جمهورية العراق

وزارة التربية

المديرية العامة للتعليم المهني

حماية أنظمة التشغيل

فرع الحاسوب وتقنية المعلومات

اختصاص الأمن السيبراني

الصف الثاني

المؤلفون

د.عمار طعمه نمل

د. مروة مشتاق طالب

م.م. إسراء عادل حيدر

هيثم حمزة عبد

الطبعة الأولى 1447 هـ - 2025 م

المصمم الطباعي

حمزة هادي حرفش

المقدمة

في ظل التطور السريع والمتسارع في مجال تكنولوجيا المعلومات والاتصالات، برزت أهمية الأمن السيبراني كعنصر أساسي في حماية المعلومات والأنظمة الرقمية من التهديدات والهجمات المختلفة. ويُعد أمن أنظمة التشغيل أحد المحاور الجوهرية في منظومة الأمن السيبراني، نظراً للدور الحيوي الذي تؤديه هذه الأنظمة في إدارة موارد الحاسوب وتوفير بيئة تشغيل للبرمجيات والتطبيقات. ونظراً لأن أنظمة التشغيل تمثل الطبقة الأساسية التي تعتمد عليها معظم البنى التحتية الرقمية، فإن استهدافها من قبل الجهات الخبيثة قد يؤدي إلى تهديد سلامة البيانات وتعطيل الخدمات الحيوية. وعليه، فإن حماية أنظمة التشغيل تمثل خطوة أساسية لضمان أمن المعلومات واستمرارية العمل في البيئات التقنية المعاصرة. وانطلاقاً من هذه الأهمية، يهدف هذا الكتاب إلى تزويد طلبة المرحلة الثانية، في تخصص الأمن السيبراني، بالمعارف النظرية والمهارات التطبيقية المتعلقة بآليات حماية أنظمة التشغيل، وفقاً لأحدث الممارسات والتقنيات المعتمدة في هذا المجال.

وفي إطار سعيها الحثيث لمواكبة التطورات المتسارعة في مجال تكنولوجيا المعلومات وأمن البيانات، أولت وزارة التربية العراقية، متمثلة بمديرية التعليم المهني، اهتماماً بالغاً بتحديث المناهج التقنية وتضمينها موضوعات ترتبط ارتباطاً وثيقاً بالأمن السيبراني، بما ينسجم مع متطلبات سوق العمل المحلي والدولي. وقد تم إعداد هذا الكتاب بالتنسيق المشترك بين أساتذة من وزارة التعليم العالي والبحث العلمي العراقية ومديرية التعليم المهني في وزارة التربية العراقية، وبالتعاون مع عدد من الخبراء والمختصين في قطاع أمن المعلومات، وذلك بهدف بناء قاعدة علمية متينة لدى طلبة التعليم المهني، تؤهلهم لفهم التحديات الأمنية والتعامل معها بكفاءة عالية ضمن بيئات العمل الحقيقية.

يتألف هذا الكتاب من عدة فصول تغطي الجوانب المختلفة لحماية أنظمة التشغيل، حيث يقدم الفصل الأول مقدمة عامة حول حماية أنظمة التشغيل و تطور التهديدات الأمنية وبعض الهجمات الشائعة على هذه الأنظمة. بينما يتطرق الفصل الثاني إلى إدارة صلاحيات المستخدمين من ناحية إدارة حسابات المستخدمين، وأنماط التحكم في الوصول، وكيفية تقليل الصلاحيات لتقليل المخاطر، وتحليل سجلات الدخول وتحديد الحسابات غير الآمنة. أمّا الفصل الثالث فيوضح طرق حماية الاتصال في أنظمة التشغيل ، حيث تم التطرق إلى كيفية تأمين الاتصالات في أنظمة التشغيل، وإعداد جدران الحماية لتأمين الاتصالات الواردة والصادرة، وحماية بروتوكولات الاتصال، وتحليل حركة البيانات لفهم الانشطة المشبوهة, اضافة إلى أدوات منع الهجمات المرتبطة بالاتصالات. تناول الفصل الرابع طرق حماية التخزين والبيانات من حيث تقنيات التشفير الحديثة، وحماية البيانات أثناء النقل بأستخدام بروتوكولات آمنة، وإدارة النسخ الاحتياطية واستراتيجيات استعادة البيانات، والتحقق الدوري من سلامة النسخ الاحتياطية، وادوات حذف البيانات بشكل أمن لمنع استعادتها مرة اخرى. أمّا الفصل الخامس فيركز على حماية التطبيقات المثبتة على نظام التشغيل، ومعالجة الثغرات الأمنية، وكشف البرامج الخبيثة وازالتها، ومراقبة إستخدام الموارد لاكتشاف التطبيقات غير المصرح بها، والتحكم في تشغيل التطبيقات بأستخدام قوائم بيضاء وصلاحيات تشغيل. الفصل السادس والاخير سلط الضوء على خطوات الاستجابة للحوادث الأمنية، واهمية مراقبة السجلات وتحليلها، وإعداد خطط طوارئ لاستعادة النظام بعد الهجمات، و منهجيات إختبار النظام بعد إصلاح الثغرات.

نأمل أن يكون هذا الكتاب مرجعاً مفيداً للطلبة، ومصدراً عملياً لفهم كيفية تأمين أنظمة التشغيل، وبدايةً راسخة لمسيرتهم في مجال الأمن السيبراني.

المؤلفون

محتويات الكتاب

الفصل الأول

مقدمة في حماية أنظمة التشغيل

Introduction to Operating System Security

أهداف الفصل الأول

1. التعرف على مفهوم أنظمة التشغيل ودورها الاساسي في الحوسبة.
2. فهم طبيعة التهديدات الأمنية التي تواجه أنظمة التشغيل.
3. الالمام بالمبادئ الأساسية للأمان (السرية، السلامة، المصادقة).
4. التمييز بين أنواع الهجمات الشائعة على أنظمة التشغيل وكيفية التعامل معها.

محتويات الفصل الأول

(1-1) تعريف أنظمة التشغيل وادوارها الأساسية.

(1-2) تطور التهديدات الأمنية لأنظمة التشغيل.

(1-3) المبادئ الأساسية لحماية أنظمة التشغيل (المصادقة، السرية، السلامة).

(1-4) نظرة عامة على الهجمات الشائعة.

(1-5) الفرق بين الأمان الوقائي والتفاعلي.

تمرين (1) إعداد كلمات مرور قوية بأستخدام أداة مثل **KeePass**.

تمرين (2) فحص الشبكات واكتشاف الأجهزة والخدمات الموجودة على الشبكة بأستخدام أداة **Nmap**

تمرين (3) إعداد سياسة مصادقة متعددة العوامل بأستخدام **Goggle Authenticator**.

الفصل الأول

مقدمة في حماية أنظمة التشغيل

Introduction to Operating System Security

تمهيد

لطالما كانت أنظمة التشغيل حجر الأساس في تشغيل الحواسيب وإدارة مواردها، حيث توفر بيئة تشغيل متكاملة للمستخدمين والبرامج. ومع تطور التكنولوجيا، أصبحت أنظمة التشغيل أكثر تعقيدًا وقدرةً على التعامل مع مهام متعددة، لكن هذا التطور صاحبه أيضًا ازدياد في المخاطر الأمنية التي تهدد سلامة البيانات واستقرار الأنظمة. أن حماية أنظمة التشغيل تعدّ من أهم الجوانب في مجال الأمن السيبراني، حيث تهدف إلى ضمان سرية وسلامة وتوافر المعلومات، بالإضافة إلى حماية المستخدمين من الهجمات الإلكترونية المختلفة.

(1-1) تعريف أنظمة التشغيل وادوارها الأساسية

نظام التشغيل **(Operating System - OS)** هو البرنامج الأساسي الذي يدير موارد الجهاز (مثل المعالج، الذاكرة، والأجهزة المتصلة) ويوفر بيئة تشغيل للمستخدم والتطبيقات الأخرى. وبدون نظام التشغيل، لن تتمكن من تشغيل أي برامج ولن تستعمل الجهاز بسهولة.

(1-1-1) أنواع أنظمة التشغيل

تصنف أنظمة التشغيل حسب الأجهزة التي تعمل عليها إلى:

1. **أنظمة تشغيل الحواسيب**: هذه الأنظمة تُستخدم في أجهزة الكمبيوتر المكتبية والمحمولة، ومن أشهرها:

- **Windows (ويندوز):** من أكثر أنظمة التشغيل شيوعًا، تطوره شركة مايكروسوفت. يتميز بواجهة سهلة ودعم واسع للبرامج.
- **macOS (ماك أو إس):** من تطوير شركة أبل، مخصص لأجهزة ماك، ويتميز بالسلاسة والأمان العالي.
- **Linux (لينكس):** نظام مفتوح المصدر، يُستخدم في السيرفرات والأجهزة المتقدمة، ويوفر مرونة كبيرة للمطورين.

2. **أنظمة تشغيل الهواتف الذكية والأجهزة اللوحية:** هذه الأنظمة مصممة للعمل على الأجهزة المحمولة، وتتميز بدعمها للمس وسهولة الاستخدام، ومن أشهرها:

- **Android** (أندرويد): من تطوير جوجل، ويُستخدم في معظم الهواتف الذكية من شركات مثل سامسونج وهواوي.
- **iOS (آي أو إس):** نظام حصري لأجهزة أبل مثل الآيفون والآيباد، ويتميز بأمانه العالي وتكامله مع أجهزة أبل الأخرى.

3. **أنظمة تشغيل الأجهزة الأخرى وتشمل:**

- نظام التشغيل في الأجهزة الذكية مثل التلفزيونات الذكية (مثل **Android TV** و**Tizen**)، والساعات الذكية (مثل **watchOS** و**Wear OS**).
- نظم تشغيل مدمجة (**Embedded OS**) تُستخدم في الأجهزة الإلكترونية مثل السيارات، الكاميرات، وأجهزة التحكم الصناعي.

(2-1-1) وظيفة نظام التشغيل

يقوم نظام التشغيل بعدة وظائف رئيسة، منها:

1- إدارة الموارد: يتحكم في إستخدام المعالج، الذاكرة، والتخزين لتشغيل البرامج بكفاءة.

2- واجهة المستخدم: يتيح للمستخدمين التفاعل مع الجهاز عبر واجهة رسومية أو سطر الأوامر.

3- تشغيل التطبيقات: يسمح بتشغيل البرامج وإدارتها مثل المتصفحات، الألعاب، وبرامج العمل.

4- إدارة الملفات: ينظم الملفات والمجلدات، ويسمح بالتخزين والاسترجاع بسهولة.

5- الأمان والحماية: يوفر الحماية ضد الفيروسات والهجمات الإلكترونية عبر التحديثات وإدارة الأذونات.

6- إدارة الأجهزة المتصلة: يتعرف على الأجهزة مثل الطابعات، الكاميرات، ولوحات المفاتيح ويجعلها تعمل بشكل صحيح.

ولحماية نظام التشغيل بشكل صحيح، يجب أولًا معرفة نوع النظام التشغيلي المستخدم وخصائصه، حيث تختلف طرق الحماية حسب نوع النظام وإمكانياته. على سبيل المثال، أنظمة التشغيل الشائعة مثل **Windows** و**macOS** و**Linux** للحواسيب، و**Android** و**iOS** للهواتف الذكية، تمتلك كل منها إعدادات مختلفة للتحكم في الأمان وحماية البيانات.

1 حماية انظمة التشغيل

(3-1-1) أهمية حماية وأمن نظام التشغيل

حماية نظام التشغيل تنقسم بصورة رئيسة إلى قسمين متكاملين، يمثل كل منهما طبقة أساسية في تأمين النظام ضد التهديدات الإلكترونية:

اولاً: حماية نواة النظام (kernel security)

النواة هي الجزء الأساسي من نظام التشغيل الذي يتحكم في العتاد، ويوفّر الخدمات الرئيسية لبقية أجزاء النظام، مثل إدارة الذاكرة، إدارة المعالج، وعمليات الإدخال والإخراج. تهدف حماية النواة إلى منع الوصول غير المصرح به للموارد، تأمين العمليات الحساسة التي تنفذ بصلاحيات عالية، و كشف ومنع الشيفرات الضارة التي تحاول التسلل إلى النواة (مثل **rootkits**). ومن أهم تقنيات حماية النواة:

1. عزل الذاكرة (**Memory Isolation**): وهو فصل فضاء المستخدم عن فضاء النواة لمنع البرمجيات من التلاعب بمكونات حساسة.
2. التحقق من التوقيع الرقمي للسواقات (**Drivers Signing**): أي منع تحميل مشغلات غير موثوقة إلى النواة.
3. وحدات الحماية النمطية (**Kernel Module Signing**): والتي تمنع تحميل وحدات نواة غير مصدقة.
4. آليات كشف البرمجيات الخبيثة في النواة: والتي تُطبق سياسات صارمة للتحكم بالوصول.
5. تقنية (**KASLR**) لتُغييّر مواقع بيانات النواة في الذاكرة بشكل عشوائي لمنع الاستغلال.

ثانيًا: حماية فضاء المستخدم (User-Space Security)

فضاء المستخدم هو الجزء الذي يتفاعل معه المستخدم مباشرة مثل واجهات التطبيقات والبرامج والمستعرضات. وبما أن المستخدم العادي لا يمكنه الوصول إلى النواة، فإن أكثر التهديدات تبدأ من هنا. تهدف حماية فضاء المستخدم إلى منع البرامج الضارة من العمل أو الوصول إلى البيانات الحساسة، حماية المستخدم من التصرفات الخاطئة أو الهندسة الاجتماعية، تأمين التفاعل بين التطبيقات ونظام التشغيل. من أهم تقنيات حماية فضاء المستخدم:

1. برامج مكافحة الفيروسات (**Antivirus Software**): التي تفحص الملفات والبرامج بحثًا عن البرمجيات الضارة.
2. جدران الحماية (**Firewalls**): وظيفتها تنظيم حركة المرور من وإلى الجهاز لمنع الهجمات الشبكية.
3. التحكم في التطبيقات (**Application Control**): للتحكم في ما يُسمح بتشغيله مثل **AppLocker** أو **Windows Defender Application Control**.

4. تقنيات التحديث التلقائي: وهذه بدورها تسد الثغرات فورًا عند اكتشافها.
5. التحكم في الامتيازات (**Least Privilege Principle**): وتعني منع البرامج والمستخدمين من العمل بصلاحيات أعلى مما يحتاجونه.
6. أنظمة كشف التسلل (**IDS**) ومنع التسلل (**IPS**): نظام كشف التسلل (**Intrusion Detection System**) هو برنامج أو جهاز يراقب الأنشطة في الشبكة أو النظام بحثًا عن سلوكيات مشبوهة أو محاولات اختراق، ويقوم بتنبيه المسؤولين عند اكتشاف شيء غير طبيعي. وقد برز حديثا تقنيات وانظمة كشف التسلل المعتمدة على الذكاء الاصطناعي (**AI-Based IDS**) والتي هي نوع من أنظمة **IDS** يستخدم تقنيات الذكاء الاصطناعي (**AI**) والتعلم الآلي (**Machine Learning**) لتحليل الأنشطة والتعرف على الهجمات الأمنية، حتى تلك التي لم يتم تحديدها من قبل (**Zero-day attacks**).

عزيزي الطالب، نستنتج في النهاية انه من دون حماية النواة، يمكن لأي تهديد صغير في فضاء المستخدم أن يتسلل ويضر النظام بالكامل. ومن دون تأمين فضاء المستخدم، فإن أي تطبيق غير موثوق قد يستغل النواة إذا اكتُشفت فيها ثغرة. لذلك فالتكامل بين الحمايتين ضروري لضمان سريّة البيانات، سلامة العمليات، وتوفر الخدمات.

(2-1) تطور التهديدات الامنية لأنظمة التشغيل

شهدت التهديدات الأمنية لأنظمة التشغيل تطورًا ملحوظًا على مر العقود، نتيجة التوسع الكبير في إستخدام أنظمة الحاسوب، تزايد الاعتماد على الإنترنت، وتغير طبيعة الهجمات الإلكترونية. عزيزي الطالب، لأهمية هذا الموضوع سيتم تناوله بتفصيل اكبر في الفقرات اللاحقة.

(1-2-1) الثغرات الأمنية العشرة الأكثر شيوعًا في مجال أمن المعلومات

في عالم اليوم، نعتمد بشكل متزايد على تطبيقات الإنترنت في الدراسة والعمل والتواصل، وهذا يفرض علينا مسؤولية حماية هذه التطبيقات من الهجمات السيبرانية. ولهذا، حددت منظمة **OWASP** (مشروع أمن التطبيقات المفتوحة المصدر) قائمة بأكثر 10 ثغرات أمنية شيوعًا، بهدف زيادة الوعي وتوجيه المطورين ومختبري الأمن لتحسين جودة البرمجيات. وهذه القائمة تحدث كل عدة سنوات اعتمادا على تطور نوع الهجمات وظهور أنواع جديدة منها. فيما يأتي قائمة بالثغرات الأمنية العشرة الأكثر شيوعًا – **OWASP Top 10** (إصدار 2021):

1. التحكم غير الصحيح بالهوية والوصول (**Broken Access Control**): يعني أن المستخدمين يستطيعون الوصول إلى بيانات أو وظائف غير مصرح لهم بها. مثلا طالب يستطيع الوصول إلى درجات زميله في النظام الدراسي.

2. فشل التشفير (**Cryptographic Failures**): يحدث عندما لا يتم إستخدام التشفير بشكل صحيح، مما يعرّض البيانات الحساسة للسرقة. مثلاً إرسال كلمات المرور عبر الإنترنت بدون تشفير (**HTTP** بدلاً من **HTTPS**).

3. حقن الأوامر (**Injection**): وهو من أخطر الثغرات، وتحدث عند إدخال أوامر ضارة في مدخلات التطبيق. مثلا هجمات **SQL Injection** التي تُمكّن المهاجم من التلاعب بقاعدة البيانات.

4. التصميم غير الآمن (**Insecure Design**): والذي يشير إلى وجود عيوب في تصميم النظام الأمني للتطبيق من البداية. مثل تطبيق يسمح بتغيير كلمات السر بدون تأكيد الهوية.

5. إعدادات خاطئة للامان (**Security Misconfiguration**): يشمل أي خطأ في إعداد الخوادم أو البرمجيات مما يجعل النظام عرضة للهجمات. مثل إستخدام الإعدادات الافتراضية للحسابات الإدارية.

6. المكونات الضعيفة والمعرضة للخطر (**Vulnerable and Outdated Components**): وهي إستخدام مكتبات أو إضافات قديمة تحتوي على ثغرات معروفة. مثل إستخدام نسخة قديمة من **JavaScript** بها ثغرة أمنية.

7. فشل في تحديد الهوية والمصادقة (**Identification and Authentication Failures**): والذي يشير إلى سوء إدارة الجلسات وكلمات المرور والتحقق من الهوية. مثل السماح بعدد غير محدود من محاولات تسجيل الدخول.

8. فشل في سلامة البرمجيات والبيانات (**Software and Data Integrity Failures**):

وتعني ضعف في التحقق من موثوقية التحديثات أو الأكواد التي يتم تشغيلها. مثل تثبيت تحديثات من مصدر غير موثوق.

9. فشل في تسجيل ومراقبة الأنشطة الأمنية (**Security Logging and Monitoring Failures):** وتشير إلى عدم وجود أنظمة تراقب وتحذر من الهجمات المحتملة. مثل عدم وجود سجل لتسجيل محاولات الدخول غير المصرح بها.

10. تزوير طلبات الخادم (**Server-Side Request Forgery - SSRF**)

وتحدث عندما يُجبر الخادم على إرسال طلبات داخلية إلى أنظمة أخرى بدون التحقق. مثلاً المهاجم يستخدم تطبيقًا لإرسال طلبات إلى شبكة داخلية لا يُسمح له بالوصول إليها.

(1-2-2) المراحل الزمنية لتطور التهديدات الأمنية

يمكن تتبع وفهم التطور في الهجمات الأمنية على أنظمة المعلومات من خلال تقسيمه على مراحل زمنية رئيسة، مع توضيح خصائص وأساليب التهديد في كل مرحلة:

1 حماية انظمة التشغيل

أ.المرحلة الأولى: التهديدات التقليدية (السبعينيات – التسعينيات)

في البدايات، كانت أنظمة التشغيل تعمل غالبًا في بيئات مغلقة ومعزولة عن الشبكات العامة، وكان الوصول إلى النظام يتطلب تواجدًا ماديًا. خلال هذه المدة، ركزت التهديدات على ما يأتي:

- الهجمات الفيزيائية :كالدخول غير المصرح به إلى الجهاز.
- الفيروسات البسيطة :التي كانت تنتشر عبر الأقراص المرنة وتستهدف ملفات نظام التشغيل أو البيانات.
- الهندسة الاجتماعية :للحصول على كلمات المرور.

كانت هذه التهديدات محدودة النطاق والتأثير، لكنها وضعت الأساس لفهم أهمية الأمان.

ب. المرحلة الثانية: ظهور البرمجيات الخبيثة (أواخر التسعينيات – منتصف الألفينيات)

مع التوسع الشبكي واستخدام الإنترنت، بدأت التهديدات تأخذ شكلاً أكثر تعقيدًا وانتشارًا. وبرزت:

- الدودة :(**Worms**) مثل **Code Red** و**Blaster**، التي تستغل ثغرات في النظام وتنتشر ذاتيًا عبر الشبكات.
- حصان طروادة :(**Trojans**) الذي يختبئ داخل برامج تبدو مشروعة، ويمنح المهاجمين تحكمًا عن بُعد.
- البرمجيات الجاسوسية :(**Spyware**) التي تجمع بيانات المستخدم دون علمه.
- الاستغلال الآلي للثغرات.(**Exploit Kits**)

في هذه المرحلة، أصبح أمان أنظمة التشغيل يعتمد بشكل أساسي على التحديثات الأمنية وبرامج مكافحة الفيروسات.

ت.المرحلة الثالثة: الهجمات المتقدمة والموجهة (من 2010 فصاعداً)

في العقد الأخير، تطورت التهديدات لتصبح أكثر احترافية وتنظيمًا، خاصة مع دخول الفاعلين المدعومين من دول .(**APT – Advanced Persistent Threats**) من بين هذه التهديدات:

- البرمجيات الخبيثة المعقدة والتي استهدفت أنظمة صناعية عن طريق استغلال ثغرات متعددة مثل (**Stuxnet**) .
- هجمات الفدية :(**Ransomware**) مثل **WannaCry** ، والتي تشفّر البيانات وتطلب فدية مقابل فك التشفير.
- الهجمات عبر سلاسل التوريد :(**Supply Chain Attacks**) والتي تستهدف برامج موثوقة أثناء عملية تطويرها.

- الاستغلال عبر الشبكات اللاسلكية أو الأجهزة الذكية (**IoT**).
- استهداف البنية التحتية للثقة (مثل الشهادات الرقمية وDNS).

تتطلب هذه المرحلة حلولًا متقدمة مثل نظم كشف التسلل(**IDS/IPS**) ، والتحليل السلوكي، وتطبيق سياسات "عدم الثقة الافتراضية.(**Zero Trust**) "

ث.المرحلة الرابعة: التهديدات المستقبلية (2020 فصاعدًا)

مع التوسع في إستخدام الذكاء الاصطناعي، والحوسبة السحابية، والأنظمة الموزعة، ظهرت تهديدات جديدة تشمل:

- البرمجيات الخبيثة المدعومة بالذكاء الاصطناعي.
- الهجمات على نماذج الذكاء الاصطناعي نفسها مثل **Poisoning وEvasion**).
- اختراقات البنى التحتية السحابية والخوادم الافتراضية.
- الهجمات على البيانات الضخمة وسلاسل الكتل(**Blockchain**) .

(3-1) المبادئ الأساسية لحماية أنظمة التشغيل

تُعد حماية أنظمة التشغيل إحدى الركائز الأساسية لضمان أمن المعلومات وسلامة تشغيل الأنظمة الحاسوبية. وتقوم هذه الحماية على مجموعة من المبادئ الأمنية التي تضمن منع الوصول غير المصرح به، والحفاظ على خصوصية البيانات، وضمان سلامة المعالجة والتخزين. ومن بين هذه المبادئ، تبرز ثلاثة مفاهيم رئيسة تُستخدم كأساس لتصميم وتنفيذ الأنظمة الأمنية، وهي: المصادقة (**Authentication**) ، والسرية (**Confidentiality**) ، والسلامة (**Integrity**) .

أ- المصادقة (Authentication)

تشير المصادقة إلى عملية التحقق من هوية المستخدم أو الجهة التي تحاول الوصول إلى النظام. تهدف هذه العملية إلى التأكد من أن الشخص أو الجهاز هو فعلاً ما يدّعيه، قبل منحه صلاحية الوصول إلى الموارد. يتم ذلك بأستخدام مجموعة من الوسائل، منها:

- كلمات المرور (**Passwords**): وهي أكثر وسائل المصادقة شيوعاً، لكنها عرضة للاختراق إذا لم تُستخدم بطريقة آمنة.
- البطاقات الذكية أو الرموز الأمنية (**Smart Cards / Tokens**).
- القياسات الحيوية (**Biometrics**): مثل بصمة الإصبع أو التعرف على الوجه.

- المصادقة متعددة العوامل (**MFA**): وهي طريقة تعتمد على أكثر من عامل للتحقق، مثل كلمة مرور بالإضافة إلى رمز يُرسل إلى الهاتف.

توفر المصادقة حماية أساسية للنظام من محاولات الدخول غير المصرح به، وتشكل الخطوة الأولى في بناء نظام أمن.

ب- السرية (Confidentiality)

تعني السرية الحفاظ على خصوصية المعلومات ومنع كشفها أو الاطلاع عليها من قبل أشخاص غير مخولين. في سياق أنظمة التشغيل، تشمل السرية حماية الملفات، قواعد البيانات، وسجلات النظام من التسريب أو التجسس. من وسائل تحقيق السرية:

- تشفير البيانات (**Encryption**): سواء أثناء نقل البيانات عبر الشبكة أو أثناء تخزينها.
- سياسات التحكم بالوصول (**Access Control**) :التي تضمن أن المستخدمين يمتلكون فقط الصلاحيات اللازمة لأداء مهامهم، دون الوصول إلى معلومات لا تخصهم.
- إدارة الصلاحيات والملفات بأستخدام نظام الأذونات (**Permissions**) الذي يُحدد من يستطيع قراءة أو تعديل الملفات.

السرية ضرورية بشكل خاص عند التعامل مع معلومات حساسة، مثل البيانات الشخصية أو السجلات المالية.

ت- السلامة (Integrity)

تشير السلامة إلى ضمان أن البيانات أو النظام لم تتعرض للتعديل أو التلاعب بشكل غير مصرح به، سواء عن قصد أو عن طريق الخطأ. الهدف من هذا المبدأ هو التأكد من أن المعلومات تحتفظ بصحتها ودقتها طوال دورة حياتها. وتتحقق السلامة من خلال:

- إستخدام التواقيع الرقمية (**Digital Signatures**) : للتحقق من أن المحتوى لم يتغير منذ إنشائه.
- إستخدام التجزئة (**Hashing**) : للتحقق من تطابق القيم والتحذير من أي تغيير طفيف.
- السجلات ومراقبة الأحداث :(**Logs & Auditing**) لتوثيق العمليات التي تحدث داخل النظام، مما يساعد في اكتشاف التعديلات غير المصرح بها.

السلامة ضرورية للحفاظ على الثقة بالنظام ولتجنّب نتائج خطيرة قد تترتب على بيانات خاطئة أو ملوّثة .أن المصادقة، والسرية، والسلامة ليست مجرد مفاهيم نظرية، بل هي أساسيات عملية يجب أن يُتقنها كل من يعمل أو يدرس في مجال الأمن السيبراني. وتطبيق هذه المبادئ في حماية أنظمة

1 حماية انظمة التشغيل

التشغيل يُسهم في إنشاء بيئة رقمية آمنة وموثوقة، ويُمكّن المؤسسات من التصدي للمخاطر السيبرانية المتزايدة.

(4-1) نظرة عامة إلى الهجمات الشائعة

تتعدد التهديدات الأمنية التي تستهدف أنظمة التشغيل، ولكل نوع منها آلية عمل خاصة وتأثير مختلف. لفهم هذه التهديدات بشكل أوضح، سنقدم أمثلة عملية عن كل نوع، مع توضيح كيفية تطورها وطرق التعامل معها.

1. البرمجيات الخبيثة (Malware): هي برامج مصممة للتسلل إلى الأنظمة التشغيلية دون إذن المستخدم، بهدف سرقة البيانات أو التسبب في أضرار. تشمل الفيروسات، والديدان، وأحصنة طروادة، وبرامج الفدية.

كيفية تطورها

- في البداية، كانت الفيروسات تنتقل عبر الأقراص المرنة وتحتاج إلى تفاعل المستخدم.
- مع ظهور الإنترنت، تطورت الديدان لنشر نفسها تلقائيًا عبر الشبكات.
- حاليًا، تعتمد البرمجيات الخبيثة على تقنيات الذكاء الاصطناعي والتشفير لتجنب الكشف.

كيفية التعامل معها

- إستخدام برامج مكافحة الفيروسات المحدثة باستمرار.
- تجنب تنزيل البرامج والملفات من مصادر غير موثوقة.
- تحديث نظام التشغيل بشكل دوري لسد الثغرات الأمنية.

مثال على ذلك هو فيروس **Trojan FakeAV:** يقوم هذا الفيروس بمحاكاة برنامج مضاد للفيروسات "مزيف"، حيث يظهر للمستخدم أنه برنامج مكافحة فيروسات يتطلب التثبيت على جهازه، وبعد تحميل البرنامج، يعرض رسائل مزيفة تدعي أن الجهاز مصاب بالفيروسات ويطلب من المستخدم شراء نسخة "مدفوعة" لتنظيف الجهاز. في الواقع لا يقوم البرنامج بأي عمليات تنظيف بل يسرق معلومات المستخدم مثل كلمات المرور أو البيانات المالية، لاحظ الشكل (1-1). ينتشر هذا الفيروس من خلال تحميله عبر روابط مشبوهة أو مرفقات في رسائل البريد الإلكتروني، وقد يظهر كمحاكي برنامج موثوق أو كإشعار تحذيري مزيف وعند تثبيته، يتم تنشيط الفيروس على الجهاز ويبدأ في تنفيذ مهام ضارة.

1 حماية انظمة التشغيل

الشكل (1-1) نظام تشغيلي مصاب بفيروس Trojan FakeAV

أمّا كيفية التعامل مع فيروس Trojan FakeAV فهي:

- إستخدام برامج مكافحة الفيروسات: يجب تثبيت برنامج مكافحة فيروسات موثوق ومحدث باستمرار لاكتشاف وإزالة البرمجيات الخبيثة.
- تجنب تحميل البرامج من مصادر غير موثوقة: تجنب النقر على الروابط أو المرفقات المجهولة في الرسائل الإلكترونية أو المواقع المشبوهة.
- التحديثات المستمرة: تأكد من تحديث النظام والبرامج بشكل دوري لسد الثغرات التي قد يستغلها الفيروس.

2. هجمات التصيد الاحتيالي (Phishing Attacks): هي محاولات احتيالية لخداع المستخدمين عبر رسائل بريد إلكتروني أو مواقع مزيفة، بهدف سرقة بيانات تسجيل الدخول أو المعلومات المالية.

كيفية تطورها:

- بدأت برسائل بريد إلكتروني تحتوي على روابط ضارة.
- تطورت لتشمل رسائل مزيفة تحمل شعارات جهات رسمية (البنوك، الشركات الكبرى).
- اليوم، يتم إستخدام الذكاء الاصطناعي لإنشاء هجمات تصيد موجهة (**Spear Phishing**).

كيفية التعامل معها:

- تجنب النقر على الروابط المشبوهة في الرسائل الإلكترونية.

- التحقق من هوية المرسل وعنوان البريد الإلكتروني قبل إدخال أي معلومات.
- تفعيل المصادقة الثنائية (2FA) لحماية الحسابات.

ويقصد بالمصادقة الثنائية (Two-Factor Authentication - 2FA): هي طبقة أمان إضافية لحماية الحسابات عبر الإنترنت. تعني أنه بعد إدخال كلمة المرور، يجب تقديم خطوة تحقق ثانية، مثل:

- رمز يُرسل إلى هاتفك عبر رسالة نصية أو تطبيق المصادقة، لاحظ الشكل (1-2).
- بصمة الإصبع أو التعرف على الوجه
- مفتاح أمان مادي

تهدف المصادقة الثنائية إلى منع الوصول غير المصرح به حتى لو تم اختراق كلمة المرور.

شكل (1-2) المصادقة الثنائية عبر الهاتف المحمول

مثال: احتيال بنك PayPal المزيف: يُرسل بريد إلكتروني يبدو وكأنه من **PayPal**، يطلب من المستخدم تسجيل الدخول عبر رابط مزيف لسرقة بيانات الحساب.

التطور: انتقلت من رسائل بريد إلكتروني بسيطة إلى مواقع مزيفة متطورة تستخدم بروتوكولات **HTTPS** لجعلها تبدو شرعية.

كيفية التعامل: التحقق من عنوان البريد المرسل، تجنب النقر على الروابط المشبوهة، وتفعيل المصادقة الثنائية.

3. هجمات حجب الخدمة الموزعة (DDoS Attacks): تستهدف هذه الهجمات إغراق خادم أو موقع إلكتروني بعدد هائل من الطلبات، مما يؤدي إلى تعطيله.

كيفية تطورها:

- في الماضي، كانت الهجمات تعتمد على عدد محدود من الأجهزة المصابة.

- تطورت مع ظهور "البوت نت" (**Botnets**)، وهي شبكات ضخمة من الأجهزة المخترقة.
- الآن، يتم إستخدام أجهزة إنترنت الأشياء (**IoT**) لشن هجمات أكثر تعقيدًا.

كيفية التعامل معها:

- إستخدام خدمات الحماية السحابية لمواجهة هجمات **DDoS**.
- تفعيل جدران نارية متقدمة وأنظمة كشف التسلل (**IDS**).
- تقليل معدل الطلبات على الخوادم لمنع التدفق غير الطبيعي للبيانات.

مثال هجوم على شركة GitHub (2018م): تم إغراق خوادم GitHub بـ 1.3 تيرابت من البيانات في الثانية، مما أدى إلى تعطل الموقع مؤقتًا، في الماضي، كانت الهجمات تتم بواسطة عدد محدود من الأجهزة، لكنها اليوم تعتمد على "البوت نت" مثل **Mirai** الذي يستغل أجهزة إنترنت الأشياء.

كيفية التعامل: إستخدام مزودي خدمة الحماية ضد **DDoS**، ضبط جدران الحماية، ومراقبة الشبكة لاكتشاف أي نشاط غير طبيعي.

4. استغلال ثغرات مجهولة في النظام التشغيلي (يوم الصفر) (Zero-Day Exploits): يحدث عندما يستغل المهاجمون ثغرات أمنية غير معروفة في البرمجيات قبل أن يتم اكتشافها وإصلاحها من قبل الشركات المطورة وفي البداية، كانت هذه الهجمات نادرة وعشوائية ومع الوقت، أصبح هناك سوق سري لبيع الثغرات الأمنية للمهاجمين، حاليًا تستغل مجموعات الهاكرز المتقدمة والحكومات هذه الثغرات في الهجمات السيبرانية.

كيفية التعامل معها

- تحديث الأنظمة والتطبيقات فور صدور تصحيحات الأمان.
- إستخدام برامج أمان متقدمة تراقب السلوكيات غير العادية.
- تطبيق سياسة "الحد من الامتيازات" لتقليل فرص استغلال الثغرات.

مثال: ثغرة EternalBlue (2017م): استُخدمت هذه الثغرة في **Windows** من قبل مجموعة قرصنة لاستهداف أنظمة لم يتم تحديثها، وساهمت في انتشار **WannaCry**.

التطور: كانت الثغرات تُكتشف بالصدفة، أمّا اليوم فهناك سوق سوداء يتم فيها بيع الثغرات للحكومات والمجرمين الإلكترونيين.

كيفية التعامل: تثبيت التحديثات الأمنية فور صدورها، إستخدام برامج كشف الثغرات، وتقليل الصلاحيات الإدارية على الأجهزة.

5. الهندسة الاجتماعية (Social Engineering): هي تقنيات نفسية يستخدمها المهاجمون لخداع الأفراد ودفعهم للكشف عن معلومات حساسة، مثل كلمات المرور أو البيانات المالية، في البداية كانت تعتمد على المكالمات الهاتفية أو البريد التقليدي ومع انتشار الإنترنت، أصبحت تشمل رسائل البريد الإلكتروني الاحتيالية والمواقع المزيفة واليوم يتم إستخدام تقنيات متطورة مثل تقليد الصوت والذكاء الاصطناعي لزيادة فعالية الهجمات.

كيفية التعامل معها:

- توعية المستخدمين بأساليب الاحتيال الشائعة.
- عدم مشاركة المعلومات الشخصية أو كلمات المرور مع أي جهة غير موثوقة.
- التحقق من هوية أي شخص يطلب معلومات حساسة قبل الاستجابة.

مثال هجوم "مدير الشركة المزيف" (CEO Fraud): يتلقى موظف في قسم المالية بريدًا إلكترونياً يبدو أنه من المدير التنفيذي، يطلب تحويل مبلغ مالي لحساب معين، في الماضي كانت الهجمات بسيطة، أمّا الآن فتستخدم تقنيات الذكاء الاصطناعي لتقليد أسلوب الكتابة أو حتى الصوت.

كيفية التعامل: تدريب الموظفين على التحقق من الطلبات الحساسة، إستخدام بروتوكولات أمان إضافية مثل التحقق المزدوج.

6. برامج الفدية (Ransomware): هي نوع من البرمجيات الخبيثة التي تقوم بتشفير ملفات الضحية، ثم تطلب فدية مالية لفك التشفير، في البداية، كانت تستهدف الأفراد وتطلب مبالغ صغيرة، لاحقًا تطورت لاستهداف الشركات والمنظمات الكبرى بمبالغ ضخمة واليوم، أصبحت أكثر تعقيدًا، حيث تستخدم تقنيات متقدمة لمنع اكتشافها.

كيفية التعامل معها

- الاحتفاظ بنسخ إحتياطية مشفرة في أماكن منفصلة.
- تجنب دفع الفدية، لأن ذلك يشجع المهاجمين على تكرار الهجمات.
- إستخدام أنظمة كشف التهديدات المتقدمة والاستجابة السريعة (**XDR**).

مثال1: فيروس WannaCry:هذا الفيروس **WannaCry** استغل ثغرة أمنية في نظام **Windows** تُعرف باسم **EternalBlue**، والتي تحمل رقم التعريف **CVE-2017-0144** لنشر نفسه وتشفير ملفات الضحايا، مطالبًا بفدية لفك التشفير كما موضح بالشكل (1-3)، بدأ كفيروسات تصيب الملفات فقط، ثم تطورت إلى برمجيات أكثر تعقيدًا مثل الفدية التي تستهدف المؤسسات والبنى التحتية.

ويتم التعامل معه بتحديث النظام باستمرار، تثبيت مضاد فيروسات قوي، وتجنب فتح مرفقات البريد الإلكتروني غير الموثوقة.

شكل (1-3) صورة لفيروس WannaCry

مثال2: هجوم Ryuk على مستشفيات أمريكية (2020م): أصاب هذا الفيروس مستشفيات، مشفرًا بيانات المرضى، مما اضطر المؤسسات لدفع فدية لاستعادة الملفات، في السابق كانت الهجمات فردية، لكنها الآن أصبحت موجهة ضد الشركات والبنى التحتية الحرجة لتحقيق أرباح أكبر.

كيفية التعامل: النسخ الاحتياطي الدوري، إستخدام حلول أمان متقدمة، وتجنب دفع الفدية لتجنب دعم المهاجمين.

واليوم تتطور التهديدات الأمنية لأنظمة التشغيل بشكل مستمر، مما يستدعي اتباع استراتيجيات دفاعية قوية لحماية البيانات والأنظمة. يعتمد الأمان السيبراني على التحديث المستمر، الوعي الأمني، واستخدام تقنيات الحماية الحديثة للحد من المخاطر والتعامل مع التهديدات بفعالية.

(1-5) الامن الوقائي والامن التفاعلي

مع تزايد الهجمات السيبرانية وتعقيدها، أصبح من الضروري اعتماد استراتيجيات شاملة لحماية الأنظمة والبيانات. يعتمد الأمن السيبراني على نهجين رئيسيين: الأمن الوقائي، الذي يهدف إلى منع التهديدات قبل وقوعها، والأمن التفاعلي، الذي يركز على الاستجابة للهجمات والتخفيف من آثارها بعد حدوثها. فهم الفرق بين هذين النهجين يساعد على بناء بيئة سيبرانية أكثر أمانًا.

الأمن الوقائي (**Preventive Security**) هو مجموعة من الإجراءات والتدابير المصممة لمنع التهديدات والهجمات السيبرانية قبل حدوثها و يعتمد على تقنيات مثل:

- الجدران النارية (**Firewalls**) لمنع الوصول غير المصرح به.
- التشفير (**Encryption**) لحماية البيانات أثناء النقل والتخزين.
- المصادقة متعددة العوامل (**MFA**) لتعزيز أمان تسجيل الدخول.

- التحديثات الأمنية (**Security Patches**) لسد الثغرات في الأنظمة.
- التوعية الأمنية (**Security Awareness**) لتقليل الأخطاء البشرية.

الأمن التفاعلي (**Reactive Security**) هو نهج يركز على التعامل مع التهديدات بعد وقوعها، من خلال اكتشافها والاستجابة لها والحد من أضرارها. يعتمد على أدوات واستراتيجيات سوف يتم التطرق اليها في الفصول المقبلة مثل:

- أنظمة كشف التسلل (**IDS**) والاستجابة (**IPS**) لرصد النشاطات المشبوهة.
- إدارة الأحداث الأمنية (**SIEM**) لتحليل الهجمات والاستجابة لها.
- التحليل الجنائي الرقمي (**Digital Forensics**) لتحديد أسباب الهجمات ومنع تكرارها.
- خطط الاستجابة للحوادث (**Incident Response Plans**) لمعالجة الاختراقات بسرعة.
- استراتيجيات التعافي من الكوارث (**Disaster Recovery**) لاستعادة الأنظمة والبيانات بعد الهجمات.

ولا يمكن الاعتماد على أحد النهجين فقط، بل يجب الدمج بينهما لتحقيق حماية سيبرانية فعالة. فالأمن الوقائي يقلل من فرص الهجمات، بينما يضمن الأمن التفاعلي الاستجابة السريعة وتقليل الأضرار عند وقوع الحوادث. الجمع بينهما يخلق استراتيجية متكاملة تحمي المؤسسات من المخاطر السيبرانية بشكل شامل. يوضح جدول (1-1) أوجه الاختلاف بين الأمن الوقائي والتفاعلي.

جدول (1-1) أوجه الاختلاف بين الأمن الوقائي والتفاعلي

الخصائص	الأمن التفاعلي	الأمن الوقائي
الاستراتيجية	استجابية: تهدف إلى تقليل الاضرار بعد وقوع الهجمات.	استباقية: تهدف إلى تقليل المخاطر قبل حدوثها.
الكفاءة	يقلل الاضرار، لكنه لا يمنع وقوع الهجوم من الاساس.	يمنع التهديدات، لكنه لا يضمن حماية كاملة.
التحديات	قد يكون بطيئاً في الاستجابة للهجمات المتقدمة. قد يكون مكلفاً إذا لم يكن هناك خطة استجابة جيدة.	صعوبة توقع جميع أنواع الهجمات المستقبلية. الحاجة إلى استثمارات كبيرة في التكنولوجيا والتدريب.
أمثلة على الادوات	أنظمة إدارة الحوادث الأمنية وتقنيات التحليل الجنائي الرقمي.	برامج مكافحة الفايروسات وجدران الحماية وتقنيات التشفير.
المرونة	أكثر قدرة على التكيف مع التهديدات الجديدة والمفاجئة.	أقل مرونة في التعامل مع التهديدات غير المعروفة.
الاعتماد على الذكاء الصناعي	يعتمد على الذكاء الاصطناعي في التحليل السريع للاحداث بعد وقوعها.	يستخدم الذكاء الاصطناعي لاكتشاف التهديدات المحتملة وتحليل الأنماط.

1 حماية انظمة التشغيل

رقم التمرين: 1 الزمن المخصص: ساعة واحدة

اسم التمرين: اعداد كلمات مرور قوية باستخدام أداة مثل **KeePass**

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

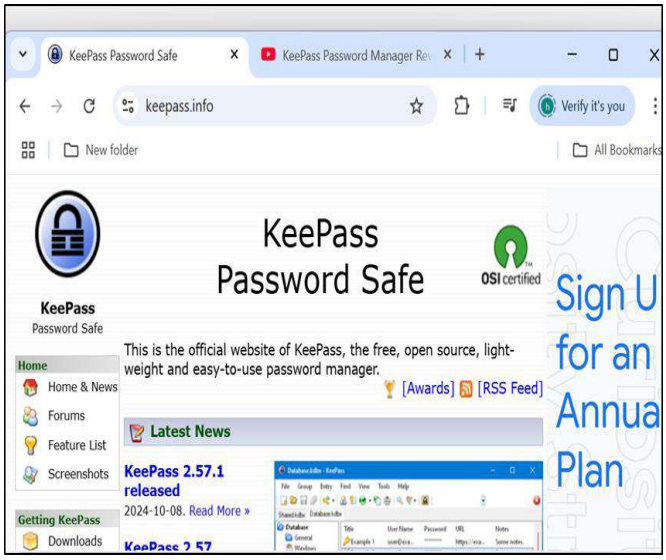
بعد إتمام هذا التمرين، سيتمكن الطالب من:

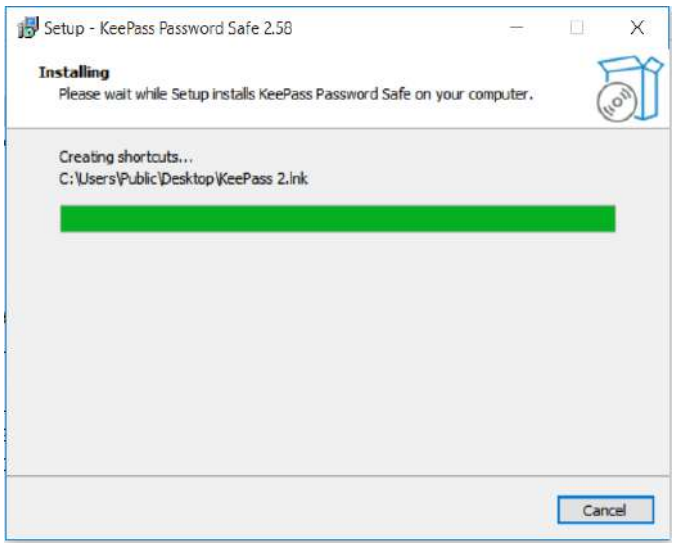
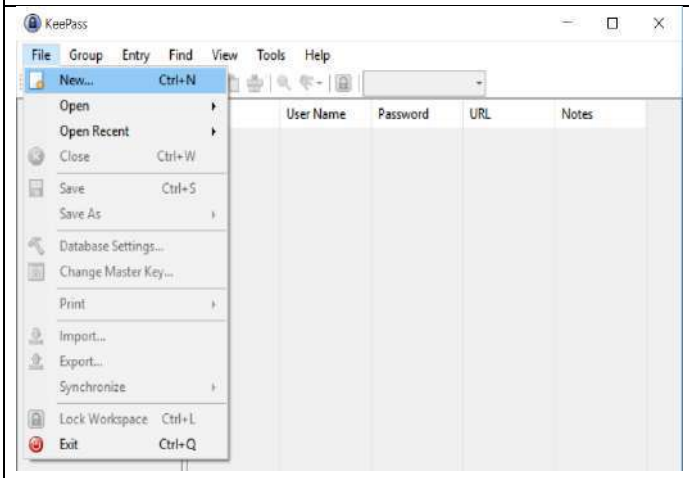
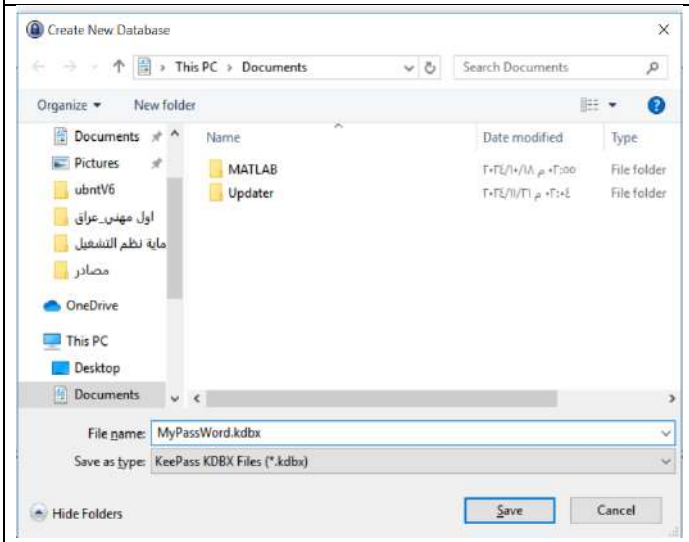
- التعرف على أهمية إدارة كلمات المرور.
- تدريب الطلبة على استخدام برنامج **KeePass** لإنشاء قاعدة بيانات آمنة لتخزين كلمات المرور.
- تطبيق مبادئ :المصادقة، السرية، والسلامة عملياً.

ثانياً: التسهيلات التعليمية

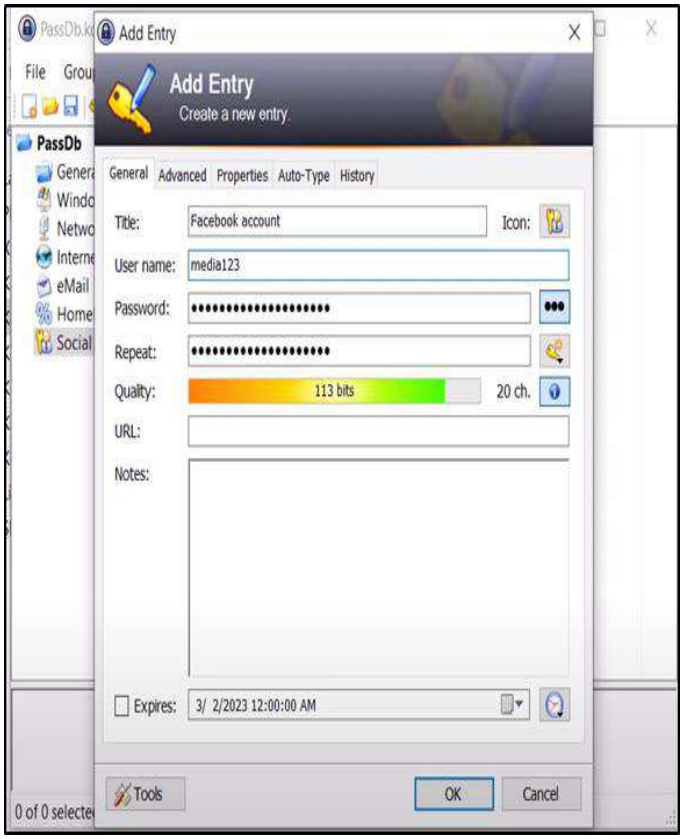
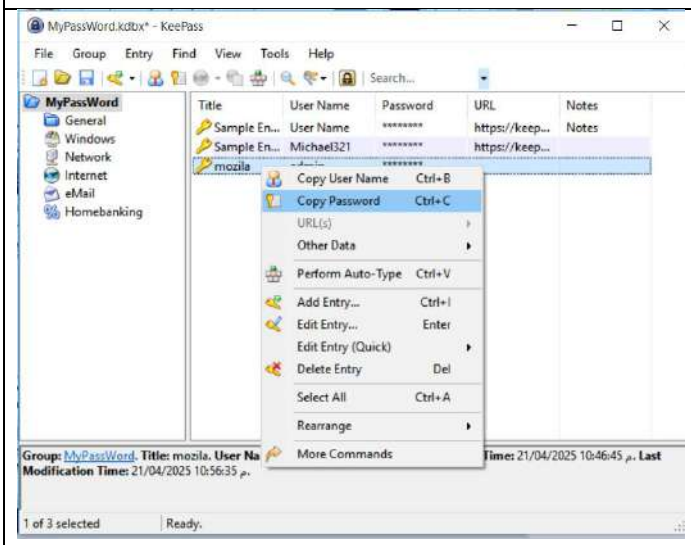
- أجهزة حاسوب مع نظام تشغيل **Windows**.
- برنامج **KeePass** .

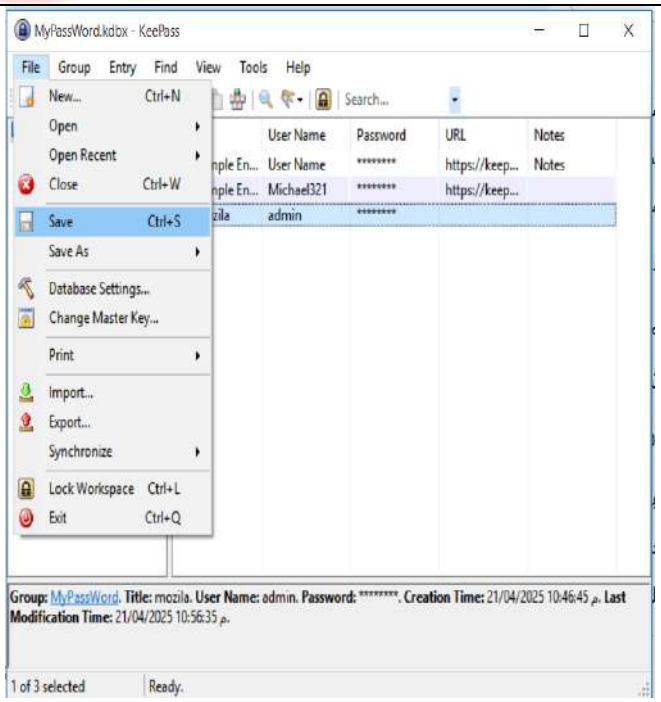
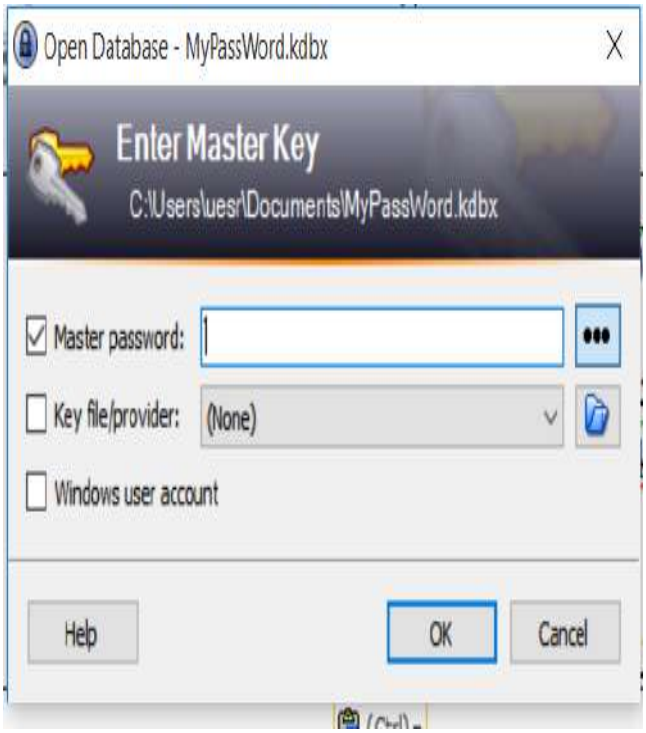
ثالثاً: خطوات تنفيذ التمرين:

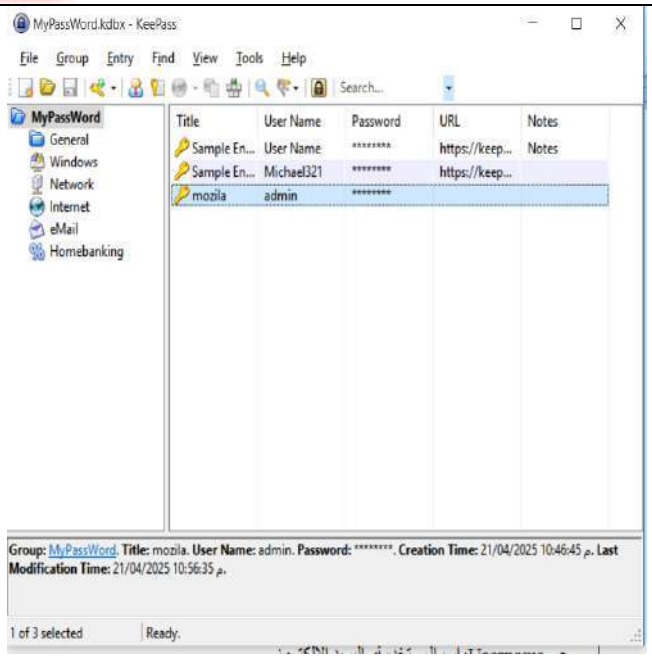
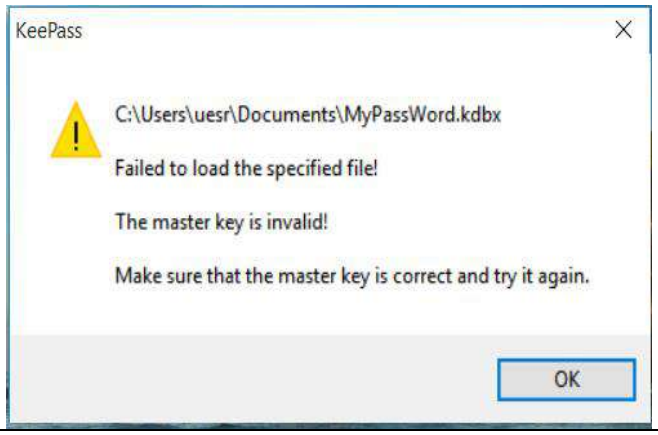
1	حمل نسخة حديثة من برنامج **KeePass** من الموقع الرسمي: (https://**keepass.info/**) (يفضل الإصدار 2.x). أو قم بتثبيت نسخة جاهزة في حال توفرها بدون انترنت.	

2	قم بتثبيت البرنامج واتبع خطوات التثبيت.	
3	افتح **KeePass**، ومن القائمة العلوية، اضغط على **File** ← **New**.	
4	اختر مكان حفظ ملف قاعدة البيانات (مثلاً، في مجلد **"Documents"**). واختر اسمًا للملف، مثل: **MyPasswords.kdbx** ثم اضغط **Save**.	

5	في نافذة **Set Master Key**، أدخل كلمة مرور قوية (مثلاً، مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز)، ويمكنك إستخدام مفتاح أمان إضافي (**Key File**) لتعزيز الحماية.	
6	اضغط **OK**، ثم قم بحفظ كلمة المرور في مكان أمن لأنك لن تستطيع استرجاعها إذا نسيتها.	

7	اضغط **Ctrl + N** أو اختر **Entry → Add Entry**، ثم أدخل التفاصيل: • **Title**: اسم الموقع أو الخدمة (مثلاً، **"Gmail"**). • **Username**: اسم المستخدم أو البريد الإلكتروني. • **Password**: اضغط على الأيقونة الصغيرة بجانب كلمة المرور لإنشاء كلمة مرور قوية عشوائية. • **URL**: رابط الموقع (مثلاً، https://gmail.com)، ثم اضغط **OK** لحفظ البيانات.	
8	اضغط بزر الماوس الأيمن على الحساب الذي أنشأته. واختر **Copy Password** (سيتم نسخه مؤقتًا لحمايتك من الاختراق (لمدة 12 ثانية ففي الذاكرة العشوائية))، ثم الصقها عند تسجيل الدخول للموقع المطلوب.	

9	من قائمة **file** اختر **save** وقم بحفظ نسخة احتياطية مشفرة (**.kdbx**) في مكان أمن مثل **USB** مشفر أو خدمة سحابية محمية.	
10	إختبار الاسترجاع أغلق البرنامج. أعد فتحه، ثم افتح القاعدة **MyPasswords.kdbx**. أدخل كلمة المرور الرئيسية التي انشأتها بالبداية (**Master Key**) وتحقق من ظهور الإدخالات.	

11	عند ادخال كلمة المرور الصحيحة سيتم فتح قاعدة البيانات التي انشأتها	
12	إذا كانت كلمة المرور غير صحيحة لا يمكن الدخول إلى قاعدة البيانات التي انشأتها كما في الصورة جانباً	

المناقشة

- جرّب تصدير واستيراد قاعدة البيانات.
- قم بإضافة فئات لتنظيم كلمات المرور (مثل: "حسابات بنكية"، "حسابات عمل"، "حسابات شخصية").
- استخدم ميزة البحث للعثور على كلمات المرور بسرعة.

1 حماية انظمة التشغيل

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:1	
اسم التمرين: : إعداد كلمات مرور قوية بأستخدام أداة مثل **KeePass**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب وتحميل البرنامج	%10		
2	تثبيت برنامج **KeePass**.	%10		
3	مراحل تنفيذ التمرين	%10		
4	المناقشة	%10		
5	الزمن المخصص	%10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

1 حماية انظمة التشغيل

رقم التمرين: 2 الزمن المخصص: ساعة واحدة

اسم التمرين: فحص الشبكات واكتشاف الأجهزة والخدمات الموجودة على الشبكة باستخدام الاداة **Nmap**

اولاً: الأهداف التعليمية

بعد إتمام هذا التمرين، سيتمكن الطالب من:

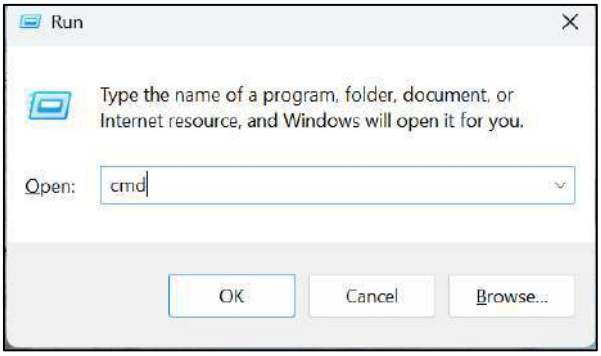
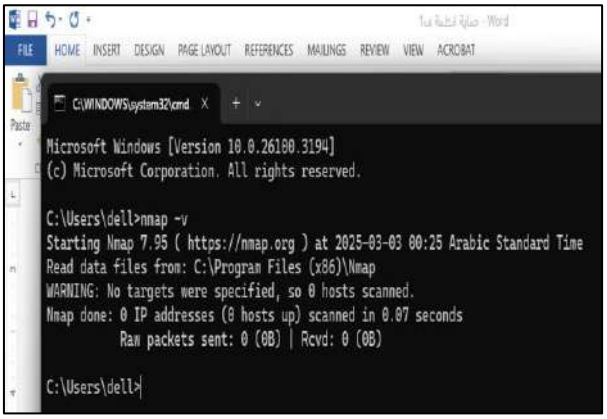
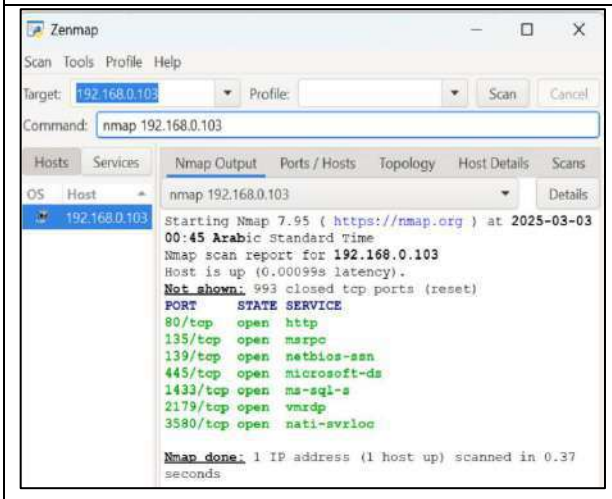
- تثبيت واستخدام أداة **Nmap**.
- إجراء فحص للأجهزة المتصلة على الشبكة المحلية.
- تحليل المنافذ والخدمات المفتوحة.
- استخدام أوامر متقدمة للكشف عن الأنظمة والخدمات.
- تطوير مهارات التحليل الأمني للمخرجات.

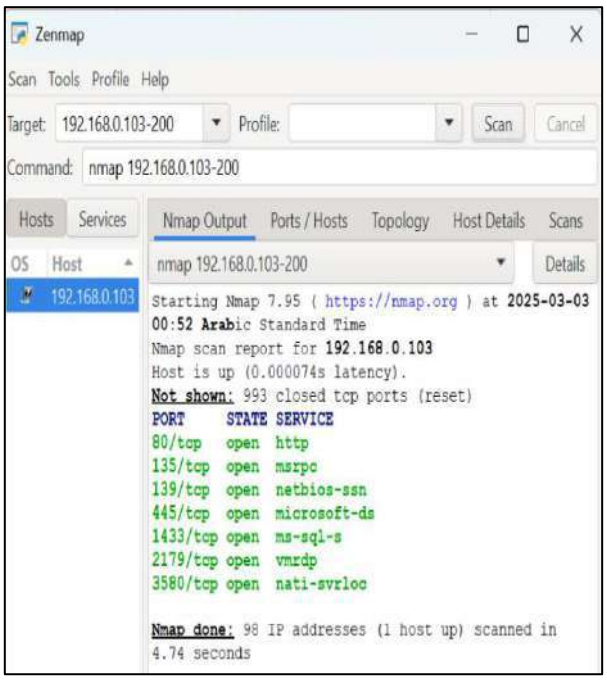
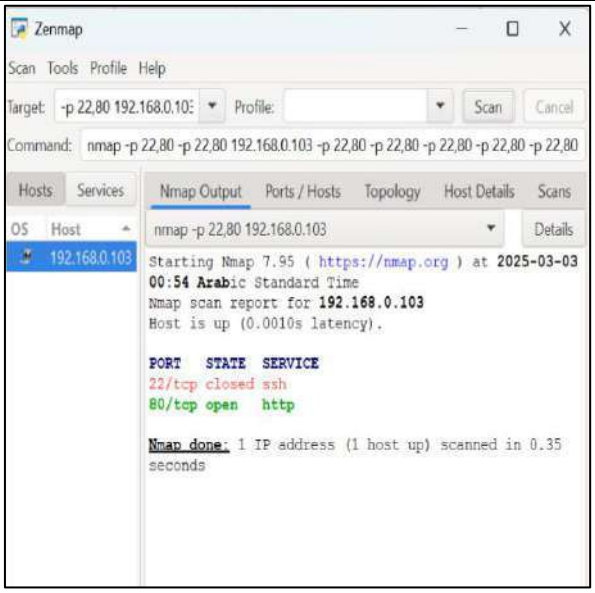
ثانياً: التسهيلات التعليمية

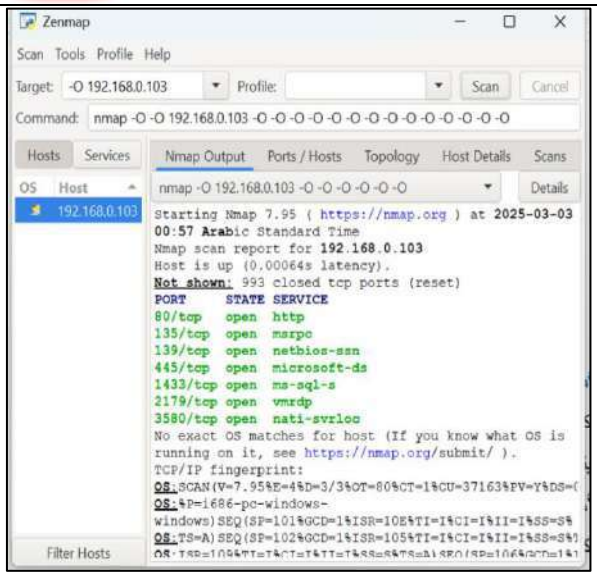
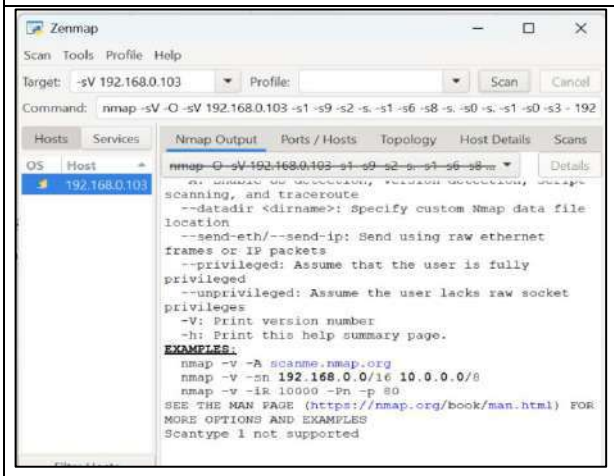
- جهاز **Windows 10/11**.
- اتصال فعّال بالشبكة والانترنت.

ثالثاً: خطوات تنفيذ التمرين

1	قم بتنزيل البرنامج من الموقع الرسمي لأداة **Nmap**: **nmap.org (https://nmap.org/download.html)** • أختر الإصدار المناسب لنظام **Windows**. • بعد اكتمال التنزيل، قم بتثبيت البرنامج على جهازك.	

2	بعد التثبيت، يمكنك تشغيل الأداة من خلال سطر الأوامر (**Command Prompt**) ثم اضغط على **Windows + R** لفتح مربع التشغيل ثم اكتب **cmd** واضغط **Enter**.	
3	في نافذة سطر الأوامر، اكتب الأمر الآتي للتحقق من تثبيت **Nmap**: **nmap -v** يجب أن تظهر لك معلومات حول إصدار الأداة إذا كانت قد تم تثبيتها بنجاح.	
4	بعد تشغيل برنامج **Zmap** من سطح المكتب إستخدام بعض الأوامر الأساسية لـ **Nmap**: **الأمر 1: فحص جهاز واحد (Single Host Scan):** • قم بتحديد **IP** جهازك الحالي من الـ **DOS** بأستخدام الأمر **ipconfig**. • لتحديد المنافذ المفتوحة على جهاز معين بأستخدام عنوان **IP**، استخدم هذا الأمر: **nmap 192.168.0.103** (استبدل **192.168.0.103** بعنوان **IP** للجهاز الذي تريد فحصه). • سيقوم **Nmap** بفحص المنافذ الأساسية للجهاز المحدد.	

5	**الأمر 2: فحص نطاق من الأجهزة (Range Scan):** • لفحص نطاق من الأجهزة بأستخدام **Nmap**، استخدم هذا الأمر: **nmap** 192.168.0.103-200 (استبدل 192.168.0.103-200 بالنطاق الذي ترغب في فحصه). • سيقوم **Nmap** بفحص الأجهزة في النطاق المحدد (من 192.168.0.103 إلى 192.168.0.200).	
6	**الأمر 3: اكتشاف المنافذ المفتوحة (Port Scan):** • لفحص المنافذ المفتوحة على جهاز معين: **nmap -p** 22,80 192.168.1.1 (سيقوم هذا الفحص بالتحقق من المنافذ 22 و 80 على جهاز الـ **IP** المحدد). • يمكنك إضافة المزيد من المنافذ بتعديل القائمة بعد **-p**.	

7	**الأمر 4: اكتشاف نظام التشغيل (OS Detection):** • لاكتشاف نوع نظام التشغيل على جهاز معين: **nmap -O** 192.168.1.1 • سيقوم **Nmap** بمحاولة تحديد نظام التشغيل الذي يعمل عليه الجهاز.	
8	**الأمر 5: اكتشاف إصدار الخدمة (Service Version Detection):** • لاكتشاف إصدارات الخدمات التي تعمل على المنافذ المفتوحة: **nmap -sV 192.168.1.1** • سيعرض هذا الفحص تفاصيل عن إصدارات التطبيقات والخدمات التي تعمل على الجهاز.	
9	**تحليل النتائج:** بعد تشغيل أي من الأوامر المذكورة، سيعرض **Nmap** تقريرًا يحتوي على: • المنافذ المفتوحة: قائمة بالمنافذ التي يمكن الوصول إليها. • إصدارات الخدمات: معلومات عن التطبيقات والخدمات التي تعمل على المنافذ المفتوحة. نظام التشغيل: إذا تم تحديده، سيعرض **Nmap** نوع النظام الذي يعمل عليه الجهاز.	
10	**المناقشة** • ما الفرق بين الفحص البسيط **nmap** والفحص المتقدم **-A**؟ • هل يمكن التلاعب بنتائج الفحص من قبل النظام المستهدف؟ كيف؟ • كيف يمكن إستخدام النتائج لتقوية دفاعات النظام؟ • ما الإجراءات المناسبة بعد اكتشاف منفذ مفتوح على خادم حقيقي؟	

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:2	
اسم التمرين: فحص الشبكات واكتشاف الأجهزة والخدمات الموجودة على الشبكة بأستخدام الاداة **Nmap**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب وتحميل البرنامج.	%10		
2	تثبيت البرنامج	%10		
3	مراحل تنفيذ التمرين	%10		
4	المناقشة	%10		
5	الزمن المخصص	%10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

1 حماية انظمة التشغيل

رقم التمرين: 3 الزمن المخصص: ساعة واحدة

اسم التمرين: تأمين حسابك على فيسبوك باستخدام المصادقة الثنائية عبر تطبيق **Google Authenticator**

اولاً: الأهداف التعليمية

بعد إتمام هذا التمرين، سيتمكن الطالب من:

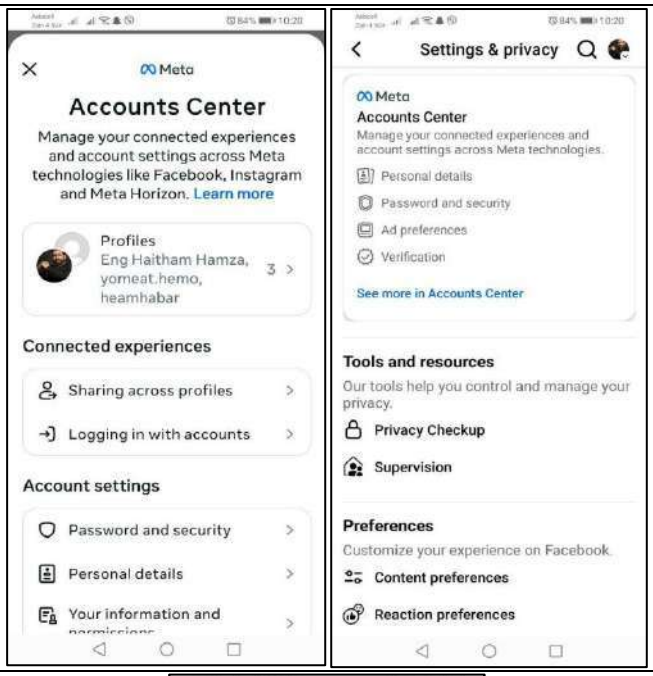
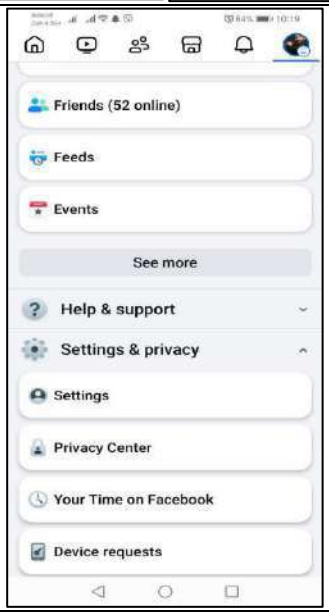
- تعريف الطلبة بالمصادقة الثنائية (**2FA**) ودورها في حماية الحسابات.
- تدريب عملي على تثبيت وإستخدام **Google Authenticator**.
- ربط حساب فعلي (مثل حساب فيسبوك) بالتطبيق.
- تجربة تسجيل دخول فعلي باستخدام المصادقة الثنائية.

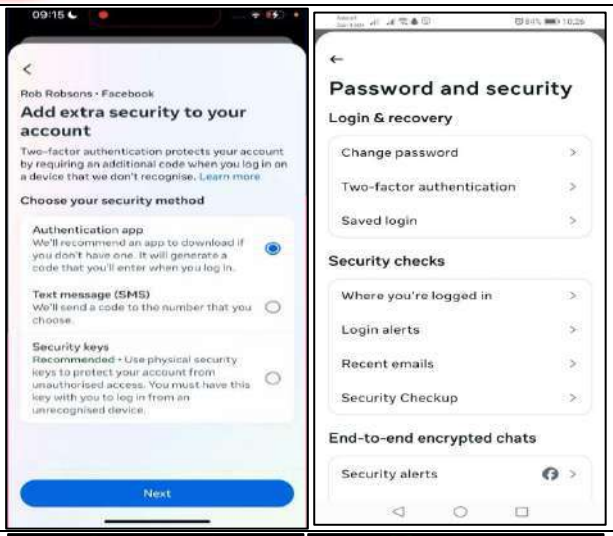
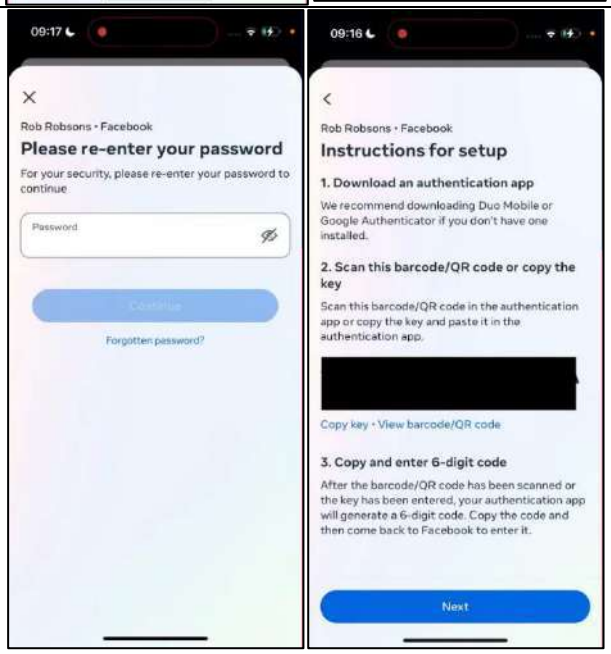
ثانياً: التسهيلات التعليمية

- حساب فيسبوك فعال.
- هاتف ذكي مثبت عليه تطبيق **Google Authenticator**.
- اتصال بالإنترنت.
- متصفح على الحاسوب لتسجيل الدخول وإجراء التعديلات.

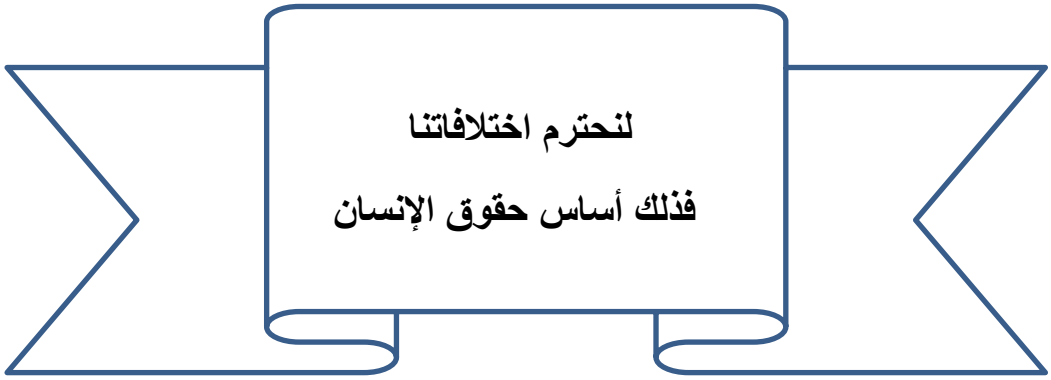
ثالثاً: خطوات تنفيذ التمرين

1	لأجهزة الأندرويد: تحميل من **Google Play** واجهزة الآيفون: تحميل من **App Store** وبعد التنزيل، افتح التطبيق واستعد لإضافة حساب فيسبوك.	

2	تفعيل المصادقة الثنائية على فيسبوك: من تطبيق فيسبوك (الموبايل) أو موقع فيسبوك (الكمبيوتر):	
3	افتح تطبيق فيسبوك وانتقل إلى ☰ القائمة (أو الصورة الشخصية في الزاوية العلوية) ثم اختر الإعدادات والخصوصية ثم الإعدادات.	

4	انتقل إلى الأمان وتسجيل الدخول ثم اضغط على إستخدام المصادقة الثنائية.	
5	اختر تطبيق المصادقة (Authenticator App) بدلاً من الرسائل النصية، سيظهر لك فيسبوك رمز QR على الشاشة، افتح تطبيق Google Authenticator واضغط على إضافة (+). ثم اختر مسح رمز QR، ووجّه الكاميرا نحو رمز QR في فيسبوك. إذا لم تتمكن من مسح الرمز، اضغط على إدخال مفتاح يدويًا، ثم أدخل المفتاح السري الذي يظهر في فيسبوك، بعد إضافة الحساب، سيظهر رمز متغير كل 30 ثانية في التطبيق.	
6	إذا لم تتمكن من مسح الرمز، اضغط على إدخال مفتاح يدويًا، ثم أدخل المفتاح السري الذي يظهر في فيسبوك، بعد إضافة الحساب، سيظهر رمز متغير كل 30 ثانية في التطبيق.	

7	**تفعيل Google Authenticator في حساب فيسبوك:** ارجع إلى فيسبوك وأدخل الرمز المؤقت الذي ظهر في **Google Authenticator** ثم اضغط تأكيد لإنهاء الإعداد ثم احتفظ بنسخة من الرموز الاحتياطية التي يوفرها فيسبوك، لاستخدامها عند فقدان الهاتف وبالتالي عند تسجيل الدخول إلى فيسبوك، سيطلب منك إدخال رمز المصادقة الثنائية من **Google Authenticator**.
8	**المناقشة** • هل يمكن اختراق الحساب رغم وجود **Google Authenticator** ؟ • ماذا تفعل إذا لم تعد تستطيع الوصول إلى هاتفك؟ • ما التطبيقات والخدمات الأخرى التي يمكن حمايتها بنفس الطريقة؟



استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:3	
اسم التمرين: تأمين حسابك على فيسبوك بأستخدام المصادقة الثنائية عبر تطبيق **Google Authenticator**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب أو الموبايل وتحميل البرنامج.	%10		
2	تثبيت البرنامج	%10		
3	مراحل تنفيذ التمرين	%10		
4	المناقشة	%10		
5	الزمن المخصص	%10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

أسئلة الفصل الاول

س1:عرف ما يأتي:

1- النظام التشغيلي 2- الأمن الوقائي 3-البرمجيات الخبيثة 4- برامج الفدية 5- جدران الحماية.

س2: املأ الفراغات الاتية بما يناسبها:

1- العملية التي يتم فيها منح المستخدمين أذونات محددة للوصول إلى موارد النظام تُعرف بـ .....

2- الطريقة التي يتم بها خداع المستخدمين للكشف عن معلومات حساسة، مثل كلمات المرور، تُسمى .....

3- تُستخدم أداة ..... لفحص الشبكات واكتشاف الأجهزة المتصلة بها والمنافذ المفتوحة.

4- البرمجيات التي تُستخدم لاكتشاف وإزالة الفيروسات من أجهزة الكمبيوتر تُعرف بـ .....

5- من أمثلة أنظمة تشغيل الهواتف الذكية ..... و .....

6- يُطلق على الثغرات الأمنية غير المعروفة التي يتم استغلالها قبل اكتشافها وإصلاحها اسم .....

س3:عدد ثلاثاً من وظائف نظام التشغيل الأساسية، ووضح دور كل منها.

س4: اشرح كيفية عمل المصادقة الثنائية (**2FA**) ولماذا تعد ضرورية في تأمين الحسابات.

س5: ما الفرق بين الأمن الوقائي والأمن التفاعلي، مع ذكر مثال على كل منهما.

س6: عدد أهم ممارسات الأمان التي يجب اتباعها لحماية أنظمة التشغيل من الاختراقات.

س7: اشرح كيف يمكن لفيروسات الفدية (**Ransomware**) التأثير على المؤسسات، وما هي طرق الحماية منها؟

س8: فرّق بين أنظمة التشغيل المستخدمة في الحواسيب المكتبية والهواتف الذكية من حيث الأمان والتطبيقات والتفاعل مع المستخدم.

س9: ما هي العوامل التي تؤثر على تصنيف كلمة المرور كضعيفة أو قوية؟

الفصل الثاني

إدارة صلاحيات المستخدمين

User permissions management

أهداف الفصل الثاني

1. فهم أهمية إدارة حسابات المستخدمين في أنظمة التشغيل
2. التعرف على أنماط التحكم في الوصول المختلفة مثل أدوات (**MAC،DAC** ، **RBAC**).
3. اكتساب مهارات في تطبيق مبدأ أقل الصلاحيات

(Principle of Least Privilege) لتقليل المخاطر الأمنية.

4. القدرة على تحليل وتحديد الحسابات ذات المخاطر الأمنية العالية

محتويات الفصل الثاني

(2-1) إدارة حسابات المستخدمين في أنظمة التشغيل المختلفة.

(2-2) أنماط التحكم في الوصول (**MAC, DAC, RBAC**).

(2-3) التمييز بين الحسابات العادية والادارية.

(2-4) كيفية تقليل الحقوق لتقليل المخاطر.

(2-5) تحليل سجلات الدخول وتحديد الحسابات غير الآمنة.

تمرين (4) إعداد صلاحيات الملفات والمجلدات بأستخدام أوامر مثل **chmod** و **chown** في أنظمة **Linux**

تمرين (5) فحص حسابات المستخدمين بأستخدام **Nessus**.

تمرين (6) إنشاء وادارة سياسات المجموعات (GPO) في **Windows Server**.

الفصل الثاني

ادارة صلاحيات المستخدمين

User permissions management

تمهيد

في العصر الرقمي أصبحت الحواسيب ذات أنظمة التشغيل المختلفة واتصالها بشبكة الإنترنت جزءا أساسيا من حياتنا اليومية وتتزايد يوما بعد يوم، مع هذا التوسع تأتي الحاجة إلى إدارة حسابات المستخدمين بشكل فعال لضمان حماية أنظمة التشغيل وأمن الشبكة وسلاسة استخدامها، كما تسمح أنظمة التشغيل المختلفة بإضافة عدد من حسابات المستخدمين للاستخدام في الجهاز نفسه بصلاحيات إدارية تمكنه من التحكم في الوصول إلى الموارد الرقمية وكيفية تحديد مستوى الوصول لتلك الموارد ، أن إدارة صلاحيات المستخدمين هي جزء من نظام الأمن السيبراني وتلعب دورا هاما في تأمين النظام وحماية البيانات الحساسة فهي تمثل خط الدفاع الأول ضد التهديدات الداخلية والخارجية والتقليل من فرص حدوث المخاطر الأمنية الناجمة عن الاختراق من قبل المستخدم غير المصرح به أو الأخطاء البشرية

(2- 1) إدارة حسابات المستخدمين في أنظمة التشغيل المختلفة

أن إدارة حسابات المستخدمين في نظام التشغيل هو إنشاء نوع من حساب المستخدم في نظام التشغيل تمنح له صلاحيات الوصول إلى الأجهزة والبرامج والخدمات.

في هذا الموضوع، نستعرض خطوات وأساسيات إدارة حسابات المستخدمين في أنظمة التشغيل المختلفة لضمان تجربة آمنة وفعالة لجميع المستخدمين، ومنها:

1. **إنشاء حسابات فردية لكل مستخدم:** عندما يكون لكل مستخدم حساب خاص به يصبح من السهل إدارة الحساب من تحديد حقوق الوصول لكل شخص وضمان تخصيص الموارد بفعالية بهذه الطريقة يمنح المستخدمين خصوصية أكبر ويسمح النظام بالتحكم في الأنشطة داخل الشبكة ولكل مستخدم يحتاج إلى حساب مع قيود أمان مختلفة حسب مستوى الحساب المستخدم لنظام التشغيل .

2. **إستخدام كلمات مرور قوية وفريدة لكل حساب:** لضمان أمان حسابات المستخدمين يتطلب لكل حساب كلمات مرور قوية وفريدة فهي واجهة الدخول لنظام التشغيل عبر الشبكة فإن إستخدام كلمات مرور ضعيفة أو متكررة يعرض نظام التشغيل عبر الشبكة للخطر مما يسهل اختراق نظام التشغيل من قبل المهاجمين للوصول إلى الشبكة بأكملها.

3. التحكم في حقوق الوصول الموارد الرقمية: ليس كل مستخدم يحتاج إلى الوصول إلى جميع الموارد عبر الشبكة فهناك نوعان من حسابات المستخدمين منها الحسابات الإدارية(المسؤول أو المدير) والحسابات العادية (الضيوف) بالإضافة إلى ذلك يمكن أن يكون للحسابات العادية قيود مختلفة ومحدودة مقارنة بالحسابات الإدارية ولكنها محمية بكلمة مرور قوية (توفر أقصى درجة تحكم) ويجب استخدامها فقط عند الضرورة.

4. مراقبة الأنشطة على الأجهزة في الشبكة: من المهم مراقبة الأنشطة داخل الشبكة للتأكد من عدم وجود محاولات دخول مشبوهة أو إستخدام غير مناسب ويمكن أن يتم ذلك بأستخدام أدوات مدمجة في جهاز التوجيه أو تطبيقات خارجية.

و لمعالجة هذه التحديات، على المستخدم اتخاذ التدابير والإجراءات اللازمة وكما يأتي:

- إستخدام لوحة التحكم في جهاز التوجيه لمراجعة الأجهزة المتصلة والنشطة.
- القيام بضبط تنبيهات لإعلامك بمحاولات الدخول غير مصرح بها.
- مراقبة إستخدام البيانات لتجنب التحميلات غير المرغوب فيها.

مما تقدم يتبين أن إدارة حسابات المستخدمين تتطلب تخطيطاً جيداً وجهداً مستمراً من خلال تخصيص الحسابات، وحماية البيانات بكلمات مرور قوية، ومراقبة الأنشطة، وتحديث الأجهزة. فيمكنك إنشاء نظام تشغيل أمن يلبي احتياجات الشركات والمؤسسات الحكومية ومع تزايد التهديدات الرقمية والأمان لم يعد خيارا بل هو ضرورة يجب أن تكون على رأس الأولويات.

(2-2) أنماط التحكم في الوصول (MAC, DAC, RBAC)

في عصر التكنولوجيا والتعليم الرقمي، أصبحت حماية البيانات والمعلومات جزءًا أساسيًا من أي نظام إلكتروني. سواء كان ذلك داخل منصة تعليمية، أو نظام درجات، أو بريد إلكتروني خاص بالمدرسة، لا بد من وجود آلية تحدد "من يحق له الوصول إلى ماذا؟".

هنا يأتي دور أنماط التحكم في الوصول، وهي طرق تنظيمية وتقنية تهدف إلى تحديد الأذونات أو الصلاحيات التي يمتلكها كل مستخدم داخل النظام، بناءً على موقعه أو وظيفته أو مستوى الأمان المطلوب للوصول إلى الموارد.

ومن أجل تحقيق هذا الهدف. تم تطوير أنماط متعددة للتحكم في الوصول، لكل منها استخدامات ومزايا معينة، وأبرز هذه الأنماط هي:

- **DAC** التحكم التقديري في الوصول (**Discretionary Access Control**): النظام يحدد السياسات عن طريق تحديد تصنيف أمني للمستخدمين والموارد.

- **MAC** التحكم الإلزامي في الوصول (**Mandatory Access Control**): المالك هو الذي يحدد الأذونات للمستخدمين.

- **RBAC** التحكم القائم على الأدوار **(Role-Based Access Control)** : الدور الوظيفي للمستخدم يحدد الأذونات وليس الهوية الشخصية.

كل نمط من هذه الأنماط يتميز بخصائص معينة تجعله مناسبًا لبيئات محددة. فبعضها يمنح المستخدمين حرية أكبر في مشاركة المعلومات، بينما يعتمد بعضها الآخر على سياسات مركزية صارمة تفرضها الإدارة لضمان حماية البيانات بشكل أكبر.

عند تطبيق نماذج التحكم في الوصول المختلفة في نظام إدارة الشركات والمؤسسات الحكومية كإدارة مدرسة مثلاً، أول ما نفكر به هو:-

أولاً: تحديد الهيكل التنظيمي للمدرسة وما هي أدوار المستخدمين داخل المدرسة من مدير ومعاونين ومدرسين وإداريين وطلاب ومن ثم تحديد المستويات التي تحتاج إلى صلاحيات مختلفة

ثانياً: تحديد البيانات والموارد التي تحتاج إلى حماية

- بيانات الطلاب مثل الدرجات والمعلومات الشخصية.
- المواد الدراسية والمصادر التعليمية.
- سجلات الحضور والغياب.

ثالثاً: اختيار نموذج التحكم المناسب لكل نوع من البيانات

- نمط التحكم **MAC** هو حماية البيانات الحساسة مثل درجات الطلاب ومنع تغييرها من قبل الطالب ومنح صلاحية التغيير للمدير والمدرس فقط.
- نمط التحكم **RBAC** لتنظيم الوصول حسب الأدوار مثل المعلمين يمكنهم تعديل الدرجات، ولكن الطلاب لا يمكنهم ذلك.
- نمط التحكم **DAC** يوفر للمستخدمين من مدرسين وطلاب مشاركة الموارد عند الحاجة بشكل فردي لكل طالب على سبيل المثال يمكن للمدرس أن يشارك المواد الدراسية مع الطلاب وتنزيلها على الحاسبة.

كل أنواع أنظمة التحكم في الوصول قد فشلت في حماية البيانات عندما تكون المصادقة ضعيفة، أي أن المخترق قد يتجاوز كل طبقات الحماية بمجرد سرقة كلمة مرور أو اختراق جلسة مستخدم. فعلى سبيل المثال اذاكانت كلمة المرور ضعيفة وتمكن المخترق من تخمينها فبمجرد دخوله سيتمتع بكل صلاحيات المستخد. لذلك يعد مخاطر أمان المصادقة وإدارة الجلسات (**Broken Authentication & Session Management)** من الثغرات الشائعة في إدارة المستخدمين والتي تعني ضعف المصادقة وإدارة الجلسات، حيث يمكن للمهاجمين استغلال كلمات مرور ضعيفة أو جلسات غير منتهية الصلاحية للوصول غير المصرح به. لتجنب ذلك، يجب تطبيق سياسات مثل:

- قفل الحساب بعد عدة محاولات دخول فاشلة، وسوف نتطرق إليه عمليا في التمرين 6.
- إستخدام جلسات **(Session IDs)** عشوائية وآمنة.
- تفعيل المصادقة متعددة العوامل **(MFA)**.

(3-2) التمييز بين الحسابات العادية والإدارية

يعتمد التمييز بين الحسابات العادية والحسابات الإدارية في أي نظام إلكتروني على الصلاحيات والمهام الممنوحة لكل نوع، عزيزي الطالب جدول (2-1) يوضح مقارنة مبسطة بالاعتماد على مجموعة من الخصائص التي توضح الفرق من حيث الصلاحيات، والاستخدام، والوظيفة.

جدول (2-1) مقارنة بين الحسابات العادية والإدارية

الخصائص	الحساب العادي **Standard user**	الحساب الإداري **(Administrator)**
الصلاحيات	صلاحيات محدودة، لا يمكنه تعديل إعدادات النظام أو تثبيت البرامج.	صلاحيات كاملة، يمكنه الوصول إلى كافة إعدادات النظام وتثبيت/إزالة البرامج.
الوصول للموارد	وصول مقيد لبعض الموارد والملفات.	وصول كامل لجميع الملفات والمجلدات والموارد الرقمية.
الغرض من الاستخدام	الاستخدام اليومي كالتصفح، قراءة وكتابة ملفات معينة، تشغيل البرامج المثبتة.	إدارة النظام، صيانة الشبكة، تثبيت برامج، إعداد السياسات الأمنية.
الأمان	أقل خطورة في حال الاختراق، لكنه معرض للقيود.	أكثر حساسية، اختراقه يعني السيطرة الكاملة على النظام.
المهام الممكنة	لا يمكنه إنشاء حسابات أخرى أو تغيير صلاحيات.	يمكنه إنشاء أو حذف حسابات، وتغيير الصلاحيات.
أمثلة	مستخدم حاسوب في شركة أو طالب في مختبر.	مشرف النظام في شركة أو مؤسسة معينة.

(4-2) كيفية تقليل الحقوق لتقليل المخاطر

مبدأ أقل الصلاحيات **(Principle of Least privilege)** هو مفهوم أساسي في أمن المعلومات ويعني منح كل مستخدم أو برنامج أقل قدر ممكن من الصلاحيات التي يحتاجها لأداء مهامه فقط وليس أكثر. هدف هذا المبدأ هو تقليل المخاطر في حال حدوث خطأ أو اختراق، لأن المهاجم أو المستخدم نفسه لن يتمكن من الوصول إلى أشياء لا يحتاجها.

تخيل أنك تعمل في مدرسة، وتملك مفتاحًا واحدًا يفتح كل الغرف: غرفة المدير، وغرفة المعلمين، والمختبر، والمكتبة ثم تُعطي هذا المفتاح للطالب لكي يدخل المكتبة فقط. هل هذا أمن؟ طبعا لا، لأن الطالب قد يدخل أماكن لا ينبغي له الوصول إليها. من المعقول أن تعطيه مفتاحًا يفتح فقط باب المكتبة. هذا هو بالضبط مبدأ أقل الصلاحيات. وعليه تطبيق هذا المبدأ يقلل من المخاطر الأمنية عن

طريق تحديد المهام لكل مستخدم بدقة من خلال منحه فقط الصلاحيات المرتبطة بهذه المهام، وبالتالي منع الوصول غير الضروري إلى المعلومات أو الأنظمة. أن اعتماد مبدأ أقل الصلاحيات في أمن البيانات والمعلومات يمكن أن يوفر للمؤسسات الفوائد الآتية:-

- **يمنع انتشار البرمجيات الخبيثة**: حيث يفرض قيوداً على أنظمة أجهزة الحاسوب ولا تستطيع هجمات البرمجيات الخبيثة إستخدام حسابات ذات صلاحيات أعلى (حسابات مسؤول) لتثبيت البرمجيات الخبيثة أو إتلاف النظام.

- **الحد من الضرر الناتج عن الاختراق**: إذا تم اختراق حساب مستخدم أو برنامج، فإن المهاجم لا يمكنه الوصول إلاّ إلى ما كان مخولًا له فقط. فمثلاً إذا اخترق المهاجم حساب موظف لا يمتلك صلاحية حذف الملفات، فلن يتمكن من إحداث ضرر كبير.

- **الحماية من الأخطاء البشرية:** قد يرتكب المستخدمون أخطاء عن غير قصد، مثل حذف ملف أو تعديل إعدادات حرجة. مبدأ أقل الصلاحيات يقلل احتمالية هذه الأخطاء بمنع الوصول غير الضروري.

- **تعزيز الرقابة والتحقيق:** حيث أن الصلاحيات المحدودة تجعل من السهل تتبع الأنشطة المشبوهة، وربطها بمستخدم معين ويساعد في التحقيقات وتحليل الحوادث الأمنية.

- **تحسين استقرار النظام:** عندما لا تكون للبرامج أو المستخدمين القدرة على تعديل إعدادات النظام أو حذف ملفات حرجة، فإن احتمال تلف النظام ينخفض.

فمع خفض الصلاحيات للمستخدمين والبرامج لأقل مستوياتها الممكنة لأداء المهام، سيحدّ من الضرر الناتج عن اختراق الحسابات، **ولكن ماذا لو تم اختراق حساب المستخدم حتى مع تقليل الصلاحيات؟**

فبالرغم من وجود جودة خفض الصلاحيات إلاّ أنها لا تضمن ديمومة المحافظة على الأمان عندما يتم اختراق حساب المستخدم، ولهذا تطلب ضرورة النظر إلى أهمية دور سياسة الأمن القائم على السلوك (**Behavior-Based Security**) التكميلي مع سياسة تقليل الصلاحيات لتعزيز الأمان من خلال القيام بمراقبة وتحليل أنماط السلوك الطبيعية للمستخدمين لاكتشاف الحسابات المخترقة أو الأنشطة المشبوهة ، مثل محاولات وصول متكررة فاشلة تليها نجاح (علامة على هجوم **Brute Force**) وسوف نتطرق اليها عمليا في تمرين رقم 5.

(5-2) تحليل سجلات الدخول وتحديد الحسابات غير الآمنة

يُعد تحليل سجلات الدخول (**Login Logs Analysis**) من أهم خطوات تعزيز أمن الأنظمة، حيث يتم من خلاله مراقبة الأنشطة المرتبطة بالحسابات داخل النظام، مثل وقت الدخول، مصدر الاتصال، والأجهزة المستخدمة. يساعد هذا التحليل في كشف الحسابات غير الآمنة، والتي قد تتضمن:

- محاولات دخول متكررة فاشلة.
- تسجيل دخول من مواقع جغرافية غير معتادة.
- إستخدام حسابات غير نشطة منذ فترة.
- نشاط مريب في ساعات غير طبيعية.

من خلال أدوات مثل **Nessus** أو أنظمة تسجيل الدخول المركزية (مثل **Active Directory**)، يمكن جمع هذه السجلات وتحليلها بشكل دوري لاكتشاف التهديدات مبكرًا، وحماية النظام من أي اختراق محتمل. ويمكن تحليل وتحديد الحسابات ذات المخاطر الأمنية العالية من خلال مفهوم تقنية تقييم خطورة الحساب المستخدم وتحليلها.

وعملية تقييم خطورة الحساب منهجية منظمة لتحديد الحسابات غير الآمنة المحتملة والذي قد يؤثر سلبا على أهداف المؤسسة أو الشركة ويلعب دورا حاسما في تحسين صنع القرار من قبل المؤسسة بالاعتماد على البيانات لضمان المعالجة الحرجة ويعمل على تعزيز وتحسين تخصيص الموارد بشكل فعال. هذه الاستراتيجية يتم فيها تحديد خطورة الحساب على أساس معايير تقييم معينة وفيها يتم تقييم كل خطر على وفق احتمالية حدوثه وتأثيره المحتمل. تقييم خطورة الحساب وتحليلها هو عملية فحص حسابات المستخدمين داخل النظام لتحديد مدى تعرضها للتهديدات الأمنية وتصنيف مستوى خطورتها والتي تعتمد على معايير تقييم تلك الخطورة. هناك عدة معايير معتمدة لتقييم خطورة الحساب ومنها:

- **قوة كلمة المرور:** وصف قوة كلمة المرور إذا كانت ضعيفة أو مكررة أو سهلة التخمين.
- **سجلات الدخول المشبوهة:** محاولات تسجيل دخول من مواقع أو أجهزة غير مألوفة مثلاً دولة أو عنوان **IP** غير معروف أو تعدد محاولات دخول فاشلة.
- **الصلاحيات الممنوحة:** صلاحيات الحساب غير المناسبة، مثلاً إعطاء صلاحيات غير مناسبة لأنواع من الحسابات العادية، على سبيل المثال حساب عادي يمتلك صلاحيات مدير نظام.
- **فترة الخمول:** يوصف الحساب نشطاً لكنه غير مستخدم لفترة طويلة.
- **سلوك غير طبيعي للحساب:** مثل تحميل ملفات مشبوهة وتنفيذ أوامر غير معتادة أو محاولة الوصول إلى أنظمة لم يسبق للحساب استخدامها.

بعد جمع البيانات على أساس مرحلة معايير تقييم خطورة الحساب، يتم البدء بمرحلة تحليل بيانات الحساب وتصنيف الخطورة والذي يتم فيه تصنيف الحسابات وفقا لمستويات الخطورة وكما يأتي:

- مستوى حساب مرتفع الخطورة: يعبر عن حالة الحساب "مسؤول" (**Admin**) مثلاً بكلمة مرور ضعيفة وتم رصد نشاط غير مشبوه.
- مستوى حساب متوسط الخطورة: يعبر عن حالة الحساب "مستخدم عادي" لم يغير كلمة المرور منذ فترة طويلة.

- مستوى حساب منخفض الخطورة: يعبر عن حالة "الحساب نشط" بكلمة مرور قوية ولا يوجد عليه أنشطة مشبوهة.

بعد معرفة مستوى خطورة الحساب، هناك بعض الممارسات أو الإجراءات المتخذة للتعامل مع مستوى الخطورة وكما يأتي:

- إذا كان الحساب مرتفع الخطورة يتم تعطيل الحساب المخترق فورا وتغيير كلمه المرور أو تحديثه ومراقبة الحساب بشكل دوري.
- إذا كان الحساب متوسطة الخطورة يطلب من المستخدم تغيير كلمة المرور أو تحديثها.
- إذا كان الحساب منخفض الخطورة يتم تفعيل المصادقة الثنائية **2FA** للحسابات المهمة أو تعطيل الحسابات غير النشطة.

مثال:- لدينا نظام إداري إلكتروني لمدرسة يحتوي على معلومات مهمة مثل درجات الطلاب، البيانات الشخصية للطلبة والكادر التدريسي والاداري، وسجلات الحضور تعرضت لهجمات سيبرانية. قررت الادارة إجراء فحص أمني للحسابات وتحليلها واكتشاف الحسابات غير الآمنة أو المخترقة بأستخدام إحدى أدوات الفحص وبعد انتهاء الفحص وتحليل بيانات الفحص تم تحديد الحسابات غير الآمنة كما موضح في جدول (2-2).

جدول (2-2) تحليل بيانات وتحديد خطورة الحسابات لنظام إلكتروني لمدرسة

نوع الحساب	المشكلة المكتشفة	مستوى المخاطر	الإجراء المطلوب
حساب مدير **(Admin)**	تسجيل دخول من عنوان **IP** غير معروف	مرتفع	تعطيل الحساب وتغيير كلمة المرور
حساب معلم **Teacher**	كلمة مرور ضعيفة جدا **"password=123"**	مرتفع	فرض تغيير كلمة المرور فورا
حساب طالب **Student**	لم يغير كلمة المرور منذ سنة	متوسط	تنبيه المستخدم لتحديث كلمة المرور
حساب الإداريين **(Staff)**	لا يوجد مصادقة ثنائية العوامل **2FA**	منخفض	توصية بتفعيل المصادقة متعددة العواملMFA

2 حماية أنظمة التشغيل

رقم التمرين: 4 الزمن المخصص: ساعة واحدة

اسم التمرين: إعداد صلاحيات الملفات والمجلدات بإستخدام أوامر chmod و chown في أنظمة Linux

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

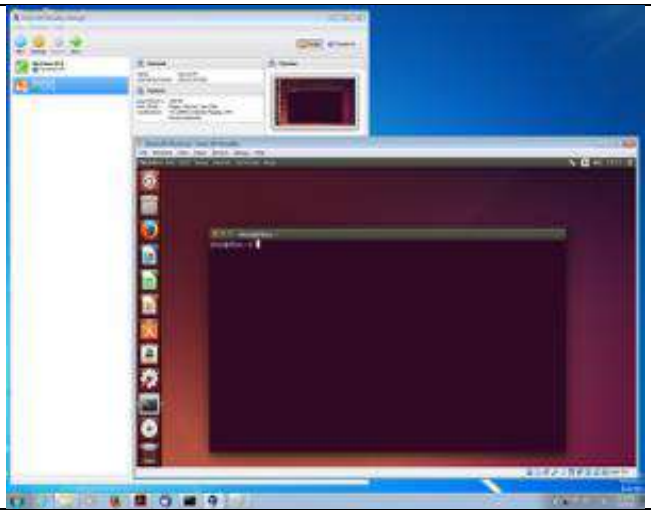
بعد إتمام هذا التمرين، سيتمكن الطالب من:

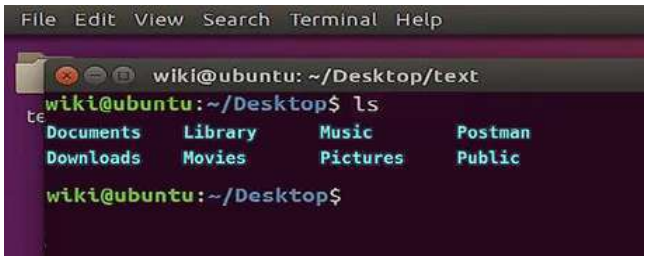
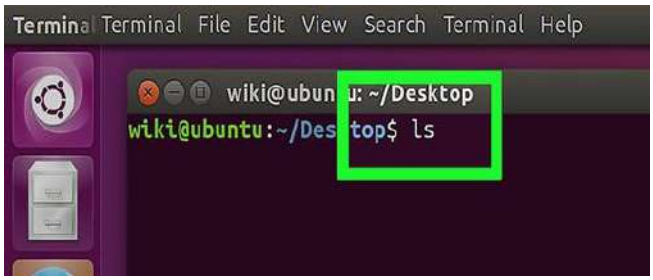
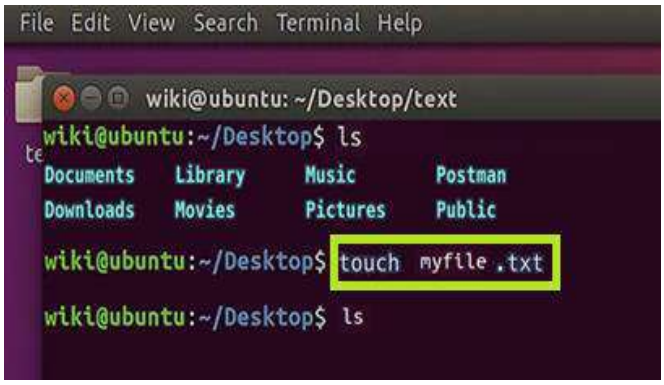
- التعرف على كيفية ضبط صلاحيات الملفات والمجلدات وتطبيقها عملياً بأستخدام أوامر chmod وchown.
- فهم تأثير هذه الصلاحيات على أمان النظام..
- تدريب الطلبة على استخدام أوامر chmod و chown نظام Linux .

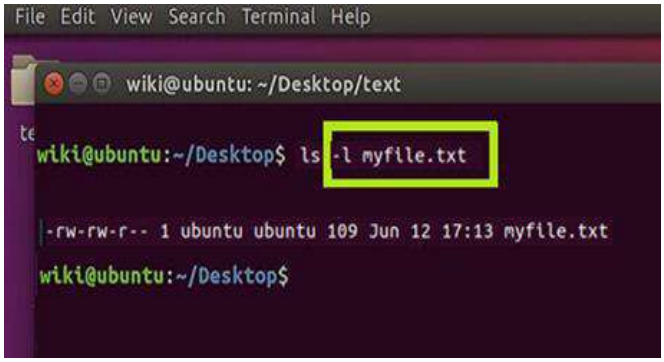
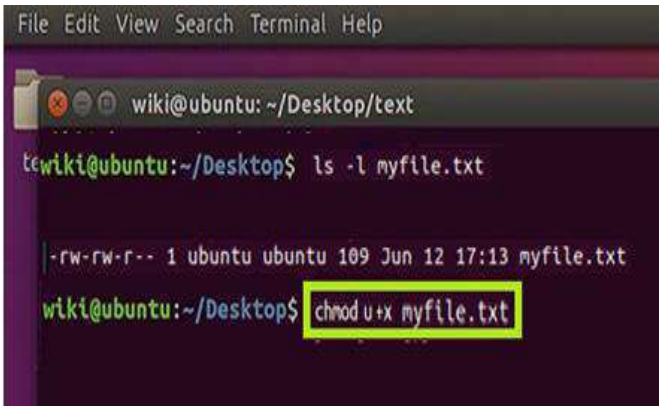
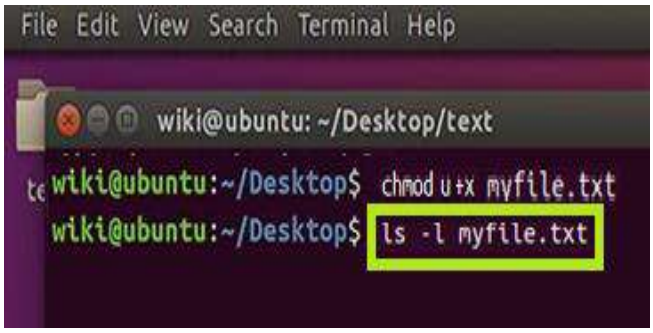
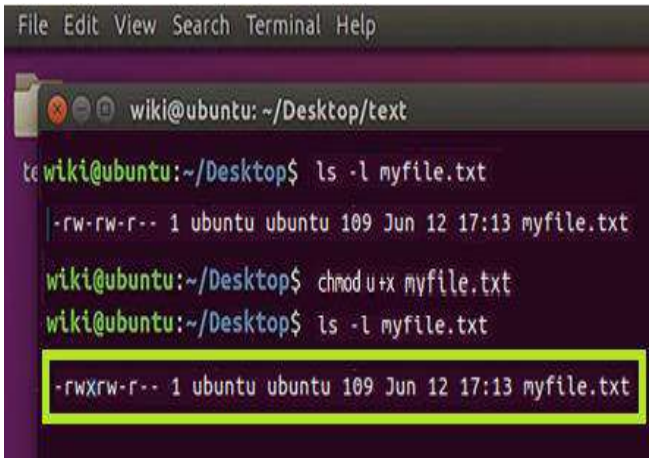
ثانياً: التسهيلات التعليمية

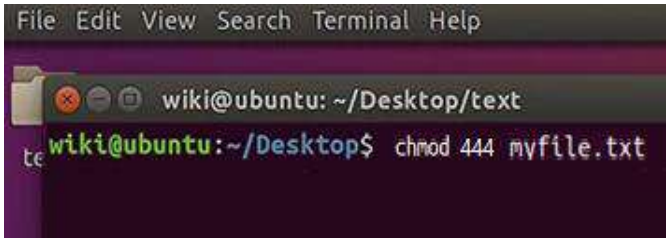
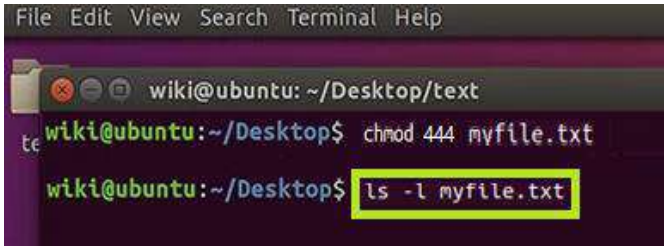
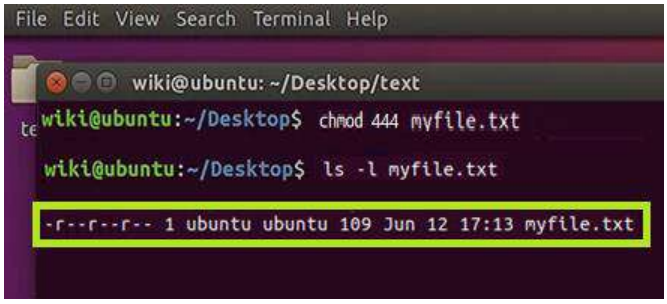
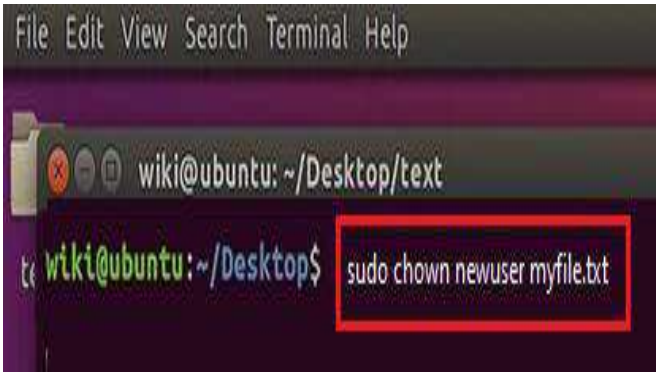
- برنامج محاكاة الأنظمة الافتراضية VirtualBox لتشغيل نظام Linux مثل Ubuntu.
- أجهزة الحاسوب بصلاحيات المستخدم (User) وصلاحيات المدير (Administrator) .

ثالثاً: خطوات تنفيذ التمرين:

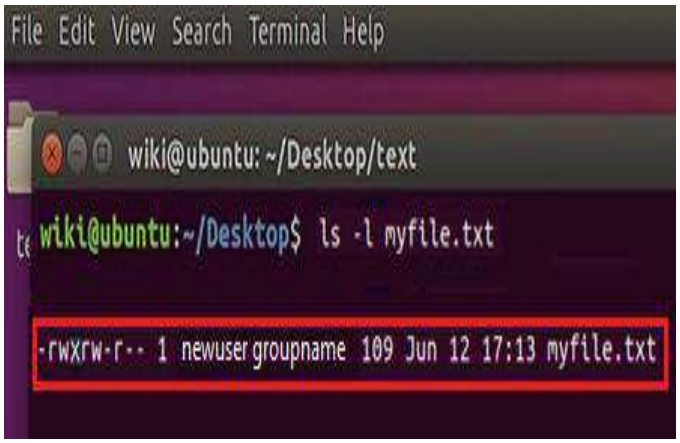
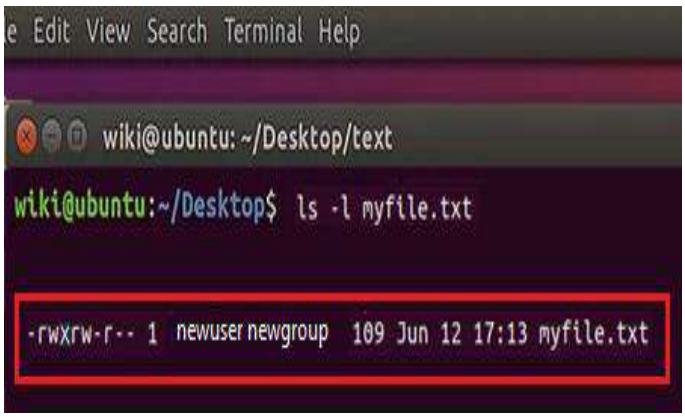
1	افتح برنامج **VirtualBox** من قائمة ابدأ أو سطح المكتب. واختر الآلة الافتراضية (**VM**) التي تحمل اسم **Ubuntu** (مثل **Ubuntu** 22.04) من القائمة الجانبية. ثم إنقر على **Start** (الزر الأخضر أو أيقونة التشغيل).	

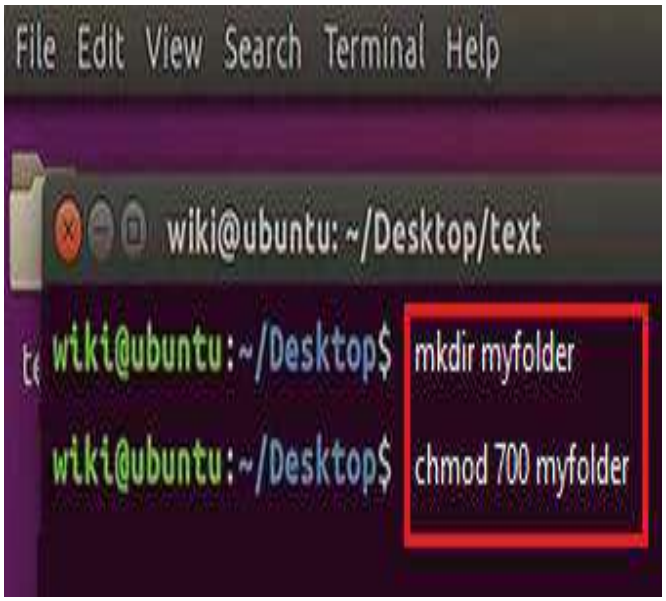
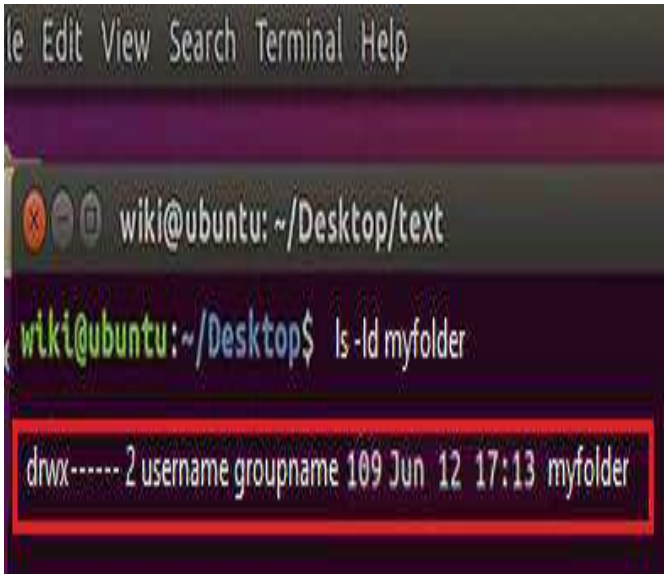
2	افتح واجهة النظام **linux** واكتب Ter للدخول إلى واجهة ال **Terminal** كما موضح في الشكل	
3	أكتب الأمر **ls** لعرض الملفات والمجلدات تحت الدليل مجلد **Desktop**	 
4	أكتب الأمر **touch** لإنشاء الملف النصي باسم **Myfile** تلميح : الحرف الموجود في هذا المثال هو حرف **L** صغير وليس حرف **i** كبير.	

5	اكتب الأمر **ls -l** لعرض صلاحيات الملف. تم ظهور صلاحيات الملف **–rw-rw-r—** اي أن الملف قابل للقراءة والكتابة من قبل المالك فقط دون التنفيذ	
6	أكتب الأمر **chomd u+x** لتغير صلاحية الملف **myfile.txt** بجعل الملف قابلًا للتنفيذ من قبل المالك	
7	للتحقق من نتيجة الأمر **chomd u+x** بكتابة الأمر **ls -l** مع اسم الملف.	
8	لاحظ عزيزي الطالب قد تم تغيير صلاحيات الملف **myfile.txt** من ملف قابل للقراءة والكتابة فقط إلى قابل للتنفيذ مع القراءة والكتابة من قبل المالك **User (u)** بأضافة الحرف x تحت عمود **"u"** (المالك).	

9	أجعل الملف قابلا للقراءة فقط من قبل الجميع بأستخدام الامرchomd	
10	اعرض صلاحية الملف **myfile.txt**.	
11	للتأكد من معرفة صلاحية الملف، الرموز **-r--r--r--** يبين أن الملف قابل للقراءة من قبل الجميع.	
12	غير مالك الملف بأستخدام الأمر **chown** إلى مستخدم آخر **newuser** (نفّذ كـ **root**):	

أن هذا الأمر يُستخدم لتغيير مالك الملف **myfile.txt** إلى المستخدم الجديد **newuser**، ويتم تنفيذ الأمر بصلاحيات الجذر (**root**) بأستخدام الأمر **sudo** لأنه لا يُسمح للمستخدم العادي بتغيير ملكية الملفات التي لا يملكها.

13	تحقق من نتيجة التغيير بأستخدام الأمر **ls -l** ،وسيُظهر اسم المالك الجديد الآن هو **newuser**، وهذا يعني أن أي صلاحيات مخصصة للمالك أصبحت تنطبق عليه، بينما لم تتغير صلاحيات المجموعة أو الآخرين.	
14	غير مالك الملف والمجموعة بأستخدام الأمر **chown**.	
15	تأكد من تغير مالك الملف والمجموعة بأستخدام أمر **ls -l** لمشاهدة معلومات الملف بأن المالك الجديد هو **newuser** ومجموعة المالكة هو **newgroup** مع بقاء الصلاحيات.	

16	قم بإنشاء مجلد جديد بأسم **myfolder** وتطبيق صلاحيات بأستخدام الأمر **chmod** "قراءة، كتابة، وتنفيذ" للمجلد لصالح المالك فقط، ومنع أي صلاحيات عن المجموعة والآخرين.	
17	أكتب الأمر **ls -ld** لعرض معلومات عن صلاحيات المجلد. لاحظ عزيز الطالب أن الخانة الاولى من سطر الأمر الحرف **d** = يعني أن العنصر هو مجلد (**Directory**) وبقية خانات الرموز**rwx**= يعني للمالك صلاحية القراءة والكتابة والتنفيذ ولا يمكن للمجموعة والاخرين بذلك. والرموز ----= يعني لا يمكنهم حتى رؤية محتويات المجلد أو الدخول عليه.	
18	المناقشة • ما الفرق بين الأوامر **chmod** و **chown** ؟ ومتى نستخدم كل منهما ؟ • هل يمكن فتح أوتعديل ملف معطى له صلاحية تنفيذ فقط (X- -)؟	

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين: 4	
اسم التمرين: إعداد صلاحيات ملفات أومجلدات بأستخدام أوامرLinux				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب والوصول إلى نظام التشغيل **Linux**	%10		
2	مراحل تنفيذ إعداد صلاحيات الملفات بأستخدام أمر **chmod**	%10		
3	مراحل تنفيذ إعداد صلاحيات المجلدات بأستخدام أمر **chown**	%10		
4	المناقشة	%10		
5	الزمن المخصص	% 10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

2 حماية أنظمة التشغيل

رقم التمرين: 5 الزمن المخصص: ساعة واحدة

اسم التمرين: فحص حسابات المستخدمين باستخدام أداة الفحص **Nessus**

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

بعد إتمام هذا التمرين، سيتمكن الطالب من:

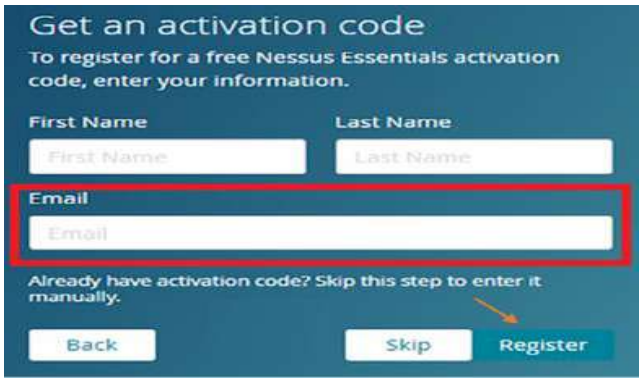
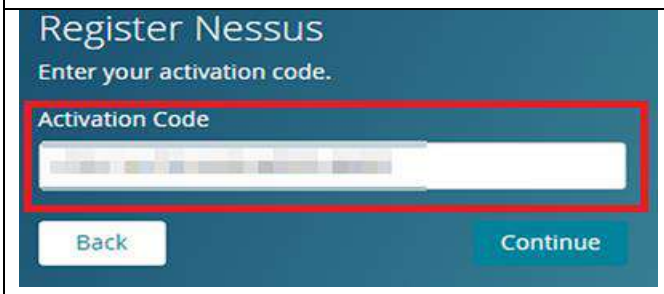
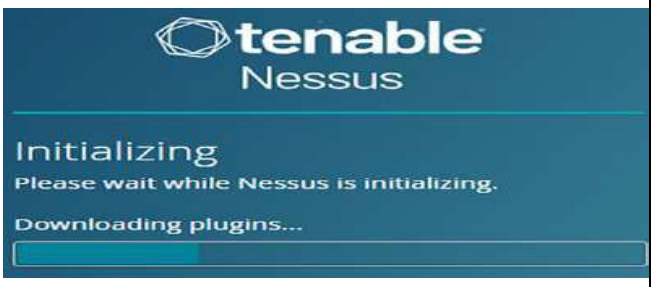
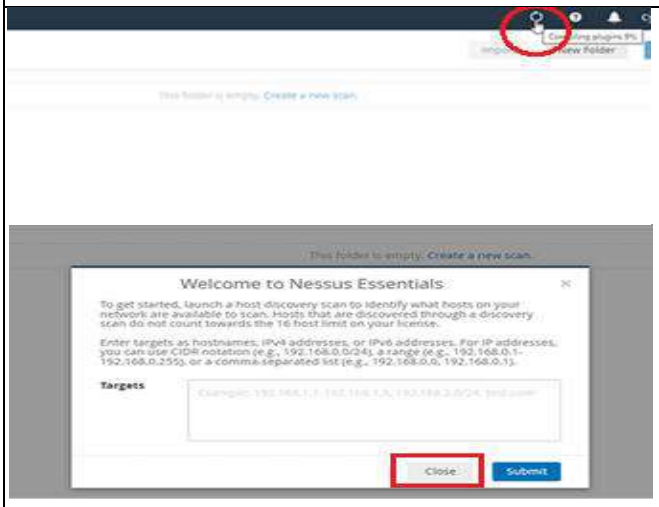
- التعرف على اعداد وتنصيب برنامج (**Tenable Nessus Essentials**)
- تطبيق أداة الفحص برنامج(**Nessus**) لكشف الحسابات غير الآمنة أوالمخترقة .
- تطبيق عملية اعداد كشف الحساب وتقييم مستوى خطورة الحساب ًوالتقرير بنتائج الفحص.

ثانياً: التسهيلات التعليمية

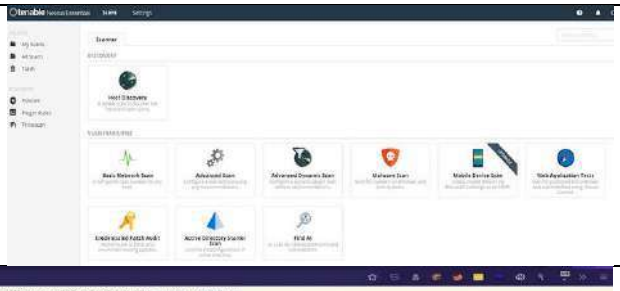
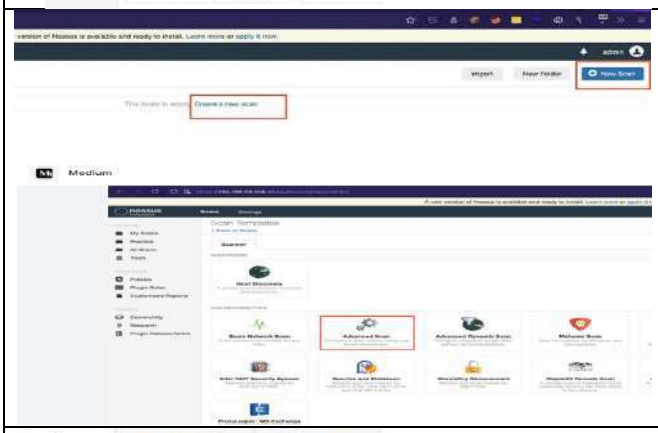
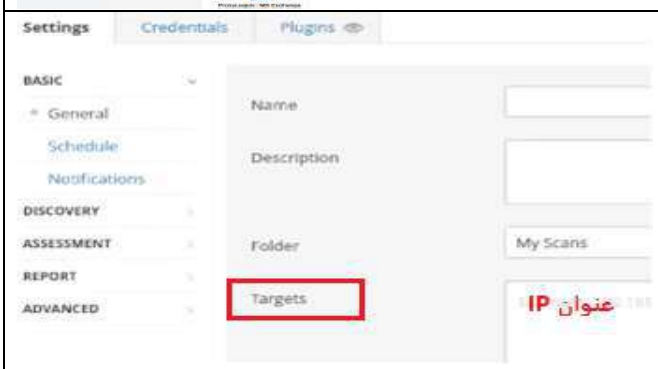
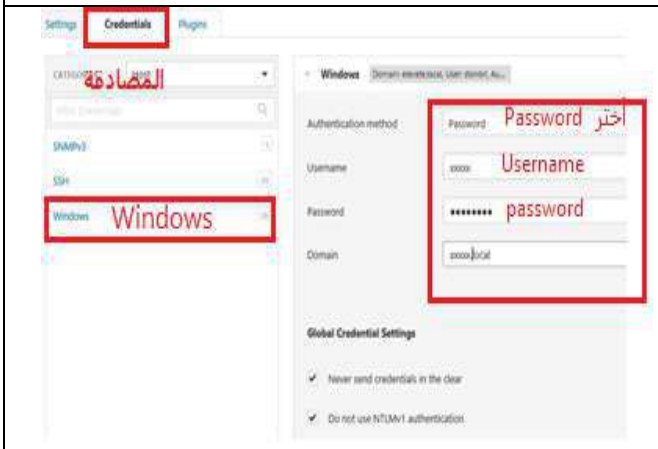
- أجهزة حاسوب يعمل بنظام تشغيل **Windows10** فما فوق.
- اتصال بالشبكة المحلية للوصول إلى الخوادم وأجهزة المستخدمين.
- حساب إداري لتنفيذ الفحص بأفضل أداء.
- برنامج (**Tenable Nessus Essentials**).

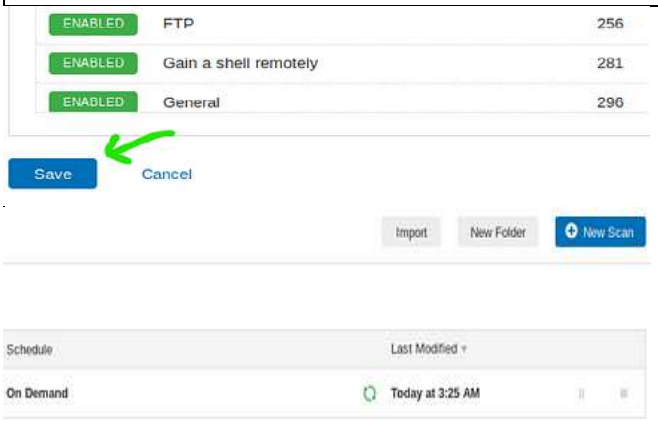
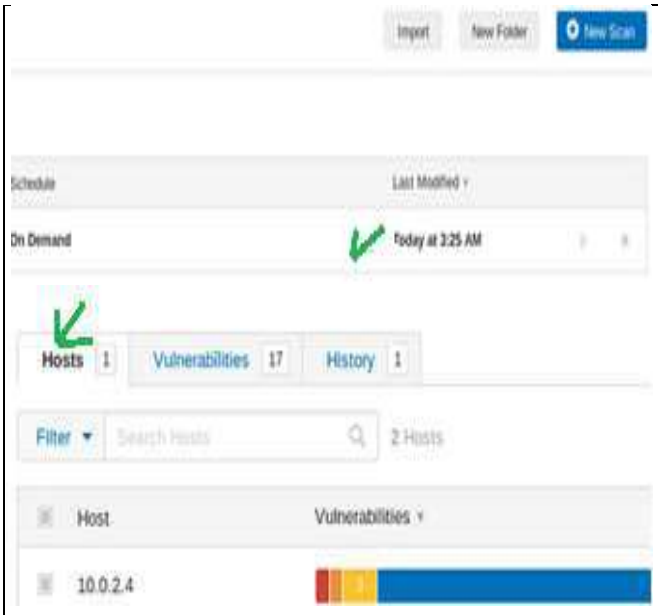
ثالثاً: خطوات تنفيذ التمرين:

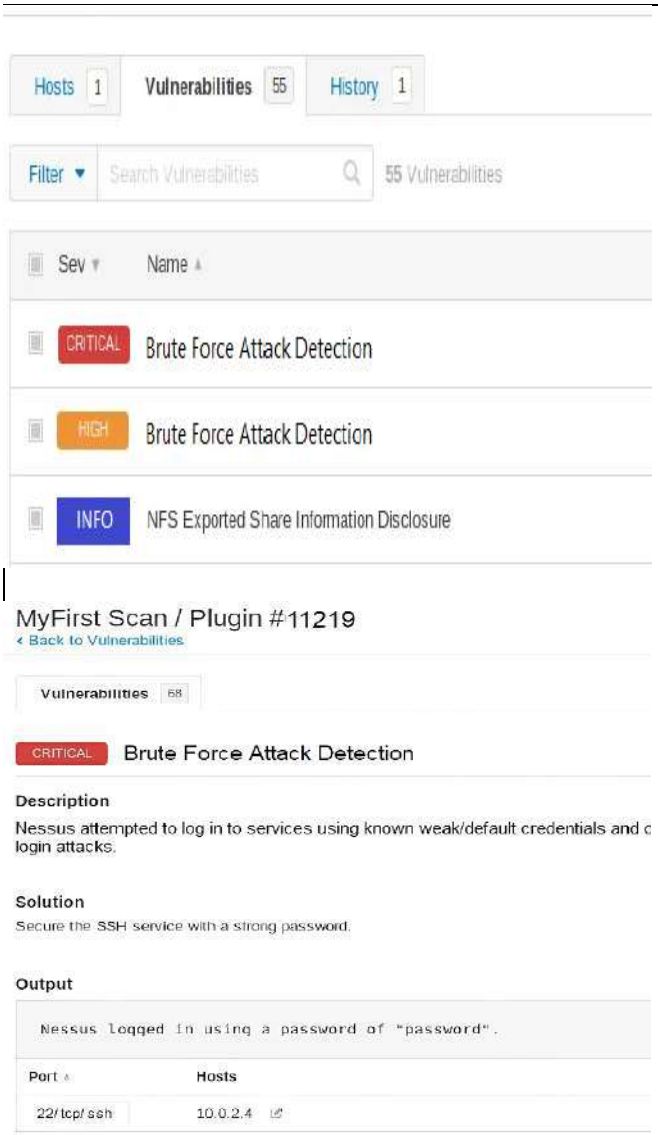
1	حمل نسخة حديثة من برنامج **Tenable Nessus Essentials** من الموقع الرسمي: **https://www.tenable.com/downloads/nessus** تأكد من تنزيل اصدار برنامج الفحص المناسب لنظام التشغيل.	

2	أدخل بريدك الإلكتروني للحصول على **Activation Code** مجانًا ثم إنقر **Register** كما موضح في الشكل.	
3	أدخل رمز التفعيل الخاص بك في حقل التفعيل.	
4	حمل البرنامج وثبته ستستغرق عملية التثبيت بعض الوقت	
5	بمجرد الانتهاء من ذلك، يجب أن ترى الصفحة الآتية مع السهمين اللذين يدوران في الزاوية اليمنى العليا. يقوم **Nessus** بتثبيت المكونات الإضافية، وسيتعين علينا الانتظار حتى اكتماله. ثم إنقر على الأمر **close**	

2 حماية أنظمة التشغيل

6	ستظهر واجهة البرنامج لبدء تحديد فحص جديد	
7	إنشأ فحص جديد للحسابات • انتقل إلى علامة التبويب **Scans** • إنقر على الأمر **New Scan** لأنشاء فحص جديد • اختر قالب الفحص المناسب	
8	أضف عنواناً للحاسبة المتصل بالشبكة المحلية المراد فحصها. • في حقل **Targets** ادخل عنوان **IP** أو نطاق عناوين الأجهزة المراد فحصها • أكتب في حقل **Targets** عنوان **IP** ليكن 10.0.2.4 أو 10.0.2.4/24	
9	فعل فحص المصادقة **Credentials** • انتقل إلى قسم **Credentials** في إعدادات الفحص. • اختر نظام التشغيل الفعلي المستخدم على حاسبة المضيف ليكن **Windows** • أختر **Password** من حقل **Authentication method** • أكتب اسم المستخدم وكلمة المرور في الحقول المخصصة للحساب الإداري. • أكتب اسم النطاق (**Domain**) إذا كان الجهاز ضمن **Active Directory**	 تلميح : إذا كان نظام التشغيل **Linux** على الحاسوب المضيف ، أختر **Linux/SSH** ثم اكتب اسم المستخدم وكلمة المرور

10	تخصيص الفحص عن فئة ثغرة معينة مثل ثغرة فحص كلمات المرور الضعيفة كما يأتي: • شغل (فعّل) التبويب **plugins** • أكتب اسم الاضافة وليكن **Brute Force Attack Detection**(لفحص كلمات المرور الضعيفة) عند البروتوكولات **HTTP Log in Forms,FTP,SSH,Telnet,** عندما تظهر الإضافة، اضغط على زر التفعيل (**Enable Plugin**) أن كانت غير مفعّلة.	
11	حفظ وتشغيل الفحص كما يأتي: • إنقر على **Save** وسيتم حفظ السياسة، ستمتلك سياسة الفحص الخاصة بك. ثم من قائمة الفحص، اضغط على زر **Run** ▶ لتشغيل الفحص.	
12	لاحظ النتائج وكما يأتي: • إنقر على الفحص • إنقر على تبويب **Host** سيظهر شريط تصنيف **Nessus** بألوان مختلفة فاللون الأحمر يمثل ثغرة ذات مستوى أعلى خطورة ، واللون البرتقالي يمثل ثغرة ذات مستوى عالية الخطورة أمّا اللون الأصفر فيمثل ثغرة ذات مستوى متوسطة الخطورة بينما اللون الأزرق معلومات غير مخترقة.	

	• إنقر على التبويب **Vulnerabilities** ستظهر جميع الثغرات الأمنية الموجودة في الجهاز حسب مستويات الخطورة، ويبين أن مستوى أعلى خطورة للثغرة هنا اذاكان الوصول للحساب ناجحا من قبل المهاجم ومستوى متوسط خطورة الثغرة إذا تم اكتشاف محاولات ولكنها لم تنجح. • إنقر على الثغرة ذات مستوى أعلى خطورة للاطلاع على تفاصيلها.	
13	حلل النتائج ركز على اسم الثغرة ووصفها وطريقة حلها، و المنفذ **Port** والمضيف الذي تم العثور على الثغرة الأمنية فيه. ثم يمكنك ايضا تصدير النتائج من خلال النقر على **Export** لحفظ التقرير بصيغة **PDF** لمشاركته مع فريق الأمن.	

14	المناقشة 1.ما أنواع نقاط الضعف التي يمكن لـ **Nessus** اكتشافها في الحسابات؟ 2.كيف تساعد نتائج **Nessus** في تصنيف الحسابات حسب مستوى الخطورة (مرتفع – متوسط – منخفض)؟ 3.ما فائدة دمج **Nessus** مع أنظمة مثل **Active Directory** في تحليل الحسابات؟ نشاط: • ما الخطوات التي يجب اتباعها لإنشاء فحص على شبكة داخلية محددةفي **Nessus** لتحليل الحسابات؟ ، ثم أجب: • كم حسابًا تم اكتشافه؟ • هل ظهرت تنبيهات مرتبطة بكلمات مرور ضعيفة أو صلاحيات زائدة؟ • هل لاحظت تسجيل دخول لحساب من عنوان **IP** غريب؟ ما هو؟ وما الإجراء المقترح؟ • كيف تصنف مستوى الخطورة لهذا الحساب؟ (🔴 مرتفع / 🟠 متوسط / 🟡 منخفض) ولماذا؟ • ما الإجراءات التي تقترحها للتعامل مع هذا الحساب؟ (اختر من: إعادة تعيين كلمة المرور – تقليل الصلاحيات – حذف الحساب – مراقبته فقط)

التنمية المستدامة تبدأ من وعيك.

كن جزءًا من الحل، لا من المشكلة.

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:5	
اسم التمرين: فحص حسابات المستخدمين بأستخدام أداة الفحص **Nessus**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب وتحميل البرنامج	%10		
2	تثبيت البرنامج	%10		
2	مراحل تنفيذ إعدادات الفحص	%10		
4	المناقشة	%10		
5	الزمن المخصص	% 10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

2 حماية أنظمة التشغيل

رقم التمرين: 6 الزمن المخصص: ساعة واحدة

اسم التمرين: إنشاء وادارة سياسات المجموعات **(GPO) في Windows Server**

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

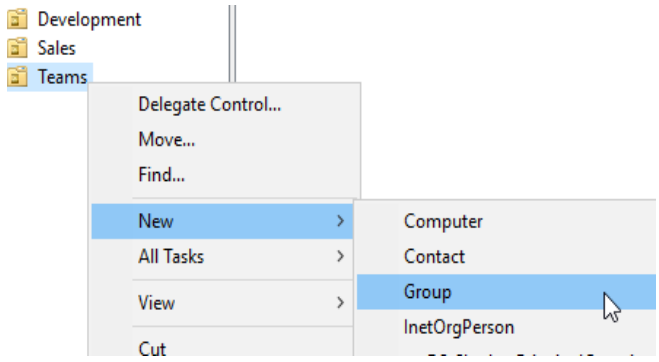
بعد إتمام هذا التمرين، سيتمكن الطالب من:

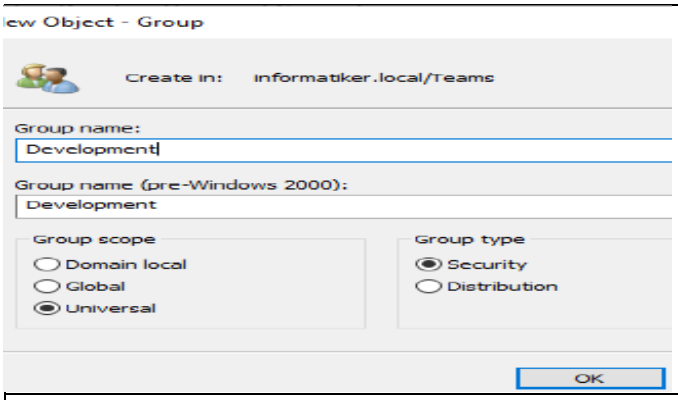
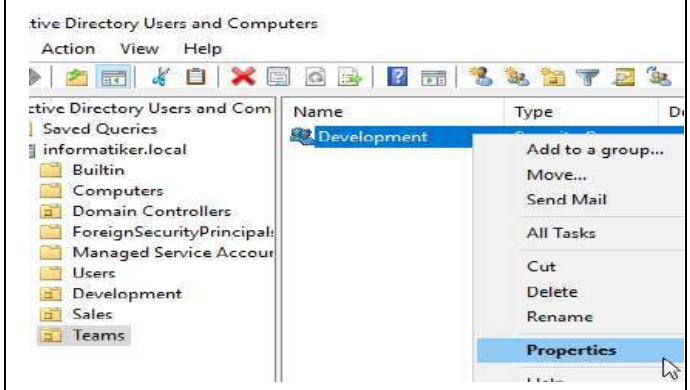
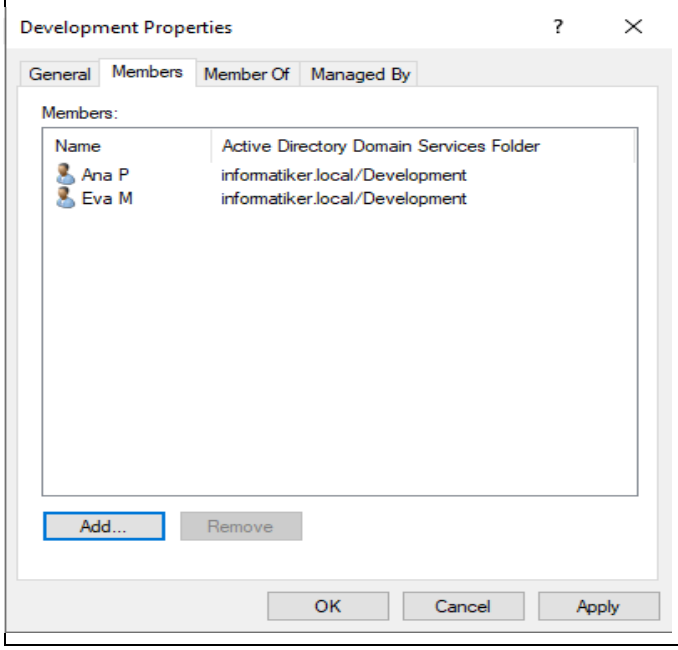
- تطبيق عملية إنشاء وادارة سياسة المجموعات **Group Policy** في النظام **Windows Server** لتعزيز الأمان والتحكم في صلاحيات المستخدمين والتطبيقات.
- تطبيق سياسة قفل الحساب على نظام **Windows server.**

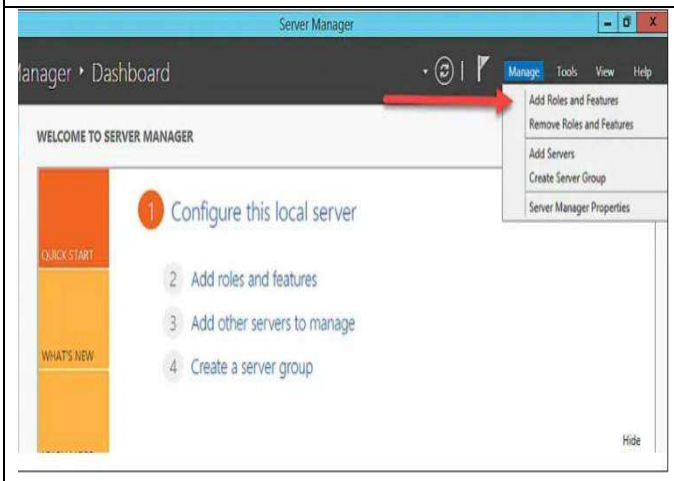
ثانياً: التسهيلات التعليمية

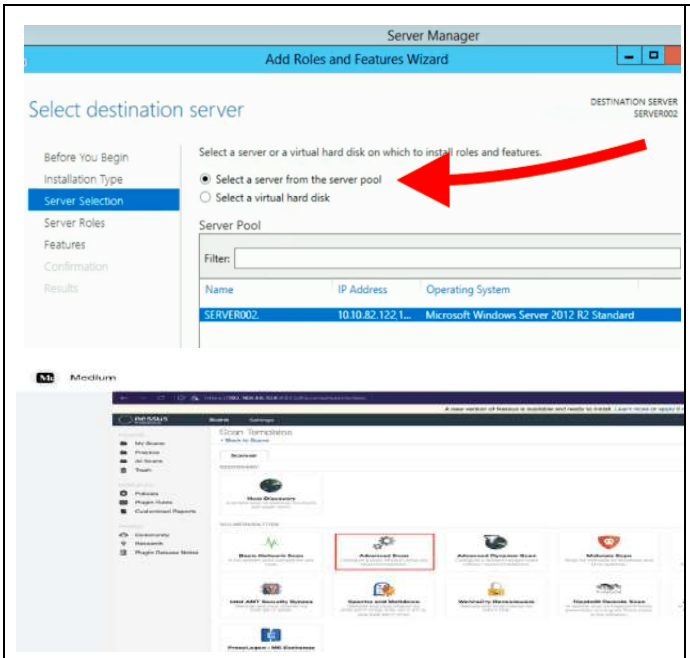
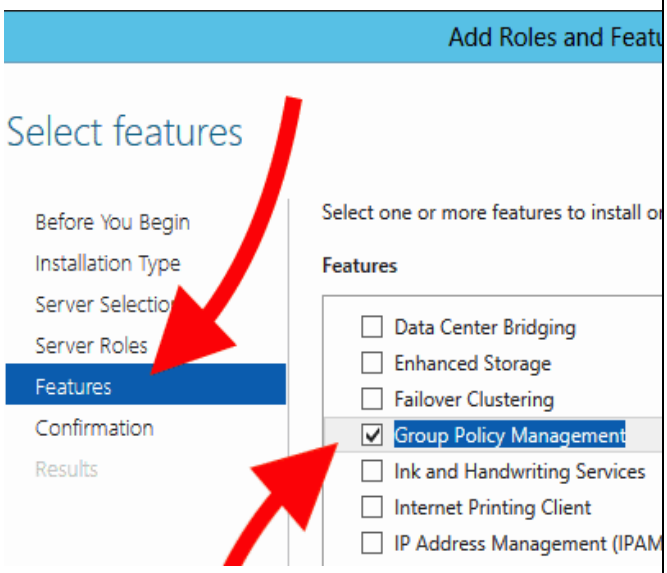
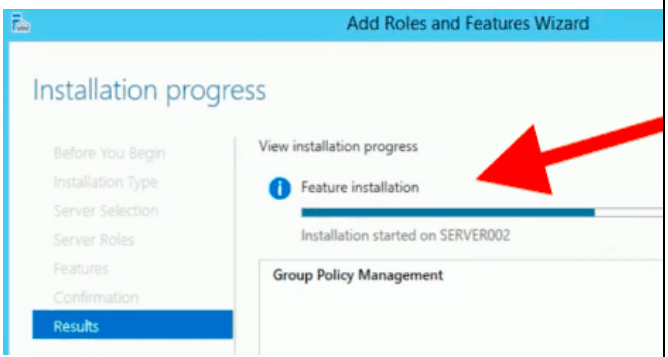
- جهاز يعمل بنظام **Windows Server 2019/2022** مع خدمات **Active Directory.**
- جهاز عميل منضم إلى نفس المجال **(Windows 10/11)** .
- حساب مسؤول **(Admin)**

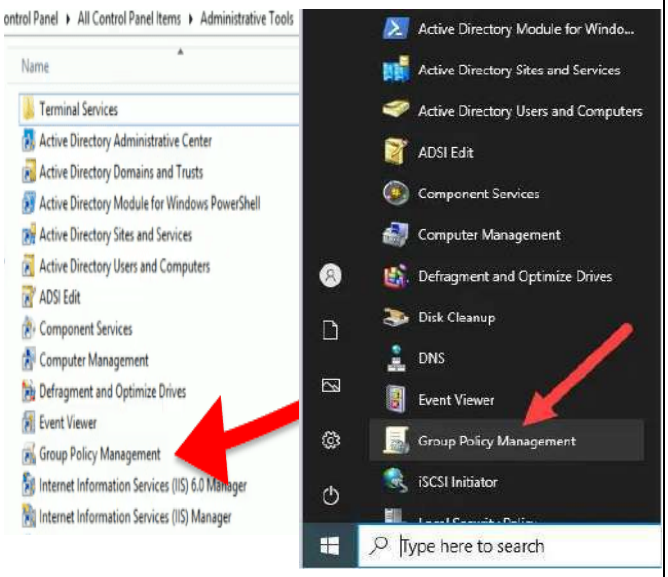
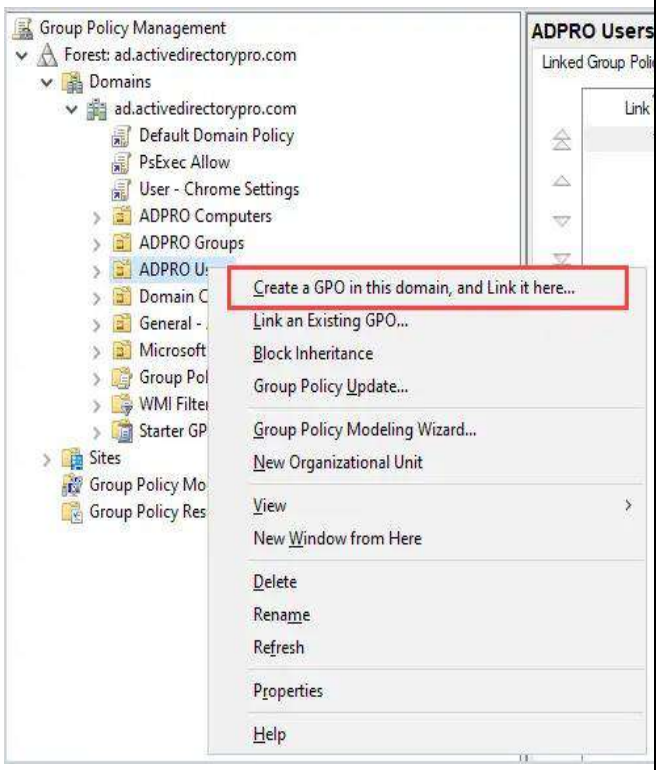
ثالثاً: خطوات تنفيذ التمرين:

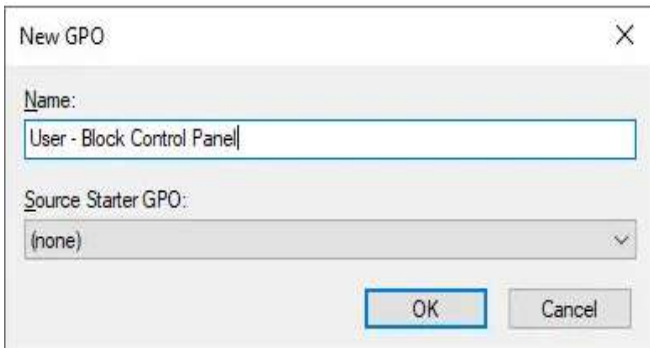
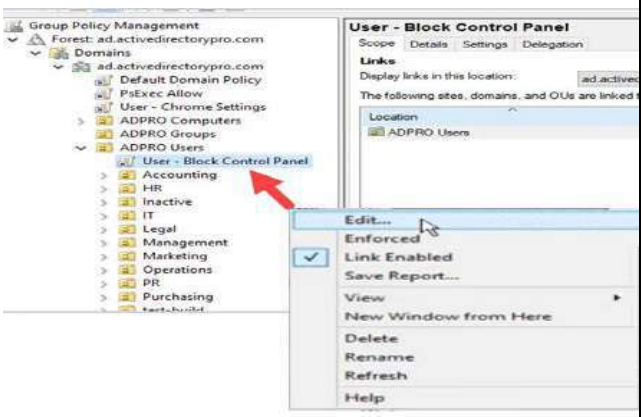
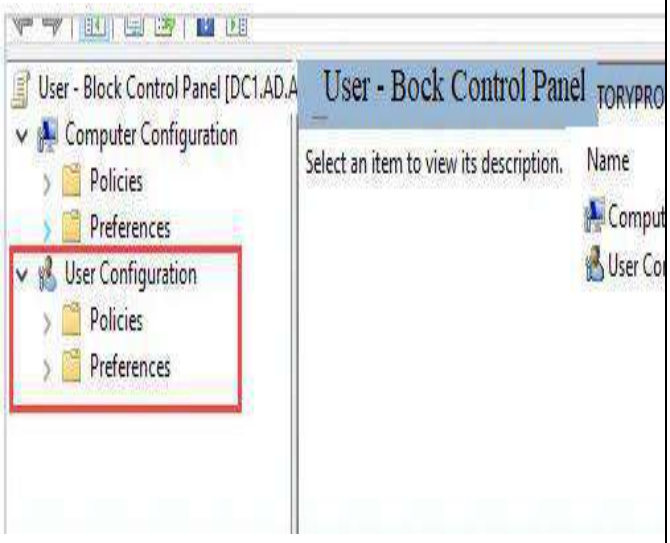
1	افتح أداة إدارة السياسات **Group Policy)** **(Management** في **windows server** وقم بإنشاء مجموعة • إنشيء وحدة تنظيمية **Teams**، ثم إنقر بزر الفأرة الأيمن عليها **New>** **Group** • تعيين اسم المجموعة: سأُعيّنها كمجموعة **Development**. يجب أن يكون نوع نطاق المجموعة **"Universal"** ونوع المجموعة **"Security".**	

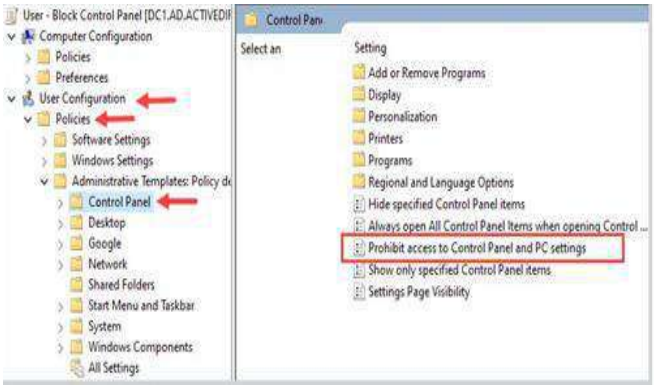
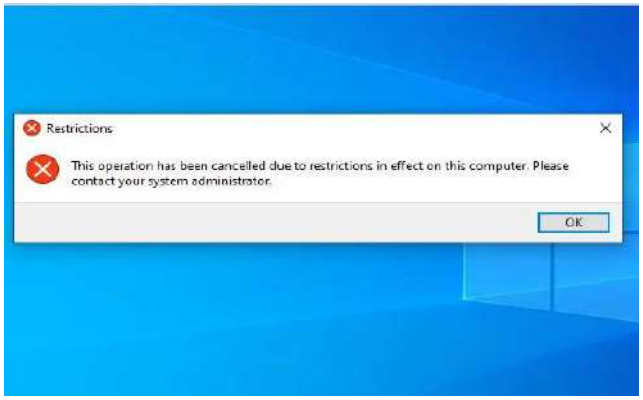
	إنقر على موافق **OK**.	
2	أضف الأعضاء إلى المجموعة. • إنقر بزر الفأرة الأيمن على المجموعة **Development** أو المجلد الذي يحتوي على المجموعة التي تم إنشاؤها وحدد خصائص **(Properties)**	
3	انتقل إلى تبويب **"Members "** وأنقر على **Add** وأدخل اسم المستخدم **Ana** من وحدة التنظيمية **Development** **OU** لإضافتهما إلى مجموعة **Development Group** أكد ذلك بـ **OK** > **Apply** كرر العملية وأضف ايفا **Eva** كعضو في المجموعة **Development**. ستظهر النافذة الآتية كنتيجة نهائية للتأكد من مشاهدة إتمام إضافة الأعضاء أنفسهم.	

4	ثبت وحدة التحكم في إدارة سياسة المجموعة لانشاء **GPO** جديدة كما يأتي: شغّل " **Server Manager** " بإحدى الطرق الآتية: • إنقر على أيقونة " **Server Manager**" في شريط المهام، كما هو موضح أدناه: • إنقر على زر "**Start**" في نظام التشغيل **Windows** واكتب " **Server Manager**" في مربع البحث.ثم إنقر على أيقونة "**Server Manager**".	
5	لفتح المعالج، إنقر على **Add roles and features**.	
6	إنقر على "**Next**" للمتابعة.	

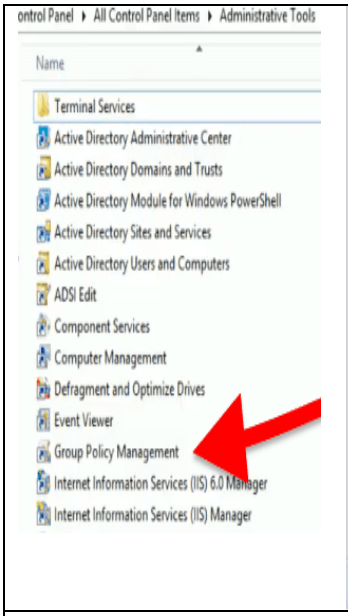
7	سيفتح **Add Features and Roles Wizard** اترك "**Installation Type**" على القيمة الافتراضية: "**Role-based or Feature-based installation**".	
8	تخطّ **Server Roles** وانتقل إلى "**Features**". في قسم "**Features**" ستجد أداة "**Group Policy Management**" فعِّل المربع، ثم إنقر على "**Next**" ثم إنقر على "**Install**".	
9	ينبغي أن تستغرق عملية التثبيت بضعة دقائق حتى تكتمل.	

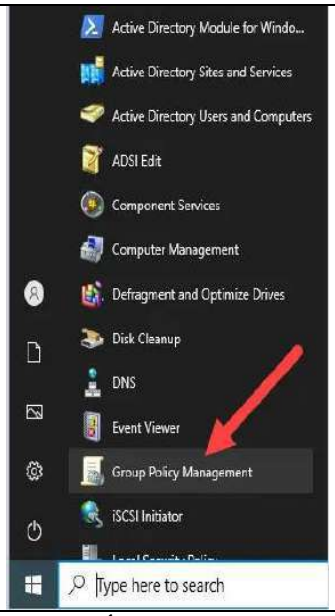
10	إنشاء **GPO** (**Group Policy Objects**) الجديدة وكما يأتي :- إفتح **Group Policy Management** من خلال الضغط **Win + R** وأكتب "**Administrator Tools**" ، ابحث عن " **Group Policy Management Console**"	
11	• أختر وحدة تنظيمية (**OU**) أو **Domain** وبالاخص ابحث عن الوحدة التنظيمية التي تحتوي على حسابات المستخدم الخاصة بك كما انشأته في الخطوة السابقة اسمها (**Development**)، بالنسبة لي وحدتي التنظيمية هنا اسمها " **ADPRO Users**" • إنقر بزر الفأرة الأيمن على الوحدة التنظيمية وحدد "**Create a GPO in this domain, and Link it here**"	

12	أعطِ اسمًا لـ **GPO** الجديد. على سبيل المثال، " **User – Block Control Panel**" ثم إنقر على **OK**.	
13	إنقر على الأمر **Edit** في هذه المرحلة، يوجد كائن سياسة مجموعة (**GPO**) جديد مرتبط بجميع المستخدمين، ولكن لا توجد سياسات مُحددة له.	
14	لذا يتم تحديد سياسة للمجموعة الجديدة " **User – Block Control Panel**" عدل الإعدادات تحت :- • **Computer Configuration** • **User Configuration** سيتم فتح إدارة سياسة المجموعة **User - Block Control Panel**" تلقائيًا في المحرر في نافذة جديدة.	

15	انتقل إلى تكوين المستخدم -> **Policies** <- **Administrative Templates** <- **Control Panel**	
16	إنقر بزر الفأرة الأيمن على السياسة (**Policy**) وحدد **"Edit"**. • قم بتغيير إعداد السياسة إلى "Enabled(تمكين)" ثم إنقر فوق **"OK"**	
17	للتأكد من عمل**GPO** ، أعد تشغيل الكمبيوتر(**Reboot a computer**) وسجّل الدخول بأستخدام حساب مستخدم نطاق (**domain user account**). عند محاولة فتح لوحة التحكم، ستظهر لك رسالة تعني"لا يمكنك الوصول إلى تطبيق لوحة التحكم " كما موضح في الشكل جانبا.	 تذكر أن هذا كان **user configuration** وينطبق فقط عندما يقوم المستخدم بتسجيل الدخول (**user logs**) إلى الكمبيوتر.

18	لحماية **Active Directory** في حال تعرضها لهجمة **Brute Force** قم بعزل الحساب المخترق بواسطة إنشاء سياسة قفل الحساب كما يأتي: a. أفتح أداة **Group Policy Management Console (GPMC)**.

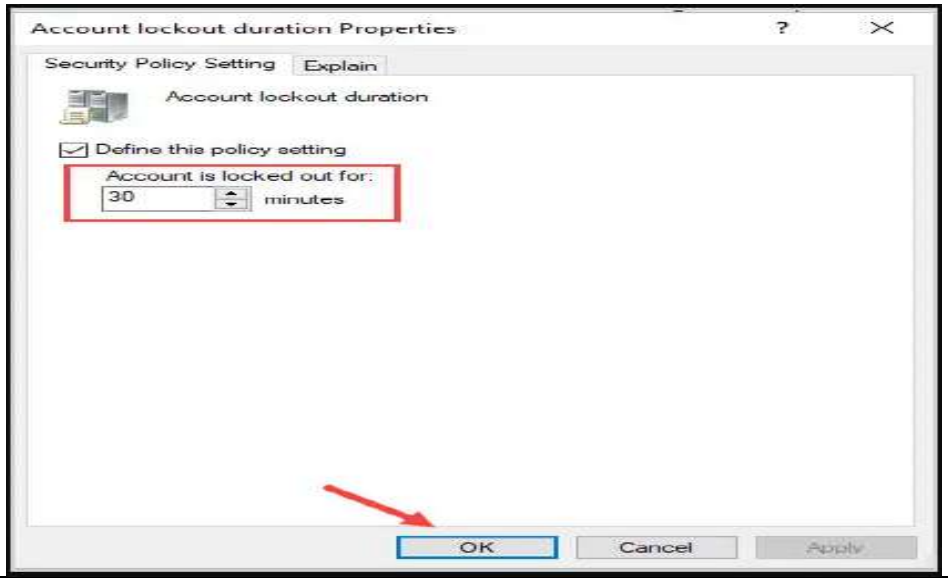




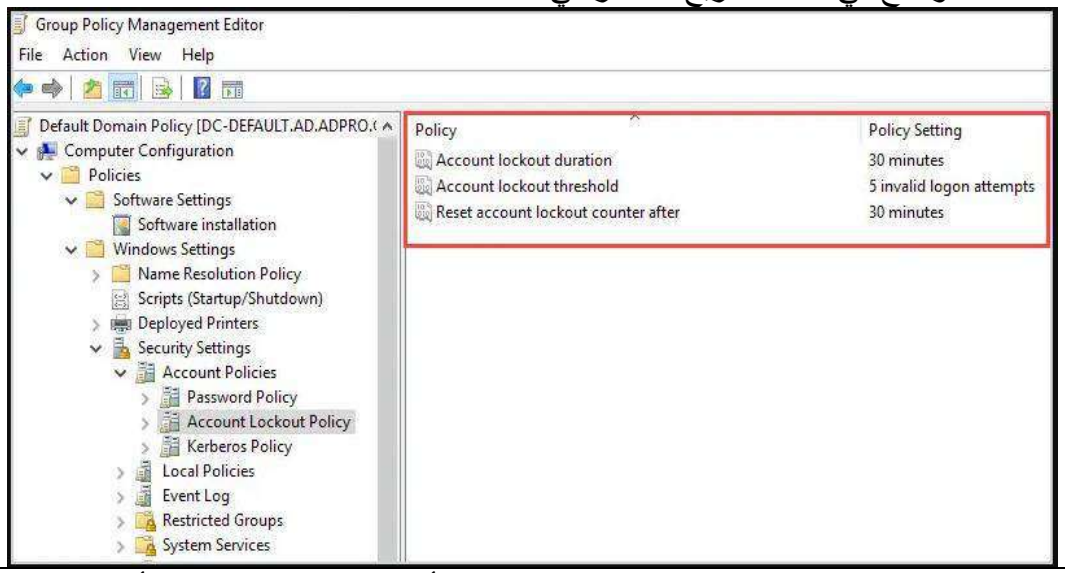
b. تعديل سياسة **Account Lockout Policy** كما يأتي: من **Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Account Lockout Policy**.

قم بتحديد الإعدادات الآتية:

- ✓ **Account lockout threshold**: عدد المحاولات الفاشلة قبل القفل (مثال: 3 محاولات).
- ✓ **Account lockout duration**: مدة القفل (مثال: 30 دقيقة).
- ✓ **Reset account lockout counter after**: الوقت قبل إعادة تعيين العداد (مثال: 15 دقيقة). لتعديل كل إعداد سياسة، إنقر نقرًا مزدوجًا عليها لتعديل إعداداتها. على سبيل المثال، فتحتُ "مدة قفل الحساب"، وأدخلتُ 30، ثم نقرتُ على "موافق".وكما موضح في الشكل ادناه :-

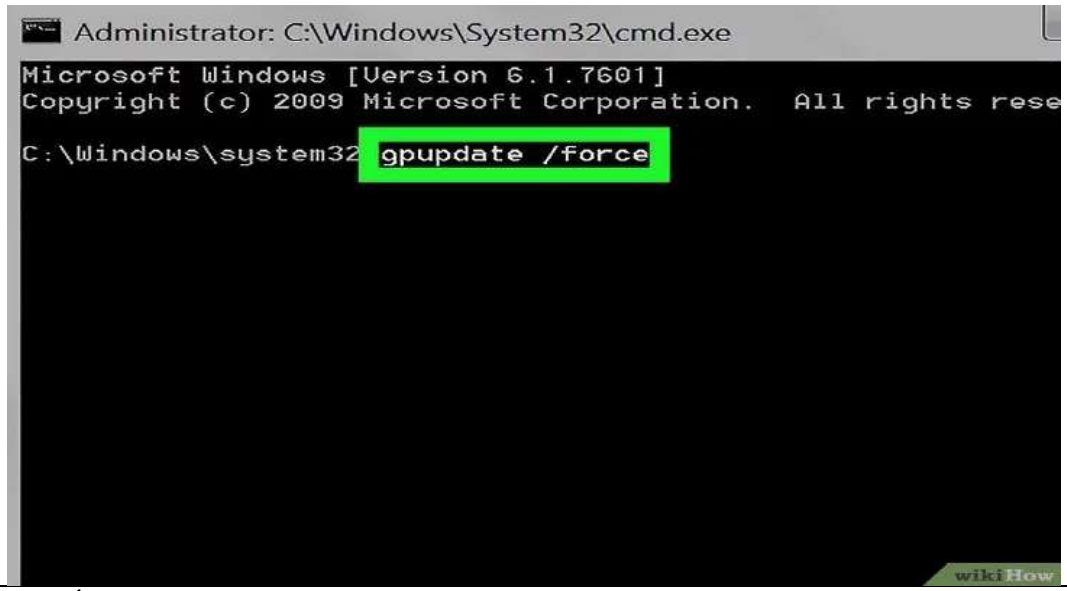


وبعد تعيين جميع إعدادات السياسة الثلاثة ستظهر تلك قيم الإعدادات مثبتة لكل إعداد كما موضح في داخل المربع الاحمر في الشكل ادناه :-



قم بالبحث عن **Command Prompt** في قائمة ابدأ، ثم إنقر بزر الماوس الأيمن واختر **Run as administrator**

c. حدث **GP** يدوياً بكتابة الأمر **gpupdate /force** في سطر الاوامر عن طريق فتح موجه الاوامر **cmd** كمسؤول **Admin** وبعد كتابة الأمر اضغط **Enter**



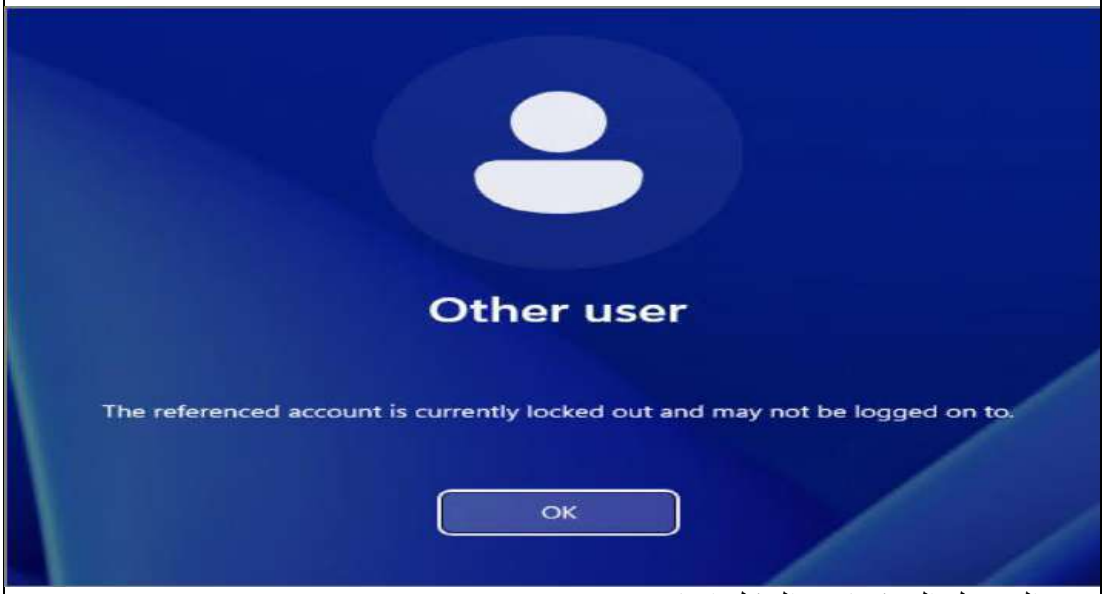
d. قم باختبار السياسة قفل الحساب المخترق بمحاولات تسجيل دخول فاشلة لرؤية تأثير القفل. وكما موضح في الشكل ادناه :-

حاول أن تكتب اسم المستخدم وكلمة المرور غير صحيحة

ستضهر هذه الرسالة النصية " **The user name or password is in correct. Try again**" تخبرك بأن محاولتك دخول الحساب كانت فاشلة عن طريق ادخال أسم المستخدم وكلمة المرور غير صحيحة. حاول مرة ثانية

e. ثم إنقر على **OK**

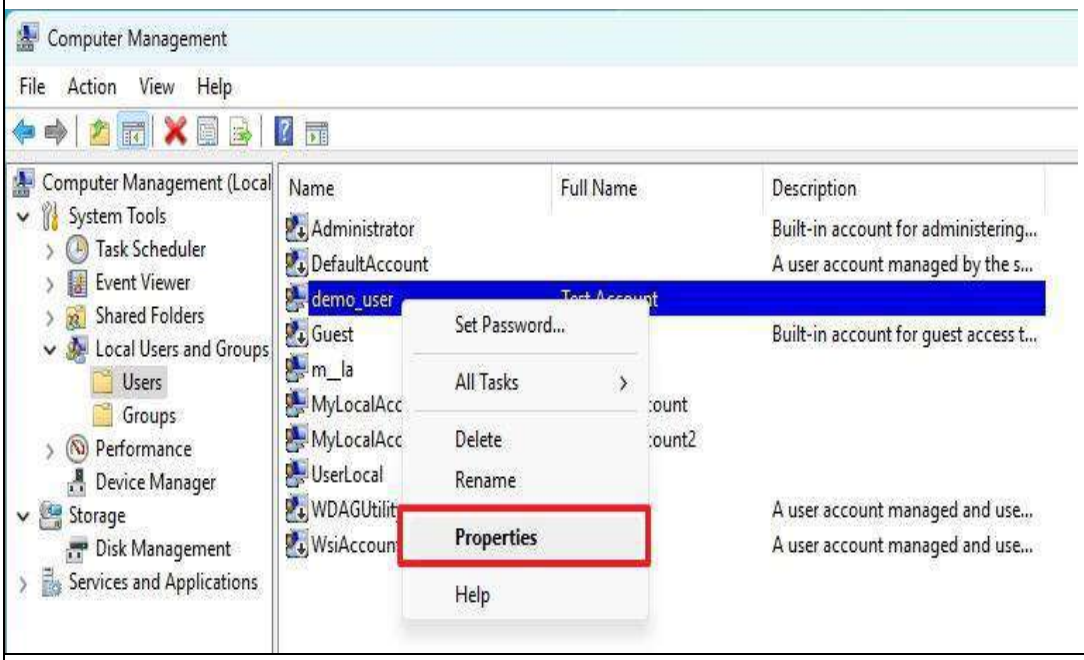
f. كرر هذه العملية ثلاث مرات بمحاولات دخول فاشلة فعند المحاولة الرابعة ستظهر لك هذه الرسالة النصية " **The refrenced account is currently lookout and may not be logged on to**" يشير إلى حساب المستخدم مغلق حالياً وقد لا يتم

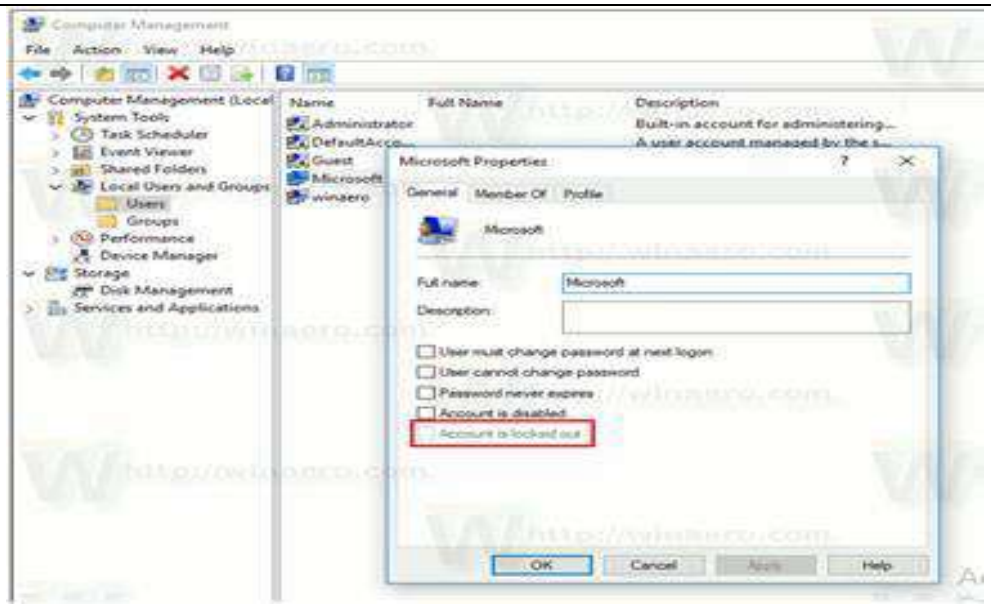


التسجيل إليه كما في الشكل ادناه:-

g. إنقر على **OK**

والان الحساب مغلق ولن تتمكن من تسجيل الدخول إلى جهاز الحاسوب حتى وان ادخلنا اسم مستخدم وكلمة مرور صحيحة

19	h. لتسجيل الدخول إلى جهاز الحاسوب مرة اخرى كما يأتي :- ✓ قم بألغاء قفل الحساب المستخدم أفتح **Start** واختر **Computer Management** ✓ انتقل إلى المسار الآتي: **Computer Management > System Tools > Local Users and Groups > Users** ✓ إنقر بزر الماوس الأيمن فوق المستخدم وحدد خيار الخصائص **Properties**. 
20	✓ إنقر فوق علامة التبويب **General**. ✓ قم بازالة تحديد خيار**Account is locked out** بمعنى تم الغاء قفل الحساب كما موضح في الشكل ادناه :- ✓ إنقر على **Apply** ✓ إنقر على **OK** بالتالي يمكن المستخدم من تسجيل الدخول إلى جهاز الحاسوب مرة أخرى



19

المناقشة:

1. ما أهمية إنشاء سياسات المجموعات؟
2. لو كنت مسؤول نظام في مختبر حاسوب مدرسي، ما هي السياسات التي ستطبقها لحماية الأجهزة؟
3. ما الذي يحدث عند ربط أكثر من **GPO** بوحدة تنظيمية واحدة؟ أي **GPO** يتم تطبيقه أولًا؟

نشاط:

عزيزي الطالب، قم بإنشاء **GPO** على وحدة تنظيمية تُسمى (طلاب التدريب)، بحيث تقوم بـ:

منع الوصول إلى لوحة التحكم (**Control Panel**).

- بعد ذلك، قم بإنشاء **GPO** مماثلة ولكن بأستخدام **Local Group Policy** على جهاز مستقل (ليس عضو في الدومين).
- الآن، قيم الفرق بين الطريقتين من حيث:
  - ✓ مستوى التطبيق (محلي أم مركزي؟).
  - ✓ سهولة الإدارة والتحديث.
  - ✓ مدى الأمان في البيئات الكبيرة.
  - ✓ حالات الاستخدام المناسبة لكل نوع.

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:6	
اسم التمرين: إنشاء وادارة سياسات المجموعات (GPO) في **Windows Server**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب والوصول إلى الإعدادات المطلوبة	%10		
2	مراحل تنفيذ إنشاء سياسة المجموعات (GPO)	%10		
3	مراحل تنفيذ تثبيت وحدة التحكم في إدارة سياسة المجموعة	%10		
4	المناقشة	%10		
5	الزمن المخصص	% 10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

أسئلة الفصل الثاني

س1:- عرف ما يأتي:

1- إدارة حساب المستخدم 2- مبدأ أقل الصلاحيات 3- تقييم خطورة الحساب

س2:- املا الفراغات الآتية بما يناسبها:

1. الصلاحيات الثلاثة الأساسية في نظام **Linux** هي .....و.....و.....
2. لتغيير صلاحيات الوصول إلى ملف معين نستخدم الأمر.....
3. من أفضل الممارسات الأمن ية هو تقليل ..... الممنوحة للمستخدمين لتقليل المخاطر.
4. يتم إستخدام الأمر ..... لتغيير مالك الملف أو المجلد.
5. يسمى النظام الذي يسمح لمالك المورد بالتحكم في من يمكنه الوصول إليه بـ . . . . .
6. من عيوب نموذج **DAC** أنه قد يؤدي إلى ..... إذا لم تتم إدارته بشكل جيد.

س3:- قارن بين أنماط التحكم في الوصول **DAC** و **MAC** و **RBAC** من ناحية طريقة إدارة الصلاحيات، مستوى الأمان ، مع ذكر مثال عملي لكل منها.

س4:- ما الفرق بين الحساب العادي والحساب الإداري من حيث الصلاحيات وإمكانية التحكم في إعدادات النظام؟

س5:- اعطِ مثالًا من الحياة اليومية يوضح تطبيق مبدأ أقل الصلاحيات.

س6:- ما هي معايير تقييم خطورة الحساب؟

س7:- كيف يمكن إستخدام سجلات الدخول في نظام المدرسة لاكتشاف الحسابات غير الآمنة؟ س8:- اذكر بعض الأنماط التي قد تشير إلى اختراق الحسابات وكيف يمكن التعامل معها بشكل فعال.

س9:- ما هي الصلاحيات الممنوحة للمستخدم عند تعيين قيمة **chmod 755** لملف؟ اشرح كيف تؤثر هذه الصلاحيات على الوصول إلى الملف.

س10:- ما هو تصنيف مستويات الخطورة للمستخدمين؟ وضح ذلك مع ذكر مثال لكل نوع.

الفصل الثالث

حماية الاتصال و أنظمة التشغيل

Securing Communication and Operating Systems

أهداف الفصل الثالث

1. التعرف على أدوات وتقنيات تأمين الاتصال في أنظمة التشغيل.
2. فهم أهمية جدران الحماية وآلية عملها.
3. اكتساب القدرة على حماية بروتوكولات الاتصال المستخدمة في الأنظمة.
4. تعلم تحليل حركة البيانات للكشف عن الأنشطة المشبوهة.

محتويات الفصل الثالث

(3-1) مفهوم تأمين الاتصالات في أنظمة التشغيل.

(3-2) إعداد جدران الحماية لتأمين الاتصالات الواردة والصادرة.

(3-3) حماية بروتوكولات الاتصال مثل **SSH** و **HTTPS** .

(3-4) تحليل حركة البيانات لفهم الأنشطة المشبوهة.

(3-5) أدوات لمنع الهجمات المرتبطة بالاتصالات والبروتوكولات.

تمرين (7) إعداد جدار حماية مدمج في نظام **Windows**

تمرين (8) مراقبة وتحليل حركة البيانات بأستخدام **Wireshark**

تمرين (9) إعداد نظام حماية من التهديدات الموجهة للاتصال بأستخدام **Comodo Firewall**.

الفصل الثالث

حماية الإتصالات وأنظمة التشغيل

Securing Communication and Operating Systems

تمهيد

تُشكّل الاتصالات الرقمية البنية الأساسية لعالمنا المعاصر، حيث أصبحت الشبكات جزءًا لا يتجزأ من أنظمة التعليم والعمل والتواصل والإدارة. هذا الاعتماد الواسع على الاتصال الشبكي يستدعي مستوى عاليًا من الحماية، خاصةً مع تزايد التهديدات السيبرانية التي تستهدف البيانات أثناء انتقالها بين الأجهزة حيث لم تعد الحماية مقتصرة على إستخدام برامج خارجية فحسب، بل غدت أنظمة التشغيل نفسها مزوّدة بأدوات داخلية متقدمة تُمكّن المستخدم من مراقبة وتنظيم حركة البيانات والتحكم بها. يُسلّط هذا الفصل الضوء على المفاهيم الأساسية لتأمين الاتصالات داخل أنظمة التشغيل، ويستعرض الأدوات المستخدمة لتحليل الحزم، وحماية البروتوكولات، واكتشاف الأنشطة المشبوهة، في إطار منهجي يجمع بين النظرية والتطبيق العملي.

(3- 1) مفهوم تأمين الاتصالات في أنظمة التشغيل

في عصر أصبحت فيه الاتصالات الرقمية جزءًا أساسيًا من الحياة اليومية، لم يعد إستخدام الشبكات أمرًا اختياريًا، بل ضرورة لا غنى عنها في التعليم والعمل والتواصل. ومع هذا الانتشار الواسع، ظهرت الحاجة إلى تأمين الاتصالات داخل أنظمة التشغيل التي نستخدمها على أجهزتنا، سواء كانت حواسيب مكتبية أو محمولة أو قد تكون هواتف ذكية. يُقصد بتأمين الاتصالات في أنظمة التشغيل هو عملية تنظيمية وتقنية تهدف إلى حماية البيانات أثناء تنقلها عبر الشبكة من الاختراق أو التعديل أو الوصول غير المصرح به، بأستخدام أدوات داخل نظام التشغيل نفسه.

تُظهر أنظمة التشغيل الحديثة مثل **Windows** و **Linux** و **macOS** قدرة متقدمة في مراقبة الاتصالات والتحكم بها، إذ تقوم بدور أساسي في منع البرامج الضارة من إستخدام الشبكة للانتقال أو سرقة المعلومات. ومن المهم أن نفهم أن تأمين الاتصال لا يقتصر فقط على إستخدام برامج خارجية، بل هو جزء من بنية نظام التشغيل نفسه، إذ توفر هذه الأنظمة أدوات داخلية تمنح المستخدم التحكم الكامل في نوع الاتصال، وجهته، ووقته، وما إذا كان آمناً أو لا. من أبرز آليات تأمين الاتصال في أنظمة التشغيل:

1. إستخدام جدران الحماية لمنع الاتصالات غير الموثوقة.
2. تحليل سلوك الشبكة واكتشاف محاولات التسلل أو الأنشطة الغريبة.
3. تحديد الصلاحيات ومنح التطبيقات الموثوقة فقط إمكانية الوصول إلى الإنترنت.

4. تحديث النظام باستمرار لتصحيح الثغرات الأمنية التي قد تُستغل في الاتصال

ويُلاحظ أن التطور في أدوات تأمين الاتصال داخل أنظمة التشغيل يتجه نحو الدمج بين الأمن الاستباقي (**Proactive Security**) القائم على التنبؤ وتحليل السلوك، وبين الأمن التفاعلي (**Reactive Security**) الذي يتعامل مع الحوادث بعد وقوعها. وهذا الدمج يتطلب تصميمات معمارية متقدمة داخل نواة أنظمة التشغيل (**Kernel-level Security**) لضمان معالجة فعالة في الوقت الحقيقي، دون التأثير الكبير على أداء النظام.

وفي ضوء ما تقدم، يمكن القول أن أمن الاتصالات لم يعد وظيفة خارجية تعتمد على أجهزة أو برامج إضافية، بل أصبح مكونًا جوهريًا في تصميم وتطوير أنظمة التشغيل الحديثة، في ظل الحاجة المتزايدة إلى بيئات تشغيل قادرة على الصمود أمام التهديدات المعقدة والمستمرة.

(2-3) إعداد جدران الحماية لتأمين الاتصالات الواردة والصادرة

تُعد جدران الحماية (**Firewalls**) من الأدوات الأساسية التي يعتمد عليها نظام التشغيل لحماية الجهاز من التهديدات التي قد تدخل أو تخرج عبر الشبكة , ويُحدد ما إذا كانت البيانات المرسلة أو المستقبلة مسموحًا بها أو لا، بناءً على مجموعة من القواعد والإعدادات.

يقصد بجدار الحماية (**Firewall**) هو نظام أمني رقمي وظيفته الأساسية هي مراقبة وتنظيم حركة البيانات بين الجهاز والشبكات الأخرى، سواء كانت هذه البيانات واردة إلى الجهاز أو صادرة منه. يعمل هذا النظام وفق قواعد يحددها المستخدم أو نظام التشغيل، تهدف إلى السماح فقط بالاتصالات الموثوقة ومنع الاتصالات المشبوهة أو الضارة. تمثل الوظيفة الرئيسية لجدار الحماية في تنظيم الاتصالات الواردة والصادرة، وهما نوعان من حركة البيانات يجب فهم الفرق بينهما:

1. الاتصالات الواردة: هي البيانات التي تأتي إلى الجهاز من مصدر خارجي، مثل حزمة بيانات تصل من الإنترنت إلى الحاسوب. هذه الاتصالات قد تحمل مخاطر في حال كانت من مصادر مجهولة أو مشبوهة، لذا يقوم جدار الحماية بفحصها قبل السماح بها.
2. الاتصالات الصادرة: هي البيانات التي يرسلها الجهاز إلى جهة خارجية، مثل طلب اتصال بموقع ويب. أحيانًا، قد تحاول برامج ضارة إرسال بيانات من الجهاز إلى خوادم مخترقة، وهنا تتجلى أهمية مراقبة الاتصالات الصادرة لمنع التسرب المعلوماتي.

من الناحية التقنية، يعمل جدار الحماية على فحص كل حزمة بيانات (**Packet**) تمر عبره ويتم ذلك عن طريق مجموعة من القواعد المنظمة (**Rules**) التي تحدد آلية السماح أو الحظر لكل اتصال ويتحقق من مجموعة من المعلومات المرافقة لها، مثل:

- عنوان المصدر (**Source IP Address**): من أين جاءت البيانات؟
- عنوان الوجهة (**Destination IP**): إلى أين تتجه البيانات؟
- نوع البروتوكول المستخدم (مثل **TCP** أو **UDP**).

- رقم المنفذ (**Port Number**): هل المنفذ مفتوح ومسموح به؟
- اتجاه الاتصال: أ هو دخول (**Inbound**) أم خروج (**Outbound**)؟

إذا كانت هذه البيانات تطابق القواعد الآمنة، فإن جدار الحماية يسمح بمرورها. وإذا كانت مشبوهة أو غير مصرّح بها، فإنه يمنعها ويقوم بتسجيل ذلك ضمن سجلات النظام (**Logs**) لأغراض التتبع والتحليل لاحقًا , فإذا توافقت هذه الحزمة مع القواعد المسموح بها، يتم تمريرها، وإذا لم تتوافق، يتم حظرها فورًا.

ويُعد ضبط هذه القواعد عملية دقيقة تُسهم بشكل كبير في تحقيق الحماية المطلوبة، لذلك سيُخصص التمرين رقم (7) لتطبيق إعداد جدار الحماية في نظام **Windows**، والتعرف عمليًا على كيفية تخصيص القواعد، وتحديد التطبيقات المسموح لها بالوصول إلى الشبكة، ومنع التطبيقات المشبوهة.

يوجد أكثر من نوع لجدران الحماية، ويمكن تصنيفها بعدة طرق، من أبسط التصنيفات وأكثرها وضوحًا هو التصنيف حسب مكان التشغيل. وهنا نميز بين:

1. جدار الحماية المعتمد على الجهاز: هو برنامج يتم تثبيته على جهاز حاسوب واحد، ويتولى حماية هذا الجهاز فقط من الاتصالات غير المصرح بها .يعمل هذا النوع على مراقبة التطبيقات التي تحاول الاتصال بالشبكة، ويسمح أو يمنع هذه المحاولات حسب إعدادات المستخدم. يعد مثاليًا للمستخدمين الفرديين أو أجهزة الحاسوب المنزلية مثل: **Windows Defender Firewall** الذي يعد أشهر جدران الحماية المعتمدة على الجهاز، ويتوفر ضمن نظام التشغيل **Windows** بشكل تلقائي.

   مميزات هذا النوع:
   - سهل التثبيت والاستخدام.
   - يسمح للمستخدم بتخصيص إعدادات الأمان حسب الحاجة
   - يحمي الجهاز من التطبيقات الخبيثة التي تحاول الاتصال بالشبكة.
2. جدار الحماية المعتمد على الشبكة: يُثبَّت على مستوى جهاز التوجيه (**Router**) أو شبكة محلية يتحكم في الاتصالات التي تمر عبر الشبكة بأكملها، وليس فقط جهازًا واحدًا. يُستخدم غالبًا في الشركات أو المؤسسات التي تحتوي على عدد كبير من الأجهزة. ويتحكم في حركة البيانات على مستوى الشبكة بأكملها ويُستخدم غالبًا في المؤسسات الكبيرة.

   مميزات هذا النوع:
   - يوفر حماية شاملة لجميع الأجهزة داخل الشبكة.
   - يُستخدم لحظر المواقع غير المرغوب فيها أو التحكم في حركة الإنترنت داخل المدرسة أو المؤسسة.
   - يمكنه تطبيق سياسات أمنية موحدة على نطاق واسع.

على الرغم من أن جدار الحماية يُعد أحد المكونات المحورية في تأمين الشبكات والأجهزة، إلاّ أنه لا يعمل بمعزل عن غيره من آليات الحماية، بل يشكل جزءًا من إطار أوسع يُعرف بـ"الدفاع متعدد

الطبقات" (**Defense in Depth**). ففي البيئات الرقمية الحديثة، لم تعد التهديدات تقتصر على محاولات الدخول غير المشروع، بل أصبحت أكثر تعقيدًا وذكاءً، إذ قد تأتي عبر قنوات مشفّرة أو ضمن حركة بيانات تبدو طبيعية ظاهريًا. من هنا تبرز الحاجة إلى تعزيز الحماية عبر تقنيات إضافية تمكننا من تكوين صورة أكثر اكتمالاً واستيعابًا لآليات الحماية المعتمدة في أنظمة التشغيل والشبكات المعاصرة كما سيتبين في الفقرات القادمة.

(3-3) حماية بروتوكولات الاتصال

أن تأمين الاتصال بين الأجهزة داخل الشبكات الرقمية لا يعتمد فقط على منع الاتصالات غير المصرح بها، بل يتطلب أيضًا تأمين البروتوكولات نفسها التي تُستخدم لنقل البيانات. فالبروتوكولات تُعد القواعد الأساسية التي تنظّم كيفية تبادل المعلومات بين الأنظمة، وإن لم تكن مؤمَّنة بشكل كافٍ، فإنها تصبح بوابة مفتوحة أمام التهديدات الأمنية. ضمن هذا السياق، برزت بروتوكولات مثل **SSL** (**Secure Socket Layer**) و**TLS** (**Transport Layer Security**) كحلول متقدمة تهدف إلى ضمان أمان البيانات أثناء الاتصال. وتُعد هذه البروتوكولات من الطبقات العليا التي تُضاف إلى بروتوكولات الشبكة التقليدية (مثل **TCP**)، لتقديم خصائص تشفير وحماية متقدمة تمنع التنصت، التعديل، أو إعادة الإرسال غير المشروع للبيانات بالإضافة الى بروتوكول **HTTPS** الذي يعد النسخة الآمنة من بروتكول **HTTP**.

يركز نظام التشغيل عند تأمين الاتصال على دعم إستخدام هذه البروتوكولات المشفرة وتوفير البيئة المناسبة لها، سواء عبر تطبيقات المتصفح أو خدمات البريد الإلكتروني أو الاتصالات البعيدة. ومن خلال تضمين دعم هذه البروتوكولات ضمن أنظمة التشغيل، يتم تفعيل آلية حماية متكاملة تشمل:

- المصادقة بين الطرفين للتأكد من الهوية.
- تشفير الاتصال بالكامل لحماية البيانات.
- التحقق من سلامة الرسائل لضمان عدم التلاعب بها.

وتعتمد هذه البروتوكولات على تقنيات التشفير غير المتماثل لتبادل المفاتيح، ثم تنتقل إلى التشفير المتماثل الذي يُستخدم لتأمين الجلسة بكفاءة عالية، مما يوفر توازنًا بين الأمان والسرعة في نقل البيانات كما سيتم التطرق إليه بصورة تفصيلية في الفصل الرابع.

(4-3) تحليل حركة البيانات لفهم الأنشطة المشبوهة

أصبح من الضروري دمج آليات أكثر تقدمًا ترتكز على الرصد والتحليل الفعّال لحركة البيانات (**Traffic Analysis**) للكشف عن الأنشطة المشبوهة قبل أن تتحول إلى تهديدات فعلية. وتُعد هذه العملية جزءًا تكامليًا من بنية حماية أنظمة التشغيل، لا سيما في الأنظمة التي تعتمد على الاتصال الدائم بالشبكة، مثل الخوادم أو أنظمة المعلومات المؤسسية.

(3-4-1) مفهوم تحليل حركة البيانات

يشير تحليل حركة البيانات إلى العملية التي يتم من خلالها مراقبة الاتصالات الشبكية وفحصها بشكل مستمر بهدف التعرف على الأنماط السلوكية الطبيعية ومقارنتها مع أنماط قد تُعد غير اعتيادية أو ضارة. يشمل ذلك فحص الحزم التي يتم إرسالها واستلامها عبر الشبكة، وتحديد الجهات المرسلة والمستقبلة، ونوع البروتوكولات المستخدمة، وتواتر الاتصالات، وحجم البيانات المنقولة.

تعد الحزمة (**Packet**) هي الوحدة الأساسية التي تُستخدم لنقل البيانات عبر الشبكات وهي كتلة من البيانات تتكوّن من معلومات المستخدم بالإضافة إلى رؤوس (**Headers**) تُستخدم لتوجيه الحزمة عبر الشبكة، والتحقق من سلامتها سواء كانت شبكة محلية أو الإنترنت. فعند إرسال رسالة أو طلب من جهازك إلى جهة أخرى (مثل الدخول إلى موقع ويب)، لا تُرسل البيانات دفعة واحدة، بل تُجزأ إلى عدد من الحزم الصغيرة، تُرسل كل منها بشكل منفصل، ثم يعاد تجميعها عند الوصول إلى الجهة المقصودة.

الشكل (3-1) يبين مثالا لحزمة تُظهر أن المستخدم يحاول زيارة موقع ويب من خلال منفذ 80 بأستخدام بروتوكول **HTTP**، وبهذا يستطيع محلل البيانات أو نظام التشغيل أن يتخذ قرارًا: أهذا اتصال مشروع؟ أم مشبوه؟ هل تم تكرار هذه العملية من عنوان **IP** غير مألوف؟ هل البيانات المنقولة آمنة؟ كل هذا يتحدد بناءً على تحليل هذه الحزم.

```
Packet
■ Source IP: 192.168.1.5
■ Destination IP: 172.217.16.142 (مثلاً: google.com)
■ Protocol: TCP
■ Source Port: 50534
■ Destination Port: 80 (HTTP)
■ Payload: GET /index.html HTTP/1.1
```

شكل(3-1) حزمة لزيارة موقع ويب

و بالتالي تبرز أهمية تحليل الحزم في تأمين أنظمة التشغيل بالنقاط الآتية:

1. يكتشف المحاولات غير المصرح بها للوصول إلى الجهاز.
2. يتحقق من وجود برامج خبيثة تحاول إرسال بيانات خارج الجهاز.
3. يُحدد ما إذا كان هناك هجوم من نوع **Denial of Service (DoS)** عبر إرسال آلاف الحزم خلال وقت قصير.

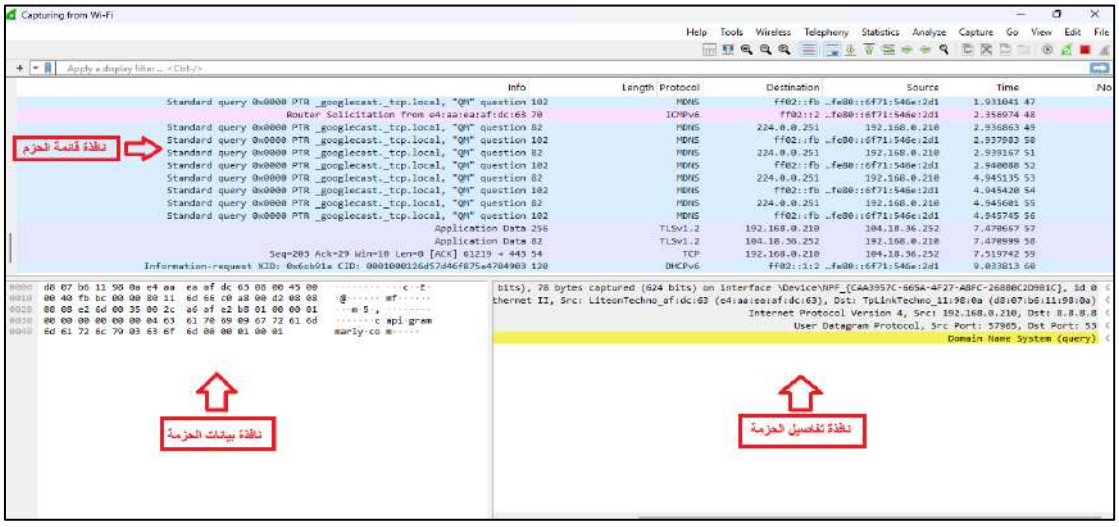
(2-4-3) أدوات تحليل البيانات و أهميتها في نظام التشغيل

هناك العديد من الأدوات البرمجية، بعضها مدمج داخل أنظمة التشغيل، وبعضها الآخر يُستخدم خارجيًا لتحليل حركة البيانات. ومن أهم هذه الأدوات هو برنامج **Wireshark** الذي يُعد من الأدوات البرمجية الرائدة في مجال تحليل الشبكات، وهي أداة مفتوحة المصدر ومجانية، تُستخدم لتحليل حركة مرور البيانات عبر الشبكات السلكية أو اللاسلكية بشكل تفصيلي لتُمكّن المحلل من مراقبة كل حزمة بيانات تمر عبر واجهة الشبكة، وتفسير محتواها ضمن سياق طبقات الشبكة المختلفة، مما يجعلها أداة لا غنى عنها في مجالات الإدارة الشبكية، واختبار الأمان، والتعليم الأكاديمي.

في هذا البرنامج تُحوَّل البيانات الملتقطة إلى واجهة رسومية تفاعلية تعرض الحزم بترتيب زمني، وتُتيح تصنيفها وتحليلها بدقة. ما يجعل هذه الأداة فريدة هو قدرتها على تحليل عدد كبير جدًا من البروتوكولات، يصل إلى أكثر من 1500 بروتوكول، منها: **HTTP**، **TCP**، **UDP**، **DNS**، **ICMP**، وغيرها.

تُقسم واجهة **Wireshark** الرسومية على ثلاثة أقسام رئيسة , كما مبين في الشكل (3-2) , تتيح للمستخدم التنقل بين الحزم وتحليلها بشكل دقيق:

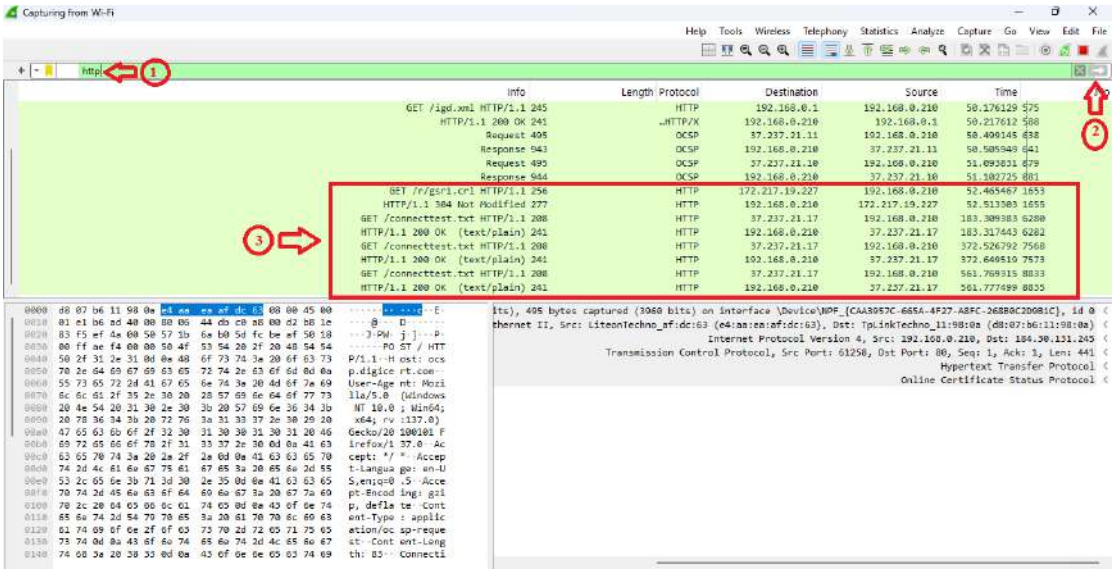
1. نافذة قائمة الحزم (**Packet List Pane**:) وتُعرض فيها الحزم الملتقطة بشكل تسلسلي، مع معلومات ملخصة عن كل حزمة مثل التوقيت، والمصدر والوجهة، والبروتوكول المستخدم.
2. نافذة تفاصيل الحزمة (**Packet Details Pane**): عند تحديد أي حزمة، تُعرض تفاصيلها الكاملة هنا، مقسمة على طبقات (**Layered View**) بدءًا من طبقة الربط (**Data Link**) وكذلك طبقة التطبيق (**Application Layer**).
3. نافذة بيانات الحزمة (**Packet Bytes Pane**): تُظهر تمثيل الحزمة بصيغة ثنائية (**hexadecimal** وASCII)، ما يُستخدم في تحليل محتوى الحزمة على المستوى الأدنى.



الشكل (2-3) واجهة المستخدم في برنامج Wireshark.

ويتميّز برنامج **Wireshark** بقدرته المتقدمة على إستخدام ما يُعرف بفلاتر العرض (**Display Filters**)، وهي إحدى الوظائف الحيوية التي تتيح للمستخدمين تصفية البيانات المعروضة ضمن واجهة البرنامج بناءً على شروط محددة، دون التأثير على الحزم الأصلية التي تم التقاطها. وتكتسب هذه الميزة أهمية خاصة في سياقات التحليل الأمني أو الاختبارات التعليمية، حيث تُستخدم لتقليل عدد الحزم المعروضة، والتركيز على تلك التي تتوافق مع نمط معين، مثل البروتوكول المستخدم، أو عنوان **IP** المصدر أو الوجهة، أو رقم المنفذ، أو حتى نوع الخطأ في الاتصال.

يعتمد **Wireshark** في تنفيذ هذه الفلاتر على بنية شرطية مرنة تُكتب بلغة وصفية تتيح تكوين معايير دقيقة للتحليل، كما يمكن الجمع بين أكثر من شرط بأستخدام المعاملات المنطقية مثل **AND** وOR وNOT. فعلى سبيل المثال، يمكن عرض الحزم التي تستخدم بروتوكول **HTTP** فقط، من خلال كتابة عبارة تصفية بسيطة هي **"http"**، أو عرض جميع الحزم القادمة من عنوان **IP** محدد و ليكن**"192.168.1.10"** بأستخدام الشرط **"ip.src == 192.168.1.10"**. ويمكن أيضًا دمج هذه الشروط لتحليل أكثر دقة، مثل مراقبة جميع الحزم القادمة من جهاز معين والتي تستخدم بروتوكول **HTTP**، بأستخدام الفلتر: **"ip.src == 192.168.1.10 and http"**. الشكل (3-3) يبين تطبيق فلتر لتصفية الحزم التي تستخدم بروتوكول **http** فقط



شكل (3-3) تطبيق فلتر http على الحزم

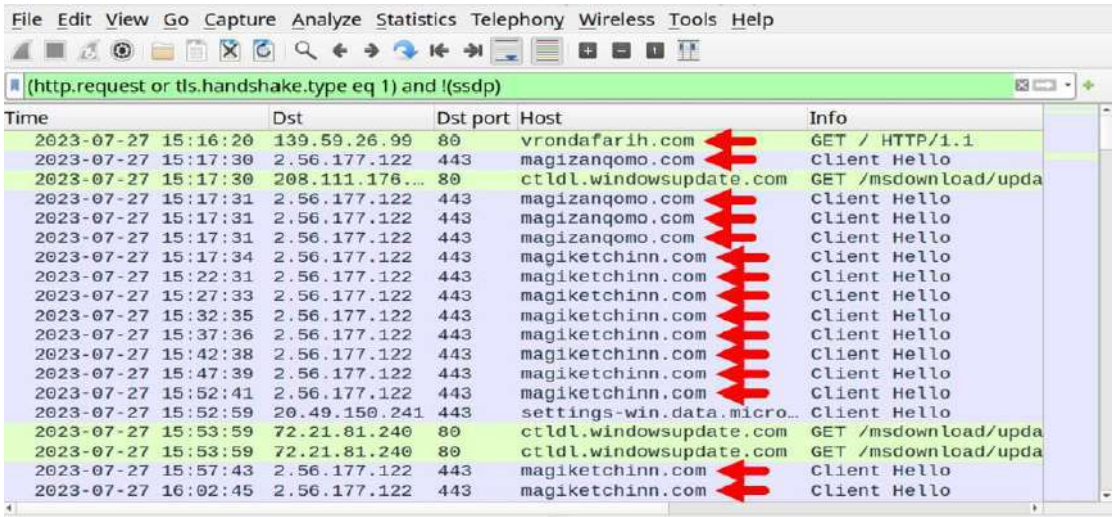
بين الشكل أعلاه الخطوات الأساسية لاستخدام فلاتر العرض داخل برنامج **Wireshark**. ففي البداية، يجب إدخال شرط التصفية في خانة الفلاتر، وهنا تم إستخدام الفلتر **http** بهدف عرض جميع الحزم التي تحتوي على بيانات تتعلق ببروتوكول **http**. بعد كتابة الفلتر، يتم الضغط على زر "تطبيق" لتفعيل الفلتر وتنفيذه. وبمجرد تفعيل الفلتر، ستُعرض في الجزء الأوسط من الواجهة جميع الطلبات التي تندرج تحت هذا البروتوكول، والتي يتم إرسالها من الجهاز المحلي إلى خادم الويب عبر الشبكة. كما يمكن ملاحظة معلومات إضافية تشمل عنوان المصدر والوجهة، والبروتوكول المستخدم، والزمن الذي أُرسلت فيه كل حزمة. ومن خلال تحليل هذه البيانات، يمكنك تتبع سلوك

المستخدم داخل الشبكة، وفهم كيفية انتقال البيانات من متصفح الإنترنت إلى الخادم والعكس، مما يتيح لك ربط المفاهيم النظرية الخاصة بطبقة التطبيق (**Application Layer**) بالتطبيق العملي الفعلي لتحليل الشبكات.

وتجدر الإشارة إلى أن فلاتر العرض لا تُستخدم فقط في الأوساط التعليمية، بل تُعد أداة لا غنى عنها في تحليل الحوادث الأمنية. فهي تُمكّن المتخصصين من تتبع الحزم المرتبطة بسلوك مشبوه حيث من خلال تحليل حركة البيانات، يمكن رصد مجموعة من المؤشرات التي تُعد علامات تحذيرية على وجود تهديد أمني محتمل، ومنها:

1. ارتفاع غير مبرر في حجم البيانات الصادرة من الجهاز.
2. تكرار الاتصالات الفاشلة من عنوان **IP** محدد.
3. وجود اتصالات إلى خوادم خارجية غير مألوفة.
4. محاولات الوصول إلى منافذ مغلقة أو غير مفعّلة.
5. ظهور بروتوكولات اتصال غير مصرح بها ضمن الشبكة.

يبين الشكل (3-4) مثالا لحركة مشبوهة للبيانات تم التقاطها ممن خلال برنامج **Wireshark** خلال تحليل لحركة مرور بيانات ناتجة عن إصابة الجهاز ببرمجية خبيثة. توضح الأسهم الحمراء مجموعة من الاتصالات الشبكية التي تستهدف نطاقات مشبوهة مثل **vrondafarih.com** و**magiketchinn.com**، وهي نطاقات تُستخدم في الغالب كخوادم تحكم وسيطرة للبرمجيات الخبيثة. حيث يتبين من خلال الشكل أعلاه عدة أمور تشير إلى نشاط مشبوه و منها كثافة الاتصالات الصادرة من جهاز واحد نحو خوادم غير معروفة، وهذا لا يحدث عادة في الاستخدام الطبيعي بالإضافة إلى أسماء نطاقات عشوائية وغير منطقية، ما يشير إلى محاولات من البرمجية الخبيثة للتواصل مع خادم التحكم للحصول على أوامر.



شكل (3-4) رصد اتصالات مشبوهة صادرة من الجهاز نحو خوادم خارجية بأستخدام Wireshark

3 حماية انظمة التشغيل

رقم التمرين: 7 الزمن المخصص: ساعة واحدة

اسم التمرين: اعداد جدار حماية مدمج في نظام windows

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

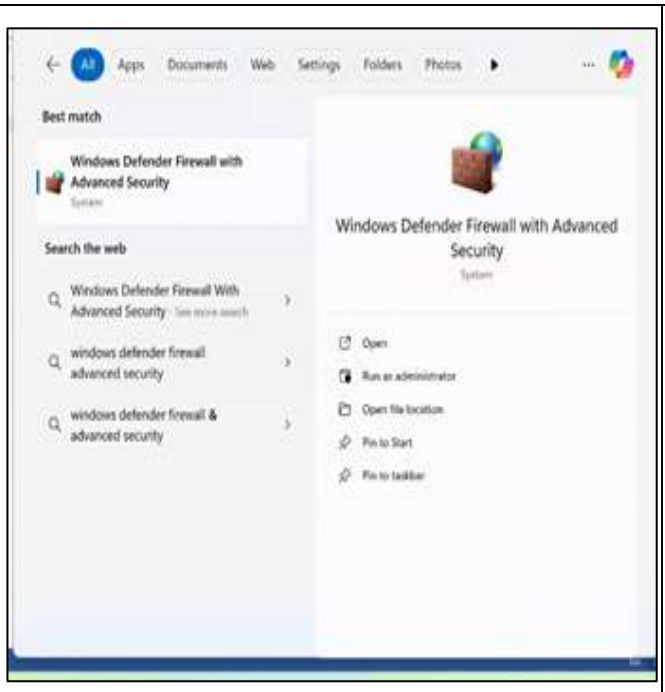
بعد إتمام هذا التمرين، سيتمكن الطالب من:

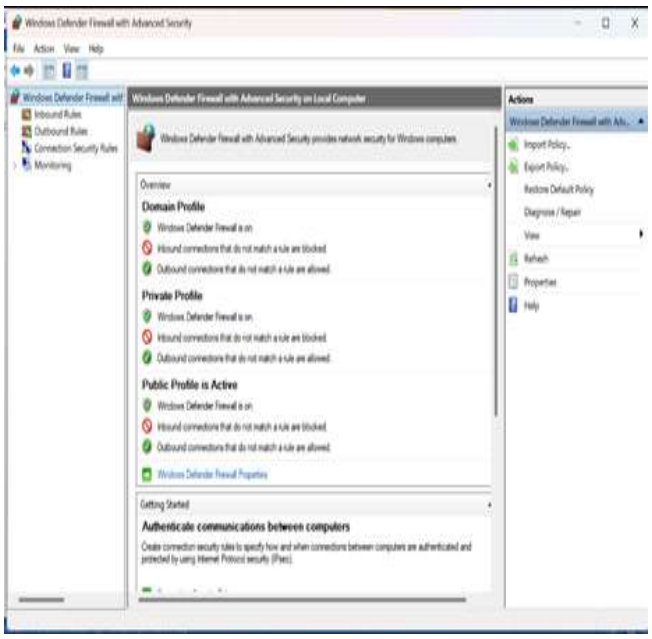
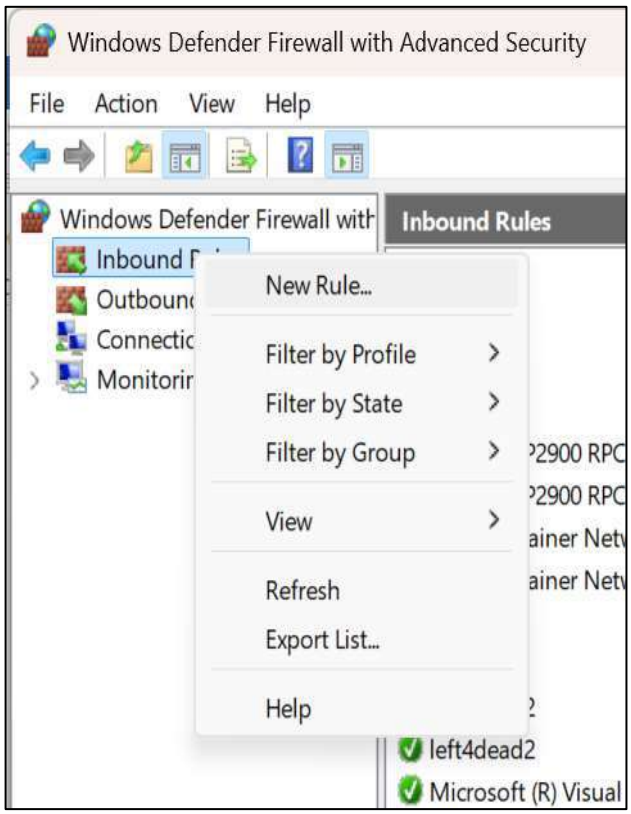
- اعداد نظام حماية مدمج في نظام Windows.

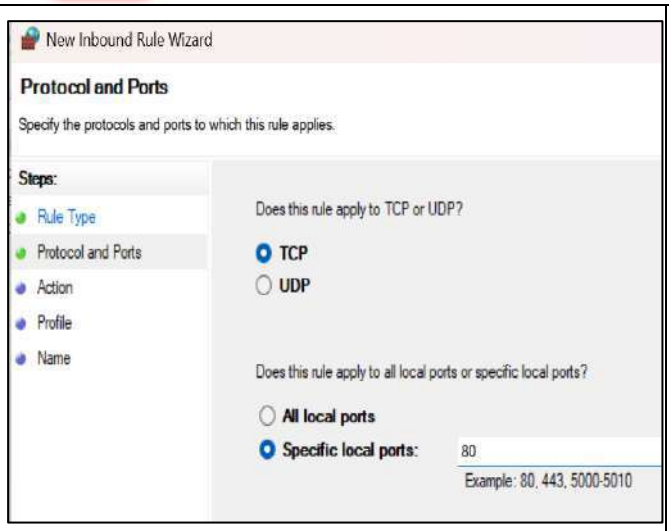
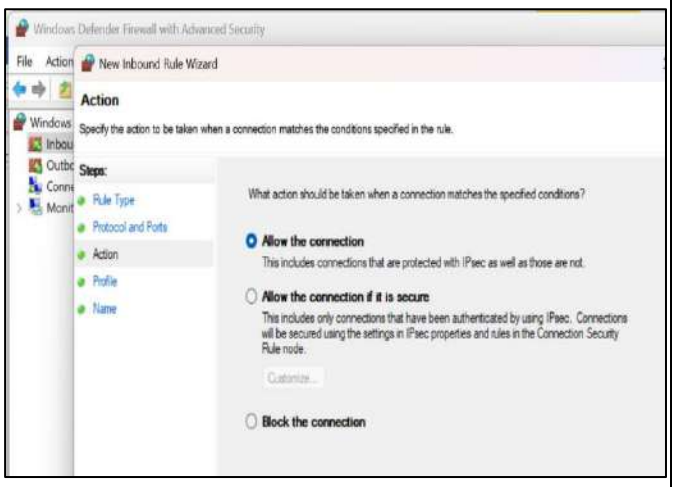
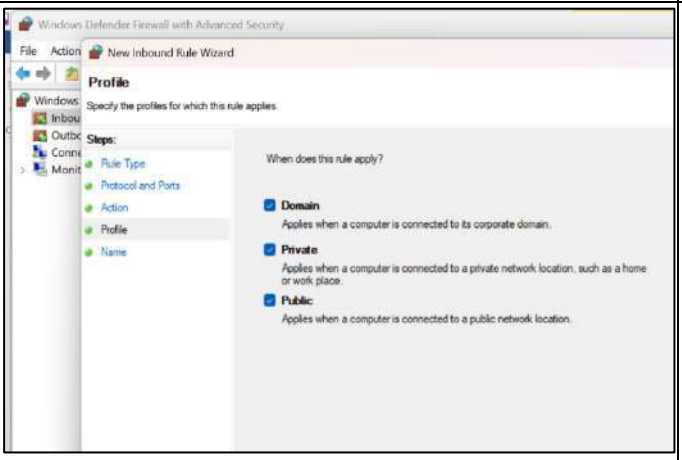
ثانياً: التسهيلات التعليمية

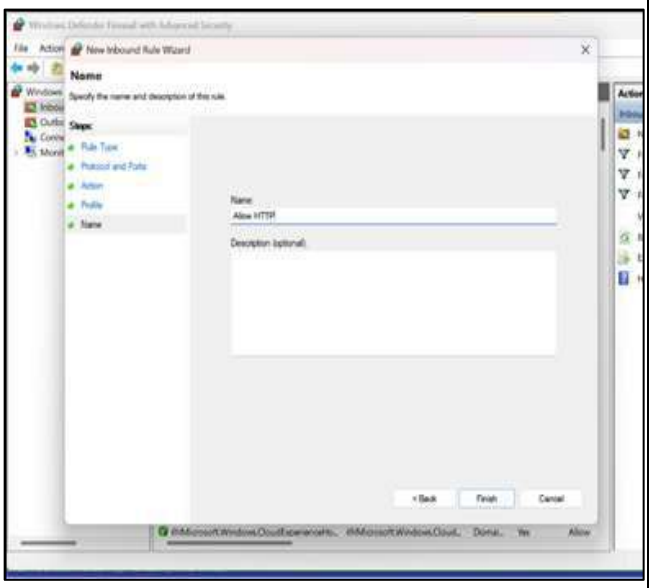
- أجهزة حاسوب مع نظام تشغيل Windows 10/11.
- اتصال بالإنترنت.

ثالثاً: خطوات تنفيذ التمرين

1	قم بتشغيل الحاسوب وانقر زر ابدأ (**Start**) في الزاوية السفلية اليسرى من الشاشة:	

2	ستفتح نافذة جديدة تحتوي على إعدادات متقدمة لجدار الحماية مثل: -القواعد الواردة (**Inbound Rules**): خاصة بالاتصالات الواردة. - القواعد الصادرة (**Outbound Rules**): خاصة بالاتصالات الصادرة. - مراقبة الاتصالات (**Monitoring**): لمراقبة نشاط الجدار الناري.	
3	قم بأنشاء قاعدة للسماح بمنفذ (مثلاً **HTTP**): -من قسم **Inbound Rules** اضغط **New Rule**.	

4	اختر **Port**، ثم حدد المنفذ مثل **80.**	
5	اختر **Allow the connection:**	
6	اختر الشبكات التي تُطبق عليها القاعدة **(Domain/Private/Public)**	

7	اسم القاعدة مثلاً: " **Allow HTTP**": 
8	المناقشة • ما الفرق بين القواعد الواردة (**Inbound**) والصادرة(**Outbound**) ؟ • كيف يمكن استغلال ضعف إعدادات الجدار في الهجمات؟ • هل يمكن إستخدام جدار الحماية لحماية الملفات المحلية؟ لماذا؟

نشاط: اعد التمرين السابق ثم قم بما يأتي:

1- إنشاء قاعدة لحظر منفذ (مثل 23 – Telnet):

- نفس الخطوات السابقة ثم اختر **Block the connection**
- غيّر رقم المنفذ إلى **23**.

2- السماح فقط لعناوين IP محددة (اختياري):

في خطوة **Scope** أثناء إنشاء القاعدة، حدد **IP** معين في خانة **Remote IP address**.

3- مراقبة وتعديل القواعد:

بعد الإنشاء، يمكنك تعديل أي قاعدة أو حذفها من القائمة اليمنى.

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:**7**	
اسم التمرين: **إعداد نظام حماية مدمج في نظام Windows**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب والوصول إلى الإعدادات المطلوبة	%15		
2	مراحل تنفيذ خيارات جدار الحماية	%15		
3	المناقشة	%10		
5	الزمن المخصص	%10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

3 حماية انظمة التشغيل

رقم التمرين: 8 الزمن المخصص: ساعة واحدة

اسم التمرين: مراقبة وتحليل حركة البيانات باستخدام **Wireshark**.

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

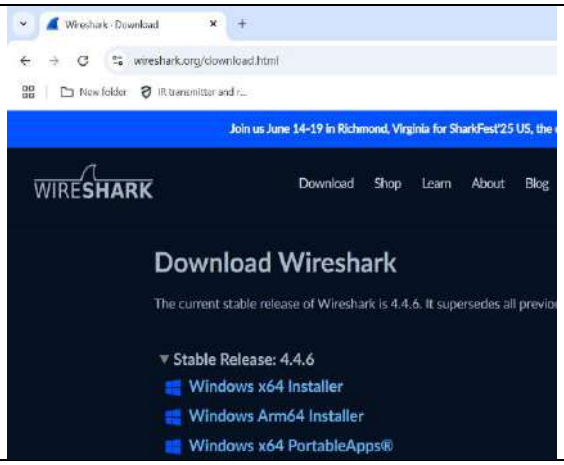
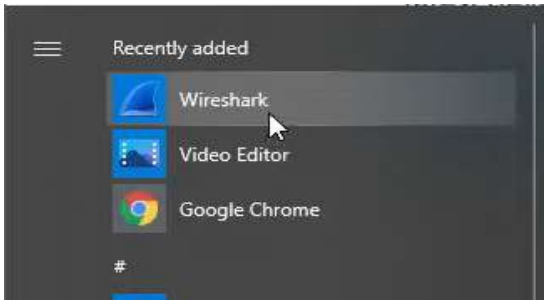
بعد إتمام هذا التمرين، سيتمكن الطالب من:

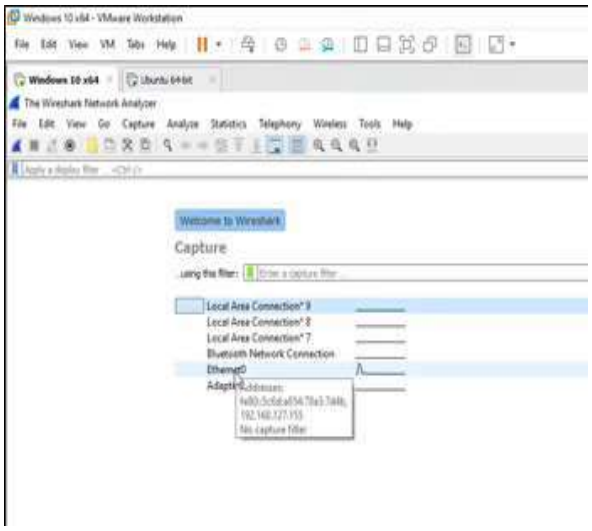
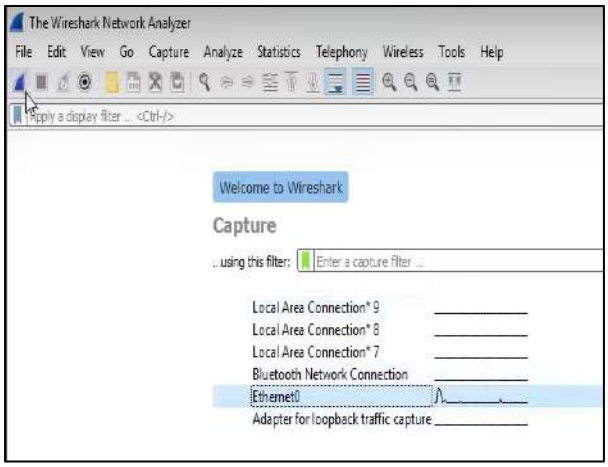
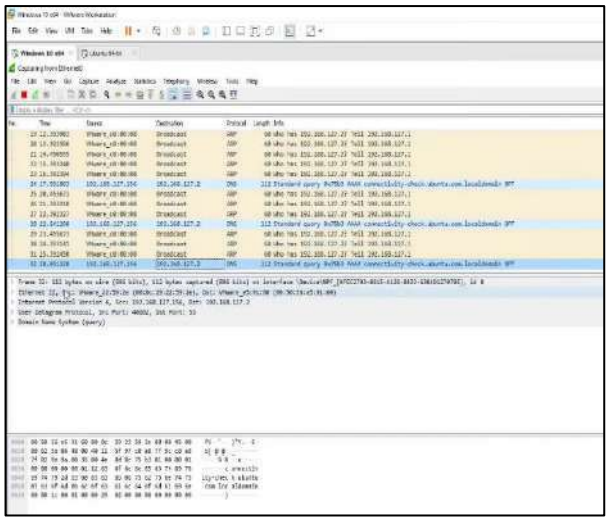
- التعرف على الاداة **Wireshark**.
- استخدام الاداة في تحليل ومراقبة حركة البيانات.

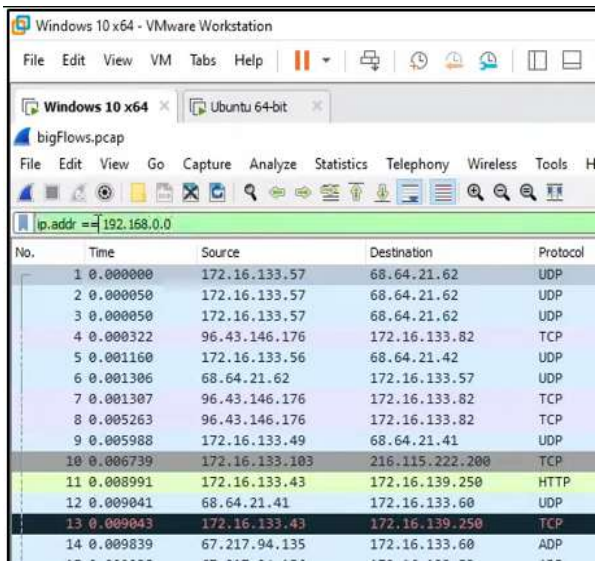
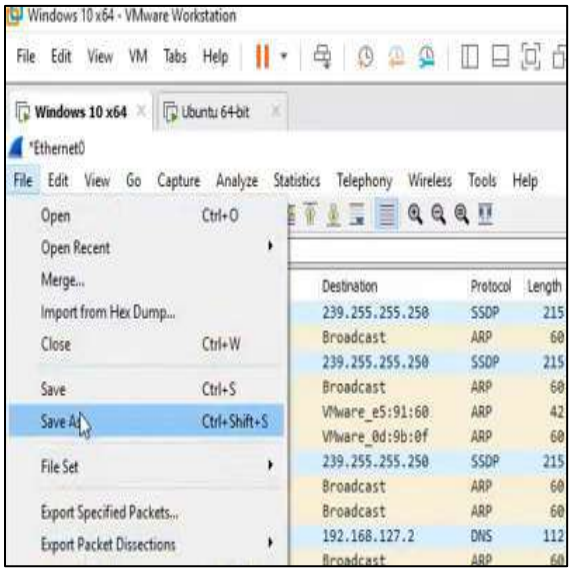
ثانياً: التسهيلات التعليمية

- أجهزة حاسوب مع نظام تشغيل **Windows 10/11**.
- اتصال بالإنترنت.

ثالثاً: خطوات تنفيذ التمرين

1	قم بتحميل البرنامج من الموقع الرسمي: https://www.wireshark.org، ثم قم بتثبّيته حسب نظام التشغيل لديك:	
2	افتح البرنامج بصلاحيات المسؤول (**Run as administrator**).	

3	اختر بطاقة الشبكة المتصلة بالإنترنت (غالبًا يكون **Wi-Fi** أو **Ethernet**):	
4	اضغط على الواجهة المناسبة ثم زر **"Start capturing packets"**:	
5	الآن يبدأ البرنامج في التقاط كل حركة البيانات:	

6	استخدم الفلاتر الآتية لعرض أنواع معينة من الحزم: • **http** لعرض طلبات **HTTP**. • **ip.addr == 192.168.1.X** لتتبع جهاز معين. • **tcp.port == 80** لرؤية الحزم الخاصة ببروتوكول **HTTP**.	
7	ثم إنقر على أي حزمة لرؤية التفاصيل وبعد الانتهاء، اضغط على **"File"** > **"Save As"** لحفظ ملف الالتقاط بامتداد **.pcapng**:	
8	المناقشة • كيف يمكن إستخدام **Wireshark** في اكتشاف الهجمات مثل **ARP Spoofing** أو **DoS**؟ • ما هي خطورة ترك **Wireshark** يعمل بدون إذن في شبكة عمل؟ • هل يمكن التقاط بيانات حساسة (مثل كلمات مرور)؟ وكيف يتم حماية الشبكة ضد ذلك؟	

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:8	
اسم التمرين: مراقبة وتحليل حركة البيانات بإستخدام **Wireshark.**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب وتحميل البرنامج	%10		
2	تثبيت البرنامج	%10		
3	تنفيذ التمرين والتقاط الحركات واستخدام الفلاتر	%10		
4	المناقشة	%10		
6	الزمن المخصص	%10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

3 حماية انظمة التشغيل

رقم التمرين: 9 الزمن المخصص: ساعة واحدة

اسم التمرين: إعداد نظام حماية من التهديدات الموجهة للاتصال باستخدام **Comodo Firewall.**

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

بعد إتمام هذا التمرين، سيتمكن الطالب من:

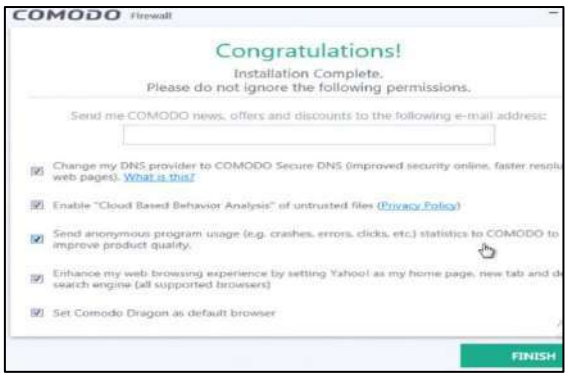
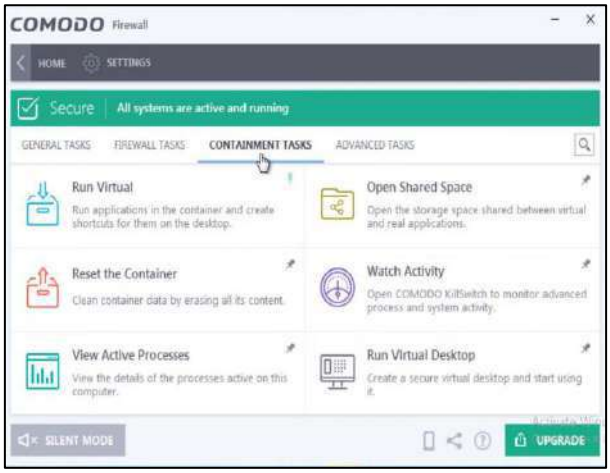
- اعداد نظام حماية من التهديدات الموجهة للاتصال.
- التعامل مع الاداة **Comodo Firewall**.

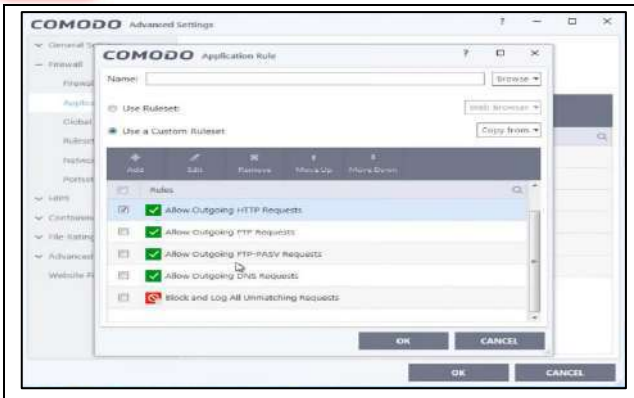
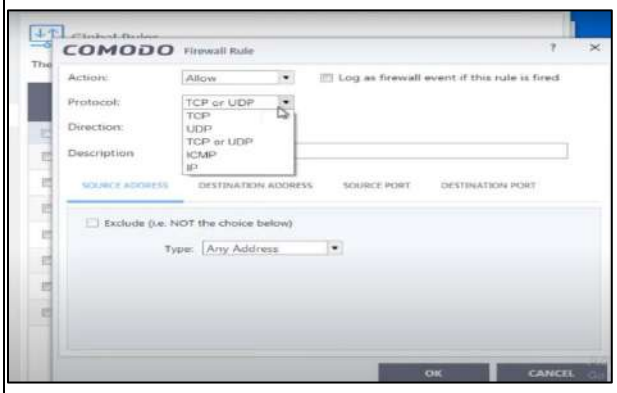
ثانياً: التسهيلات التعليمية

- أجهزة حاسوب مع نظام تشغيل **Windows 10/11**.
- اتصال بالإنترنت.

ثالثاً: خطوات تنفيذ التمرين

1	حمل البرنامج من الموقع الرسمي للبرنامج: (**https://www.comodo.com**) ثم اختر **Comodo Firewall** (النسخة المجانية) ثم اضغط على **Download**.	

2	بعد تحميل الملف، قم بتثبيت البرنامج:	
3	بمجرد تثبيت البرنامج، افتحه من قائمة ابدأ أو من خلال اختصار سطح المكتب، ستظهر لك واجهة **Comodo Firewall** التي ستحتاج إلى إعدادها:	
4	بدأ بالانتقال إلى **Firewall** من القائمة الرئيسية في البرنامج، اختر **Advanced Settings** لتمكين الإعدادات المتقدمة، في قسم **Application Rules**، اختر **Add Rule** لإنشاء قاعدة جديدة. اختر **Allow** أو **Block** بناءً على ما إذا كنت ترغب في السماح أو حظر التطبيقات أو الخدمات:	

5	حدد التطبيق أو الخدمة التي تريد إضافة قاعدة لها، على سبيل المثال، إذا كنت تريد حظر **SSH**، اختر **SSH** من القائمة وأضف قاعدة لحظر الاتصال.	
6	في قسم **Network Rules**، يمكنك إضافة قواعد للمنافذ التي ترغب في حظرها. اختر البروتوكول (مثل **TCP** أو **UDP**) وأدخل المنفذ المطلوب (على سبيل المثال، 22 لـ **SSH**) واضغط على **Block**:	
7	المناقشة • لماذا يعد وجود نظام حماية مستقل أفضل من الاعتماد على جدار الحماية الافتراضي فقط؟ • كيف يساعد احتواء التطبيقات **Auto-Containment** في منع تنفيذ البرمجيات الخبيثة؟ • ماذا تفعل لو حصلت على إنذار متكرر من نفس التطبيق؟ أ تحظره أم تسمح له؟	

نشاط:

1- اذهب إلى قسم **Defense+** في **Comodo Firewall**، اختر **Automatic Sandbox** لحماية الجهاز من البرمجيات الضارة التي قد تحاول الوصول إلى النظام، قم بتمكين **Intrusion Prevention** للكشف عن الهجمات ومنعها.

2- قم بإعداد الحماية ضد الهجمات من خلال تفعيل **Buffer Overflow Protection** و **HIPS** (**Host Intrusion Prevention System**) لتعزيز الحماية ضد البرمجيات الخبيثة.

3- قم بتفعيل الإشعارات، انتقل إلى **Settings** في **Comodo Firewall** ثم اختر **Notifications** لتمكين إشعارات الحماية، قم بتفعيل التنبيهات لحظة اكتشاف تهديدات أو محاولات اتصال مشبوهة.

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:9	
اسم التمرين: **إعداد نظام حماية من التهديدات الموجهة للاتصال باستخدام Comodo Firewall.**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب وتحميل البرنامج	%10		
2	تثبيت البرنامج	%10		
3	تنفيذ خطوات التمرين	%10		
4	إختبار القواعد والسياسات التي تم تطبيقها	%10		
5	المناقشة	%5		
6	الزمن المخصص	% 5		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

أسئلة الفصل الثالث

س1: عرف ما يأتي:

1-الاتصالات الواردة 2- تحليل حركة البيانات. 3- **Wireshark** 4- البروتوكولات المشفرة.
5- الدفاع متعدد الطبقات.

س2: املأ الفراغات الآتية بما يناسبها:

1-تُعد ـــــــــــ البنية الأساسية للعالم الرقمي المعاصر، مما يستدعي وجود حماية متقدمة داخل أنظمة التشغيل لحماية البيانات أثناء تنقلها.

2- من أهم مهام ـــــــــــ أنها تُحدد ما إذا كانت البيانات الواردة أو الصادرة من الجهاز آمنة، وتُطبق قواعد محددة للسماح أو الحظر.

3- البروتوكولات مثل ـــــــ و ـــــــ تُستخدم لتأمين الاتصال من خلال المصادقة وتشفير البيانات أثناء نقلها.

4- يُشير ـــــــــــ إلى العملية التي يتم فيها مراقبة وفحص حركة البيانات عبر الشبكة لاكتشاف الأنشطة غير الطبيعية أو الضارة.

5- من أهم الأدوات التي تُستخدم لتحليل الحزم الشبكية وتفسير محتواها عبر طبقات الشبكة المختلفة هي أداة ـــــــــــ.

6- يعتمد نموذج ـــــــــــ على إستخدام أكثر من وسيلة أمنية في وقت واحد لتعزيز الحماية ضد التهديدات المعقدة.

س3: اشرح مفهوم تأمين الاتصالات في أنظمة التشغيل، وبيّن أهميته في ظل تزايد التهديدات السيبرانية.

س4: عدّد أبرز آليات تأمين الاتصال التي توفرها أنظمة التشغيل الحديثة.

س5: قارن بين جدار الحماية المعتمد على الجهاز وجدار الحماية المعتمد على الشبكة من حيث الخصائص ومجال الاستخدام.

س6: ما المقصود بالاتصالات الواردة والصادرة؟ وضّح الفرق بينهما مع ذكر أمثلة.

س7: ما وظيفة القواعد (**Rules**) في إعداد جدران الحماية؟ وكيف تؤثر على أمن النظام؟

س8: تحدث عن دور البروتوكولات المشفّرة مثل **HTTPS** و**TLS** في حماية البيانات أثناء النقل.

الفصل الرابع

حماية التخزين و البيانات

Storage and Data Protection

أهداف الفصل الرابع

1. عرض المفاهيم الأساسية لعلوم التشفير، مع تصنيف خوارزميات التشفير وفق آلياتها وأنواع المفاتيح وكمية البيانات المعالجة، وبيان الفروق بين النماذج المختلفة.
2. تحليل دور بروتوكولات النقل الأمن مثل **TLS** في حماية البيانات أثناء انتقالها عبر الشبكات، وشرح بنيتها وآلية عملها.
3. استعراض استراتيجيات النسخ الاحتياطي وتصنيفاتها المتنوعة، وأثرها في دعم استمرارية العمل وضمان توافر المعلومات.
4. بيان أهمية استراتيجيات استعادة البيانات والعوامل المؤثرة في بناء خطط استجابة فعالة في حالات الكوارث.
5. مناقشة التحديات التقنية المرتبطة بتخزين النسخ الاحتياطية وضرورة التحقق الدوري من سلامتها لضمان فعاليتها على المدى الطويل.
6. تسليط الضوء على آليات حذف البيانات الآمن ، والتقنيات المستخدمة لمنع استعادتها، وأثرها في حماية الخصوصية في البيئات المؤسسية والشخصية.

محتويات الفصل الرابع

الفصل الرابع

حماية التخزين و البيانات

Storage and Data Protection

تمهيد

تعد حماية البيانات الرقمية ركيزة أساسية في مجال الأمن السيبراني وواحدة من أكثر القضايا أهمية في تصميم أي نظام معلوماتي أو شبكة حاسوبية وقد طورت عبر السنوات عدة نماذج نظرية لتأطير مفاهيم أمن المعلومات وكان من أبرز هذه النماذج و اكثرها قبولا و انتشاراً هو ما يعرف بمثلث الأمان أو مثلث الحماية (**CIA Triad**). يجسد هذا المثلث كما هو موضح في الشكل (4-1) ثلاثة أهداف رئيسة يجب أن تتحقق مجتمعة لضمان حماية البيانات والأنظمة الرقمية بشكل متكامل وهي:

1. **السرية (Confidentiality):** تعرف السرية على أنها خصوصية البيانات و تعني أن المعلومات لا يمكن الوصول اليها إلاّ من قبل الجهات أو الأشخاص المخولين ويتطلب ذلك إستخدام عدة تقنيات مثل التشفير و إدارة الوصول (**Access Control**).
2. **التكامل (Integrity):** يشير مفهوم التكامل إلى سلامة البيانات سواء كانت مخزنة أم منقولة. و يضمن هذا المبدأ أن أي تعديل في البيانات لا يمكن أن يتم إلاّ بطريقة مصرح بها و موثوقة.
3. **التوافر (Availability):** المقصود بالتوافر هو ضمان أن تكون المعلومات والأنظمة متاحة دائما للمستخدمين المخولين في الوقت المناسب ويمكن أن يشمل ذلك التخطيط الجيد للبنية التحتية. ووجود النسخ الإحتياطية بالإضافة إلى الحماية من هجمات تعطيل الخدمة (**DoS/DDoS**).

الشكل (4-1) مثلث الحماية

4 حماية انظمة التشغيل

من الجدير بالذكر أن نموذج مثلث الحماية (**CIA Triad**) لا يُعد مجرد إطار نظري، بل يمثل مرتكزًا أساسياً تُبنى عليه السياسات الأمنية في مختلف أنظمة المعلومات. وتتجلى فعاليته في القدرة على ترجمته إلى إجراءات عملية تضمن حماية شاملة للبيانات. فعلى سبيل المثال، يمكن تعزيز السرية من خلال إستخدام خوارزميات تشفير قوية مثل (**AES**)، وتطبيق سياسات تصنيف البيانات بناءً على درجة حساسيتها. أمّا تحقيق سلامة البيانات (التكامل) فيتطلب إستخدام تقنيات تحقق موثوقة كالتوقيعات الرقمية (**Digital Signatures**) وخوارزميات التحقق من صحة البيانات مثل (**SHA-256**). وفيما يتعلق بـالتوافر، فإنه يُعزز من خلال تبني خطط فعّالة لاستمرارية العمل واستعادة البيانات بعد فقدها بالإضافة إلى اعتماد بنى تحتية مرنة تضمن الوصول المستمر للخدمات الرقمية دون انقطاع.

ومع تزايد تعقيد التهديدات السيبرانية، تطورت الحاجة إلى توسيع نطاق هذا النموذج ليشمل مفاهيم إضافية مكملة تعزز أمن المعلومات بشكل أكثر شمولًا، ومن أبرزها: المساءلة (**Accountability**)، التي تضمن تتبّع النشاطات وربطها بالمستخدمين المسؤولين، والمصادقة (**Authentication**)، التي تتحقق من هوية المستخدمين، وعدم الإنكار (**Non-Repudiation**)، التي تمنع الأطراف من إنكار تنفيذ إجراءات معينة. وبهذا يُصبح مثلث الحماية جزءاً من إطار متكامل يُعرف بـإطار الأمن المعلوماتي الشامل (**Comprehensive Information Security Framework**)، الذي يُعد مرجعاً معتمدًا لتصميم وتقييم استراتيجيات حماية المعلومات في البيئات الرقمية الحديثة.

(4-1) تقنيات التشفير الحديثة لحماية البيانات

يُعد التشفير (**Encryption**) من أهم الوسائل التقنية المعتمدة لضمان أمن المعلومات، خاصة عندما يتعلق الأمر بتحقيق السرية (**Confidentiality**)، وهي إحدى ركائز مثلث الحماية (**CIA Triad**). تتمثل وظيفة التشفير في تحويل البيانات الأصلية (**Plain Text**) إلى صيغة غير مفهومة (**Cipher Text**)، بحيث لا يمكن قراءتها أو الاستفادة منها دون معرفة المفتاح الصحيح المستخدم في عملية التشفير.

وتُصنّف خوارزميات التشفير إلى فئات متعددة، ويمكن تنظيمها وفقًا لعدة معايير، كما هو موضح في الشكل (4-2)، منها:

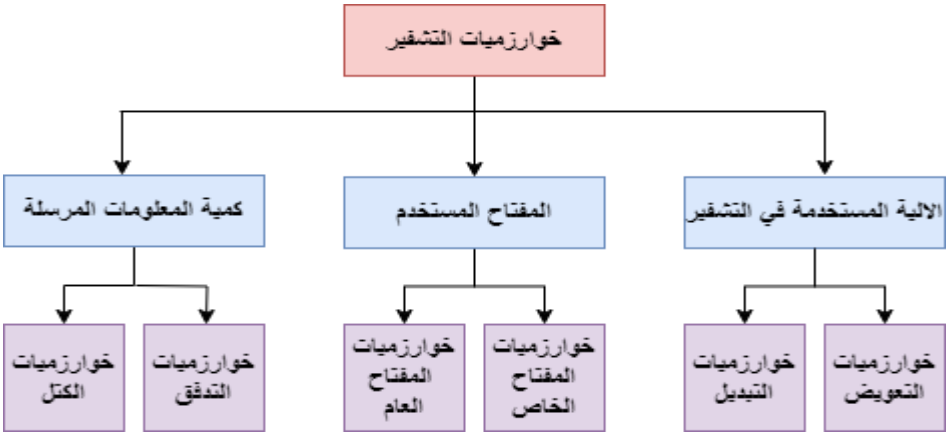
1. **الآلية المستخدمة في التشفير:** ويُقصد بها الأسلوب الذي تعتمد عليه الخوارزمية في معالجة البيانات، ويشمل خوارزميات التعويض (**Substitution**)، حيث تُستبدل عناصر البيانات بأخرى وفق نظام معين، وخوارزميات التبديل (**Transposition**)، التي تُغيّر مواقع البيانات دون تغيير قيمتها.
2. **نوع المفتاح المستخدم:** ويُعد هذا التصنيف من أكثر التصنيفات شيوعًا، حيث تُقسم الخوارزميات على:

- التشفير المتماثل (**Symmetric Encryption**): حيث يُستخدم نفس المفتاح في عمليتي التشفير وفك التشفير.

- التشفير غير المتماثل (**Asymmetric Encryption**): ويعتمد على زوج من المفاتيح (مفتاح عام وآخر خاص)، بحيث يُستخدم أحدهما للتشفير والآخر لفك التشفير.

3. **كمية المعلومات المرسلة:** وتُصنّف الخوارزميات بحسب هذا المعيار إلى:

- خوارزميات الكتل (**Block Ciphers**): التي تُجزئ البيانات إلى كتل ثابتة الحجم وتعالج كل كتلة على حدة.
- خوارزميات التدفق (**Stream Ciphers**): التي تُعالج البيانات بتسلسل بتات أو بايتات دون تجزئتها إلى كتل.



الشكل (4-2): تصنيف خوارزميات التشفير

وعلى الرغم من هذه التصنيفات المتعددة، فان التصنيف الأكثر شيوعا ، هو: التشفير المتماثل والتشفير غير المتماثل، اللذان يشكّلان جوهر البنى التحتية الآمنة في أنظمة المعلومات والاتصالات. وبناءً على ذلك، ستتناول الفقرات اللاحقة شرحًا تفصيليًا لهذين النوعين، مع بيان مبادئ عملهما وأبرز خوارزمياتهما.

(4-1-1) التشفير المتماثل (Symmetric Encryption)

يعد التشفير المتماثل من أقدم المفاهيم في مجال أمن المعلومات وهو يشكل الأساس الذي بنيت عليه معظم تقنيات التشفير المعاصرة. يتميز هذا النوع من التشفير بأستخدام مفتاح واحد فقط لكل من عمليتي التشفير و فك التشفير أي أن نفس المفتاح الذي يستخدم لتحويل البيانات إلى صيغة غير مفهومة هو ذاته الذي يستخدم لإعادتها إلى حالتها الأصلية. يعتمد التشفير المتماثل على خمسة عناصر أساسية تشمل:

- **النص الصريح (Plain Text):** وهي الرسالة الأصلية أو البيانات المفهومة التي يراد حمايتها.

- **خوارزمية التشفير(Encryption algorithm):** تقوم هذه الخوارزمية بتنفيذ مجموعة من التحويلات و الاستبدالات على النص الصريح لتحويله لشكل غير مفهوم وتعتمد جزئيا على المفتاح السري.
- **المفتاح السري (Secret Key):** هو عنصر مستقل عن النص الصريح والخوارزمية وتختلف نتائج التشفير باختلاف هذا المفتاح حتى لو كان البيانات نفسها.
- **النص المشفر (Cipher Text):** هو الناتج النهائي من خوارزمية التشفير ويبدو كمجموعة من الرموز العشوائية غيرالمفهومة ويتم انتاج هذا النص من خلال الجمع بين خوارزمية التشفير والمفتاح السري.
- **خوارزمية فك التشفير (Decrypting algorithm) :** وهي بالأساس نفس خوارزمية التشفير حيث تأخذ النص المشفر والمفتاح السري وتقوم بإعادة بناء النص الصريح.

من أبرز مميزات التشفير المتماثل هو كفاءته العالية في التعامل مع كميات كبيرة من البيانات خاصة في الأنظمة التي تتطلب سرعة عالية في معالجة البيانات وتبادلها. يوضح الشكل (4-3) المفهوم الأساسي للتشفير المتماثل حيث يستخدم مفتاح واحد لإجراء كل من عمليتي التشفير وفك التشفير مع الإشارة إلى أن كلا الطرفين (المرسل والمستقبل) يجب أن يمتلكا هذا المفتاح مسبقا وبشكل آمن.

الشكل: (4-3) التشفير المتماثل

ولك أن تعرف عزيزي الطالب أن جذور التشفير المتماثل تعود إلى العصور القديمة حيث استخدمته الامبراطوريات لحماية اسرارها العسكرية والدبلوماسية إذ تعد شفرة قيصر من أبرز الأمثلة التاريخية على ذلك وهي نظام بسيط لتحويل الحروف من خلال ازاحتها بعدد معين داخل الابجدية, ومع تطور الرياضيات والحوسبة ظهرت خوارزميات عديدة تعتمد على التشفير المتماثل وسنتطرق إلى ثلاثة أنواع منها وهي (**DES, Triple DES, AES**):

1. **خوارزمية DES (Data Encryption Standard):**

هي من أوائل الخوارزميات القياسية المعتمدة للتشفير المتماثل اعتمدت رسميا في سنة 1977 تعتمد هذه الخوارزمية على تشفير الكتل (**Block Ciphering**) حيث تقسم البيانات على كتل (**Blocks**) كل كتلة حجمها 64 بت ثم يتم تبديل الأرقام والرموز بطرق خاصة ويتم ذلك على 16 مرحلة متتالية وتعتمد هذه الخوارزمية على مفتاح سري طوله 56 بت. في الوقت الحالي ومع تطور الهجمات أصبح من الممكن على المهاجمين إستخدام برامج متطورة وتجربة عدد كبير جدا من المفاتيح لاكتشاف المفتاح الصحيح وهذا يعني أن **DES** لم تعد آمنة كفاية لحماية المعلومات الحساسة

2. **خوارزمية Triple DES (3DES)**

هي طريقة محسنة من خوارزمية **DES** تقوم بتكرار عملية التشفير ثلاث مرات بدلا من مرة واحدة بأستخدام ثلاث مفاتيح ولهذا سميت "**Triple**" أي "ثلاثية" حيث يتم تشفير البيانات بأستخدام المفتاح الأول وفك تشفير البيانات بالمفتاح الثاني ثم إعادة التشفير مرة أخرى بالمفتاح الثالث. تقدم هذه الخوارزمية حماية افضل لكنها بطيئة جدا وبالتالي تتكون غير مناسبة للأنظمة التي تحتاج إلى سرعة وأداء عالي.

3. **خوارزمية AES (Advanced Encryption Standard)**

تعد واحدة من اقوى واكثر خوارزميات التشفير إستخداماً و تم اعتمادها رسميا في عام 2001 من قبل المعهد الوطني الأمريكي للمعايير والتقنية (**NIST**) بعد تنظيم مسابقة دولية لاختيار بديل آمن و حديث لخوارزميات التشفير القديمة مثل **DES** و **3DES**.

تمتاز خوارزمية **AES** بقوتها وكفاءتها العالية حيث صممت لتكون مناسبة للاستخدام في التطبيقات التي تتطلب حماية قوية للبيانات منها:

- تشفير الاتصالات عبر الإنترنت مثل (**HTTPS**)
- الشبكات الخاصة الافتراضية (**VPN**)
- حماية الملفات على الهواتف والحواسيب المحمولة.
- تشفير قواعد البيانات
- أنظمة الدفع الذكية والبطاقات البنكية

يتم في هذه الخوارزمية تقسيم البيانات على كتل (**Blocks**) بحجم **128** بت ويجري على كل (**Block**) التشفير بأستخدام مفتاح سري يمكن أن يكون طوله 128 بت أو 192 بت أو 256 بت و ذلك حسب مستوى الأمان المطلوب. تعتمد خوارزمية **AES** في عملها على عدد من الجولات (**Rounds**) و هي مراحل متتالية يتم فيها إجراء تغيرات معقدة على البيانات لجعلها غير قابلة للفهم, عدد هذه الجولات:

- 10 جولات للمفتاح بطول 128 بت.
- 12 جولة للمفتاح بطول 192 بت.
- 14 جولة للمفتاح يطول 256 بت.

كل جولة من هذه الجولات تتم على اربع مراحل رئيسة تنفذ على البيانات وهي:

1. **استبدال البايت (SubBytes):** حيث يتم استبدال كل بايت من البيانات مع بايت آخر وفق جدول استبدال معد مسبقا يسمى (**S-Box**).
2. **إزاحة الصفوف (Shift Rows):** يتم فيها تحريك مواقع الصفوف داخل الكتل (**Blocks**) لتغيير ترتيب البيانات.
3. **مزج الأعمدة (Mix Columns):** تنفذ عمليات رياضية على الأعمدة داخل الكتل لمزيد من التشفير العشوائي.
4. **إضافة المفتاح (Add Round Key):** يتم فيها دمج البيانات مع جزء من المفتاح السري بأستخدام **XOR**.

هذه العمليات الأربعة تكرر داخل كل جولة (**Round**), ومع تكرارها لعدد كاف من المرات تصبح البيانات المشفرة غير مفهومة اطلاقا ولا يمكن استرجاعها إلى شكلها الأصلي إلاّ بأستخدام نفس المفتاح السري. تمرين رقم (10) يبين عملية تشفير للبيانات من خلال برنامج **VeraCrypt** بالاعتماد على خوارزمية **AES**.

(4-1-2) التشفير غير المتماثل (Asymmetric Encryption)

في الفقرة السابقة تعرفنا إلى التشفير المتماثل والذي يعتمد على مفتاح واحد فقط للتشفير وفك التشفير, لكن في الشبكات المفتوحة مثل الإنترنت عند تبادل البيانات بين المرسل و المستقبل يكون من الصعب تبادل هذا المفتاح , وهنا يأتي دور التشفير غير المتماثل الذي حل هذه المشكلة. في هذا النوع من التشفير لا نستخدم مفتاحا واحدا بل نستخدم زوجا من المفاتيح:

- **مفتاح عام (Public Key):** يمكن لأي شخص الحصول عليه.
- **مفتاح خاص (Private Key):** يحتفظ به صاحبه فقط ولا يتم مشاركته مع أحد.

الفكرة ببساطة عزيزي الطالب إذا أراد شخص ما أن يرسل رسالة مشفرة لك فانه يستخدم المفتاح العام الخاص بك لتشفير الرسالة, وعند استلام الرسالة يمكنك انت فقط فك تشفيرها بأستخدام المفتاح الخاص بك وكما مبين في الشكل (4-4). هذا النظام يسهل عملية تبادل المعلومات بصورة آمنة لكنه يكون عادة بطئ وغير مناسب للتطبيقات التي تحتاج إلى السرعة في نقل البيانات، ولذلك غالبا ما يستخدم في حالات محددة مثل:

- إرسال المفاتيح السرية بأمان (ليتم بعدها إستخدام التشفير المتماثل لتبادل البيانات بسرعة).
- توقيع الوثائق إلكترونياً.

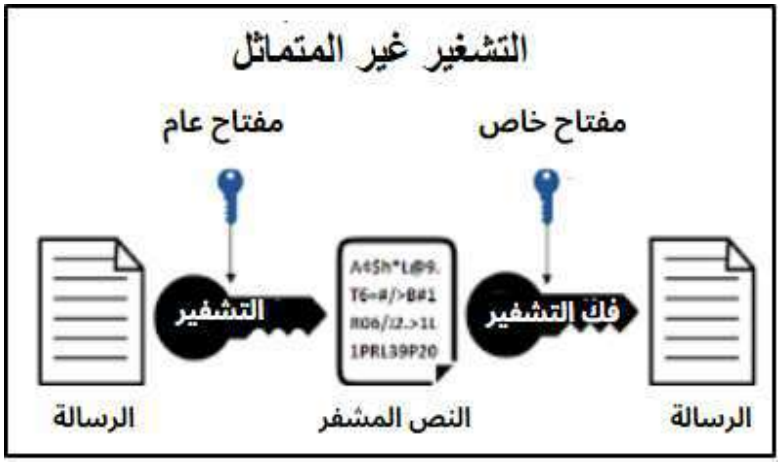
ومن اشهر الخوارزميات المستخدمة في التشفير غير المتماثل خوارزمية **RSA** التي تشير إلى أسماء العلماء الثلاثة الذين ابتكروها (**Rivest – Shamir – Adleman**) وتستخدم بكثرة في الأنظمة البنكية وتامين المواقع الإلكترونية وتعتمد في بنيتها على صعوبة تحليل حاصل ضرب عددين أوليين كبيرين. وعلى الرغم من كفاءتها الأمنية العالية، إلاّ أن هذه الخوارزمية تُعد بطيئة نسبيًا مقارنة بخوارزميات التشفير المتماثل، ما يجعلها غير ملائمة لتشفير البيانات ذات الحجم الكبير.

وبالتالي من أبرز مزايا التشفير غيرالمتماثل هي:

- أمان عالٍ في تبادل المفاتيح
- إمكانية إستخدام المفتاح العام من قبل أطراف متعددة.
- دعم التوقيع الرقمي.

أمّا بالنسبة للسلبيات فهي:

- بطئ في الأداء حيث أن عمليات التشفير وفك التشفير أبطأ بكثير من نظيراتها في التشفير المتماثل.
- تعقيد رياضي أكبر مما يتطلب موارد حسابية أعلى.
- زيادة في حجم المفاتيح.



الشكل (4-4) التشفير غير المتماثل

(4-2) حماية البيانات أثناء النقل باستخدام بروتوكولات SSL/TLS

تعد حماية البيانات أثناء انتقالها عبر الشبكات من أهم متطلبات أمن المعلومات؛ نظراً لأن البيانات المنقولة تكون عرضة لمجموعة من التهديدات مثل التنصت أو التعديل أو إعادة الارسال غيرالمشروع و لمعالجة هذه التحديات طورت بروتوكولات تهدف إلى تأمين الاتصال بين الأطراف المختلفة. ومن أبرز هذه البروتوكولات **SSL (Secure Socket Layer)** و **TLS (Transport Layer Security).**

بروتوكول **TLS** يعد امتداداً وتطويرا لبروتوكول **SSL** الذي تم استخدامه تجاريا في تسعينيات القرن الماضي وقد تم اعتماده رسميا كبروتوكول قياسي من قبل منظمة **IETF** لتأمين البيانات المنقولة على شبكات الحاسوب ولا سيما عبر الإنترنت. يعمل بروتوكول **TLS** فوق بروتوكول طبقة النقل **TCP** لضمان موثوقية الاتصال .

يتكون بروتوكول TLSمن بروتوكولين رئيسين:

1. بروتوكول المصافحة (**Handshake Protocol**): الذي يكون مسؤولاً عن التفاوض بشأن خوارزميات التشفير التي سيتم استخدامها وإنشاء المفاتيح بالإضافة إلى التنبيهات الأمنية.
2. بروتوكول التسجيل (**Record Protocol**): ويكون مسؤول عن تأمين البيانات عبر التشفير بالخوارزميات التي تم اختيارها بواسطة بروتوكول المصافحة والتحقق من سلامتها.

آلية عمل بروتوكول TLS

تبدأ العملية بما يعرف بالمصافحة (**Handshake**) وهي سلسلة من الرسائل المتبادلة بين أطراف الاتصال تهدف إلى التفاهم على مجموعة من المعايير الأمنية التي سيتم تطبيقها لتأمين الاتصال حيث يتم في هذه المرحلة تحديد خوارزميات التشفير التي يدعمها كل طرف والتحقيق في هوية الأطراف المتصلة بواسطة شهادة رقمية موثوقة (**Certificate**) وبعد ذلك يتم توليد و تبادل المفاتيح اللازمة لتأمين الاتصال. يتم في هذه المرحلة عادة إستخدام خوارزمية **RSA** للتشفير غير المتماثل (**Asymmetric Encryption**) لتبادل المفاتيح بشكل أمن حيث يرسل العميل (**Client**) المفتاح العام للخادم (**Server**) أو يستقبله منه و يتم من خلال إنشاء مفتاح سري مشترك يستخدم لاحقا لتشفير البيانات بطريقة متماثلة (**Symmetric Encryption**).

بعد إتمام عملية المصافحة يتم الانتقال إلى مرحلة تشفير البيانات أثناء النقل والتي تستخدم فيها خوارزميات التشفير المتماثل مثل **AES** حيث يعد التشفير المتماثل الخيار الأمثل في هذه المرحلة بسبب سرعته في تشفير البيانات خاصة عند التعامل مع كميات كبيرة منها. ولضمان سلامة البيانات وعدم التلاعب بمحتوى الرسائل يتم تطبيق إليه تحقق تعتمد على خوارزميات التجزئة (**Hash Function**) مثل خوارزمية **SHA** (**Secure Hash Algorithm**) حيث تقوم هذه الخوارزمية بإنشاء بصمة رقمية فريدة لكل رسالة بحيث يتم اكتشاف أي تغيير أو تعديل في البيانات.

بروتوكول HTTPS هو التطبيق العملي لبرتوكول TLS

عزيزي الطالب لابد وأن مر عليك عند تصفحك لمواقع الإنترنت ولاحظت في أعلى المتصفح وجود نوعين من العناوين **http://** أو **https://** فما هو الفرق بينهما ؟ **http** هو اختصار (**Hyper Text Transfer Protocol**) وهو بروتوكول يستخدم لنقل صفحات الويب من الخادم (Server) إلى المتصفح ويعمل بصورة افتراضية على منفذ (**port 80**) لكن المشكلة في **http** أنه لا يشفر البيانات أثناء نقلها مما يعني أن أي شخص على نفس الشبكة يمكنه قراءة ما ترسله أو تستقبله أمّا **https** فهو اختصار (**http secure**) أي نفس البروتوكول السابق لكن يضاف إليه طبقة حماية بأستخدام **SSL/TLS** ويعمل على منفذ 443 و يضمن تشفير جميع مكونات جلسة الاتصال بما في ذلك عناوين **URL** ومحتويات الصفحة والملفات التعريفية و الترويسات (**Headers**) وبهذا يتم تحقيق حماية شاملة للبيانات ضد أي محاولة لاعتراض و تعديل البيانات من قبل أي طرف خارجي أثناء النقل.

(4-3) إدارة النسخ الاحتياطية واستراتيجيات استعادة البيانات

رغم أن تقنيات التشفير وبروتوكولات الحماية مثل **TLS** تمثل وسائل فعالة لحماية البيانات أثناء النقل إلاّ أن ذلك لا يغني عن اتخاذ تدابير إضافية تضمن الحفاظ على توافر البيانات (**Availability**) وسهولة استعادتها في حالة حدوث أي خلل أو فقدان غير متوقع للبيانات وبالتالي نضمن تحقيق نظام متكامل لحماية البيانات يشتمل على المفاهيم الأساسية (السرية و التكامل والتوافر)التي تمثل ما يعرف بمثلث الأمان أو مثلث الحماية (**CIA Triad**) التي تم مناقشتها في بداية الفصل. ستتعرف عزيزي الطالب في الفقرات القادمة على مفهوم النسخ الاحتياطي و الاستعادة الآمنة للبيانات التي تكون أنظمة آمنة يعتمد عليها على المستوى البعيد.

(4-3-1) إدارة النسخ الاحتياطية

تشير إدارة النسخ الاحتياطية إلى العملية التي يتم من خلالها إنشاء نسخ مكررة من البيانات الهامة وتخزينها بشكل أمن في مواقع بديلة. تهدف هذه النسخ إلى توفير بديل موثوق يمكن الرجوع إليه في حالات فقدان البيانات بسبب خلل تقني أو حذف غير مقصود للبيانات أو تلف في الأجهزة وكذلك الهجمات الإلكترونية مثل برامج الفدية. ومن أنواع النسخ الاحتياطي:

- **النسخ الاحتياطي الكامل (Full Backup):** يتضمن نسخ جميع البيانات المحددة في كل مرة يتم فيها إنشاء النسخ الاحتياطي. يوفر هذا النوع استعادة شاملة للبيانات ولكنه يتطلب مساحة تخزين كبيرة و وقتا أطول لإتمام العملية.
- **النسخ التفاضلي (Differential Backup):** يقوم بنسخ جميع البيانات التي تم تغييرها منذ آخر نسخة احتياطية ويتطلب مساحة خزن أقل من النسخ الاحتياطي الكامل.
- **النسخ التزايدي (Incremental Backup):** ينسخ فقط التعديلات التي طرأت منذ آخر نسخة احتياطية أيا كان نوعها. يتميز بكفاءة إستخدام مساحة التخزين وسرعة في عملية النسخ ولكن استعادة البيانات تستغرق وقتا أطول.

تعد استراتيجيات النسخ الاحتياطي الحجر الأساس في خطط استمرارية الأنظمة و يتم تحديد هذه الاستراتيجيات بناء على:

1. تحديد أولويات البيانات بناء على أهميتها ومستوى الحماية المناسب لها.
2. اختيار نوع النسخ الاحتياطي المناسب بالاعتماد على حجم البيانات و تكرار التغيير.

سوف تتعرف عزيزي الطالب في تمرين (11) على إنشاء نسخة احتياطية كاملة للنظام (**System Image**) يتم خزنها على قرص صلب خارجي.

(4-3-2) استراتيجية استعادة البيانات

تعد استراتيجيات استعادة البيانات مكونا رئيسيا لا يقل أهمية عن تقنيات التشفير أو النسخ الاحتياطي. فوجود نسخ احتياطية من البيانات لا يعني بالضرورة ضمان استعادتها ما لم تكن هناك خطة واضحة ومنهجية لاسترجاع تلك البيانات في الوقت المناسب و بأقل تأثير ممكن على استمرارية العمل.

تعرف استراتيجيات استعادة البيانات بانها مجموعة من الإجراءات و التقنيات التي تهدف إلى إسترجاع البيانات الحساسة والمهمة في حال تعرضها للفقد أو التلف نتيجة لأعطال فنية أو هجمات إلكترونية, وتبنى هذه الاستراتيجيات على مفهومين أساسيين:

- **هدف زمن الاستعادة (Recovery Time Objective – RTO)** و هو أقصى وقت مسموح لتعطل النظام قبل أن يبدأ تأثيره السلبي.
- **هدف نقطة الاستعادة (Recovery Point Objectives – RPO)** وهو الحد الأقصى لكمية البيانات التي يمكن فقدانها دون أن تأثر بشكل كبير على النظام.

تعتمد فعالية استراتيجيات الاستعادة على مجموعة من العوامل التقنية والتنظيمية من ابرزها:

1. **تحديد الأولويات:** يتم تصنيف البيانات حسب درجة أهميتها بحيث تكون الأنظمة و البيانات الحرجة في مقدمة الأولويات.
2. **نوعية النسخ الاحتياطية:** تختلف خطة الاستعادة تبعا لنوعية النسخ المستخدمة (كاملة – تزايديه – تفاضلية) إذ أن لكل نوع مزايا وسلبيات تؤثر على سرعة الاستعادة ومدى تعقيدها.
3. **تعدد أماكن التخزين:** يشمل إستخدام أكثر من موقع لتخزين النسخ الاحتياطية مثل التخزين المحلي أو الخارجي أو السحابي.
4. **إختبار البيانات بشكل دوري:** تعد الاختبارات الدورية لاستعادة البيانات من النسخ الاحتياطية ضرورية للتحقق من جاهزية البيانات عند الطوارئ.
5. **التوثيق الدقيق:** تشمل الاستراتيجيات الناجحة دليلا مكتوبا يوضح بالتفصيل الخطوات الواجب اتباعها عند تنفيذ عملية الاستعادة للبيانات.

وتبرز الحاجة إلى هذه الاستراتيجيات بشكل خاص في البيئات التي تتطلب استمرارية في توافر البيانات مثل البنوك والأنظمة الحكومية وبالتالي يتم تحقيق مفهوم التوافر **(Availability)** الذي تعتمد عليه هذه المؤسسات. من خلال تمرين (11) سوف تتعرف عزيزي الطالب على كيفية استعادة النظام من نسخة احتياطية كاملة **(System Image)**

4-4 أهمية التحقق الدوري من سلامة النسخ الاحتياطية

في ظل الاعتماد المتزايد على النظم الرقمية لحفظ البيانات الحساسة والمؤسسية، يبرز النسخ الاحتياطي كأحد الأركان الجوهرية في استراتيجية حماية البيانات. غير أن النسخ الاحتياطي في حد ذاته لا يُعد ضمانًا كافيًا لاستعادة البيانات، إذ تبقى فعاليته مشروطة بمدى صلاحية النسخ وقدرتها

الفعلية على إسترجاع المعلومات عند الطوارئ. من هنا، تكتسب عملية التحقق الدوري من سلامة النسخ الاحتياطية أهمية خاصة في إطار الحفاظ على استمرارية العمل وحماية البيانات من التلف أو الفقدان.

تشير دراسة بحثية أعدت في **Stanford University** إلى أن أنظمة التخزين طويلة الأمد تُواجه تحديات خطيرة تتعلق بما يُعرف بـ الأعطال الكامنة **(Latent Faults)**، وهي الأخطاء أو المشكلات التي تُصيب البيانات أو وسائط التخزين دون أن تكون مرئية أو قابلة للكشف في الوقت الفعلي. فهي لا تظهر عند عملية النسخ أو أثناء تخزين البيانات، بل تُكتشف فقط عند محاولة الوصول إلى هذه البيانات بعد مرور فترة زمنية طويلة. ويعود ذلك غالبًا إلى تعرّض وسائط التخزين لتلف فيزيائي تدريجي، مثل تدهور القطاعات **(sectors)** أو تعفّن البتات **(bit rot)**، أو بسبب أخطاء برمجية في عمليات النسخ أو الكتابة لم يتم رصدها في وقتها. هذا النوع من الأعطال يمثل تحديًا خطيرًا لأن البيانات تبدو سليمة ظاهريًا، لكن عند الحاجة الفعلية إلى استعادتها، يتبين أنها تالفة أو غير قابلة للقراءة. وقد تؤدي هذه الحالات إلى فقدان دائم للبيانات، خاصة إذا كانت النسخ الاحتياطية المتاحة قد أُنشئت على وسائط مصابة بنفس الخلل أو تم تخزينها دون آلية تحقق دورية. أوضحت الدراسة أن الاعتماد فقط على النسخ الاحتياطية دون إجراء تحقق دوري، يؤدي إلى انخفاض كبير في موثوقية النظام، حيث قد تمر شهور أو سنوات قبل اكتشاف الخلل، وحينها تكون استعادة البيانات مستحيلة. ولهذا السبب، يجب تبني آلية تحقق دورية تُعرف بعملية **"Scrubbing"**، يتم فيها فحص النسخ الاحتياطية ومقارنتها بنسخ مرجعية أو بأستخدام رموز التحقق **(Checksums)**. هذه العملية لا تقتصر فقط على اكتشاف الأخطاء، بل تساعد أيضًا في تحديد معدل تلف البيانات وتقدير عمر وسائط التخزين المستخدمة.

من أهم المشكلات المرتبطة بخزن النسخ الاحتياطية:

1. **الخطأ البشري:** يُعد الخطأ البشري من الأسباب الشائعة لفقدان البيانات، سواء من خلال الحذف غير المقصود، أو سوء التعامل مع الأجهزة والبرمجيات. وقد يؤدي ذلك إلى إتلاف أو حذف بيانات حساسة، خصوصًا في بيئات العمل التي تفتقر إلى ضوابط دقيقة.
2. **أعطال المكونات:** تتضمن أعطال المكونات المادية والبرمجية، بما في ذلك أجهزة التخزين، البرمجيات والشبكات
3. **تقادم الوسائط والأجهزة:** يتسبب تقادم الوسائط والأجهزة في صعوبة إسترجاع البيانات المخزنة، خاصة عند عدم توفر أدوات القراءة المناسبة. ومن الأمثلة الشائعة تقنيات التخزين القديمة التي لم تعد مدعومة في الأنظمة الحديثة.
4. **تقادم البرمجيات وتنسيقات الملفات:** مع مرور الوقت، قد تصبح تنسيقات الملفات غير قابلة للقراءة نتيجة توقف دعم البرمجيات الخاصة بها، مما يؤدي إلى فقدان إمكانية الوصول إلى البيانات رغم توافرها ماديًا.

5. **فقدان السياق والمعلومات التعريفية:** تُعد البيانات التعريفية (**Metadata**) ضرورية لفهم محتوى البيانات المخزنة وتفسيرها. وفقدانها يُعقّد من عملية الاسترجاع، خصوصًا في حالات البيانات المشفرة التي تعتمد على حفظ المفاتيح والمعلومات المرتبطة بها.
6. **الهجمات الإلكترونية:** تعرض الأنظمة الرقمية لهجمات إلكترونية تؤثر بشكل مباشر أو تدريجي على موثوقية البيانات وسلامتها.

ولضمان فعالية النسخ الاحتياطية، يجب مراعاة عدة نقاط من أهمها:

1. إختبار استعادة البيانات بشكل منتظم إذ من الضروري عدم الاكتفاء بتنفيذ عمليات النسخ، بل يجب إسترجاع البيانات على بيئة اختبارية بشكل دوري للتحقق من سلامة الملفات والإعدادات.
2. إستخدام آليات تحقق آلي التي توفرها بعض أنظمة النسخ الاحتياطي الحديثة متمثلة بأدوات مدمجة تقوم بالتحقق الفوري من النسخ بعد اكتمال العملية.
3. تحديد سياسة تحقق واضحة تتضمن جداول زمنية دقيقة للتحقق، مع تحديد المسؤوليات والمهام.
4. الاحتفاظ بسجلات موثقة لجميع عمليات التحقق ونتائجها لتكون مرجعًا عند الحاجة.

من خلال ما ذُكر أعلاه، يتبين لك عزيزي الطالب أن التحقق الدوري من البيانات لا يقل أهمية عن عملية النسخ الاحتياطي نفسها، بل يُعد مكملًا أساسيًا لها. إذ أن النسخ دون تحقق منتظم قد يُخفي أعطالًا كامنة تؤدي إلى فقدان البيانات عند الحاجة إليها. لذا، فإن ضمان سلامة النسخ هو أحد الركائز المهمة في بناء أنظمة موثوقة لاستعادة البيانات وضمان استمرارية العمل المؤسسي. كما يسهم التحقق الدوري في الكشف المبكر عن الأعطال وتصحيحها قبل أن تتحول إلى مشاكل تؤثر على توافر البيانات وتكاملها. وبالتالي، فإن دمج هذا الإجراء ضمن سياسات النسخ الاحتياطي يُعد ضرورة استراتيجية وليس مجرد خيار تقني.

(5-4) أدوات حذف البيانات بشكل آمن لمنع استعادتها

النمو المتسارع لحجم البيانات الرقمية وتوسع استخدامها في مختلف المجالات، جعل هناك حاجة فعلية إلى تطبيق إجراءات فعالة لحذف البيانات بشكل أمن ودائم، لا سيما مع تزايد المخاطر المرتبطة بتسرب المعلومات أو استعادتها من قبل جهات غير مخولة. لا يقتصر هذا التحدي على المؤسسات الكبرى فحسب، بل يشمل كذلك الأفراد الذين يواجهون سيناريوهات يومية مثل استبدال الأجهزة أو التخلص منها، دون إدراك أن حذف الملفات أو إجراء إعادة ضبط المصنع لا يُعد كافيًا لمسح آثار البيانات الحساسة. وفي هذا السياق، تلعب أدوات الحذف الأمن دورًا أساسيًا في منع إسترجاع البيانات بأستخدام التقنيات المتقدمة.

تتنوع وسائل حذف البيانات بحسب طبيعة جهاز التخزين المستخدم، مثل الأقراص الصلبة (**HDD**) و (**SSD**)، وأجهزة التخزين المحمولة (**USB flash drives**)، وبطاقات الذاكرة، وغيرها من الوسائط. ورغم اختلاف خصائص هذه الأجهزة، فإن الهدف المشترك هو منع إمكانية استعادة البيانات بعد حذفها، وخاصة عندما تتضمن معلومات ذات طابع حساس أو سري.

يمكن تصنيف أهم الأساليب المُتبعة لحذف البيانات من الأجهزة المحلية كما يأتي:

1. الكتابة الفوقية (Overwriting)

تُعد هذه الطريقة من أكثر الأساليب شيوعًا لحذف البيانات بشكل أمن، حيث تعتمد على إعادة الكتابة فوق البيانات الأصلية بمحتوى عشوائي أو أنماط غير مفهومة، مما يُصعب عملية الاسترجاع. وتُستخدم أدوات برمجية متخصصة تُتيح للمستخدم تحديد عدد مرات الكتابة فوق البيانات، وفقًا لسياسات الأمان المطلوبة. على سبيل المثال، قد تقوم إحدى المؤسسات بأستخدام أداة متخصصة لمسح قرص يحتوي على معلومات مالية حساسة، وتُجري عملية الكتابة الفوقية عدة مرات لضمان إزالة البيانات بالكامل.

2. التهيئة (Formatting)

رغم أن تهيئة جهاز التخزين تُعد إجراء تقليديًا لحذف البيانات، إلاّ أنها في الغالب لا توفر مستوى أمان كافٍ. إذ تقوم عملية التهيئة بإزالة بُنية نظام الملفات فقط، دون أن تُزيل فعليًا المحتوى المخزن. ونتيجة لذلك، تظل البيانات قابلة للاسترجاع بأستخدام أدوات متقدمة، ما يجعل التهيئة غير كافية كإجراء مستقل لحذف البيانات الحساسة.

3. المسح الأمن (Secure Erase)

توفّر بعض الأجهزة، خصوصًا محركات أقراص **SSD**، خاصية "المسح الأمن " كميزة مدمجة، والتي تُتيح إزالة شاملة للبيانات من مناطق الذاكرة المختلفة، بما في ذلك المناطق المخفية التي لا يمكن الوصول إليها بالطرق التقليدية. وتعمل هذه الخاصية على الكتابة فوق جميع القطاعات بأستخدام أنماط محددة أو عشوائية، ما يجعل البيانات غير قابلة للاستعادة حتى من خلال أدوات تحليل متقدمة.

4. التدمير الفيزيائي (Physical Destruction)

في الحالات التي تكون فيها الحاجة إلى ضمان الإزالة التامة وغير القابلة للاسترداد للبيانات، تُلجأ بعض المؤسسات إلى التدمير المادي لوسائط التخزين. تشمل هذه الإجراءات تمزيق محركات الأقراص، أو سحقها ميكانيكيًا، أو تعريضها للحرارة الشديدة (الحرق)، أو إزالة مغناطيسيتها. ويُعد هذا الأسلوب معتمدًا في المؤسسات الأمنية أو الهيئات الحكومية التي تتعامل مع معلومات شديدة الحساسية.

5. التشفير وحذف المفاتيح (Encryption and Key Destruction)

رغم أن التشفير لا يُعد طريقة مباشرة لحذف البيانات، إلاّ أنه يُستخدم كوسيلة فعّالة لضمان عدم الوصول إلى البيانات في حالة عدم توفر مفاتيح التشفير. عند تشفير الملفات بمستوى أمان مرتفع، يصبح الوصول إلى محتواها مستحيلاً بدون المفاتيح المناسبة. وعليه، فإن حذف مفاتيح التشفير يعادل عمليًا إلغاء إمكانية الوصول إلى البيانات نهائيًا، حتى وإن لم يتم حذفها فعليًا من وسائط التخزين.

أمّا بالنسبة للأجهزة المحمولة التي تعد وسيطاً أساسيًا لتخزين المعلومات الحساسة والشخصية، بات من الضروري اعتماد ممارسات فعالة لحذف البيانات منها بشكل أمن ودائم، ولا سيما عند اتخاذ قرار استبدال الأجهزة أو التخلص منها. إذ أن الحذف التقليدي أو إعادة ضبط المصنع قد لا يكون كافيًا لضمان إزالة جميع آثار البيانات، مما قد يُعرّض خصوصية الأفراد أو المؤسسات لمخاطر الاسترجاع غير المصرح به. ويمكن تلخيص أهم الإجراءات المتبعة لضمان حماية المعلومات في الأجهزة المحمولة:

1. إستخدام أدوات الحذف الأمن **(Secure Erase)** لإجراء عملية حذف متقدمة، حيث تعمل على استبدال كامل محتوى وسائط التخزين بأنماط بيانات عشوائية، مما يجعل استعادة البيانات أمرًا بالغ الصعوبة.
2. إزالة البيانات المخزنة على خدمات الحوسبة السحابية المرتبطة بالجهاز، مثل الصور، والمستندات، وجهات الاتصال، لتفادي بقاء أي نسخ مخزنة خارج الجهاز قد تكون عرضة للوصول غير المصرح به.
3. الانتباه إلى مكونات التخزين القابلة للإزالة، كشرائح **SIM** وبطاقات **SD**، ومسح محتواها بشكل أمن أو التخلص منها بطرق مادية مناسبة لضمان عدم إسترجاع البيانات.
4. مراجعة التطبيقات المثبتة من أطراف ثالثة (التطبيقات التي لم تأتِ مع نظام التشغيل بصورة افتراضية وانما يتم تثبيتها من قبل المستخدم) وحذف أي معلومات حساسة مخزنة ضمنها.
5. في الحالات التي تتطلب درجات عالية من السرية أو الامتثال الأمني، قد يكون التدمير الفيزيائي للجهاز وسيلة نهائية مضمونة، حيث يتم تدمير وسائط التخزين ماديًا لضمان عدم إمكانية إسترجاع أي بيانات منها مستقبلاً.

توجد أدوات جاهزة على الإنترنت تستخدم لإزالة البيانات وضمان عدم استرجاعها مرة اخرى، ويُعد برنامج **Eraser** واحدًا من أبرز البرامج المجانية مفتوحة المصدر التي تُستخدم على نطاق واسع في بيئة نظام التشغيل **Windows**. يتميز البرنامج بقدرته على تنفيذ عمليات الحذف الأمن من خلال الكتابة الفوقية المتكررة على الملف أو المجلد المراد حذفه بأستخدام خوارزميات قوية التي تجعل البيانات غير قابلة للاسترداد نهائيًا. عزيزي الطالب، من خلال تنفيذك لتمرين رقم (12)، تكون قد اكتسبت مهارة أساسية في مجال أمن المعلومات تتمثل في حذف الملفات الحساسة بشكل أمن ودائم. أن فهمك لكيفية عمل أدوات الحذف المتقدمة وتطبيقك لها يعزز وعيك الرقمي، ويمكّنك من حماية بياناتك الشخصية والمؤسسية من مخاطر الاسترجاع غير المصرح به، وهي خطوة ضرورية في بناء سلوك مسؤول وآمن في العالم الرقمي.

كل خطوة نحو الاستدامة

هي استثمار في المستقبل

4 حماية انظمة التشغيل

رقم التمرين: 10 الزمن المخصص: ساعة واحدة

اسم التمرين: تشفير الملفات باستخدام **VeraCrypt**

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

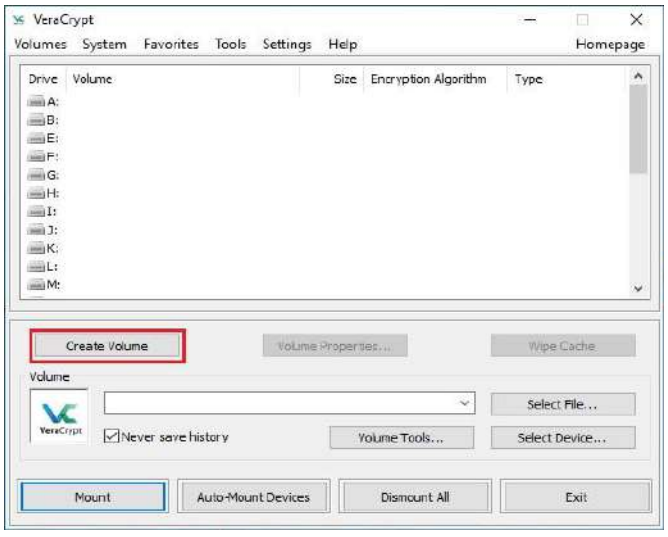
بعد إتمام هذا التمرين، سيتمكن الطالب من:

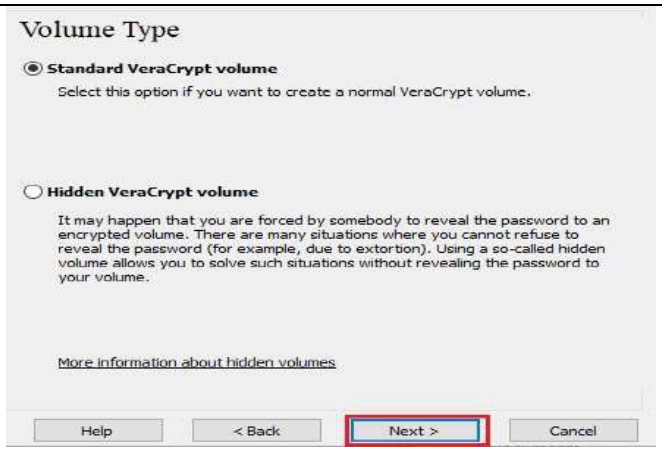
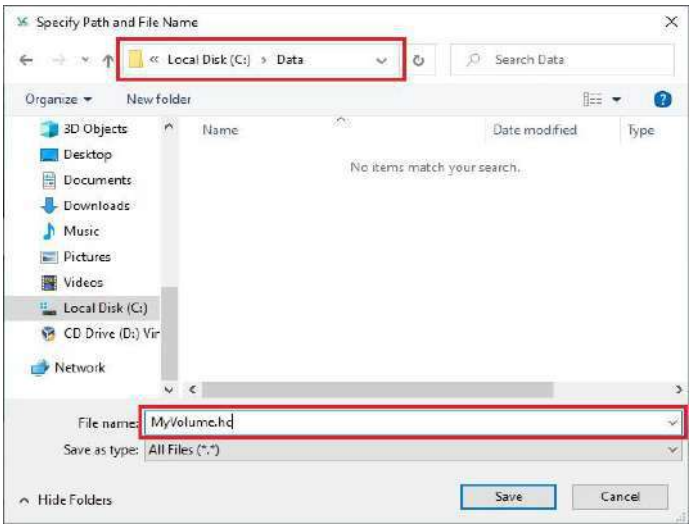
- إنشاء وحدة تخزين مشفرة باستخدام برنامج **VeraCrypt** وتحديد موقعها وحجمها.
- استخدام وحدة التخزين المشفرة في إضافة الملفات وحمايتها، مع القدرة على تنفيذ عمليات الربط (**Mount**) وفك الربط (**Unmount**) بشكل صحيح.

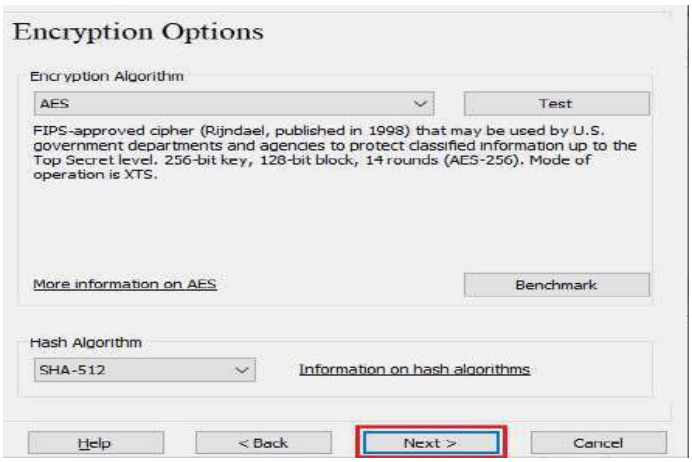
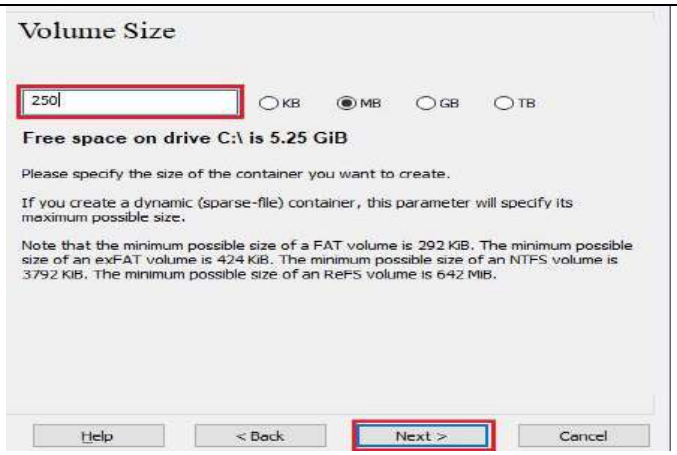
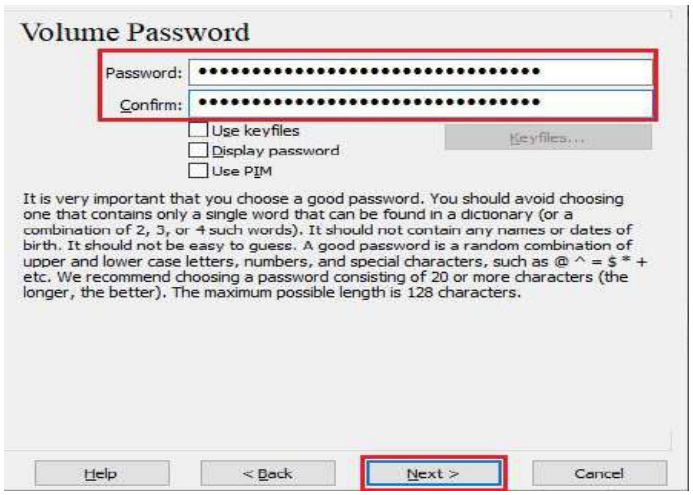
ثانياً: التسهيلات التعليمية

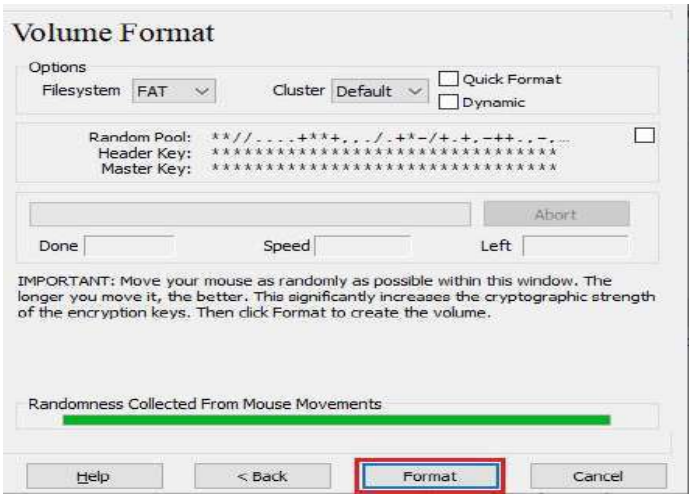
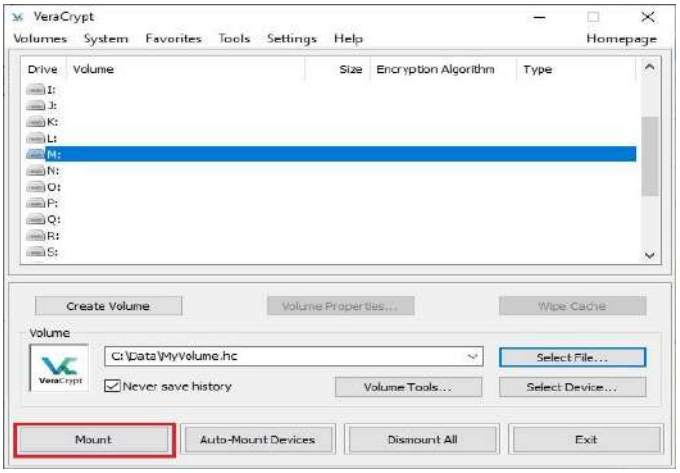
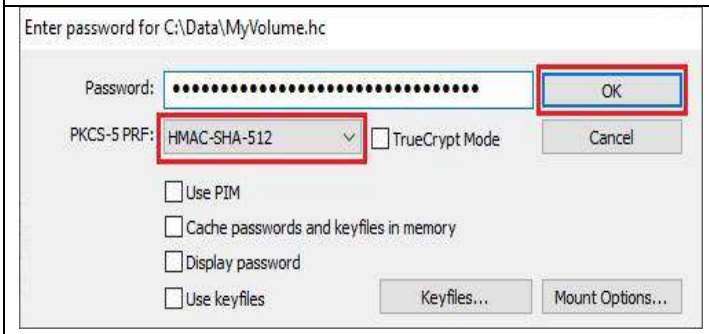
- أجهزة حاسوب مع نظام تشغيل **Windows 10/11**.

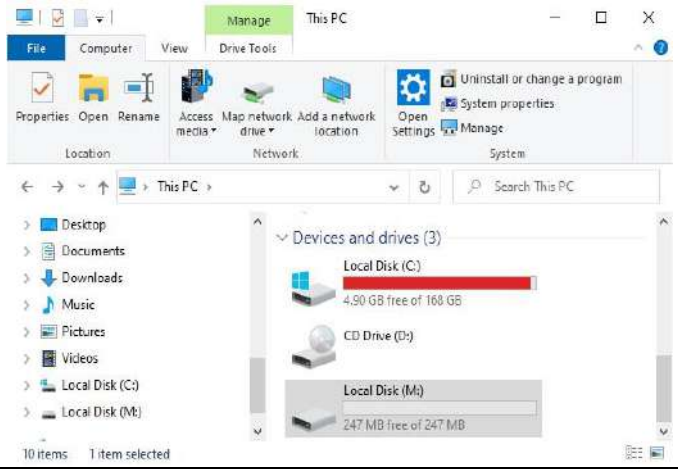
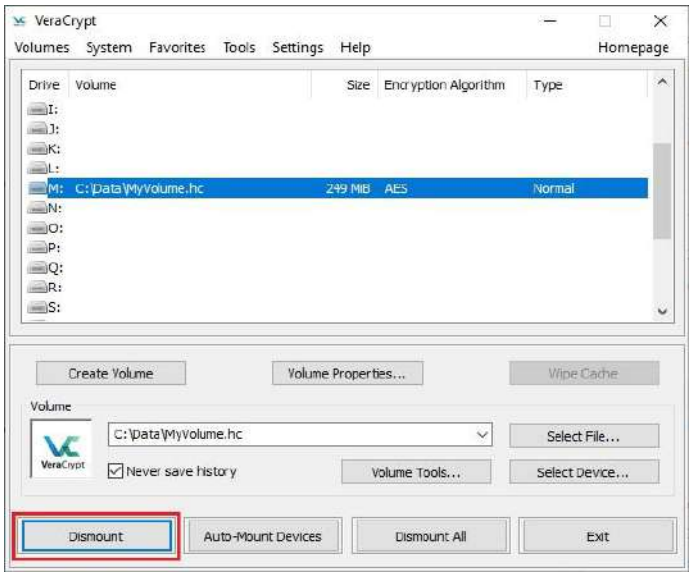
ثالثاً: خطوات تنفيذ التمرين

1	- اذهب إلى الموقع الرسمي للبرنامج: https://www.veracrypt.fr - قم بتحميل النسخة الأخيرة - شغّل ملف التثبيت واتبع التعليمات حتى يتم تثبيت البرنامج بنجاح. - قم بتشغيل البرنامج بالنقر المزدوج على ايقونته سوف تظهر لك نافذة تشغيل البرنامج واختر (**Create Volume**)	

2	قم باختيار إنشاء وحدة التخزين (الحاوية) ثم اضغط **Next**	
3	في هذه الخطوة يطلب منك تحديد نوع وحدة التخزين إذا كانت بالشكل القياسي **(Standard)** أو مخفي **(Hidden)** , في هذا التمرين، سيتم اختيار الوحدة القياسية، وهي الخيار الافتراضي ثم اضغط **Next**	
4	قم بتحديد المكان الذي ترغب في إنشاء ملف وحدة التخزين (الحاوية). ثم اعطه اسما مناسباً واضغط **Save**	

5	اختر خوارزمية التشفير المناسبة ثم اضغط **Next**	
6	في هذه الخطوة، يتم تحديد حجم ملف الحاوية الذي سيتم إنشاؤه بأستخدام **VeraCrypt**. في هذا التمرين، سنقوم باختيار حجم 250 ميغابايت كوحدة تخزين. (ملاحظة: يمكنك اختيار حجم مختلف حسب الحاجة).	
7	اختر كلمة مرور و يجب أن تكون قوية و آمنة ثم اضغط **Next**.	

8	في هذه الخطوة، يُطلب منك تحريك مؤشر الفأرة بشكل عشوائي قدر الإمكان داخل نافذة استمر في تحريك الفأرة حتى يتحول مؤشر العشوائية إلى اللون الأخضر. يُنصح بتحريك الفأرة لمدة لا تقل عن 30 ثانية؛ فكلما زادت مدة الحركة، زادت قوة المفاتيح التشفيرية. تهدف هذه العملية إلى تعزيز قوة التشفير من خلال توليد مفاتيح أكثر أمانًا بأستخدام بيانات عشوائية من حركة الفأرة. ثم اضغط **format** , سوف تظهر رسالة بأن العملية تمت بنجاح و اخرج من البرنامج.	
9	قم بفتح البرنامج من جديد واختر حرف لمحرك الأقراص من القائمة المتاحة ثم اختر نفس الملف الذي تم إنشاؤه في خطوة رقم (4) في هذه الخطوة تم ربط ملف وحدة التخزين (الحاوية) بهذا الحرف ليظهر كمحرك أقراص عادي في النظام بحيث ممكن نقل أي ملف إليه ويتم تشفيره مباشرة, ثم اضغط **Mount**.	
10	قم بطباعة نفس كلمة المرور التي تم تعيينها مسبقا في خطوة رقم (7)	

11	سوف يظهر محرك أقراص جديد باسم **Local disk: (M)** يمكنك عزيزي الطالب إضافة أي ملف ترغب بتشفيره	
12	بعد الانتهاء من إضافة الملفات افتح برنامج **VeraCrypt** ثم اختر **Unmount** سوف تلاحظ أن محرك الأقراص الجديد **Local disk: (M)** سوف يختفي من قائمة محركات الأقراص الصلبة مما يدل على تشفير الملفات بنجاح وحفظها بصورة آمنة	

المناقشة

1. ما الفرق بين وحدة التخزين القياسية والمخفية في **VeraCrypt**؟
2. ما الهدف من تحريك مؤشر الفأرة في خطوة إنشاء وحدة التخزين؟ وماذا يعني تحول المؤشر إلى اللون الأخضر؟
3. هل يمكن حذف ملف وحدة التخزين (الحاوية) من النظام؟ وماذا يحدث للبيانات المخزنة داخله إذا تم حذفه؟
4. ما هي وظيفة زر **(Mount)** في البرنامج؟ وماذا يحدث عند النقر عليه؟
5. كيف يتم التعامل مع محرك الأقراص الذي يظهر بعد الربط؟ وهل يمكن نقل ملفات إليه مثل أي محرك أقراص عادي؟

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:10	
اسم التمرين: تشفير الملفات بأستخدام **VeraCrypt**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب وتحميل البرنامج	%10		
2	تثبيت البرنامج	%10		
3	إنشاء وحدة التخزين و خوارزمية التشفير المناسبة و حمايتها بكلمة المرور	%10		
4	ربط وحدة التخزين بمحرك الأقراص ونقل البيانات لتأمينها	%10		
5	المناقشة	%5		
6	الزمن المخصص	%5		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

4 حماية انظمة التشغيل

رقم التمرين: 11 الزمن المخصص: ساعة واحدة

اسم التمرين: اعداد النسخ الاحتياطي باستخدام **Windows Backup**

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

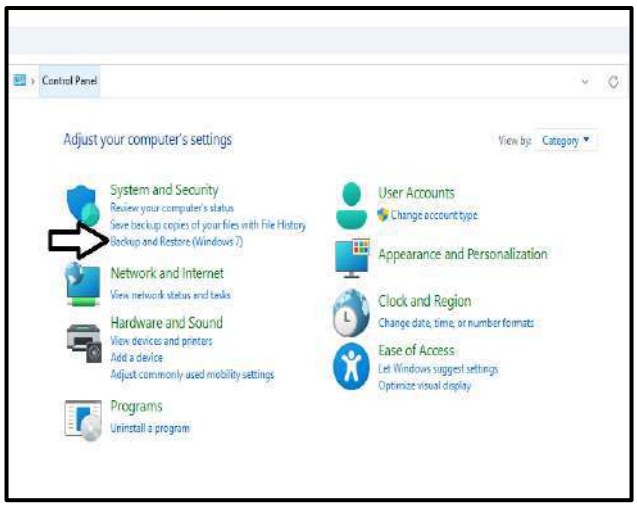
بعد إتمام هذا التمرين، سيتمكن الطالب من:

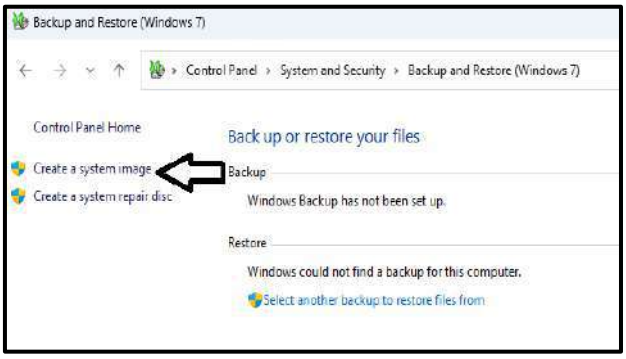
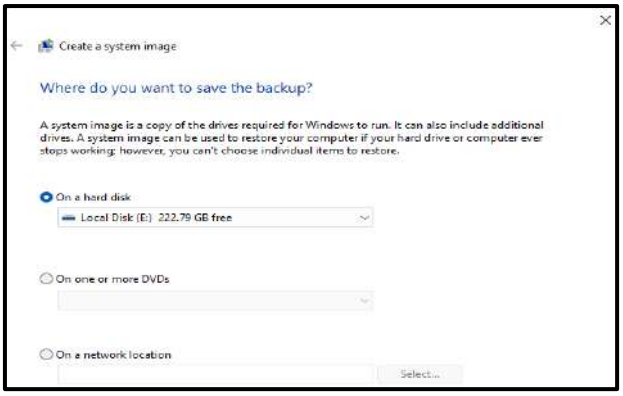
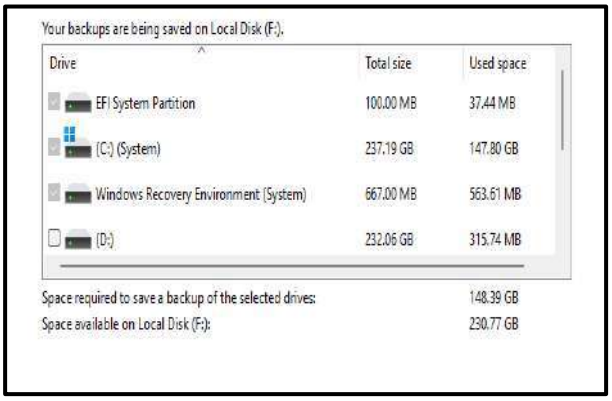
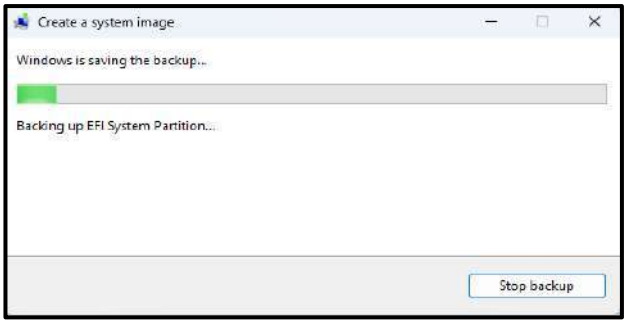
- إنشاء نسخة احتياطية كاملة للنظام (**System Image**) باستخدام أدوات **Windows**.
- تحديد الأقسام التي تشملها النسخة الاحتياطية، مثل قرص النظام (C).
- تنفيذ خطوات استعادة النظام باستخدام صورة احتياطية محفوظة مسبقًا (**System Image Recovery**).

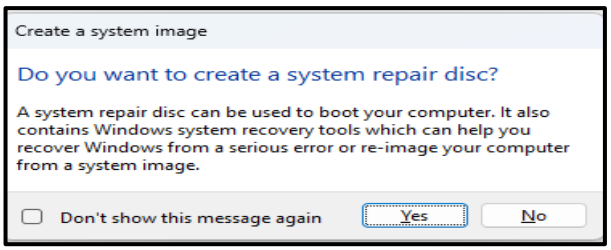
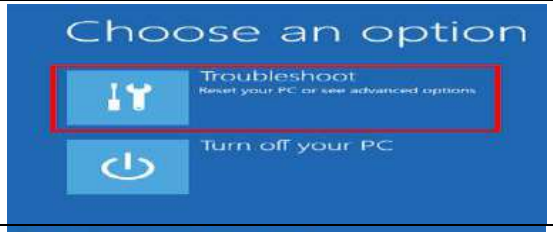
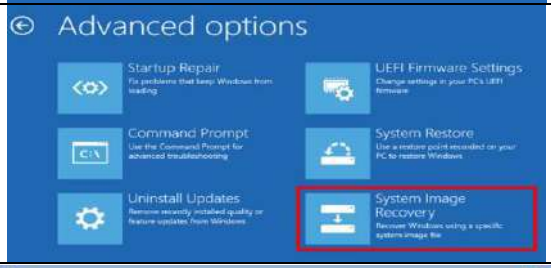
ثانياً: التسهيلات التعليمية

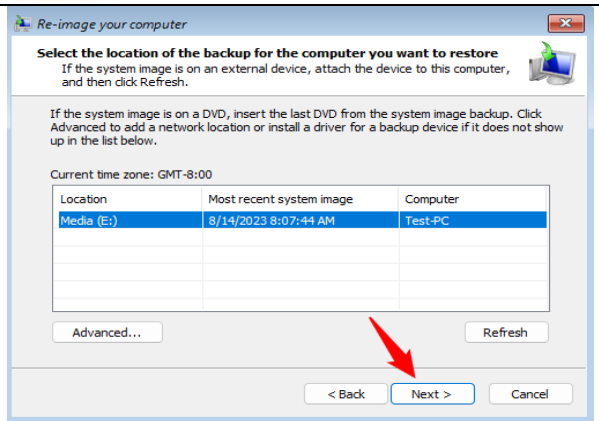
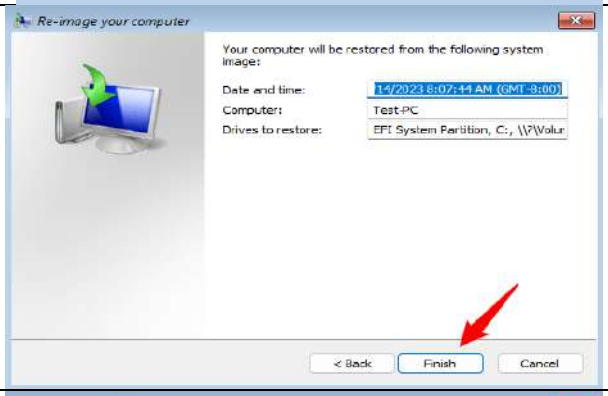
- أجهزة حاسوب مع نظام تشغيل **Windows 10/11**.
- قرص صلب خارجي (**External Hard Drive**) أو قسم ثانوي في القرص الصلب المحلي لحفظ النسخة الاحتياطية.

ثالثاً: خطوات تنفيذ التمرين

1	افتح لوحة التحكم (**Control Panel**) ومن خلال خيار (**System and Security**) اختر (**Backup and Restore**).	

2	من القائمة الجانبية اختر إنشاء صورة للنظام (**Create a System Image**).	
3	اختر أين تريد حفظ النسخة الاحتياطية (يفضل على قرص صلب خارجي).	
4	حدد الأقسام التي تريد نسخها (عادة تكون قرص **C** والنظام), يمكنك اختيار أي قرص آخر لعمل نسخة احتياطية.	
5	اضغط الآتي ثم إبدأ النسخ الاحتياطي.	

6	بعد الانتهاء من عملية إنشاء نسخة احتياطية للنظام سوف تظهر نافذة تسال المستخدم بإنشاء قرص إصلاح للنظام يمكنك تجاوز هذه الخطوة لعدم الحاجة لها حاليا.	
7	عند إسترجاع النسخة الاحتياطية قم بالآتي: - افتح قائمة إبدا (**Start**) ثم الإعدادات (**Settings**) - من الشريط الجانبي اختر **System** ثم **Recovery**. - من خلال **Recovery Options** اضغط على زر **Restart Now** بجوار **Advanced Setup** الجهاز سيعيد التشغيل وتظهر نافذة زرقاء إشارة لبداية إعدادات استعادة النظام من نسخة احتياطية محفوظة مسبقا.	
8	بمجرد أن يعمل الجهاز **Restart** وتظهر الشاشة الزرقاء: اختر **Troubleshot**.	
9	من نافذة **Advanced Options** اختر **System Image Recovery** سوف يبحث النظام عن النسخة الاحتياطية التي تم حفظها.	
10	حدد اختيار آخر صورة للنظام تم حفظها ثم اضغط **Next**.	

11	سوف يظهر آخر موقع تم حفظ نسخة احتياطية فيه حدده بالنقر عليه ثم اضغط **Next**.	
12	سوف يعرض لك استرداد صورة النظام ملخصًا لإجراءات الاستعادة المطلوب تنفيذها. إنقر على **Finish** للمتابعة.	
13	بعد ذلك تبدأ عملية استعادة صورة النظام التي قد تستغرق بعض الوقت، حسب حجم النسخة الاحتياطية.	
14	انتبه عزيزي الطالب للنقاط الآتية عند استعادة نسخة احتياطية للنظام: 1. أثناء عملية الاستعادة، ستتم إعادة مسح المحتوى من القسم **C** وإعادة تأهيله للحالة التي كانت عليها أثناء النسخ الاحتياطي. 2. يُفضل فصل أي أقراص خارجية لا تحتوي على النسخة الاحتياطية لتجنب الخطأ. 3. لا تقم بإيقاف تشغيل الجهاز أثناء العملية.	
15	المناقشة • ما الفرق بين النسخ الاحتياطي الكامل (**System Image**) والنسخ الاحتياطي للملفات فقط؟ وفي أي الحالات يُفضل إستخدام كل منهما؟ • ما أهمية اختيار قرص صلب خارجي لحفظ النسخة الاحتياطية؟ وهل هناك مخاطر في تخزين النسخة الاحتياطية على نفس القرص الرئيسي؟ • ما الفرق بين استعادة النظام من نسخة احتياطية (**System Image**) وبين استعادة إعدادات النظام (**System Restore**)؟	

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:11	
اسم التمرين: إعداد النسخ الاحتياطي بأستخدام **Windows Backup**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب والوصول إلى **Backup and Restore**	%10		
2	حفظ النسخة الاحتياطية على القرص الصلب	%10		
3	إجراء عملية الاستعادة للنسخة الاحتياطية	%10		
4	المناقشة	%10		
6	الزمن المخصص	%10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

4 حماية انظمة التشغيل

رقم التمرين: 12 الزمن المخصص: ساعة واحدة

اسم التمرين: حذف ملف بشكل آمن باستخدام برنامج **Eraser**

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

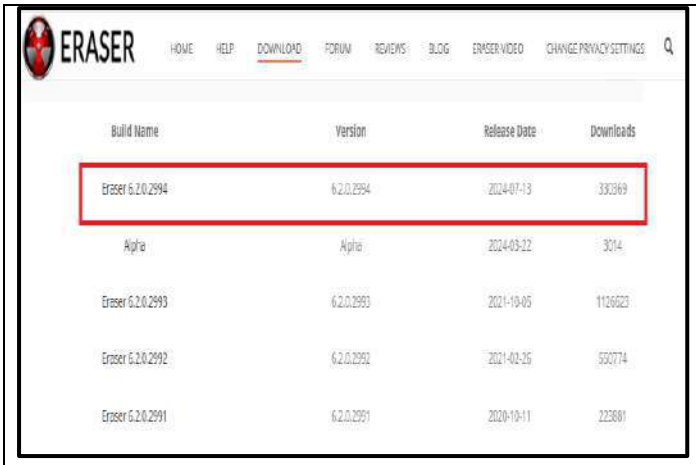
بعد إتمام هذا التمرين، سيتمكن الطالب من:

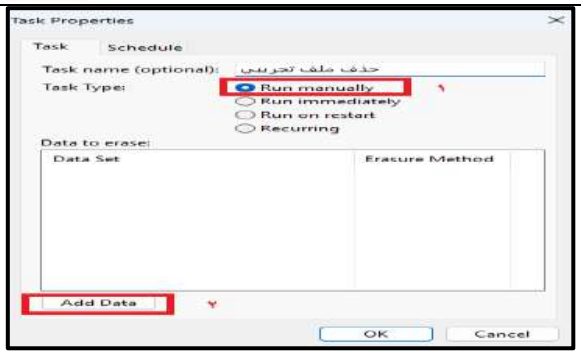
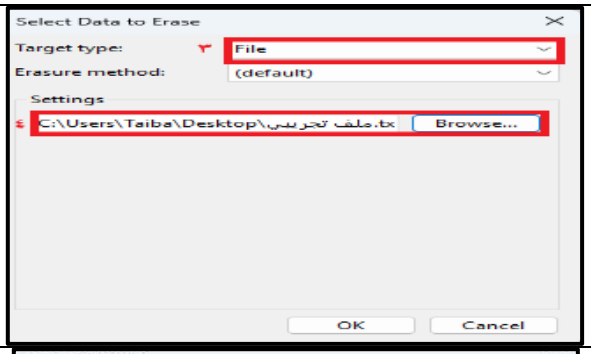
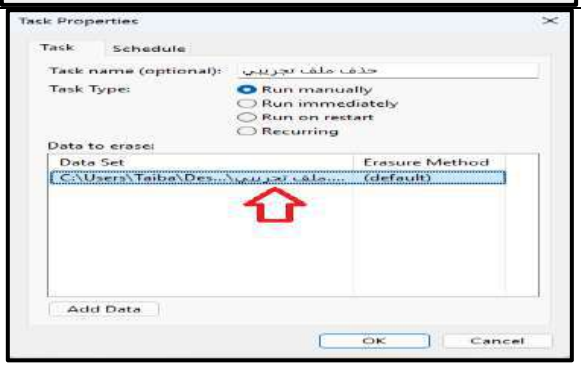
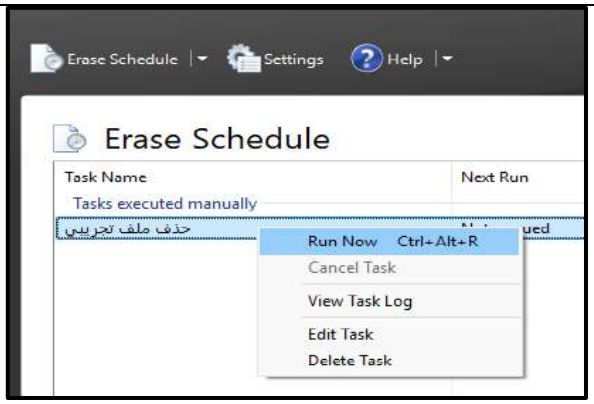
- استخدام برنامج **Eraser** لحذف الملفات بطريقة آمنة وغير قابلة للاسترجاع.
- فهم الفرق بين الحذف التقليدي والحذف الآمن باستخدام أدوات متخصصة.

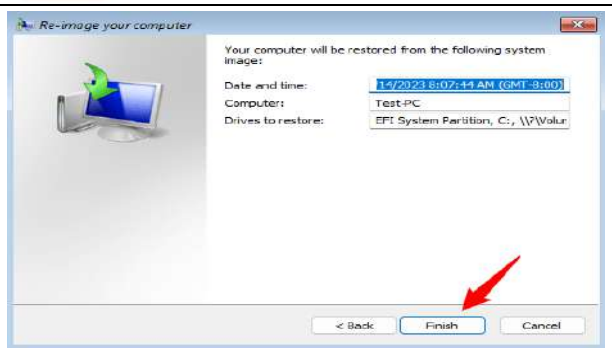
ثانياً: التسهيلات التعليمية

- جهاز كمبيوتر يعمل بنظام تشغيل **Windows10/11**.
- اتصال بالأنترنيت.

ثالثاً: خطوات تنفيذ التمرين

1	- اذهب إلى الموقع الرسمي للبرنامج: https://eraser.heidi.ie/ - قم بتحميل النسخة الأخيرة من البرنامج كما مبين بالشكل ادناه. - شغّل ملف التثبيت واتبع التعليمات حتى يتم تثبيت البرنامج بنجاح.	

2	- لإضافة مهمة حذف جديدة, إنقر بزر الماوس الأيمن داخل نافذة البرنامج، ثم اختر **New Task**. - أدخل اسمًا للمهمة، مثل "حذف ملف تجريبي"، ثم اضغط **Add Data**.	
3	- من نافذة الإعدادات، حدد **File**، ثم اضغط على **Browse** لاختيار الملف الذي ترغب بحذفه. - اضغط **OK** لتأكيد إضافة الملف.	
4	إنقر على الملف لتحديده ثم اضغط **OK**.	
5	- اضغط بزر الماوس الأيمن على اسم المهمة واختر **Run Now**. - انتظر حتى تكتمل العملية، وستظهر رسالة تؤكد نجاح الحذف الأمن .	

5	سوف يعرض لك استرداد صورة النظام ملخصًا لإجراءات الاستعادة المطلوب تنفيذها. إنقر على **Finish** للمتابعة.	
6	بعد ذلك تبدأ عملية استعادة صورة النظام التي قد تستغرق بعض الوقت، حسب حجم النسخة الاحتياطية.	

9

المناقشة

- ما الفرق بين الحذف التقليدي للملفات والحذف الأمن بأستخدام أدوات مثل **Eraser**؟
- ناقش مدى قابلية استعادة البيانات في كلتا الحالتين، وأثر ذلك على أمان المعلومات.
- لماذا يُعد الحذف الأمن ضروريًا قبل بيع أو التخلص من جهاز حاسوب أو وسائط تخزين؟
- وضّح لماذا يُستخدم التكرار في عمليات الكتابة، وما العلاقة بين عدد مرات الكتابة وقوة الحماية؟

نشاط

عزيزي الطالب، قم بالبحث عن أداة حذف بيانات أخرى مجانية ومفتوحة المصدر (مثل: **BleachBit** أو **SecureDelete**)، ثم قارنها ببرنامج **Eraser** من حيث:

- طريقة عملها.
- أنظمة التشغيل المدعومة.
- خيارات الحذف المتاحة.
- عدد خوارزميات الكتابة الفوقية.
- مدى سهولة الاستخدام.

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:12	
اسم التمرين: حذف ملف بشكل أمن بأستخدام برنامج **Eraser**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب و تحميل البرنامج	%10		
2	تثبيت البرنامج على الحاسوب	%10		
3	اختيار ملف لحذفه واتمام عملية الحذف	%10		
4	المناقشة	%10		
5	الزمن المخصص	% 10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

أسئلة الفصل الرابع

س1: عرف ما يأتي:

1-التشفير 2- النسخ التزايدي 3- المسح الآمن 4- خوارزمية DES 5- هدف زمن الاستعادة

س2: املأ الفراغات الآتية بما يناسبها:

1- يتكوّن مثلث الحماية (**CIA Triad**) من ثلاث ركائز أساسية هي ..... و .....و.....

2- عند إستخدام نفس المفتاح لعمليتي التشفير وفك التشفير، فإننا نستخدم التشفير من نوع .....

3- البروتوكول المسؤول عن التفاوض وإنشاء المفاتيح في **TLS** يُعرف بـ .....، بينما المسؤول عن تشفير البيانات يُسمى .....

4- الطريقة التي تعتمد على إعادة كتابة البيانات العشوائية فوق البيانات الأصلية تسمى .....

5- خوارزمية ..... تُستخدم على نطاق واسع في التطبيقات الحديثة وتُعد معيارًا عالميًا في التشفير المتماثل.

6- من أدوات الحذف الأمن المجانية والمفتوحة المصدر والتي تعمل على نظام **Windows** .....

س3- ما العناصر التي يعتمد عليها التشفير المتماثل؟ عددها مع الشرح.

س4- وضح الفرق بين خوارزمية **DES** و خوارزمية **3DES**

س5- ارسم مخططا يبين تصنيف خوارزميات التشفير إلى فئات متعددة.

س6- ما المقصود بخوارزمية **AES**؟ و ماهي التطبيقات التي تستخدم فيها هذه الخوارزمية؟

س7- عدد مع الشرح أنواع النسخ الاحتياطي.

س8- ما المقصود باستراتيجيات استعادة البيانات ؟ و ماهي المفاهيم الأساسية التي تتضمنها؟

س9- ماهي أهم المشكلات المرتبطة بخزن النسخ الاحتياطية ؟

س10- عدد الإجراءات المتبعة لضمان حماية المعلومات في الأجهزة المحمولة.

الفصل الخامس

حماية التطبيقات المثبتة على النظام

Protect applications installed on the operating system

أهداف الفصل الخامس

1. فهم أهمية تحديث التطبيقات لسد الثغرات الأمنية.
2. التعرف على الطرق المختلفة لاكتشاف البرامج الخبيثة وإزالتها.
3. تعلم كيفية التحكم في تشغيل التطبيقات بأستخدام قوائم بيضاء وصلاحيات تشغيل.
4. مراقبة استهلاك الموارد لتحديد التطبيقات غير الآمنة.

محتويات الفصل الخامس

(5-1) أهمية تحديث البرمجيات لسد الثغرات الأمنية.

(5-2) تحديد البرمجيات غير الآمنة وإزالتها.

(5-3) التعامل مع البرامج الخبيثة واكتشافها.

(5-4) مراقبة إستخدام الموارد لاكتشاف التطبيقات غير المصرح بها.

(5-5) التحكم في تشغيل التطبيقات بأستخدام قوائم بيضاء وصلاحيات التشغيل.

تمرين (13) إعداد التحديث التلقائي في أنظمة التشغيل.

تمرين (14) فحص البرمجيات الخبيثة بأستخدام أدوات مثل **Malwarebytes**.

تمرين (15) تكوين سياسات التحكم في التطبيقات بأستخدام **AppLocker**

الفصل الخامس

حماية التطبيقات المثبتة على النظام

Protect applications installed on the operating system

تمهيد

في عصر التكنولوجيا المتقدمة، تُعد التطبيقات المثبتة على أنظمة التشغيل جزءًا أساسيًا من حياتنا اليومية، سواء في العمل أو الترفيه أو التواصل. و مع تزايد الاعتماد على هذه التطبيقات، تبرز أهمية حمايتها من التهديدات الأمنية التي قد تعرض بياناتنا وأجهزتنا للخطر. حماية التطبيقات ليست مجرد مسؤولية مطوري البرمجيات، بل هي مسؤولية مشتركة بين المستخدمين والمؤسسات. في هذا السياق، يُعد فهم أساسيات حماية التطبيقات مهارة ضرورية لأي شخص يعمل في المجال التقني، حيث يساهم في بناء بيئة رقمية أكثر أمانًا وموثوقية.

(5- 1) أهمية تحديث البرمجيات

تحديث البرمجيات المثبتة على نظام التشغيل يُعد من الممارسات الأساسية التي يجب الاهتمام بها في عالم التكنولوجيا، سواء على مستوى الأفراد أو المؤسسات. هذه التحديثات ليست مجرد إضافات بسيطة، بل هي ضرورية لضمان استمرارية عمل النظام بكفاءة وأمان. وفيما يأتي شرح مفصل لأهمية هذه التحديثات فيما يخص الأمان والحماية:

- غالبًا ما تحتوي التحديثات على إصلاحات للثغرات الأمنية التي تم اكتشافها في الإصدارات السابقة. حيث يستغل القراصنة (**hackers**) هذه الثغرات لاختراق الأنظمة، لذا فإن التحديث يقلل من فرص الهجمات.
- تعزز التحديثات من قوة البرمجيات ضد الهجمات الإلكترونية، مثل هجمات الفيروسات والبرمجيات الخبيثة.
- قد تشمل التحديثات إضافة تقنيات أمان متقدمة، مثل تحسين جدران الحماية أو إضافة تشفير أقوى.
- تعالج بعض التحديثات مشكلات في الأداء قد تؤثر على أمان النظام، مثل تسريبات الذاكرة أو الأخطاء التي قد تُستغل.
- تساعد التحديثات في مواكبة التهديدات الأمنية الجديدة، حيث يتم تحديث قواعد البيانات الخاصة بالبرامج الأمنية لاكتشاف البرمجيات الخبيثة الحديثة.
- تضمن التحديثات توافق النظام مع أحدث معايير الأمان والخصوصية، مما يحمي البيانات من الاختراق. عزيزي الطالب سنتاول في التمرين رقم (13) كيفية تحديث نظام التشغيل **Windows**.

(2-5) تحديد البرمجيات غير الآمنة وإزالتها

في العصر الرقمي، يعتمد الناس بشكل كبير على البرمجيات في أجهزة الحاسوب والهواتف الذكية لإنجاز المهام اليومية. لكن ليست كل البرمجيات آمنة، فقد تحتوي بعضها على فيروسات أو برامج تجسس تهدد خصوصية المستخدمين وأمن معلوماتهم. في هذا الدرس، سنتعرف على كيفية تحديد البرمجيات غير الآمنة وإزالتها لحماية أجهزتنا ومعلوماتنا الشخصية.

يمكن تحديد البرمجيات غير الآمنة في نظام التشغيل من خلال عدة طرق تعتمد على ملاحظة أداء الجهاز وسلوك البرامج المثبتة. يجب الانتباه إلى أي بطء غير معتاد في الجهاز أو استهلاك مفرط لموارده مثل المعالج والذاكرة، حيث يمكن أن تكون هذه علامات على وجود برمجيات ضارة تعمل في الخلفية. كذلك قد تظهر نوافذ إعلانية منبثقة بشكل متكرر أو يتم إعادة توجيه المتصفح تلقائيًا إلى مواقع مشبوهة مما يشير إلى احتمال وجود برمجيات غير آمنة. بالإضافة إلى ذلك، يمكن ملاحظة تثبيت برامج جديدة دون علم المستخدم، وهو ما قد يكون ناتجًا عن برمجيات خبيثة تعمل على تنزيل تطبيقات غير موثوقة. لفحص الجهاز والتأكد من سلامة البرامج، يمكن إستخدام أدوات الحماية مثل برامج مكافحة الفيروسات التي تقوم بتحليل التطبيقات والملفات بحثًا عن أي تهديدات أمنية. كما يمكن التحقق من قائمة العمليات النشطة في مدير المهام لمعرفة ما إذا كان هناك أي تطبيقات تعمل دون سبب واضح أو تستهلك موارد زائدة. يفضل أيضًا مراجعة قائمة البرامج المثبتة عبر إعدادات النظام وإزالة أي برامج غير معروفة أو لم يقم المستخدم بتثبيتها بنفسه. من المهم تحديث نظام التشغيل والبرامج بانتظام، لأن التحديثات تتضمن إصلاحات للثغرات الأمنية التي قد تستغلها البرمجيات الضارة. وأخيرًا، يجب تجنب تنزيل البرامج من مصادر غير موثوقة وعدم فتح الروابط أو المرفقات المشبوهة لأنه يمكن أن تكون وسائل لنشر البرمجيات غير الآمنة في النظام. لحماية الأجهزة من البرمجيات غير الآمنة، يجب تجنب تحميل الملفات من مصادر غير رسمية وعدم فتح الروابط أو المرفقات المشبوهة في البريد الإلكتروني. كما يُفضل إستخدام كلمات مرور قوية وتفعيل جدار الحماية لحماية الجهاز من التهديدات الإلكترونية. من خلال اتباع هذه الإجراءات، يمكن للمستخدمين الحفاظ على أمان أجهزتهم وبياناتهم أثناء إستخدام التكنولوجيا في حياتهم اليومية.

لإزالة البرمجيات غير الآمنة من جهازك، اتبع الخطوات الآتية بشكل منظم:

- **تحديد البرامج المشبوهة**

ابحث عن البرامج غير المعروفة أو التي لم تقم بتثبيتها بنفسك، أو تلك التي تستهلك موارد النظام بشكل غير طبيعي. يمكن التحقق من ذلك عبر "إدارة المهام" أو "قائمة التطبيقات المثبتة".

- **إزالة البرامج يدويًا**

افتح لوحة التحكم أو إعدادات النظام وتوجه إلى إزالة البرامج أو **Apps & Features** واختر البرنامج المشبوه واضغط على إلغاء التثبيت (**Uninstall**).

- **إستخدام الوضع الأمن (Safe Mode)**

بعض البرمجيات الضارة قد تمنع حذفها أثناء التشغيل العادي. ولحل ذلك أعد تشغيل الجهاز في الوضع الأمن . ثم حاول إزالة البرنامج مجددًا من خلال نفس الخطوات أعلاه.

- **إستخدام أدوات متخصصة**

استخدم برامج موثوقة لإزالة البرامج غير المرغوب فيها، مثل **"Revo Uninstaller"** أو **"Obit Uninstaller"** هذه الأدوات تزيل أيضًا الملفات المتبقية بعد الحذف.

- **فحص الجهاز ببرنامج مكافحة الفيروسات**

من المهم بعد إزالة البرمجيات غير الآمنة إجراء فحص شامل للجهاز والتأكد من عدم وجود أي ملفات متبقية قد تعيد تثبيت البرامج الضارة تلقائيًا. احذف أي ملفات أو تهديدات يتم اكتشافها. تأكد من تحديث قاعدة بيانات الفيروسات قبل الفحص.

- **التأكد من إزالة الملفات المتبقية**

بعض البرامج تترك ملفات في مجلدات النظام. تفقد مجلد **"Program Files"** و**"AppData"** وامسح أي مجلدات متبقية تخص البرنامج المحذوف (بحذر).

- **تحديث نظام التشغيل وبرامج الحماية**

يُنصح بتحديث نظام التشغيل وجدار الحماية وبرامج الأمان لضمان حماية الجهاز من أي تهديدات مستقبلية.

- **الوقاية المستقبلية**

للوقاية من البرمجيات الضارة، لا تقم بتحميل برامج من مصادر غير موثوقة، تجنّب فتح الروابط أو الملفات المرفقة من جهات غير معروفة، واستخدم إضافات متصفح للحماية من المواقع الضارة.

(3-5) التعامل مع البرامج الخبيثة واكتشافها

يتضمن اكتشاف البرامج الضارة والخبيثة مراقبة سلوك النظام واستخدام أدوات الأمان وإجراء عمليات التفتيش اليدوية. فيما يأتي بعض الطرق الرئيسة لتحديد البرامج الضارة على نظامك:

غالبًا ما يكون السلوك غير المعتاد للنظام هو أول علامة على الإصابة بالبرامج الضارة. إذا أصبح جهاز الكمبيوتر الخاص بك بطيئًا فجأة، أو تعطل بشكل متكرر، أو عرض إعلانات منبثقة بشكل غير متوقع، فقد يكون مصابًا. تشمل العلامات الأخرى التغييرات غير المصرح بها لإعدادات النظام، أو إستخدام وحدة المعالجة المركزية أو الذاكرة بشكل كبير دون سبب واضح، أو نشاط شبكة غير مبرر. إذا أعاد متصفح الويب توجيهك إلى مواقع ويب غير مألوفة أو ظهرت أشرطة أدوات جديدة دون إذنك، فقد يشير هذا إلى وجود برامج ضارة.

يعد إستخدام برامج مكافحة الفيروسات والبرامج الضارة أحد أكثر الطرق فعالية لاكتشاف البرامج الضارة. يمكن أن يساعد تشغيل فحص كامل للنظام بأستخدام برنامج أمان محدث في تحديد البرامج الضارة وإزالتها. توفر العديد من أدوات الأمان أيضًا حماية في الوقت الفعلي لمنع تثبيت البرامج الضارة في المقام الأول. يمكن لـ **Windows Defender** وMalwarebytes وبرامج الأمان الأخرى اكتشاف الملفات المشبوهة وحجرها.

يمكن أن يساعد الفحص اليدوي أيضًا في اكتشاف البرامج الضارة. يمكن أن يكشف فحص "إدارة المهام" عن العمليات غير المعروفة أو المشبوهة التي تعمل في الخلفية عن التهديدات المخفية. أن مراجعة البرامج المثبتة في إعدادات النظام والبحث عن التطبيقات غير المألوفة هي طريقة أخرى لاكتشاف البرامج الضارة. بالإضافة إلى ذلك، فإن مراقبة نشاط الشبكة بأستخدام أدوات مدمجة مثل **Windows Resource Monitor** أو تطبيقات الطرف الثالث يمكن أن تكشف عن عمليات نقل البيانات المشبوهة إلى خوادم غير معروفة.

إذا تم اكتشاف البرامج الضارة، فيجب إزالتها على الفور بأستخدام برنامج أمان أو عن طريق إلغاء تثبيت البرنامج المشبوه يدويًا. في بعض الحالات، يمكن أن يساعد التمهيد في الوضع الأمن في إزالة البرامج الضارة التي تقاوم الحذف. يمكن أن يساعد تحديث البرامج ونظام التشغيل وتجنب التنزيلات المشبوهة واستخدام كلمات مرور قوية في منع الإصابات المستقبلية. يتناول التمرين رقم (14) طريقة فحص واكتشاف البرمجيات الخبيثة بأستخدام برنامج **Malwarebytes**.

(4-5) مراقبة استخدام الموارد لاكتشاف التطبيقات غير المصرح بها

تُعد مراقبة إستخدام موارد النظام من الطرق الفعالة لاكتشاف التطبيقات غير المصرح بها التي قد تعمل على أجهزة الحاسوب أو الشبكات. في عالم تقنية المعلومات الحديث، قد يحاول بعض المستخدمين تثبيت برامج غير مصرح بها على أجهزة العمل أو الدراسة، وهذه البرامج قد تشكل مخاطر أمنية أو تؤثر سلبًا على أداء النظام بأكمله.

عند النظر إلى استهلاك موارد النظام، يمكن للمسؤول التقني ملاحظة أنماط غير عادية تشير إلى وجود تطبيقات غير مصرح بها. فمثلاً، قد يلحظ إستخداماً مرتفعًا للمعالج في أوقات غير متوقعة، أو استنزافًا للذاكرة العشوائية بشكل غير طبيعي، أو زيادة في حركة البيانات عبر الشبكة دون وجود سبب واضح. هذه المؤشرات قد تنبه المسؤول إلى وجود برامج تعمل في الخلفية لم يتم التصريح بها.

5 حماية انظمة التشغيل

يمكن إستخدام أدوات مراقبة النظام المدمجة في أنظمة التشغيل مثل مدير المهام في ويندوز (**Windows**) أو مراقب النشاط في ماك (**Mac**) أو أدوات مثل "**top**" و "**htop**" في أنظمة لينكس (**Linux**). تعرض هذه الأدوات قائمة بالتطبيقات النشطة والموارد التي تستهلكها. كما توجد برامج متخصصة للمراقبة مثل "**ProcessExplorer**" أو "**Sysmon**" يمكنها تسجيل إستخدام الموارد على مدار فترات زمنية طويلة وإنشاء تقارير مفصلة عن أداء النظام.

عند فحص إستخدام الشبكة، يمكن تحديد البرامج التي تتصل بالإنترنت ومراقبة كمية البيانات المرسلة والمستلمة. قد تقوم بعض التطبيقات غير المصرح بها بإرسال بيانات إلى خوادم خارجية، مما يمكن اكتشافه من خلال مراقبة حركة الشبكة غير المعتادة. من المهم أيضًا مراقبة العمليات التي تبدأ مع بدء تشغيل النظام، حيث تميل البرامج غير المصرح بها إلى تكوين نفسها للبدء تلقائيًا. يمكن فحص قائمة برامج بدء التشغيل للتأكد من أن جميع البرامج المدرجة هي برامج معتمدة ومعروفة.

يعد تنفيذ سياسة للتحكم في التطبيقات خطوة وقائية مهمة لمنع تثبيت البرامج غير المصرح بها. يمكن إستخدام حلول البرمجيات التي تسمح فقط بتشغيل التطبيقات المعتمدة وتحظر تشغيل أي برنامج غير معتمد. إضافة إلى ذلك، يمكن الاستفادة من تقنيات مثل التوقيع الرقمي للبرامج والتحقق من سلامة الملفات لضمان أن البرامج المثبتة هي نسخ أصلية وغير معدلة. يمكن أيضًا مراقبة سجلات الأحداث في النظام للكشف عن أي محاولات لتثبيت برامج أو إجراء تغييرات غير مصرح بها.

أن تثقيف المستخدمين حول مخاطر البرامج غير المصرح بها وتأثيرها على أمن وأداء النظام يُعد جزءًا أساسيًا من استراتيجية الحماية الشاملة. عندما يفهم المستخدمون أهمية الالتزام بسياسات البرمجيات المعتمدة، تقل احتمالية محاولتهم تجاوز هذه السياسات. من خلال الجمع بين المراقبة المستمرة لاستخدام الموارد، وتطبيق سياسات التحكم في التطبيقات، وتثقيف المستخدمين، يمكن للمؤسسات التعليمية والشركات حماية أنظمتها من المخاطر المحتملة للتطبيقات غير المصرح بها والحفاظ على بيئة حوسبة آمنة وفعالة.

(5-5) التحكم في تشغيل التطبيقات باستخدام قوائم بيضاء وصلاحيات التشغيل

يعد التحكم في تشغيل التطبيقات بأستخدام القوائم البيضاء (**Allow List**) وصلاحيات التشغيل (**permissions**) من أبرز الأساليب الأمنية الفعالة التي تساعد المؤسسات في حماية أنظمتها. القائمة البيضاء هي طريقة تعتمد على مبدأ بسيط لكنه قوي، وهو السماح فقط بتشغيل التطبيقات المعروفة والموثوقة المدرجة في القائمة المعتمدة ، ومنع تشغيل أي تطبيق آخر غير مدرج في القائمة المعتمدة. تبدأ عملية التحكم في التطبيقات بإنشاء قائمة بيضاء تحتوي على جميع البرامج المسموح بها. يتم ذلك عن طريق تحديد التطبيقات الضرورية للعمل والتأكد من مصادرها ومن سلامتها. يمكن تعريف التطبيقات في القائمة البيضاء بعدة طرق مثل اسم الملف التنفيذي (**execution file**)، مسار التثبيت (**path**)، التوقيع الرقمي للناشر (**digital signature**)، أو قيمة التجزئة للملف (**Hash**). كلما كانت معايير التعريف أكثر تحديداً، كانت الحماية أكثر فعالية.

5 حماية انظمة التشغيل

عند تطبيق سياسة القوائم البيضاء، يتم ضبط النظام بحيث يجري التحقق من كل برنامج يحاول التشغيل، ويقارنه بالقائمة المعتمدة. إذا كان البرنامج مدرجاً في القائمة، يُسمح له بالعمل. أمّا إذا لم يكن كذلك، فسيتم حظره تلقائياً، وقد يتم إرسال إشعار للمسؤول عن النظام. يمنع هذا النهج تشغيل البرامج الضارة أو غير المصرح بها حتى لو تمكنت من الوصول إلى النظام.

توفر أنظمة التشغيل الحديثة أدوات مدمجة لتطبيق سياسات القوائم البيضاء. فمثلاً في نظام التشغيل ويندوز، يمكن إستخدام خاصية **"AppLocker"** أو **" Windows Defender Application Control"** التي تسمح بإنشاء قواعد للتحكم في التطبيقات المسموح بتشغيلها. في أنظمة ماك، توجد ميزة **"Gatekeeper"** التي تسمح بتقييد تثبيت البرامج حسب مصدرها. أمّا في أنظمة لينكس، فيمكن إستخدام أدوات مثل **"SELinux"** أو **"AppArmor"** لتطبيق سياسات أمنية صارمة.

بالإضافة إلى القوائم البيضاء، يمكن تطبيق صلاحيات التشغيل (**permissions**) التي تعتمد على مستويات الوصول المختلفة للمستخدمين. يُمنح كل مستخدم صلاحيات محددة تناسب دوره ومسؤولياته. على سبيل المثال، قد يُسمح للمدرسين بتشغيل برامج إدارية معينة، بينما يقتصر طلاب المدارس على تشغيل البرامج التعليمية فقط.

يمكن أيضاً تطبيق ما يُعرف بـ "التشغيل المقيد" للتطبيقات، حيث يُسمح بتشغيل التطبيق لكن مع تقييد وصوله إلى موارد النظام. على سبيل المثال، قد يُسمح لتطبيق معين بالعمل، لكن دون السماح له بالوصول إلى ملفات معينة أو إلى الإنترنت. تتطلب إدارة القوائم البيضاء وصلاحيات التشغيل عملية مراجعة وتحديث مستمرة. كلما ظهرت حاجة لتطبيقات جديدة، يجب تقييمها وإضافتها إلى القائمة البيضاء إذا كانت آمنة وضرورية. كما يجب مراجعة صلاحيات المستخدمين بشكل دوري وتعديلها حسب التغيرات في الأدوار والمسؤوليات.

من المهم أيضاً تنفيذ عمليات مراقبة وتسجيل لمحاولات تشغيل التطبيقات، سواء الناجحة أو المحظورة. هذا يساعد في اكتشاف أي محاولات للتحايل على القيود المفروضة، كما يوفر معلومات قيمة لتحسين السياسات الأمنية. تعتبر توعية المستخدمين جزءاً أساسياً من نجاح هذه الاستراتيجية. يجب شرح سبب وجود هذه القيود وأهميتها في حماية النظام، وتوفير آلية واضحة لطلب إضافة تطبيقات جديدة إلى القائمة البيضاء عند الحاجة. من خلال تطبيق هذه الإجراءات، يمكن للمؤسسات تحقيق توازن بين توفير بيئة عمل مرنة وضمان مستوى عالٍ من الأمان لأنظمتها المعلوماتية. عزيزي الطالب ستتعرف أكثر على هذا الموضوع عند تطبيق تمرين رقم (15) والذي يتطرق الى تكوين سياسات التحكم في التطبيقات بأستخدام **AppLocker** .

5 حماية انظمة التشغيل

رقم التمرين: 13 الزمن المخصص: ساعة واحدة

اسم التمرين: اعداد التحديث التلقائي في أنظمة التشغيل.

مكان التنفيذ: مختبر الحاسوب.

اولاً: الأهداف التعليمية

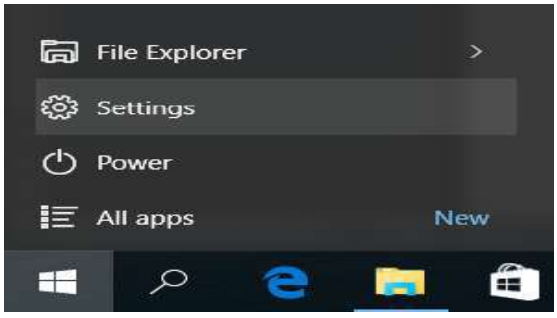
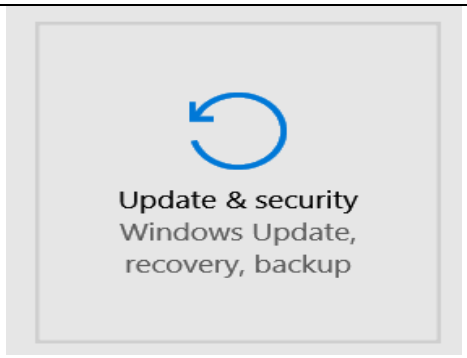
بعد إتمام هذا التمرين، سيتمكن الطالب من:

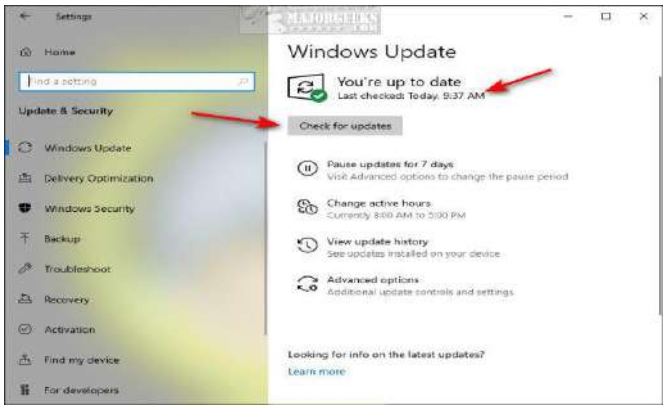
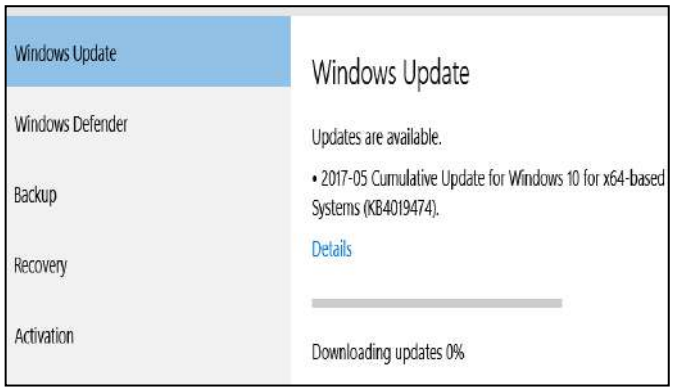
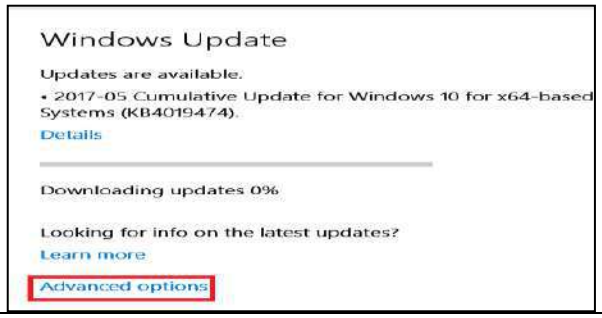
- فهم أهمية التحديثات الأمنية في حماية الأنظمة.
- إعداد التحديث التلقائي في نظام **Windows**.
- التحقق من حالة التحديثات وتاريخها.
- التعامل مع المشكلات الشائعة في عمليات التحديث.

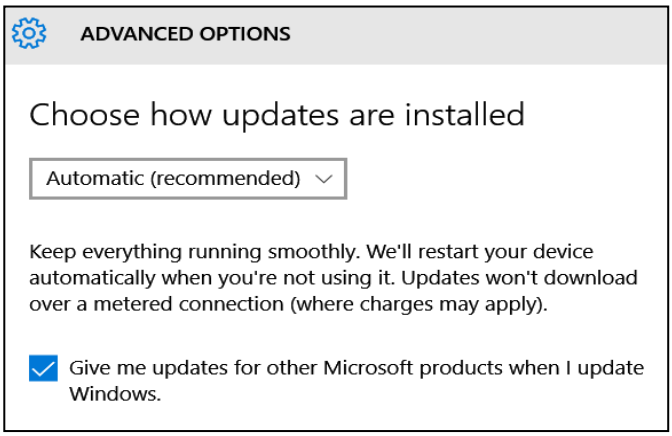
ثانياً: التسهيلات التعليمية

- أجهزة حاسوب مع نظام تشغيل **Windows 10/11**.
- اتصال بالإنترنت.

ثالثاً: خطوات تنفيذ التمرين

1	افتح قائمة ابدأ (**Start**) واختر الإعدادات (**Setting**).	
2	في نافذة الإعدادات، ستجد عدة خيارات اختر منها التحديث والأمان الموجود عادة في أسفل القائمة. (**Update & Security**).	

3	في القائمة الجانبية، اختر تحديثات ويندوز (**Windows Update**).	
4	اضغط على **Check for updates** (التحقق من التحديثات) لمعرفة إذا كانت هناك تحديثات متاحة.	
5	في حالة توفر تحديثات جديدة ستعرض امامك. ما عليك إلاّ الضغط على تنزيل التحديثات (**download update**) بعدها سيبدأ تنزيل التحديثات.	
6	لجعل التحديث تلقائي اذهب إلى خيارات متقدمة (**advanced options**) في نفس الصفحة.	

7	تأكد من تفعيل الخيارات الآتية: **Automatic updates** (التحديثات التلقائية). **Receive updates for other Microsoft products** (تلقي تحديثات لمنتجات مايكروسوفت الأخرى): يمكن تفعيلها إذا كنت تستخدم منتجات مايكروسوفت مثل **Office**.	
8	**المناقشة** • ما الفرق بين التحديث اليدوي والتحديث التلقائي في نظام **Windows** ؟ • كيف يمكنك التأكد من أن التحديثات تم تثبيتها بنجاح بعد تنزيلها؟ • في رأيك، هل يمكن أن يكون هناك سلبيات للتحديثات التلقائية؟ وضّح ذلك. • إذا لم تظهر لك أي تحديثات بعد الضغط على"**Check for updates**" ، ما الأسباب المحتملة؟	

صوتك من حقك

فعبّر عنه باحترام

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:**13**	
اسم التمرين: إعداد التحديث التلقائي في أنظمة التشغيل				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب والوصول إلى الإعدادات المطلوبة	%15		
2	مراحل تنفيذ خيارات التحديث التلقائي	%15		
3	المناقشة	%10		
4	الزمن المخصص	%10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

5 حماية انظمة التشغيل

رقم التمرين: 14 الزمن المخصص: ساعة واحدة

اسم التمرين: فحص البرمجيات الخبيثة باستخدام أدوات مثل **Malwarebytes**

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

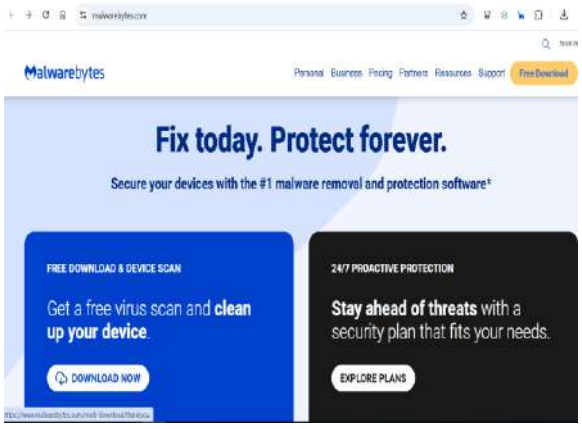
بعد إتمام هذا التمرين، سيتمكن الطالب من:

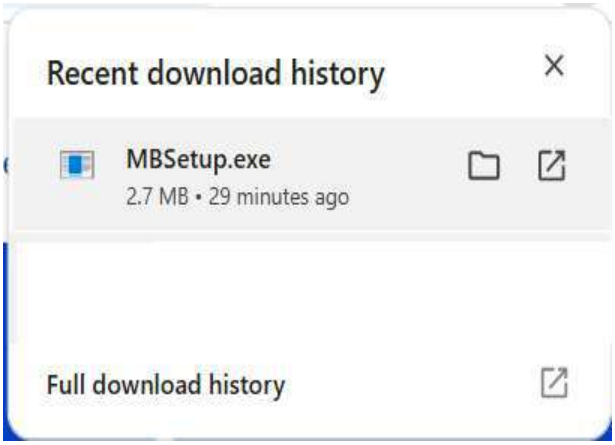
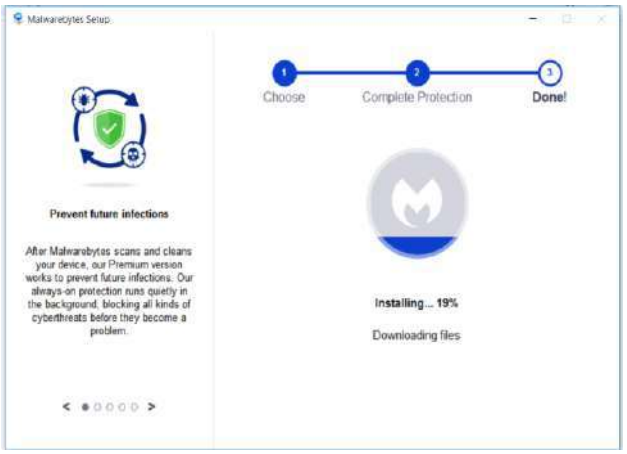
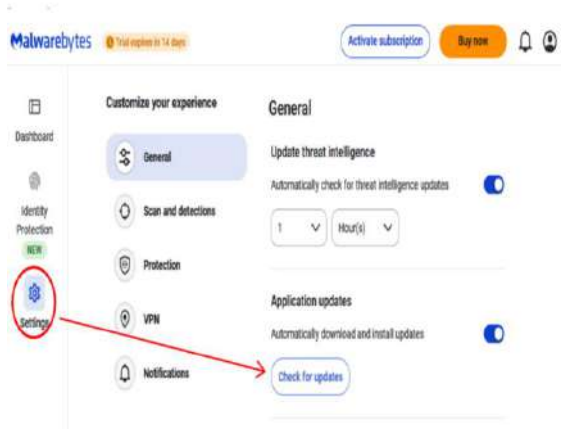
- فهم كيفية اكتشاف الفيروسات والبرمجيات الضارة باستخدام أدوات الأمن السيبراني.
- تجربة استخدام برنامج **Malwarebytes** على نظام **Windows**.
- تحليل التقارير واكتشاف الثغرات الأمنية في الملفات.

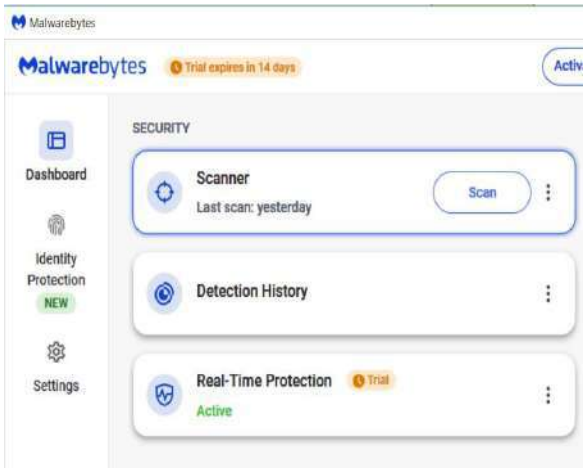
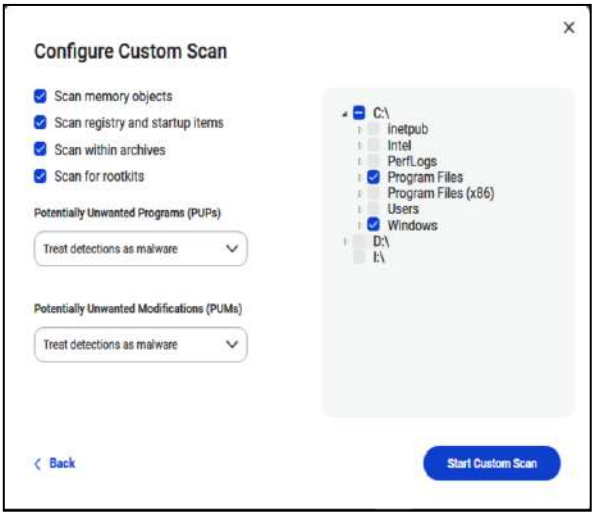
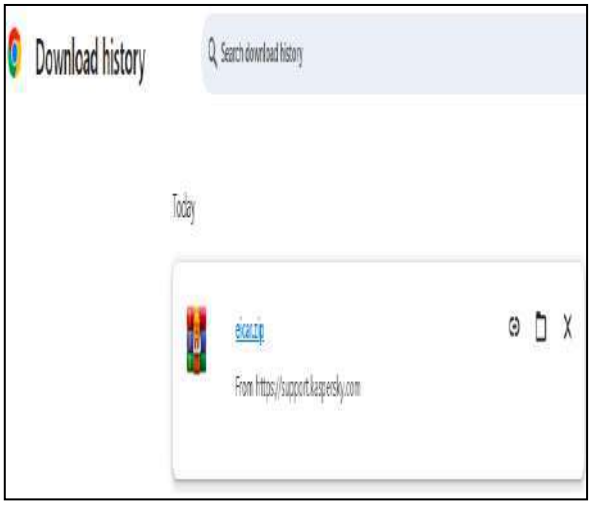
ثانياً: التسهيلات التعليمية

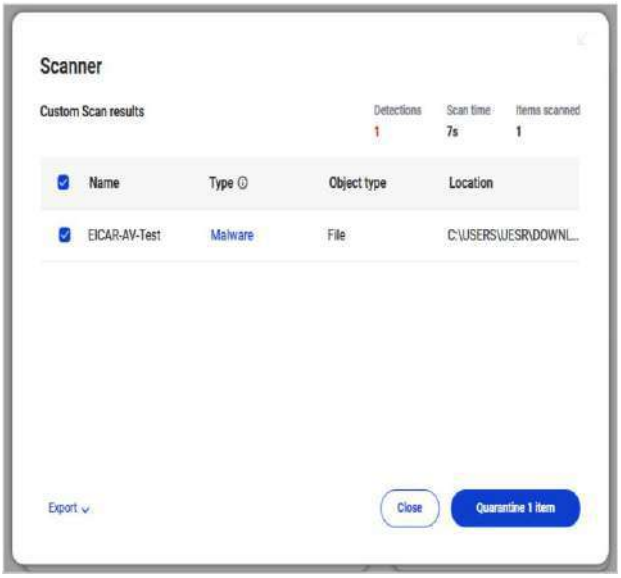
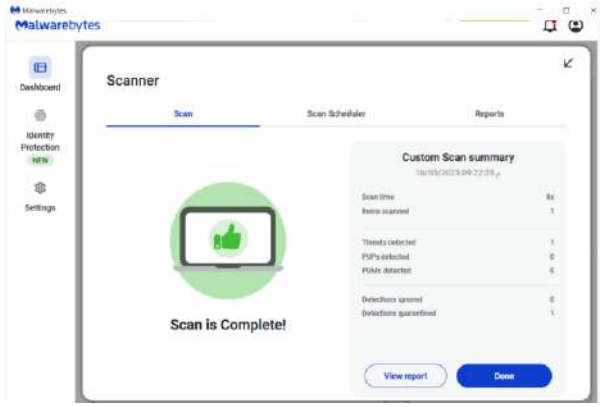
- جهاز كمبيوتر بنظام تشغيل **Windows** (لتثبيت **Malwarebytes**).
- اتصال بالإنترنت لتحميل البرامج وتحديثها.
- مجموعة من ملفات اختبار بعضها يحتوي على برمجيات خبيثة آمنة للتدريب مثل **EICAR Test File** وهو ملف آمن يستخدم لاختبار برامج مكافحة الفيروسات.

ثالثاً: خطوات تنفيذ التمرين

1	قم بتحميل نسخة تجريبية أو مجانية من **Malwarebytes** مناسبة من الموقع الرسمي **https://www.malwarebytes.com/** قم بالنقر على (**Free download**) اي تحميل مجاني.	

2	بعد النقر على (**Free download**) سيتم تنزيل الملف من الموقع الرسمي للبرنامج وتجده في مجلد التنزيلات (**download**) على حاسوبك باسم **MBSetup.exe**.	
3	قم بتشغيل الملف الذ تم تنزيله في الخطوة السابقة واتبع خطوات التثبيت.	
4	بعد اكتمال تثبيت البرنامج على نظام التشغيل **Windows** قم بفتح البرنامج وحدث قاعدة بيانات البرنامج باخر التحديثات المتاحة.	

5	عند الانتهاء من التحديث قم بإجراء مسح عام لحاسوبك اذهب إلى **Dashboard→ Scanner→ Scan.**	
6	عند الرغبة بإجراء فحص مخصص حدد الملفات أو المجلدات التي ترغب بفحصها (مثل ملفات **USB** أو مجلد **Windows** قم باتباع المسار الآتي: **Dashboard→ Scanner→ Scan→Advanced Scan→ Custom Scan** حدد القرص والمجلدات أو الملفات المراد فحصها وانقر على بدء الفحص الاختياري **Start custom Scan** المضللة باللون الأزرق في أسفل يمين الشاشة.	
7	لفحص فعالية البرنامج قم بتنزيل ملف (**EICAR**) من خلال الرابط الآتي أو أي موقع يسمح بتنزيل ملفات فحص مضادات الفايروسات **https://www.virusanalyst.com/eicar.zip** وهذا الملف هو ملف إختبار معتمد عالميًا لمحاكاة البرامج الضارة. يمكن استخدامه لاختبار ما إذا كان برنامج مضاد الفيروسات قادرًا على اكتشافه أم لا. الملف غير ضار تمامًا ولا يشكل أي خطر على النظام.	

8	افحص الملف الذي تم تنزيله والذي ستجده في مجلد التنزيلات بأستخدام برنامج **Malwarebytes** ستلحظ أن البرنامج تمكن من تشخيص أن الملف مشبوه ويحوي عنصرا واحدا ضارا ويمثل تهديد للنظام. لمعالجة هذا المحتوى الضار في الملف اضغط على **Quarantine** في أسفل يمين الشاشة والتي تعني (الحجر الصحي). هو إجراء أمني احترازي يضمن حماية الجهاز مع تقليل خطر الحذف غير الضروري للملفات. تمكن ميزة الحجر الصحي المستخدم من حذف الملف بشكل نهائي، استعادة الملف إذا كان غير ضار، أو إرسال الملف إلى الشركة المطورة لمضاد الفيروسات لتحليل إضافي.	
9	عند الانتهاء من معالجة المحتوى الضار ستظهر خلاصة المسح الذي قمت به. إنقر على **Done** للانتهاء من عملية الفحص. للاطلاع على التفاصيل الكاملة للملف الضار الضار بإمكانك النقر على (**View report**).	
10	**المناقشة** • ما معنى وضع الملفات في"**Quarantine**" ؟ ولماذا يُعد هذا الخيار بديلاً عن الحذف المباشر؟ • ماذا تتوقع أن يحدث لو لم يتم وضع الملف المشبوه في الحجر الصحي؟ ما المخاطر الممكنة؟ • كيف يمكن الاستفادة من خاصية "**View report**" بعد انتهاء الفحص؟ وما المعلومات التي تتوقع رؤيتها فيها؟ • إذا اكتشف البرنامج ملفًا ضارًا ولكنك متأكد أنه ملف سليم، كيف تتعامل مع الموقف؟	

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:14	
اسم التمرين: فحص البرمجيات الخبيثة بأستخدام أدوات مثل **Malwarebytes**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تنزيل برنامج **Malwarebytes** وتثبيته	%10		
2	تحديث قاعدة بيانات البرنامج	%10		
3	فحص الملفات بأستخدام البرنامج	%10		
4	المناقشة	%10		
5	الزمن المخصص	%10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

5 حماية انظمة التشغيل

رقم التمرين: 15 الزمن المخصص: ساعة واحدة

اسم التمرين: تكوين سياسات التحكم في التطبيقات باستخدام **AppLocker**

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

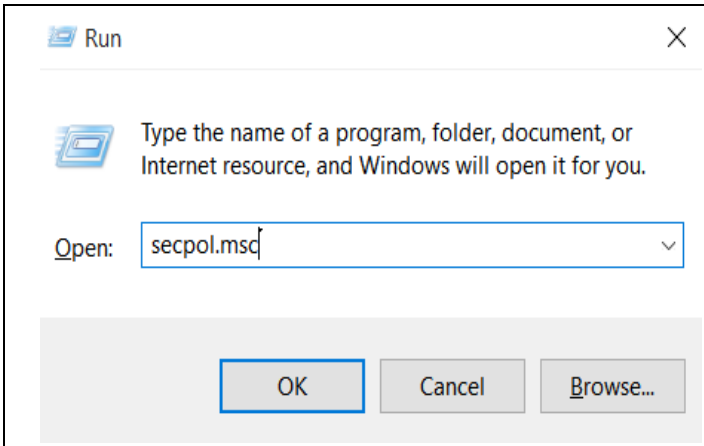
بعد إتمام هذا التمرين، سيتمكن الطالب من:

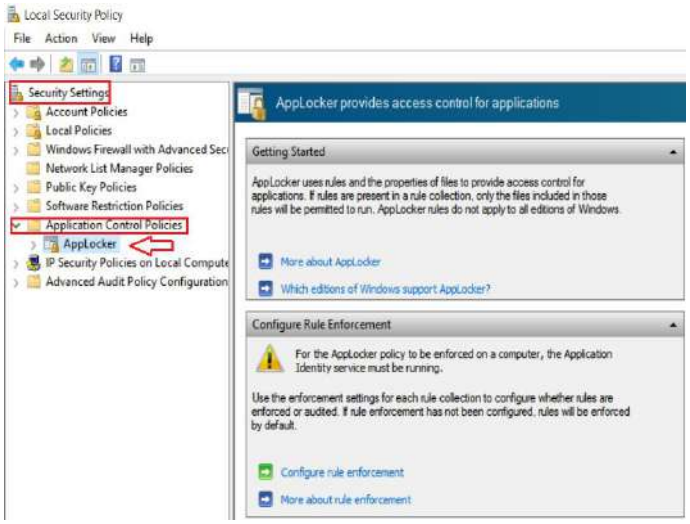
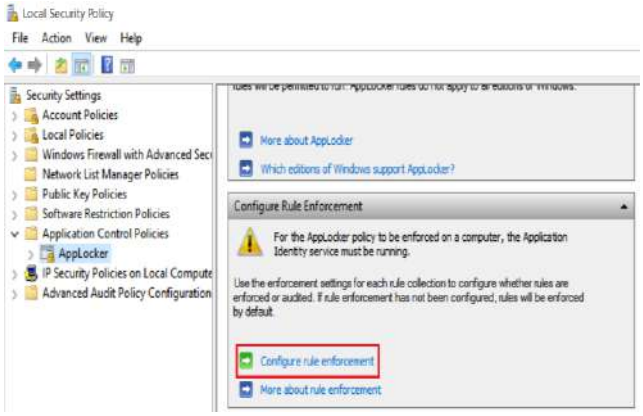
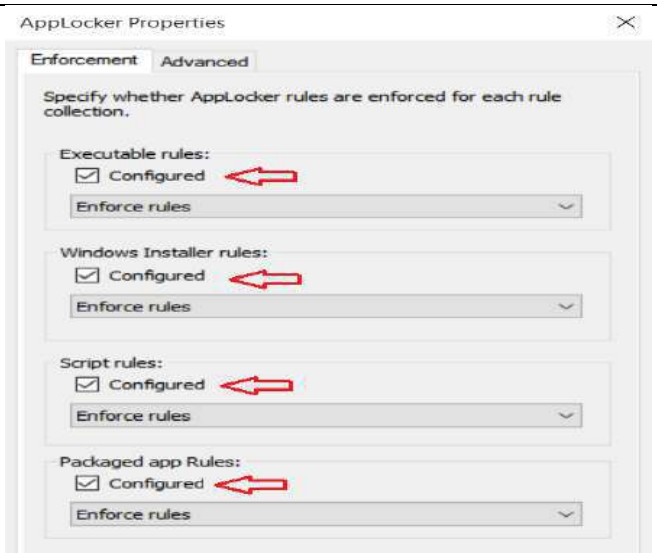
- تكوين سياسة **AppLocker** لتقييد تشغيل التطبيقات غير المصرح بها في نظام التشغيل **Windows**.
- اختبار فعالية السياسات والتأكد من عملها بالشكل المطلوب.

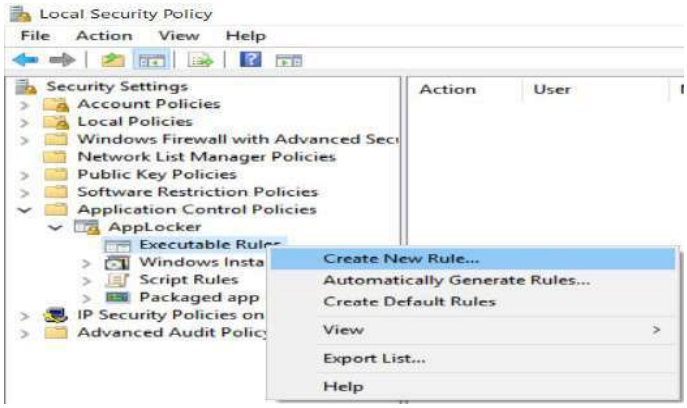
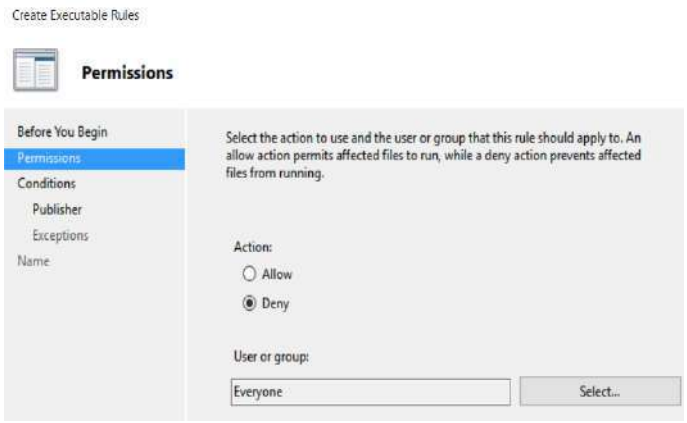
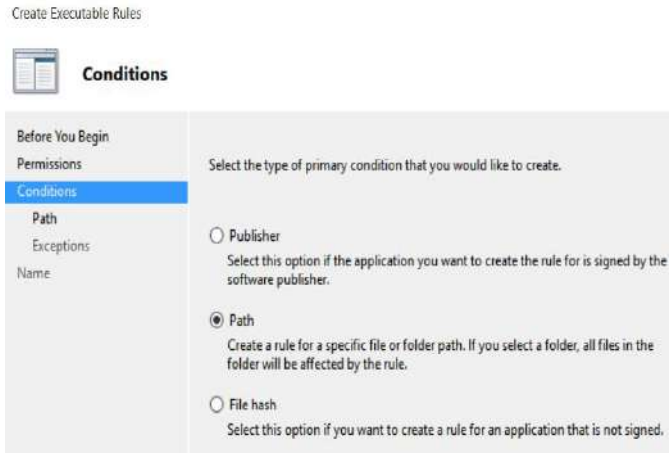
ثانياً: التسهيلات التعليمية

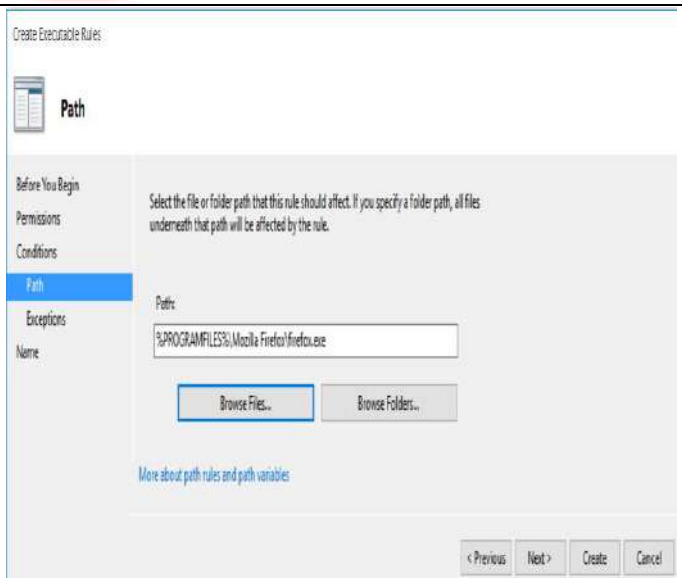
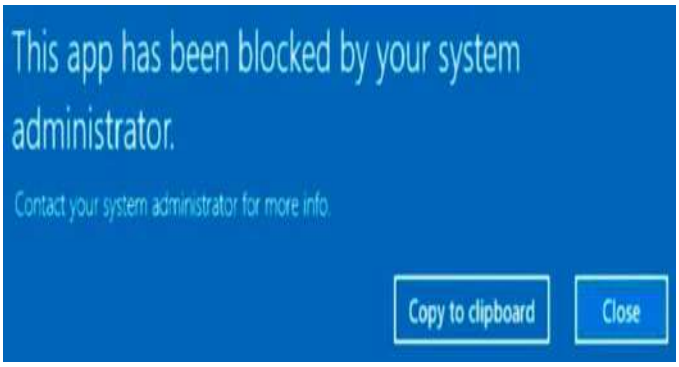
- جهاز كمبيوتر يعمل بنظام تشغيل **Windows10/11**.
- صلاحيات مدير النظام (**Administrator**).

ثالثاً: خطوات تنفيذ التمرين

1	قم بتشغيل **Local Security Policy** من خلال الضغط على مفتاح **Win + R** ثم كتابة **secpol.msc**	

2	انتقل إلى **Security Settings > Application Control Policies > AppLocker**	
3	اذهب إلى تكوين تنفيذ القواعد **configure rule) (enforcement**	
4	قم بتمكين جميع أنواع القواعد **Executable Rules.** **Windows Installer Rules.** **Script Rules.** **Packaged app Rules.**	

5	قم بانشاء قاعدة لمنع تشغيل تطبيق محدد. داخل **AppLocker** إنقر بزر الماوس الأيمن على **Executable Rules** واختر **Create New Rule**.	
6	كأجراء للقاعدة (**Deny**) تستخدم لأنشاء قوائم التطبيقات المحضورة من التشغيل أو ما تسمى احيانا القائمة السوداء (**Black list**) أو (**Deny List**) أمّا (**Allow**) فتستخدم لانشاء قوائم التطبيقات المرخصة للتشغيل أو تسمى احيانا القوائم البيضاء (**White list**) أو (**Allow List**) . في هذا التمرين اختر (**Deny**) لمنع تشغيل تطبيق معين.	
7	حدد **Path** كشرط للقاعدة	

8	أدخل مسار تطبيق غير مراد تشغيله (مثل **C:\Program Files\Mozila FireFox\firefox.exe**) أو اختر (**Browse Files**) وحدد مكان الملف التشغيلي للتطبيق المراد منعه من التشغيل وانقر على (**Create**) سيتم إنشاء سياسة منع التطبيق من التشغيل	
9	قم باختبار القاعدة وذلك بتنفيذ متصفح **FireFox**. يجب أن تظهر العبارة في الصورة جانبا. أي أن التطبيق تم حجبه من قبل مسؤول النظام.	
10	**المناقشة** • ما الفرق بين القوائم السوداء (**Black List**) والقوائم البيضاء (**White List**) في إدارة التطبيقات؟ • ما التحديات أو المشاكل التي قد تواجهها عند إستخدام **AppLocker** في بيئة تحتوي على عدد كبير من التطبيقات؟ • إذا أردت منع جميع المستخدمين من تشغيل لعبة معينة في مختبر المدرسة، كيف تنفذ ذلك بأستخدام **AppLocker**؟ • كيف تتعامل مع سيناريو يتم فيه منع تطبيق ضروري عن طريق الخطأ؟ ما الخطوات لاستثناء تطبيق معين؟	

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:15	
اسم التمرين: تكوين سياسات التحكم في التطبيقات بأستخدام **AppLocker**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب والوصول إلى الإعدادات المطلوبة	%10		
2	تنفيذ تكوين قواعد السياسات الأمنية	%10		
3	إختبار القواعد والسياسات التي تم تطبيقها	%10		
4	المناقشة	%10		
5	الزمن المخصص	% 10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

أسئلة الفصل الخامس

س1:- ما هي أهمية تحديث نظام التشغيل والتطبيقات المثبتة عليه؟

س2:- كيف يتم تحديد البرمجيات غير الآمنة؟ وضح ذلك.

س3:- ما العلامات التي قد تشير إلى وجود برمجيات خبيثة في النظام؟

س4:- ما الفرق بين إستخدام أدوات إزالة البرمجيات المتخصصة والازالة اليدوية؟

س5:- كيف يمكن لمراقبة العمليات في "مدير المهام" أن تساعد في اكتشاف البرامج غير الآمنة؟

س6:- ما الفرق بين التحديثات التي تعالج الثغرات الأمنية والتحديثات التي تحسن الأداء؟

س7:- ما الفرق بين القوائم البيضاء **(Allow list)** والقوائم السوداء **(Deny list)**؟

س8:- لماذا تعد مراجعة الصلاحيات الممنوحة للمستخدمين خطوة ضرورية في إدارة الأمان؟

س9:- املأ الفراغات الآتية بما يناسبها

1. تُعد ..... المثبتة على أنظمة التشغيل جزءًا أساسيًا من حياتنا اليومية، سواء في العمل أو الترفيه أو التواصل.
2. غالبًا ما تحتوي ..... على إصلاحات للثغرات الأمنية التي تم اكتشافها في الإصدارات السابقة.
3. يمكن ملاحظة وجود برمجيات غير آمنة من خلال ظهور ..... بشكل متكرر أو إعادة توجيه المتصفح تلقائيًا إلى مواقع مشبوهة.
4. من أدوات إزالة البرامج غير المرغوب فيها والتي تزيل أيضًا الملفات المتبقية بعد الحذف هي .....أو .....
5. للتحكم بتشغيل التطبيقات على أنظمة ويندوز، يمكن إستخدام خاصية ..... أو **Windows Defender Application Control**.

الفصل السادس

الاستجابة للحوادث الأمنية وإصلاح الثغرات

Incident Response and Vulnerability Fixing

أهداف الفصل السادس

1. التعرف على أنواع الحوادث الأمنية وكيفية الاستجابة لها.
2. القدرة على مراقبة وتحليل سجلات الأنظمة لتحديد الانشطة المشبوهة.
3. اكتساب مهارات إصلاح الثغرات واختبار النظام بعد الإصلاح.
4. إعداد خطط طوارئ لاستعادة النظام بعد الهجمات.

محتويات الفصل السادس

الفصل السادس

الاستجابة للحوادث الأمنية وإصلاح الثغرات

Incident Response and Vulnerability Fixing

تمهيد

تعد الاستجابة للحوادث الأمنية وإصلاح الثغرات من الركائز الأساسية في منظومة أمن المعلومات، حيث تهدف إلى تعزيز قدرة المؤسسات على التصدي للهجمات السيبرانية وتقليل أثرها على الأصول التقنية والبيانات الحساسة. أن البيئة الرقمية المعقدة والمتغيرة باستمرار تُنتج تحديات أمنية متزايدة، مما يجعل من الضروري تبني نهج استباقي وفعّال في إدارة الحوادث والثغرات.

(6- 1) أنواع الحوادث الأمنية وخطوات الاستجابة لها

الحادث الأمني في الأمن السيبراني هو أي ضرر يهدد أمن الأنظمة سواء كانت حواسيب أو شبكات، أمّا الاستجابة للحوادث فهي نهج استراتيجي لمعالجة وإدارة عواقب الهجوم الإلكتروني . والهدف هو التعامل مع الموقف بطريقة تحد من الأضرار، وتقلل من وقت التعافي والتكاليف، وتقلل من الاضطراب الذي قد تتعرض له المؤسسة. كما يمكن لخطة الاستجابة الفعالة للحوادث أن تساعد في منع الحوادث المستقبلية من خلال توفير نظرة ثاقبة لنقاط ضعف المؤسسة وتقديم خارطة طريق لتعزيز تدابير الأمن .

في تكنولوجيا المعلومات، هناك ثلاثة مصطلحات تُستخدم أحياناً بالتبادل ولكنها تعني أشياء مختلفة:

- الحدث (**event**): - هو إجراء غير ضار يحدث بشكل متكرر مثل إنشاء ملف أو حذف مجلد أو فتح بريد إلكتروني. لا يُعد الحدث في حد ذاته عادةً مؤشراً على وجود اختراق ولكن عند إقرانه بأحداث أخرى قد يشير إلى وجود تهديد.
- التنبيه (**Alert**):- هو إشعار يتم إصداره عند وقوع حدث ما، والذي قد يشير أو لا يشير إلى وجود تهديد.
- الحادث (**Incidence**):- هي مجموعة من التنبيهات المترابطة التي اعتبرها البشر أو أدوات الأتمتة على الأرجح تهديداً حقيقياً. قد لا يبدو أن كل تنبيه بمفرده يمثل تهديداً كبيراً، ولكن عند الجمع بينهم، فإنها تشير إلى وجود اختراق محتمل.

تتمثل أهداف الاستجابة للحوادث الأمنية في القضاء على الهجوم إلكتروني والتعافي منه في أسرع وقت ممكن وإخطار العملاء أو الجهات الحكومية وفقاً لما تتطلبه القوانين الإقليمية، ومعرفة كيفية تقليل مخاطر حدوث اختراق مشابه في المستقبل. ويتم الاستجابة لها عبر اربع مراحل رئيسة

- الإعداد: وهو إنشاء فريق للاستجابة للحوادث وتزويده بالأدوات والمعرفة اللازمة.

- التحديد: وهوعملية اكتشاف الحادث والتحقق منه.
- الاحتواء والتخفيف: وهو الحد من نطاق وحجم الحادث، ثم القضاء على السبب الجذري للحادث.
- التعافي: هو استعادة الأنظمة والخدمات إلى وظائفها الطبيعية، والدروس المستفادة تتعلق بمراجعة الحادث واستجابة المنظمة له، وإجراء التحسينات اللازمة على خطة الاستجابة للحوادث.

لتوجيه جهود الاستجابة لحوادث الأمن السيبراني، وفهم نطاق وتأثير حادث الأمن السيبراني، قم بتطوير قائمة بأسئلة التحقيق. لاحظ أنه قد لا تكون جميع الأسئلة قابلة للإجابة بالبيانات المتاحة وقد تتغير الأسئلة مع تقدم التحقيقات كما و تتضمن أسئلة التحقيق المحتملة ما يأتي:

- من هو ناقل الاختراق الأولي؟
- ما هو النشاط الذي حدث بعد الاستغلال؟ هل تم اختراق الحسابات؟ ما هو مستوى الامتياز الذي كان متضمنًا؟
- هل يتمتع الفاعل الخبيث باستمرارية على الأنظمة أو الخدمات أو الشبكات؟
- هل يُشتبه في الحركة الجانبية أو معروفة؟ إلى أين انتقل الفاعل الخبيث جانبيًا وكيف؟
- كيف يحافظ الفاعل الخبيث على القيادة والسيطرة؟
- هل تم الوصول إلى البيانات أو استخراجها، وإذا كان الأمر كذلك، فما نوع البيانات؟

(6- 2) مراقبة السجلات وتحليلها

إن إدارة السجلات تشير إلى الممارسات والأدوات التي تهدف إلى إدارة كميات كبيرة من بيانات السجلات التي يتم إنتاجها بواسطة التطبيقات والموارد المتنوعة ضمن بيئة تكنولوجيا المعلومات. وهي تتعلق بجمع البيانات، وتخزينها، وتحليلها، وفي النهاية التخلص منها بمجرد أن تتجاوز فترة حياتها المفيدة. الهدف الأساسي منها هو تسهيل المراقبة والتفسير السهل لبيانات السجلات عبر البنية التحتية بأكملها. من خلال مراجعة بيانات السجلات، يصبح من الأسهل تحديد المشكلات في النظام وحلها وهذا يلغي الحاجة إلى الفحص اليدوي لملفات السجلات المنفصلة، مما يعزز بشكل كبير الكفاءة في اكتشاف المشكلات وحلها.

(6-2-1) أهمية إدارة السجلات

السجلات ليست مجرد ملفات بل هي كنز من المعلومات التي إن تم إدارتها بشكل صحيح، فيمكن أن تقدم قيمة هائلة في جوانب مختلفة من عمليات تكنولوجيا المعلومات مثل:

- استكشاف الأخطاء وإصلاحها: تُعد السجلات غالبًا أول مكان يجب النظر فيه عندما يحدث خطأ. فهي توفر المعلومات اللازمة لتتبع المشكلة وفهم أسبابها الجذرية.

- التحذير والتنبيه: تتيح السجلات اكتشاف السلوكيات غير الطبيعية أو غير المتوقعة في الأنظمة، مما يساعد في تنشيط التنبيهات التي تحفز التدخلات الفورية.
- تحليل النظام: عند تمركز بيانات السجلات، يمكنك الحصول على رؤى حول كيفية أداء الأنظمة وتفاعلها مع بعضها البعض، وهو أمر ضروري لتحقيق الكفاءة التشغيلية والتخطيط الاستراتيجي.
- منع تكرار المشاكل: بمجرد تحديد المشكلة وحلها، يمكن للسجلات أن تساعد في فهمها بعمق، مما يساعد في تطوير استراتيجيات لمنع حدوث مشاكل مشابهة في المستقبل.

(6-2-2) انواع السجلات

كل مكون في الشبكة يولد نوعًا معينًا من البيانات، ويقوم بتسجيل هذه البيانات في سجل خاص به. نتيجة لذلك، هناك العديد من أنواع السجلات، وكل نوع يخدم غرضًا محددًا في مراقبة الأداء أو الأمان أو الاستخدام وإليك أبرزها:

1. سجل الأحداث (**Event Log**): هو سجل عالي المستوى يحتوي على معلومات تتعلق بحركة المرور على الشبكة والاستخدام، مثل محاولات تسجيل الدخول، المحاولات الفاشلة لكلمات المرور، وأحداث التطبيقات.
2. سجل الخادم (**Server Log**): هو مستند نصي يحتوي على سجل للأنشطة المرتبطة بخادم معين خلال فترة زمنية معينة، مثل الطلبات المستلمة، والأخطاء، وتحذيرات الأداء.
3. سجل النظام (**Syslog**): هو سجل يحتوي على أحداث خاصة بنظام التشغيل، مثل رسائل بدء التشغيل، وتغييرات النظام، وتوقفات غير متوقعة، وأخطاء وتحذيرات، وعمليات النظام الأساسية.
4. سجلات التفويض والوصول (**Authorization & Access Logs**) هي سجلات تسرد الأشخاص أو الروبوتات الذين قاموا بالوصول إلى تطبيقات أو ملفات معينة، وتشير إلى ما إذا كان الوصول مسموحًا أو مرفوضًا.
5. سجلات التغييرات (**Change Logs**): تحتوي هذه السجلات على قائمة زمنية بالتعديلات التي أُجريت على تطبيق أو ملف، مما يساعد في تتبع التحديثات أو التكوينات.
6. سجلات التوافر (**Availability Logs**): تُستخدم لمراقبة أداء النظام، ومدة التشغيل (**uptime**)، والتوافر العام للخدمة.
7. سجلات الموارد (**Resource Logs**): هي سجلات توفر معلومات حول مشكلات الاتصال أو حدود السعة في الموارد مثل المعالجات، الذاكرة، أو التخزين.
8. سجلات التهديدات (**Threat Logs**) هي سجلات تحتوي على بيانات عن حركة المرور في النظام أو الملفات أو التطبيقات التي تطابق ملفات تعريف أمان محددة داخل جدار الحماية (**Firewall**)، وتُستخدم لرصد السلوكيات المشبوهة أو الهجمات المحتملة.

(3-6) إعداد خطط الطوارئ لإستعادة النظام بعد الهجمات

إعداد خطط الطوارئ لاستعادة النظام بعد الهجمات يُعد من المكونات الجوهرية في استراتيجيات الأمن السيبراني الحديثة، ويشكل جزءًا من خطة استمرارية الأعمال وخطة التعافي من الكوارث. يهدف هذا النوع من الخطط إلى ضمان قدرة المؤسسة على استعادة أنظمتها وخدماتها الحيوية بسرعة وكفاءة بعد تعرضها لهجوم سيبراني، مع تقليل فترات التوقف والخسائر المحتملة.

تبدأ عملية إعداد خطة طوارئ فعالة بفهم شامل للبنية التحتية الرقمية للمؤسسة، بما في ذلك تحديد الأنظمة الحرجة والبيانات الحيوية التي لا بد من استعادتها أولاً لضمان استمرار الأعمال. يُعرف هذا التحليل بتحديد أولويات الاسترداد ويُبنى عليه تحديد مؤشرين رئيسيين هما: نقطة الاسترداد المستهدفة والتي تعبر عن أقصى مدة يمكن خلالها فقدان البيانات، ونقطة الزمن المستهدفة للاسترداد والتي تمثل أقصى مدة يُسمح للنظام أن يكون فيها غير متاح.

بعد ذلك، يتم تصميم آليات النسخ الاحتياطي بشكل يضمن حفظ البيانات بشكل دوري وآمن، وتوزيع النسخ الاحتياطية في مواقع مختلفة لضمان إمكانية الوصول إليها حتى في حال استهداف أحد المواقع. من المهم أن تُجرى اختبارات دورية لهذه النسخ للتأكد من صلاحيتها وسلامتها.

تشمل الخطة كذلك إعداد بيئة بديلة جاهزة للعمل عند حدوث الخلل، مثل المواقع البديلة الباردة (**Cold Sites**) أو الساخنة (**Hot Sites**)، والتي تُستخدم كنسخ تشغيلية للطوارئ يمكن نقل العمليات إليها بشكل سريع. كما يجب تضمين الإجراءات التفصيلية التي ينبغي اتباعها بعد وقوع الهجوم، مثل خطوات تقييم الضرر، وتحديد مصدر الهجوم، واحتواء الخطر، واستعادة النظام تدريجيًا بطريقة منظمة وآمنة، مع ضمان عدم عودة البرمجيات الخبيثة أو الثغرات إلى النظام المعاد تشغيله.

أحد العناصر المهمة في خطة الطوارئ هو توزيع المسؤوليات بوضوح ضمن فريق الاستجابة للحوادث، بحيث يعرف كل عضو دوره بدقة خلال الأزمة، ويشمل ذلك فرق الأمن ، والدعم الفني، والإدارة العليا، والإعلام والعلاقات العامة. بالإضافة إلى ذلك، يجب تطوير سيناريوهات مختلفة للهجمات المحتملة (مثل هجمات الفدية، وتسريب البيانات، أو الحرمان من الخدمة) ووضع خطط مخصصة لكل سيناريو.

أخيرًا، تُعد مرحلة التقييم بعد الهجوم (**Post-Incident Review**) من أهم الخطوات، حيث يتم تحليل أداء الخطة أثناء الطوارئ، وتحديد نقاط القوة والضعف، وتحديث الخطة بناءً على الدروس المستفادة لضمان تحسن الاستجابة في المستقبل.

(6-4) أدوات مسح الأنظمة واكتشاف الثغرات

يُعد فحص الثغرات الأمنية ممارسةً لا غنى عنها لمتخصصي الأمن السيبراني. يستخدم هؤلاء الأفراد أدوات فحص الثغرات الأمنية لتحديد نقاط الضعف في الأنظمة ومحاولة إزالة أوجه القصور المكتشفة لضمان أمن النظام. كما تُستخدم نتائج فحص هذه الأدوات لتقييم مستوى المخاطر الإجمالي للأنظمة، وذلك لإدارة الثغرات المكتشفة بطريقة مُرتبة حسب الأولوية ومن المتوقع أن يستخدمها المستخدمون المتمرسون، مثل متخصصي الأمن السيبراني أو مُختبري الاختراق، إلاّ أن ماسحات الثغرات الأمنية لا تُصمم عادةً مع مراعاة سهولة الاستخدام. ومع ذلك، فإن سهولة إستخدام هذه الأدوات بالغة الأهمية لتوليد نتائج فحص دقيقة وشاملة، وتقييم تقارير الفحص بشكل صحيح، بحيث يُمكن منع الهجمات غير المرغوب فيها الناتجة عن ثغرات أمنية غير ملحوظة أو متبقية في الأنظمة بشكل استباقي. من الادوات البرمجية المعروفة في هذا المجال هو ماسح الثغرات الأمنية **OpenVAS** . وقد اختير **OpenVAS** للتحليل نظراً لانتشار استخدامه بين المُمارسين، كونه أداة مفتوحة المصدر، بالإضافة إلى احتوائه على مكتبة شاملة من مُكونات الكشف عن الثغرات الأمنية. **OpenVAS** هي أداة قوية ومفتوحة المصدر لتقييم الثغرات الأمنية، قادرة على فحص الثغرات وإدارتها. بالإضافة إلى ذلك، يمكنها تحديد الخدمات النشطة والمنافذ المفتوحة والتطبيقات قيد التشغيل على جميع الأجهزة. تحتوي على محرك فحص يُحدث بانتظام بمكونات إضافية لاكتشاف الثغرات تُسمى اختبارات ثغرات الشبكة (**NVTs**). بالإضافة إلى كونها مجانية، فإن قدرتها على اكتشاف الثغرات الأمنية في مجموعة واسعة من أنظمة التشغيل والتطبيقات تجعلها أداة شائعة بين مُختبري الاختراق.ولتثبيت وتفعيل أداة **OpenVAS** على برنامج الـ**Linux** أو أي توزيعة من **Debian**. عزيزي الطالب سيتم تطبيق واستخدام هذه الاداة في التمرين رقم 18.

(6-5) منهجيات اختبار النظام بعد إصلاح الثغرات

إختبار النظام بعد إصلاح الثغرات يُعد مرحلة حاسمة ضمن دورة حياة معالجة الثغرات الأمنية، ويهدف إلى التحقق من فعالية الإصلاحات المطبقة وضمان عدم وجود آثار جانبية غير مرغوبة على وظائف النظام. يُعرف هذا النوع من الاختبار بـ "إختبار ما بعد التصحيح" أو "إختبار التحقق من الإصلاح"، ويُعد من الممارسات الأساسية في بيئة الأمن السيبراني، خصوصًا في المؤسسات التي تعتمد على أنظمة حرجة وتحتاج إلى ضمان استمرارية الخدمة وسلامة البيانات.

تبدأ منهجية إختبار النظام بعد إصلاح الثغرات بإعادة تنفيذ إختبار الثغرة نفسها للتأكد من أنها لم تعد قابلة للاستغلال. يُستخدم في ذلك أدوات فحص الثغرات الأمنية أو الهجمات المُحاكاة للتحقق مما إذا كان التصحيح المطبق قد أغلق بالفعل الثغرة دون ترك مسارات بديلة للاستغلال. هذا النوع من الاختبار يُعرف أحيانًا باختبار إعادة التحقق ويُعد ضروريًا قبل الانتقال إلى البيئات الحية.

بعد التأكد من معالجة الثغرة، يُنتقل إلى إختبار التكامل للتحقق من أن التصحيح لم يؤثر سلبًا على وظائف النظام الأخرى أو يتسبب في تعارضات مع تطبيقات أو مكونات أخرى. في هذا السياق، يتم

التركيز على استقرار النظام، واختبار العمليات المرتبطة بالوحدات المصححة، وضمان أن الأداء لا يتدهور بعد الإصلاح.

ضمن إطار المنهجيات الأكاديمية، يُنصح بتطبيق إختبار الانحدار **(Regression Testing)** بعد الإصلاح، وهو منهجية تُستخدم للتحقق من أن التحديثات لم تؤدِ إلى ظهور ثغرات جديدة أو خلل في وظائف أخرى كانت تعمل سابقًا بشكل سليم. ويتم ذلك من خلال تنفيذ مجموعة من حالات الاختبار المخزنة مسبقًا **(Test Cases)** التي تمثل سلوك النظام الطبيعي. كذلك، تُستخدم اختبارات الأمان الديناميكية **(Dynamic Security Testing)** في البيئات شبه الحية **(Staging Environments)** لمحاكاة تفاعل المستخدمين الفعليين مع النظام، والتحقق من استمرارية الحماية ضد هجمات مثل الحقن البرمجي، أو تجاوز الصلاحيات، أو تنفيذ الأوامر عن بُعد، خاصة إذا كانت الثغرة المُصلَحة من هذا النوع.

منهجية إختبار النظام بعد إصلاح الثغرات تعتمد أيضًا على التغذية الراجعة من أنظمة مراقبة السجلات **(Log Monitoring)** التي تُحلل الأحداث غير الطبيعية أو محاولات الوصول الفاشلة بعد التحديث. هذه التحليلات تساعد في الكشف عن آثار جانبية غير مباشرة قد لا تظهر خلال الاختبارات المباشرة. في النهاية، من الضروري توثيق نتائج جميع هذه الاختبارات بشكل منهجي، وتحديث سجل الثغرات الأمنية، وتقديم تقارير مفصلة لفرق التطوير والإدارة، مما يُسهم في تحسين عملية إدارة الثغرات، وتقديم مادة تعليمية تطبيقية يمكن أن تُدرَّس لطلبة الأمن السيبراني من خلال مشاريع محاكاة واختبارات مختبرية عملية تمكّنهم من فهم التطبيق الواقعي لهذه المنهجيات.

ويمكن تصنيف الاختبارات حسب التكنولوجيا ومنهجيات الاختبار إلى:-

- إختبار الاختراق للشبكات: يركز على تقييم أمان الشبكات والبنية التحتية لتحديد الثغرات في الأجهزة والخوادم والجدران النارية.
- إختبار تطبيقات الويب: يستهدف اكتشاف الثغرات الأمنية في مواقع الويب والتطبيقات مثل حقن **SQL Injection-SQL** وهجمات **Cross-Site Scripting-XSS**.
- إختبار تطبيقات الهواتف المحمولة: يختبر أمان التطبيقات على أنظمة التشغيل مثل **Android** وiOS للكشف عن الثغرات التي قد تؤدي إلى تسريب بيانات المستخدمين.
- إختبار الاختراق الداخلي: يتم من داخل المؤسسة لمحاكاة هجوم يقوم به مستخدم لديه صلاحيات داخل الشبكة.
- إختبار الاختراق الخارجي: يتم من خارج المؤسسة لمحاكاة هجوم من قبل مخترق خارجي لا يمتلك صلاحيات داخل النظام.
- إختبار الهندسة الاجتماعية: يركز على استهداف العنصر البشري بأستخدام تقنيات مثل التصيد الاحتيالي **(Phishing)** للحصول على بيانات حساسة.

6 حماية انظمة التشغيل

رقم التمرين:16 الزمن المخصص: ساعة واحدة

اسم التمرين: إعداد نظام مراقبة السجلات باستخدام **Graylog**

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

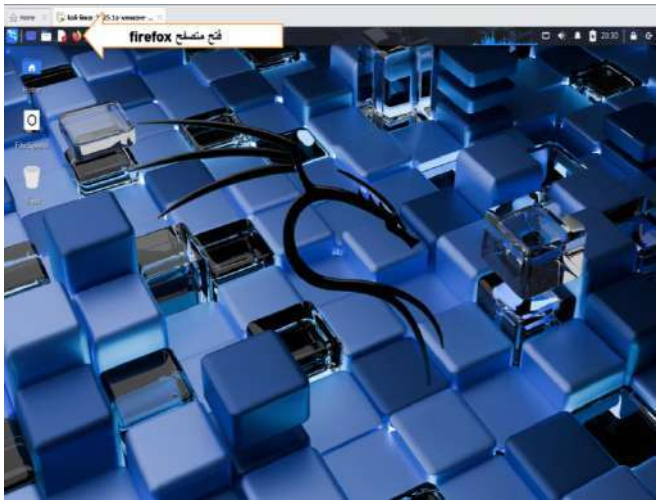
بعد إتمام هذا التمرين، سيتمكن الطالب من:

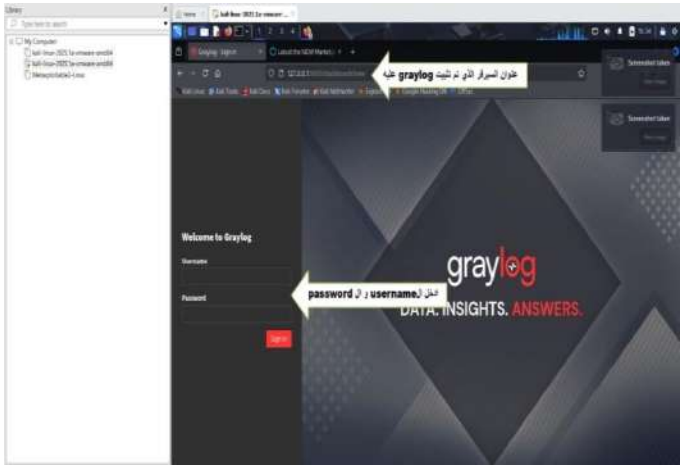
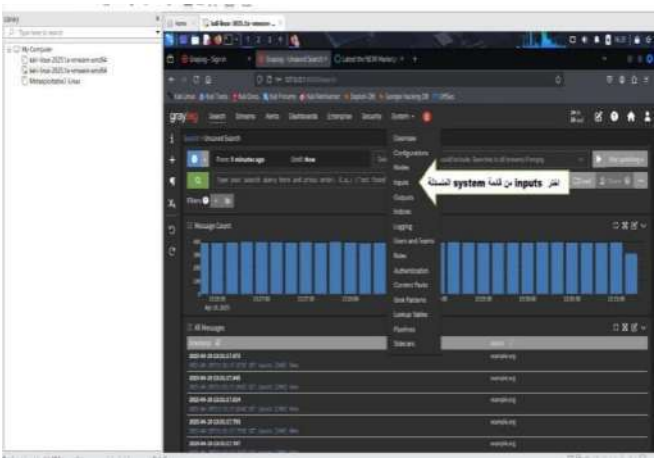
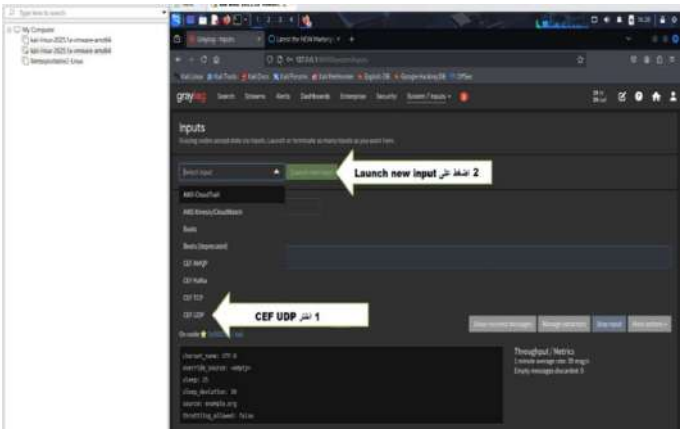
- التعرف على كيفية إعداد **Graylog** لاستقبال السجلات من أجهزة مختلفة.
- تحليل سجلات الدخول ومحاولات الوصول غير المصرح به.
- إنشاء تنبيهات ولوحات مراقبة لمراقبة الأنشطة المشبوهة.

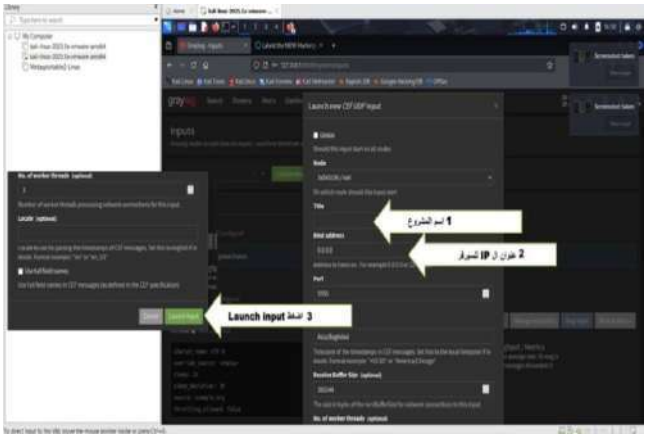
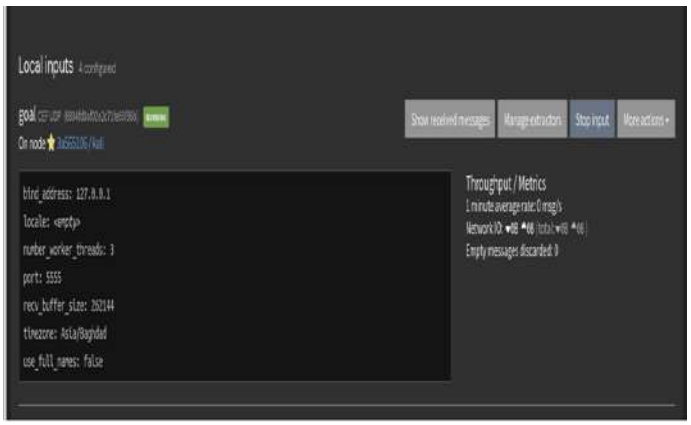
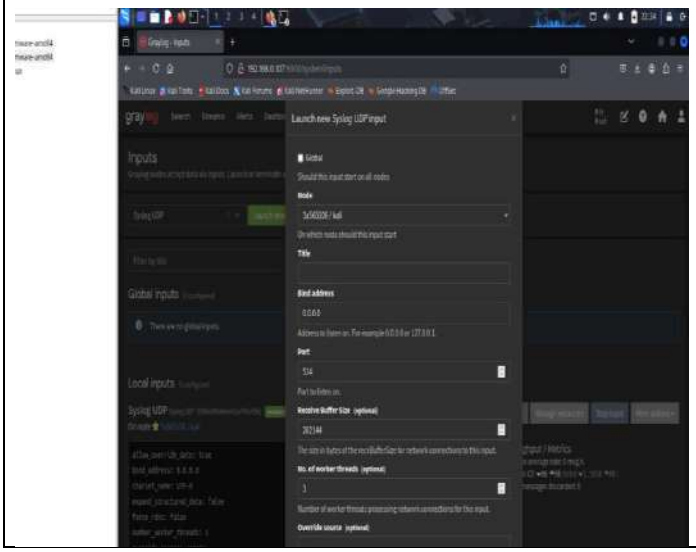
ثانياً: التسهيلات التعليمية

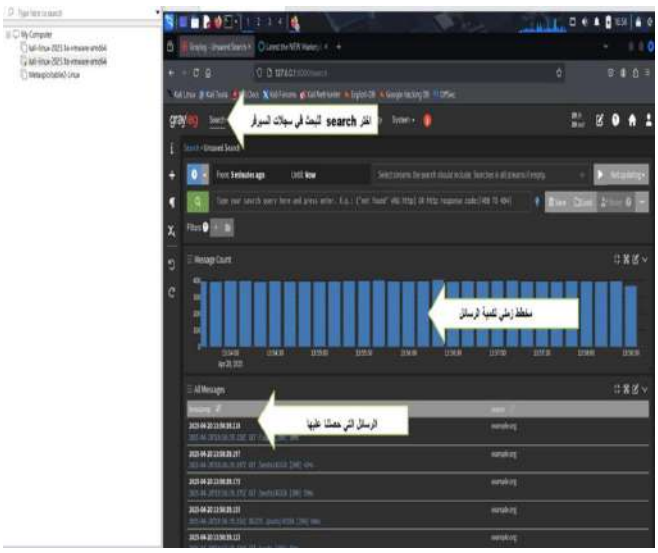
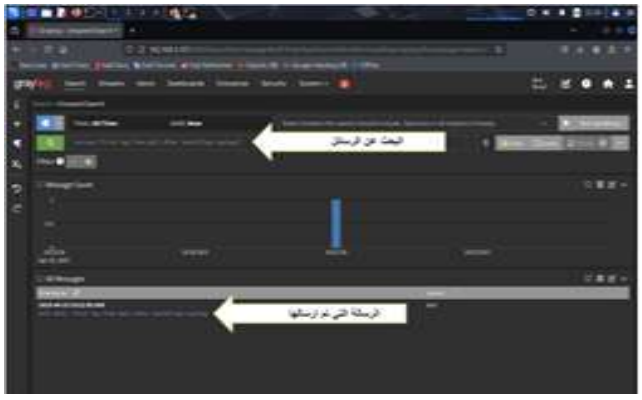
- نظام تشغيل **Linux** يفضل **Kali Linux**.
- أجهزة الحاسوب بصلاحيات المستخدم (**User**) وصلاحيات المدير(**Administrator**) .
- اتصال بالانترنت

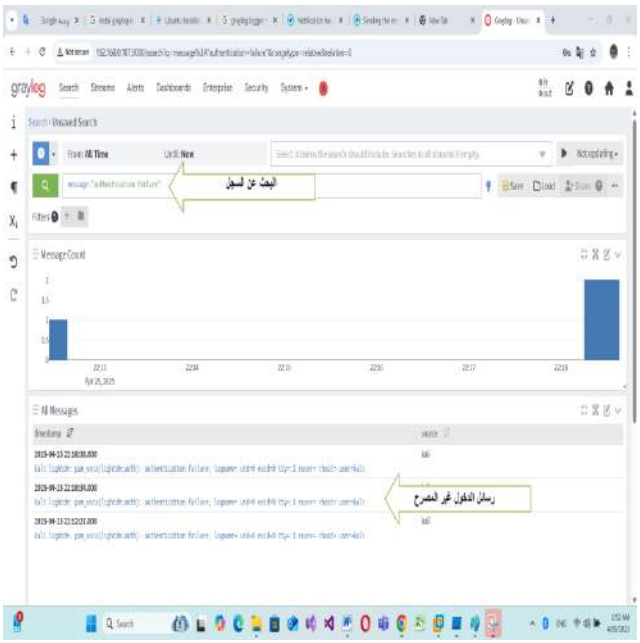
ثالثاً: خطوات تنفيذ التمرين

	تفتح أداة **Graylog** عن طريق أي متصفح ولكن بالنظر إلى أن أنظمة الـ **kali linux** تدعم متصفح **Firefox** سيتم الدخول للاداة من خلاله.	

2	بعد فتح المتصفح قم بإدخال الـ(IP) **http**://127.0.0.1:9 سوف تفتح لك نافذة كما مبين بالشكل إدخال **username** و**password** للوصول إلى النافذة الرئيسية تثبت الأداة على جهاز ويمكن الدخول إليها من جميع الأجهزة المربوطة على نفس الشبكة للحصول على المعلومات.	
3	للبدأ بإنشاء ملف جديد لاستقبال الطلبات اختر **System** في شريط التنقل العلوي من القائمة المنسدلة اختر **inputs**.	
4	بعد الدخول إلى الـ inputs اذهب إلى القائمة المنسدلة **Select input** و اختر **GELF UDP** ثم اضغط على **Launch new input.**	

5	من خلال النافذة التي ستنبثق اكتب اسم المشروع وعنوان الـ **IP** 0.0.0.0 والمنفذ **Port** 5140 واضغط على **launch input**.	
6	بمجرد تشغيل الإدخال يجب أن تراه يظهر أسفل الصفحة **inputs** في **local input**.	
7	لبدء استقبال رسائل السجلات يجب إضافة **Syslog** من قائمة**select input** اختر **syslog udp** ثم اضغط على **Launch new input** ستنبثق قائمة اضف العنوان 0.0.0.0 **IP** لاستقبال كل الرسائل والـport 5140 ثم اضغط **launch input**.	

8	بعد اكمال إعدادات الـ inputs اختر من القائمة العلوية **search** سيبدأ خادم **Graylog** الخاص بك بعد وقت قليل بجمع الرسائل، يمكنك البحث في الرسائل . للتحقق من الرسائل التي يتم إرسالها إلى خادم **Graylog** يمكن تخصيص وقت جمع الرسائل وتنظيم جداول خاصة للبحث في رسائل معينة	
9	من برنامج ال **kali linux** قم بإرسال رسالة للتأكد من أن الرسائل تصل إلى ال **Graylog** افتح نافذة الـ **terminal emulator** واكتب **logger "First log from Kali after installing rsyslog"**<< اضغط **Enter** واذهب إلى برنامج الGraylog	
10	اذهب إلى القائمة **search** وقم بالبحث عن الرسالة في مربع البحث سوف نجد الرسالة التي تم إرسالها إلى برنامج الـ**Graylog** مما يعني أن الربط بين النظام و**Graylog** قد تم بالشكل الصحيح.	

11	أمّا للكشف عن محاولات الدخول غير المصرح بها عن طريق سجل الدخول حاول اقفال برنامج ال**kali linux** ثم العودة للدخول مرة أخرى ولكن أدخل الرمز السري بالخطأ مرة أو أكثر ثم أدخل الرمز الصحيح وأُدخل للنظام.	
12	افتح نافذة ال**Graylog** عن طريق برنامج **chrome** في حاسوب آخر يعمل على نظام الوندوز المربوط على نفس الشبكة واختر search. اكتب في مربع النص للبحث عن رسالة الدخول غير المصرح بها من خلال سجل الدخول هذه العبارة. **message:"authenticati "on failure** ستلحظ وجود رسائل للدخول غير المصرح به وعدد المحاولات واسم الحاسوب. يمكن قرأة السجلات من حاسوب آخر ونظام آخر عبر نفس الشبكة.	
13	**المناقشة** : • كيفية إرسال و استلام السجلات عبر بروتوكول **Syslog** . • البحث في السجلات داخل **Graylog** وتحليلها. • أهمية تحليل السجلات وتتبع النشاطات واكتشاف المشاكل الأمنية. • ما هي السجلات الأخرى التي يمكن الحصول عليها؟	

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:16	
اسم التمرين: إعداد نظام مراقبة السجلات بأستخدام **Graylog**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب والوصول إلى البرنامج وتشغيله عبر المتصفح	%15		
2	خطوات تنفيذ إعداد البرنامج والحصول على بيانات الخادم المستخدم	%15		
3	المناقشة	%10		
4	الزمن المخصص	%10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

6 حماية انظمة التشغيل

رقم التمرين:17 الزمن المخصص: ساعة واحدة

اسم التمرين: تحليل الهجمات باستخدام **Process Monitor**

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

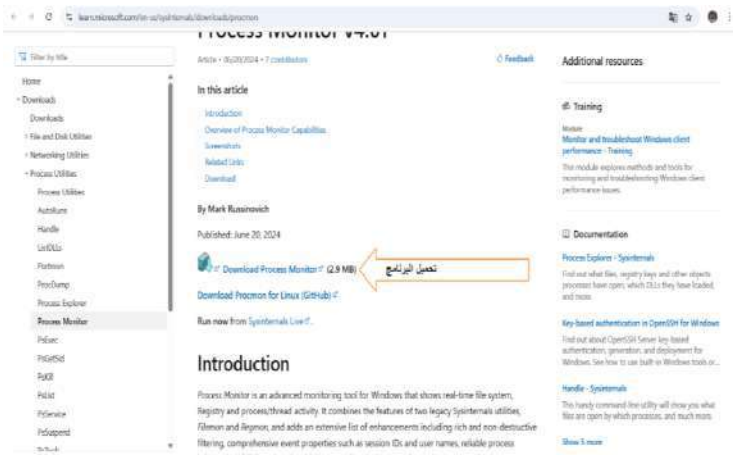
بعد إتمام هذا التمرين، سيتمكن الطالب من:

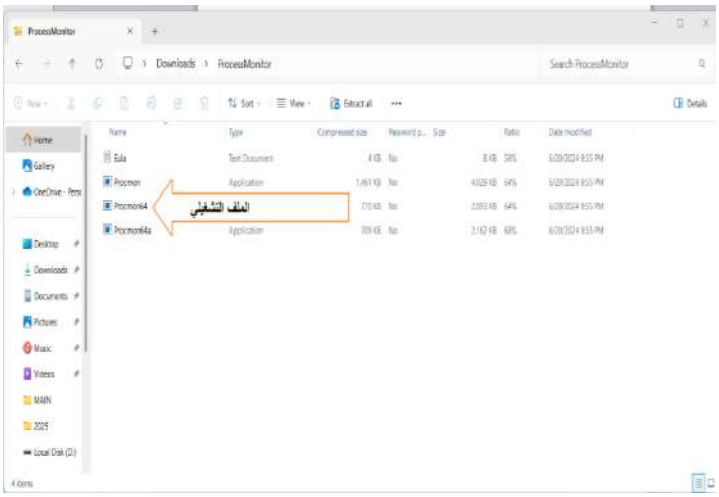
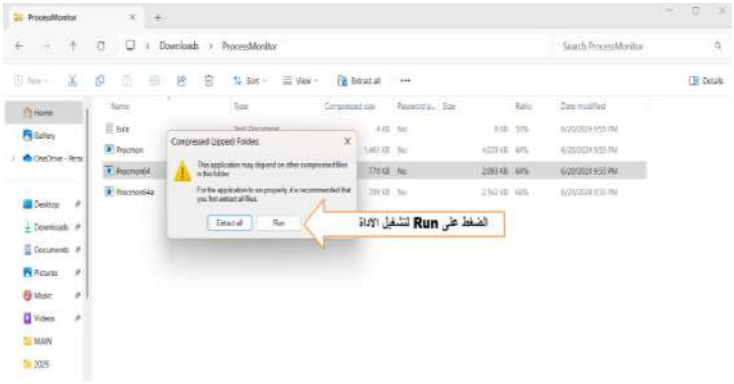
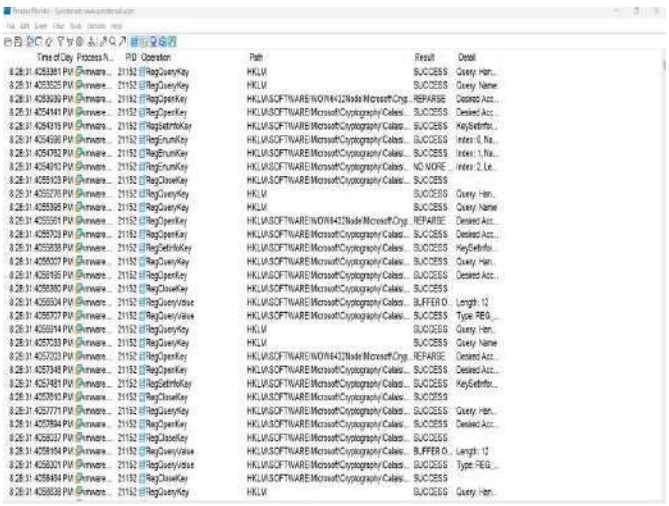
- التعرف على كيفية استخدام **Process Monitor** لمراقبة العمليات الجارية في نظام التشغيل.
- تحليل الأحداث المتعلقة بالملفات، الريجستري، الشبكة، والعمليات.
- إكتشاف سلوك مشبوه قد يدل على وجود برمجية خبيثة أو نشاط غير طبيعي.
- التعرف على مفاتيح تسجيل النظام المستخدمة من قبل التطبيقات.

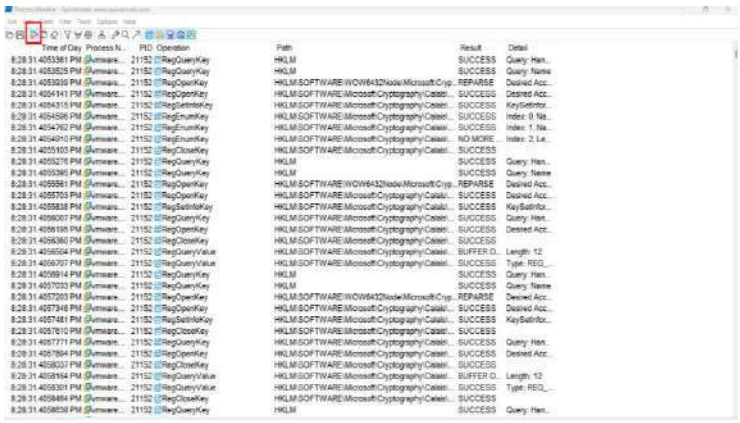
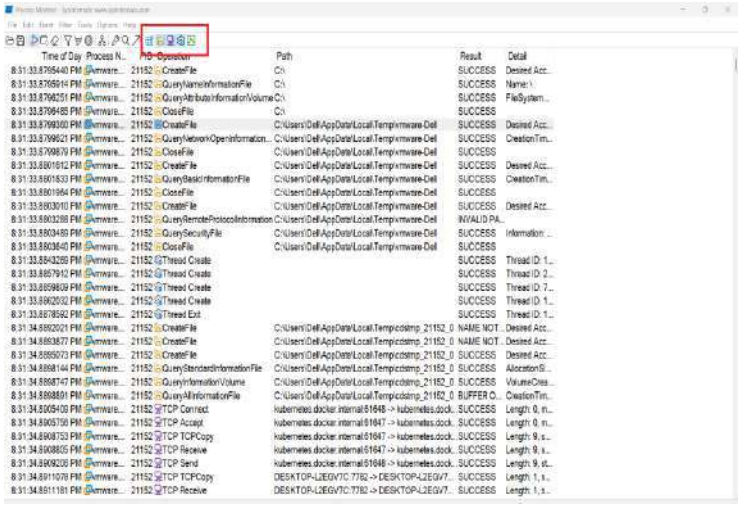
ثانياً: التسهيلات التعليمية

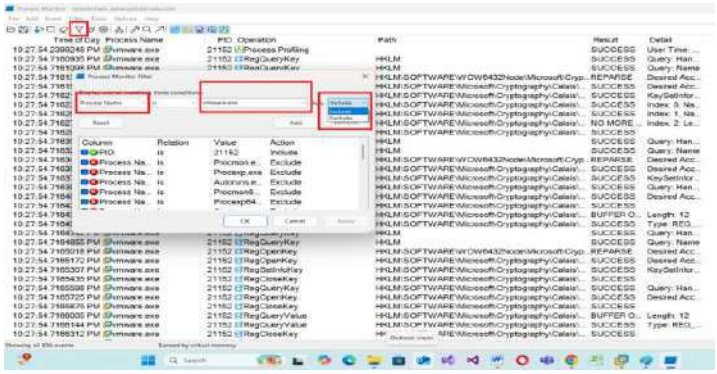
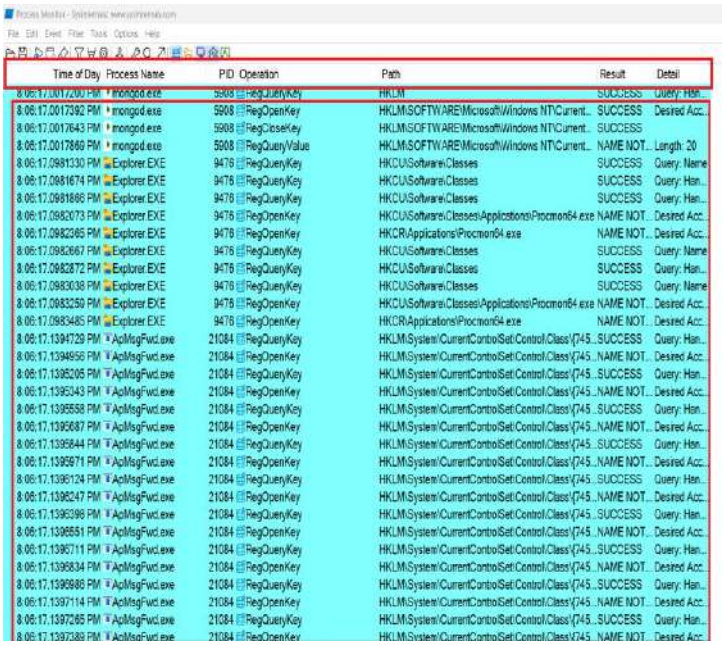
- جهاز يعمل بنظا **Windows** .
- أداة **Process Monitor** من **Microsoft Sysinternals**.
- صلاحيات إدارية لتشغيل الأداة.
- برنامج بسيط يمكن مراقبة نشاطه (مثل المفكرة أو أداة مخصصة للتجربة).

ثالثاً: خطوات تنفيذ التمرين

1-	الذهاب إلى الموقع الرسمي **https://learn.microsoft.com/en-us/sysinternals/downloads/procmon** و تحميل الأداة كملف مضغوط **ZIP**.	

-2	بعد التحميل قم بفك الضغط عن الملف و سيكون لديك ملف تنفيذي باسم : Procmon64 لا تحتاج الأداة إلى تثبيت بل هي أداة تنفيذ مباشرة عن التشغيل.	
-3	عند تشغيل الاداة سوف يطلب منك تشغيلها كمسؤول اضغط على **Run.**	
-4	بعد التشغيل ستظهر لك نافذة البرنامج البسيطة.	

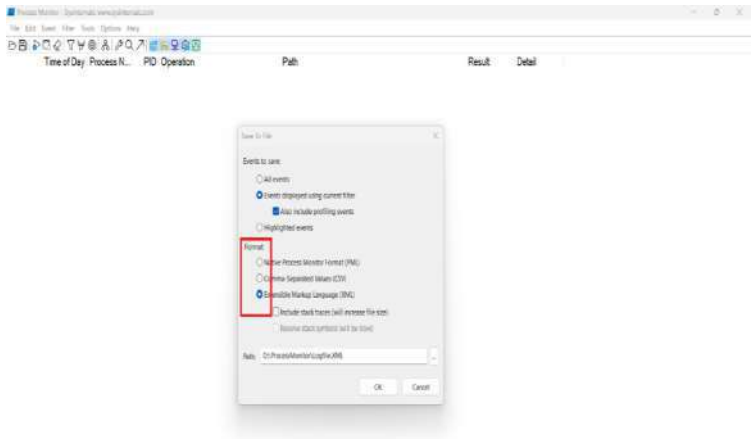
-5	عند الضغط على زر التشغيل سيبدأ البرنامج بتسجيل العمليات الحاصلة بالنظام عن طريق الإيعاز **capture** سيتغير شكل الإيعاز وتظهر عليه علامة التسجيل الأحمر أمّا لايقاف التشغيل فالضغط عليه مرة اخرى وستظهر علامة الإيقاف المؤقت	 ملاحظة : يستهلك الذاكرة العشوائية **(RAM)** بشكل كبير عند التشغيل لفترات طويلة
-6	تمثل هذه الايقونات كل نشاط يحصل في النظام وهي السجلات التي يتعامل عليها النظام التشغيلي • **Registrys** السجلات • **FileSystem** ملفات النظام • **Processes** سجل العمليات • **Network** سجلات الشبكة	
-7	يمكن تحديد نوع واحد من البيانات أمّا السجلات أو ملفات النظام أو العمليات أو سجلات الشبكة فقط من خلال النقر على الايقونات لتفعيل أو إلغاء تفعيل عرض البيانات.	

-8	إستخدام الفلاتر اضغط على **Ctrl + L** أو من خلال الموجود في شريط الأدوات لعرض أنشطة برنامج معين مثل **notepad.exe**	
-9	يمكن من خلال الأعمدة معرفة التفاصيل الكاملة للسجلات المنفذة • **Time of Day** وقت التنفيذ • **Process Name** اسم العملية • **PID (Process ID)** رقم العملية • **Operation** نوع العملية • **Path** المسار الذي يتم التعامل معه • **Result:** نتيجة العملية أ نجحت أم لا	

10. إذا كنت تريد مسح كل المعلومات اضغط على الممحاة **Clear** المؤشرة بالمربع الأحمر

11. يوفر البرنامج حفظ الملفات بثلاثة صيغ وهي :

- **PML**
- **CSV**
- **XML**



12. **المناقشة :**

- تحليل ما يفعله برنامج محدد عند التشغيل.
- تتبع التغييرات في الريجستري.
- تتبع العمليات التي تحدث في سجلات الشبكة والبرامج التي تستخدمها.
- اكتشاف الأنشطة غير المعتادة لبرامج مشبوهة.

استمارة قائمة الفحص				
اسم الطالب:			المرحلة: الثانية	
التخصص:			رقم التمرين:17	
اسم التمرين: تحليل الهجمات بأستخدام أداة **Process Monitor**				
ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب والوصول إلى البرنامج وتشغيله	%15		
2	خطوات تنفيذ البرنامج والتعرف على الأدوات المتاحة والتعامل معها	%15		
3	المناقشة	%10		
4	الزمن المخصص	%10		
المجموع				
اسم الفاحص:		التاريخ		التوقيع

6 حماية انظمة التشغيل

رقم التمرين:18 الزمن المخصص: ساعة واحدة

اسم التمرين: اختبار النظام بعد إصلاح الثغرات باستخدام **OpenVAS**

مكان التنفيذ: مختبر الحاسوب

اولاً: الأهداف التعليمية

بعد إتمام هذا التمرين، سيتمكن الطالب من:

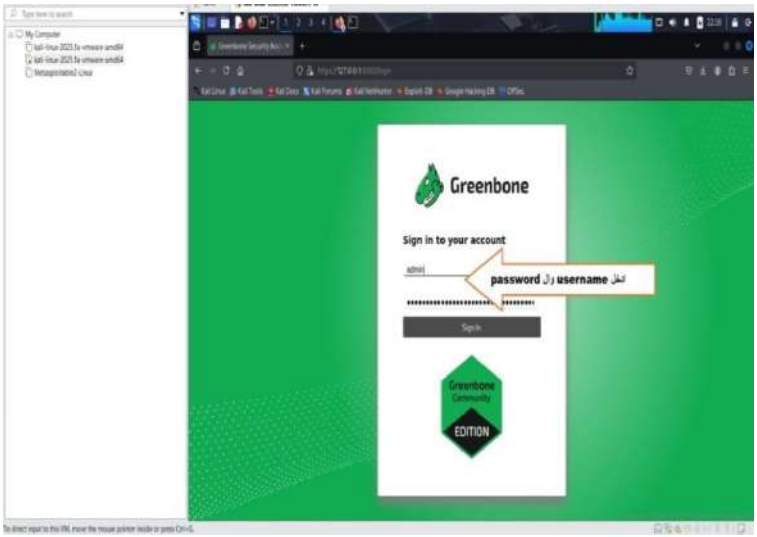
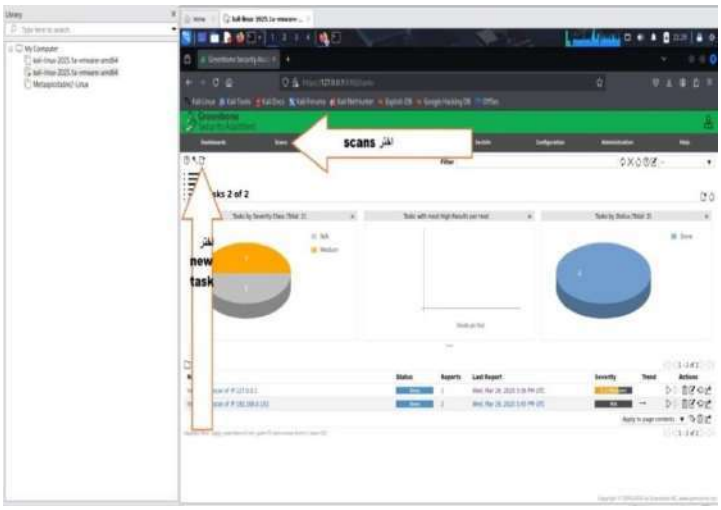
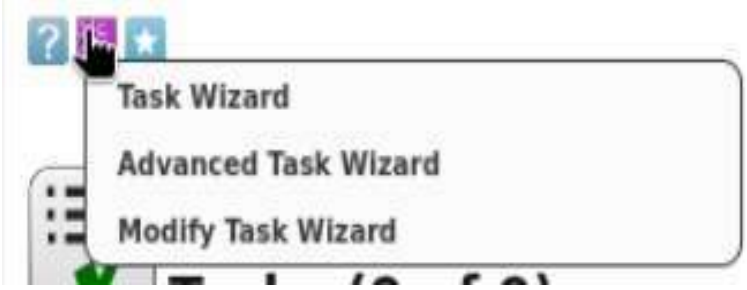
- تدريب الطلبة على استخدام أداة **OpenVAS** لفحص الأنظمة بحثًا عن الثغرات الأمنية.
- التحقق من إغلاق ثغرة تم تحديدها مسبقًا وتطبيق تصحيح أمني.
- تقييم نتائج الفحص ومقارنتها قبل وبعد التصحيح.

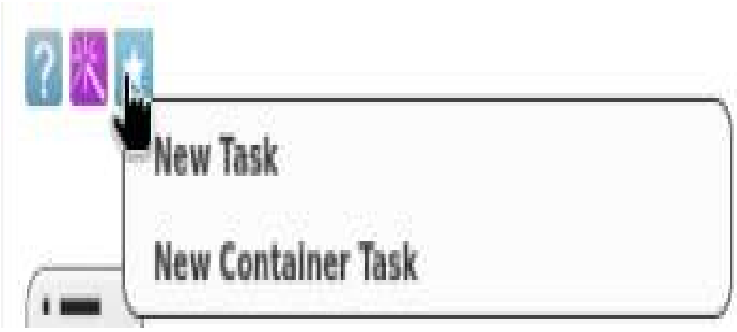
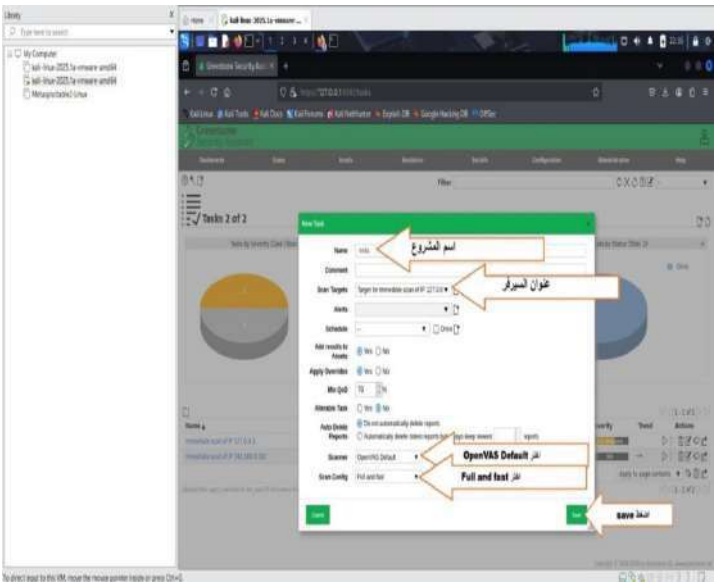
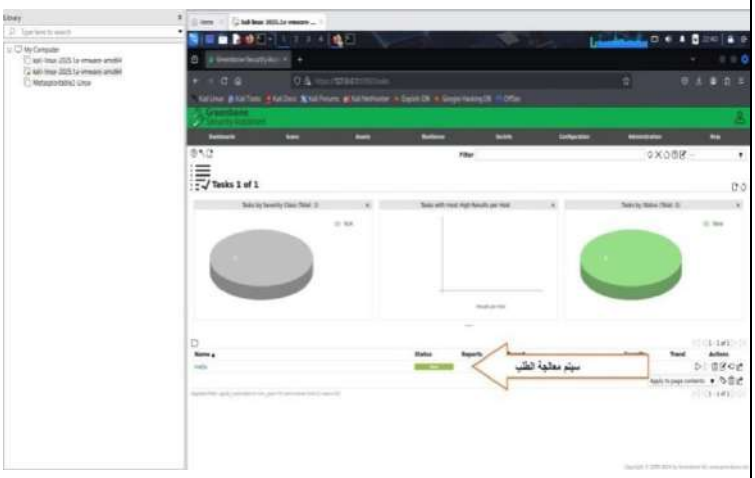
ثانياً: التسهيلات التعليمية

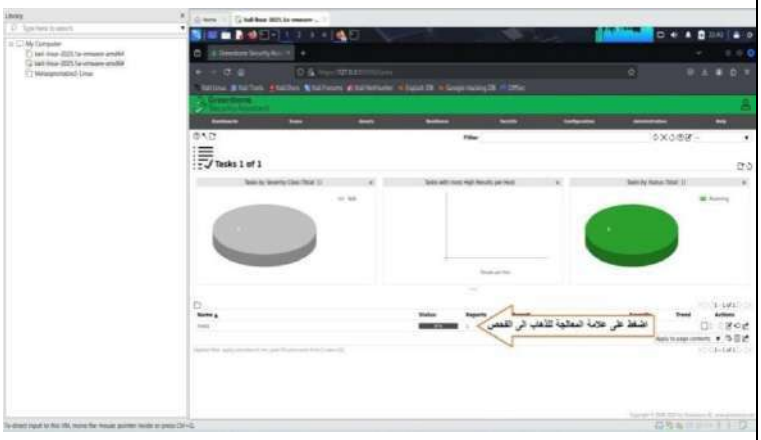
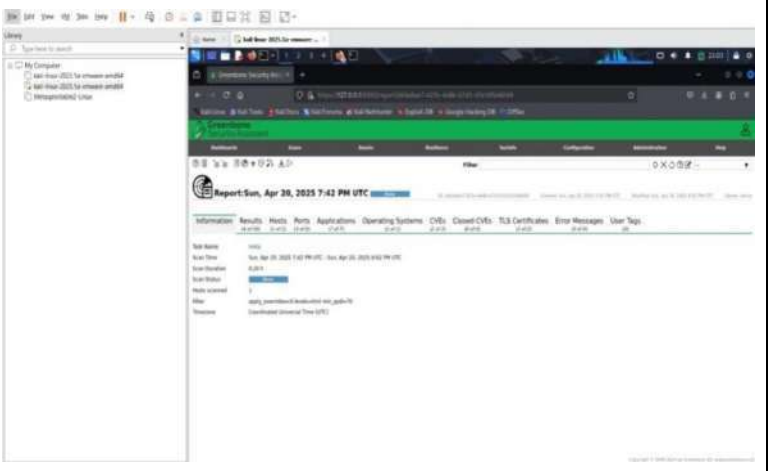
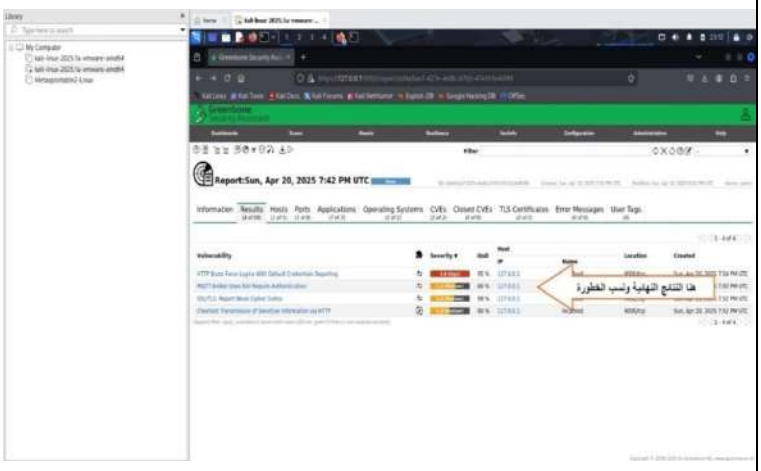
- نظام تشغيل يدعم **OpenVAS** (مثل **Kali Linux** أو توزيعة **Debian/Ubuntu**).
- أداة **OpenVAS** (غالبًا يكون مثبتًا مسبقًا في Kali أو يُثبت باستخدام **gvm-setup**).
- جهاز مستهدف يحتوي على ثغرة معروفة (مثلاً جهاز وهمي بنظام **Windows** أو **Linux** قديم).

ثالثاً: خطوات تنفيذ التمرين

-1	تفتح أداة **OpenVAS** عن طريق أي متصفح ولكن بالنظر الى أنّ أنظمة الـ **kali linux** تدعم متصفح **Firefox** سيتم التدخول من خلاله.	

-2	بعد فتح المتصفح قم بإدخال الـ(IP) 127.0.0.1:9392 سوف تفتح لك نافذة كما مبين بالشكل إدخال **username** و **password** للوصول إلى النافذة الرئيسية.	
-3	في لوحة معلومات **OpenVAS**، ابحث عن علامة التبويب **"scans"** وانقر عليها. من قائمة ثم اختر **"new Task"**.	
-4	هناك طريقتان لبدء الفحص. الطريقة الأولى **Task Wizard** هي طريقة إعداد تفصيلية	

-5	أمّا الطريقة الثانية **New Task** فتعد طريقة سريعة لأنها تقبل إدخال عنوان الجهاز فحسب.	
-6	اختر **New Task** للبدأ بفحص جديد ومفصل ستنبثق قائمة اكتب اسم المشروع وادخل عنوان السيرفر المراد جمع المعلومات عنه ثم اضغط **Create** للبدأ بانشاء مسح للنظام	
-7	سيقوم البرنامج باجراء فحص شامل على جميع الثغرات الموجودة ولكن يجب الانتظار قليلا ليتم الانتهاء من البحث عن الثغرات.	

-8 بعد الانتهاء من البحث نضغط على رمز التحميل للدخول إلى عرض النتائج.	
-9 عند الدخول سيتم عرض الكثير من الأحداث منها نوع النظام والمنافذ المفتوحة والشهادات الممنوحة للمواقع وعنوان الجهاز والثغرات المغلقة.	
-10 اضغط على **result** للحصول على النتائج النهائية بعد اكتمال التحميل النتائج تحتوي على حالة النظام من منافذ مفتوحة مع حالة المنفذ أهي عادية أم خطرة؟ وما مستوى الخطورة؟	

-11 المناقشة:

- كيف تقيم مستوى الخطورة للنظام الذي تم فحصه عبر برنامج **OpenVAS؟**
- ما هي الثغرات المفتوحة في النظام؟
- كيف يمكن إغلاق تلك الثغرات ؟

استمارة قائمة الفحص

اسم الطالب: المرحلة: الثانية

التخصص: رقم التمرين:18

اسم التمرين: إختبار النظام بعد إصلاح الثغرات بأستخدام **OpenVAS**

ت	الخطوات	الدرجة القياسية	درجة الأداء	الملاحظ
1	تشغيل الحاسوب والوصول إلى البرنامج وتشغيله عبر المتصفح	%15		
2	خطوات تنفيذ البرنامج والتعرف على المنافذ المفتوحة وحالة النظام	%15		
3	المناقشة	%10		
4	الزمن المخصص	%10		
المجموع				

اسم الفاحص:	التاريخ	التوقيع

أسئلة الفصل السادس

س1 : املأ الفراغات الآتية:

1. الحدث (**Event**) هو إجراء غير ..... يحدث بشكل.....
2. الحادث (**Incident**) هو مجموعة ..... المترابطة التي قد تُعد.....
3. **Process Monitor** هو أداة تُستخدم لمراقبة .....وعرض .....ومفاتيح .....
4. تطبيق إختبار الانحدار هو .....
5. تثبت الجهات المنفذة للهجمات الإلكترونية البرامج الضارة من خلال استغلال الثغرات الأمنية في .....و .....
6. إختبار تطبيقات الويب هو .....

س2: الإجابة بعلامة صح أو خطأ وتصحيح الخطأ أن وجد:

1- الاستجابة للحوادث تهدف إلى تقليل الأضرار وتسريع عملية التعافي.

2- يمكن لفريق الاستجابة تحليل رسائل البريد الاحتيالية بأستخدام أدوات خاصة مثلOpenVAS.

3- التحديثات الأمنية للنظام تساعد في الوقاية من استغلال الثغرات.

4- التصيد عبر الوسائط الاجتماعية يُعرف باسم **Phishing**.

5- إختبار الاختراق الخارجي يتم من داخل المؤسسة لمحاكاة هجوم يقوم به مستخدم لديه صلاحيات داخل الشبكة.

س3 : ما هي أنواع الاختبارات لاختبار النظام بعد إصلاحه؟

س4: بيّن أنواع السجلات

س5 : ما المقصود بادوات مسح الأنظمة واكتشاف الثغرات؟

س6 : وضح باختصار منهجيات إختبار النظام بعد إصلاح الثغرات.

المصادر

المصادر الأجنبية:

1. Practical malware analysis: The hands-on guide to dissecting malicious software by Michael Sikorski and Andrew Honig, 2012.

2. Incident Response & Computer Forensics by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia, 2014.

3. Access Control and Identity Management (Information Systems Security & Assurance) by Mike Chapple, 2020.

4. Modern Operating Systems by Andrew S. Tanenbaum and Herbert Bos, 2022.

5. Cryptography and network security by William Stallings, 2023.

المصادر العربية:

1. أمن المعلومات بلغة ميسرة، تأليف الدكتور خالد بن سليمان الغثبر، 2009.

2. أنظمة التشغيل, تأليف الدكتور زياد عبد الكريم القاضي , 2011.

3. أمن المعلومات, تاليف الدكتور ذيب بن عايض القحطاني , 2022.

4. الأمن السيبراني ودوره في حماية الامن القومي، تأليف الدكتورعطية السحاتي، 2024.