

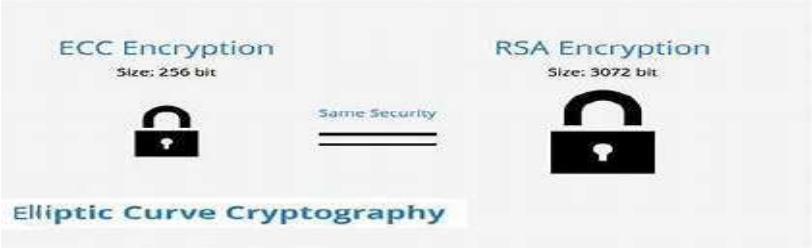
أن تقنية التشفير لا تحافظ على الخصوصية والأمان للبيانات الحساسة فحسب , بل تحافظ أيضا على أمان المستخدمين أثناء تصفح الإنترنت , وهذا الامر سيشعرهم بأمان أكبر عند إدخال معلوماتهم الشخصية في صفحات الويب اوإجراء المعاملات المالية أو التجارة الإلكترونية .وتنقسم خوارزميات التشفير إلى نوعين أساسيين ,**هي التشفير التماثلي (Symmetric) والتشفير غير التماثلي (Asymmetric).**

1- التشفير التماثلي (Symmetric Encryption)

يُستخدم في هذا النوع من التشفير مفتاح واحد لكل من التشفير وفك التشفير, ويكون هذا المفتاح مشتركًا بين الطرفين (المرسل والمستقبل) للبيانات , وتمتاز بفعليتها وسرعة أدائها .، وتستخدم خوارزميات فعالة من أبرزها خوارزمية معيار تشفير البيانات **DES (Data Encryption Standard)** , والخوارزمية الاحدث معيار التشفير المتقدم **AES (Advanced Encryption Standard)** . وهذه الطريقة في التشفير مفضلة لنقل البيانات عندما تكون بكميات كبيرة. ومع ذلك فان عملية اختراق سرية المفتاح يشكل خطرا كبيرا ولا سيما في البيئات الواسعة النطاق, لذا يجب مشاركة المفتاح بشكل آمن.

2- التشفير غير التماثلي (Asymmetric Encryption)

يقدم التشفير غير المتماثل خيارا أقوى بكثير لضمان أمان المعلومات المنقولة عبر الإنترنت . تستخدم مفتاحين مختلفين ولكنهما مرتبطان لتشفير البيانات وفك تشفيرها. مفتاح عام لتشفير البيانات , وتوزع على نطاق واسع **(Public Key)** ، ومفتاح خاص لفك التشفير **(Private Key)** ويبقى سريًا لدى مالكه. ويعدّ هذا النموذج أكثر أمانًا في تبادل المفاتيح ، ولكن غالبًا ما تكون أبطأ من التشفير التماثلي . ومن أبرز الخوارزميات المستخدمة فيها هي خوارزمية **RSA** (Rivest , Shamir , Adleman) , وخوارزمية **ECC (Elliptic Curve Cryptography)** ، ومن الجدير بالذكر ان خوارزمية **(ECC)** هي المُعتمدة بسبب كفاءتها العالية مع مفاتيح أقصر نسبيًا.



3-3-2 تحديد الهوية والمصادقة والتفويض

تشكل عملية التحقق من هوية المستخدمين وإعطائهم الصلاحيات المناسبة ركيزة أساسية لأمان الشبكات . وتعد احدى تقنيات الأمان المستخدمة لحماية البيانات من الوصول غير المصرح به لضمان عدم التلاعب بها أو تعديلها دون تصريح بالاضافة الى ضمان بقاء الموارد والبيانات متاحة للاستخدام في الوقت المناسب وبطريقة موثوق بها . و يعد فهم الاختلافات بين هذه المصطلحات أمرا ضروريا في تصميم وتنفيذ أنظمة إدارة الهوية والأمان الفعالة لضمان أمان وسلامة البيانات والمعلومات الشخصية . وإحدى الطرق لفهم الاختلافات بينها هو اعتبارها عملية من ثلاث خطوات .

الخطوة الاولى تحديد الهوية (Identification) :

يشير تحديد الهوية إلى معرفة من هو الشخص الذي يحاول تسجيل الدخول إلى الشبكة او النظام . وهل هي موجود فعليا أو أنه مستخدم مجهول أو برنامج آلي يحاول تسجيل الدخول باستخدام اسم مستخدم وكلمة مرور مسروقة , وتتم عملية تحديد الهوية للمستخدم بناء على المعلومات التي يقدمها مثل اسمه أو عنوان بريده إلالكتروني أو أي معلومات أخرى تحدد هويته .

الخطوة الثانية المصادقة (Authentication) :

إذا كان الموظف أو المستخدم قادرا على إثبات هويته بتحديد الهويه ، فإن الخطوة الثانية هي عملية التحقق من أن المستخدم هو الشخص الذي يدعي أنه صاحب الهوية قبل منحه أي صلاحيات للدخول أو الوصول الى المعلومات . ويتم ذلك من مقارنة المعلومات التي يقدمها المستخدم بمصدر موثوق به ، مثل بطاقة هوية صادرة عن جهة حكومية أو جواز سفر أو رخصة قيادة .....إلخ .

الخطوة الثالثة التفويض (Authorization) :

بمجرد أن يقدم المستخدم الهوية المناسبة ويتم تأكيدها ومصادقتها ، تاتي الخطوة الثالثة وهي إعطاؤه التفويض والسماح له بتسجيل الدخول إلى الشبكة أو النظام وتحديد ما يُسمح له بالوصول إليه من معلومات أو خدمات من خلال أذونات محددة . ويتم ذلك عادة من خلال مزيج من تحديد الهوية والتحقق ، إلى جانب تدابير أمنية إضافية مثل كلمات المرور أو المصادقة البيومترية التي تتضمن استخدام الخصائص الجسدية الفريدة للشخص ، مثل بصمة إصبع أو التعرف على الوجه أو الصوت أو قزحية العين للتحقق من هويته.

4-2 بروتوكولات الأمان الأساسية

عبر الشبكات بأمان ، ومن خلال استخدام هذه البروتوكولات معًا، يمكن إنشاء نظام أمني لحماية مصالح الشركات وعملائها. وتعد البروتوكولات الأمنية عنصراً أساسياً في تأمين البيانات وحمايتها وسلامتها من التهديدات السيبرانية، وبذلك فانها تعزز الثقة والموثوقية في بيئة الاتصالات الرقمية. وتعتبر بروتوكولات الأمان مهمة جداً للأسباب الآتية :

حماية البيانات الحساسة : البيانات والمعلومات الحساسة كالمعلومات المالية أو الطبية .

الحفاظ على الخصوصية : ويقصد بالخصوصية كل ما يتعلق بالمعلومات الشخصية للعملاء والمستخدمين.

تجنب الخسائر المالية : مثل الخسائر المالية التي تتعرض لها الشركات والتي من الممكن ان تكلف ملايين الدولارات نتيجة تعرضها للهجمات السيبرانية.

منع الاختراقات : الاختراقات وهي المخاطر التي تتعرض الأنظمة والشبكات نتيجة الاختراقات السيبرانية والهجمات الإلكترونية .

الامتثال للتشريعات والمعايير: التشريعات هي القوانين والأنظمة المتعلقة بحماية الخصوصية ومصالح العملاء .

الحفاظ على سمعة الشركة : مثل تجنب التسريبات المتعلقة باسرار الشركة وبياناتها, التي قد تؤثر سلباً في سمعتها ومصداقيتها.

تحقيق الثقة والموثوقية : كتعزيز الثقة والموثوقية بالخدمات الرقمية والتطبيقات عبر لإنترنت مما يسهم في جذب المزيد من المستخدمين والعملاء.

ويتم اتستخدم بروتوكولات الأمان وتطبيقها في الكثير من المجالات وكما يأتي :

الشبكات اللاسلكية : تأمين الشبكات اللاسلكية المنزلية أو التجارية مثل (**WiFi , Bluetooth**)

التجارة الإلكترونية : حماية المعاملات المالية عبر الإنترنت مثل بطاقات الامان.

الخدمات السحابية : تأمين البيانات المخزنة في السحابة مثل (**Googel Drive**).

هذا ويمكن -عزيزي الطالب- أن نصنف عمل بروتوكولات الأمان الأساسية في الواقع الى ما يأتي :-

1. بروتوكولات التشفير
2. بروتوكولات المصادقة
3. بروتوكولات إدارة الوصول
4. بروتوكولات التوقيت
5. بروتوكولات إدارة المفاتيح العامة والخاصة
6. بروتوكولات الوقاية من التزوير

2-4-1 البروتوكول (TLS & SSL)

أن البروتوكول (**SSL**) والبرتوكول (**TLS**) من بروتوكولات التشفير المؤمنة, التي تستخدم لتأمين الاتصالات عبر الإنترنت والتي تتطلب تناقل معلومات حساسة كمواقع التجارة الإلكترونية والتطبيقات العاملة والبريد الإلكتروني . وتستخدم لتشفير البيانات أثناء عملية نقلها عبر الشبكة مما يجعلها غير قابلة للقراءة إلا بواسطة الأطراف المعتمدة ويصعب اعتراضها جدا على المتسللين.

طبقة المآخذ الآمنة (SSL / Secure Sockets Layer)

تم تطوير هذا البروتوكول في تسعينيات القرن الماضي وذلك لغرض إنشاء رابط مشفر بين خادم الويب والمتصفح . يقوم هذا البروتوكول باستتخدم خوارزميات التشفير لحماية البيانات أثناء الإرسال ، مما يضمن بقاء المعلومات الحساسة مثل تفاصيل بطاقات الائتمان والبيانات الشخصية سرية .

أمان طبقة النقل (TLS / Transport Layer Security)

يعد البروتوكول (**TLS**) خليفة للبروتوكول (**SSL**). أذ تم تطويره ومعالجة نقاط الضعف المختلفة ودمج تقنيات التشفير الحديثة بالاضافة الى تضمينها تحسينات كبيرة, وهذا ما جعلها توفر أداء أفضل من البروتوكول (**SSL**) . ويتلخص الاختلافت بين البروتوكول (**SSL**) و البروتوكول (**TLS**) فيما يأتي:-

خوارزميات التشفير : يستخدم البروتوكول (**TLS**) خوارزميات تشفير أقوى من البروتوكول (**SSL**).

الأمان : يوفر البروتوكول (**TLS**) أمانا أعلى وأكثر موثوقية من البروتوكول (**SSL**) .

الأداء : يوفر البروتوكول (**TLS**) أداء أفضل و زمن انتقال أقل من البروتوكول (**SSL**) .

2-4-2 بروتوكول الإنترنت الآمن (IPsec)

بروتوكول الإنترنت الآمن (**IPsec / Internet Protocol Security**) هو عبارة عن مجموعة من قواعد لإعداد اتصالات آمنة عبر شبكة لغرض تبادل حزم البيانات في طبقة النقل .

وكما هو معلوم ان بروتوكول الإنترنت (**IP**) هو المعيار الشائع الذي يحدد كيفية انتقال البيانات عبر الإنترنت , فيقوم (بروتوكول الإنترنت الآمن **IPSec**) باضافة التشفير والمصادقة لجعل (بروتوكول الانترنت **IP**) أكثر أمانًا , لذلك يقوم بروتوكولات (الإنترنت الآمن **IPSec**) بإرسل و اعداد حزمة البيانات لنقلها عبر الشبكة بشكل آمن حيث يستخدم التشفير المتماثل و غير المتماثل لتوفير الأمان والسرعة في نقل حزم البيانات , فينشئ اتصالاً آمنًا مع التشفير غير المتماثل ويتحول إلى التشفير المتماثل لتسريع نقل البيانات . ويجب ان ننوه هنا بأن حزمة البيانات هي هيكل محدد لتنسّيق المعلومات تتكون من ثلاثة أجزاء **(العنوان , الحمولة , معلومات ملحقة)** .

العنوان : هو قسم يتضمن معلومات إرشادية لتوجيه حزمة البيانات إلى الوجهة الصحيحة .

الحمولة : هو مصطلح يصف المعلومات الفعلية الموجودة في حزمة البيانات

المعلومات الملحقة : هي بيانات إضافية ملحقة بذيل الحمولة للإشارة إلى نهاية حزمة البيانات .

ويعمل البروتوكول (**IPsec**) في وضعين (وضع النقل و وضع النفق) . ويعتمد الاختيار بين الوضعين على متطلبات الأمان المحددة للاتصال .

يتم استخدام البروتوكول (**IPsec**) عادةً في وضع النقل للاتصال الشامل بين مضيفين , حيث يقوم بتشفير الرسالة (الحمولة) في حزمة البيانات فقط ، ويترك عنوان **IP** بشكله الأصلي بدون تشفير وذلك للسماح لأجهزة التوجيه بتحديد عنوان الوجهة لكل حزمة بيانات.

كما يتم استخدام البروتوكول (**IPsec**) ايظا في وضع النفق بشكل شائع في سيناريوهات الشبكات الافتراضية الخاصة (**VPN**) وذلك لتأمين الاتصال الآمن بين الشبكتين, حيث يتم تشفير جميع البيانات في حزمة (**IP**) وتغليفها داخل حزمة (**IP**) جديدة. بما في ذلك الرأس والحمولة والعنوان، ويلحق عنوانًا جديدًا بها .

يتضمن بروتوكول الإنترنت الآمن (**IPsec**) عددا من البروتوكولات وهي, بروتوكول تبادل مفتاح الإنترنت (**IKE**) , وبروتوكولين لتأمين حزم (**IP**), بروتوكول رؤوس المصادقة (**AH**) و بروتوكول تغليف حمولة الأمان(**ESP**) . وفيما يأتي شرح موجز لهذه البروتوكولات.

بروتوكول تبادل مفتاح الإنترنت (IKE / Internet Key Exchange)

ينشئ هذا البروتوكول اتصالاً آمنًا بين جهازين على الإنترنت. يعِّد كلا الجهازين ارتباط أمان (**SA / Security Association**) يتضمن التفاوض حول مفاتيح التشفير والخوارزميات لإرسال حزم البيانات اللاحقة واستقبالها.

رؤوس المصادقة (AH / Authentication Header)

وهو البروتوكول الذي يصادق على أصل حزم البيانات ويضمن سلامتها , ويحمي محتوياتها (الرأس والحمولة) من تعديل الأطراف غير مصرَّح لهم ويؤكد ان المصدر الاصلي لحزمة البيانات لم تتغير منذ إرسالها .

تغليف حمولة الأمان (ESP / Encapsulating Security Protocol)

يجري بروتوكول تغليف حمولة الأمان بتشفيرً حزمة (**IP**) بأكملها أو للحمولة فقط , مما يوفر سلامة وسرية البيانات وتشفيرها ومصادقة أصول البيانات (الحزمة بأكملها) ، والسلامة غير المتصلة ، ودرجة معينة من السرية على مستوى حركة المرور , واضافة عنوانً ومعلومات ملحقة لحزمة البيانات عند التشفير .

وهناك الكثير من الفوائد المرتبطة باستخدام بروتوكول الانترنت الآمن (**IPsec**) وهي :-

سلامة البيانات: تضمن عدم التلاعب بالحزم أثناء النقل
السرية: تقوم بتشفير البيانات، ومنع الوصول غير المصرح به.
المصادقة: تتحقق من هوية المرسل والمستقبل.
مكافحة إعادة التشغيل: يحمي من هجمات إعادة التشغيل.
وعلى الرغم من الفوائد المتنوعة لبروتوكول الانترنت الآمن (**IPsec**), يأتي معها مجموعة من التحديات الخاصة بها وهي :-
التعقيد: مجموعة ميزات **IPsec** الواسعة تجعل من عملية التنفيذ والإدارة معقدة.
الأداء: يمكن أن تؤثر عملية تشفير البيانات وفك تشفيرها في أداء الشبكة.
التوافق: قد يكون هناك مشكلات في العمل كالمشاكلات في آلية عمل ترجمة عُناوين الشَّبكة **NAT** (**Network Address Translation**), ومثل عناوين أو ارقام المنافذ.

3-4-2 بروتوكول نقل النص التشعبي الآمن (HTTPs)

قبل ان نتعرف على مايعنيه البروتوكول (**HTTPS**) , دعنا قبل ذلك نتعرف على بروتوكول النص التشعبي (**HTTP Hyper Text Transfer Protocol**) . يستخدم هذا البروتوكول فى الأساس لنقل البيانات بين الخادم (**Server**) الذى يحتوى الموقع ومتصفح المستخدم (**Clint**). أذ يتم الاتصال بين المستخدم و الخادم عن طريق ارسال طلبات والحصول على ردود وتسمى هذا الطريقة بنموذج الخادم والعميل وهى من اشهر نماذج نقل البيانات على الإنترنت . اما (**HTTPS**) فتعنى بروتوكول نقل النص التشعبي الآمن (**HTTP Secure**) فهو الإصدار الآمن من البروتوكول (**HTTP**) ، وهو البروتوكول الأساسي المستخدم لإرسال البيانات بين متصفح الويب وموقع الويب حيث يتم تشفير البيانات اثناء نقلها
وذلك لزيادة أمان للبيانات ، وهذا ما يجعلها مهمة بشكل خاص عندما ينقل المستخدمون بيانات حساسة ، مثل تسجيل الدخول إلى الحسابات المصرفية أو خدمة بريد إلكتروني أو مزود تأمين صحي وغيرها من البيانات الحساسة. ومن الجدير بالذكر ان ننوه هنا بأن المتصفحات الحديثة مثل جوجل كروم او فايرفوكس تقوم بوضع علامة (غير أمن) على المواقع التى تستخدم بروتوكول (**HTTP**) بدلًا من (**HTTPS**) , ويمكن ملاحظة ذلك اثناء تصفح المواقع كما موضح في الشكل رقم (2-1)

الشكل رقم (2-1) يوضح موقعا لمتصفح (غير أمن)

يستخدم (**HTTPS**) بروتوكول التشفير المسمى بروتوكول أمان طبقة النقل (**TLS**) لتشفير الاتصال بين المتصفح والخادم. ويستخدم هذا النوع من أنظمة الأمان للبيانات زوجين من المفاتيح مختلفين لتشفير الاتصالات بين الخادم والعميل :
المفتاح الخاص (Private Key) : ويتم حفظه بأمان على الخادم الذى يحتوى على الموقع , و يستخدم لفك تشفير المعلومات المشفرة بوساطة المفتاح العام .
المفتاح العام (Public Key) : ويكون متاحا لاي مستخدم يريد الإتصال والتفاعل مع الموقع بشكل آمن . و يستخدم هذا المفتاح لتشفير البيانات التي لا يمكن فك تشفيرها إلا بوساطة المفتاح الخاص .

في الواقع إن جميع الاتصالات التي تحدث عبر (**HTTP**) تحدث بنص عادي (**Plain Text**) غيرمشفر . مما يجعلها متاحة لأي شخص يحاول اعتراضها وتكون مفهومة له. أما عند استخدام (**HTTPS**) فيتم تشفير حركة المرور بحيث أنه حتى إذا تم الوصول إلى البيانات فستظهر بطريقة مشفرة لايمكن فكها إلا بالمفتاح الخاص الذى لا يمكن الوصول إليه كما أشرنا أليه سابقا.
البروتوكول (**HTTPS**) يمنع مواقع الويب من بث معلوماتها بطريقة يسهل من أي شخص يتطفل على الشبكة من الأصلاع عليها . بالإضافة إلى ذلك ، يلغي قدرة الجهات الخارجية غير الخاضعة للإشراف على حقن المحتوى في صفحات الويب دون موافقة مالك موقع الويب .هذا مهم بشكل خاص لمنع مزودي خدمة الإنترنت أو غيرهم من الوسطاء من حقن الإعلانات أو المحتوى الضار في صفحات الويب. ويمكن حصر الاختلافات بين البروتوكول (**HTTP**) و البروتوكول (**HTTPS**) بالآتي:-
التشفير : ينقل (**HTTP**) البيانات بنص عادي ، بينما ينقل (**HTTPS**) البيانات بتنسيق مشفر.
الأمان : يوفر (**HTTPS**) اتصالا آمنا وسلامة البيانات والخصوصية بتشفير البيانات أثناء الإرسال.
الأداء : قد يكون البروتوكول (**HTTPS**) ابطاء نوعا ما من البروتوكول (**HTTP**) وذلك بسبب النفقات العامة للتشفير وفك التشفير، وهذا يسبب تأثيرا طفيفا على الأداء .

WPA 2 / WPA / WEP 4-4-2

نظرًا إلى أن الشبكات اللاسلكية تنقل البيانات عبر موجات الراديو ، فمن الممكن اعتراضها بسهولة ما لم تكن هناك تدابير أمنية مطبقة. ويعدُّ أمان الشبكة اللاسلكية جانبًا مهمًا لتبقى آمنًا على الإنترنت. وتسرب بيانات اعتماد الحساب ، ويعدُّ الاتصال بالإنترنت عبر روابط أو شبكات غير آمنة خطرًا أمنيًّا قد يؤدي إلى فقدان البيانات وتثبيت البرمجيات الضارة في الشبكة . ويحظى استخدام إجراءات أمان **Wi-Fi** المناسبة بأهمية بالغة ولكن عند القيام بذلك من المهم فهم الاختلافات بين بروتوكولات التشفير اللاسلكية المختلفة ، بما في ذلك **WEP** و **WPA** و **WPA 2**

الخصوصية السلكية المكافئة / (WEP)

تم ابتكار بروتوكول الخصوصية السلكية المكافئة (**Wired Equivalent Privacy**) وكان الهدف منها هو إضافة مستوى أمان إلى الشبكات اللاسلكية بتشفير البيانات , وبذلك لن يتمكن المعترضون من التعرف على البيانات اللاسلكية إذا تم اعتراضها لأنها مشفرة. اما الأنظمة المصرح بها على الشبكة فانها قادرة على التعرف على البيانات وفك تشفيرها , وذلك لأن الأجهزة الموجودة على الشبكة تستخدم خوارزميات التشفير نفسها.
يقوم البروتوكول (**WEP**) بتشفير حركة البيانات باستخدام مفتاح بطول (بت 64) أو (بت 128) بالنظام الست عشري . يسمح مفتاح (**WEP**) لأجهزة الكمبيوتر الموجودة على الشبكة بتبادل الرسائل المشفرة مع إخفاء محتويات الرسائل عن المتطفلين في الوقت نفسه. هذا المفتاح هو الذي يستخدم للاتصال بشبكة لاسلكية مؤمنة.

و بمرور الوقت تم اكتشفت عيوب وثغرات أمنية كثيرة في البروتوكول (**WEP**) . ومع زيادة قوة الحوسبة أصبح من السهل على المجرمين استغلال هذه العيوب والثغرات . ولهذا السبب قامت الشركات العالمية مثل (**Wi-Fi Alliance**) بالتوقف عن استعمالها رسميًا . وفي الوقت الحاضر يعدّ أمان البروتوكول (**WEP**) قديمًا على الرغم من أنه لا يزال قيد الاستخدام في بعض الأحيان , وذلك لأن مسؤولي الشبكة لم يغيروا الأمان الافتراضي على أجهزة التوجيه اللاسلكية لديهم أو لأن الأجهزة أقدم من أن تدعم طرق التشفير الأحدث مثل الوصول المحمي الواي-فاي (**WPA**) .

الوصول المحمي الواي - فاي / (WPA)

الوصول المحمي الواي - فاي (**Wi-Fi Protected Access**) تم ابتكار هذا البروتوكول وكان يعد بمثابة البديل لبروتوكول الخصوصية السلكية المكافئة (**WEP**) . وقد كانت تجمعه معها أوجه تشابه وأدخلت فيه تحسينات بخصوص كيفية التعامل مع مفاتيح الأمان والطريقة التي يتم التصريح بها للمستخدمين . بينما يوفر البروتوكول (**WEP**) لكل نظام مصرح له المفتاح نفسه ، يستخدم (**WPA**) بروتوكول سلامة المفتاح المؤقت (**TKIP Temporal Key Integrity Protocol**) , الذي يغير المفتاح الذي تستخدمه الأنظمة ديناميكيًا. و هذا من شأنه أن يحول دون قيام المتسللين بإنشاء مفتاح التشفير الخاص بهم لمطابقة المفتاح الذي تستخدمه الشبكة الآمنة.
استغني عن معيار تشفير بروتوكول سلامة المفتاح المؤقت (**TKIP**) لاحقًا بمعيار التشفير المتقدم (**AES**) . بالإضافة إلى ذلك يضمن البروتوكول (**WPA**) فحوصات سلامة الرسائل لتحديد ما إذا كان المهاجم قد استولى على حزم البيانات أو قام بتغييرها. كانت المفاتيح المستخدمة بواسطة البروتوكول (**WPA**) بطول (بت 256) وهي زيادة كبيرة عن المفاتيح المُستخدمة في البروتوكول نظام (**WEP**) , وعلى الرغم من هذه التحسينات فإن عناصر البروتوكول (**WPA**) قد تعرضت للاستغلال مما أدى إلى ابتكار البروتوكول (WPA2).

النسخة الثانية من الوصول المحمي بتقنية الواي – فاي / (WPA2)

تم ابتكار النسخة الثانية من بروتوكول الوصول المحمي بتقنية الواي – فاي , والتي تسمى (WPA2) وكان بمثابة إصدارا تمت ترقيته من البروتوكول (**WPA**) . يعتمد هذا البروتوكول على آلية شبكة الأمان القوية (**RSN / Robust Security Network**) ويعمل على وضعين :-

الوضع الشخصي أو المفتاح المشترك سلفا (WPA2 - PSK): الذي يعتمد على رمز مرور مشترك للوصول وعادةً ما يُستخدم في البيئات المنزلية.
وضع المؤسسة (WPA2- EAP): وهذا أكثر ملائمة للاستخدام المؤسسي أو التجاري .
يستخدم كلا الوضعين للبروتوكول (**CCMP**)
The Counter Mode with Cipher Block Chaining Message Authentication Code Protocol ، وهو اختصار لعبارة بروتوكول رمز مصادقة رسائل سلسلة كتلة شفرة وضع العداد. يعتمد بروتوكول (**CCMP**) على خوارزمية معيار التشفير المتقدم (**AES**) التي توفر مصادقة الرسالة والتحقق من سلامتها. يعدُّ بروتوكول (**CCMP**) أقوى وأكثر موثوقية من بروتوكول سلامة المفتاح المؤقت (**TKIP**) الأصلي الخاص بمعيار (**WPA**) ، مما يجعل من الصعب على المهاجمين اكتشاف أنماط التشفير فيها.

5-2 أساليب الهجوم والوقاية

في هذا الموضوع سنتعرف على بعض أنواع الهجمات والحوادث الإلكترونية الشائعة ، والمخاطر المحتملة التي تشكلها واستراتيجيات الوقاية الفعالة ضدها. تأتي التهديدات والحوادث الإلكترونية (السيبرانية) بأشكال كثيرة ويمكن أن يكون لها عواقب وخيمة مثل (خروقات البيانات , الخسائر المالية , الاضطراب التشغيلي , تهديدات الأمن القومي) . ومعظم هذه الحوادث تكون لها دوافع مالية وأصبحت أكثر تعقيدا وخبثا , وفيما يأتي بعض أنواع الهجمات والتهديدات الإلكترونية :-

- التصيد الاحتيالي
- البرامج الضارة
- هجمات رفض الخدمة (**DoS**) ورفض الخدمة الموزع (**DDoS**)
- هجوم رجل في الوسط (**Man Middle In a Ttak**)
- حقن **SQL**

1-5-2 الهجمات (DoS & DDoS)

هجوم رفض الخدمة **DoS** (**Denial-of-Service**) . يهدف هذا الهجوم إلى إيقاف تشغيل جهاز أو شبكة ويسبب عدم تمكن المستخدمين من الوصول إليه. وتحقق هجمات (**DoS**) ذلك عن طريق بإغراق الهدف بحركة المرور أو إرسال معلومات إليه تؤدي إلى حدوث عطل.
هجوم رفض الخدمة الموزع **DDoS** (**Distributed Denial-of-Service**) . في هذا الهجوم يحاول المهاجم جعل خدمة معينة غير متوفرة عن طريق توجيه حركة مرور مستمرة وضخمة من أنظمة طرفية متعددة . ويمكن وصف هجوم رفض الخدمة الموزع (**DDoS**) بأنه هجوم يستفيد من الكمية على الجودة. حيث ان متوسط هجوم (**DDoS**) بسيط بشكل لا يصدق, إنه مجرد طلب قياسي لتحميل موارد الشبكة ، مثلا الصفحة الرئيسية لموقع الويب. ومع ذلك تعمل هذه الهجمات من خلال العدد الهائل من الطلبات المقدمة في وقت واحد والتي تصل الى ملايين الطلبات المتزامنة الى تعجيز حتى الخوادم القوية للتعامل معها. وغالبا ما يكون هجوم (**DDoS**) جزءا ثانويا أو ثالثا من تهديد آخر. على سبيل المثال، قد يفتح الفيروس المتنقل كمبيوتر شخص ما للاستخدام عن بعد كنقطة هجوم (**DDoS**) , قد تتصرف الآلاف من أجهزة الكمبيوتر المصابة بشكل طبيعي حتى يصبح المتسلل جاهزا للمضي قدما في هجوم (**DDoS**) .عند هذه النقطة تصبح أجهزة الكمبيوتر المصابة جزءا من الترسانة الكبرى. ويعد هجوم (**DDoS**) أحد أقوى الأسلحة على المنصة الإلكترونية التي تهدف الى تعطيل الموقع الالكترونية او الانظمة بسبب التحميل الزائد.
وهنالك أنواع مختلفة من هجمات رفض الخدمة الموزع (**DDoS**) , وفيما يأتي أهم تلك الانواع :-

- الهجمات الحجمية
- هجمات البروتوكول
- هجمات التطبيق
- هجمات التجزئة

2-5-2 الهجمات الخفية

في المشهد الرقمي المترابط اليوم ، أصبحت تهديدات الأمن السيبراني أكثر تعقيدا من أي وقت مضى . وهذا يتطلب اعتماد استراتيجيات استباقية عبر المجالات لاكتشاف الهجمات الخفية والدفاع عنها . يستفيد المهاجمون من التقنيات المتقدمة لاستغلال الثغرات الأمنية والتسلل إلى الشبكات واختراق البيانات ، مما

يجعل آليات الدفاع التقليدية غير مجدية. سنتعرف في هذا الموضوع الأساليب والأدوات والاستراتيجيات التي يمكن استخدامها لاكتشاف الهجمات الخفية وإنشاء دفاعات قوية لتحصين وضعك الأمني في هذه البيئة المتغيرة باستمرار.

الهجمات الخفية هي تهديدات إلكترونية لا يمكن اكتشافها باستخدام أدوات الأمان التقليدية . وهي مصممة لتبقى غير مكتشفة لفترات طويلة ، حتى أن بعضها تتلف قبل اكتشافها والتعرف عليها .غالبا ما يتم تنفيذ هذه الهجمات باستخدام طرق متقدمة , وفي ما يأتي بعض انواع الهجمات الخفية :-

التهديد المستمر المتقدم **(Advanced persistent Threat) (APTs)** :

- البرامج الضارة بلا ملفات.
- ثغرة يوم الصفر أو **(Zero-Day)**.
- البرامج الضارة متعددة الأشكال.

ان الهجمات الخفية تعد خطيرة جدا لانها تتميز بقدرتها على التخفي , وطول العمر , وتاثيرها الواسع النطاق , ونتيجة لخطورة هذه الأنوع من الهجمات يجب اتخاذ أستراتيجيات معينة للكشف عنها وهي ما يأتي :-

اعتماد التحليلات السلوكية : تركز التحليلات السلوكية على تحديد الحالات الشاذة في سلوك المستخدم والنظام .

تحليل سلوك الشبكة : يحدد أنماط حركة المرور غير الطبيعية التي تشير إلى التهديدات المحتملة.

تنفيذ خطوات الاستخباراتية للتهديدات : يوفر التحليل الذكي للتهديدات رؤى حول التهديدات المعروفة والناشئة، مما يمكن المؤسسات من الدفاع بشكل استباقي ضد الهجمات الخفية.

مؤشرات الاختراق : استخدم الادوات المناسبة لتحديد الأنشطة الضارة.

مواجز معلومات التهديدات : وهي تدفقات من معلومات التهديدات في الوقت الفعلي . في حين أن بعض منها تتضمن معلومات التهديدات التي تمت معالجتها أو تحليلها ، فإن البعض الآخر يتكون من بيانات التهديدات الأولية وتسمى أحيانًا (مواجز بيانات التهديدات) .

التعاون : مشاركة معلومات التهديدات مع نظيراتها في الصناعة للدفاع الجماعي.

الاستفادة من التعلم الآلي (الذكاء الاصطناعي) : يعمل التعلم الآلي (الذكاء الاصطناعي) على تحسين قدرات الكشف من خلال تحليل كميات هائلة من البيانات وتحديد الأنماط التي تشير إلى الهجمات الخفية.

نشر تقنية الخداع : تستخدم تقنية الخداع الأفخاخ والفخاخ لجذب المهاجمين وتحديد أساليبهم .

3-5-2 الوقاية (IDS , IPS , VPN)

مع استمرار نمو التهديدات السيبرانية، من المهم البقاء على اطلاع بأمن الشبكة . يمكن أن يساعد التحديث المنتظم للإجراءات الأمنية وصيانتها مثل جدران الحماية و أنظمة الكشف عن التسلل **(IDS)** وأنظمة منع التسلل **(IPS)** والشبكات الافتراضية الخاصة **(VPNs)** , على حماية الشبكات من الهجمات المحتملة . ومن فهم هذه الأدوات واستخدامها ، يمكن للأفراد والمؤسسات الحفاظ على بياناتهم بشكل آمن في العالم الرقمي . وستناول فيما يأتي شرحا لثلاث أدوات رئيسية تساعد على حماية الشبكات وهي أنظمة الكشف عن التسلل وأنظمة منع التسلل والشبكات الافتراضية الخاصة , ومن خلال التعرف على هذه الأدوات يمكننا فهم كيفية الحفاظ على أمان الشبكات بشكل أفضل .

نظام الكشف عن التسلل (IDS)

يعمل نظام الكشف عن التسلل (**IDS Intrusion Detection System**) كنظام الإنذار للشبكة. حيث يراقب حركة المرور فيها ، ويبحث عن الأنشطة المشبوهة التي قد تشير إلى وجود تهديد أمني. وعندما يكتشف شيئا غير عادي ، فإنه ينبه مسؤولي الشبكة حتى يتمكنوا من اتخاذ الإجراءات المناسبة . وهناك نوعان رئيسيان من نظام الكشف عن التسلل :-

نظام الكشف عن التسلل المستندة إلى الشبكة (Network IDS) : يراقب هذا النوع حركة المرور عبر الشبكة بأكملها .

نظام الكشف عن التسلل المستندة إلى المضيف (Host IDS) : يركز هذا النوع على الأجهزة الفردية ، ويراقب سجلات النظام والملفات بحثا عن علامات المشاكلات. وتقسم أنظمة كشف التسلل المستندة إلى المضيف **IDS** على نوعين رئيسيين, نظام الكشف عن التسلل المستند إلى المضمون (**Signature-Based IDS**) ونظام الكشف عن التسلل المستند إلى السلوك (**Behavior-Based IDS**) .

نظام الكشف عن التسلل المستند إلى المضمون

يستخدم قاعدة بيانات تحتوي على توقيعات للهجمات المعروفة والتي حللت سابقًا، وتستخدم هذه القاعدة للكشف عن تواجد الهجمات الجديدة التي تشابه الهجمات المعروفة في القاعدة .

نظام الكشف عن التسلل المستند إلى السلوك

يعتمد على تحليل الأنشطة في الشبكة ومقارنتها بالسلوك العادي للمستخدمين والأجهزة في الشبكة. وبما أنه يتم تحليل السلوك العادي للمستخدمين والأجهزة، تتيح هذه الطريقة الكشف عن الهجمات الجديدة المتطورة التي لم تسبق الكشف عنها.

تتطلب أنظمة كشف التسلل **IDS** الكثير من الخوارزميات والتقنيات المعقدة للكشف عن الهجمات والأنشطة غير المعتادة في الشبكة ، وتتطلب أيضًا إدارة وصيانة دورية لضمان عمل النظام بكفاءة عالية والتحديث المستمر للقواعد البياناتية والتوقيعات .

أنظمة منع التسلل (IPS)

يأخذ نظام منع التسلل (**IPS Intrusion Prevention System**) أمان الشبكة خطوة إلى الأمام ليس فقط من خلال اكتشاف التهديدات ولكن أيضا من خلال اتخاذ إجراءات فورية لمنعها .إنه مثل وجود نظام أمان لا يصدر إنذارا فحسب، بل يغلق الأبواب أيضا عندما يكتشف دخيلا. ويمكن إعداد نظام منع التسلل بطرق مختلفة منها ما يأتي :-

طريقة الوضع المضمن : حيث يراقب بنشاط حركة المرور ويتحكم فيها في الوقت الفعلي ، ويمنع أي شيء ضار قبل أن يتسبب في ضرر.

طريقة الوضع السلبي : حيث يراقب ببساطة النشاط المشبوه ويبلغ عنه دون التدخل المباشر في الشبكة. يستخدم نظام منع التسلل طرقا مشابهة لنظام الكشف عن التسلل ، مثل الكشف المستند إلى المضمون او الكشف المستند إلى السلوك ، ولكن لديه أيضا القدرة على إيقاف التهديدات تلقائيا بمجرد اكتشافها. يسهم هذا النهج الاستباقي في تقليل مخاطر الهجمات الإلكترونية .

الشبكات الافتراضية الخاصة (VPN)

تشبه الشبكة الافتراضية الخاصة **(VPN Virtual Private Network)** نفقا آمنا يحمي بياناتك أثناء انتقالها عبر الإنترنت . وتعد الشبكة الافتراضية الخاصة مهمة بشكل خاص للعمل عن بعد ، مما يسمح للموظفين بالاتصال بأمان بشبكة شركاتهم من أي مكان في العالم . تعمل الشبكة الافتراضية الخاصة عن طريق تشفير البيانات التي تنتقل بين جهاز المستخدم والشبكة ، مما يجعلها غير قابلة للقراءة لأي شخص قد يحاول اعتراضها . وهناك أنواع مختلفة من الشبكات الافتراضية الخاصة :-

الشبكة الافتراضية الخاصة من موقع إلى موقع : وهي تربط شبكات بأكملها .

الشبكة الافتراضية الخاصة للوصول عن بعد : وهي تسمح للمستخدمين الفرديين بالاتصال بأمان بالشبكة من موقع بعيد.

تمرين رقم 1 : اعداد جدار نارى بسيط باستخدام جهازك

الهدف من التمرين:

تعريف الطلاب بخطوات إعداد جدار الحماية (الناري) بسيط باستخدام جهازك

المتطلبات الأساسية:

جهاز حاسوب يحتوي على نظام التشغيل (Windows 10)

ملاحظة :- يجب ان يكون الجدار الناري في الجهاز غير مفعل حتى يتم تنفيذ هذا التمرين

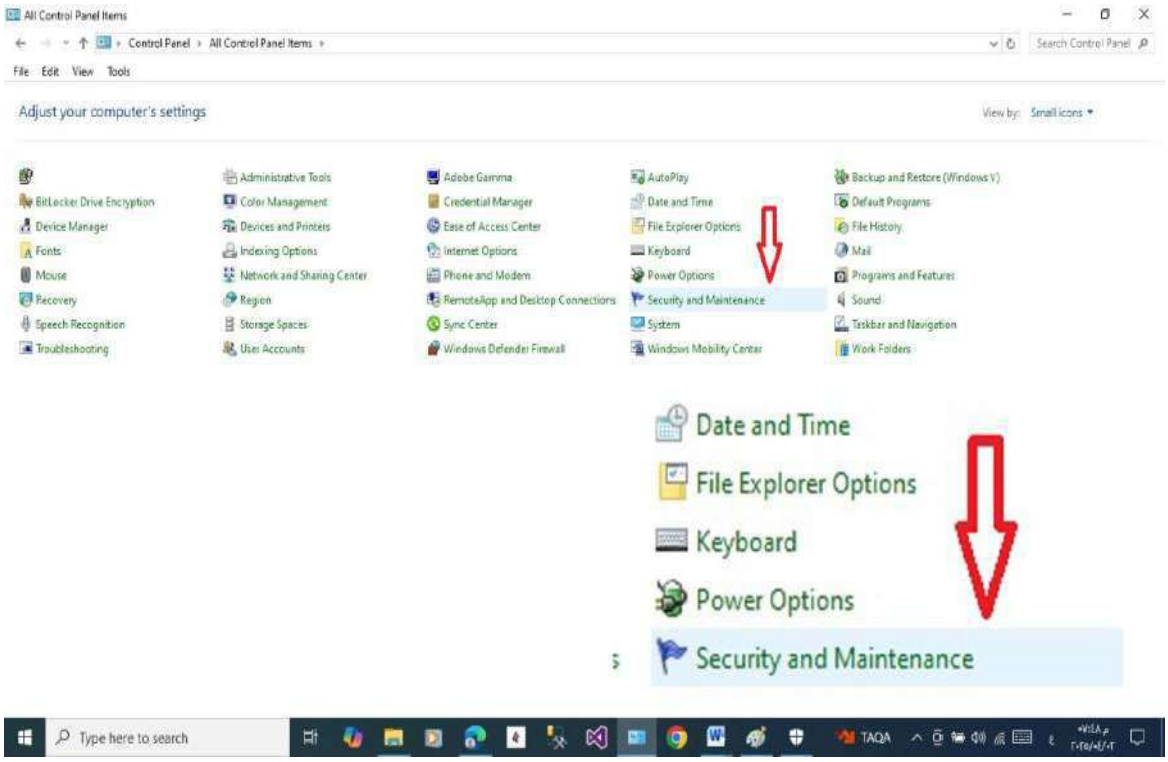
الخطوات العملية:

الخطوة 1: الدخول الى لوحة التحكم (Control Panel)

من قائمة ابدأ نقوم بالدخول الى لوحة التحكم (Control Panel)

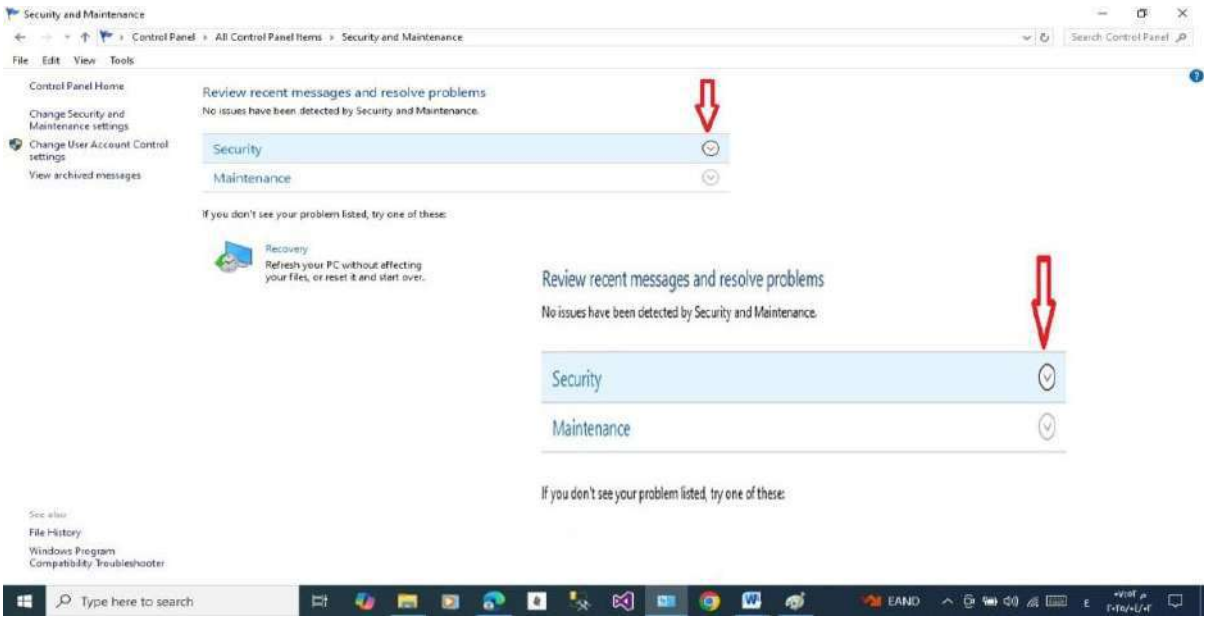
تظهر النافذة (All Control Panel Items) كما في الشكل (2-2), وفيها مجموعة اختيارات,

نضغط على الاختيار الأمن والصيانة (Security and Maintenance)



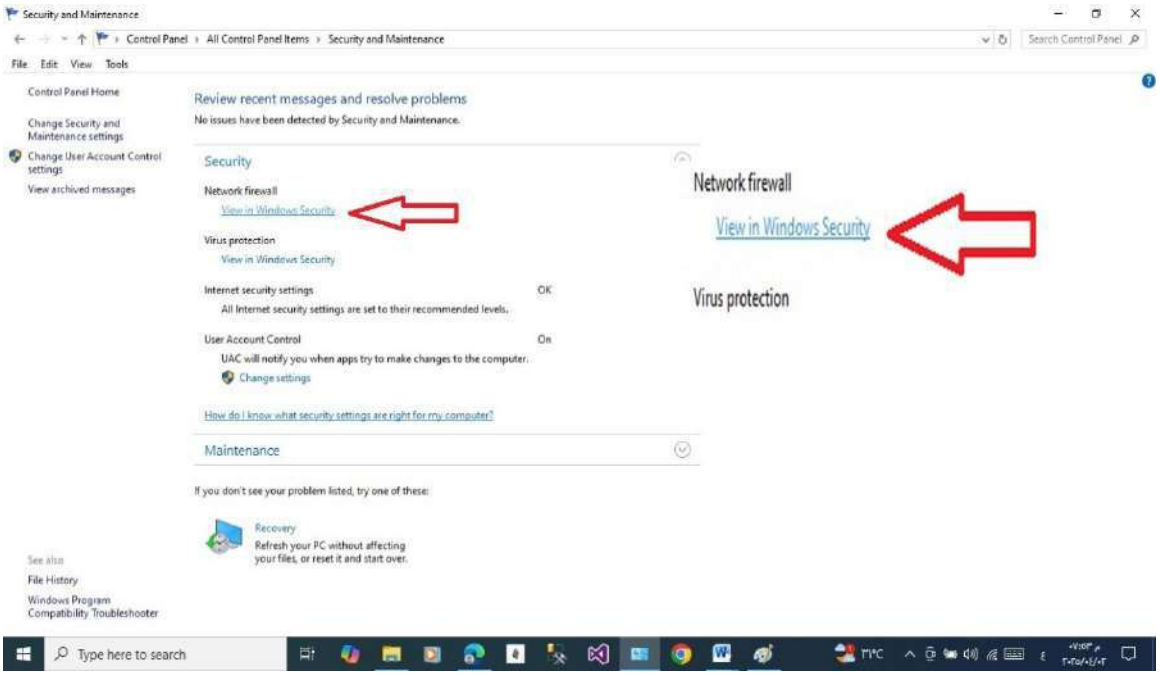
الشكل (2-2) نافذة لوحة التحكم (Control Panel)

الخطوة 2: نفتح قائمة (Security) الموجودة في نافذة الأمن والصيانة, كما في الشكل (2-3).



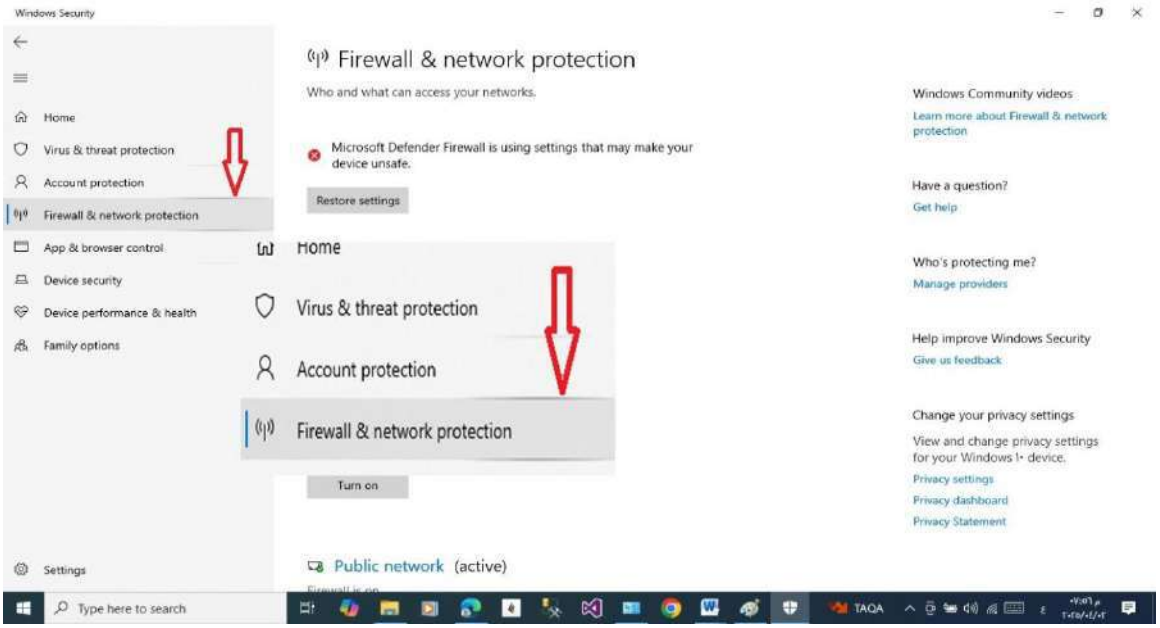
الشكل (2-3) نافذة الأمن والصيانة

الخطوة 3: تحت خيار جدار حماية (الناري) للشبكة (**Network firewall**) نضغط على الخيار عرض نوافذ الأمن (**View in Windows Security**) , كما في الشكل (2-4).



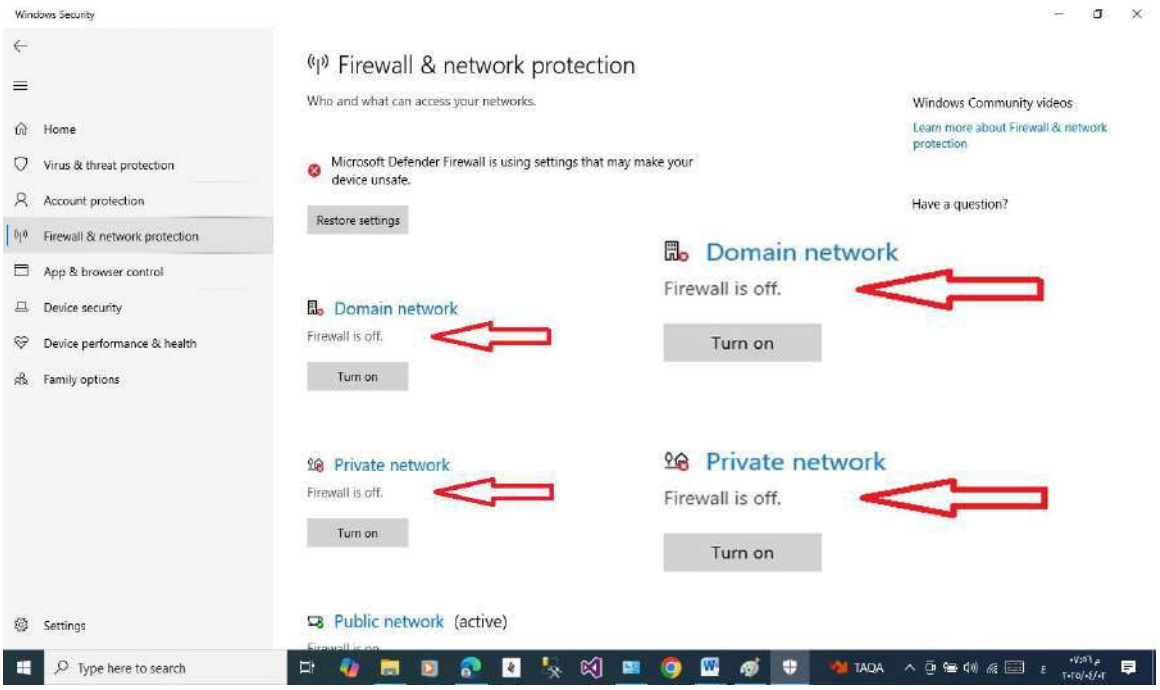
الشكل (2-4)

الخطوة 4: في نافذة الأمن (**Windows Security**) نضغط على الخيار جدار الحماية وحماية الشبكة (**Firewall & network protection**), كما في الشكل (2-5).



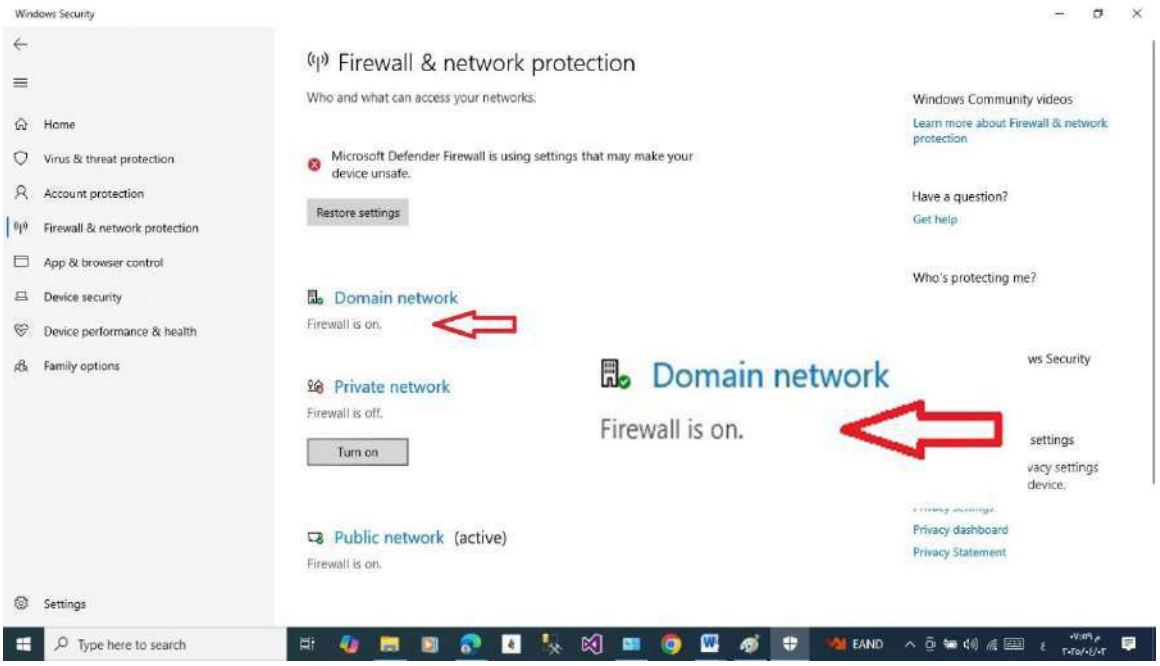
الشكل (2-5)

الخطوة 5: نلاحظ ان جدار الحماية غير مفعل (**Firewall is off**) تحت الاختيار نطاق الشبكة (**Domain network**) والاختيار الشبكة الخاصة (**Private network**) , كما في الشكل (2-6).



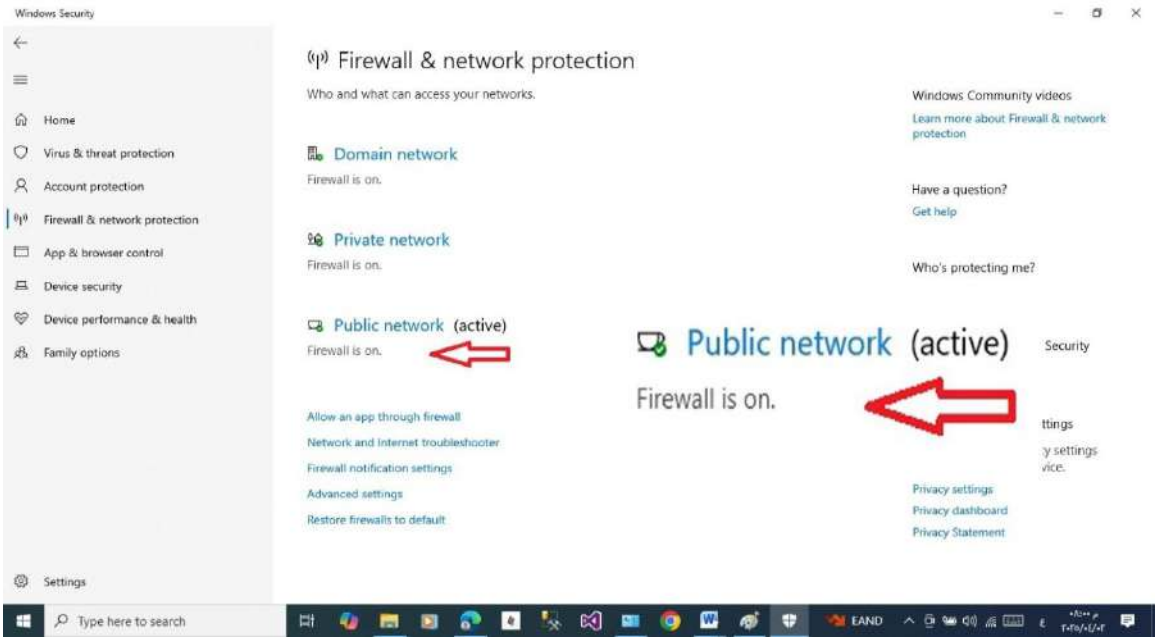
الشكل (2-6)

الخطوة 6: نضغط على الاختيار (**Turn on**) الموجود تحت الاختيار نطاق الشبكة , فتظهر رسالة نختار (نعم / **Yes**) , فنلاحظ ظهور (**Firewall is on**) تحت الاختيار نطاق الشبكة, كما في الشكل (2-7).



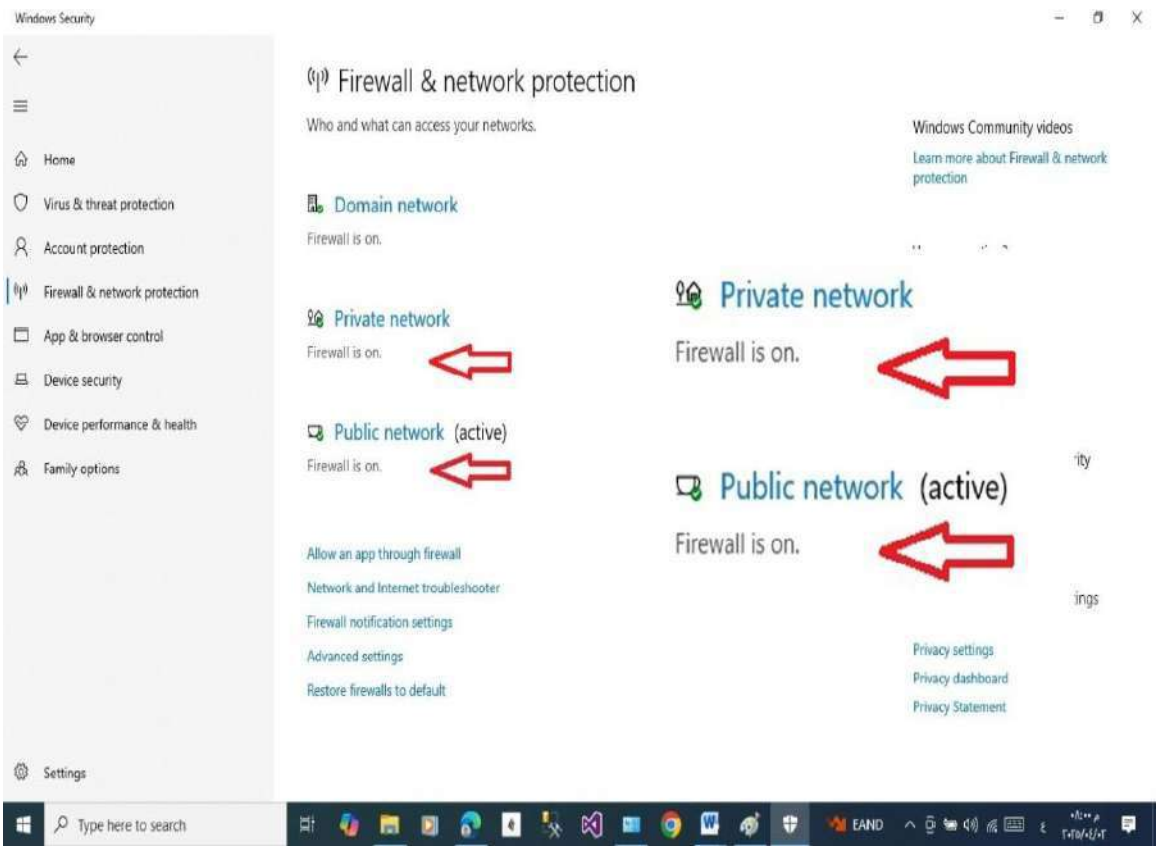
الشكل (2-7)

الخطوة 7: نضغط على الاختيار (**Turn on**) الموجود تحت الاختيار الشبكة الخاصة , فتظهر رسالة نختار (نعم / **Yes**) فنلاحظ ظهور (**Firewall is on**) تحت الاختيار الشبكة الخاصة, كما في الشكل (2-8).



الشكل (2-8)

الخطوة 8: نلاحظ ظهور (**Firewall is on**) تحت الاختيار نطاق الشبكة وتحت الاختيار الشبكة الخاصة دلالة على انتهاء إعداد تفعيل جدار الحماية في الجهاز, كما في الشكل (2-9).



الشكل (2-9)

النتيجة المتوقعة

بعد تنفيذ هذا التمرين سيكون الطلبة قادرين على إعداد جدار ناري بسيط باستخدام جهاز الحاسوب

استمارة الفحص تمرين رقم (1)			
الجهة الفاحصة:			
اسم الطالب : **المرحلة الثالثة** **التخصص : الامن السيبراني**			
اسم التمرين : إعداد جدار ناري بسيط باستخدام جهازك			
ت	**الخطوات**	**الدرجة القياسية % 50**	**درجة الاداء %50**	**الملاحظات**
1	الدخول الى لوحة التحكم **(Control Panel)**	%5		
2	فتح قائمة **(Security)** الموجودة في نافذة الأمن والصيانة	%5		
3	ضغط على الخيار عرض نوافذ الأمن **(View in Windows Security)**.	%5		
4	ضغط على الخيار جدار الحماية وحماية الشبكة **(Firewall & network protection)**.	%5		
5	ضغط على الاختيار **(Turn on)** الموجودة تحت الاختيار نطاق الشبكة	%5		
6	ضغط على الاختيار **(Turn on)** الموجودة تحت الاختيار الشبكة الخاصة و ظهور **(Firewall is on)**	%5		
7	**المناقشة**	%10		
8	**الزمن المخصص**	%10		
المجموع				
اسم الفاحص		**التوقيع**		

تمرين رقم 2 : تجربة تقنيات التشفير باستخدام أداة مثل OpenSSL لتشفير وفك تشفير الملفات

هدف من التمرين:

تعريف الطلاب بخطوات تشفير وفك تشفير ملف باستخدام الاداة (**OpenSSL**)

المتطلبات الأساسية:

جهاز حاسوب منصب علية نظام التشغيل (**Windows 10**)

تثبيت الاداة **OpenSSL**

ملاحظة :- يجب تثبيت الاداة **OpenSSL** حتى يتم تنفيذ هذا التمرين

إنشاء ملف من نوع النص ذي الامتداد (**.txt**) . في هذا التمرين قمنا بتسميتها **Myfile** ووضعناها في مجلد اسمه **Myfolder** على سطح المكتب **Desktop** , وكتبنا فيها نصا معينا

ملاحظة :- تستطيع اختيار اسم أخر للملف او المجلد , ولكن انتبه يجب عليك تغيير أسمائها أيضا في الاوامر المستخدمة.

استخدم امر التشفير ذات الصيغة العامة الآتية

Openssl enc –aes-256-cbc –in file name with dirction.txt –out file name with dirction.txt

استخدم امر فك التشفير ذات الصيغة العامة التالية

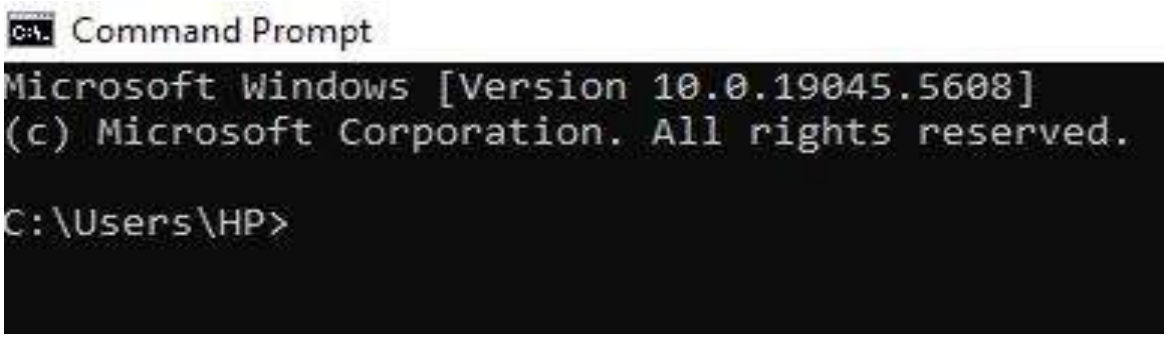
Openssl enc – d -256-cbc –in file name with dirction.txt –out file name with dirction.txt

الخطوات العملية:

الخطوة 1: الدخول الى نافذة موجه الأوامر (**Command Prompt**)

من قائمة ابدأ نقوم بالدخول الى نافذة موجه الأوامر (**Command Prompt**)

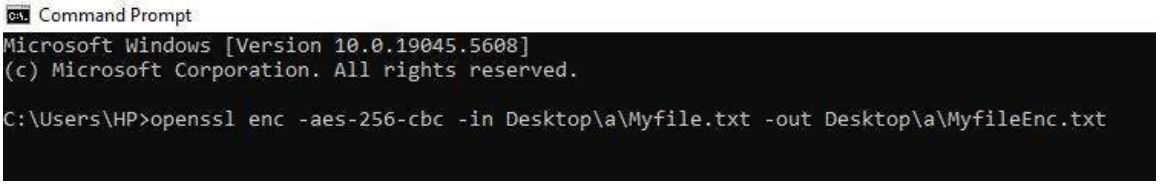
تظهر النافذة موجه الأوامر (**Command Prompt**) , كما في الشكل (2-10).



الشكل (2-10)

الخطوة 2: نقوم بتشفير الملف (**Myfile**) باستخدم أمر التشفير في نافذة موجه الأوامر وتنفيذها . لذا نقوم بكتابة الامر الآتي في نافذة موجه الأوامر وننفذها بالضغط على مفتاح (**Enter**) الموجود في لوحة المفاتيح , كما في الشكل (2-11).

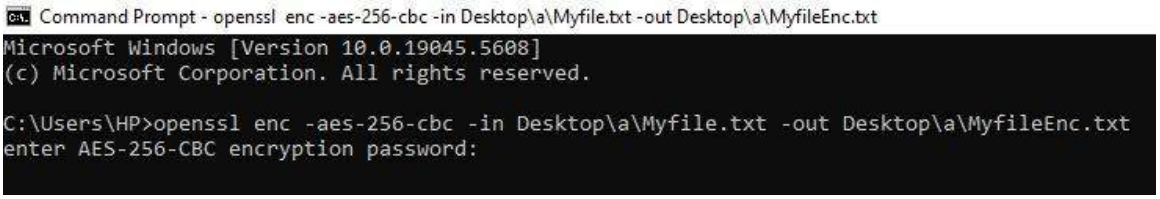
Openssl enc –aes-256-cbc –in Desktop\Myfolder\ Myfile.txt –out Desktop\ Myfolder\ MyfileEnc.txt



الشكل (2-11)

بعد تنفيذ الامر , تظهر صيغة تطلب منك كتابة كلمة مرور(**Password**) , كما في الشكل (2-12).

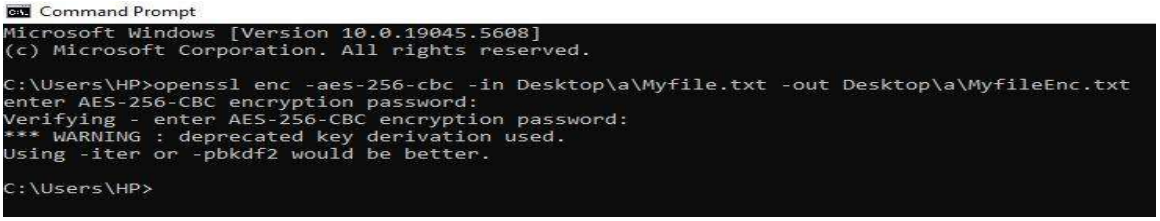
ملاحظة :- يجب كتابة كلمة مرور(**Password**) قوية جدا لكي يستجيب لها الأداة **OpenSSL**



الشكل (2-12)

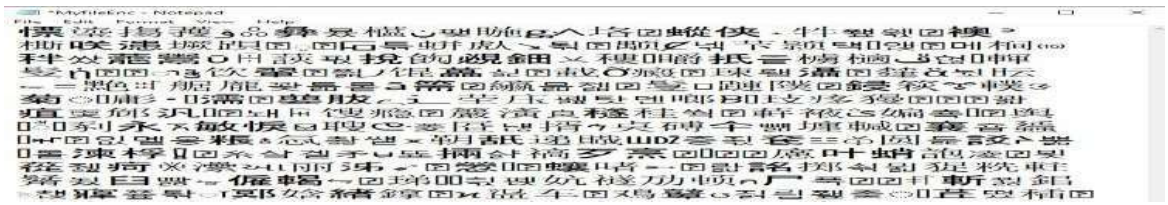
الخطوة 3: بعد إدخال كلمة المرور, من لوحة المفاتيح نضغط المفتاح (**Enter**) , ويجب كتابة كلمة المرور مرة ثانية , فنقوم بإدخال كلمة المرور مرة ثانية ونضغط المفتاح (**Enter**) .

ملاحظة :- عند كتابة كلمة مرور في نافذة موجه الأوامر لا تظهر في النافذة ويبقى مؤشر الكتابة في مكانه, كما في الشكل (2-13), وهذا أمر طبيعي واستمر بكتابة كلمة المرور ولا تقلق .



الشكل (2-13)

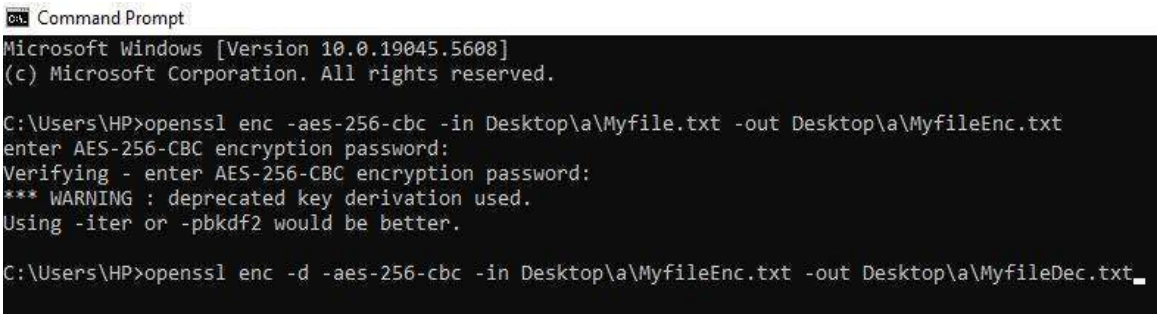
الخطوة 4: عند فتح المجلد (**Myfolder**) الموجود على سطح المكتب نلاحظ وجود ملف آخر باسم(**MyfileEnc**) , وعندما نقوم بفتحه نلاحظ أن النص مكتوب بشكل غير قابل للقراءة , كما في الشكل (2-14). ان اسم الملف (**MyfileEnc**) قد اخترناه في أمر التشفير في الخطوة 2 فراجع صيغة الأمر.



الشكل (2-14)

الخطوة 5: نقوم بفك تشفير ملف (**MyfileEnc**) باستخدم أمر فك التشفير في نافذة موجه الأوامر وتنفيذها, كما في الشكل (2-15).

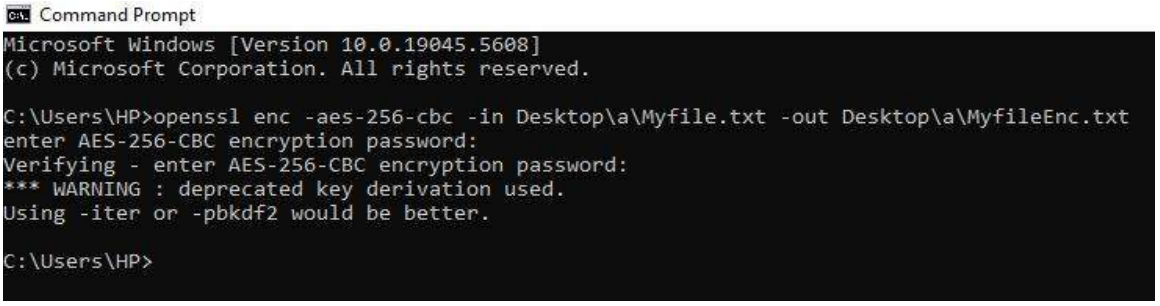
Openssl enc –d -256-cbc –in Desktop\ Myfolder\ MyfileEnc.txt –out Desktop \ Myfolder\ MyfileDec.txt



الشكل (2-15)

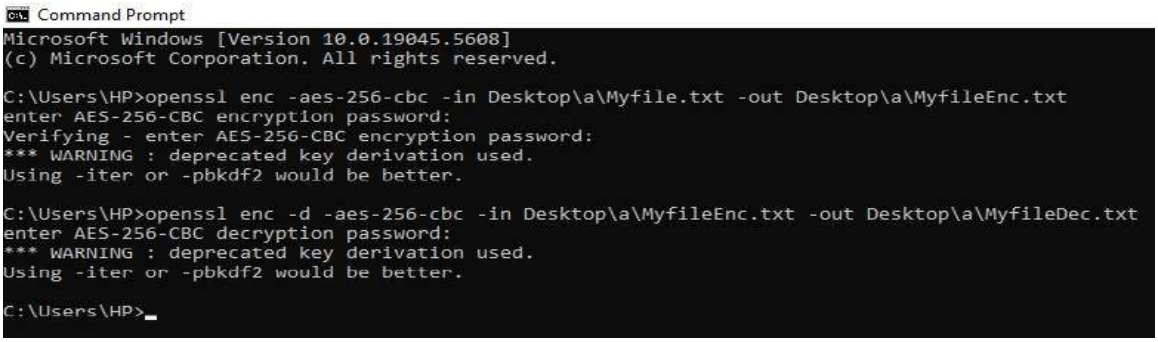
الخطوة 6: إدخال كلمة المرور السابقة ومن لوحة المفاتيح نضغط المفتاح (**Enter**) مرة واحدة فقط, كما في الشكل (2-16).

ملاحظة :- يجب كتابة كلمة المرور السابقة نفسها التي استخدمناها في عملية التشفير.



الشكل (2-16)

الخطوة 7: عند فتح المجلد (**Myfolder**) الموجود على سطح المكتب نلاحظ وجود ملف آخر باسم (**MyfileDec**) وعندما نقوم بفتحه نلاحظ ان النص مكتوب بشكل غير قابل للقراءة . اسم الملف (**MyfileDec**) قد اخترناه في امر فك التشفير في الخطوة 5 فراجع صيغة الامر



الشكل (2-17)

الخطوة 8: عند فتح المجلد (**Myfolder**) الموجود على سطح المكتب نلاحظ وجود ملف آخر باسم (**MyfileDec**) وعندما نقوم بفتح الملف نلاحظ ان النص المكتوب في الملف مشابة للنص المكتوب في الملف (**Myfile**) .

النتيجة المتوقعة

بعد تنفيذ هذا التمرين سيكون الطلبة قادرين على تشفير الملفات وإعادة فك تشفيرها باستخدام الأداة (**OpenSSL**)

استمارة الفحص تمرين رقم (2)			
الجهة الفاحصة:			
اسم الطالب :	**المرحلة الثالثة**	**التخصص : الامن السيبراني**	
اسم التمرين : تجربة تقنيات التشفير باستخدام اداة مثل OpenSSL لتشفير وفك تشفير الملفات			

ت	الخطوات	الدرجة القياسية % 50	درجة الاداء %50	الملاحظات
1	الدخول الى نافذة موجه الأوامر (Command Prompt)	%5		
2	تشفير الملف (Myfile) باستخدم أمر التشفير	%15		
3	فك تشفير ملف (MyfileEnc) باستخدم أمر فك التشفير	%15		
4	**المناقشة**	%5		
5	**الزمن المخصص**	%10		
المجموع				
اسم الفاحص		**التوقيع**		

تمرين رقم 3 : تكوين شبكة خاصة افتراضية VPN

الهدف من التمرين:

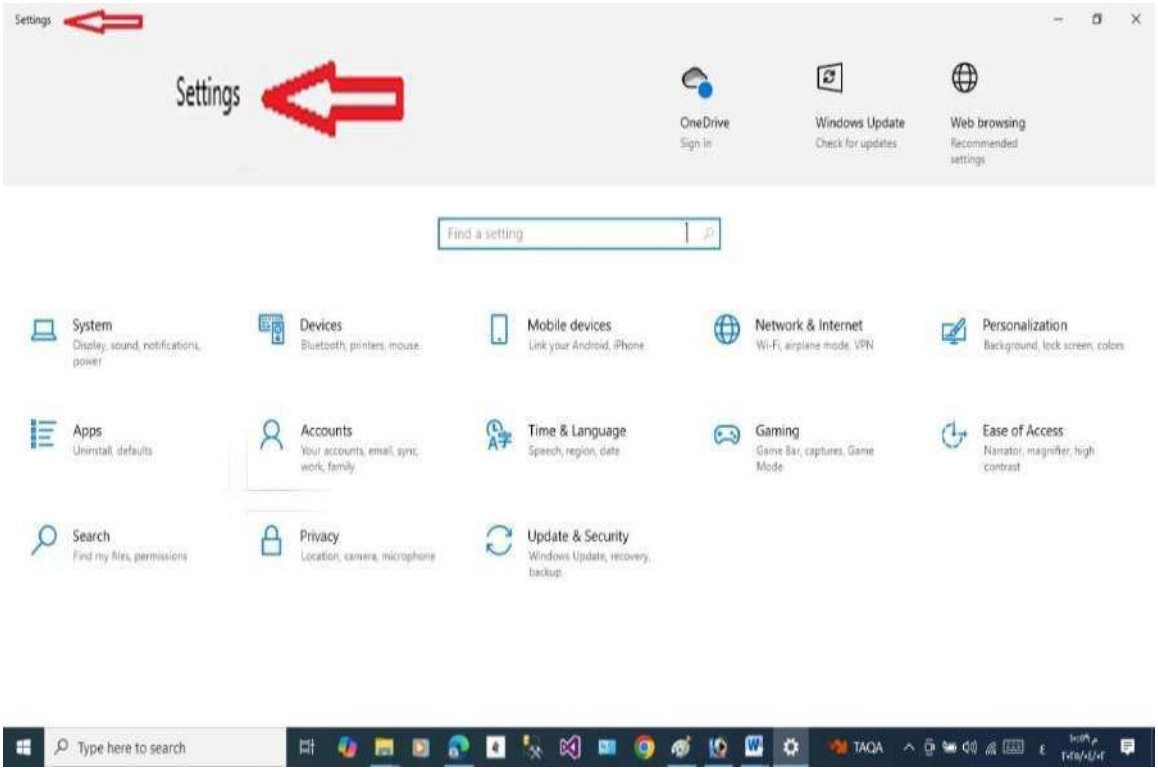
تعريف الطلاب بخطوات تكوين شبكة خاصة افتراضية (**VPN**)

المتطلبات الأساسية:

1. جهاز حاسوب منصب عليه نظام التشغيل (Windows10) ومتصل بالانترنت
2. تثبيت برنامج **VPNBOOK**

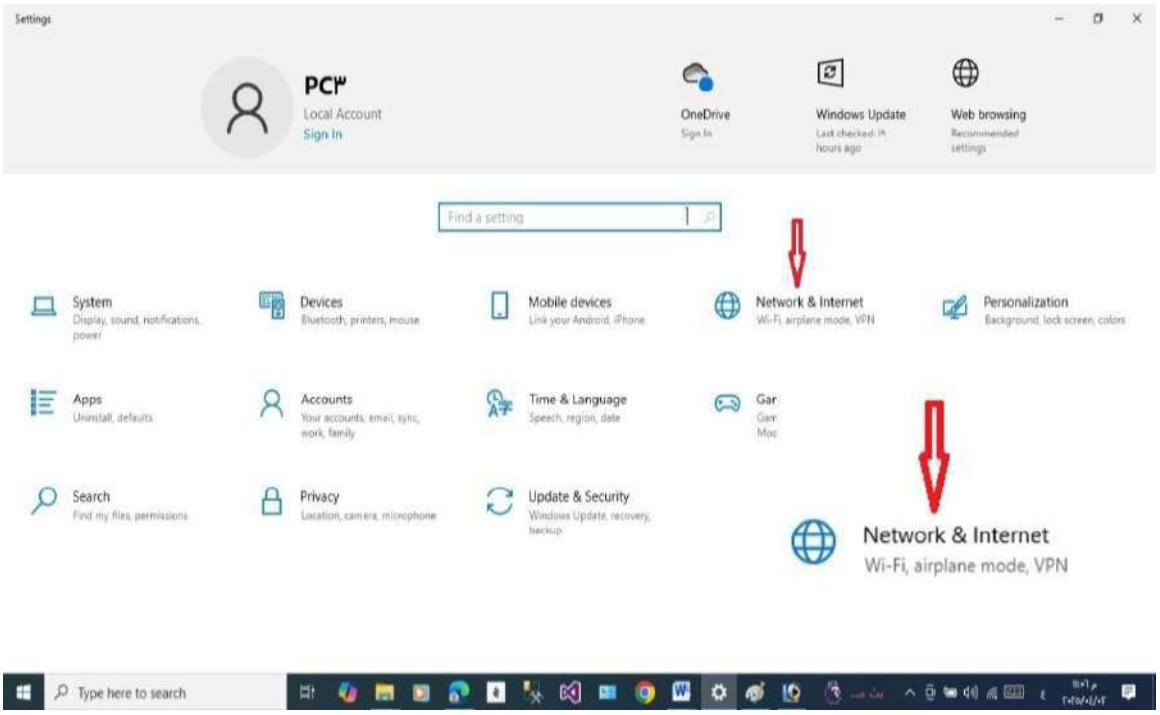
الخطوات العملية:

الخطوة 1: الدخول الى نافذة الإعدادات (**Settings**) . من قائمة ابدأ نقوم بالدخول إلى نافذة الإعدادات (**Settings**) فيها مجموعة اختيارات, كما في الشكل (2-18).



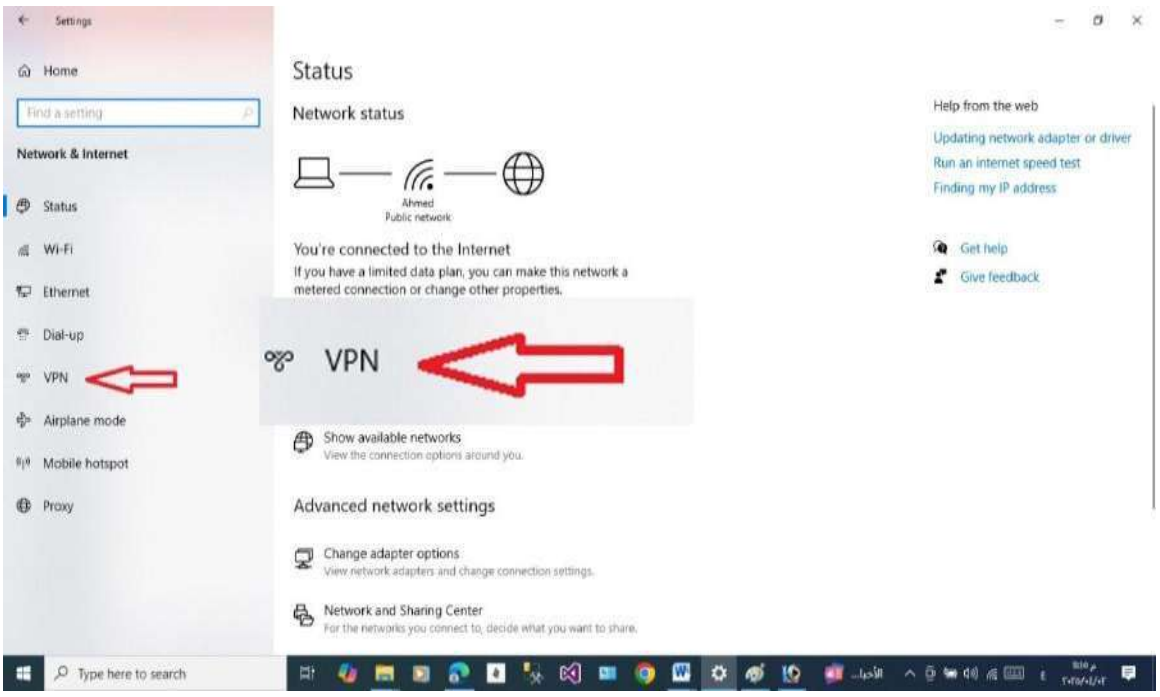
الشكل (2-18)

الخطوة 2: نضغط على الاختيار الشبكة والإنترنت (**Network & Internet**),كما في الشكل (2-19).



الشكل (2-19)

الخطوة 3: نضغط على الخيار عرض نوافذ الأمن (**VPN**) الموجودة في نافذة الشبكة والإنترنت , كما في الشكل (2-20).

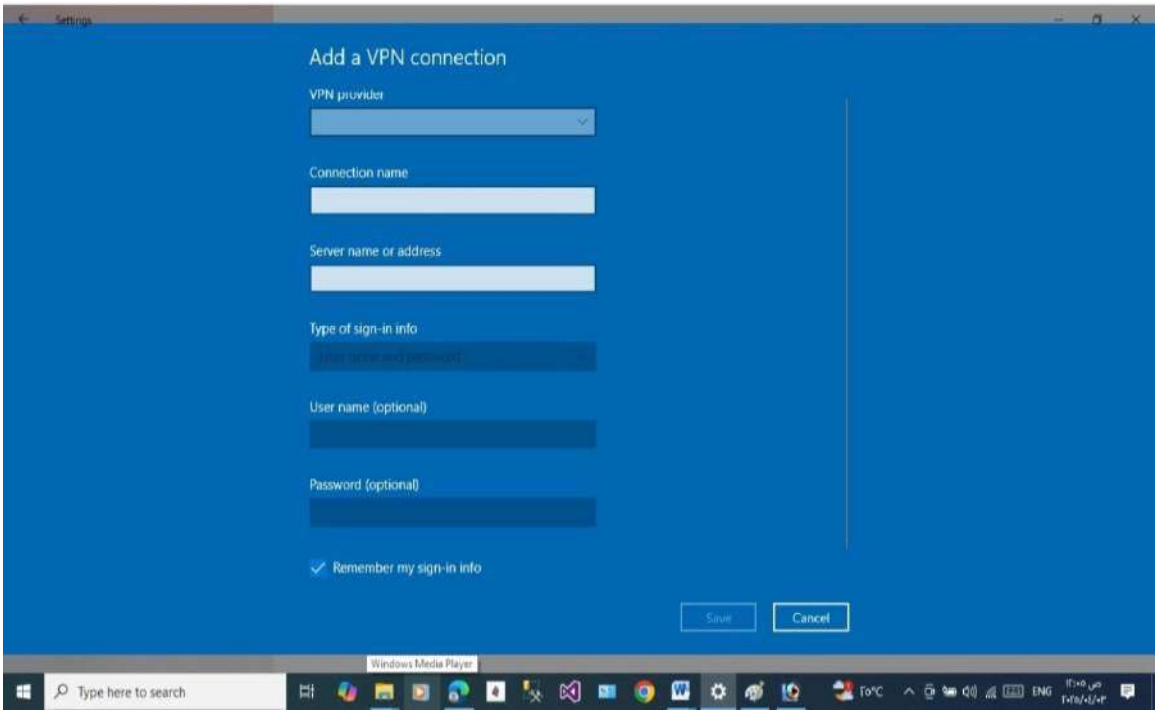


الشكل (2-20)

الخطوة 4: نضغط على الخيار (**Add a VPN connection**) الموجودة في نافذة الشبكة والإنترنت, كما في الشكل (2-21).

الشكل (2-21)

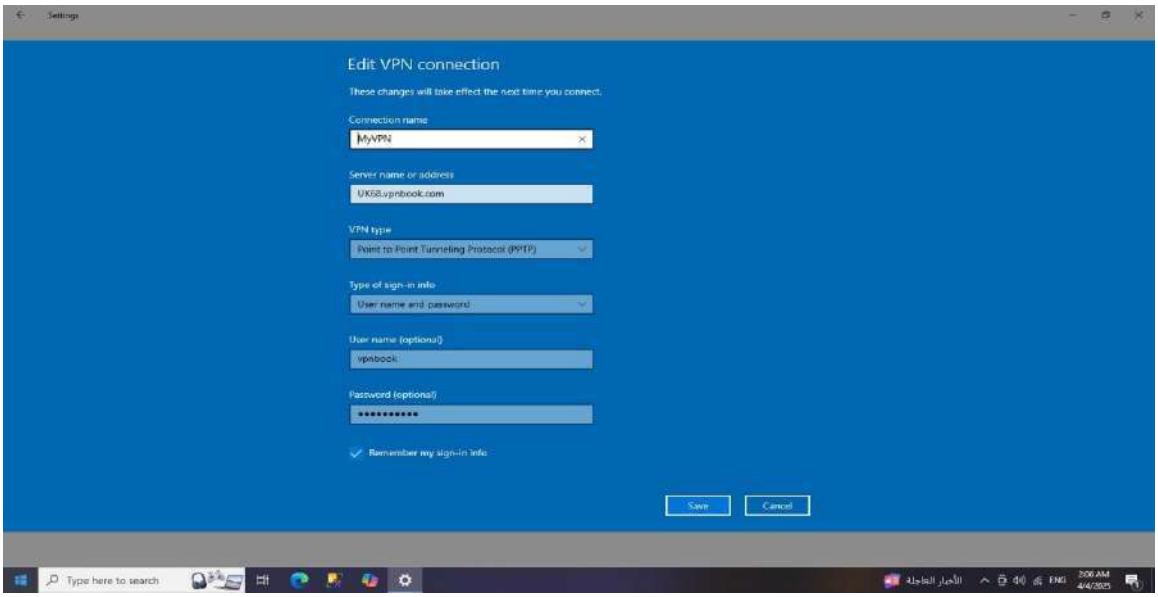
الخطوة 5: تظهر نافذة (**Add a VPN connection**) , كما في الشكل (2-22).



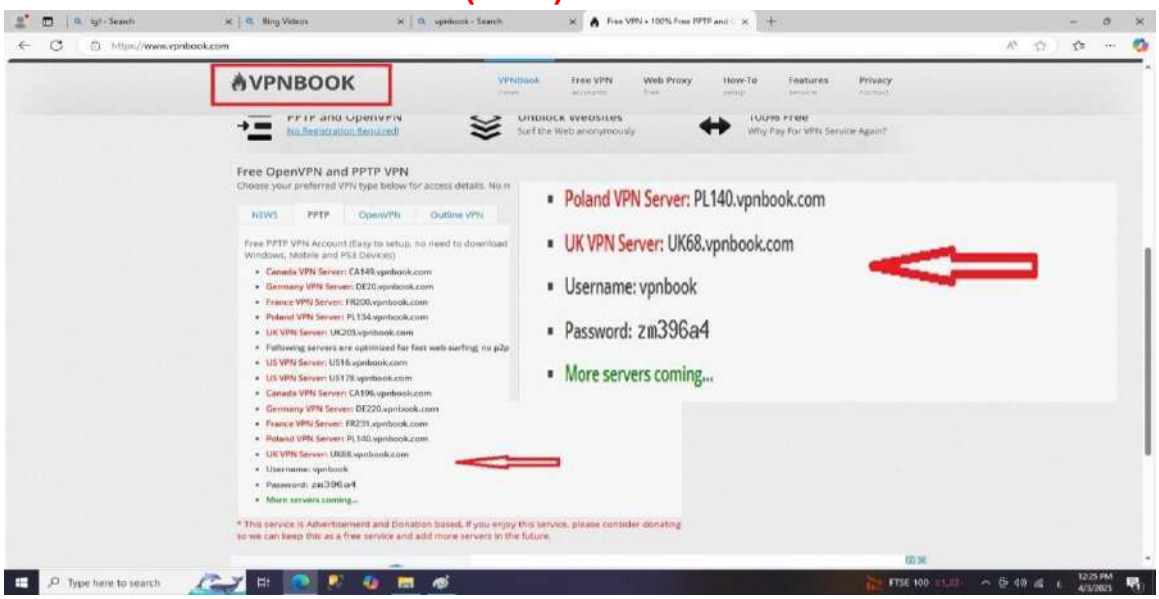
الشكل (2-22)

الخطوة 6: نقوم بملء الحقول الظاهرة في النافذة , وكما في الشكل (2-23) بما يأتي :-

- ✓ في الحقل **VPN Provider** نختار **Windows (built-in)**
- ✓ في الحقل **Connection name** نكتب اسم الشبكة وليكن **MyVPN**
- ✓ في الحقل **VPN Type** نختار **Point to Point Tunneling Protocol**
- ✓ في الحقل **Server name or address** نكتب اسم السيرفر ونأخذه من أحد المواقع المجانية الموجودة في **VPNBOOK** ومن النافذة **Free Open VPN and PPTP VPN**
- ✓ في الحقل **User name (optional)** نكتب اسم المستخدم من الموقع نفسه في الفقرة (4).
- ✓ في الحقل **Password (optional)** نكتب اسم المستخدم من الموقع نفسه في الفقرة (4) .



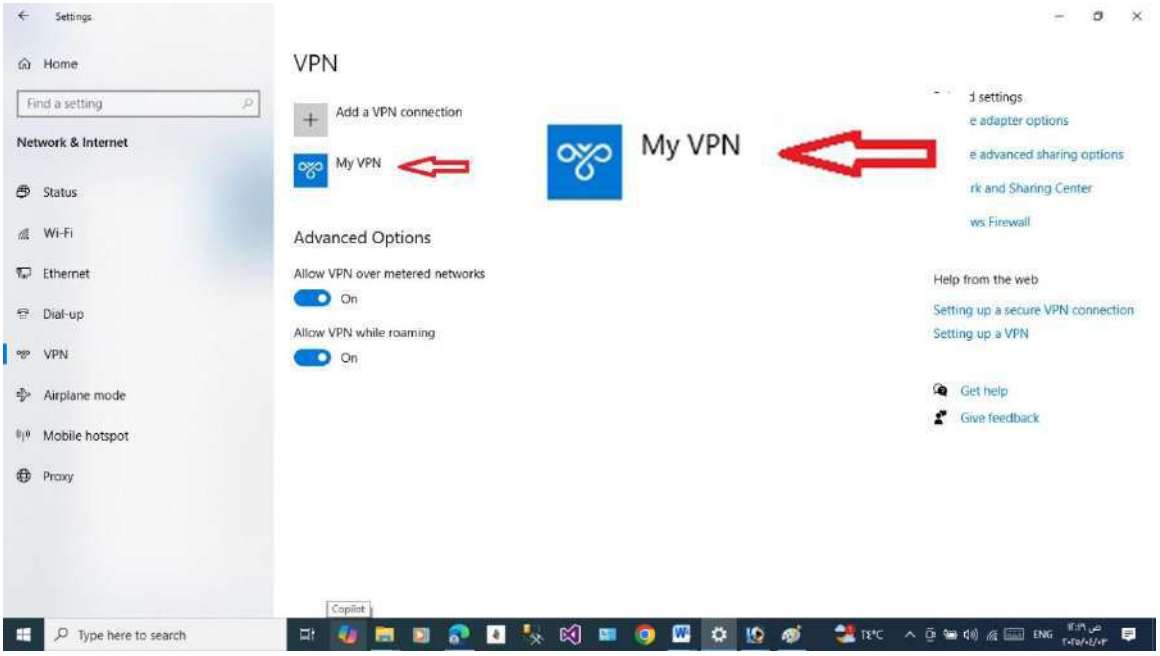
الشكل (2-23)



الشكل (2-24)

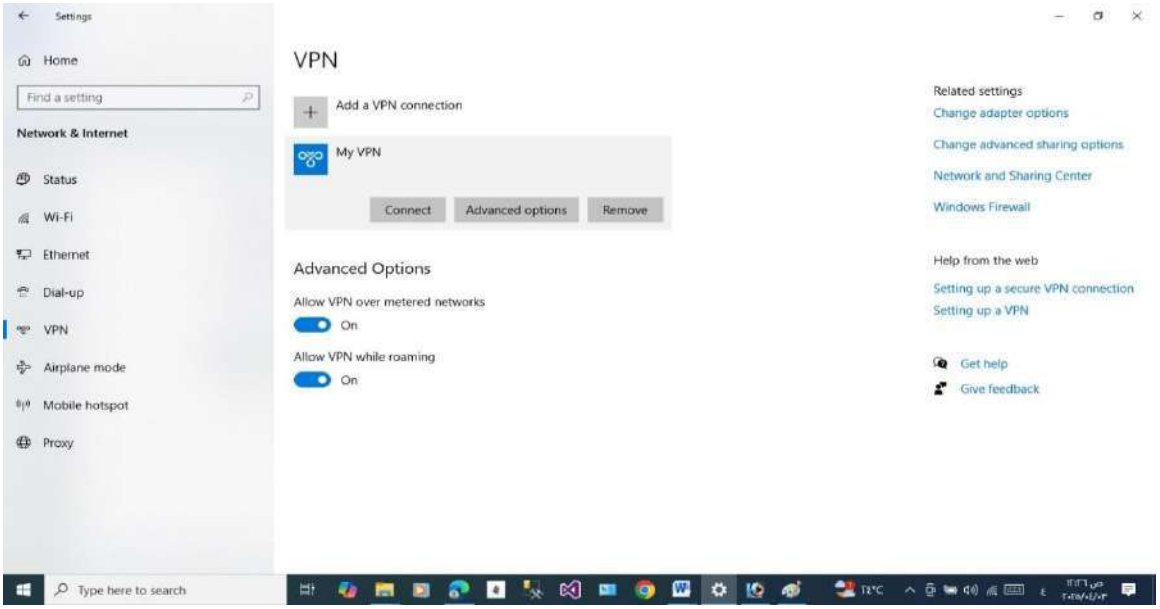
نضغط على المفتاح **Save** فتحفظ التعديلات على النافذة

الخطوة 7: نلاحظ ظهور ايقونة باسم الشبكة (**My VPN**) في صفحة **VPN** , وكما في الشكل (25-2)



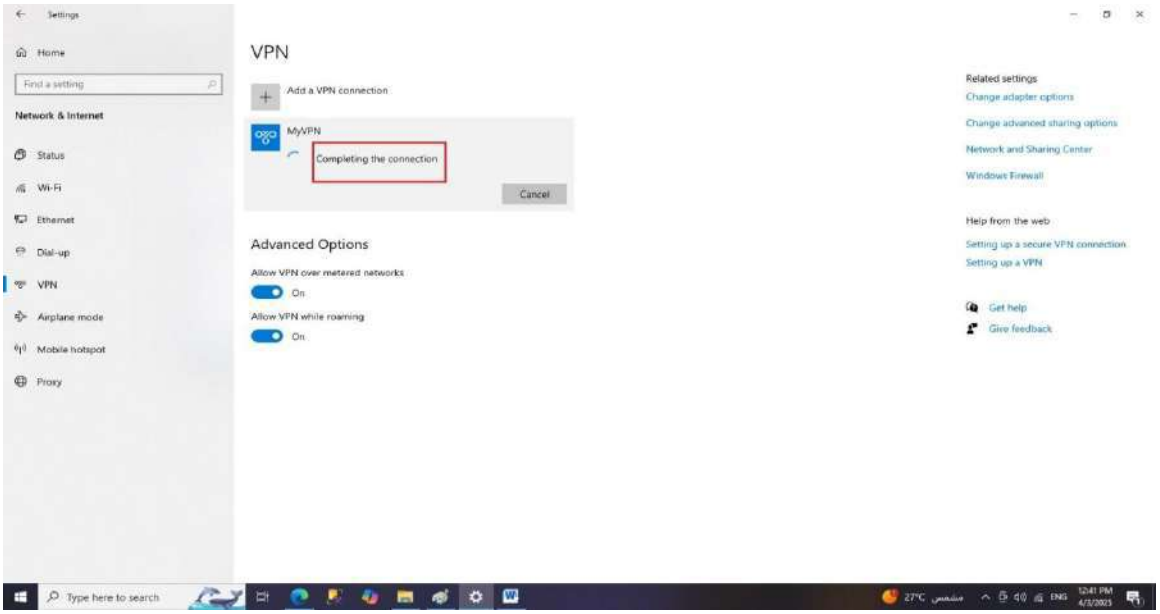
الشكل (2-25)

الخطوة 8: نضغط عل الأيقونة الخاصة باسم الشبكة (**My VPN**) فتظهر رسالة اختيارات نضغط على **Connect**, وكما في الشكل (2-26).



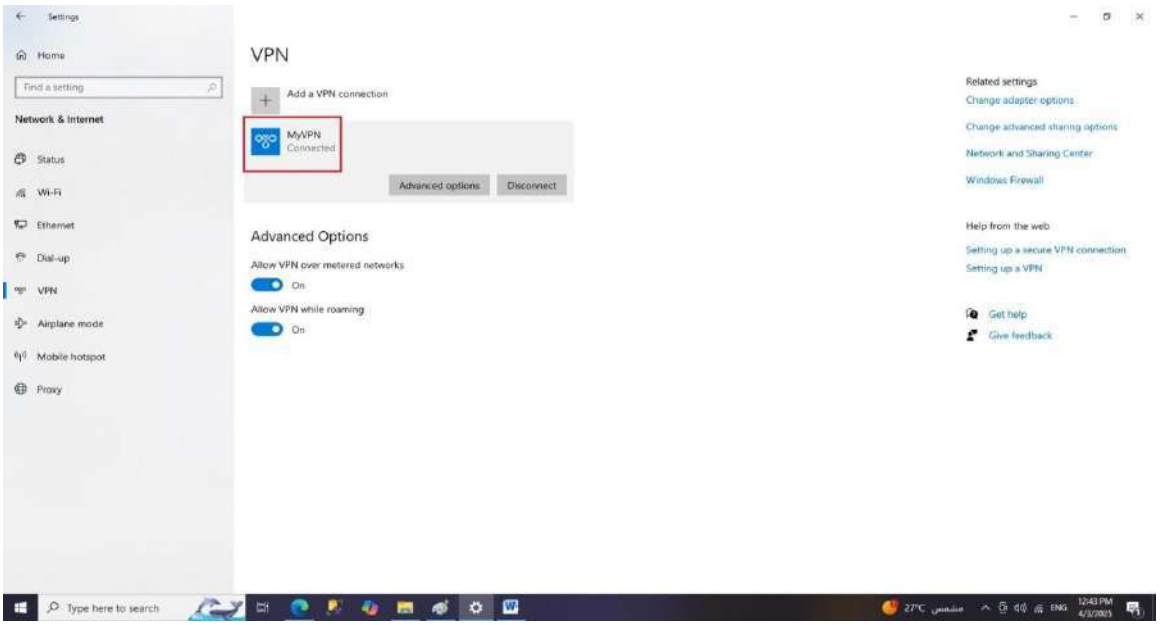
الشكل (2-26)

الخطوة 9: تبدأ عملية الاتصال بالشبكة الخاصة (**My VPN**) , وكما في الشكل (2-27).



الشكل (2-27)

الخطوة 10: عندما يتم الاتصال **Connect** بنجاح ستكون الشبكة (**My VPN**) جاهزة للعمل, وكما في الشكل (2-28).



الشكل (2-28)

النتيجة المتوقعة

بعد تنفيذ هذا التمرين سيكون الطلبة قادرين على تكوين شبكة خاصة افتراضية (**VPN**) بنجاح

استمارة الفحص تمرين رقم (3)			
الجهة الفاحصة:			
اسم الطالب :	المرحلة الثالثة	التخصص : الامن السيبراني	
اسم التمرين : تكوين شبكة خاصة افتراضية VPN			

ت	الخطوات	الدرجة القياسية % 50	درجة الاداء %50	الملاحظات
1	الدخول الى نافذة الإعدادات (Settings)	%5		
2	اختيار الشبكة والأنترنت (Network & Internet)	%5		
3	اضافة شبكة (VPN) جديدة من خلال الاختيار (Add a VPN connection)	%5		
4	ملء الحقول الظاهرة في النافذة بنجاح	%5		
5	ظهور الايقونة الخاصة باسم الشبكة (VPN) الجديدة	%5		
6	عمل الاتصال مع شبكة (VPN) الجديدة	%5		
7	المناقشة	%10		
8	الزمن المخصص	%10		
المجموع				
اسم الفاحص		التوقيع		

تمرين رقم 4 : استخدام أداة Wireshark لاكتشاف حركة البيانات المشبوهة في الشبكة

هدف من التمرين:

تعريف الطلاب باستخدام أداة **Wireshark** لاكتشاف حركة البيانات المشبوهة في الشبكة

المتطلبات الأساسية:

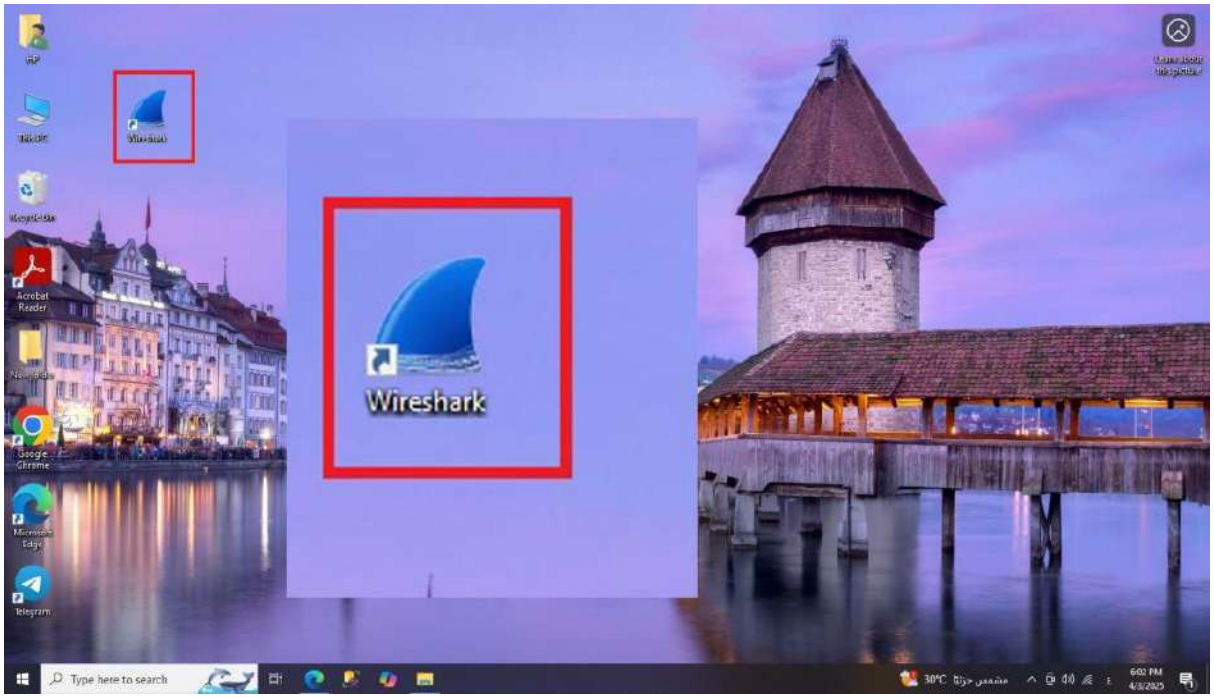
جهاز حاسوب منصب علية نظام التشغيل (Windows10)

تثبيت الاداة **Wireshark**

ملاحظة :- يجب تثبيت الاداة **Wireshark** حتى يتم تنفيذ هذا التمرين

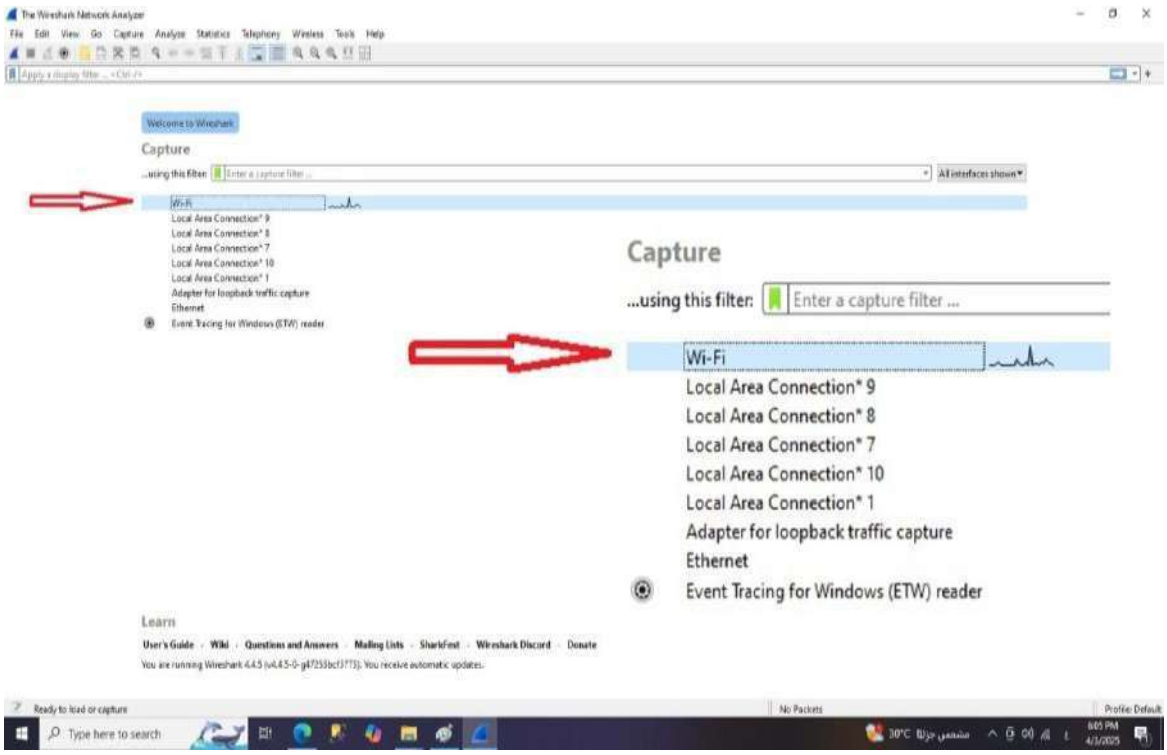
الخطوات العملية:

الخطوة 1: تشغيل الاداة **Wireshark** بالضغط على الايقونة الخاصة بها, وكما في الشكل (2-29).



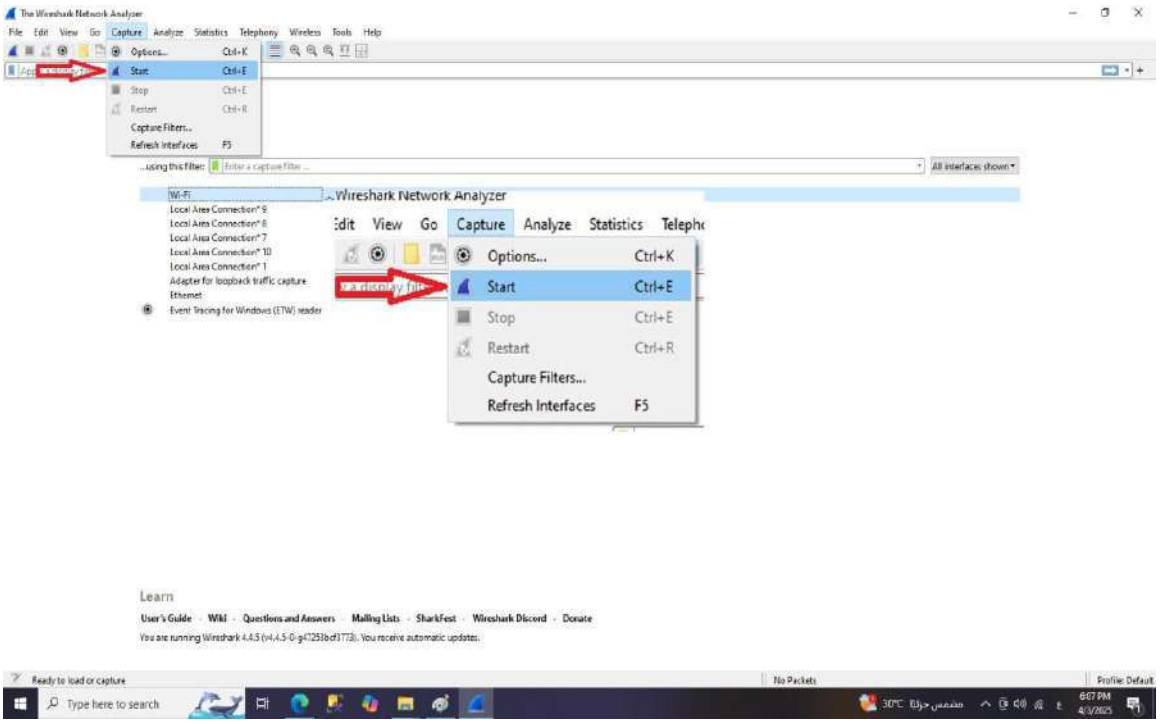
الشكل (2-29)

الخطوة 2: في النافذة تظهر مجموعة من الشبكات فنقوم باختيار الشبكة المراد عمل تحليل بياناتها و هي **Wi - Fi** , وكما في الشكل (2-30).



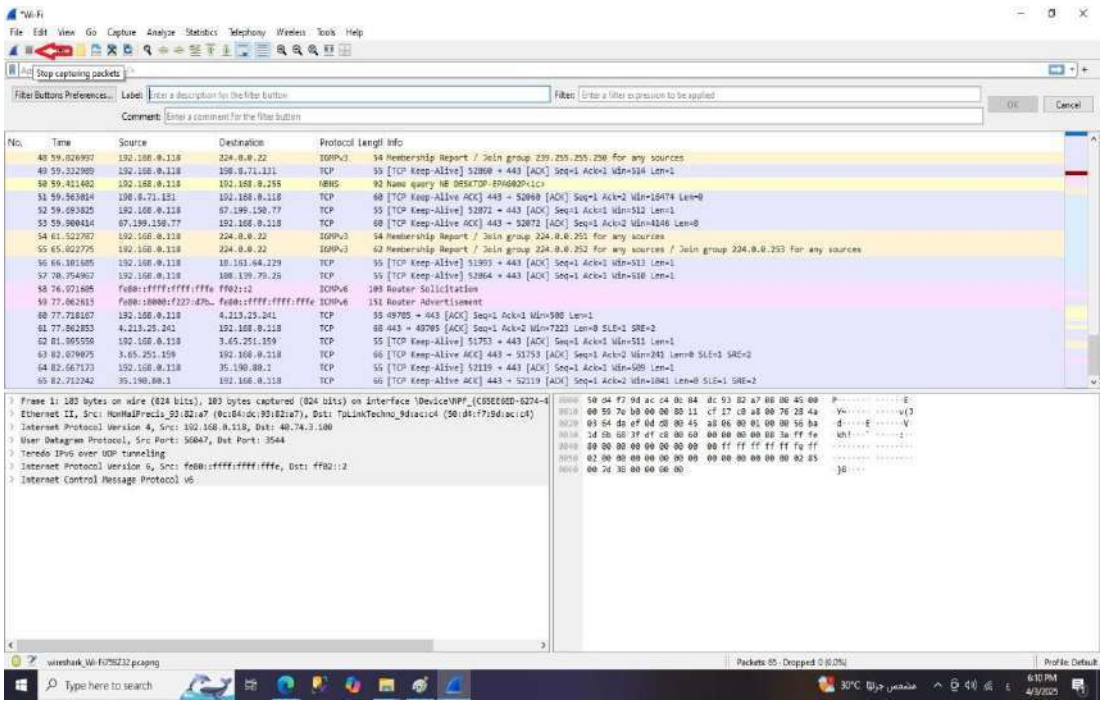
الشكل (2-30)

الخطوة 3: بعد اختيار الشبكة نضغط على المفتاح **Capture** الموجود في شريط القوائم فتظهر قائمة فيها اختيارات نضغط على الاختيار **Start** , وكما في الشكل (2-31).



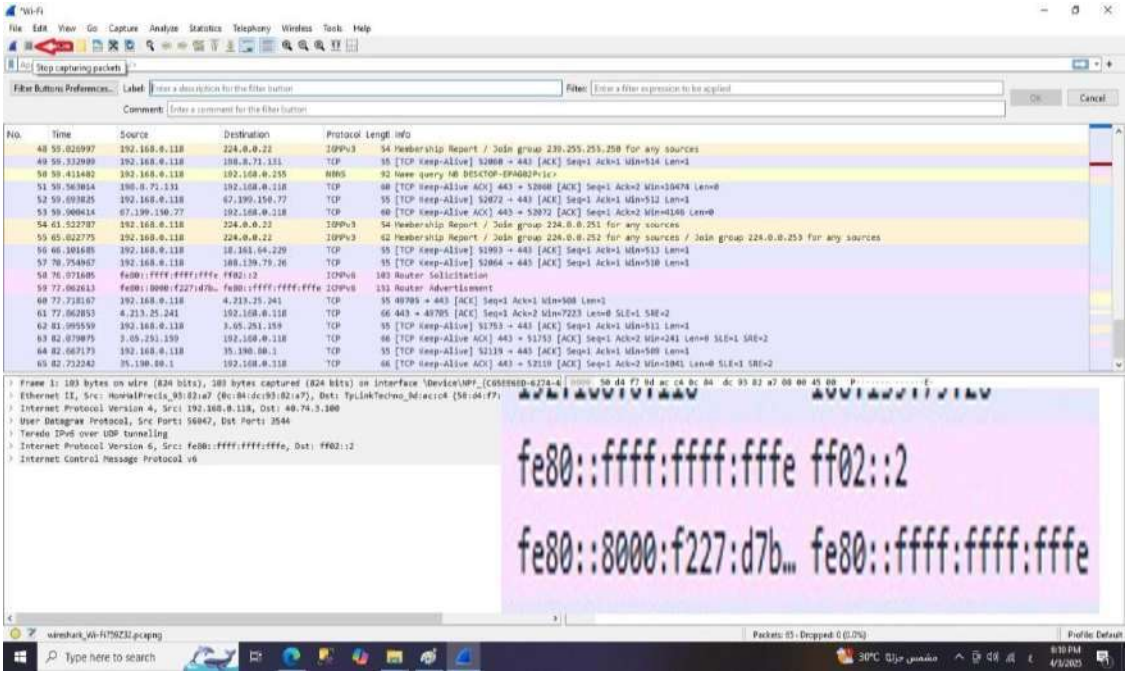
الشكل (2-31)

الخطوة 5: تبدأ الأداة **Wireshark** بتحليل البيانات , وكما في الشكل (2-32).



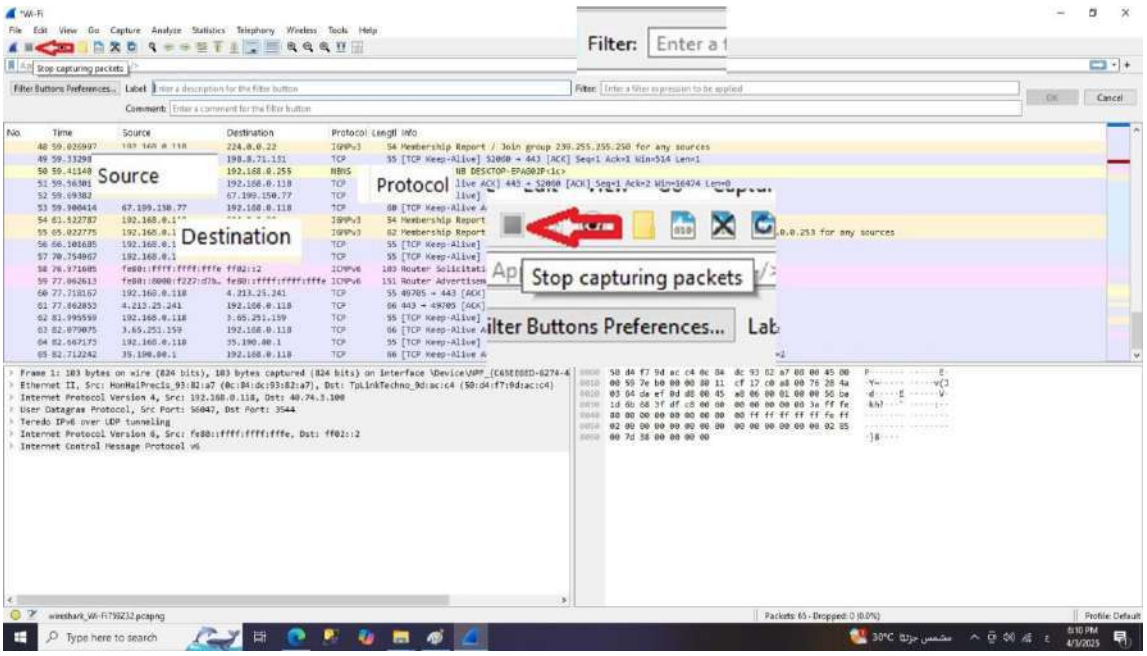
الشكل (2-32)

الخطوة 6: من متابعة حركة البيانات نلاحظ وجود بعض البيانات المشبوة في الشبكة, مثل البيانات التي تظهر بالنافذة في الشكل (2-33), التي هي عبارة عن بيانات فاشلة في التناقل.



الشكل (2-33)

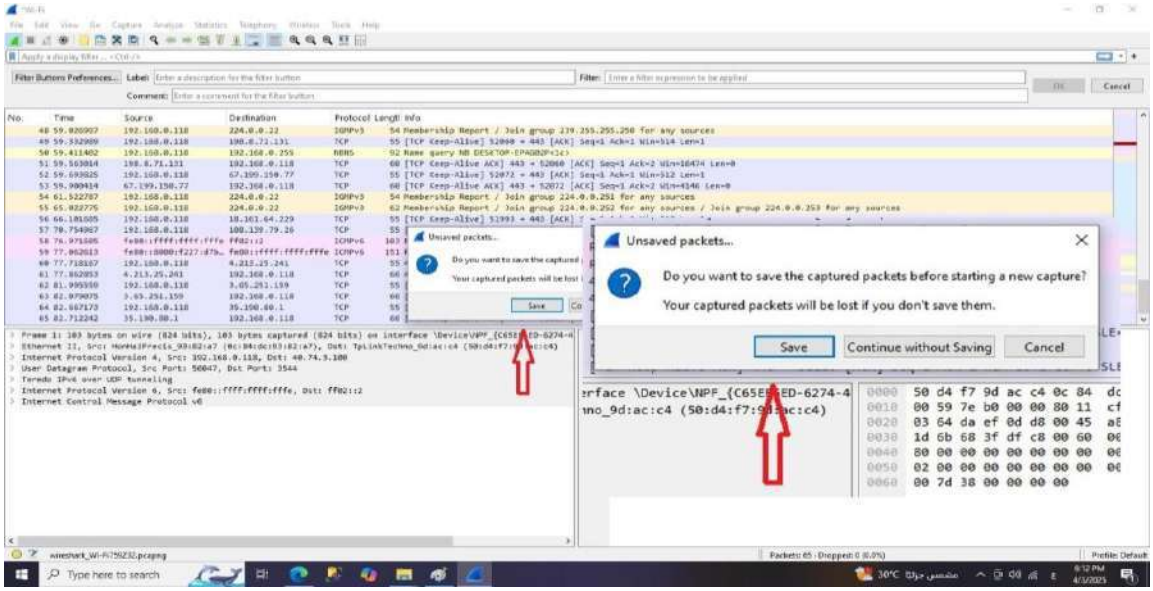
الخطوة 7: نستطيع أن نقوم بعمل فلترة للبيانات إما على أساس المصدر **Source**, أو على أساس الوجهة **Destination**, أو على أساس البروتوكول **Protocol**, وكما في الشكل (2-34).



الشكل (2-34)

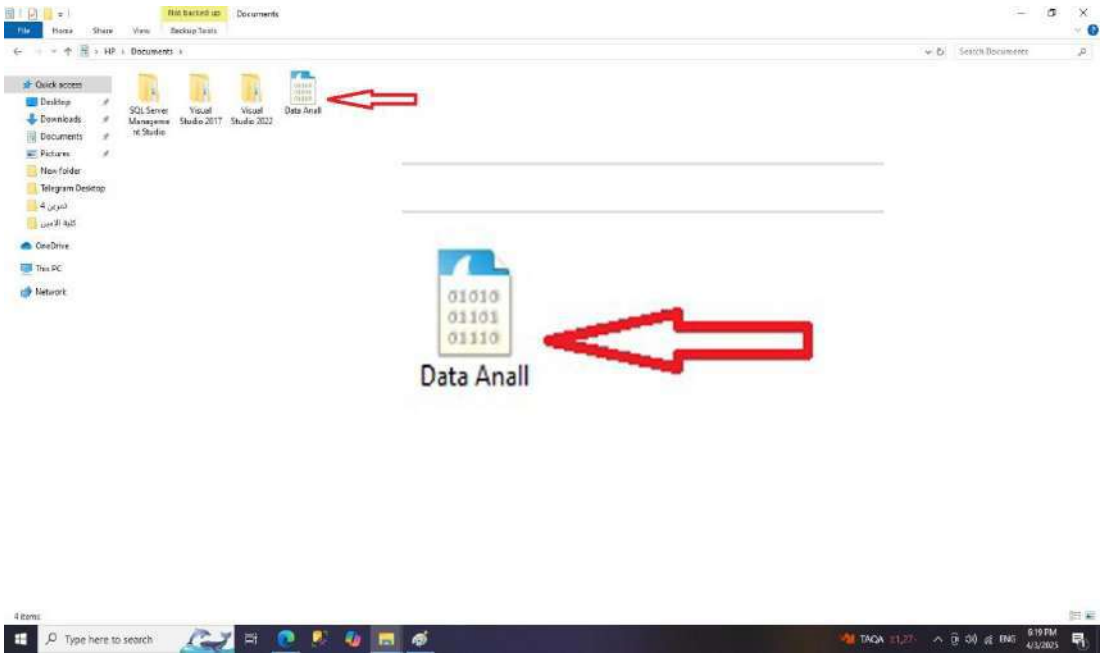
الخطوة 8: وتستمر عملية التحليل الى ان يتم توقيفها بالضغط على المفتاح **Stop** الموجود في القائمة. فتظهر رسالة فيها خيارات وكما في الشكل (2-35):-

- **إلغاء الأمر Cancel** عند الضغط عليه تعود عملية التحليل للبيانات مرة ثانية بعد أن توقفت.
- **الاستمرار بلا حفظ Continue without Saving** عند الضغط عليه سيخرج من الاداة.
- **حفظ Save** عند الضغط عليه ستحفظ البيانات المحللة في ملف, يمكن تشغيله في أي وقت.



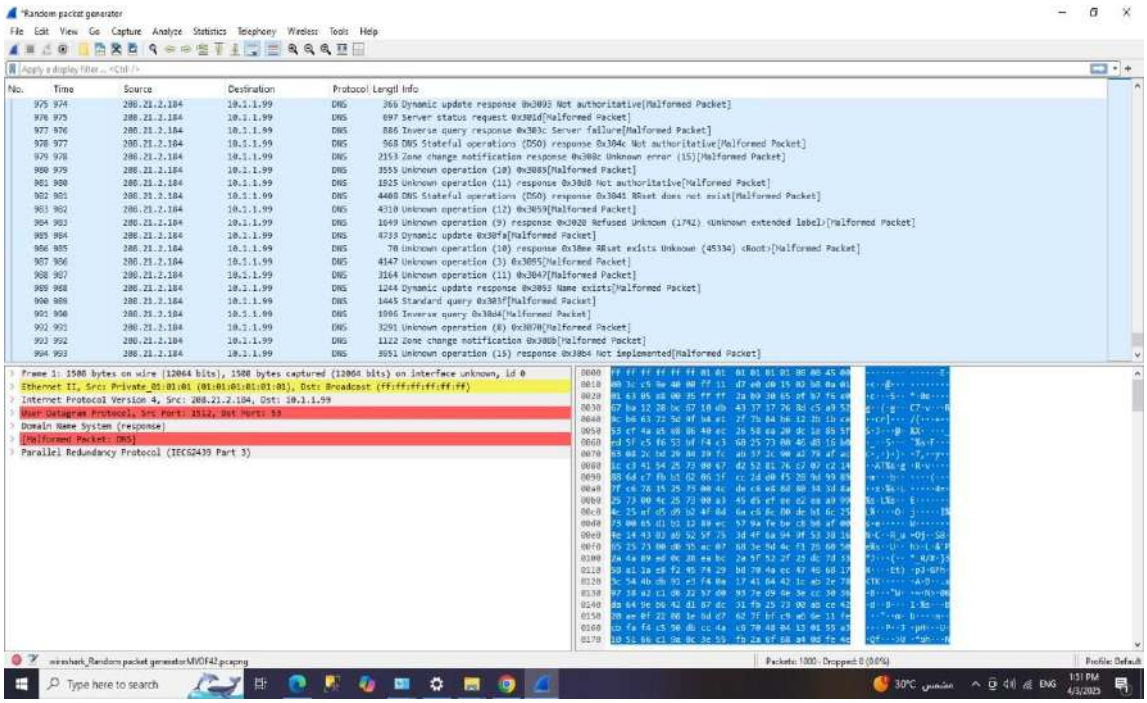
الشكل (2-35)

الخطوة 9: عند الضغط على المفتاح حفظ تظهر واجهة نختار منها المكان الذي نحفظ فية الملف, وكما في الشكل (2-36).



الشكل (2-36)

الخطوة 10: يمكن أن نسترجع البيانات مرة ثانية, وذلك بتشغيل الملف الذي تم حفظة في الخطوة رقم 8 وذلك بالضغط عليه نقرتين (**Double Click**) , وكما في الشكل (2-37).



الشكل (2-37)

النتيجة المتوقعة

بعد تنفيذ هذا التمرين سيكون الطلبة قادرين على استخدام الأداة **Wireshark** لاكتشاف حركة البيانات المشبوهة في الشبكة وحفظ البيانات في ملف يمكن تشغيله في وقت اخر.

استمارة الفحص تمرين رقم (4)			
الجهة الفاحصة:			
اسم الطالب :	المرحلة الثالثة	التخصص : الامن السيبراني	
اسم التمرين : استخدام أداة Wireshark لإكتشاف حركة البيانات المشبوة في الشبكة			

ت	الخطوات	الدرجة القياسية % 50	درجة الاداء %50	الملاحظات
1	تشغيل الاداة Wireshark , و اختيار الشبكة المراد عمل تحليل للبياناتها	%5		
2	البداء باجراء عملية تحليل بيانات الشبكة	%5		
3	التعرف اوتحديد البيانات المشبوه	%5		
4	عمل فلترة للبيانات على المصدر Source او الوجهة Destination او البروتوكول Protocol	%5		
5	ايقاف عملية فلترة البيانات وحفظها في ملف	%5		
6	استرجاع البيانات مرة ثانية من الملف الذي تم حفظة في الفقرة (5)	%5		
7	المناقشة	%10		
8	الزمن المخصص	%10		
المجموع				
اسم الفاحص		التوقيع		

أسئلة الفصل الثاني

س1: ما المقصود بأمن الشبكات ؟ وما المبادئ الأساسية لها ؟

س2: ما هي عناصر امان الشبكة ؟

س3: وضح المفاهيم الآتية (السرية والنزاهة والتوافر) .

س4: عرف الفيروسات , ثم عدد اهم انواعها .

س5: ما المقصود بالهجمات السيبرانية ؟ وما أسبابها ؟

س6: وضح مفهوم التشفير التماثلي , والتشفير غير التماثلي .

س7: وضح المفاهيم الآتية (تحديد الهوية والمصادقة والتفويض) .

س8: بين أهمية بروتوكولات الأمان .

س9: عدد مع الشرح مكونات حزمة البيانات .

س10: عدد البروتوكولات التي يقدمها بروتوكول الإنترنت الامن مع الشرح .

س11: عدد التحديات الخاصة ببروتوكول الانترنت الامن .

س12: ما الاختلافات بين البروتوكول (**HTTP**) والبروتوكول (**HTTPS**) ؟

س13: عدد أنواع الهجمات والتهديدات الإلكترونية .

س14: ما الفرق بين الهجمات **DoS** وهجمات **DDoS** ؟

س15: عدد أنواع هجمات رفض الخدمة الموزع (**DDoS**) .

س16: ما المقصود بالهجمات الخفية ؟ وما أنواعها ؟

س17: ما هي الاستراتيجيات المعتمدة للكشف عن الهجمات الخفية ؟

س18: ما الطرق التي يستخدمها نظام الكشف عن التسلل للكشف عن التهديدات ؟

س19: عدد طرق إعداد نظام منع التسلل .

س20: وضح مفهوم الشبكة الافتراضية الخاصة **VPN** .

الفصل الثالث

المفاهيم الأساسية للحوسبة السحابية

الهدف العام

تعليم الطالب المفاهيم الأساسية للحوسبة السحابية

الأهداف الخاصة

أن يكون الطالب قادرا على:-

- التعرف على مفهوم الحوسبة السحابية وأهميتها.
- التمييز بين أنواع الحوسبة السحابية.
- فهم نماذج الخدمات السحابية (IaaS, PaaS, SaaS).
- معرفة مكونات البنية التحتية السحابية وآلية الوصول للخدمات.
- إدراك مزايا وعيوب الحوسبة السحابية.
- اكتساب مهارات عملية في استخدام المنصات السحابية.
- تنفيذ تطبيقات بسيطة على بيئة السحابية.

::: مفردات الفصل :::

1-3 مفهوم الحوسبة السحابية

2-3 أنواع الحوسبة السحابية (عامة ، خاصة ، هجينة

3-3 مكونات الحوسبة السحابية

4-3 نماذج الخدمات السحابية(IaaS, PaaS, SaaS

البنية التحتية السحابية IPsec

كيفية الوصول إلى الخدمات السحابية

WPA2 / WPA / WEP

5-3 مزايا وعيوب الحوسبة السحابية.

التمارين العملية:

تمرين :1 إ تجربة إنشاء حساب علىGoogle Cloud

تمرين :2 استخدام Google Compute Engine لإنشاء جهاز افتراضي.

تمرين :3 إنشاء موقع ويب باستخدام Google Sites .

الفصل الثالث

المفاهيم الأساسية للحوسبة السحابية

1-3 مفهوم الحوسبة السحابية

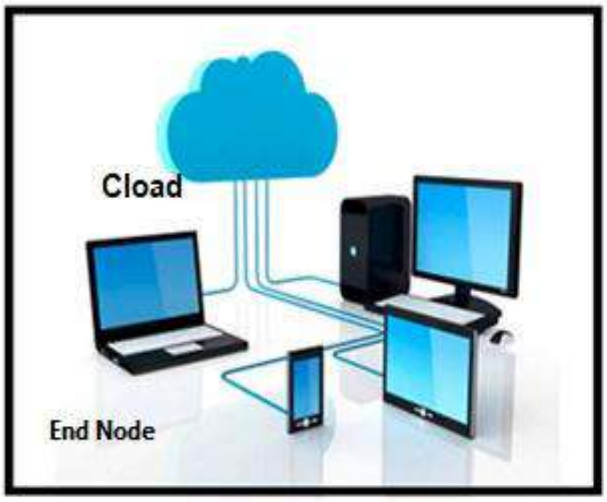
الحوسبة السحابية هي البنية التحتية لتكنلوجيا المعلومات, تعتمد على استخدام موارد الحاسبة والتخزين والشبكات لتمكين الوصول الملائم عند الطلب عبر الشبكة إلى مجموعة مشتركة من موارد الحوسبة القابلة للتكوين (مثل الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها وإطلاقها بسرعة بأقل جهد إداري وتفاعل مع مزود الخدمة .

ببساطة تعني استخدام الإنترنت لتوفير خدمات الحوسبة، مثل تخزين البيانات تشغيل البرامج، وتشغيل الخوادم دون الحاجة إلى امتلاك أجهزة مادية خاصة. وهنا ياتي التساؤل التالي:-

كيف تعمل الحوسبة السحابية؟

بدلاً من شراء خادم (كمبيوتر قوي) وتخزين البيانات عليه، يمكنك استخدام خدمات الحوسبة السحابية لتخزين بياناتك والوصول إليها من أي مكان عبر الإنترنت. تعتمد الحوسبة السحابية على مراكز بيانات (**Data Center**) ضخمة موزعة حول العالم، حيث يتم تخزين البيانات وتشغيل التطبيقات مثال أستخدام **Google Drive** لتخزين ملفاتك بدلاً من حفظها على جهاز الكمبيوتر (االتخزين التقليدي لشكل (1-3))، فأنت تستخدم الحوسبة السحابية (التخزين السحابي الشكل (2-3)) .

الشكل (1-3) التخزين التقليدي



الشكل (2-3) التخزين السحابي

2-3 أنواع الحوسبة السحابية

تعد الحوسبة السحابية من أبرز التقنيات الحديثة التي أحدثت تحولًا كبيرًا في طريقة تخزين البيانات وتشغيل التطبيقات وإدارة الخدمات التقنية عبر الإنترنت. تعتمد هذه التقنية على استخدام موارد الحوسبة عن بُعد، مما يوفر أداءً عاليًا وتكلفة أقل مقارنة بالبنية التحتية التقليدية. ومن أجل تلبية احتياجات المؤسسات والأفراد، صنفت الحوسبة السحابية في ثلاثة أنواع رئيسية وفقًا لكيفية نشرها وإدارتها، هي:

1-2-3 الحوسبة السحابية العامة (Public Cloud)

- تقديم هذه الخدمات للجميع عبر الإنترنت.
- تستخدمها الشركات الصغيرة والأفراد لأنها منخفضة التكلفة وسهلة الاستخدام.
- تعتمد على بنية تحتية مشتركة بين عدة مستخدمين.
- أمثلة **Google Cloud Platform (GCP)** :، **Amazon Web Services (AWS)**، **Microsoft Azure**.

الشكل (3-3) نموذج لخدمات السحابة العامة

2-2-3 الحوسبة السحابية الخاصة (Private Cloud)

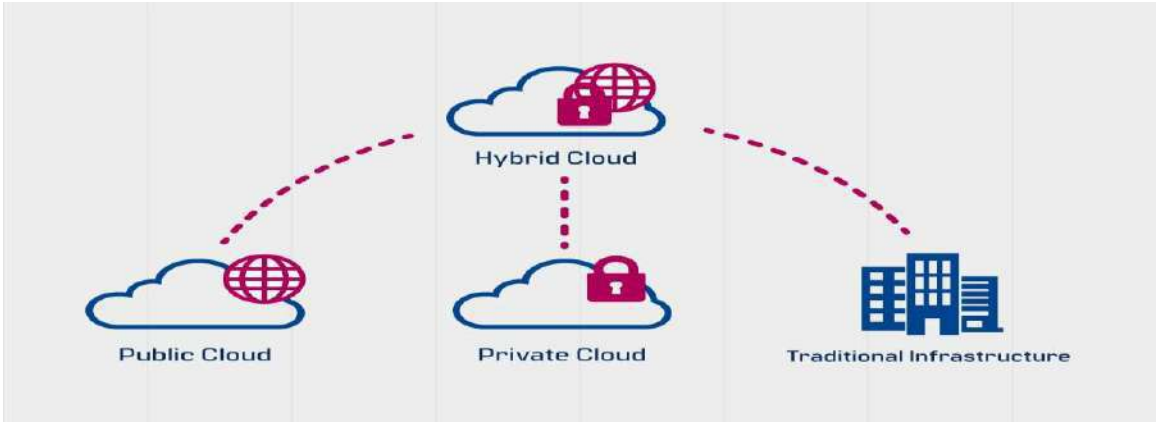
- تستخدمها الشركات الكبيرة والمؤسسات الحكومية.
- توفر أمانًا عاليًا لأن البيانات لا تُشارك مع مستخدمين آخرين.
- تعتمد على بنية تحتية مخصصة للشركة أو المؤسسة.
- يمكن أن تكون مُدارة داخليًا أو بواسطة طرف ثالث.

- أمثلة **IBM Cloud Private** : خدمات السحابة الخاصة للمؤسسات مثل **VMware**.

الشكل (3-4) نموذج لخدمات السحابة الخاصة

3-2-3 الحوسبة السحابية الهجينة (Hybrid Cloud)

- تجمع بين الحوسبة السحابية العامة والخاصة.
- تستخدمها الشركات التي تحتاج إلى توازن بين الأمان والمرونة.
- تسمح للشركات بتشغيل بعض التطبيقات على السحابة العامة (مثل التطبيقات التي تتطلب مرونة عالية) والبعض الآخر على السحابة الخاصة (مثل التطبيقات التي تتطلب أمانًا عاليًا).



الشكل (3-5) نموذج لخدمات السحابة الهجينة

3-3 مكونات الحوسبة السحابية

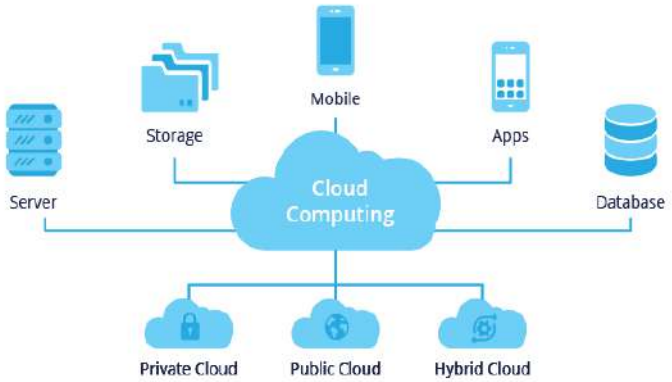
3-3-1 البنية التحتية السحابية

- تتكون من خوادم، شبكات، أنظمة تخزين، وبرامج تشغيل.
- تعمل في مراكز بيانات ضخمة موزعة حول العالم.
- تعتمد على تقنيات مثل المحاكاة الافتراضية (**Virtualization**) والتوزيع.(**Distribution**)

الشكل (3-6) مراكز بيانات ضخمة مملوءة بالخوادم

3-3-2 كيفية الوصول إلى الخدمات السحابية

- يمكن الوصول إليها عبر الإنترنت باستخدام:
- المتصفحات (مثل **Chrome**، **Firefox**).
- عبر التطبيقات المخصصة (مثل **Google Drive**).
- عبر واجهات برمجة التطبيقات (**APIs**).



الشكل (3-7) طرق الوصول إلى خدمات السحابية

4-3 نماذج الخدمات السحابية

تنقسم الخدمات السحابية على ثلاث فئات رئيسية:

1- البنية التحتية كخدمة (IaaS - Infrastructure as a Service)

يُعد (**IaaS**) وكما موضح في الشكل (3-8) النموذج الأساسي للحوسبة السحابية، حيث يوفر للمستخدمين موارد البنية التحتية الحاسوبية مثل الخوادم، والتخزين، والشبكات، ونظم التشغيل، دون الحاجة إلى امتلاك الأجهزة أو إدارتها بشكل مباشر. يُمكن للمستخدمين استئجار هذه الموارد عبر الإنترنت وتحدد وتكاليفها حسب الاستخدام.

الخصائص

1- توفير موارد حوسبية عند الطلب دون الحاجة إلى شراء أجهزة مادية.
2- دعم التوسع المرن، حيث يمكن زيادة أو تقليل الموارد وفق الحاجة.
3- المستخدم مسؤول عن إدارة التطبيقات ونظم التشغيل، بينما يدير مزود الخدمة البنية التحتية.
4- يعتمد على نموذج الدفع حسب الاستخدام.(**Pay-as-you-go**)

أمثلة على IaaS

Amazon **Web Services (AWS) – EC2**
Microsoft Azure - Virtual Machines
Google Cloud Compute Engine

الشكل (3-8) نموذج IaaS

2- المنصة كخدمة (PaaS - Platform as a Service)

يوفر نموذج **PaaS** و كما موضح في الشكل (3-9) بيئة تطوير متكاملة على السحابة، حيث يمكن للمطورين إنشاء التطبيقات واختبارها وتشغيلها دون الحاجة إلى القلق بشأن إدارة الخوادم أو أنظمة التشغيل أو التخزين. يتم توفير جميع الأدوات والموارد اللازمة لتطوير البرمجيات، مما يساعد على تقليل الوقت والجهد المبذولين في إعداد البنية التحتية.

الخصائص

- بيئة متكاملة لإنشاء وتشغيل التطبيقات دون الحاجة إلى إدارة البنية التحتية.
- دعم التطوير السريع ونشر التطبيقات بسهولة.
- توفير أدوات وخدمات مثل قواعد البيانات، بيئات التشغيل، وخوادم التطبيقات.
- مناسب للشركات والمطورين الذين يريدون التركيز على تطوير البرمجيات دون الانشغال بالإعدادات التقنية.

أمثلة على PaaS

- **Google App Engine**
- **Microsoft Azure App Services**
- **Heroku**

الشكل (3-9) نموذج PaaS

3- البرمجيات كخدمة (SaaS - Software as a Service)

يعد **SaaS** و كما موضح في الشكل (3-10) النموذج الأكثر استخدامًا بين الأفراد والشركات، حيث تقديم البرامج والتطبيقات عبر الإنترنت، مما يلغي الحاجة إلى تثبيتها على الأجهزة المحلية. يمكن للمستخدمين الوصول إلى هذه البرامج من متصفح الويب ودفع اشتراك شهري أو سنوي لاستخدامها.

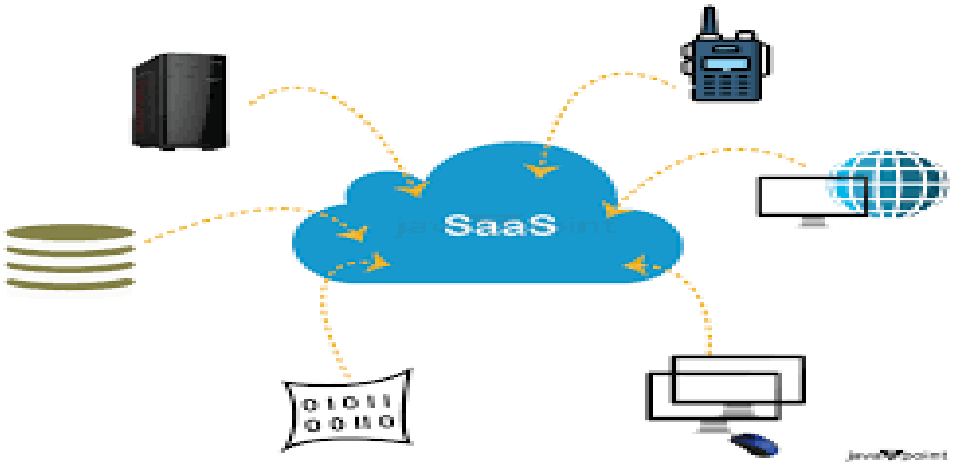
الخصائص

- لا يحتاج المستخدم إلى تثبيت أو إدارة التطبيقات، لأنها تشغل مباشرة عبر الإنترنت.
- يتم تحديث البرامج وصيانتها تلقائيًا من مزود الخدمة.
- يُستخدم عادة في التطبيقات المكتبية، برامج إدارة المشاريع، البريد الإلكتروني، وأنظمة إدارة علاقات العملاء.(**CRM**)

- مناسب للأفراد والشركات التي تحتاج إلى حلول جاهزة دون الحاجة إلى تطوير برامج خاصة بها.

أمثلة علىSaaS

- **Google Workspace (Gmail, Google Drive, Google Docs)**
- **Microsoft 365 (Word, Excel, Outlook, Teams)**
- **Salesforce – CRM**



الشكل (3-10) نموذج SaaS

3-5 ميزات وعيوب الحوسبة السحابية

3-5-1 مميزات الحوسبة السحابية:

1- **توفير التكاليف:** لا تحتاج إلى شراء أجهزة غالية الثمن أو توظيف خبراء لإدارتها.
2- **إمكانية الوصول من أي مكان:** تحتاج فقط إلى الإنترنت.
3- **قابلية التوسع:** يمكنك زيادة أو تقليل الموارد حسب الحاجة.
4- **المرونة:** يمكنك اختيار الخدمات التي تحتاجها فقط.
5- **التحديثات التلقائية:** يتم تحديث البرامج والتطبيقات تلقائيًا.

3-5-2 عيوب الحوسبة السحابية:

1- **مخاوف الأمان :** تحتاج إلى حماية قوية للبيانات من الاختراق.
2- **الاعتماد على الإنترنت :** لا يمكن الوصول للخدمات في حال انقطاع الإنترنت.
3- **التحكم المحدود :** بعض الخدمات لا تسمح بتخصيص كامل للإعدادات.
4- **الامتثال :** قد يكون من الصعب الامتثال للوائح تنظيمية معينة عند تخزين البيانات في السحابة.
5- **نقل البيانات :** قد يكون نقل كميات كبيرة من البيانات إلى السحابة مكلفًا ويستغرق وقتًا طويلاً.

تمرين رقم 1 : إنشاء حساب على Google Cloud

الهدف من التمرين:

تعريف الطلاب بخطوات إنشاء حساب على **Google Cloud** .

المتطلبات الأساسية:

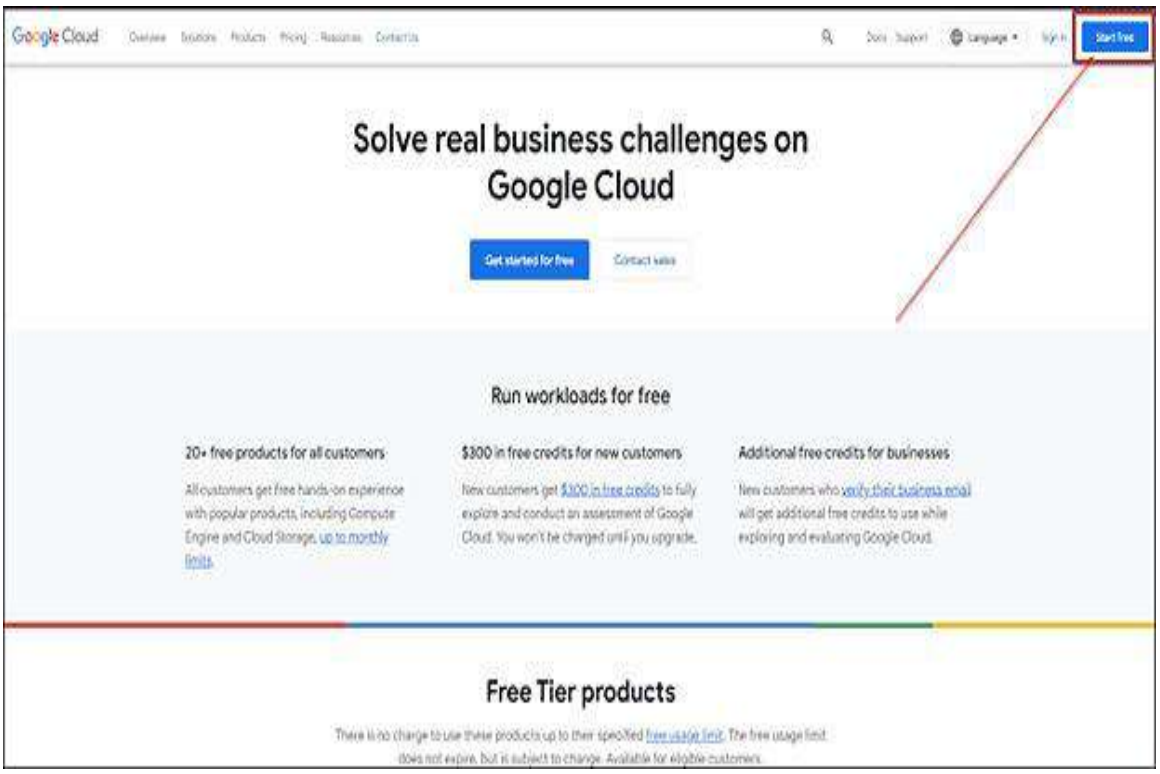
1. اتصال بالإنترنت.
2. حساب **Gmail** فعال.
3. متصفح ويب مثل **Google Chrome** أو **Mozilla Firefox** .

الخطوات العملية:

الخطوة 1: فتح موقع **Google Cloud**

افتح المتصفح وانتقل إلى **Google Cloud** كما موضح في الشكل (3-11) .

اضغط على زر **"Get started for free"** أو "ابدأ مجانًا."



الشكل (3-11)

ملاحظة : يجب أن يكون لديك حساب **Gmail** لاستخدام هذه الخدمة.

الخطوة 2: تسجيل الدخول بحساب **Google**

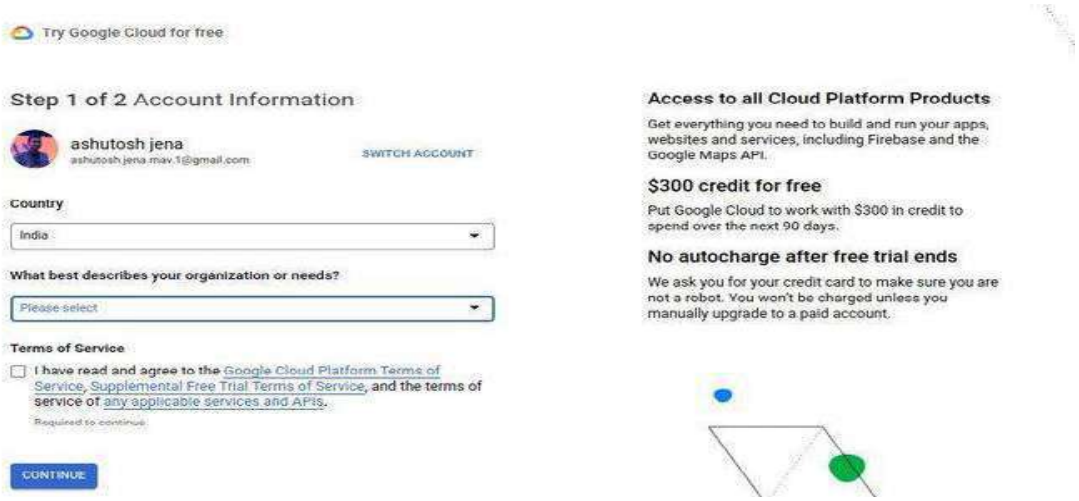
عند ظهور صفحة تسجيل الدخول، أدخل بريدك الإلكتروني واضغط التالي.

أدخل كلمة المرور الخاصة بك، ثم اضغط التالي.

الخطوة 3: الموافقة على شروط الخدمة

ستظهر صفحة تطلب منك الموافقة على شروط وأحكام **Google Cloud**.

اقرأ الشروط، ثم اضغط على أوافق أو **Accept**. كما موضح في الشكل (3-12)



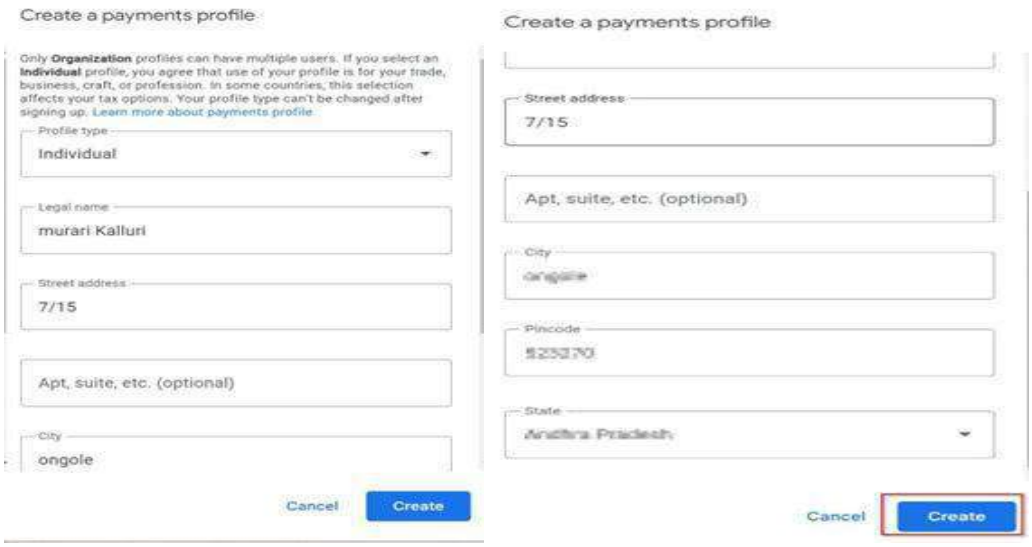
الشكل (3-12)

الخطوة 4: إدخال معلومات الحساب

اختر دولتك مثلاً: العراق.

أدخل معلومات الحساب المطلوبة، مثل الاسم ورقم الهاتف.

اختر "**Individual**"(فردي) عند طلب نوع الحساب كما موضح في الشكل (3-13).

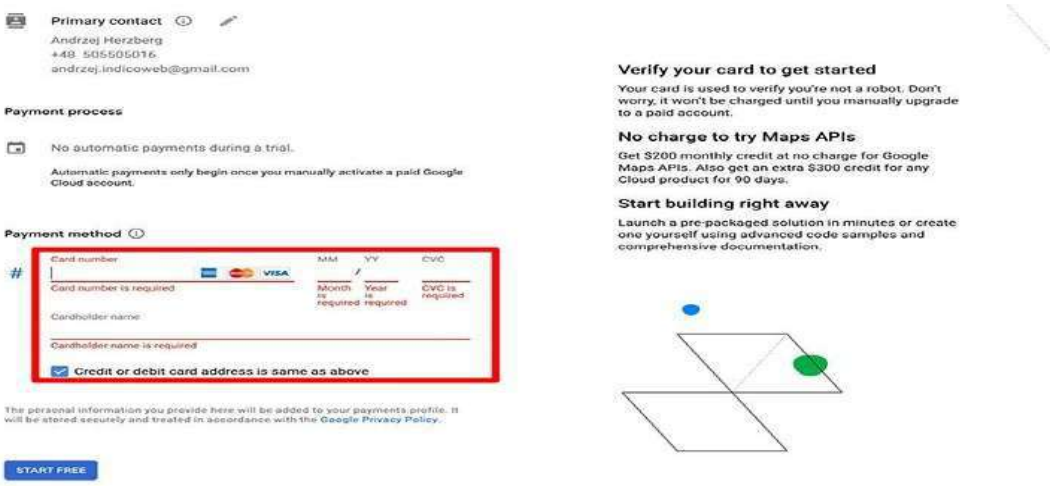


الشكل (3-13)

الخطوة 5: إضافة وسيلة دفع (اختياري)

أدخل تفاصيل البطاقة الائتمانية أو اختر وسيلة دفع أخرى.

اضغط "ابدأ تجربتك المجانية." كما موضح في الشكل (3-14).

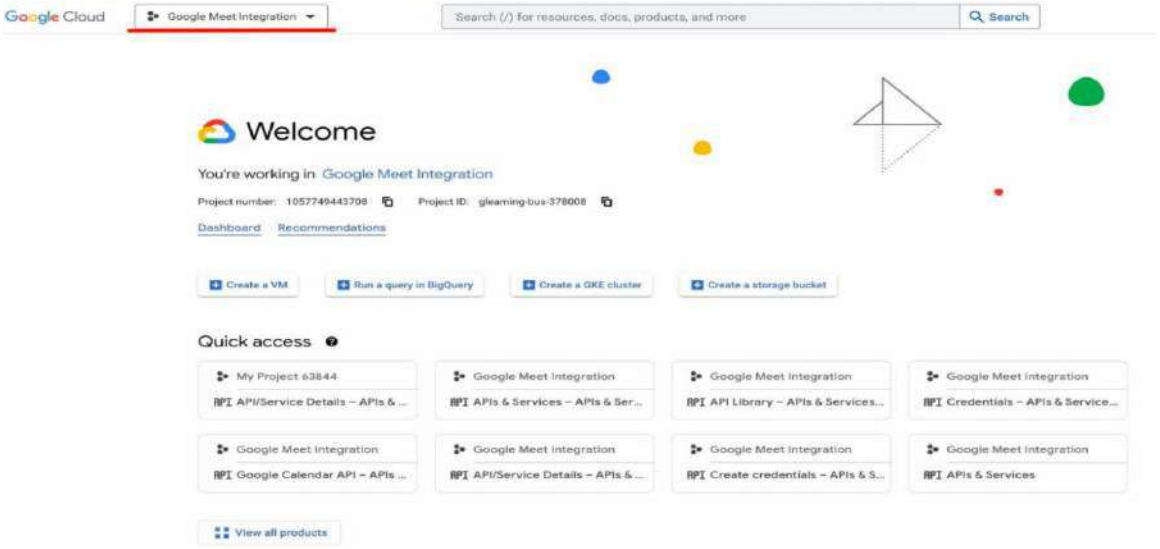


الشكل (3-14)

الخطوة 6: تفعيل الحساب

بعد إدخال معلومات الدفع، سيتم التحقق من الحساب.

عند نجاح العملية، سيتم توجيهك إلى لوحة تحكم **Google Cloud** كما موضح في الشكل (3-15).



الشكل (3-15)

النتيجة المتوقعة:

بعد تنفيذ هذا التمرين سيكون الطلبة قادرين على إنشاء حساب مفعّل على **Google Cloud** ، ويمكن البدء في استخدامه

استمارة الفحص تمرين رقم (1)			
الجهة الفاحصة:			
اسم الطالب :	المرحلة الثالثة	التخصص : الامن السيبراني	
اسم التمرين : انشاء حساب على Google Cloud			
ت	الخطوات	الدرجة القياسية % 50	درجة الاداء %50	الملاحظات
1	فتح موقع Google Cloud	%5		
2	تسجيل الدخول بحساب Google والموافقة على شروط الخدمة	%10		
3	إدخال معلومات الحساب	%10		
4	تفعيل الحساب	%5		
5	المناقشة	%10		
6	الزمن المخصص	%10		
المجموع				
اسم الفاحص		التوقيع		

تمرين رقم 2 : استخدام Google Compute Engine لإنشاء جهاز افتراضي مع تطبيق بسيط

الهدف من التمرين:

تعلم كيفية إنشاء جهاز افتراضي (**VM / Virtual Machine**) باستخدام **Google Compute Engine** ضمن **Google Cloud** .

المتطلبات الأساسية:

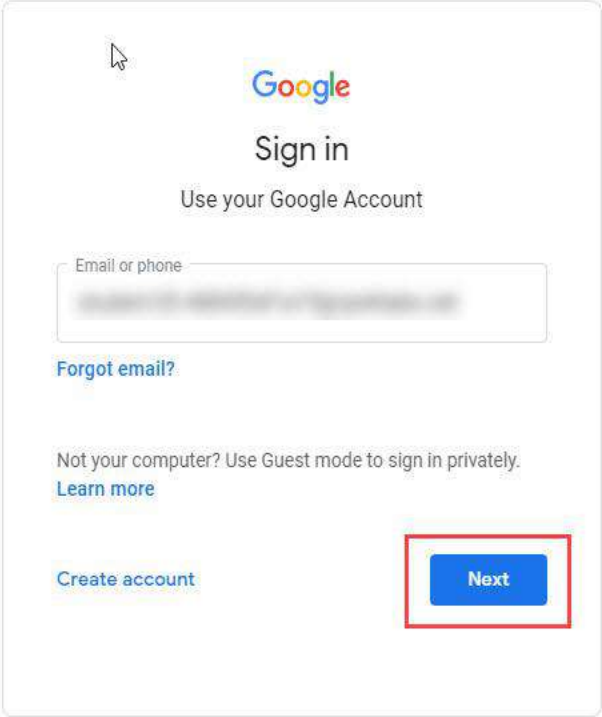
اتصال بالإنترنت.

الخطوات العملية:

الخطوة 1: تسجيل الدخول إلى **Google Cloud Console**

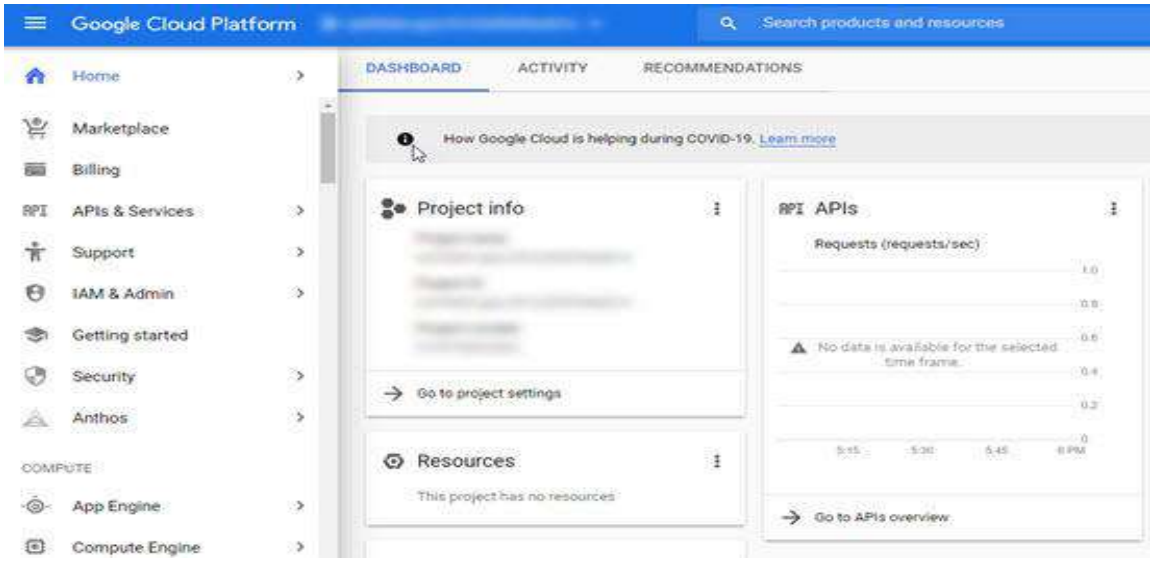
افتح **Google Cloud Console**.

قم بتسجيل الدخول إلى حسابك في **Google** كما موضح في الشكل (3-16).



الشكل (3-16)

الخطوة 2: بمجرد تسجيل الدخول إلى منصة **Google Cloud** ، سترى لوحة المعلومات وكما موضح في الشكل (3-17).

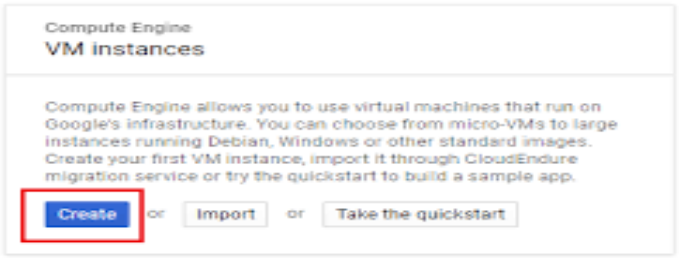


الشكل (3-17)

الخطوة 3: انقر فوق محرك الكمبيوتر (**Computer Engine**) ثم انقر فوق مثيلات (**VM instances**) كما موضح في الشكل (3-18).

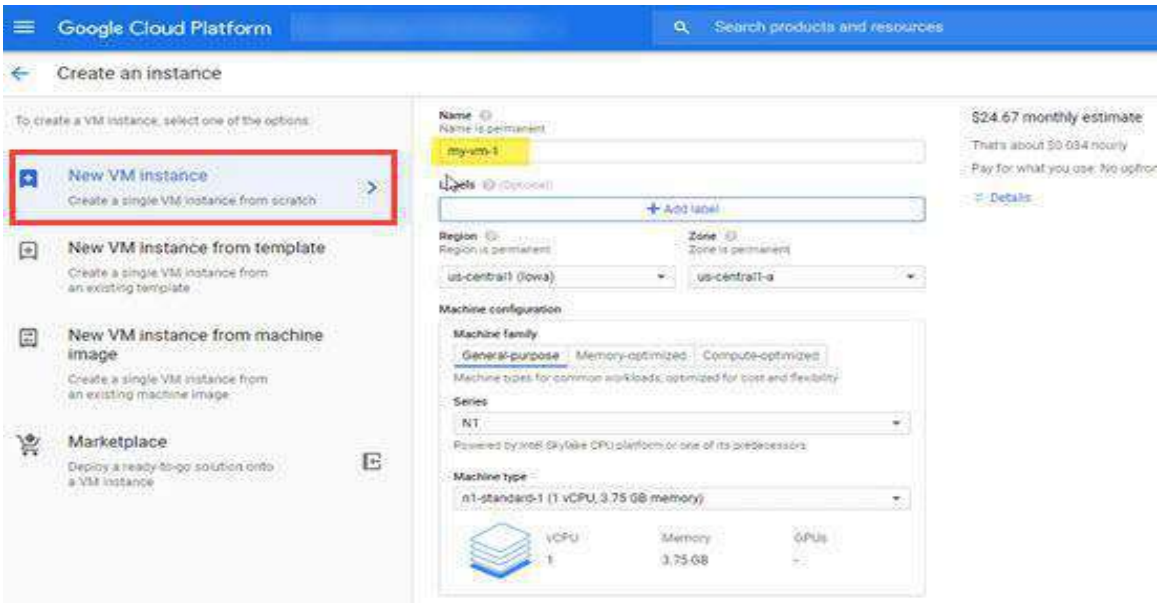
الشكل (3-18)

الخطوة 4: في الشاشة التالية، أي صفحة "حالات الجهاز الافتراضي"، سترى زر إنشاء حالة الجهاز الافتراضي كما هو موضح أدناه. (في حال وجود أي جهاز افتراضي، فسيظهر للمستخدم تفاصيل الحالة في الشبكة) كما موضح في الشكل (3-19).



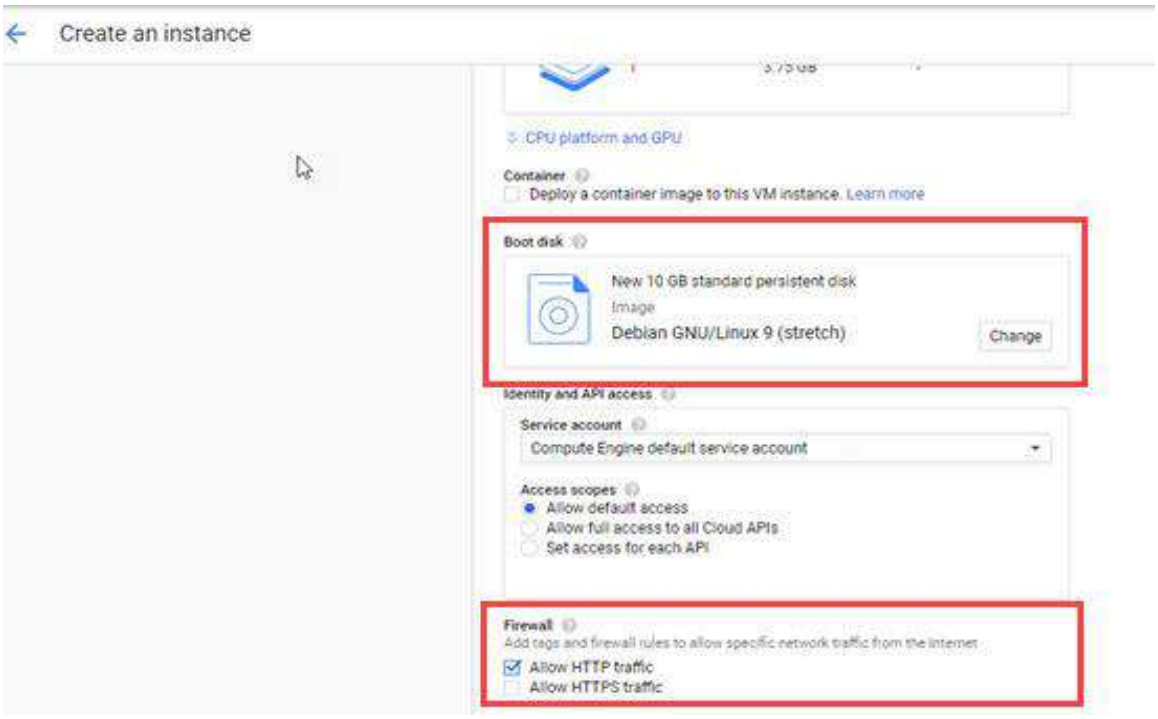
الشكل (3-19)

الخطوة 5: انقر على (نسخة جديدة من الجهاز الافتراضي **New VM Instance**) لإنشاء نسخة جديدة من البداية. أدخل اسمًا للنسخة (مثل: **my-vm-1**) ، ثم حدد **"Region"** و **" Machine type"** (مثل : **CPU 1** ، ذاكرة **GB 3.75**) وتكوين الجهاز حسب احتياجاتك كما موضح في الشكل (3-20).



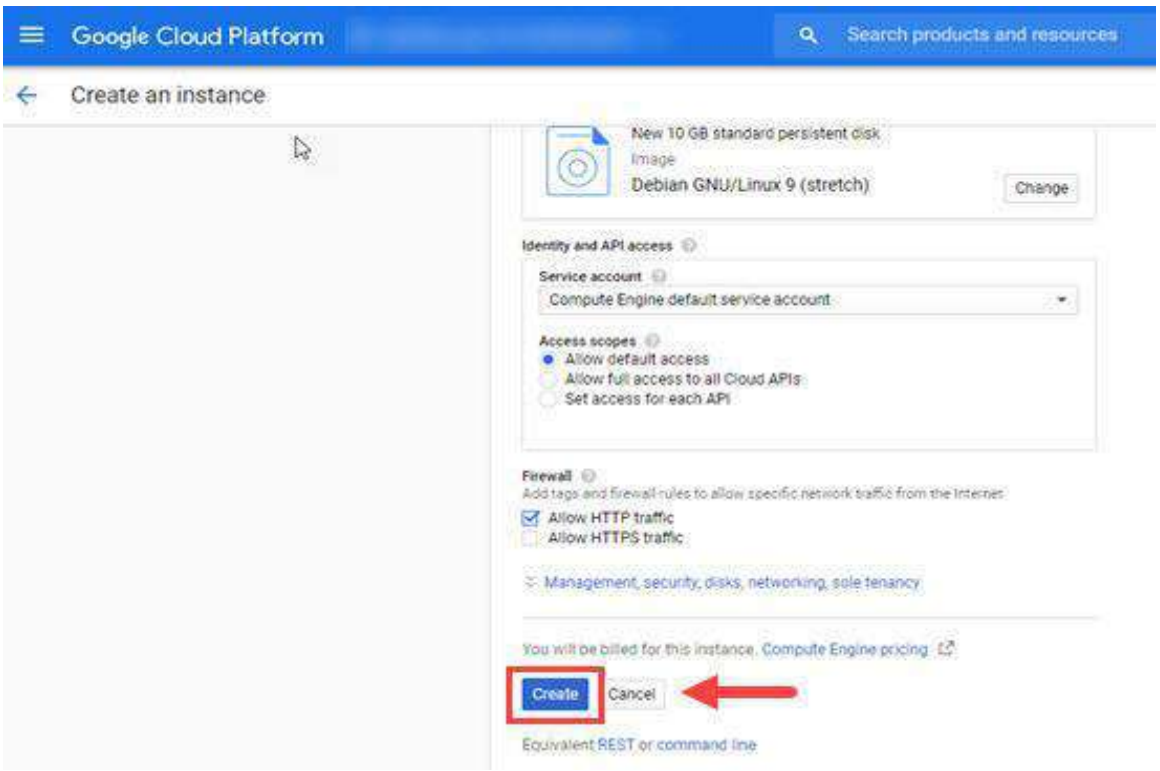
الشكل (3-20)

الخطوة 6: اختر قرص التمهيد. كما في المثال، استخدم نظام تشغيل **Debian** ، وهو نظام تشغيل مبني على **Linux** كما موضح في الشكل (3-21).



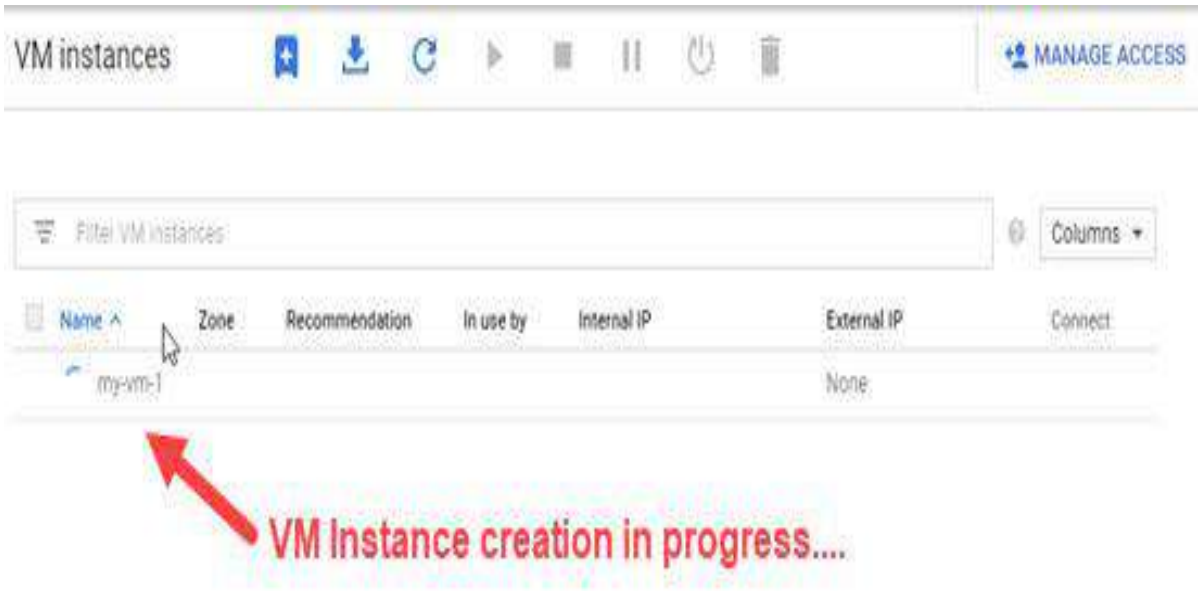
الشكل (3-21)

الخطوة 7: لأنني أخطط لاستضافة صفحة ويب، أسمح بحركة مرور **HTTP** عبر جدار الحماية. انقر على زر "إنشاء" لإنشاء الجهاز الافتراضي كما موضح في الشكل (3-22).



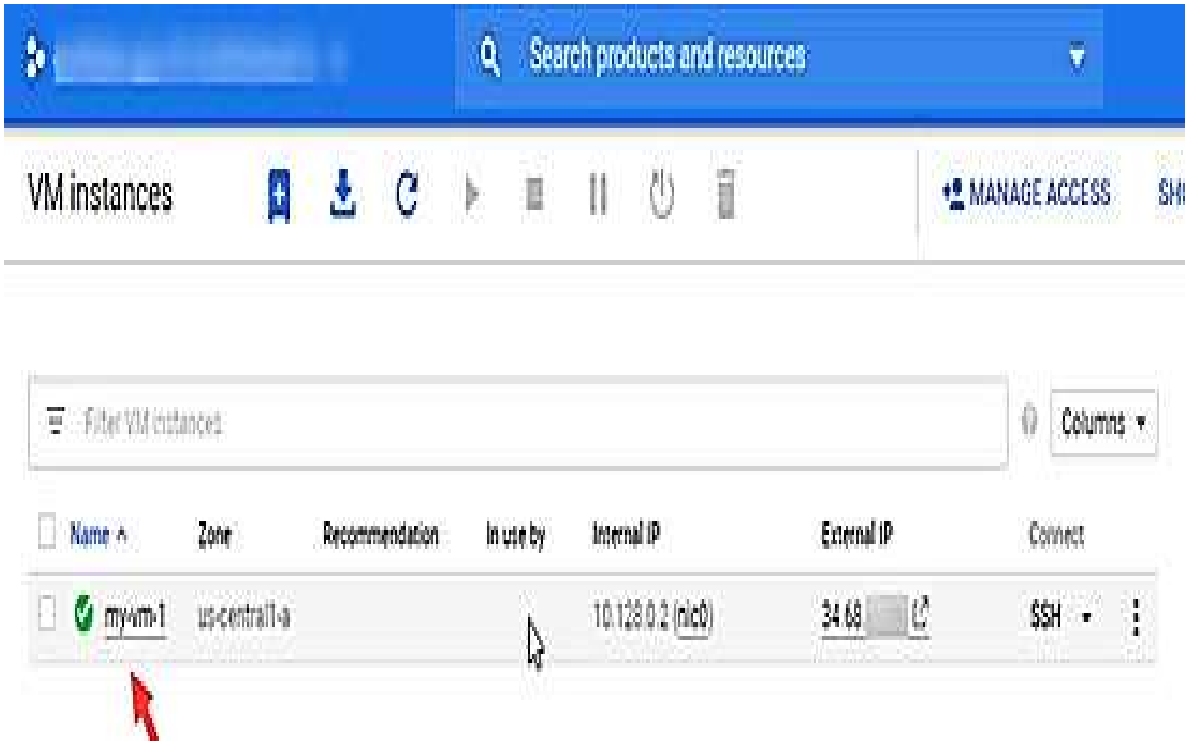
الشكل (3-22)

الخطوة 8: عند النقر فوق زر "إنشاء"، سيستغرق إنشاء مثيل **VM** المحدد أقل من دقيقة كما موضح في الشكل (3-23).



الشكل (3-23)

الخطوة 9: بمجرد أن يصبح نموذج الآلة الافتراضية جاهزًا، سترى علامة صح خضراء أمام اسم الآلة الافتراضية. سيظهر عنوان **IP** الخارجي والداخلي بمجرد أن يصبح نموذج الآلة الافتراضية جاهزًا كما موضح في الشكل (3-24).



الشكل (3-24)

النتيجة المتوقعة:

بعد تنفيذ هذا التمرين سيكون الطلبة قادرين على إنشاء جهاز افتراضي **(VM)** باستخدام **Google Compute Engine** ضمن **Google Cloud**.

استمارة الفحص تمرين رقم (2)			
الجهة الفاحصة:			
اسم الطالب :	المرحلة الثالثة	التخصص : الامن السيبراني	
اسم التمرين : استخدام Google Compute Engine لإنشاء جهاز افتراضي مع تطبيق بسيط			

ت	الخطوات	الدرجة القياسية % 50	درجة الاداء %50	الملاحظات
1	تسجيل الدخول إلى Google Cloud Console	%5		
2	الوصول الى محرك الكمبيوتر	%5		
3	إنشاء حالة الجهاز الافتراضي	%5		
4	عمل نسخة جديدة من الجهاز الافتراضي (New VM Instance)	%5		
5	اختيار قرص التمهيد، وأستخدم نظام تشغيل Debian	%5		
6	إنشاء الجهاز الافتراضي (نموذج الآلة الافتراضية VM)	%5		
7	المناقشة	%10		
8	الزمن المخصص	%10		
المجموع				
اسم الفاحص		التوقيع		

تمرين رقم 3 : إنشاء موقع ويب باستخدام Google Sites بسيط

الهدف من التمرين:

تعلم كيفية إنشاء موقع ويب باستخدام **Google Sites** بسيط.

المتطلبات الأساسية:

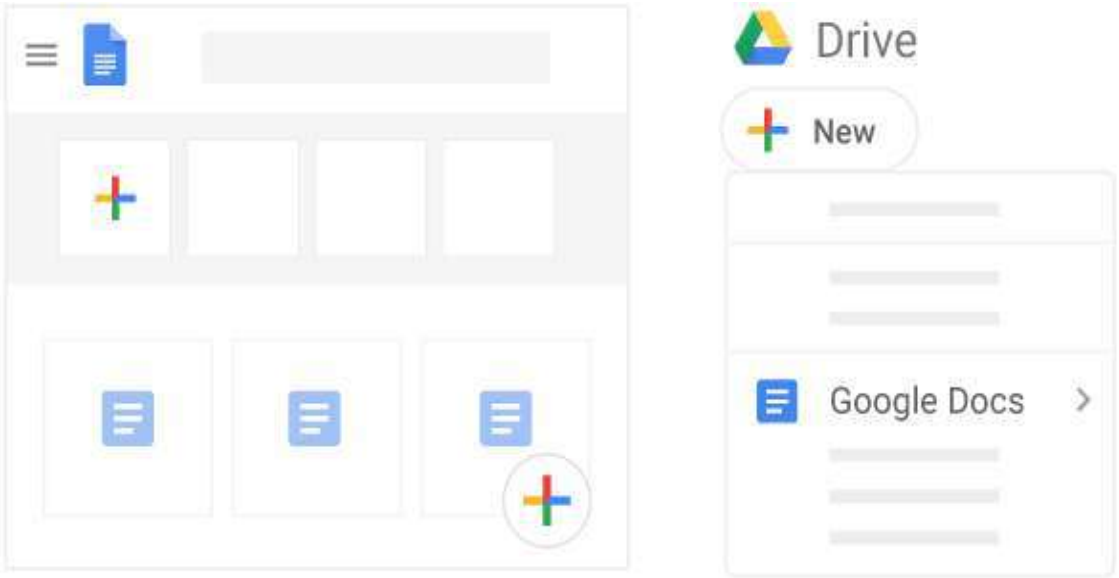
اتصال بالإنترنت.

قبل البدء في خطوات إنشاء موقع إلكتروني مجاني على **Google** تحقق من أن لديك حسابا فعالا على جوجل وإذا لم يكن لديك، فأنشئ حسابا جديدا على جوجل لتتمكن من الولوج واستخدام جوجل سايت.

الخطوات العملية

لإنشاء موقع إلكتروني مجاني على **Google** يجب اتباع الخطوات الأتية :-

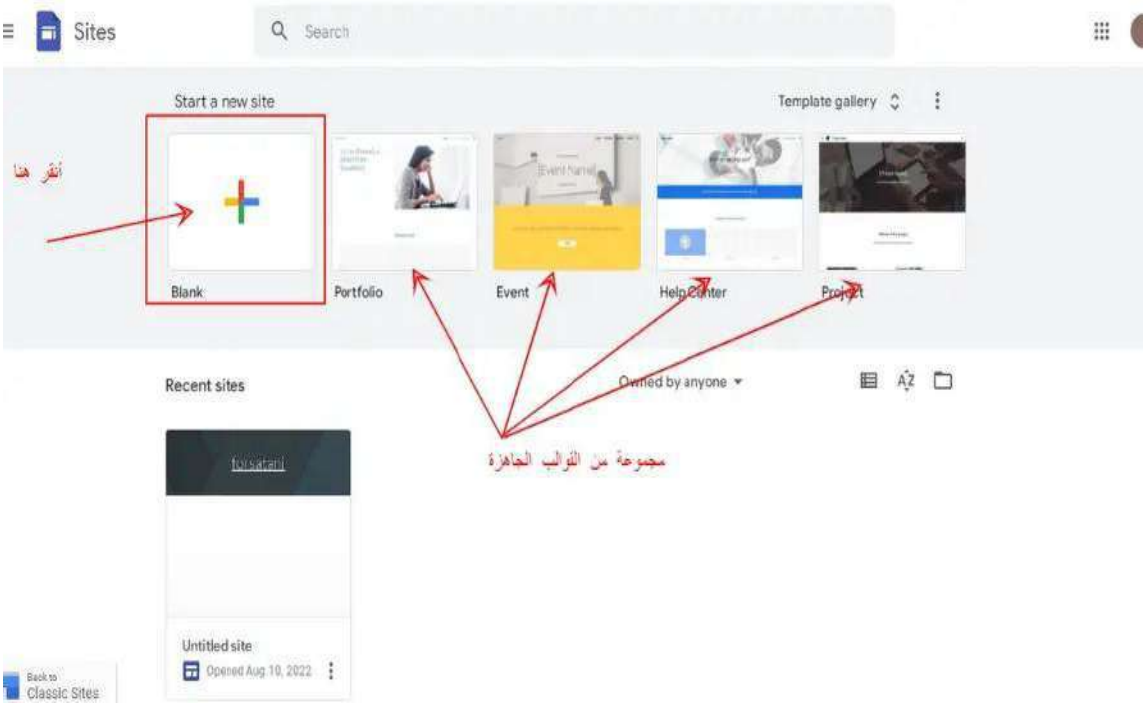
الخطوة 1 : الانتقال إلى موقع جوجل سايت إلى (**https://sites.google.com**) من متصفح الويب الخاص بك (كروم **Chrome**) أو (**Mozilla Firefox**) ، سيؤدي هذا إلى فتح صفحة جوجل سايت مواقع **Google** كما موضح في الشكل (3-25).



الشكل (3-25)

الخطوة 2 : اختيار شكل القالب

يمكنك بعد الدخول على موقع جوجل سايت والاختيار بين مجموعة من القوالب الجاهزة أو البدء بإنشاء موقع جديد كلياً, كما موضح في الشكل (3-26).



الشكل (3-26)

الخطوة 3 : تسمية الموقع الخاص بك

في الزاوية العلوية اليمنى من الصفحة (لمستخدمي اللغة العربية) بامكانك إدخال اسم الموقع الالكتروني الذي ترغب فيه كما موضح في الشكل (3-27).

الشكل (3-27)

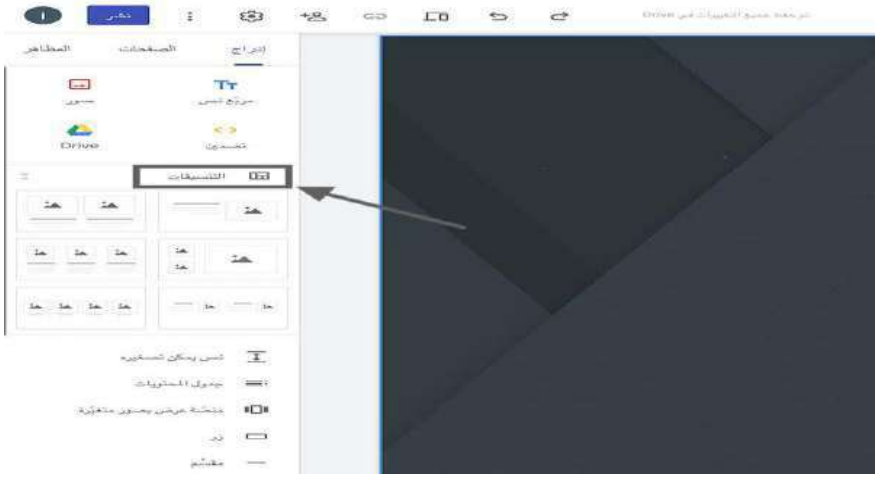
الخطوة 4 : تغيير عنوان الصفحة

بالضغط على عبارة عنوان الصفحة يمكنك تغييّر عنوان الصفحة الرئيسية للموقع وتغيير حجم الخط المستخدم ولونه بالإضافة إلى طريقة العرض كما موضح في الشكل (3-28).

الشكل (3-28)

الخطوة 5 : إضافة تنسيق للصفحة

من القائمة الرئيسية في الجهة اليسرى، يمكنك اختيار تنسيقات لإضافتها إلى موقعك ولمساعدتك على تصميم موقعك على جوجل سايت كما موضح في الشكل (3-29).



الشكل (3-29)

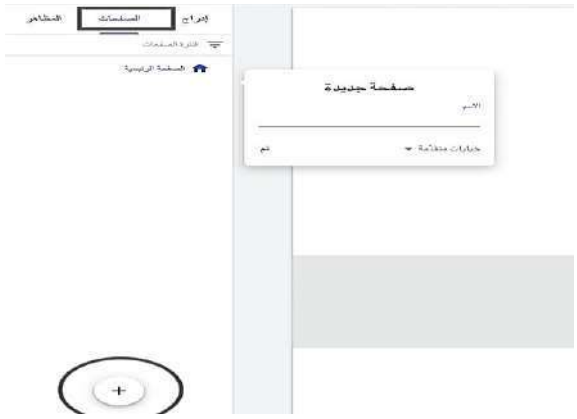
الخطوة 6 : تحديد المظهر العام

لتغييّر المظهر قم بالضغط على زر المظاهر في الزاوية العلوية اليسرى للشاشة، من هنا يمكنك اختيار التصميم العام لشكل الصفحة والوان الخلفية ونمط الخطوط ولونها, كما موضح في الشكل (3-30).

الشكل (3-30)

الخطوة 7 : إضافة الصفحات

يمكنك إضافة صفحات جديدة للحصول على المزيد من المحتوى في موقعك على جوجل سايت ويمكنك ربط الصفحات ذات المحتوى المتشابه بعضها مع بعض من خلال دمج الصفحات، انقر على صفحات في الزاوية العلوية اليسرى ومن ثم انقر على أيقونة الإضافة **(+)** والآن قم باختيار اسم للصفحة الجديدة كما موضح في الشكل (3-31).



الشكل (3-31)

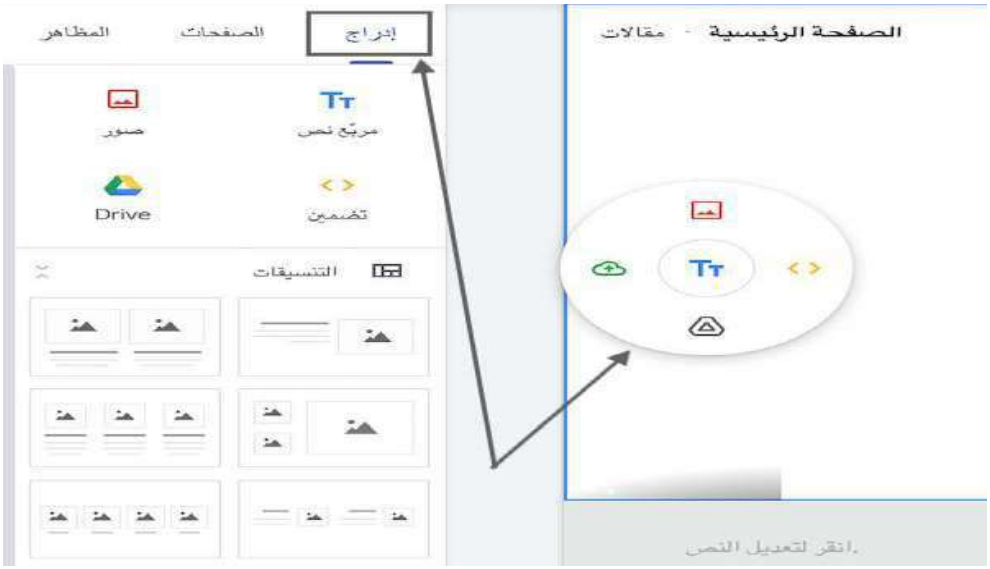
الخطوة 8 : تعديل قائمة التنقل الرئيسية

الآن وبعد أن أصبح لديك أكثر من صفحة واحدة، سيستخدم زائرو موقعك الإلكتروني قائمة التنقل للانتقال إلى صفحات مختلفة، حيث تظهر قائمة التنقل تلقائيًا في أعلى الصفحة من موقعك الإلكتروني. في أعلى يمين الصفحة قم بالنقر على أيقونة واعدادات قائمة التنقل (بجانب اسم الموقع) للتحكم في موضع قائمة التنقل كما موضح في الشكل (3-32).

الشكل (3-32)

الخطوة 9 : تصميم الموقع الالكتروني وتخصيصه

يمكنك البدء في إطلاق العنان لإبداعاتك إما باختيار قائمة ادراج من القائمة العلوية على يسار الشاشة أو بالنقر مرتين على أي جزء فارغ في الصفحة لظهور دائرة إضافة المحتوى كما موضح في الشكل (3-33).



الشكل (3-33)

الخطوة 10 : معاينة الموقع

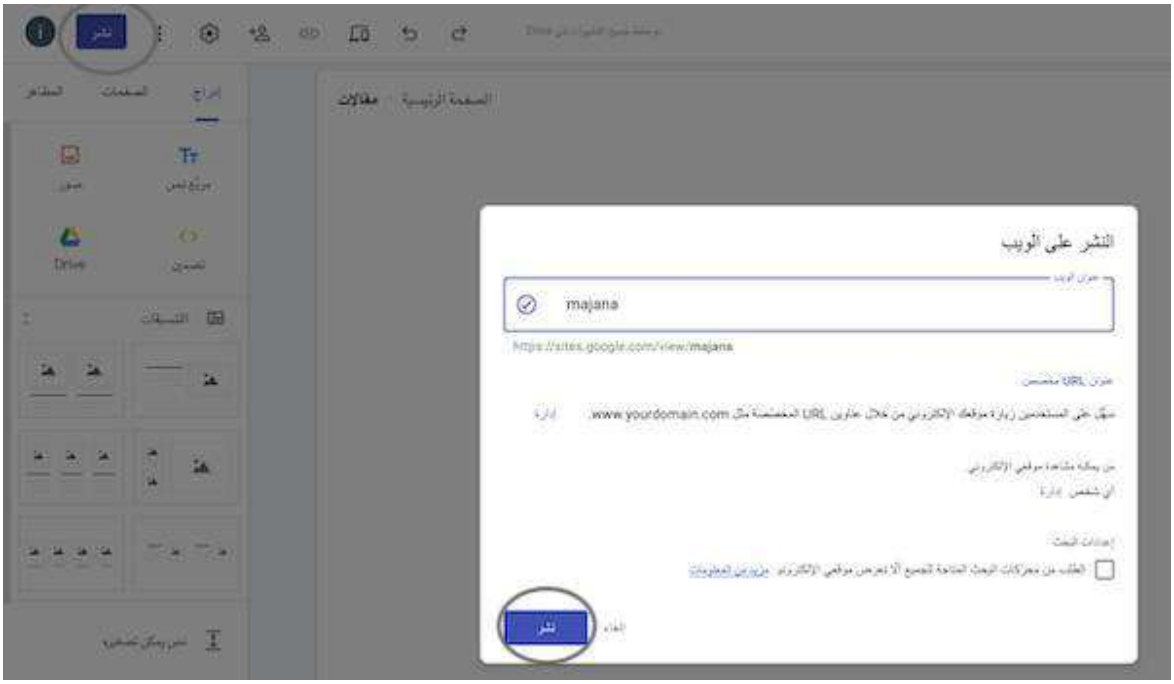
قم بالضغط على أيقونة المعاينة في أعلى الصفحة الرئيسية لرؤية شكل موقعك على مختلف أنواع الأجهزة كما موضح في الشكل (3-34).

الشكل (3-34)

الخطوة 11 : نشر الموقع الالكتروني

عند نشر موقعك الإلكتروني للمرة الأولى، يجب إضافة عنوان الرابط **URL** للموقع الإلكتروني تحقق من استخدام الأحرف اللاتينية في رابط الموقع.

اضغط على كلمة نشر في القائمة العلوية ثم حدد اسم عنوان **URL** , ثم اضغط على نشر كما موضح في الشكل (3-35).



الشكل (3-35)

الآن أصبح لديك موقع بالفعل , قم بنسخ رابط الموقع ونشره.

النتيجة المتوقعة:

بعد تنفيذ هذا التمرين سيكون الطلبة قادرين على إنشاء موقع الكتروني مجاني ونشره على قوقل.

استمارة الفحص تمرين رقم (3)			
الجهة الفاحصة:			
اسم الطالب :	المرحلة الثالثة	التخصص : الامن السيبراني	
اسم التمرين : إنشاء موقع ويب باستخدام Google Sites بسيط			

ت	الخطوات	الدرجة القياسية % 50	درجة الاداء %50	الملاحظات
1	فتح صفحة جوجل سايت مواقع Google	%5		
2	انشاء الموقع اما بالاختيار من بين مجموعة من القوالب الجاهزة أو البدء بإنشاء موقع جديد وتسميتها	%5		
3	تغيّر عنوان الصفحة الرئيسية للموقع وتغير حجم ولون الخط المستخدم وطريقة العرض وتصميم الموقع على جوجل وإضافة تنسيقات للصفحة (الوان الخلفية ونمط ولون الخطوط)	%5		
4	إضافة صفحات جديدة للحصول على المزيد من المحتوى في الموقع على جوجل سايت وربط الصفحات ذات المحتوى المتشابه مع بعضها البعض ودمج الصفحات والتنقل بينها و إضافة المحتوى و معاينة الموقع	%10		
5	نشر الموقع الالكتروني	%5		
6	المناقشة	%10		
7	الزمن المخصص	%10		
المجموع				
اسم الفاحص		التوقيع		

أسئلة الفصل الثالث

س1: عرف كلاً مما يأتي:

1- الحوسبة السحابية 2 - البنية التحتية كخدمة **(IaaS)** 3 - المنصة كخدمة **(PaaS)**

4 - البرمجيات كخدمة **(SaaS)**

س2: اختر العبارة الصحيحة لكل مما يأتي :

1- ما هي الفائدة الأساسية للحوسبة السحابية؟

a. الحاجة إلى شراء أجهزة خوادم باهضة الثمن.

b. إمكانية الوصول إلى البيانات والتطبيقات من أي مكان.

c. تقليل الحاجة إلى الإنترنت في العمليات الحاسوبية.

d. استبدال جميع أنظمة التشغيل التقليدية.

2- أي نوع من الحوسبة السحابية يناسب الشركات الكبيرة التي تحتاج إلى أمان عالٍ؟

a. الحوسبة السحابية العامة.

b. الحوسبة السحابية الخاصة.

c. الحوسبة السحابية الهجينة.

d. الحوسبة السحابية المفتوحة المصدر.

3- أي مما يأتي يُعد مثالًا على IaaS؟

a. Google Workspace (Gmail, Docs, Drive).

b. Google App Engine

c. Amazon EC2.

d. Microsoft Power BI.

4- عند استخدام الحوسبة السحابية، كيف يمكن الوصول إلى الخدمات السحابية؟

a. من خلال أجهزة متخصصة متصلة بالشبكة المحلية فقط.

b. عبر الإنترنت باستخدام المتصفحات أو التطبيقات المخصصة.

c. من خلال تثبيت برامج على الأجهزة المحلية فقط.

س3: وضح بالرسم نموذجا لخدمات السحابة الهجينة ؟

س4: املأ الفراغات الآتية بما يناسبها؟

1. تعتمد الحوسبة السحابية على مراكز بيانات ضخمة موزعة حول العالم تُستخدم لتخزين _____ وتشغيل _____ .
2. من أمثلة مقدمي خدمات الحوسبة السحابية _____ و _____ و _____.
3. من عيوب الحوسبة السحابية أنها تعتمد على _____ مما قد يسبب مشكلات في حالة انقطاعه .
4. من مميزات الحوسبة السحابية إمكانية _____ حسب الحاجة، مما يساعد على تقليل التكاليف.
5. يمكن الوصول إلى الخدمات السحابية عبر _____ او _____ او _____ .

الفصل الرابع

تهديدات الأمان في بيئة الحوسبة السحابية

الهدف العام

تعليم الطالب المفاهيم الخاصة بتهديدات الأمان في بيئة الحوسبة السحابية

الأهداف الخاصة

ان يكون الطالب قادرا على:-

- التعرف على التحديات الامنية في السحابية.
- التعرف على كيف تتم الحماية من هجمات السحابة.
- فهم إدارة الهوية والوصول (IAM).
- التعرف على الاجراءات الخاصة بالنسخ الاحتياطي واسترداد البيانات في السحابة.
- تنفيذ بعض التطبيقات البسيطة لفهم التهديدات الامان ومعالجتها في بيئة الحوسبة السحابية .

::: مفردات الفصل :::

4-1 التحديات الأمنية في السحابية

الهجمات السيبرانية في بيئة السحابة

تسريب البيانات

4-2 الحماية من الهجمات في السحابة

التقنيات المستخدمة لحماية البيانات

أدوات الكشف عن التهديدات

4-3 إدارة الهوية والوصول (IAM)

اهمية التحكم في الوصول

كيفية إدارة الصلاحيات في السحابة

4-4 النسخ الاحتياطي واسترداد البيانات في السحابة

التمارين العملية:

تمرين 1: تشفير البيانات في السحابة بأستخدام AWS KMS

تمرين 2: تحليل حركة البيانات في شبكة سحابية باستخدام Cloud Trail

تمرين 3: استخدام AWS IAM لإنشاء حسابات مستخدمين مع صلاحيات محددة.

تمرين 4: إدارة النسخ الاحتياطي في السحابة باستخدام AWS Backup .

الفصل الرابع
تهديدات الأمان في بيئة الحوسبة السحابية

4-1 التحديات الامنية في السحابة

مع تطور التكنولوجيا، بدأت الكثير من الشركات والمؤسسات تعتمد على "الحوسبة السحابية" لتخزين ملفاتها وتشغيل برامجها عبر الإنترنت بدلاً من استخدام أجهزة خوادم محلية (سيرفرات).
السحابة تعني ببساطة أنك تحفظ بياناتك أو تستخدم تطبيقاتك على الإنترنت، ويمكنك الوصول إليها من أي مكان.
لكن، هذا التقدم الكبير جلب معه تحديات أمنية جديدة، لأن البيانات لم تعد مخزّنة في مكان مغلق وآمن داخل الشركة فقط، بل أصبحت جزءاً من شبكة أكبر، وهذا يجعلها أكثر عرضة للهجمات أو التسريب. في هذا السياق، هناك تحديان كبيران نركز عليهما:

- الهجمات السيبرانية في بيئة السحابة.
- تسريب البيانات (**Data Leakage**).

4-1-1 الهجمات السيبرانية في بيئة السحابة

الهجمات السيبرانية تعني محاولات من أشخاص قراصنة (**Hackers**) لاختراق النظام الإلكتروني وسرقة المعلومات أو تعطيل الخدمات. في بيئة السحابة، هذه الهجمات تأخذ أشكالاً مختلفة:

1. هجوم عبر واجهات API: خدمات السحابة تعتمد على واجهات برمجية (**APIs**) للتعامل مع البيانات والأنظمة. إذا لم تؤمن هذه الواجهات جيداً، يمكن للمخترقين استغلالها.
مثال: في 2019 اكتشفت ثغرة في خدمة **Amazon Web Services (AWS)** وكان بإمكان أي شخص استغلال **API** معينة للوصول إلى معلومات مخزنة على خدمة التخزين **S 3**، بسبب الإعدادات الخاطئة.

2.المستخدم الداخلي الخطر (Insider Threat): أحياناً لا يكون الخطر من خارج الشركة، بل من موظف لديه صلاحيات واسعة داخل النظام ويستغلها لأغراض شخصية أو لأذية الشركة.
مثال: في شركة **Tesla**، نقل أحد الموظفين شفرة مصدرية خاصة بالشركة إلى حسابه الشخصي دون إذن، واكتشف ذلك لاحقاً.

3. هجمات الفدية (Ransomware): بعض الهجمات تعتمد على إرسال ملفات تحتوي على فيروسات أو برامج تخريبية. في حال فتحها قد تشفير الملفات على السحابة ويطلب مبلغ مالي لفك التشفير.
مثال: في عام 2020، تعرضت شركة البرمجيات الأمريكية **Blackbaud** لهجوم فدية أثّر في بيانات مئات الجامعات والمنظمات. المهاجمون تمكنوا من الوصول إلى البيانات المخزنة على السحابة وطلبوا فدية.

4. مشاركة الموارد (Multi-Tenancy Risks): في السحابة، عدة شركات قد تستخدم البنية التحتية نفسها وبالاخص الخوادم (لكن كل شركة لها بياناتها الخاصة). إذا تمكّن أحدهم من اختراق النظام، فقد يضر الجميع، ويُعد هذا من أكبر التحديات.

مثال: في بعض خدمات استضافة المواقع الرخيصة، قد يتسبب اختراق موقع واحد بالتأثير في مواقع أخرى مستضافة على الخادم السحابي نفسه.

2-1-4 تسريب البيانات (Data Leakage):

تسريب البيانات يعني أن معلومات سرية أو خاصة تكشف للعامة أو تقع بيد جهات غير مخوّلة. هذا ممكن ان يحصل بأكثر من طريقة، وأسبابه كثيرة، منها:

1- **إعدادات خاطئة (Misconfiguration):** عند تخزين ملفات في السحابة، يجب تعيين صلاحيات الوصول. في بعض الأحيان تُترك هذه الملفات متاحة للجميع بطريق الخطأ.

مثال: في 2017، سربت بيانات ملايين من عملاء شركة **Verizon** لأن أحد الخوادم السحابية ترك بلا حماية، وكان يمكن لأي شخص الوصول إليه باستخدام رابط فقط.

2- **سوء إدارة الصلاحيات:** إذا أعطي موظف أو مستخدم صلاحيات كثيرة لا يحتاج إليها، يمكن أن يستخدمها للوصول إلى بيانات لا ينبغي له رؤيتها.

مثال: أحد العاملين في شركة صغيرة كان لديه صلاحية الوصول إلى ملفات العملاء والبريد الإلكتروني، وإرسل عن غير قصد بيانات العملاء في بريد جماعي.

3- **النقل غير الآمن للبيانات:** عند إرسال البيانات بين الجهاز والسحابة، يجب أن يكون الاتصال مشفرًا. إذا لم يستخدم تشفير (مثل **HTTPS** أو **VPN**)، يمكن لأي شخص في الشبكة التجسّس على البيانات.

مثال: في إحدى الشركات، تم إرسلت بيانات العملاء عبر شبكة **Wi-Fi** عامة في مقهى دون استخدام اتصال مشفّر، واستطاع هاكر في الشبكة سرقتها نفسها.

4- **الاعتماد على أطراف خارجية ضعيفة الأمان:** أحياناً تعتمد الشركات على برامج خارجية مرتبطة بالسحابة، مثل أدوات التسويق أو التحليل. إذا كانت هذه الأدوات غير مؤمنة، يمكن أن تكون نقطة دخول للمخترقين.

مثال: شركة **Target** الأمريكية تعرضت لاختراق كبير في 2013 بعد أن استغل المخترقون برنامجًا مرتبطًا بالشبكة (مقدما من طرف ثالث مسؤول عن التكييف)، وتمكنوا من سرقة بيانات ملايين بطاقات الائتمان. وهناك مجموعة من النصائح للوقاية من الخروقات التي قد تحصل للسحابة:

- ✓ استخدام كلمات مرور قوية وتفعيل المصادقة الثنائية (**2FA**).
- ✓ تشفير البيانات قبل رفعها إلى السحابة.
- ✓ مراجعة إعدادات الخصوصية والأمان بشكل دوري.
- ✓ منح الصلاحيات بناءً على الحاجة فقط (مبدأ أقل صلاحية).
- ✓ تدريب الموظفين على ممارسات الأمان الجيد.

توجد الكثير من المواقع والبرامج التي تقدم خدمة تشفير الملفات والبيانات في السحابة ما يجعل البيانات مؤمنة أشهرها خدمة **AWS KMS (Key Management Service)** وتمثل ببساطة خدمة من أمازون تُستخدم لإنشاء وإدارة مفاتيح التشفير التي تحمي بياناتك في البيئة السحابية.

وتستخدم هذه الخدمة في الحالات الآتية:

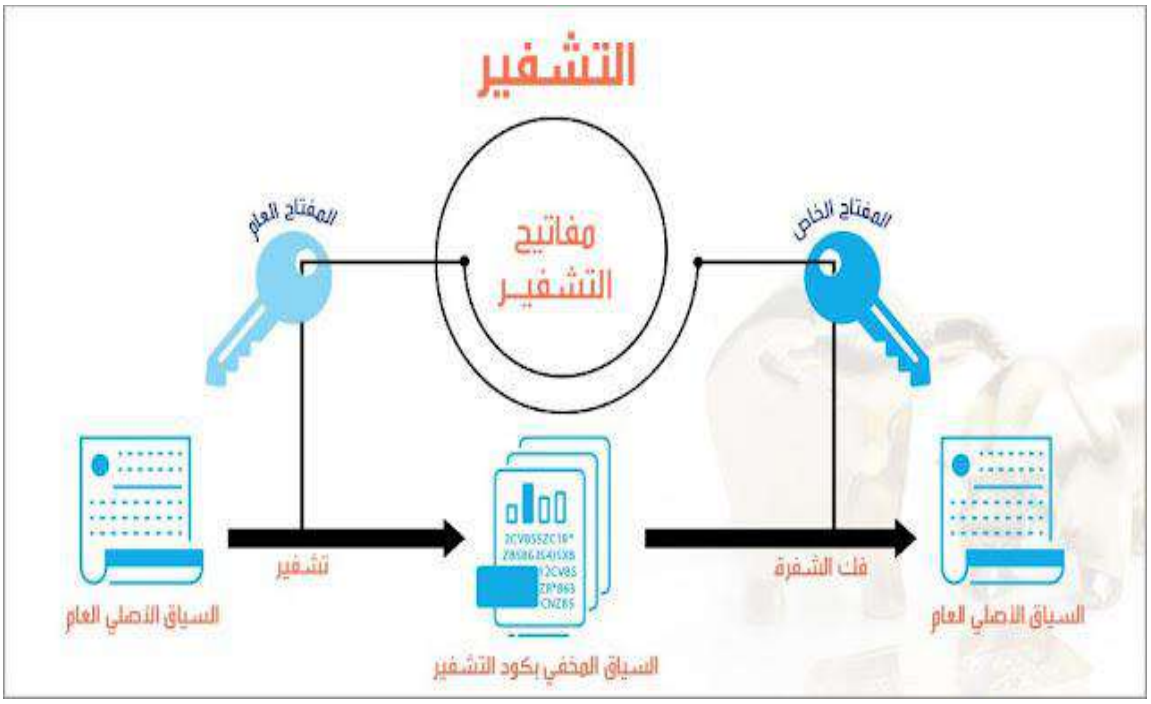
- تشفّر البيانات الحساسة (مثل الملفات أو قواعد البيانات).
- منع الوصول غير المصرّح به.
- الالتزم بالمعايير الأمنية.

أما بالنسبة لألية عملها ببساطة:

1- إنشاء مفتاح داخل **KMS**.

2- استخدام المفتاح هذا لتشفير البيانات.

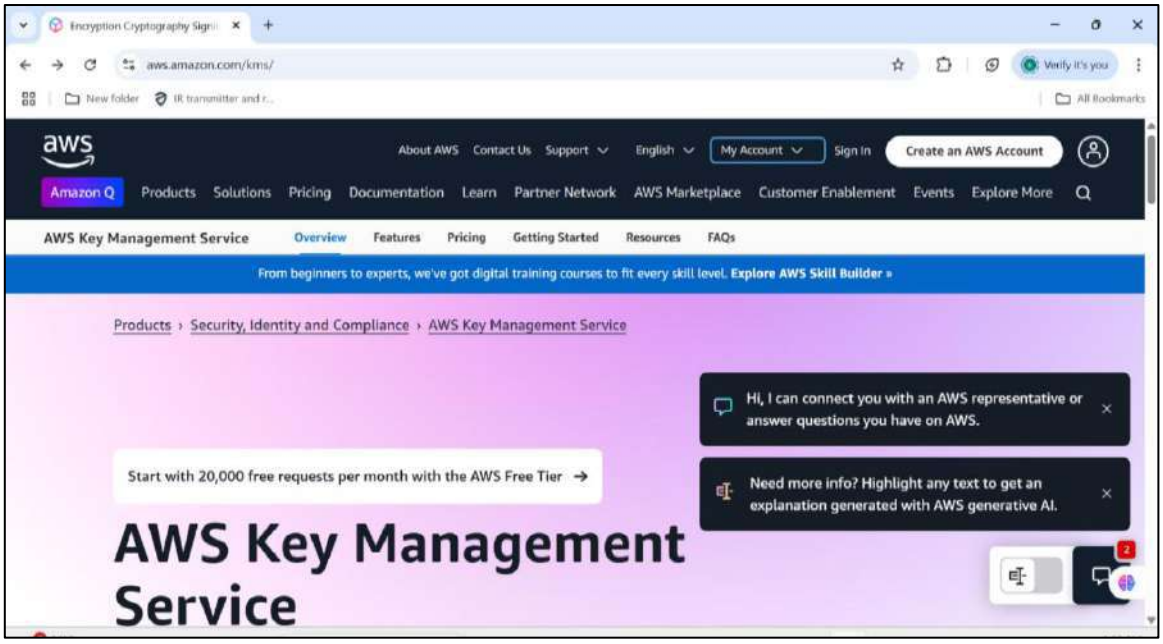
3- KMS تخزن المفتاح بأمان ولا تسمح باستخدامه إلا للأشخاص للمصرّح لهم , انظر الى الشكل رقم (4-1).



الشكل (4-1) يوضح آلية عمل التشفير

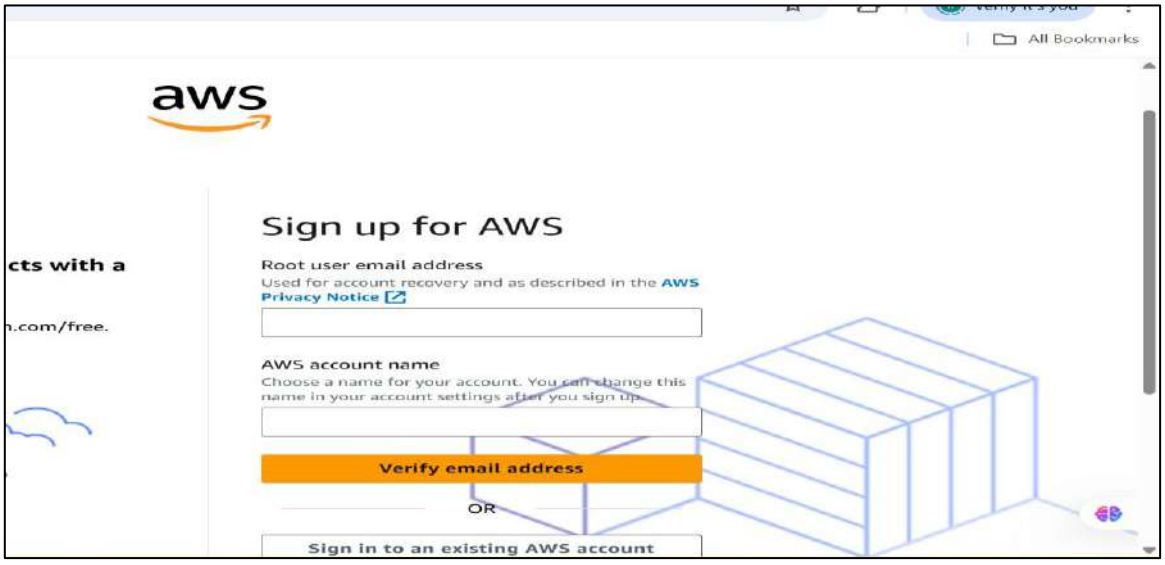
تمرين رقم 1 : تشفير ملف ضمن خدمة AWS KMS .

الخطوة 1: ندخل إلى الموقع الرسمي للخدمة **AWS Key Management Service** أو نضغط على الرابط: **https://aws.amazon.com/kms/**, فتظهر الواجهة الخاصة بالخدمة نختار منها **Greate an Aws Account**, كما في الشكل (4-2).



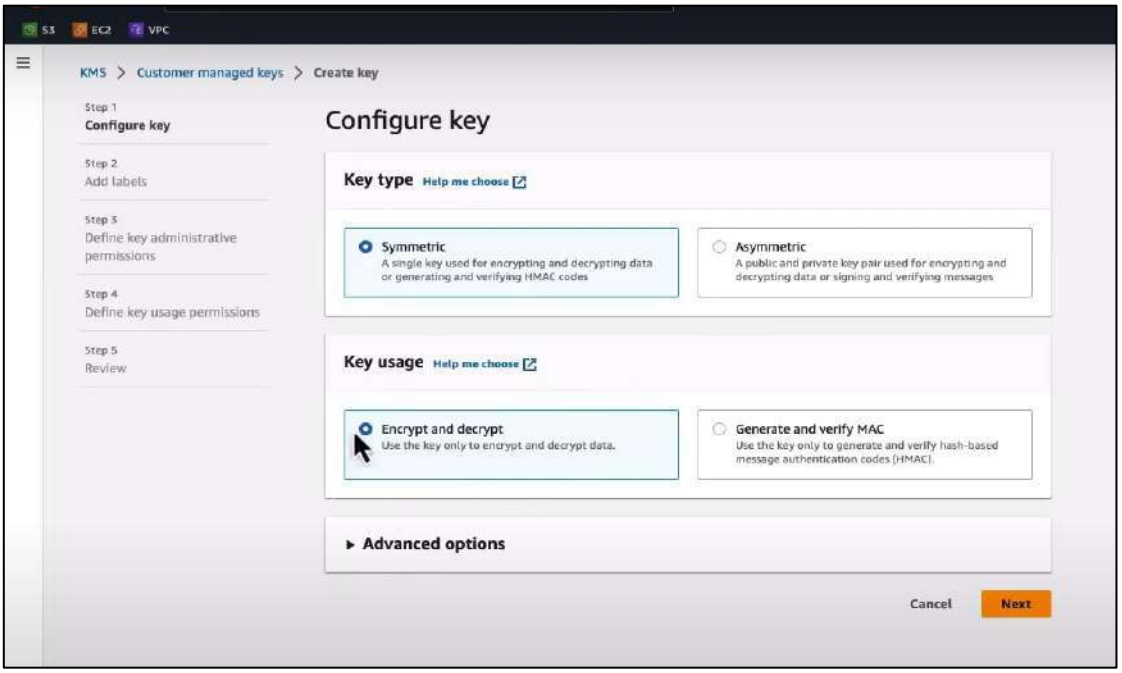
الشكل (4-2)

الخطوة 2: ندخال البريد الالكتروني (**Gmail**) الخاص بنا واسم حسابك في الخدمة, كما في الشكل (4-3).



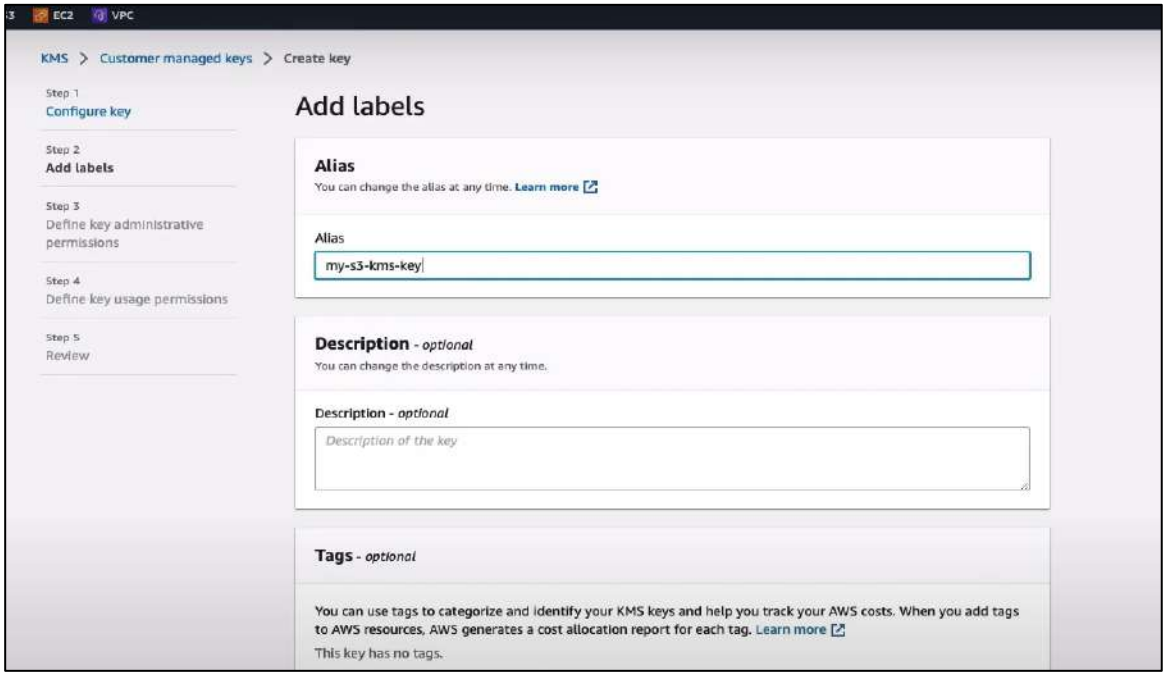
الشكل (4-3)

الخطوة 3: ارفع ملفاتك إلى **Amazon S3** ، وشفرها تلقائيًا باستخدام مفتاح من **AWS KMS** , ثم ادخل على حسابك في **AWS** وافتح خدمة **KMS**, واضغط على **Create Key** ثم اختر **Symmetric** مفتاحا التشفير, كما في الشكل (4-4).



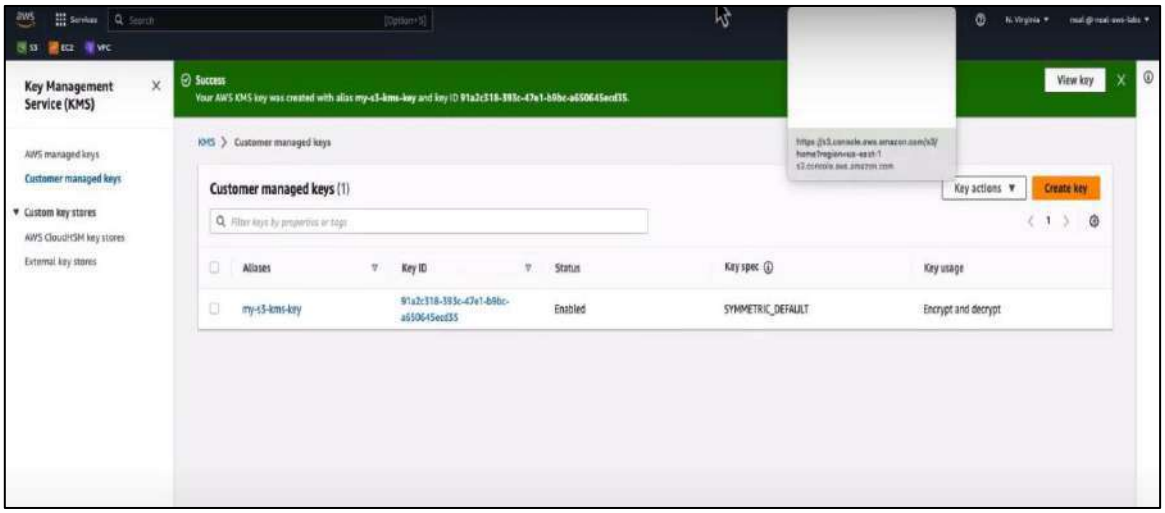
الشكل (4-4)

الخطوة 4: ثم سمّه مثلًا **My-S3Key** ثم حدّد من له صلاحية استخدام المفتاح (مثلاً نفسك أو مجموعة **IAM**) , كما في الشكل (4-5).



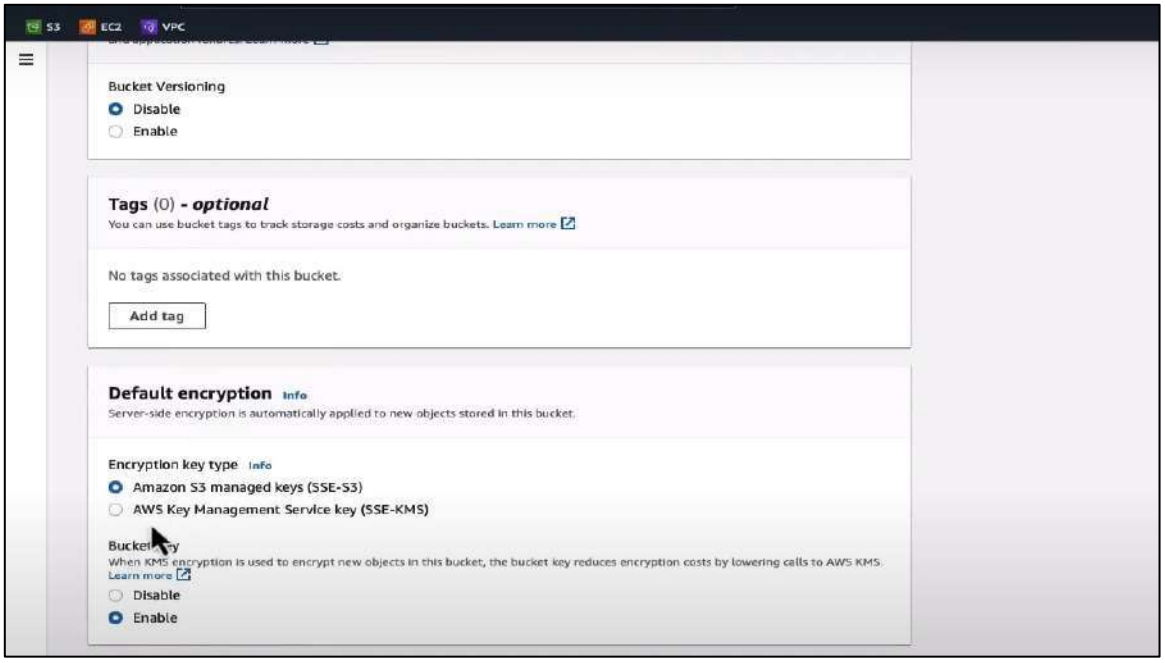
الشكل (4-5)

الخطوة 5: اضغط **Create key** واحتفظ بالاسم أو الـ **ARN** الخاص بالمفتاح, كما في الشكل (4-6).



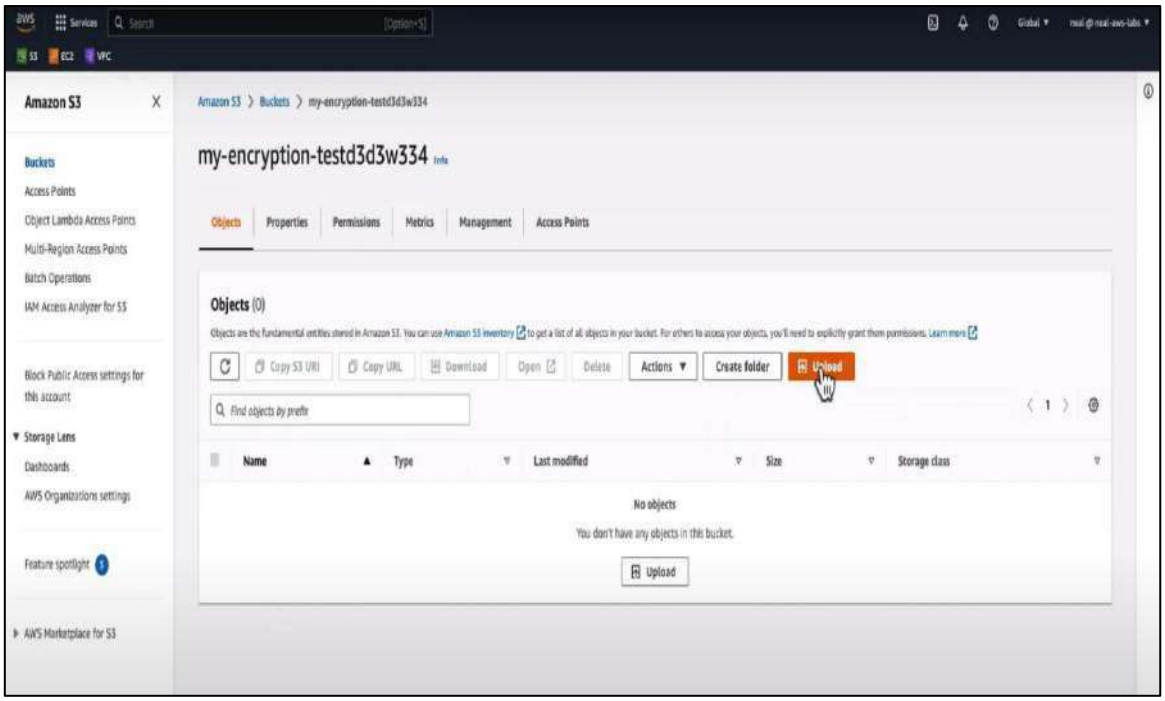
الشكل (4-6)

الخطوة 6: افتح خدمة Amazon S3 ثم اختر أو أنشئ **bucket** جديدا ومن إعدادات الـ **bucket** اذهب إلى **Properties** ثم انزل إلى **Default encryption** وفعل التشفير, كما في الشكل (4-7).



الشكل (4-7)

الخطوة 7: اختر نوع التشفير: **AWS Key Management Service keys (SSE-KMS)** ثم اختر المفتاح الذي أنشأته في **KMS (MyS3Key)**, كما في الشكل (4-8). ومن المهم ان ننوه عزيزي الطالب الى ان أي ملف ترفعه لهذا الـ **bucket** سيتشفّر تلقائيًا باستخدام المفتاح من **KMS** وعندما تقوم بتحميل الملف مرة ثانية من S3 ، يفك التشفير تلقائيًا, إذا كان لديك الصلاحية لاستخدام المفتاح في **KMS** التشفير وفك التشفير , فان هذه العملية تحدث تلقائيا بدون تدخلك.



الشكل (4-8)

النتيجة المتوقعة

1. **السهولة:** فهي لا تحتاج إلى إدارة مفاتيح أو أدوات تشفير يدويًا.
2. **أمان عال:** AWS يتكفل بكل العمليات.
3. **تحكم كامل:** قادرة على تحديد من يقوم باستخدام المفاتيح.
4. **متوافق مع السياسات الأمنية في المؤسسات:**

استمارة الفحص تمرين رقم (1)				
الجهة الفاحصة:				
اسم الطالب :	المرحلة الثالثة	التخصص : الامن السيبراني		
اسم التمرين : تشفير ملف ضمن خدمة AWS KMS .				
ت	الخطوات	الدرجة القياسية % 50	درجة الاداء %50	الملاحظات
1	الدخول الى الموقع الرسمي للخدمة AWS Key Management Service وادخال البريد الالكتروني	%5		
2	رفع الملفات إلى Amazon S3 ، وتشفيرها تلقائيًا باستخدام مفتاح من AWS KMS	%5		
3	تسمية مفتاح التشفير, وتحديّد الاشخاص الذين لديهم صلاحية استخدامة وحفظ التغييرات	%5		
4	فتح خدمة Amazon 3S , واختيار أو أنشاء bucket جديد	%10		
5	رفع ملف الى bucket الذي تم انشأه في الخطوة (5), و باستخدام المفتاح من KMS قم بتشفير الملف , ثم قم بفك تشفير الملف	%5		
6	المناقشة	%10		
7	الزمن المخصص	%10		
المجموع				
اسم الفاحص		التوقيع		

2-4 الحماية من الهجمات في السحابة

مع التوسع الكبير في استخدام خدمات الحوسبة السحابية من الأفراد والمؤسسات، أصبحت البيانات تُخزن وتعالج خارج البنية التحتية التقليدية. ورغم ما توفره هذه التقنية من مرونة وتوفير في التكاليف، تعرض المستخدمون أيضًا لمجموعة من التهديدات والهجمات السيبرانية. ولهذا، أصبحت الحماية في البيئة السحابية أمرًا بالغ الأهمية لضمان سرية البيانات وسلامتها وتوافرها.

1-2-4 التقنيات المستخدمة لحماية البيانات في السحابة

لحماية البيانات السحابية من الهجمات والاختراقات، تستخدم المؤسسات عدة تقنيات متطورة، من أبرزها:

1- **التشفير (Encryption):** تُشفّر البيانات أثناء نقلها وعند تخزينها، بحيث لا يتمكن أي طرف غير مصرح له من قراءتها. ويشمل ذلك تشفير البيانات الساكنة (**Data at Rest**) والبيانات أثناء النقل (**Data in Transit**).

2- **إدارة الهوية والوصول (IAM):** هو التحكم في من يمكنه الوصول إلى الموارد السحابية باستخدام أنظمة التحقق من الهوية وتفويض الصلاحيات، مثل المصادقة الثنائية (**2FA**) وسياسات "أقل امتياز" (**Least Privilege**).

3- **الجدران النارية السحابية (Cloud Firewalls):** تُستخدم لفلترة حركة المرور والتحكم فيها بناءً على سياسات أمان محددة سلفًا، لمنع دخول التهديدات من خارج الشبكة.

4- **العزل الافتراضي (Isolation):** تُمكّن البيئات السحابية من عزل تطبيقات وبيانات العملاء بعضهم عن بعض من خلال تقنيات المحاكاة الافتراضية والحاويات (**Containers**).

5- **النسخ الاحتياطي والتعافي من الكوارث:** تضمن استعادة البيانات بسرعة في حالة الهجمات مثل الفدية (**Ransomware**) أو الكوارث التقنية.

2-2-4 أدوات الكشف عن التهديدات

لمواجهة التهديدات المتزايدة، تعتمد المؤسسات على أدوات ذكية ومتكاملة لرصد الهجمات والاستجابة لها، منها:

1- **أدوات مراقبة الأمن (Security Monitoring Tools):** مثل **Amazon GuardDuty**، **Microsoft Defender for Cloud**، التي تراقب النشاطات غير الاعتيادية وتحلل السلوك بحثًا عن التهديدات.

2- **أنظمة الكشف عن التسلل (IDS) وأنظمة منع التسلل (IPS):** تُستخدم لرصد ومحاولة منع الهجمات المعروفة وغير المعروفة عبر تحليل حركة الشبكة.

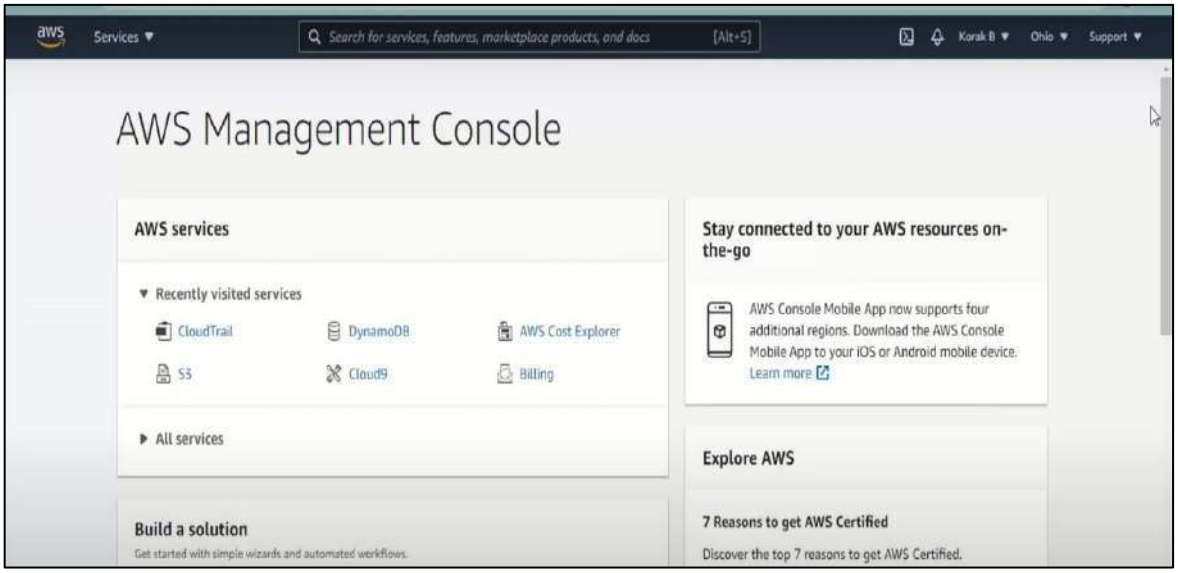
3- **خدمات تحليل السجلات (Log Analysis):** تعتمد على تجميع سجلات الاستخدام (**Logs**) وتحليلها لاكتشاف الأنشطة المشبوهة، مثل **Splunk** أو **ELK Stack**.

4- **تقنيات الذكاء الاصطناعي والتعلم الآلي:** تُستخدم لاكتشاف الأنماط غير الطبيعية والتنبؤ بالهجمات قبل حدوثها، وذلك بتحليل البيانات الضخمة في البيئة السحابية.

5- **مراكز عمليات الأمن السحابية (SOC):** تُعد مراكز متخصصة لمراقبة أمان المعلومات وتحليلها في الوقت الفعلي، وتُستخدم في البيئات الحساسة ذات التهديدات المتكررة.

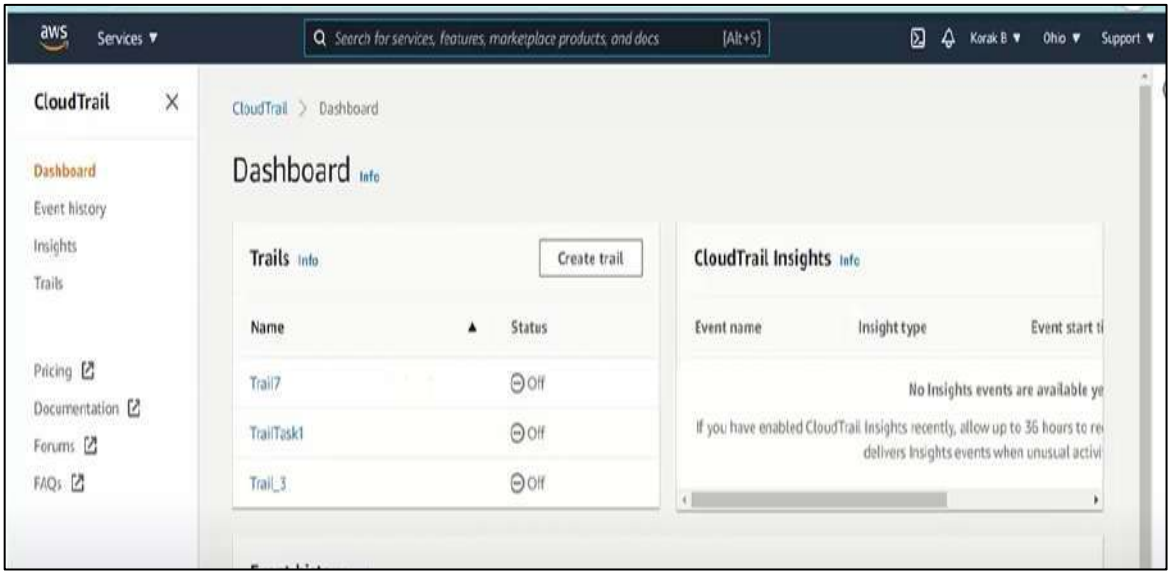
تمرين رقم 2 : تحليل حركة البيانات في شبكة سحابية باستخدام Cloud Trial .

الخطوة 1: أدخل إلى **AWS Management Console** باستخدام حسابك السابق، ثم افتح خدمة **CloudTrail** من قائمة خدمات **AWS**، ثم ابدأ بالدخول إلى صفحة **CloudTrail** في الحساب, كما في الشكل (4-9).



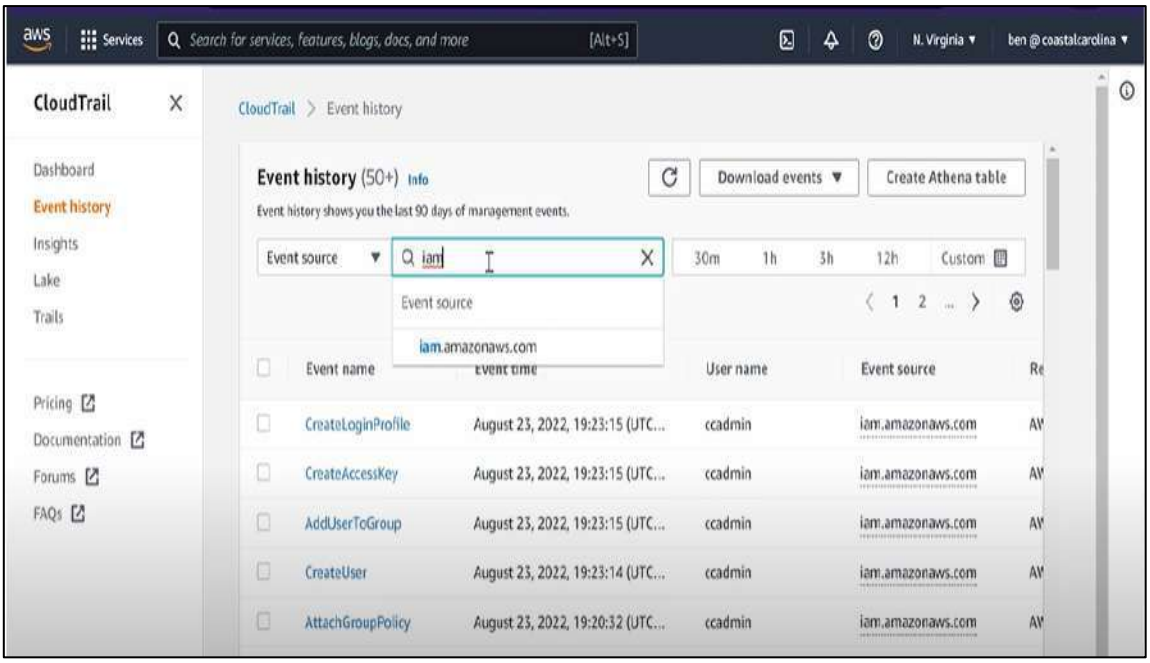
الشكل (4-9)

الخطوة 2: اختر **Event history** من القائمة الجانبية لمشاهدة الأحداث الأخيرة في الحساب و هذه الخطوة هي مكان تحليل الأنشطة التي وقعت على الحساب كلها, كما في الشكل (4-10).



الشكل (4-10)

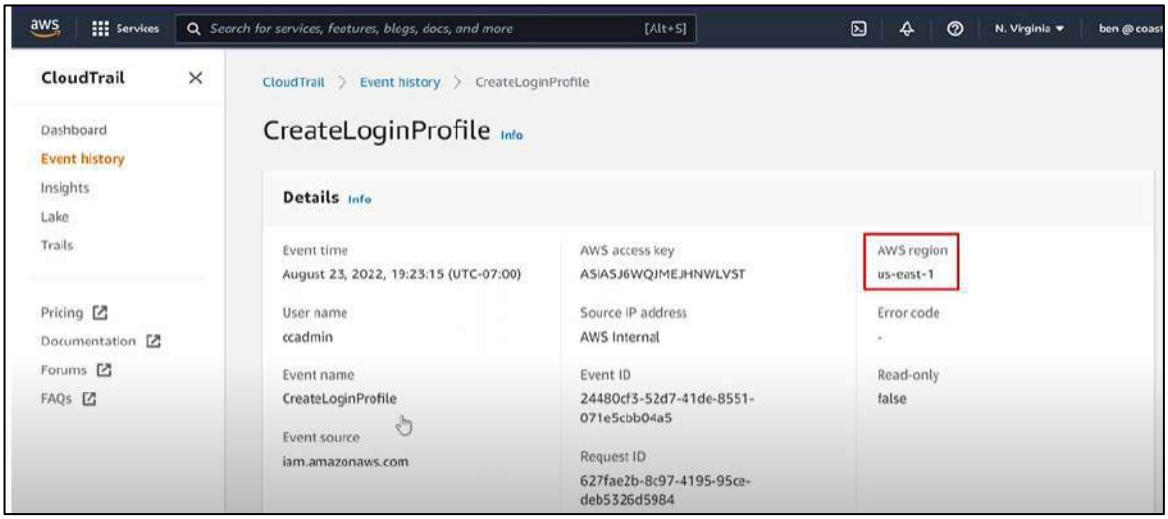
الخطوة 3: في خانة **Lookup attributes** اختر **Event source** ثم أدخل القيمة:
iam.amazonaws.com , كما في الشكل (4-11).



الشكل (4-11)

الخطوة 4: الآن نقوم بتحليل النتائج بمراقبة الأعمدة الآتية لكل حدث:

- وقت الحدث **Event Time**.
- من قام بالعملية **Username**.
- عنوان الـ **IP , Source IP Address**.
- اسم الملف المُنزَّل **Resource name**.



الشكل (4-12)

الخطوة 5: حدد النشاطات غير المألوفة التي تتمثل بالآتي:

- ✓ هل يوجد تنزيل في أوقات غير طبيعية؟
- ✓ هل هناك عناوين **IP** غير معتادة؟
- ✓ هل هناك ملفات حساسة حملت أكثر من مرة؟

استمارة الفحص تمرين رقم (2)			
الجهة الفاحصة:			
اسم الطالب :	المرحلة الثالثة	التخصص : الامن السيبراني	
اسم التمرين : تحليل حركة البيانات في شبكة سحابية باستخدام Cloud Trial			

ت	الخطوات	الدرجة القياسية % 50	درجة الاداء %50	الملاحظات
1	الدخول إلى AWS Management Console ، وفتح خدمة CloudTrail.	%5		
2	اختيار Event history , لمشاهدة الأحداث الأخيرة في الحساب.	%5		
3	اختيار Event source من خانة Lookup attributes , وأدخل القيمة iam.amazonaws.com.	%5		
4	تحليل النتائج ومراقبة الأعمدة (وقت الحدث Event Time, من قام بالعملية Username, عنوان الـ IP Source IP Address , اسم الملف المُنزَّل Resource name).	%10		
5	تحديد النشاطات غير المألوفة (تنزيل في أوقات غير طبيعية, عناوين IP غير معتادة, ملفات حساسة تم تحميلها أكثر من مرة).	%5		
6	المناقشة	%10		
7	الزمن المخصص	%10		
المجموع				
اسم الفاحص		التوقيع		

3-4 إدارة الهوية والوصول (IAM)

في العصر الرقمي الحديث، أصبحت البيانات والخدمات الرقمية من الأصول الحساسة التي تتطلب حماية عالية. ومن هنا نشأت الحاجة إلى أنظمة تُنظم من هو المستخدم، وما الذي يمكنه فعله. تُعرف هذه الأنظمة باسم إدارة الهوية والوصول (IAM)، وهي إطار عمل يتعامل مع تحديد الهويات الرقمية والتحكم في الوصول إلى الموارد والمعلومات داخل الأنظمة الرقمية.
ويمكن تعريف إدارة الهوية والوصول (IAM) على انها مجموعة من السياسات والأدوات والتقنيات التي تُستخدم لإدارة هويات المستخدمين وتحديدها (سواء كانوا أفرادًا أو تطبيقات أو أجهزة) والتحكم في ما يمكنهم الوصول إليه ضمن بيئة النظام أو المؤسسة.

4-3-1 أهمية التحكم في الوصول

1. **إثبات الهوية (Authentication):** التحقق من هوية المستخدم (مثل استخدام كلمات المرور، المصادقة الثنائية، البصمة).
2. **تفويض الوصول (Authorization):** تحديد ما الذي يمكن للمستخدم فعله بعد تسجيل الدخول.
3. **إدارة الهويات:** تتعلق بإنشاء، تعديل، وتعطيل أو حذف حسابات المستخدمين.

أن للتحكم في الوصول أهمية بالغة في الأمن السيبراني، ومن أبرز فوائده:

1. **تقليل خطر الوصول غير المصرح به:** عبر ضمان أن الأشخاص أو الأنظمة المصرح لها فقط هي التي تستطيع الوصول إلى الموارد.
2. **الامتثال للأنظمة والقوانين:** مثل اللائحة العامة لحماية البيانات (GDPR) ومعايير ISO.
3. **حماية البيانات الحساسة:** ولا سيما في المؤسسات التي تتعامل مع بيانات العملاء أو المعلومات المالية.
4. **تحسين الكفاءة التشغيلية:** من خلال أتمتة عمليات الدخول والخروج وإدارة الصلاحيات.

4-3-2 كيفية إدارة الصلاحيات في السحابة

مع التوسع في استخدام الحوسبة السحابية، أصبح من الضروري إدارة الوصول إلى الموارد السحابية بدقة، لأن أي خطأ بسيط قد يمنح صلاحيات زائدة لمستخدم غير مؤهل. إليك كيف تدار الصلاحيات في السحابة:

1- **مبدأ الأقل صلاحية (Least Privilege):** يُمنح كل مستخدم أو تطبيق أقل مستوى من الصلاحيات التي يحتاج إليها لأداء مهامه فقط.
2- **السياسات القائمة على الدور (Role-Based Access Control - RBAC):** يتم تعيين المستخدمين إلى أدوار محددة، وكل دور له مجموعة من الصلاحيات.
3- **السياسات المستندة إلى السمات (Attribute-Based Access Control - ABAC):** التحكم في الوصول بناءً على خصائص معينة مثل وقت الوصول، الموقع الجغرافي، نوع الجهاز.

4- إدارة الهوية الموحدة (Federated Identity): تمكين المستخدمين من استخدام الهوية الرقمية نفسها للوصول إلى موارد متعددة عبر منصات مختلفة (مثل تسجيل الدخول عبر **Google** أو **Microsoft**).

5- أدوات IAM في السحابة: وتتضمن:

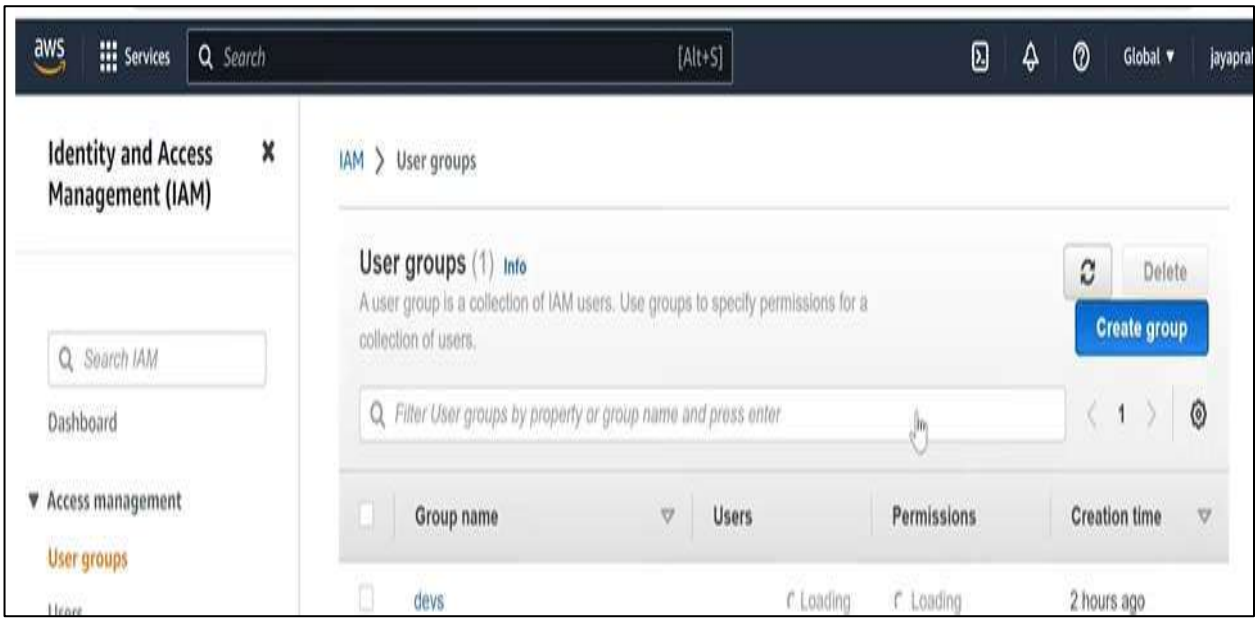
- ✓ **AWS IAM:** لإدارة الوصول إلى موارد **AWS**.
- ✓ **Azure Active Directory:** لإدارة الهوية والوصول ضمن بيئة **Microsoft Azure**.
- ✓ **Google Cloud IAM:** للتحكم الدقيق في الوصول إلى موارد **Google Cloud**.

إدارة الهوية والوصول (**IAM**) ليست مجرد نظام أمني، وإنما هي جزء أساسي من أي استراتيجية ناجحة للأمن السيبراني والحوسبة السحابية. عبر تطبيق سياسات **IAM** بشكل صحيح، يمكن للمؤسسات حماية مواردها، وضمان امتثالها للمعايير، وتحقيق كفاءة أكبر في العمليات الرقمية.

تمرين رقم 3 : استخدام AWS IAM لإنشاء حسابات مستخدمين مع صلاحيات محددة .

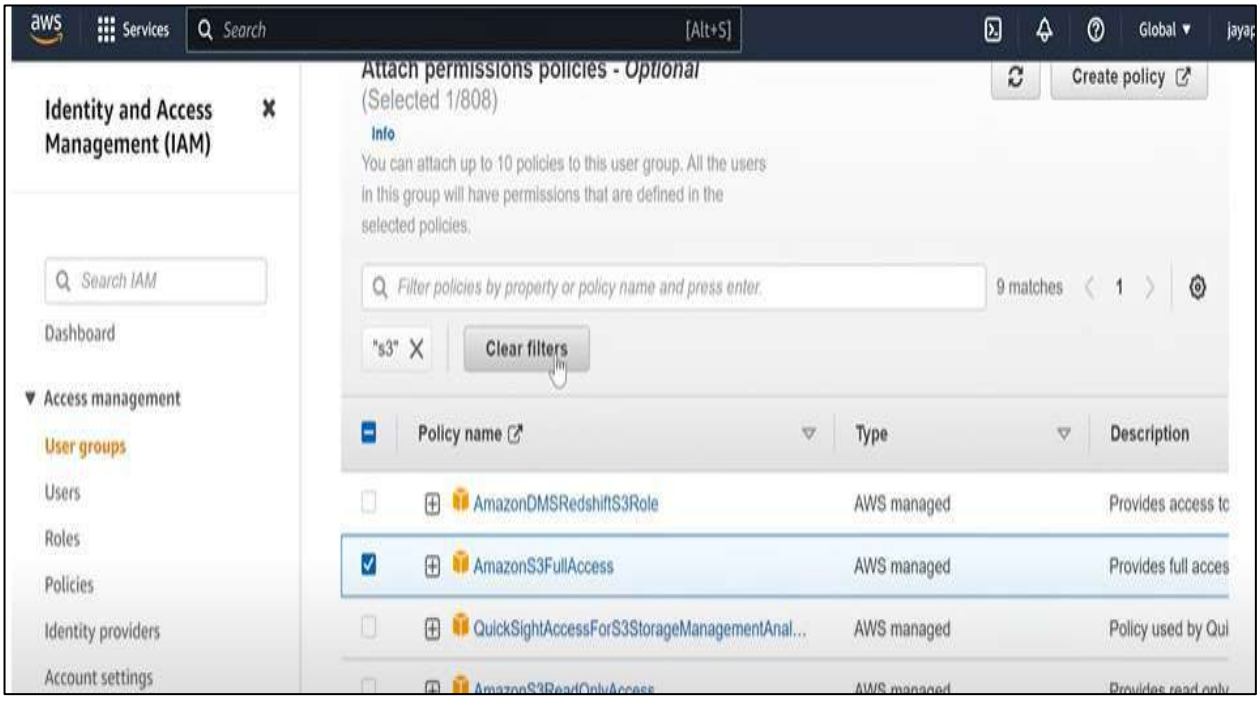
الخطوة 1 : تسجيل الدخول إلى وحدة تحكم خدمة **AWS**.

الخطوة 2: إنشاء مجموعة مستخدمين (**User Group**) باسم **Developers** , كما في الشكل (13-4).



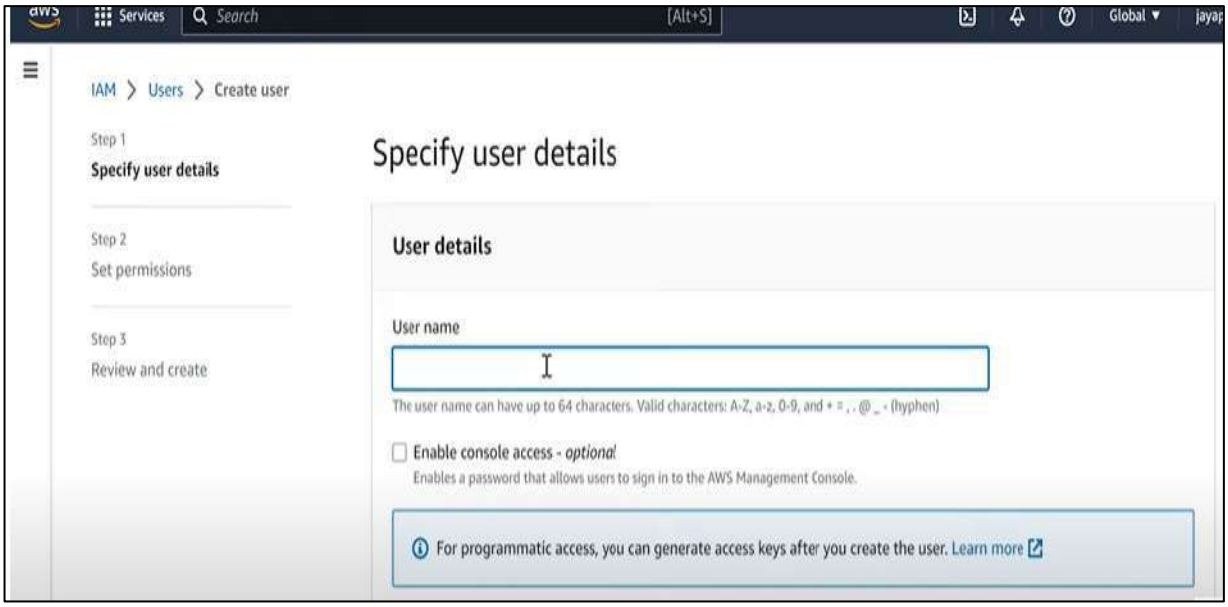
الشكل (13-4)

الخطوة 3: إنشاء مستخدم **IAM** جديد: حدد نوع الوصول (**Access type**) كـ **"Full access"** أو **"AWS Management Console access"** حسب الحاجة, كما في الشكل (14-4).



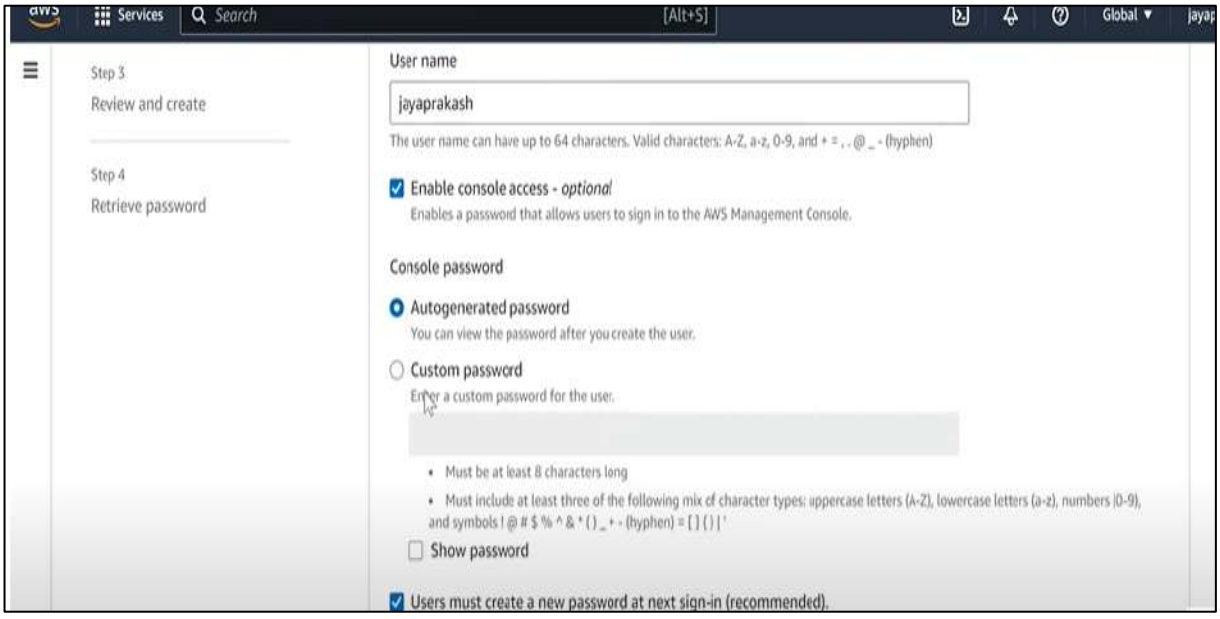
الشكل (14-4)

الخطوة 4: تعيين المستخدم إلى المجموعة: في خطوة **"Set permissions"**، اختر **" Add user to group"**. حدد المجموعة التي أنشأتها سابقًا (**Developers**) , كما في الشكل (4-15).



الشكل (4-15)

الخطوة 5: اكمل إنشاء المستخدم بمراجعة الإعدادات والنقر على **"Create user"** ثم ضع رمزا سري للدخول وكما يأتي, كما في الشكل (4-16).



الشكل (4-16)

نشاط: في التمرين السابق قم بما يأتي:

1. تحقق من تفعيل المصادقة متعددة العوامل (**MFA**) للمستخدمين لزيادة الأمان.
2. امنح المستخدمين فقط الأذونات التي يحتاجون اليها لأداء مهامهم.
3. راجع السياسات وحدثها بانتظام لضمان التوافق مع متطلبات الأمان.
4. نزل ملف **CSV** الذي يحتوي على بيانات اعتماد المستخدم الجديد.

استمارة الفحص تمرين رقم (3)			
الجهة الفاحصة:			
اسم الطالب :	المرحلة الثالثة	التخصص : الامن السيبراني	
اسم التمرين : استخدام AWS IAM لانشاء حسابات مستخدمين مع صلاحيات محددة .			

ت	الخطوات	الدرجة القياسية % 50	درجة الاداء %50	الملاحظات
1	تسجيل الدخول إلى وحدة تحكم خدمة AWS.	%5		
2	إنشاء مجموعة مستخدمين (User Group) بأسم Developers	%5		
3	إنشاء مستخدم IAM جديد	%5		
4	تعيين المستخدم إلى المجموعة	%5		
5	إكمال إنشاء المستخدم وعمل رمز سري للدخول .	%5		
6	تأكد من ما يلي :- 1- تفعيل المصادقة متعددة العوامل (MFA) للمستخدمين. 2- منح المستخدمين فقط الأذونات التي يحتاجونها لأداء مهامهم. 3- راجع السياسات وحدثها بانتظام لضمان التوافق مع متطلبات الأمان. 4- نزل ملف CSV الذي يحتوي على بيانات اعتماد المستخدم الجديد.	%5		
6	المناقشة	%10		
7	الزمن المخصص	%10		
المجموع				
اسم الفاحص		التوقيع		

4-4 النسخ الاحتياطي واسترداد البيانات في السحابة

في عالم يتزايد فيه الاعتماد على التكنولوجيا وتخزين المعلومات رقميًا، أصبحت حماية البيانات من الفقدان أو التلف أمرًا بالغ الأهمية. سواء كنت فردًا يحتفظ بذكرياته وملفاته المهمة، أو مؤسسة تعتمد على البيانات في تشغيل أعمالها، فإن أي خلل أو فقدان للمعلومات يمكن أن يؤدي إلى خسائر كبيرة مادية ومعنوية. يعرف النسخ الاحتياطي السحابي (**Cloud Backup**) بأنه عملية حفظ نسخة من البيانات الأصلية على خوادم خارجية (بعيدة) تُدار عبر الإنترنت بواسطة مزودي خدمات سحابية. تُنقل البيانات من جهاز المستخدم أو خوادم المؤسسة إلى مراكز بيانات سحابية مؤمنة، بحيث يمكن الوصول إليها واسترجاعها عند الحاجة. أما استرداد البيانات (**Data Recovery**) فهي عملية إعادة البيانات التي تم نسخها احتياطيًا إلى حالتها الأصلية بعد فقدانها أو تلفها، سواء جزئيًا أو كليًا، نتيجة حوادث تقنية، أو أخطاء بشرية، أو هجمات إلكترونية.

أسباب استخدام النسخ الاحتياطي السحابي

الحماية من الفقدان: نتيجة أعطال في الأجهزة، الحذف غير المقصود، الفيروسات، أو الكوارث الطبيعية.

سهولة الوصول: إمكانية استعادة البيانات من أي مكان باستخدام الإنترنت.

تقليل التكاليف: عدم الحاجة إلى بنية تحتية لتخزين البيانات داخليًا.

أتمتة العملية: إمكانية جدولة النسخ الاحتياطية دون الحاجة للتدخل اليدوي.

تحسين أمان البيانات: بتشفيرها ومراقبتها المستمرة.

تعزيز استمرارية الأعمال: أذ يُمكن استعادة البيانات بسرعة في حالات الطوارئ.

أما بالنسبة لأنواع النسخ الاحتياطي السحابي فهي:

1- **النسخ الاحتياطي الكامل (Full Backup):** تنسخ جميع الملفات والبيانات دفعة واحدة. وهو الأكثر شمولاً لكنه يحتاج إلى وقت ومساحة كبيرة.

2- **النسخ الاحتياطي التفاضلي (Differential Backup):** تنسخ الملفات التي تغيرت منذ آخر نسخة احتياطية كاملة فقط، مما يقلل من الوقت والمساحة.

3- **النسخ الاحتياطي التزايدي (Incremental Backup):** يُخزن فقط التغييرات التي طرأت منذ آخر نسخة احتياطية من أي نوع، وهو الأسرع والأقل استهلاكًا للمساحة.

4- **النسخ الاحتياطي في الوقت الحقيقي (Continuous Backup):** تنسخ البيانات تلقائيًا وبشكل مستمر فور حدوث أي تغيير.

اما بالنسبة لمكونات عملية النسخ الاحتياطي السحابي فهي:

عميل النسخ الاحتياطي (Backup Client): يمثل برنامج يتم تثبيته على الجهاز لمزامنة البيانات مع السحابة.

سيرفر النسخ الاحتياطي (Backup Server): يمثل الخادم الذي يستقبل البيانات ويخزنها في البنية التحتية السحابية.

واجهة المستخدم: واجهة برمجية مرئية تُمكن المستخدم من ضبط إعدادات النسخ، اختيار الملفات، ومتابعة العمليات.

نظام التشفير والأمان: لحماية البيانات أثناء النقل والتخزين من أي اختراق أو تسريب.

خطوات استرداد البيانات:

1- تحديد نوع الاسترداد:

✓ استرداد كامل للنظام.

✓ استرداد ملفات محددة.

2- اختيار النسخة المطلوبة: يمكن الرجوع إلى نسخة من تاريخ محدد.

3- تنزيل البيانات أو إعادة مزامنتها: إلى الجهاز نفسه أو جهاز جديد.

4- اختبار سلامة البيانات: للتحقق من نجاح عملية الاسترداد.

مزايا النسخ الاحتياطي السحابي:

- لا يتطلب أجهزة خاصة.
- قابلية التوسع بسهولة حسب حجم البيانات.
- مستوى عالٍ من التوافر والتكرار الجغرافي.
- أمان محسّن باستخدام تشفير متقدم.
- دعم فني متاح من مزود الخدمة.

أمثلة على خدمات النسخ الاحتياطي السحابي

1- للمستخدمين الأفراد:

- **Google Drive** – مخصص لحفظ المستندات والصور.
- **OneDrive** – مدمج مع نظام ويندوز.
- **Dropbox** – مشاركة ومزامنة ملفات شخصية.

2- للمؤسسات والشركات:

- **Amazon AWS Backup**
- **Microsoft Azure Backup**
- **Acronis Cyber Backup**
- **Backblaze B2 Cloud Storage**

الجدول (4-1) يمثل تحديات النسخ الاحتياطي السحابي والحلول المناسبة لها:

التحدي	التوضيح	الحل
الاعتماد على الإنترنت.	ضعف الاتصال يؤثر في سرعة النسخ أو الاسترداد.	استخدام اتصال ثابت وموثوق.
مخاوف الأمان.	التخوف من تسريب البيانات	اختيار مزود يقدم تشفيراً قوياً وسياسات خصوصية واضحة.
التكلفة على المدى الطويل.	تخزين كميات كبيرة قد يكون مكلفاً.	تحديد أولويات البيانات واستخدام خطط مناسبة.
صعوبة التبديل بين الخدمات.	صعوبة نقل النسخ إلى مزود آخر.	اختيار مزودات تدعم معايير تصدير واستيراد البيانات.

أمثلة على خدمات النسخ الاحتياطي السحابي

1- للمستخدمين الأفراد:

- **Google Drive** – مخصص لحفظ المستندات والصور.
- **OneDrive** – مدمج مع نظام ويندوز.
- **Dropbox** – مشاركة ومزامنة ملفات شخصية.

2- للمؤسسات والشركات:

- **Amazon AWS Backup**
- **Microsoft Azure Backup**
- **Acronis Cyber Backup**
- **Backblaze B2 Cloud Storage**

نصائح لاستخدام فعال للنسخ الاحتياطي السحابي:

- حدد الملفات الضرورية للنسخ فقط.
- استخدم التشفير المحلي قبل النسخ.
- راجع سجل النسخ دوريًا.
- اختبر عملية الاسترداد بانتظام.
- استخدم أكثر من مزود أو دمج بين النسخ المحلي والسحابي (استراتيجية 3-2-1).

إن النسخ الاحتياطي السحابي ليس إجراء اعتياديا، بل ضرورة في ظل التهديدات الرقمية والتقنية المتزايدة. بتنفيذ خطة نسخ احتياطي واسترداد بيانات فعالة، يمكن ضمان الحفاظ على الأصول الرقمية وتقليل مخاطر توقف العمل أو فقدان المعلومات الحيوية. ومع تنوع الأدوات والخدمات المتاحة اليوم، أصبح من السهل اختيار الحل المناسب حسب طبيعة الاستخدام والميزانية.

استراتيجية 3-2-1 في النسخ الاحتياطي

هي أحد المبادئ المهمة في مجال النسخ الاحتياطي للبيانات، وهي تهدف إلى ضمان الأمان والموثوقية للبيانات في حالة فقدانها أو تلفها. تشير هذه الاستراتيجية إلى توزيع البيانات بشكل متنوع لضمان عدم فقدانها في حالة حدوث كارثة أو مشكلة تقنية.

ماذا يقصد بالأرقام 3-2-1

1- نسخة خارج الموقع: يجب أن يتم تخزن نسخة واحدة من البيانات في مكان مادي مختلف (مثلاً: السحابة أو مركز بيانات بعيد)، بحيث إذا تعرضت الأجهزة المحلية أو الموقع الأساسي للتلف أو الكارثة، تظل البيانات آمنة في موقع آخر.

2-أنواع مختلفة من الوسائط: يجب تخزين البيانات على نوعين مختلفين من الوسائط أو الأجهزة، مثل القرص الصلب المحلي (HDD) أو التخزين السحابي، بحيث لا تعتمد على جهاز واحد فقط. هذا يقلل من المخاطر المرتبطة بفشل جهاز معين.

3- نسخ من البيانات: يجب أن يكون لديك ثلاث نسخ من البيانات نفسها. واحدة هي النسخة الأصلية والنسخ الأخرى هي النسخ الاحتياطية.

أهمية هذه الاستراتيجية:

- **حماية من المخاطر المتنوعة:** مثل الأعطال الميكانيكية للأجهزة، الفيروسات، أو الحوادث مثل الحريق أو الفيضانات.
- **استمرارية العمل:** ضمان وجود نسخة احتياطية يمكن الوصول إليها في حال حدوث أي مشكلة في النسخة الأصلية.

مثال على تطبيق الاستراتيجية:

1- النسخة الأصلية: البيانات الموجودة على جهاز الكمبيوتر أو الخادم.

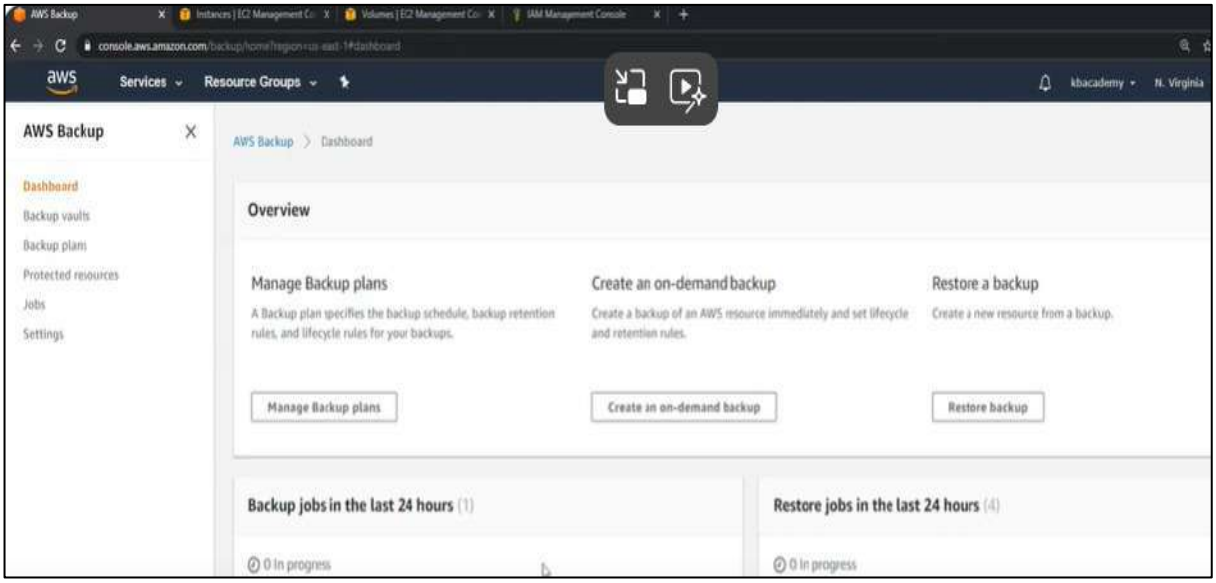
2- النسخ الاحتياطية:

- نسخة محلية على قرص صلب خارجي.
- نسخة في السحابة (مثل **Google Drive** أو **Dropbox**).
- نسخة خارج الموقع: تخزين نسخة احتياطية أخرى في مركز بيانات بعيد أو في خدمة سحابية.

باستخدام هذه الاستراتيجية، تكون قد ضمنت أن البيانات ستكون محمية بشكل جيد

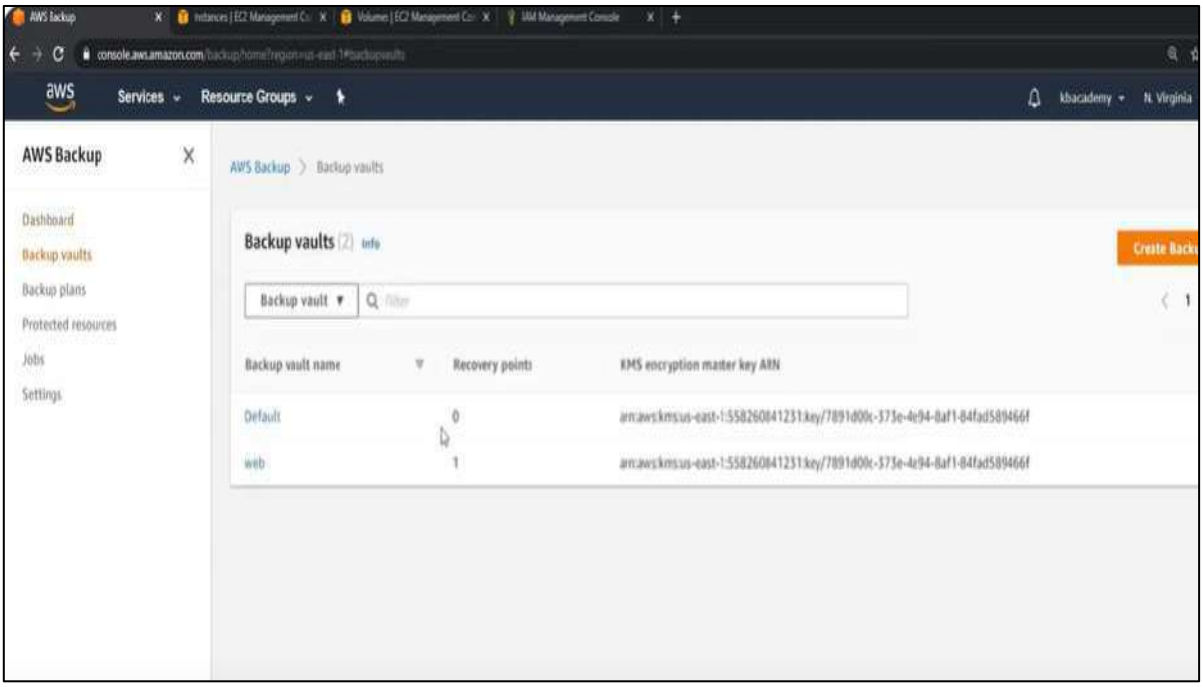
تمرين رقم 4 : إدارة النسخ الاحتياطي في السحابة بأستخدام AWS Backup.

الخطوة 1: بعد تسجيل الدخول إلى حسابك في **AWS**, انتقل إلى صفحة **AWS Backup** عبر البحث عنها في الشريط العلوي, كما في الشكل (4-17).



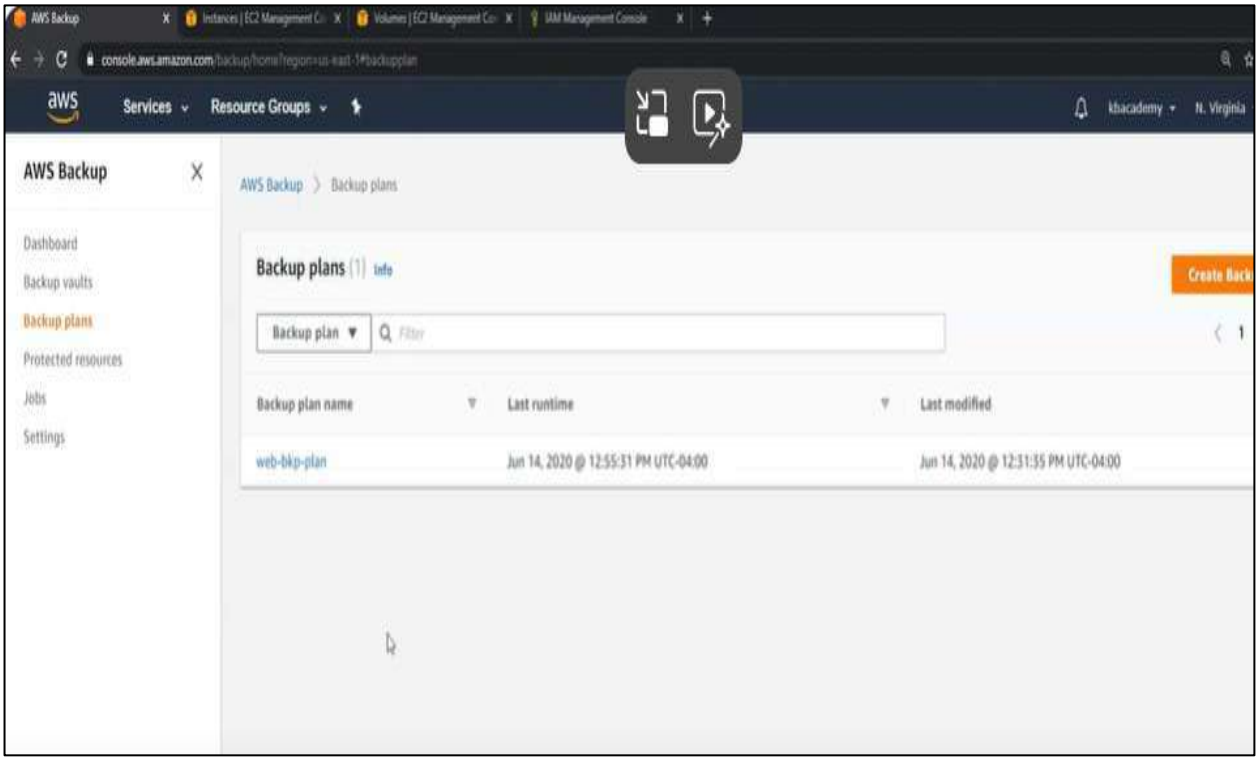
الشكل (4-17)

الخطوة 2: قم بإعداد **AWS Backup Vault** الـ **Vault** هو مكان تخزين النسخ الاحتياطية. ستحتاج إلى تحديد اسم مميز لهذا الـ **Vault** وتحديد الخيارات المناسبة مثل المنطقة الجغرافية، انقر على **"Create vault"** لإنشاء الـ **Vault**, كما في الشكل (4-18).



الشكل (4-18)

الخطوة 3: قم بإنشاء خطة نسخ احتياطي: بعد إعداد الـ **Vault**، قم بإعداد خطة حيث يتطلب ذلك تحديد الموارد (مثل **EC2** أو **RDS**) التي ترغب في إجراء نسخ احتياطي لها، ويمكنك تعيين جدولة النسخ الاحتياطي (على سبيل المثال، يوميًا أو أسبوعيًا) حسب حاجتك.
ويمكنك تحديد السياسات مثل مدة الاحتفاظ بالنسخ الاحتياطية، وتحديد الإعدادات المتقدمة مثل إدارة نسخ البيانات في طبقات متعددة مثل **S3 Glacier** أو **S3** للنسخ الباردة, كما في الشكل (4-19).



الشكل (4-19)

بعد هذه الخطوة، سيتمكن **AWS Backup** من إجراء النسخ الاحتياطي بشكل تلقائي وفقاً للإعدادات التي حددتها.

نشاط:

راقب حالة النسخ الاحتياطي عبر **AWS Backup Console** وكيفية استرجاع البيانات في حال حدوث مشكلة أو فقدان للبيانات.

استمارة الفحص تمرين رقم (4)			
الجهة الفاحصة:			
اسم الطالب :	المرحلة الثالثة	التخصص : الامن السيبراني	
اسم التمرين : إدارة النسخ الاحتياطي في السحابة بأستخدام AWS Backup			
ت	الخطوات	الدرجة القياسية % 50	درجة الاداء %50	الملاحظات
1	تسجيل الدخول إلى الحساب في AWS, وانتقل إلى صفحة AWS Backup	%5		
2	إعداد AWS Backup Vault الـ Vault	%5		
3	إنشاء خطة نسخ احتياطي, وتحديد الموارد (مثل EC2 أو RDS) التي ترغب في إجراء نسخ احتياطي لها، وتعيين جدولة النسخ الاحتياطي. وتحديد السياسات مثل مدة الاحتفاظ بالنسخ الاحتياطية، وتحديد الإعدادات المتقدمة مثل إدارة نسخ البيانات في طبقات متعددة مثل S3 Glacier أو S3 للنسخ الباردة.	%5		
4	قم مراقبة حالة النسخ الاحتياطي عبر AWS Backup Console وكيفية استرجاع البيانات في حال حدوث مشاكل أو فقدان للبيانات.	%5		
6	المناقشة	%10		
7	الزمن المخصص	%10		
المجموع				
اسم الفاحص		التوقيع		

اسئلة الفصل الرابع

س1: عرف ما يأتي:

الهجمات السيبرانية , الجدران النارية السحابية , النسخ الاحتياطي السحابي , استرداد البيانات

س2: املاء الفراغات الآتية بما يناسبها:

1- خدمات السحابة تعتمد على واجهات برمجية _____.

2- عند تخزين ملفات في السحابة يجب تعيين _____.

3- للوقاية من الخروقات يتم استخدام _____ وتفعيل _____.

4- أصبحت الحماية في البيئة السحابية امراً بالغ الأهمية لـ _____ و_____ و_____.

5- تستخدم _____ لفلترة حركة المرور والتحكم فيها بناءً على سياسات أمان محددة سلفاً .

6- تعرف إدارة الهوية للوصول **IAM** على أنها _____.

س3: عدد وظائف إدارة الهوية والوصول IAM.

س4: عدد مع الشرح الموجز أسباب استخدام النسخ الاحتياطي السحابي.

س5: عدد مع الشرح التفصيلي انواع النسخ الاحتياطي السحابي.

س6: اشرح بالتفصيل الهجمات السيبرانية في بيئة السحابة.

س7: عدد النصائح الواجب اتباعها للوقاية من الخروقات التي قد تحصل للسحابة.

س8: اشرح خدمة **AWS KMS** مبيناً أهميتها.

س9: اشرح بالتفصيل أدوات الكشف عن التهديدات في البيئة السحابية، ثم اذكر أنواعها؟

س10: كيف تدار الصلاحيات في السحابة، بين ذلك؟

س11: عدد أدوات **IAM** في السحابة؟

س12: ما مكونات عملية النسخ الاحتياطي السحابي.

س13: ما الحلول المناسبة لتحديات النسخ الاحتياطي السحابي الاتية:

a) الاعتماد على الإنترنت.
b) مخاوف الأمان.
c) التكلفة على المدى الطويل.
d) صعوبة التبديل بين الخدمات.

الفصل الخامس

تقنيات متقدمة في أمن الشبكات والحوسبة السحابية

..::: مفردات الفصل :::..

1-5 مفهوم الشبكات المعرفة بالبرمجيات SDN وتأثيها في أمان الشبكات

2-5 استخدام الذكاء الاصطناعي في تأمين الشبكات والحوسبة السحابية

3-5 إلحوسبة السحابية دون خوادم (Serverless)

4-5 الحوسبة الطرفية (Edge Computing) وتأثيرها على الامان

التمارين العملية:

تمرين 1: تطبيق تقنية SDN على شبكة محلية.

تمرين 2: تجربةانشاء بيئة سحابية بدون خوادم باستخدام AWS Lambde

الهدف العام

أن يتعلم الطالب بعض تقنيات متقدمة في أمن الشبكات والحوسبة السحابية

الأهداف الخاصة

أن يكون الطالب قادرا على:-

- التعرف على مفهوم الشبكات المعرفة بالبرمجيات SDN وتأثيرها في أمان الشبكات
- التعرف على كيفية استخدام الذكاء الاصطناعي في تأمين الشبكات والحوسبة السحابية.
- التعرف على مفهوم الحوسبة الطرفية (Edge Computing) وتأثيرها في الأمان
- التعرف على المقصود بإلحوسبة السحابية بدون خوادم (Serverless).
- تنفيذ بعض التطبيقات البسيطة لفهم بعض تقنيات المتقدمة في أمن الشبكات والحوسبة السحابية.

الفصل الخامس
تقنيات متقدمة في أمن الشبكات والحوسبة السحابية

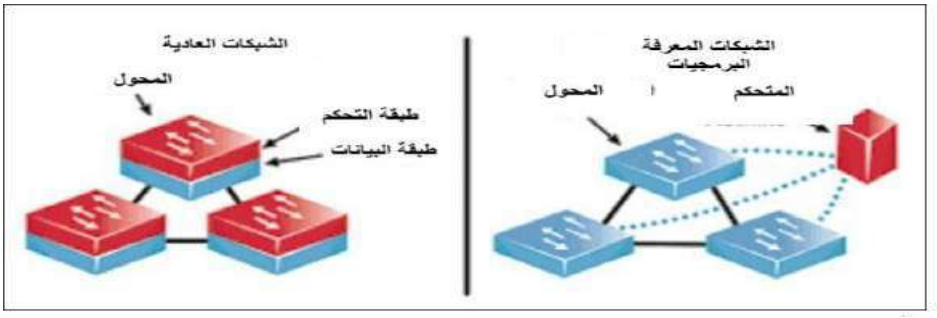
المقدمة

تُعد الشكات الحديثة والحوسبة السحابية من الركائز الأساسية التي تعتمد عليها المؤسسات في العصر الرقمي. ومع تزايد استخدام التطبيقات والخدمات الرقمية، أصبحت الشبكات هدفًا رئيسيًا للهجمات السيبرانية، ما يجعل الأمن ضرورة قصوى. تهدف هذه التقنيات المتقدمة إلى تعزيز قدرات الدفاع، وتحسين كفاءة التحكم، وتقديم حلول أمنية مرنة وقابلة للتوسع.

في هذا الفصل سنعراض مجموعة من أبرز التقنيات الحديثة في هذا المجال، مثل الشبكات المعرفة بالبرمجيات (**SDN**)، وتوظيف الذكاء الاصطناعي في الحماية، بالإضافة إلى الحوسبة السحابية بلا خوادم (**Serverless**) والحوسبة الطرفية (**Edge Computing**), وسنناقش فوائد كل تقنية والتحديات الأمنية المرتبطة بها.

1-5 مفهوم الشبكات المعرفة بالبرمجيات SDN وتأثيرها في أمان الشبكات

الشبكات المعرفة بالبرمجيات (**SDN**) هي تقنية حديثة تُستخدم في تصميم الشبكات وإدارتها بطريقة مرنة وسهلة لتحسين الأداء والمراقبة، تسمح بإدارة مركزية لجميع أجهزة الشبكة عبر متحكم مركزي. تعتمد هذه المنهجية على فصل البرمجيات (**Software**) التي تتحكم في الشبكة عن الأجهزة المادية (**Hardware**) التي تقوم بعملية تمرير البيانات ففي الشبكات التقليدية، تكون وظيفتا التحكم وتوجيه حركة المرور مدمجتين داخل كل جهاز شبكي مثل الموجهات (**Routers**) أو المبدلات (**Switches**) ، مما يؤدي إلى تعقيد عملية إدارة الشبكة والتوسع فيها. كل جهاز يتخذ قراراته الخاصة حول كيفية توجيه الحزم، ما يجعل التنسيق بين الأجهزة أمرًا صعبًا في الشبكات الكبيرة. أما في الشبكات المعرفة بالبرمجيات(**SDN**) ، فتفصل طبقة التحكم (**Control Plane**) عن طبقة البيانات .(**Data Plane**) حيث تقوم طبقة التحكم بتحديد كيفية توجيه حركة المرور، في حين تتولى طبقة البيانات مهمة نقل الحزم إلى وجهتها. وتُدار طبقة التحكم من خلال نظام برمجي مركزي يُعرف بـ "المتحكم" (**Controller**)، وهو الذي يتخذ قرارات التوجيه بشكل مركزي لجميع أجهزة الشبكة. هذا الأسلوب يتيح إدارة مركزية ومرنة للشبكة من خلال واجهة برمجية واحدة، ويُسهّل تطبيق السياسات الأمنية والتوسع الشبكي بشكل ديناميكي وسريع. شكل (5-1) يوضح الفرق بين الشبكات التقليدية والشبكات المعرفة بالبرمجيات.



شكل (5-1) الفرق بين الشبكات التقليدية والشبكات المعرفة بالبرمجيات

1.1.5 المهام التي تم استغني عنها عند استخدام الشبكات المعرفة البرمجيات؟

عند الانتقال من الشبكات التقليدية إلى الشبكات المعرفة بالبرمجيات ألغيت الكثير من المهام اليدوية والمتكررة التي كانت تُشكل عبئًا على مسؤولي الشبكات , وهذه المهام هي:

1- إعداد يدوي لأجهزة الشبكة.
2- توزيع الحركة يدويًا.
3- إعادة التوجيه اليدوي لحركة المرور.
4- تنفيذ السياسات المتفرعة على أجهزة الشبكة بشكل فردي.
5- القيام بتكوينات الشبكة وإدارتها من خلال أجهزة متعددة بشكل منفصل.
6- إجراء العمليات الإدارية والتحكمية يدويًا في كل عملية تغيير في الشبكة.

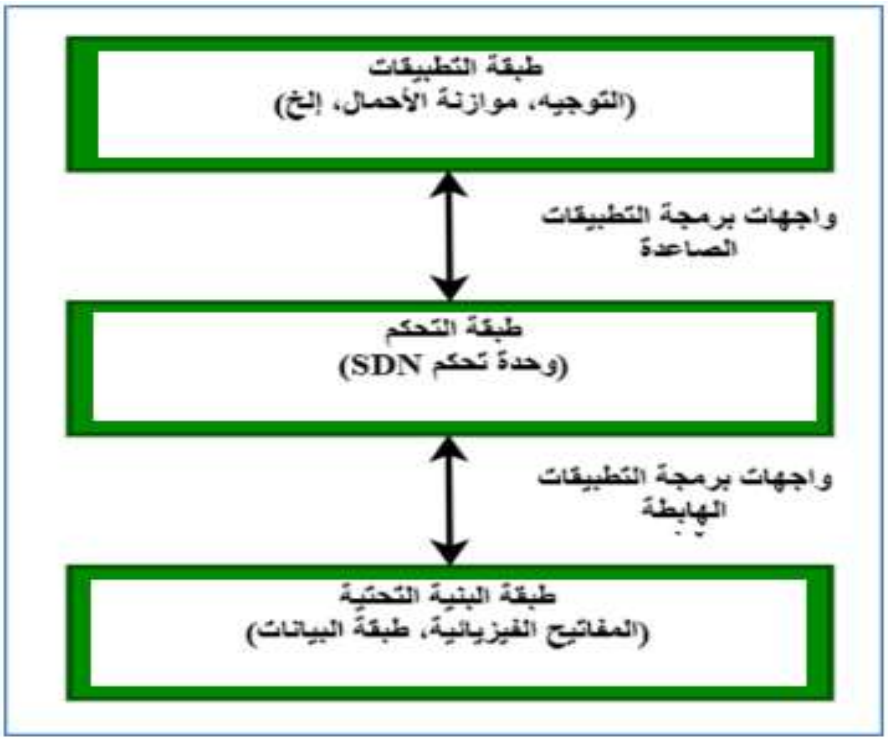
2.1.5 مكونات الشبكات المعرفة بالبرمجيات

1- **طبقة التطبيقات (Application Layer) :** وتضم هذه الطبقة التطبيقات التي تتفاعل مع الشبكة وتحتاج إلى خدمات محددة، مثل تطبيقات الأمان والمراقبة وإدارة البيانات. تقوم هذه الطبقة بإرسال طلبات إدارة الشبكة إلى وحدة التحكم المركزية.

2- **طبقة التحكم (Control Layer) :** وتُعد أهم طبقة في **SDN**، أذ تُدير وحدة التحكم لمركزية هذه الطبقة. تقوم وحدة التحكم بتفسير طلبات التطبيقات وتحليلها ثم اتخاذ قرارات تتعلق بتوجيه حركة البيانات، بناءًا على السياسات والقواعد المعرفة سلفًا.

3- **طبقة البنية التحتية (Infrastructure Layer) :** تضم هذه الطبقة الأجهزة المادية مثل الموجهات (**Routers**) والمفاتيح (**Switches**) التي تنفذ الأوامر الصادرة عن وحدة التحكم. يمكن تحديث الأجهزة وإدارتها من الأوامر البرمجية دون الحاجة إلى تغيير إعداداتها يدويًا.

هذه العناصر تعمل معًا لجعل شبكات التحديد البرمجي أكثر مرونة وسهولة في الإدارة، وتمكينها من التكيف مع متطلّبات البيئة المتغيرة بسرعة , انظر الى الشكل (2-5).



شكل (2-5) مكونات الشبكات المعرفة بالبرمجيات

تتواصل هذه الطبقات عبر مجموعة من الواجهات البرمجية تُعرف بـالواجهـات الشـمالية (**North-bound APIs**) التي تربط بين طبقة التطبيقات وطبقة التحكم، والواجهات الجنوبية (**South-bound APIs**) التي تربط بين طبقة التحكم وطبقة البنية التحتية.

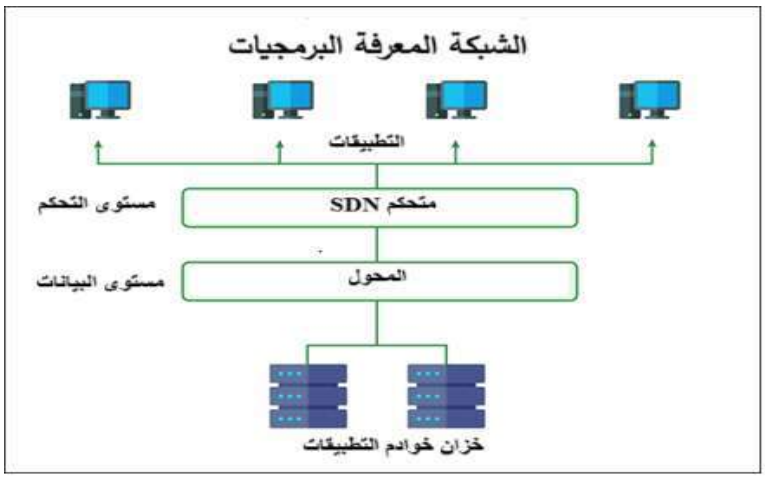
هذا ومن الجدير بالذكر ان ننوه هنا الى انه يوجد أيضا مفهومان أساسيان في **SDN** يرتبطان ارتباطًا وثيقًا بالطبقات الثلاث المذكورة آنفا وكما يظهر في الشكل (5-3), وهذان المفهومان هما:

أ- مستوى التحكم (**Control Plane**)

في هذه الطبقة تتخذ القرارات الذكية حول كيفية توجيه حركة البيانات في الشبكة. يعتمد هذا التوجيه على تحليل متطلبات الشبكة والمرور، وتطبيق السياسات المحددة لضمان تحقيق أفضل طرق لتوجيـــه الحركة في الشبكة.

ب- مستوى البيانات (**Data Plane**)

بعد اتخاذ القرارات في طبقة التحكم، تقوم طبقة البيانات بتنفيذ هذه القرارات عملياً عبر توجيـه البيانات بناءً على التوجيهات التي وضعت في طبقة التحكم، وذلك لضمان وصول البيانات إلى الوجهة المحددة بشكل سليم وفعال.



الشكل (5-3)

3.1.5 أهم مزايا تقنية الشبكات المعرفة بالبرمجيات

1- زيادة المرونة والتكيف:

يسمح **SDN** بتعديل تكوينات الشبكة بشكل ديناميكي، وهذا يتيح للمؤسسات التكيف السريع مع تغيرات متطلبات الأعمال والتطبيقات. يمكن إعادة توجيه حركة البيانات وتكوين الشبكة بشكل فوري استنادًا إلى احتياجات النظام.

2- تحسين أداء الشبكة:

بفضل القدرة على تحديد مسارات البيانات بشكل دينامي، يمكن تحسين أداء الشبكة وتقليل الازدحام، وهذا يضمن تقديم خدمات سريعة وفعّالة.

3- تبسيط الإدارة:

يسهم نموذج **SDN** في تبسيط إدارة الشبكة بشكل كبير، أذ يتيح للمشغلين استخدام واجهات برمجة تطبيقات (**API**) لتكوين وإدارة الشبكة، وهذا يقلل من تعقيد العمليات.

4- تقليل التكلفة:
بفضل تحسين استخدام الموارد وتبسيط الإدارة، يمكن أن يؤدي **SDN** إلى تقليل التكلفة الإجمالية لملكية النظام(**TCO**) ، فيعزز جاذبية هذه التقنية للمؤسسات.

5- تمكين الابتكار:
يتيح **SDN** للمطورين والمؤسسات تجريب وتنفيذ تطبيقات جديدة وابتكارات في مجال الشبكات بشكل أسرع ، وهذا يدفع بتطور البيئة التكنولوجية.

6- أمان محسن:
يسمح **SDN** بتنفيذ إجراءات أمان أكثر فعالية عبر توجيه حركة البيانات بشكل ذكي وفحص متقدم للحماية من التهديدات.

4.1.5 دور الشبكات المعرفة بالبرمجيات في أمان الشبكات

تعد قضايا الأمن محورًا أساسيًا عند اعتماد الشبكات المعرفة بالبرمجيات ومن الفوائد الكبيرة التي تقدمها هذه الشبكات في هذا الجانب القدرة على دمج الأمن في المعمارية الأساسية للشبكة بدلًا من إضافته كخدمة ثانوية حيث يُمكن للمتحكم مراقبة حركة البيانات على مستوى الحُزم (**Packets**) في الزمن الفعلي، ثم اتخاذ قرارات فورية في حال الاشتباه بسلوك خبيث أو نشاط غير مألوف. ويمكن تعزيز الأمن في الشبكات المعرفة بالبرمجيات عبر ما يأتي:

- استخدام بروتوكولات مشفّرة بين طبقة التحكم وطبقة البنية التحتية مثل **TLS** أو**DTLS** .
- توزيع المتحكمات (**Distributed Control**) بحيث لا تكون هناك نقطة مركزية وحيدة يمكن استهدافها.
- اعتماد آليات تحكم بالوصول لتحديد صلاحيات كل عنصر في الشبكة.
- تطبيق تحليلات متقدمة (**Advanced Analytics**) لرصد الشذوذ في مرور الحزم.
- النشر التلقائي لقواعد جدران الحماية في جميع أركان الشبكة، بدلًا من أجهزة محدودة المواقع.

2-5 استخدام الذكاء الأصطناعي في تأمين الشبكات والحوسبة السحابية

مع التطور السريع في تقنيات الشبكات وازدياد الاعتماد على البُنى التحتية السحابية، بات من الضروري استخدام أدوات متقدمة لحماية هذه الأنظمة من التهديدات المتزايدة والمعقدة.
ويُعد الذكاء الأصطناعي **Artificial Intelligence (AI)** من أبرز التقنيات الحديثة التي أسهمت في تعزيز أمن الشبكات, وذلك لقدرتها على تحليل البيانات الضخمة، والتعلم من الأنماط السلوكية، واتخاذ قرارات تلقائية وذكية. في هذا الجزء من الفصل، سنتناول بشكل مختصر كيف يُستخدم الذكاء الأصطناعي لتأمين الشبكات والحوسبة السحابية، بعرض التطبيقات الأساسية، مثل أنظمة كشف التسلل، وتحليل السلوك، والاستجابة التلقائية، إلى جانب التحديات المرتبطة باستخدام هذه التقنية.

1- تحسين الكشف عن التهديدات والاستجابة لها
يُعزز الذكاء الاصطناعي قدرات الأنظمة الأمنية بما يأتي:

- **الكشف التلقائي عن التهديدات** :تحليل سلوك الشبكة لاكتشاف الأنماط غير المعتادة التي قد تشير إلى هجمات سيبرانية.

- **الاستجابة الفورية** :تنفيذ إجراءات تلقائية مثل عزل الأجهزة المشبوهة أو إعادة توجيه حركة المرور عند اكتشاف تهديدات .
- **تحليل السلوك** :تحديد الأنشطة غير المعتادة للمستخدمين أو الأجهزة، ويسهم هذا في الكشف المبكر عن التهديدات .
- **إدارة الثغرات** :تقييم الأنظمة بسرعة لتحديد نقاط الضعف وتصحيحها قبل استغلالها.

2- تعزيز أمان الحوسبة السحابية

في بيئات الحوسبة السحابية، يُستخدم الذكاء الأصطناعي في:

- **أتمتة إدارة الأمان** :تنفيذ التصحيحات الأمنية وتحديثات النظام تلقائيًا.
- **تحسين إدارة البيانات** :نقل وتنقيحها البيانات، ومسح الشبكات للكشف عن مشكلات الأمان.
- **التحليلات التنبؤية** :تحديد الاتجاهات والارتباطات في البيانات لاتخاذ قرارات أمنية مستنيرة .
- **تحسين قابلية التوسع** :أتمتة العمليات لتشغيل مراكز بيانات كبيرة بكفاءة عالية.

3- التحديات

على الرغم من الفوائد الكبيرة في استخدام الذكاء الأصطناعي، الا ان هناك تحديات يجب مراعاتها :

جودة البيانات: دقة النماذج تعتمد على جودة البيانات المُدخلة وتمثيلها للسيناريوهات الواقعية.

الخصوصية: تحليل البيانات الحساسة (مثل سجلات المستخدمين) قد يُثير مخاوف تتعلق بالامتثال للقوانين.

التكلفة والتعقيد: تكامل أنظمة الذكاء الأصطناعي مع البنى التحتية القائمة قد يتطلب موارد تقنية وخبرات متخصصة.

3-5 الحوسبة السحابية دون خوادم (Serverless)

1.3.5 تعريف الحوسبة بدون خادم

وهي نموذج حوسبة سحابي يتيح للمطورين بناء التطبيقات والخدمات وتشغيلها دون الحاجة إلى إدارة الخوادم أو البنية التحتية المرتبطة بها. بدلاً من التركيز على إدارة الخوادم، يمكن للمطورين تركيز جهدهم على كتابة الشيفرات البرمجية الخاصة بهم بينما يتولى موفرو الخدمات السحابية مسؤولية إدارة الخوادم التي تدعم التطبيقات وتشغيلها.

في نموذج الحوسبة بدون خادم، تنقسم الوظائف على "وظائف" صغيرة تُنفذ عند الحاجة فقط، مما يُحسن من الكفاءة ويقلل التكاليف. على سبيل المثال، بدلاً من دفع تكلفة خادم يعمل طوال الوقت، يدفع المستخدم مقابل العمليات الحسابية التي تنفذ فقط.

2.3.5 كيف تعمل الحوسبة دون خادم؟

تعمل الحوسبة دون خادم عبر توزيع الوظائف على وحدات صغيرة تسمى الدوال (**Functions**)هذه الدوال هي وحدات من الكود البرمجي التي يمكن أن تُنفذ فقط عندما يحتاج إليها النظام. يعتمد النموذج على الآتي:

1- إلغاء الحاجة ألى إدارة الخوادم: تستخدام البنية التحتية السحابية مثل **AWS Lambda** أو **Azure Functions**، مما يعني أن المستخدمين لا يحتاجون إلى القلق بشأن الخوادم، وصيانتها، وتحديثاتها.

2- الدفع مقابل الاستخدام فقط :في الحوسبة التقليدية، تدفع الأموال بناءً على قدرة الخوادم أو السعة التخزينية. بينما في الحوسبة بدون خادم، يدفع المستخدمون فقط مقابل الوظائف التي وتنفذ فعلاً، مما يعني توفير التكاليف بشكل كبير.

3- التوسع التلقائي :أحد السمات المهمة لهذه التقنية هو التوسع التلقائي. أذ توفر الموارد بناءً على الطلب، مما يعني أن النظام يمكنه التعامل مع زيادات مفاجئة في حركة المرور دون تدخل يدوي.

3.3.5 الاستخدامات الرئيسية للحوسبة دون خادم

1- التطبيقات المبنية على الأحداث

تُستخدم الحوسبة دون خادم بشكل شائع في التطبيقات التي تعتمد على الأحداث، مثل تطبيقات الإنترنت التي تستجيب لأحداث مثل إرسال بريد إلكتروني، تحميل ملفات، أو إجراء تغييرات في قاعدة البيانات. فعلى سبيل المثال، عندما يحمل مستخدم صورة، يمكن أن يُطلق هذا الحدث وظيفة تقوم بإعادة تحجيم الصورة تلقائيًا أو تخزينها في سحابة.

2- خدمات الويب والواجهات البرمجية (APIs)

يمكن استخدام الحوسبة دون خادم في تطوير خدمات الويب والواجهات البرمجية .(**APIs**) أذ يُمكن للمطورين بناء **APIs** صغيرة تعمل على استجابة الطلبات بشكل سريع وفعال، دون القلق بشأن صيانة الخوادم أو توسيع البنية التحتية.

3- المعالجات المعقدة للبيانات

يُستخدم هذا النموذج أيضًا في معالجة البيانات الكبيرة والتحليل. أذ يمكن لمجموعة من الدوال الصغيرة أن تعمل على معالجة كميات ضخمة من البيانات بشكل متوازي، مما يوفر كفاءة عالية في معالجة البيانات.

4- التطبيقات المحمولة

يمكن استخدام الحوسبة دون خادم لتطوير التطبيقات المحمولة، أذ تتطلب هذه التطبيقات قدرًا كبيرًا من العمليات الخلفية مثل معالجة الدفع أو إرسال التنبيهات. يمكن تقليص الحاجة إلى خوادم ضخمة باستخدام هذا النموذج.

4.3.5 فوائد الحوسبة دون خادم

1- التوفير في التكاليف

يُعد التوفير في التكاليف أحد أكبر مزايا الحوسبة دون خادم. لا يحتاج المستخدمون إلى دفع رسوم ثابتة لصيانة الخوادم، بل يدفعون فقط مقابل الوقت الذي تنفذ فيه الوظائف. هذا يعني أنه يمكن تقليل النفقات شكل كبير، خاصة في التطبيقات التي لا تعمل على مدار الساعة.

2- التوسع التلقائي

يمكن لتقنية الحوسبة دون خادم التوسع تلقائيًا استجابةً للزيادة المفاجئة في حجم البيانات أو الطلبات. إذا كان هناك زيادة غير متوقعة في حركة المرور، فإن النظام سيُكثف من الموارد بشكل تلقائي لضمان استجابة سريعة ومستوى أداء عالٍ.

3- سهولة التطوير والإدارة

من خلال الحوسبة دون خادم، يمكن للمطورين التركيز على كتابة الشيفرات البرمجية بدلاً من الاهتمام بإدارة الخوادم والبنية التحتية. هذا يقلل من الوقت والجهد المبذول في صيانة الأنظمة.

4- المرونة

توفر الحوسبة دون خادم مرونة كبيرة في التطوير. يمكن تطوير التطبيقات وتوسيعها بسرعة، ويمكن تعديل الوظائف على نحو سريع دون التأثير في النظام بشكل عام.

5.3.5 العيوب والتحديات

1- القيود على الوقت

في بعض الأحيان، قد تكون هناك قيود على الوقت المخصص لكل دالة أو وظيفة، مما قد يؤثر في أداء التطبيقات التي تتطلب عمليات معالجة معقدة أو طويلة.

2- تعقيد التدقيق والاختبار

قد يصبح من الصعب اختبار التطبيقات المعتمدة على الحوسبة دون خادم بسبب تعقيد البنية التحتية التي تديرها الشركات السحابية. يتطلب الأمر أدوات اختبار متقدمة لضمان أن كل دالة تعمل كما ينبغي.

3- التكلفة غير المتوقعة

على الرغم من أن الحوسبة دون خادم قد تُخفض التكاليف في كثير من الحالات، فقد تؤدي إلى فواتير غير متوقعة إذا لم يُحسن تكوين الوظائف بشكل جيد، أو إذا كانت العمليات الحسابية تتطلب وقتًا أطول.

4-5 الحوسبة الطرفية (Edge Computing)

ينتجها، بدلاً من إرسالها إلى مراكز بيانات مركزية بعيدة كما هو الحال في الحوسبة السحابية. يُطلق على الأجهزة التي تقوم بهذه العمليات اسم "الأجهزة الطرفية"، مثل الهواتف الذكية، وأجهزة الاستشعار، والكاميرات، وحتى السيارات الذكية.

1.4.5 أهمية الحوسبة الطرفية

تتمتع الحوسبة الطرفية بأهمية كبيرة في الكثير من المجالات والصناعات، ومن أبرز أهداف الحوسبة الطرفية ما يأتي:

1. تحسين الأداء

تُتيح الحوسبة الطرفية تنفيذ العمليات المحسوبة وتخزين البيانات على الأجهزة المحلية بالقرب من مصدر البيانات. لتقليل التأخير في الاستجابة وتحسين أداء التطبيقات، خاصة تلك التي تتطلب استجابة فورية مثل التحكم في الأجهزة الذكية والسيارات المتصلة والأجهزة الطبية.

2. خفض الاعتماد على الشبكة

تنفذ العمليات وتخزن البيانات في الأجهزة المحلية، بدلاً من إرسال البيانات إلى السحابة المركزية للمعالجة، مما يقلل من حجم البيانات المرسلة عبر الشبكة ويقلل من الاعتماد على استقرار الاتصال بالشبكة ويحسن استجابة التطبيقات.

3. تعزيز الخصوصية والأمان

يُتيح الحفاظ على البيانات المحسوبة وتخزينها في الحواف المحلية حماية أفضل للبيانات الحساسة، حيث لا تحتاج البيانات إلى المرور عبر الشبكة، مما يقلل من مخاطر التعرض للاختراق ويزيد من سرية البيانات.

4. توفير تكلفة الشبكة والتخزين

بفضل الحوسبة الطرفية، يمكن تقليل الحاجة إلى نقل البيانات الكبيرة إلى السحابة السحابية المركزية، أذ توفر تكلفة الشبكة والتخزين وتسهم في تحسين كفاءة استخدام الموارد.

5. تحسين استدامة الشبكات

توزع العمليات والمعالجة على الأجهزة المحلية بدلاً من الاعتماد على السحابة السحابية المركزية، وهذا يخفض الضغط على الشبكة ويحسن استدامتها، وتوفير طاقة وموارد بيئية.

2.4.5 أنواع الحوسبة الطرفية

هناك الكثير من الطرق المستخدمة لتصنيف شبكات وتقنيات الحافة، ومنها ما يلي:

1. أنواع الحوسبة الطرفية حسب التكنولوجيا

هناك عدة أنواع من الحوسبة الطرفية (**Edge Computing**) وفقًا للتكنولوجيا المستخدمة. وتعتمد هذه الأنواع على مجموعة متنوعة من التقنيات لتحسين قدرة معالجة البيانات وتقديم خدمات فعّالة عند الحافة أو قرب المصادر. إليك بعض أنواع الحوسبة الطرفية حسب التكنولوجيا:

a- الحوسبة الطرفية للجهاز (Device edge)

تشير الحوسبة الطرفية للجهاز إلى حافة الشبكة التي توجد بها الأجهزة، التي تولد البيانات أو تستهلكها، وتتضمن حوسبة الحافة معالجة البيانات بشكل أقرب إلى هذه الأجهزة بدلاً من الاعتماد على خوادم سحابية مركزية. وتتضمن أمثلة الأجهزة المتطورة أجهزة الاستشعار والمحركات والكاميرات والهواتف الذكية وأجهزة إنترنت الأشياء الأخرى. وتعد هذه الأجهزة جزءًا لا يتجزأ من عمل التطبيقات المختلفة، وتستفيد حوسبة الحافة من قدراتها الحسابية لتوفير معالجة أسرع وأكثر كفاءة، ولا سيما في السيناريوهات التي تتطلب استجابات في الوقت الفعلي.

b- الحوسبة الطرفية السحابية (Cloud edge)

تشير السحابة إلى مركز بيانات صغير الحجم يقع على حافة الشبكة. وتوفر موارد الحوسبة والتخزين للأجهزة والمستخدمين القريبين. كما توفر حافة السحابة حلاً وسطًا بين المعالجة المحلية والمعالجة المستندة إلى السحابة بتوفير بنية تحتية خفيفة الوزن ومنخفضة المؤن للحوسبة الطرفية.

c- الحوسبة الطرفية الحسابية (Compute edge)

هي نموذج حوسبة موزع يجعل الحساب وتخزين البيانات أقرب إلى الموقع حيث تكون هناك حاجة إليه، وغالبًا ما يكون بالقرب من حافة الشبكة أو بالقرب من مصدر البيانات. وهذا على النقيض من الحوسبة السحابية التقليدية حيث ترسل البيانات إلى مركز بيانات مركزي للمعالجة. صممت الحوسبة المتطورة لمعالجة قيود الحوسبة السحابية المركزية، خاصة في السيناريوهات التي يكون فيها زمن الوصول المنخفض والمعالجة في الوقت الفعلي والاستخدام الفعال للنطاق الترددي أمرًا بالغ الأهمية.

d- الحوسبة الطرفية الاستشعارية (Sensor edge)

تشير الحوسبة الطرفية الاستشعارية إلى الحوسبة الطرفية لإنترنت الأشياء (**IoT**)، وهي تتضمن حوسبة حافة إنترنت الأشياء معالجة وتحليل البيانات التي تم إنشائها بواسطة أجهزة إنترنت الأشياء على حافة الشبكة. وتهدف إلى تقليل كمية البيانات المرسلة إلى السحابة المعالجة، مما يتيح رؤى أسرع، واتخاذ القرارات في الوقت الحقيقي، وتقليل متطلبات النطاق الترددي.

2. أنواع الحوسبة الطرفية حسب الموقع

يعد الموقع الفعلي للنشر الخاص بك طريقة شائعة أخرى لتنظيم أنواع الحوسبة الطرفية. في حين أن هذه يمكن أن تكون جزءًا من أي من الفئات القائمة على التكنولوجيا أو حتى مزيجًا منها، ومنها:

a- الحوسبة الطرفية المؤسسية (Enterprise edge)

تشير الحوسبة الطرفية المؤسسية إلى البنية التحتية للشبكة وموارد الحوسبة الموجودة على الحوسبة الطرفية لشبكة المؤسسة، إذ تؤدي دورًا حاسمًا في ضمان أمان شبكة المؤسسة وأدائها وموثوقيتها. فهي توفر بوابة محكمة وآمنة للاتصال بالشبكات الخارجية مع حماية الموارد والبيانات الداخلية. وقد تختلف المكونات والتكوينات المحددة للحوسبة الطرفية للمؤسسة وفقًا لاحتياجات المؤسسة وحجمها ومتطلبات الصناعة.

b- الحوسبة الطرفية الفرعية (Branch edge)

يشير مصطلح الحوسبة الطرفية الفرعية إلى البنية التحتية للشبكة وموارد الحوسبة الموجودة على حافة مكتب فرعي داخل شبكة المؤسسة. وهي تمثل الحدود بين الشبكة الداخلية للمكتب الفرعي وشبكة المؤسسة الأوسع. وتشتمل على مكونات ووظائف متنوعة تُتيح الاتصال والأمان والمعالجة المحلية على مستوى الفرع. فهي تُتيح الوصول المحلي إلى موارد الشبكة، وتُحسن من أداء الشبكة، وتضمن سياسات وضوابط أمان متسقة على مستوى الفرع. وقد تختلف المكونات والتكوينات المحددة للحافة الفرعية اعتمادًا على الحجم والمتطلبات والبنية التحتية لتكنولوجيا المعلومات الخاصة بالمكتب الفرعي وشبكة المؤسسة الشاملة.

c- الحوسبة الطرفية المتنقلة (Mobile edge)

تجعل الحوسبة الطرفية المتنقلة القدرات والخدمات الحسابية أقرب إلى حافة شبكة الهاتف المحمول. مما يُتيح تنفيذ مهام مثل معالجة البيانات والتخزين والتخزين المؤقت للمحتوى على حافة الشبكة الخلوية، وكذلك تقليل زمن الوصول وتحسين تجربة المستخدم لتطبيقات الهاتف المحمول.

3.4.5 مكونات الحوسبة الطرفية

تتضمن مكونات الحوسبة الطرفية عناصر وتقنيات مختلفة، منها:

1. أجهزة الحوسبة المحلية

تشمل الأجهزة المحلية مثل الخوادم الصغيرة (**servers**)، وأجهزة الشبكة (**network devices**) مثل الموجهات (**routers**) والمفاتيح (**switches**)، والأجهزة الذكية (**smart devices**) مثل الهواتف الذكية والأجهزة اللوحية والأجهزة المحمولة الأخرى. تعمل هذه الأجهزة على تنفيذ العمليات وتخزين البيانات بالقرب من مصدر البيانات ومستخدمي التطبيقات.

2. برمجيات الحوسبة المحلية

تشمل برمجيات الحوسبة المحلية أنظمة التشغيل الخاصة بالأجهزة المحلية، والبرامج والمكتبات المسؤولة عن تنفيذ العمليات وإدارة التخزين، والبرمجيات المسؤولة عن تواصل وتنسيق البيانات بين الأجهزة المحلية والسحابة السحابية الرئيسية (**central cloud**).

3. الاتصالات اللاسلكية والشبكات

تعتمد الحوسبة الطرفية على الاتصالات اللاسلكية مثل شبكات الجيل الخامس (**5G**) وإنترنت الأشياء (**IoT**)، والشبكات المحلية والشبكات اللاسلكية الأخرى لتمكين اتصال البيانات ونقلها بين الأجهزة المحلية والسحابة السحابية الرئيسية.

4. تقنيات الحاويات والأتمتة

تستخدم تقنيات الحاويات (**containers**) في الحوسبة الطرفية لتوفير بيئة معزولة وقابلة للتحميل لتشغيل التطبيقات والخدمات على الأجهزة المحلية. وتستخدم تقنيات الأتمتة (**automation**) لإدارة الأجهزة المحلية وتكوينها وتنفيذ العمليات بشكل آلي وفعال.

5. تقنيات تحليل البيانات والذكاء الاصطناعي

يؤدي التحليل الحيوي للبيانات وتقنيات الذكاء الاصطناعي (**AI**) دورًا مهمًا في الحوسبة الطرفية. تستخدم هذه التقنيات لاستخلاص المعلومات والاستدلال من البيانات المحسوبة في الوقت الفعلي، مما يمكن من تحقيق تحليلات متقدمة واتخاذ قرارات سريعة على الأجهزة المحلية.

4.4.5 مبادئ الحوسبة الطرفية

ترتكز مبادئ الحوسبة الطرفية على تحقيق مجموعة من الأهداف وتطبيق مبادئ محددة، ومن أهم مبادئ الحوسبة الطرفية ما يأتي:

1. اللامركزية (Decentralization)

تهدف الحوسبة الطرفية إلى نقل القدرة الحسابية والمعالجة والتخزين إلى الحواف أو الأجهزة المحلية بدلاً من الاعتماد بشكل حصري على السحابة السحابية المركزية. ويُتيح ذلك توزيع العمل بين الأجهزة المحلية وتحسين استجابة التطبيقات وتقليل التباين.

2. القرب من المصدر (Proximity to Source)

تتم معالجة البيانات وتحليلها وتنفيذ التطبيقات بالقرب من مصدر البيانات والمستخدمين، مما يقلل من الوقت المستغرق في نقل البيانات عبر الشبكة ويقلل من التأخير ويحسن استجابة التطبيقات في الوقت الفعلي.

3. توزيع العمل (Work Distribution)

يتم توزيع العمل والمعالجة بين الأجهزة المحلية والسحابة السحابية الرئيسية. وتنفذ الأجهزة المحلية المهام والمعالجة المحلية للبيانات، بينما تستخدم السحابة السحابية الرئيسية للمهام الأكثر تعقيدًا والتخزين بشكلل طويل الأمد.

4. الأمان والخصوصية (Security and Privacy)

يعد الأمان والخصوصية عاملين مهمين في الحوسبة الطرفية. وبتخزين البيانات ومعالجتها على الأجهزة المحلية، يمكن تحقيق مستويات أعلى من الأمان والحفاظ على خصوصية البيانات، ويقلل من انتقال البيانات عبر الشبكة.

5. التواصل الفعال (Effective Communication)

يعد التواصل الفعال بين الأجهزة المحلية والسحابة السحابية الرئيسية أمرًا أساسيًا. وتستخدم تقنيات الشبكات والاتصالات اللاسلكية المتقدمة مثل 5G و IoT لتمكين اتصال سريع وموثوق بين الأجهزة والسحابة السحابية.

6. المرونة والتطوير المستدام (Flexibility and Scalability)

تهدف الحوسبة الطرفية إلى توفير مرونة وقابلية للتطوير للبيئات المحلية. ويجب أن تكون الحوسبة الطرفية قادرة على التكيف مع تغيرات الطلب واستيعاب عدد أكبر من الأجهزة والتطبيقات دون التأثير في أداء النظام بشكل سلبي.

5.4.5 طرق تطبيق الحوسبة الطرفية

هناك عدة طرق يمكن استخدامها لتطبيق الحوسبة الطرفية. ومن أهم الطرق الشائعة لتحقيق الحوسبة الطرفية ما يأتي:

1- أجهزة الحواف المحلية (Edge Devices)

يمكن استخدام أجهزة الحواف المحلية مثل أجهزة الكمبيوتر المحمولة والأجهزة الذكية والأجهزة القابلة للارتداء والأجهزة المتصلة بالإنترنت لتنفيذ المعالجة وتخزين البيانات بشكل محلي. ويوزع العمل بين هذه الأجهزة والسحابة السحابية الرئيسية وفقًا لمتطلبات التطبيق.

2- البوابات الطرفية (Edge Gateways)

تعمل البوابات الطرفية وسيطا بين الأجهزة المحلية والسحابة السحابية الرئيسية. وتجمع البيانات من الأجهزة المحلية وتنقلها إلى السحابة السحابية للمعالجة والتحليل. وكذلك توزيع الأوامر والتحديثات من السحابة السحابية إلى الأجهزة المحلية.

3- الشبكات اللاسلكية المتقدمة (Advanced Wireless Networks)

تستخدم تقنيات الشبكات اللاسلكية المتقدمة مثل G5 وشبكات **IoT** لتمكين اتصال سريع وموثوق بين الأجهزة المحلية والسحابة السحابية الرئيسية. وتوفر هذه الشبكات سعات عالية وتأخيرا منخفضا وتدعم استخدامات الوقت الفعلي والتحكم في الأجهزة عن بُعد.

4- تقنيات التحليل والذكاء الاصطناعي المحلي (Local Analytics and AI)

يمكن استخدام تقنيات التحليل و الذكاء الصناعي المحلي لتنفيذ المعالجة والتحليل على الأجهزة المحلية. وتطبق تقنيات التعلم العميق والشبكات العصبية الاصطناعية على الأجهزة المحلية لاتخاذ القرارات في الوقت الفعلي وتحقيق تجربة مستخدم محسنة.

5- لحوسبة الحدودية (Fog Computing)

تعد الحوسبة الحدودية نموذجًا يجمع بين الحوسبة الطرفية و الحوسبة السحابية. وتستخدم الحوسبة الحدودية البنية التحتية السحابية الموجودة على الحواف لتنفيذ المعالجة والتخزين .

6.4.5 أمثلة عملية على الحوسبة الطرفية

1- السيارات ذاتية القيادة

تحتاج السيارات ذاتية القيادة إلى معالجة البيانات بسرعة فائقة لاتخاذ القرارات في الوقت الحقيقي. لذلك، تعتمد على الحوسبة الطرفية لمعالجة بيانات أجهزة الاستشعار والكاميرات داخليًا.

2- إنترنت الأشياء (IoT)

في المنازل الذكية، تُستخدم الحوسبة الطرفية لمعالجة بيانات الأجهزة مثل الكاميرات وأجهزة الإنذار محليًا، وهذا يتيح استجابة أسرع.

3- المجال الطبي

تستخدم الحوسبة الطرفية في الأجهزة الطبية مثل أجهزة مراقبة نبضات القلب، ويتم تحليل البيانات محليًا لتنبيه الأطباء أو المرضى في الحالات الطارئة.

7.4.5 الفرق بين الحوسبة الطرفية والحوسبة السحابية

1- الموقع الجغرافي

- **الحوسبة الطرفية:** تعالج البيانات بالقرب من المصدر، مما يقلل من وقت الانتقال والتأخير.
- **الحوسبة السحابية** :تعتمد على مراكز بيانات مركزية قد تكون بعيدة جغرافيًا عن المستخدم.

2- زمن الاستجابة

- **الحوسبة الطرفية** :تتيح استجابة أسرع بفضل تقليل المسافة بين مصدر البيانات والمكان الذي تُعالج فيه.
- **الحوسبة السحابية :**قد تواجه تأخيرًا بسبب الزمن المستغرق لنقل البيانات إلى الخوادم البعيدة.

3-الأمان والخصوصية

- **الحوسبة الطرفية** :توفر مستوى أمان أعلى، ويتم معالجة البيانات محليًا مما يقلل من احتمال تعرضها للاختراق أثناء النقل.

- **الحوسبة السحابية** :تعتمد على بروتوكولات الأمان المتبعة في مراكز البيانات، ولكنها تظل عرضة للهجمات الإلكترونية أثناء نقل البيانات.

4-استهلاك النطاق الترددي

- **الحوسبة الطرفية** :تقلل من استهلاك النطاق الترددي, لإنها تعالج البيانات محليًا قبل إرسالها، إن لزم الأمر.
- **الحوسبة السحابية** :تتطلب نطاقًا ترددًا عاليًا لنقل كميات كبيرة من البيانات إلى الخوادم.

5- قابلية التوسع

- **الحوسبة الطرفية :**تتطلب تجهيزات مادية على مستوى الأجهزة الطرفية، مما يجعل التوسع أكثر تعقيدًا.
- **الحوسبة السحابية** :توفر قابلية توسع مرنة بفضل مواردها الضخمة والمشتركة.

تمرين رقم 1 : تطبيق تقنية SDN على شبكة محلية

الهدف من التمرين:

تدريب الطلبة على القيام بتطبيق تقنية **SDN** على شبكة محلية .

المتطلبات الأساسية:

- جهاز حاسوب بنظام تشغيل **Windows/Linux/Mac**
- برنامج **VirtualBox** أو **VMware**
- نسخة جاهزة من **Mininet VM** يمكن تحميلها من:

https://github.com/mininet/mininet/wiki/Mininet-VM-Images

الخطوات العملية

خطوة 1: تنصيب **VirtualBox**

خطوة 2: تشغيل **Mininet** داخل **VirtualBox**

خطوة 3: حمل ملف الـ **OVA** وشغله في **VirtualBox**

خطوة 4: اسم المستخدم عادةً **mininet** وكلمة المرور **mininet**

خطوة 5: فتح الطرفية وتشغيل شبكة بسيطة

خطوة 6: اكتب الأمر الآتي لإنشاء شبكة فيها ومضيفان, ومحولا واحدا, ووحدة تحكم وحدة :

sudo mn --topo single,2 **--controller=remote --mac**

--topo single, تعني وجود محولا واحدا (**Switch**) ومضيفين (**Hosts**)

--controller=remote تعني استخدام وحدة تحكم **SDN** خارجية مثل **POX** أو **Ryu**

--mac يحدد عناوين **MAC** بشكل مباشر

خطوة 7: اختبار الاتصال بين المضيفين داخل الواجهة التفاعلية (**Mininet CLI**) ، اكتب:

pingall

يجب أن ترى أن **h1** يمكنه الاتصال بـ**h2**.

النتيجة المتوقعة:

ان يكون الطالب قادرا على تطبيق تقنية **SDN** على شبكة محلية.

استمارة الفحص تمرين رقم (1)			
الجهة الفاحصة:			
اسم الطالب :	المرحلة الثالثة	التخصص : الامن السيبراني	
اسم التمرين : تطبيق تقنية SDN على شبكة محلية			

ت	الخطوات	الدرجة القياسية % 50	درجة الاداء %50	الملاحظات
1	تنصيب VirtualBox	%5		
2	تشغيل Mininet داخل VirtualBox حمل ملف الـ OVA وشغله في VirtualBox اسم المستخدم عادةً mininet وكلمة المرور mininet فتح الطرفية وتشغيل شبكة بسيطة	%10		
3	اكتب الأمر الخاص بإنشاء شبكة بها 2 مضيف و 1 محول و 1 وحدة تحكم	%10		
4	اختبار الاتصال بين المضيفين داخل الواجهة التفاعلية (Mininet CLI)	%5		
5	المناقشة	%10		
6	الزمن المخصص	%10		
المجموع				
اسم الفاحص		التوقيع		

تمرين رقم 2: إنشاء بيئة سحابية بدون خوادم (Serverless) باستخدام AWS Lambda

الهدف من التمرين:

إنشاء دالة ترحيب باستخدام (**AWS Lambda**) تُرجع رسالة ترحيب عند تنفيذها.

المتطلبات الإساسية:

a. حساب **AWS** مجاني

b. اتصال بالإنترنت.

c. متصفح حديث.

الخطوات العملية

خطوة 1: تسجيل الدخول إلى:**AWS Console**

انتقل إلى**https://console.aws.amazon.com/** :

خطوة 2: فتح خدمة **Lambda** :

ابحث عن **Lambda** في شريط البحث، ثم اختر."**Create function**"

خطوة 3: إعداد الدالة:

اختر."**Author from scratch**"

الاسم **HelloFunction** :

Runtime: **Python** 3.12 أو أي إصدار متاح

Role اختر."**Create a new role with basic Lambda permissions**"

خطوة 4: كتابة الكود:

سيظهر محرر الكود، استبدل الكود الافتراضي بما يأتي:

```
def lambda_handler(event, context):
  {
     Return
        'statusCode': 200,
        'body': 'Hello from AWS Lambda!'
   }
```

خطوة 5: حفظ الدالة:

اضغط على "**Deploy**" لحفظ التغييرات.

خطوة 6: اختبار الدالة:
اختر **"Test"** من الأعلى.
أنشئ حدث اختبار باسم **TestEvent** واترك البيانات كما هي.
اضغط **"Test"** مرة أخرى، وستظهر رسالة:

```
{
  "statusCode": 200,
  "body": "Hello from AWS Lambda!"
}
```

النتيجة المتوقعة:

ان يكون الطالب قادرا على انشاء دالة ترحيب باستخدام (**AWS Lambda**) تُرجع رسالة ترحيب عند تنفيذها.

استمارة الفحص **تمرين رقم (2)**			
الجهة الفاحصة:			
اسم الطالب : **المرحلة الثالثة** **التخصص : الامن السيبراني**			
اسم التمرين : إنشاء بيئة سحابية بدون خوادم (Serverless) باستخدام AWS Lambda			
ت	**الخطوات**	**الدرجة القياسية % 50**	**درجة الاداء %50**	**الملاحظات**
1	تسجيل الدخول إلى:AWS Console	%5		
2	فتح خدمة Lambda وإعداد الدالة	%10		
3	كتابة الكود الدالة وحفظها	%10		
4	اختبار الدالة	%5		
5	المناقشة	%10		
6	الزمن المخصص	%10		
المجموع				
اسم الفاحص		**التوقيع**		

اسئلة الفصل الخامس

س1: عرف ما يأتي:

1. الشبكات المعرفة بالبرمجيات (**SDN**)
2. طبقة التحكم:(**Control Plane**)
3. طبقة البيانات:(**Data Plane**)
4. الحوسبة دون خوادم:(**Serverless Computing**)
5. الحوسبة الطرفية:(**Edge Computing**)

س2: املاء الفراغات الآتية:

1. تعتمد الشبكات المعرفة بالبرمجيات على فصل طبقة _____ عن طبقة _____.
2. من التحديات الرئيسية في الحوسبة بدون خوادم هي _____ و _____.
3. يستخدم الذكاء الاصطناعي في تحليل _____ و_____ للكشف عن التهديدات.
4. من بروتوكولات التشفير المستخدمة في **SDN** بين طبقة التحكم والبنية التحتية:
5. تُعد الحوسبة الطرفية مثالية للأنظمة التي تتطلب _____ في معالجة البيانات، مثل السيارات ذاتية القيادة.

س3: ناقش كيف تُسهم الشبكات المعرفة بالبرمجيات (**SDN**) في تحسين أمن الشبكات مقارنة بالشبكات التقليدية.

س4: وضّح دور الذكاء الاصطناعي في الكشف عن التهديدات والاستجابة لها في بيئات الحوسبة السحابية.

س5: قارن بين الحوسبة السحابية دون خوادم (**Serverless**) والحوسبة الطرفية (**Edge Computing**) من حيث :-

1. الأمان
2. زمن الاستجابة
3. التكلفة.

المصادر العربية

1. الحوسبة السحابية: المفاهيم والتطبيقات / تاليف د. مصطفى صادق.
2. الاتجاهات الحديثة في الحوسبة السحابية / تاليف د. محمد زكريا .
3. أمن المعلومات في الحوسبة السحابية / تاليف د. خالد حسن .
4. إدارة البيانات الضخمة في بيئة الحوسبة السحابية / تاليف د. ياسر عبد الله .
5. مقدمة في الحوسبة السحابية / تاليف د. سمير بسيوني .
6. الحوسبة السحابية وإنترنت الأشياء / تاليف د. فاطمة البكري
7. "الحوسبة السحابية: المفاهيم والتطبيقات" / تأليف: د. محمد محمود أبو زيد
8. "أمن المعلومات وحمايتها في بيئة الحوسبة السحابية" / تأليف: د. مصطفى عبد العظيم
9. "مفاهيم الأمن السيبراني وحماية المعلومات" / تأليف: د. عادل الشافعي
10. SDN ببساطة / المؤلف: عادل الحميدي , فؤاد بنعمران
11. حوسبة الحافة والتوائم الرقمية فى ظل شبكات الجيل الخامس والبيئات الذكية / المؤلف : طه محمد أحمد يوسف
12. أمن الشبكات: المفاهيم والتطبيقات / المؤلف: د. عبد الله بن عبد العزيز السعدون
13. أمن المعلومات في العصر الرقمي / المؤلف: د. فهد بن عبد الرحمن الشميري

المصادر الاجنبية

1. Computer Networking: A Top-Down Approach (James F.Kurose & Keith W.Ross) .
2. Thomas Erl, Cloud Computing: Concepts, Technology & Architecture, Published by Prentice Hall, USA, 1st Edition, 2013.
3. Rajkumar Buyya, James Broberg, Andrzej Goscinski, Cloud Computing: Principles and Paradigms, Published by Wiley, USA, 1st Edition, 2011.
4. Arshdeep Bahga, Vijay Madisetti, Cloud Computing: A Hands-On Approach, Published by CreateSpace Independent Publishing, USA, 1st Edition, 2013.
5. Software-Defined Networking and Security: From Theory to Practice (Dijiang Huang, Huijun Wu, and others)
6. SDN: Software Defined Networks (Thomas D. Nadeau , Ken Gray)
7. Secure Edge Computing: Applications, Techniques and Challenges (Mohiuddin Ahmed and Paul Haskell-Dowland)
8. Cloud Computing: Concepts, Technology & Architecture (Thomas Erl)
9. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Tim Mather, Subra Kumaraswamy, Shahed Latif)
10. Cloud Computing Security Issues and Challenges:(A Surve & Bertino)
11. Security Engineering: A Guide to Building Dependable Distributed Systems (Ross Anderson)
12. AWS Certified Security – Specialty Exam Guide (Stuart Scott)

ختامًا، نأمل أن يكون هذا الكتاب قد زوّد الطالب برؤية شاملة وأدوات معرفية تساعده على بناء بيئة شبكية وسحابية أكثر أمانًا واستقرارًا، وأن يكون دافعًا نحو مزيد من التعلم والبحث في هذا المجال الحيوي ..... والله ولي التوفيق

المؤلفون

تم بحمد الله