أساسيات أمن المعلومات

معد الحقيبة
أ. أمين عبدالرحمن المقحم

المراجعة العلمية:
د. بسام عبدالعزيز الحمادي
أ. موضي إبراهيم الرميح

معهد الإدارة العامة
INSTITUTE OF PUBLIC ADMINISTRATION

التطويرات التي تمت على حقيبة البرنامج

رمز البرنامج	اسم البرنامج	النسخة	اسم المعد / المطور
١/٨٥٦	أساسيات أمن أنظمة الحاسب	١	فادي محمد ناصر صبحي
٢/٨٥٦	أساسيات أمن المعلومات	٢	محمد عبدالهادي عايض العتيبي
٣/٨٥٦	أساسيات أمن المعلومات	٣	امين عبدالرحمن محمد المقحم

عدد النسخ : ٣

ملاحظة : يعتبر من عمل على النسخة الأولى كمعد للحقيبة ومن عملوا على باقي النسخ كمطورين لها

عزيزي المتدرب، يسر معهد الإدارة العامة التحاقك بهذا البرنامج، ويأمل أن يعود ذلك بالفائدة والتحصيل الجيد. وحرصاً من المعهد على جودة التدريب يدعوك لقراءة الضوابط التالية:

الفترة الزمنية للتدريب:

يبدأ التدريب يومياً في تمام الساعة الثامنة صباحاً وحتى الساعة الثانية وعشر دقائق ظهراً.

الانضباط والالتزام:

تهدف سياسة معهد الإدارة العامة إلى تحقيق الجودة في العملية التدريبية، وأن يحرص المتدرب على مواعيد بدء وانتهاء الجلسات التدريبية، بحيث يكرس كل وقته وجهده للاستفادة من البرنامج.

وفي حالات الغياب أو الانقطاع عن التدريب تنص القواعد والضوابط على التالي:

١- يقوم عضو هيئة التدريب بتسجيل غياب المتدربين في بداية كل جلسة تدريبية، ويعتبر متغيباً كل من يحضر بعد ذلك ولو حضر الجزء الأكبر من الجلسة.

٢- في حال بلوغ مجموع ساعات غياب المتدرب (٢٠٪) من ساعات البرنامج يتم استبعاده من البرنامج وتخطر جهته بذلك لاتخاذ الإجراءات التي تراها مناسبة.

تقييم المتدرب:

يقوم عضـــو هيئة التدريب بعملية تقييم المتدرب خلال الفترة التدريبية بناءً على المعايير التالية:

١- الحضور أكثر من ٨٠٪ من ساعات التدريب.

٢- المشاركة الفعالة أثناء التدريب.

٣- تنفيذ المهام والتمارين التي يطلبها المدرب من المتدرب خلال فترة البرنامج التدريبي.

٤- يعتبر المتدرب مجتازاً للبرنامج التدريبي عند اعتماد المدرب لنتائج المتدربين في البرنامج.

قواعد عامة:

١- يمنع التدخين منعاً باتاً في قاعات التدريب وفي جميع أروقة المعهد.

٢- يغلق الجوال أثناء الجلسات التدريبية.

٣- لا يسمح بإحضار المشروبات أو المأكولات داخل قاعات التدريب.

٤- المحافظة على الأجهزة والوسائل التدريبية الموجودة داخل القاعات.

مع التمنيات لكم بالتوفيق.

الجدول الزمني

لبرنامج أساسيات أمن المعلومات

اليوم	الجلسة	الوقت	الموضوعات
الأول	الأولى	٨:٠٠-٩:٤٠	❖ مقدمة في أمن المعلومات: • ما هو أمن المعلومات؟ • أهمية أمن المعلومات. • الصعوبات التي تواجه أمن المعلومات. • من هم المهاجمون؟ • الهجمات وتقنيات الدفاع. • المخاطر التي تهدد الأنظمة.
		٩:٤٠-١٠:٠٠	استراحة
	الثانية	١٠:٠٠-١١:٤٠	❖ حماية الأنظمة: • تدعيم أمن نظام التشغيل. • منع الهجمات التي تستهدف متصفح الويب. • مضادات الفيروسات. • تثبيت برامج الحاسوب المهمة للحماية. • الإعدادات الدورية للحفاظ على سلامة الجهاز.
		١١:٤٠-١٢:٣٠	استراحة وصلاة الظهر
	الثالثة	١٢:٣٠-٢:٣٠	❖ مقدمة في أمن الأجهزة النقالة. ❖ تطبيق استخدام برامج الحماية على الجهاز النقال.
الثاني	الأولى	٨:٠٠-٩:٤٠	❖ السياسات الأمنية لأنظمة المعلومات. ❖ ثغرات الشبكة والهجمات عليها: • ثغرات الشبكة. • أنواع الهجمات. • طرق الهجمات على الشبكة. ❖ الدفاع عن الشبكات: • تصميم شبكة آمنة. • أجهزة أمن الشبكات. • مرشحات محتوى الإنترنت.
		٩:٤٠-١٠:٠٠	استراحة

	الثانية	١٠:٠٠-١١:٤٠	❖ مقدمة في التشفير: • التشفير المتماثل. • التشفير غير المتماثل. • أساليب التشفير. • استخدام برمجيات التشفير.
		١١:٤٠-١٢:٣٠	استراحة وصلاة الظهر
	الثالثة	١٢:٣٠-٢:٣٠	❖ تطبيقات التشفير: • الشهادات الرقمية والبنية الأساسية للمفتاح العمومي. • إدارة المفاتيح.
الثالث	الأولى	٨:٠٠-٩:٤٠	❖ الأمن والحوسبة السحابية. ❖ أساسيات التحكم في الوصول: • ما هو التحكم في الوصول. • الطرق المنطقية للتحكم في الوصول. • التحكم في الوصول المادي.
		٩:٤٠-١٠:٠٠	استراحة
	الثانية	١٠:٠٠-١١:٤٠	❖ المصادقة: • تعريف المصادقة. • طرق تفويض المصادقة. • المصادقة عن بعد والأمان. ❖ تقييم الثغرات: ● تقييم وإدارة المخاطر وتخفيفها. • تحديد الثغرات.
		١١:٤٠-١٢:٣٠	استراحة وصلاة الظهر
	الثالثة	١٢:٣٠-٢:٣٠	❖ استمرارية العمل: • التحكم بالمخاطر البيئية. • البيئة المناسبة لعمل الحاسوب. • النسخ الاحتياطي وحماية الملفات. • استعادة الملفات المحذوفة.

اسم البرنامج: أساسيات أمن المعلومات

مدة البرنامج بالأيام: ٣ أيام

الهدف العام:

تنمية مهارات المتدرب على أمن المعلومات والتهديدات التي تواجهه، وتطبيق الحلول الأمنية المناسبة لمواجهة هذه التهديدات بكفاءة وفعالية.

الأهداف التفصيلية:

من المتوقع بعد أنتهاء المتدرب من المشاركة في البرنامج التدريبي الحالي أن يكون قادراً على أن:

١. يُعرف أمن المعلومات بسهولة ويسر.
٢. يتعرف على مصادر الهجمات بسهولة ويسر.
٣. يصنف أنواع الهجمات على جهاز الحاسب والشبكة بحسب أضرارها بدقه وإتقان.
٤. يطبق طرق وأساليب الحماية اللازمة للحفاظ على سلامة الأجهزة بكفاءة وفاعلية.
٥. يستخدم قوانين وأحكام الحماية حسب الأنظمة المستخدمة في المنشأة بدقة وإتقان.
٦. يميز بين ثغرات الشبكات بحسب مصادرها بسهولة ويسر.
٧. يتعرف على أساسيات وأمن الحوسبة السحابية بسهولة ويسر.
٨. يتعرف على طرق الهجمات المختلفة على الشبكات وأساليب الدفاع المناسبة بدقة وإتقان.
٩. يتعرف على طرق التشفير وكيفية استخدامه لحماية المعلومات بكفاءة وفاعلية.
١٠. يستخدم تطبيقات التشفير وأساليب إدارة مفاتيحه بكفاءة وفاعلية.
١١. يميز بين طرق التحكم في الوصول وكيفية استخدامها بدقة وإتقان.
١٢. يتعرف على وثائق تفويض المصادقة وتحقيقها بسهولة ويسر.
١٣. يحدد المخاطر في أمن المعلومات وكيفية تخفيفها وإدارتها بدقة وإتقان.
١٤. يطبق الإجراءات اللازمة لاسترداد البيانات عند حدوث الكوارث بكفاءة وفاعلية.

شروط القبول في البرنامج: (يجب أن يتوفر لدى المتدرب ما يلي):

١. الإلمام بمبادئ اللغة الإنجليزية.
٢. الإلمام بمبادئ الحاسب الآلي.
٣. الإلمام بمهام وموضوعات البرنامج.
٤. مناسبة التخصص مع الوظائف التي يستهدفها البرنامج
٥. خبرة لا تقل عن سنة في ممارسة التخصص

موضوعات التدريب:

١. مقدمة في أمن المعلومات.
٢. حماية الأنظمة.
٣. أمن المعلومات للأجهزة النقالة.
٤. السياسات الأمنية لأنظمة المعلومات.
٥. ثغرات الشبكة والهجمات عليها.
٦. الدفاع عن الشبكات.
٧. مقدمة في التشفير.
٨. تطبيقات التشفير.
٩. الأمن والحوسبة السحابية.
١٠. أساسيات التحكم في الوصول.
١١. المصادقة.
١٢. تقييم الثغرات.
١٣. استمرارية العمل.

تجهيز المعمل

يحتوي هذا البرنامج على مجوعة من التمارين العملية التي تساعد المتدرب على فهم المحتوى بطريقة أفضل. بعض التمارين يحتاج تنفيذها إلى كمبيوتر يعمل في بيئة ويندوز ٨ وله صلاحيات مدير نظام كاملة بدون قيود. لذلك يجيب توفير برنامج تخيلي يحتوي على نسخة من نظام تشغيل ويندوز ٨ للتمكن من عمل جميع التمارين.

لتجهيز المعمل بشكل مناسب يرجى اتباع التالي:

١- تعطيل أي برنامج يقوم بحذف آخر التعديلات على الجهاز مثل برنامج (Windows SteadyState)، حتى لا يقوم هذا البرنامج بحذف التجهيزات بعد إعادة تشغيل الجهاز.
٢- تثبيت أي برنامج تخيلي مثل (VMware،Windows Virtual PC).
٣- إضافة نسخة من نظام (Windows 8) للبرنامج التخيلي.
٤- يجب إضافة أدوات البرنامج التخيلي، والتي تتيح نقل الملفات من النظام التشغيلي الحقيقي إلى نظام التشغيل التخيلي.

*__ملاحظة:__ جميع خطوات التمارين والتطبيقات تم إعدادها على نظام تشغيل ويندوز ٨، لكن هذا لا يعني عدم إمكانية تطبيقها على أنظمة تشغيل سابقة.

فهرس الموضوعات

فهرس الجداول والأشكال أو الرسوم البيانية

اليوم التدريبي الأول

اليوم التدريبي الثاني

اليوم التدريبي الثالث

فهرس الجداول والأشكال أو الرسوم البيانية

فهرس التمرينات التطبيقية والحالات الدراسية

فهرس الشرائح التدريبية

معهد الإدارة العامة
INSTITUTE OF PUBLIC ADMINISTRATION

اليوم التدريبي الأول

اليوم التدريبي الأول

الجلسة	الموضوع التدريبي	الزمن	الهدف السلوكي
الأولى	❖ مقدمة في أمن المعلومات.	٩٠د	❖ التعرف على أمن المعلومات، ماهيته وأهميته. ❖ التعرف على المخاطر التي تهدد أمن المعلومات والصعوبات في مواجهتها.
الثانية	❖ حماية الأنظمة.	٩٠د	❖ التعرف على طرق وأساليب الحماية المختلفة. ❖ تطبيق بعض طرق وأساليب الحماية المختلفة.
الثالثة	❖ أمن المعلومات للأجهزة النقالة.	١٢٠د	❖ التعرف على الأمن في الأجهزة النقالة. ❖ استخدام برامج الحماية للأجهزة النقالة. ❖ مناقشة الحالات الفردية للمتدربين.

اليوم الأول - الجلسة التدريبية الأولى

مقدمة في أمن المعلومات

لم يكن هناك قلق مع بدايات شبكة الإنترنت تجاه "جرائم" يمكن أن تنتهك على الشبكة، وذلك نظراً لمحدودية مستخدميها علاوة على كونها مقصورة على فئة معينة من المستخدمين وهم الباحثين ومنسوبي الجامعات. لهذا فالشبكة ليست آمنة في تصميمها وبناءها. لكن مع توسع استخدام الشبكة ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة ازدادت مع الوقت وتعددت صورها وأشكالها. بعد التقدم والتطور الذي حصل في عالم الأمن (Security)، وبعد تطور أساليب المخترقين في عملياتهم وتنوعها، كان لابد من إيجاد طريقة آمنة لتخطي هذه الأمور وخصوصاً في الأمور الحساسة كالتجارة الإلكترونية وعمليات كشف الحسابات عن طريق الإنترنت وغيرها، فكان لابد من تأمين ذلك. [١]

أهم الأهداف المقصودة في تلك الجرائم:

- **المعلومات:** يشمل ذلك سرقة أو تغيير أو حذف المعلومات.
- **الأجهزة:** ويشمل ذلك تعطيلها أو تخريبها.
- **الأشخاص أو الجهات:** تهدف فئة كبيرة من الجرائم على شبكة الإنترنت أشخاص أو جهات بشكل مباشر كالتهديد أو الابتزاز. علماً بأن الجرائم التي تكون أهدافها المباشرة هي المعلومات أو الأجهزة تهدف بشكل غير مباشر إلى الأشخاص المعنيين أو الجهات المعنية بتلك المعلومات أو الأجهزة.

بقي أن نذكر أن هناك جرائم متعلقة بالإنترنت تشترك في طبيعتها مع جرائم التخريب أو السرقة التقليدية، كأن يقوم المجرمون بسرقة أجهزة الحاسوب المرتبطة بالإنترنت أو تدميرها مباشرة أو تدمير وسائل الاتصال كالأسلاك والأطباق الفضائية وغيرها. حيث يستخدم المجرمون أسلحةً تقليديةً ابتداء من المشارط والسكاكين وحتى عبوات متفجرة، وكمثال لهذا الصنف من الجرائم قام مشغل أجهزة في إحدى الشركات الأمريكية بصب بنزين على أجهزة شركة منافسة وذلك لإحراقها حيث دمر مركز الحاسب الآلي الخاص بتلك الشركة المنافسة برمته. [٢]

بعض جرائم الإنترنت التي تؤدي إلى إتلاف الأجهزة وفقد المعلومات في الشبكة:

صناعة ونشر الفيروسات: وهي أكثر الجرائم أنتشاراً وتأثيراً. إن الفيروسات كما هو معلوم ليست وليدة الإنترنت، فلم يكن الإنترنت الوسيلة الأكثر استخداماً في نشر وتوزيع الفيروسات إلا في السنوات الخمس الأخيرة، حيث أصبحت الإنترنت وسيلة فعالة وسريعة في نشر الفيروسات. ويعتبر الهدف

المباشر للفيروسات هي المعلومات المخزنة على الأجهزة المقتحمة حيث يقوم بتغييرها أو حذفها أو سرقتها ونقلها إلى أجهزة أخرى.

الاختراقات: تتمثل في الدخول غير المصرح به إلى أجهزة أو شبكات الحاسب الآلي. إن جل محاولات وعمليات الاختراق تتم من خلال برامج متوفرة على الإنترنت يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير، وهنا تكمن الخطورة. تختلف الأهداف المباشرة للاختراقات، فقد تكون المعلومات هي الهدف المباشر حيث يسعى المخترق لتغيير أو سرقة أو إزالة معلومات معينة. وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة عليه، كأن يقوم المخترق بعمليته بقصد إبراز قدراته "الاختراقية" أو لإثبات وجود ثغرات في الجهاز المخترق. من أكثر الأجهزة المستهدفة في هذا النوع من الجرائم هي تلك التي تستضيف المواقع على الإنترنت، حيث يتم تحريف المعلومات الموجودة على الموقع أو ما يسمى بتغيير وجهة الموقع (Defacing). إن استهداف هذا النوع من الأجهزة يعود إلى عدة أسباب من أهمها كثرة وجود هذه الأجهزة على الشبكة، وسرعة أنتشار الخبر حول اختراق ذلك الجهاز خاصة إذا كان يضم مواقع معروفة.

تعطيل الأجهزة: كثر مؤخراَ ارتكاب مثل هذه العمليات، حيث يقوم مرتكبوها بتعطيل أجهزة أو شبكات عن تأدية عملها بدون أن تتم عملية اختراق فعلية لتلك الأجهزة. تتم عملية التعطيل بإرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها الأمر الذي يعيقها عن تأدية عملياتا. من أشهر الأمثلة على هذا النوع من الجرائم تلك التي تقوم بتعطيل الأجهزة المستضيفة للمواقع على الشبكة. إن الأسباب وراء استهداف هذا النوع من الأجهزة تماثل أسباب استهدافها في جرائم الاختراقات والتي سبق ذكرها.

جرائم الإنترنت التي تستهدف جهات سواءَ كانوا أفرادًا أو مؤسسات ففيما يلي عرض لبعضها:

أنتحال الشخصية: هي جريمة الألفية الجديدة كما سماها بعض المختصين في أمن المعلومات وذلك نظراَ لسرعة أنتشار ارتكابها خاصة في الأوساط التجارية. تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية، وتهدف إما لغرض الاستفادة من مكانة تلك الهوية (أي هوية الضحية) أو لإخفاء هوية شخصية المجرم لتسهيل ارتكابه جرائم أخرى. إن ارتكاب هذه الجريمة على شبكة الإنترنت أمر سهل وهذه من أكبر سلبيات الإنترنت الأمنية. وللتغلب على هذه المشكلة، فقد بدأت كثير من المعاملات الحساسة على شبكة الإنترنت كالتجارية في الاعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي والتي تجعل من ارتكاب هذه الجريمة أمراَ صعباَ.

المضايقة والملاحقة: تتم جرائم الملاحقة على شبكة الإنترنت غالباَ باستخدام البريد الإلكتروني أو وسائل الحوارات الآنية المختلفة على الشبكة. تشمل الملاحقة رسائل تهديد وتخويف ومضايقة. تتفق

جرائم الملاحقة على شبكة الإنترنت مع مثيلاتها خارج الشبكة في الأهداف والتي تتمثل في الرغبة في التحكم بالضحية. تتميز جرائم المضايقة والملاحقة على الإنترنت بسهولة إمكانية المجرم في إخفاء هويته علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة. الأمر الذي ساعد على تفشي هذه الجريمة. من المهم الإشارة إلى كون طبيعة جريمة الملاحقة على شبكة الإنترنت لا تتطلب اتصال مادي بين المجرم والضحية لا يعني بأي حال من الأحوال قلة خطورتها. فقدرة المجرم على إخفاء هويته تساعده على التمادي في جريمته والتي قد تفضي به إلى تصرفات عنف مادية علاوة على الآثار النفسية السلبية على الضحية.

التغرير والاستدراج: غالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة. حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة على الإنترنت والتي قد تتطور إلى التقاء مادي بين الطرفين. إن مجرمي التغرير والاستدراج على شبكة الإنترنت يمكن لهم أن يتجأوزوا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد آخر. وكون معظم الضحايا هم من صغار السن، فإن كثير من الحوادث لا يتم الإبلاغ عنها، حيث لا يدرك الكثير من الضحايا أنه قد غرر بهم.

التشهير وتشويه السمعة: يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فردًا أو مجتمعًا أو دينًا أو مؤسسةً تجاريةً أو سياسية. تتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة قائمة هذه الوسائل إنشاء حسابات في شبكات التواصل الاجتماعي تحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين.

النصب والاحتيال: أصبح الإنترنت مجالاً رحبًا لمن له سلع أو خدمات تجارية يريد أن يقدمها، وبوسائل غير مسبوقة كاستخدام البريد الإلكتروني أو عرضها على موقع على الشبكة أو عن طريق ساحات الحوار. ومن الطبيعي أن يساء استخدام هذه الوسائل في عمليات نصب واحتيال. لعلنا جميعًا شاهدنا كثيرًا من صور التسويق المفخخة بأغراض وغايات تنتهي بالنصب والاحتيال مثل بيع سلع أو خدمات وهمية، أو المساهمة في مشاريع استثمارية وهمية أو سرقة معلومات البطاقات الائتمانية واستخدامها. وتتصدر المزادات العامة على البضائع عمليات النصب والاحتيال على الإنترنت. إن ما يميز عمليات النصب والاحتيال على الإنترنت عن مثيلاتها في الحياة اليومية هي سرعة قدرة مرتكبها على الاختفاء والتلاشي.

الهجوم Attacks:

يقسم الهجوم إلى أربعة أقسام وهي:

١-**هجوم التنصت على الرسائل** Interception Attacks: وفكرة عمل هذا الهجوم أن المهاجم يراقب الاتصال بين المرسل والمستقبل للحصول على المعلومات السرية وهو ما يسمى بالتنصت على الاتصال (Eavesdropping).

٢-**هجوم الإيقاف** Interruption Attacks: وهذا النوع يعتمد على قطع قناة الاتصال لإيقاف الرسالة أو البيانات من الوصول إلى المستقبل وهو ما يسمى أيضاً برفض الخدمة (Denial of service).

٣-**هجوم يعدل على محتوى الرسالة** Modification Attacks: وهنا يتدخل المهاجم بين المرسل والمستقبل (يعتبر وسيط بين المرسل والمستقبل) وعندما تصل إلى المهاجم فإنه يقوم بتغيير محتوى الرسالة ومن ثم إرسالها إلى المستقبل، ويحدث التعديل بغير علم المستقبل بتعديل الرسالة من قبل المهاجم.

٤-**الهجوم المزور أو المفبرك** Fabrication Attacks: وهنا يرسل المهاجم رسالة للضحية مفادها أنه صديقه ويطلب منه المعلومات أو كلمات سرية خاصة بالشركة مثلًا.

ما هو أمن المعلومات

قبل أن ندافع عن أجهزة الحاسوب والبيانات التي تختزنها أو تقوم بمعالجتها، من الضروري أن نعرف ماهو أمن المعلومات؟ بالإضافة لأن نفهم لماذا أمن المعلومات مهما لنا اليوم؟ ومن هم المستفيدين من الهجمات؟

تعريف أمن المعلومات:

بشكل عام، الأمن يتشكل في صورة الحرية من الخوف أو الخطر. على سبيل المثال تعيش الدول في مأمن حين يكون لها جيوش لديها القوة لحماية مواطنيها من القوى الخارجية المعادية. هذه الحالة من الحرية وجدت بسبب التدابير الوقائية التي تم إنشائها والحفاظ عليها. مع ذلك وجود الجيوش لا تكون ضمانة للدول بأن الهجوم عليها لن يتم أبدًا، فقد تقوم قوى خارجية معادية بشن هجمات قوية في أي وقت. لكن الهدف للأمن القومي هو أن تكون قادرة للدفاع عن نفسها ضد تلك الهجمات والنجاة منها في حال حدوثها. يستخدم مصطلح أمن المعلومات لوصف مهمة حماية المعلومات الموجودة بصورة رقمية. تلك المعلومات الرقمية عادة ما تكون معالجة باستخدام معالجات دقيقة (microprocessors)، ومخزنة في أجهزة تخزين ضوئية أو ممغنطة كالأقراص الصلبة، وتنتقل عن طريق شبكة كالشبكات المحلية أو الإنترنت. يمكن أن يفهم أمن المعلومات من خلال دراسة أهدافه وكيفية تحقيقها.

أولًا، أمن المعلومات يتأكد من أن التدابير الوقائية قد نفذت بشكل صحيح. لكن كما ذكرنا سابقًا في حديثنا عن الجيوش، فالتدابير الوقائية لن تمنع حدوث الهجمات أبدًا ولن تضمن أن النظام أمن تمامًا، لذلك فإن أمن المعلومات يصنع دفاعًا لدرء محاولات الهجمات، ولمنع النظام من الانهيار في حال حدوثها، إذًا فأمن المعلومات هو الحماية.

ثانيًا، يهدف أمن المعلومات لحماية المعلومات القيمة لدى الأشخاص والمنظمات، وتلك القيمة تأتي من خصائص تختص بها تلك المعلومات. ثلاثة من تلك الخصائص يجب حمايتها من قبل أمن المعلومات ألا وهن:

١-**السرية** (Confidentiality): تضمن السرية أن الأطراف المخولين فقط هم من يستطيعون استعراض المعلومات.

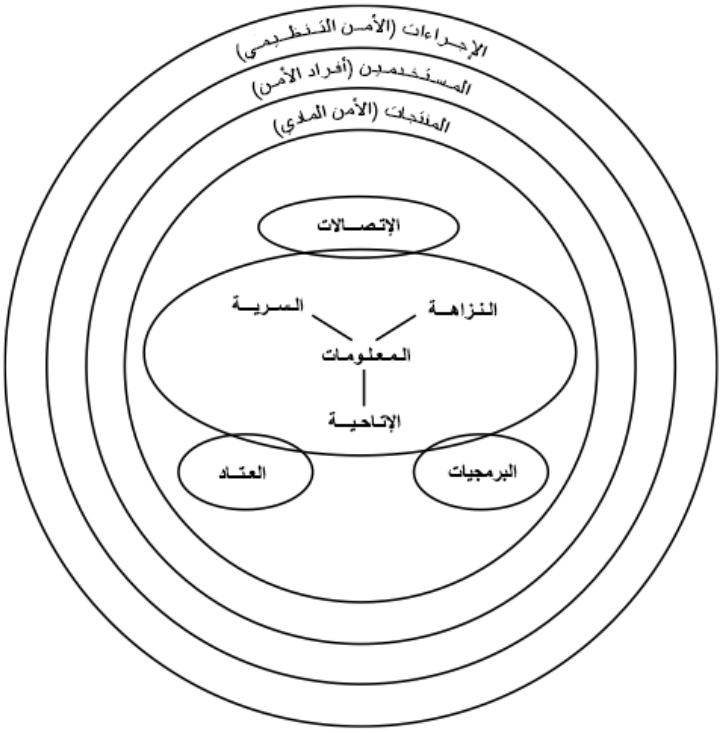
٢-**النزاهة** (Integrity): تضمن النزاهة أن المعلومات صحيحة ولم يغير تلك البيانات برمجيات خبيثة أو أشخاص غير مصرح لهم بذلك.

٣-**الإتاحية** (Availability): تضمن الإتاحية إمكانية الوصول للبيانات لكلِ من الأشخاص المرخص لهم.

أمن المعلومات يتحقق في حماية الخصائص الثلاثة السابقة والمعروفة بـ(CIA).

مع العلم أن أمن المعلومات يشتمل على ما هو أكثر من حماية المعلومات بذاتها، فتلك المعلومات تختزن في عتاد الحاسوب وتعالج ببرمجياته وتنتقل باستخدام وسائل الاتصالات. فيتوجب على أمن المعلومات حماية كلًا منها ليتوصل لحماية المعلومات. والهدف الآخر لأمن المعلومات هو حماية الخصائص الثالثة السابقة (السرية، النزاهة والإتاحية) لجهاز الحاسوب الذي يختزن ويعالج وينقل المعلومات.

يتحقق أمن المعلومات من خلال مزيج من ثلاثة عناصر. كما هي موضحة في الرسم المبين في الأسفل. المعلومات وعتاد الأجهزة والبرمجيات والاتصالات محمية بثلاثة طبقات: المنتجات، المستخدمين، الإجراءات. هذه الطبقات الثلاث تتفاعل مع بعضها البعض. على سبيل المثال، الإجراءات ترشد المستخدمين عن كيفية استخدام المنتجات لحماية المعلومات.



الشكل 1-١: عناصر أمن المعلومات

لذلك يمكننا تعريف أمن المعلومات بشكل أشمل بأنه حماية النزاهة والسرية وتوافر المعلومات أو ما يسمى بالإتاحية على الجهاز الذي يخزن ويعالج وينقل المعلومات وذلك من خلال المنتجات والمستخدمين والإجراءات.

مصطلحات أمن المعلومات

الأصول (Asset): والأصل هو الشيء ذو القيمة الثمينة والذي دائمًا ما يكون هدف أمن المعلومات هو حمايته.

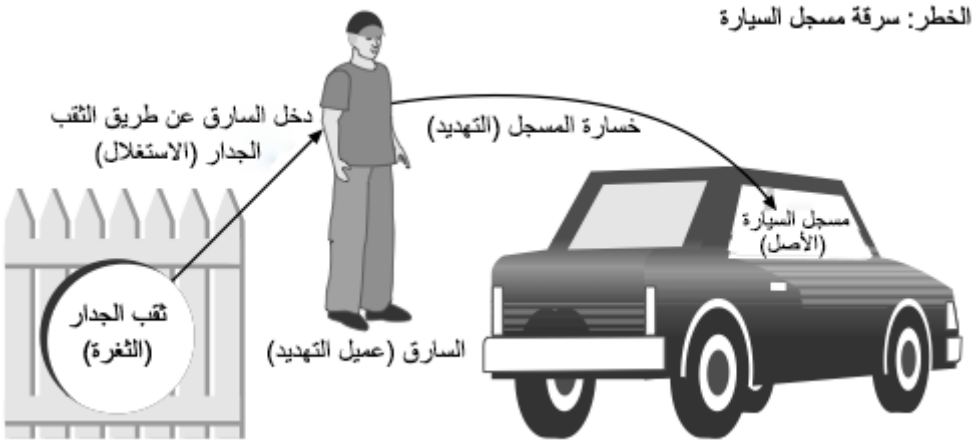
التهديد (Threat): التهديد قد يكون حدث أو كائن يتمكن من هزيمة الإجراءات الأمنية بشكل أو بآخر وبالتالي يتسبب بالخسارة. وبالمثل فإن تهديدات أمن المعلومات هي الأحداث أو الأفعال التي تشكل خطرا على المعلومات. لكن التهديد بحد ذاته لا يعني أن أمن المعلومات قد أنتهك، لكنه ببساطه يعني احتمالية حدوث خسارة حقيقية.

عميل التهديد (Threat Agent): عميل التهديد هو الشخص أو الشيء الذي يمتلك القدرة على تنفيذ التهديد. وفي أمن المعلومات من الممكن أن يكون عميل التهديد شخص يحاول اقتحام شبكة حاسوب آمنة. أو يمكنه أن يكون قوة من قوى الطبيعة، على سبيل المثال الكوارث الطبيعة كالزلازل والفيضانات التي يمكن أن تدمر أجهزة الحاسوب وبالتالي تدمر المعلومات. أو قد يكون فايروس يهاجم شبكة الحاسوب مثلاً.

الثغرات (Vulnerability): الثغرة أو الضعف هو ما يسمح لعامل الخطر تجأوز الحواجز الأمنية. على سبيل المثال، هناك ثغرة يجب لأمن المعلومات سدها، وهي خلل في برمجية نظام التشغيل التي قد تسمح لأشخاص غير مصرح لهم بالدخول للنظام بغير كلمة مرور.

الاستغلال (Exploiting): وهو استفادة عامل الخطر من الثغرات والضعف الأمني في النظام. مثالًا على ذلك حين يعرف المهاجم أن نظام بريد إلكتروني معين لا يمسح الملفات المرفقة بالبريد بحثًا عن برمجيات خبيثة، فيستغل هذه الثغرة ويرفق ملفات مطعمة بالفيروسات باستخدام نظام ذلك البريد.

الخطر (Risk): الخطر هو احتمالية أن يستغل الثغرة عامل الخطر. وفي الواقع لا يمكن أبدًا أن يُقضى على الخطر بشكل كامل. فإن ذلك يكلف الكثير من الجهد والمال ويتطلب وقتًا طويلًا. لذلك يجب علينا دائمًا افتراض إمكانية حدوث الخطر. وعليها فإن المنظمات تتساءل "كم من الخطر ممكن أن يصبح مقبولًا؟". أخيراً هنالك ثلاثة خيارات في التعامل مع المخاطر وهي: قبول المخاطر، التقليل من المخاطر أو نقل المخاطر.



الشكل 2-١: مصطلحات أمن المعلومات

أهمية أمن المعلومات

أمن المعلومات مهم للشركات والأفراد. فالأهداف الرئيسية لأمن المعلومات هي منع سرقة البيانات، إعاقة سرقة الهوية، تجنب العقوبات القانونية لعدم تأمين المعلومات، للحفاظ على الإنتاجية واستمراريتها وإحباط العمليات الإرهابية في الإنترنت.

منع سرقة البيانات: دائمًا ما يرتبط أمن المعلومات بمنع سرقة البيانات، فالهدف الرئيسي للشركات من أمن المعلومات هو غالبًا حمايتها من السرقة. سرقة بيانات الشركات والأعمال تتضمن سرقة الأعمال الملكية التجارية، كبحث يسعى لأنتاج علاج جديد أو قوائم العملاء التي غالبًا ما يسعى المنافسون في المجال ذاته للحصول عليها. سرقة البيانات هي أحد أكبر أسباب الخسائر المالية الناتجة عن الهجمات. وفقًا لدراسة أجراها مكتب التحقيقات الفيدرالية لأمن وجرائم الحاسوب، فقد تجاوزت الخسائر الناجمة عن سرقة البيانات السرية لـ٤٩٤ شخصًا أجريت عليهم الدراسة بـ١٠ ملايين دولار. مع العلم أن الخسارة الفعلية قد تتخطى ذلك الرقم بكثير لكن الكثير من الشركات تتردد في الإفصاح عن ذلك خوفًا من جلب السمعة الأمنية السيئة لها. سرقة البيانات لا تقتصر على الشركات فقط، فيكون الأفراد ضحايا لسرقة البيانات في كثير من الأحيان. وكشف الاستطلاع الذي أجراه معهد Ponemon أن ٦٢٪ ممن أجريت عليهم الدراسة تم إخبارهم بأن بياناتهم السرية قد فقدت أو سرقت. والتقارير تذكر أن الخسائر من الاحتيال في استخدام بطاقات الائتمان على الإنترنت بازدياد حيث أنها تتجاوز ٥ مليار دولار سنويًا.

إعاقة سرقة الهوية: وتشمل سرقة الهوية استخدام المعلومات الشخصية لشخص ما، مثل استخدام رقم الضمان الاجتماعي لإنشاء حساب بنكي أو استخراج بطاقة ائتمانية غير مدفوعة، تاركين الضحايا مع الديون. فقد حدث أن اشترى لصوص الهوية سيارات ومنازل باستخراج قروض بنكية بأسماء أشخاص آخرين. التكاليف على الأفراد الذين كانوا ضحايا لسرقة الهوية نتيجة لاختراق البيانات في ازدياد. فقد كشفت دراسة أجريت من قبل مركز كلية أوتيكا لإدارة الهوية وحماية المعلومات (CIMIP) أن متوسط مقدار خسارة الدولار لضحايا سرقة الهوية خلال السنوات القليلة الأخيرة وصلت لـ ٣١٣٥٦ دولار.

على المستوى الوطني، والدولة، وعلى المستوى المحلي، فالتشريعات التي تتعامل مع هذه المشكلة المتفاقمة لا تزال حديثةً. على سبيل المثال، قانون المعاملات الائتمانية العادلة والدقيقة هو القانون الاتحادي الأمريكي الذي يعالج سرقة الهوية. وينص هذا القانون على نظام وطني لكشف الغش والتنبيهات عنه. مع طلب وكالات الائتمان لتحديد نمط معين لسارقي الهوية حتى يتمكنون من منعهم. ويمكن للمستهلكين أيضاً الحصول على تقرير سنوي مجاني للائتمان الخاص بهم للمساعدة

على التعرف بشكل أسهل وأسرع في حال حدثت سرقة الهوية. ومع ذلك فإن للخبراء رأي بأن أفضل حل لمنع سرقة الهوية هو حفظ البيانات الخاصة ومنع سرقتها.

تجنب العقوبات القانونية لعدم تأمين المعلومات: في السنوات الأخيرة سنت قوانين وعقوبات للحد من الجرائم الإلكترونية وحماية المستخدمين منها. فقد تتعدى عقوبات الجرائم الإلكترونية الغرامات المالية وتصل للسجن سنوات عدة. كما لم تقتصر العقوبة على المهاجم فقط بل قد تكون المؤسسة أو المنظمة التي هوجمت وتسربت معلومات مستخدميها الخاصة أو السرية عرضة للمساءلة والعقاب نتيجة لعدم تأمين معلوماتهم بشكل كافي.

أسئلة ونقاش(١):

س١: عرف أمن المعلومات واذكر أهم مصطلحاته؟

س٢: ماهي أهم الأهداف المقصودة في جرائم أمن المعلومات؟

س٣: لماذا أمن المعلومات مهم في وقتنا الحالي، وما هي أهداف أمن المعلومات؟

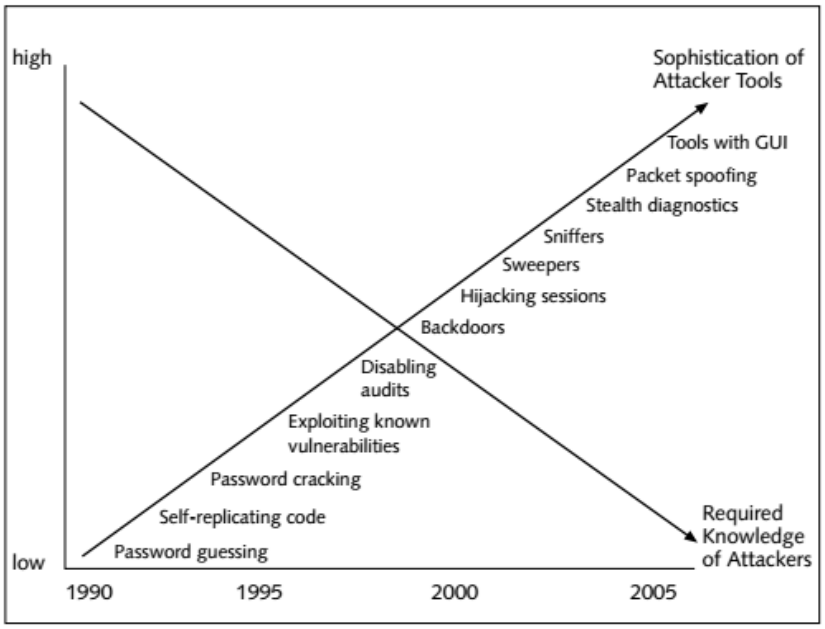
الصعوبات التي تواجه الدفاع ضد الهجمات

التحديات التي تواجهنا في إبقاء الحاسوب أمنا لم تكن بهذه الصعوبة من قبل، ليس فقط بسبب العدد الهائل من الهجمات هي أيضاً بسبب الصعوبات التي تواجهنا في الدفاع ضد هذه الهجمات. وتشتمل هذه الصعوبات على كلٍ من:

سرعة الهجمات: مع الأدوات الحديثة يتمكن المهاجمين من مسح الأنظمة للبحث عن نقاط الضعف فيها ومن ثم شن الهجمات عليها بسرعة غير مسبوقة. على سبيل المثال؛ أصابت دودة Slammer ٧٥٠٠٠ حاسوب في أول إحدى عشر دقيقة بعد إطلاقه، ويتضاعف رقم الإصابات كل ٨,٥ ثانية. في قمته أصبحت Slammer تمسح ٥٥ مليون حاسوب في الثانية باحثةً عن حاسوب آخر لإصابته. أما دودة Blaster فقد أصابت ١٣٨٠٠٠حاسوب في أول ساعة، وأنتهت بإصابة أكثر من ١,٤ مليون حاسوب. في هذه الأيام هناك العديد من أدوات الهجوم التي يمكنها البدء بالهجمات بدون أي مبادرة من الإنسان مما ينتج عنه زيادة في سرعة الهجمات على أنظمة الحاسوب.

تقدم وتطور الهجمات: مع مرور الأيام تزداد الهجمات تعقيدًا مما يجعل التعرف عليها ومواجهتها أكثر صعوبةً. فالمهاجمين اليوم يستخدمون أدوات وبروتوكولات الإنترنت الشائعة لإرسال بياناتهم وأوامرهم الخبية لمهاجمة الحواسيب. وهذا ما يجعل أمر التفرقة وتمييز البيانات الخبيثة من بين البيانات الشرعية أمرًا صعبًا، خاصة وأن سلوك أدوات المهاجمة يختلف في كل مرة حتى وإن كان نوع الهجوم واحدٍ، فيشق على المستخدم التعرف عليها ما لم يكن مسلحًا بالمعرفة اللازمة للتصدي لها.

سهولة أدوات الهجوم: في الماضي كان المهاجمون بحاجة لمعرفة تقنية عالية بأدوات المهاجمة قبل التمكن من استخدامها. أما اليوم فهناك العديد من أدوات الهجوم التي لا تتطلب أن يكون المستخدم على مستوى مهاري تقني عالي. تلك الأدوات متاحة على الإنترنت بحيث يستطيع المستخدم الحصول عليها بسهولة ويسر، علاوة على ذلك فهذه الأدوات مزودة بقوائم مجهزة مسبقًا ليختار منها المستخدم نوع الهجمات المرغوبة بدون أدنى معرفة.



الشكل 3-1: رسم بياني يوضح تطور أدوات الهجوم والانحدار في مستوى المعرفة المطلوب لاستخدامها

يستطيع المهاجمون اكتشاف الثغرات واستغلالها بشكل سريع: عدد الثغرات الجديدة التي يتم اكتشفاها في الأنظمة يتضاعف سنوياً. مما أنتج ما يسمى الهجوم بدون أنتظار (Zero Day Attack) حيث يستغل المهاجمون ثغرات قد كشفت مسبقًا وأفصح عنها دون الحاجة إلى إضاعة الوقت في اكتشاف ثغرة لدخول النظام في كل مرة يخططون فيها للهجوم. الهجوم بدون أنتظار خطر جدًا على أجهزة الحاسوب والشبكات حيث أن الهجوم عادةً يتطلب وقت طويل جدًا لاستكشافَ الثغرة أما النشاطات الخبيثة فهي سريعة جدًا ولا تستغرق وقتًا طويلًا. وهذا تمامًا ما ينافيه الهجوم بدون أنتظار.

التأخير في تطوير منتجات الحماية: منتجي برمجيات الحماية دائمًا ما يكونون تحت ضغط لأنتاج تحديثات تغطي كل أساليب الحماية ضد الهجمات الجديدة. على سبيل المثال، الفيضانات المحتملة من البرمجيات الخبيثة تزداد شهرياً حتى توصلنا إلى أن طريقة الدفاع التقليدية التي تعتمد على التوقيع والتي عن طريقها يمكننا تحديد الفايروس وبقية البرمجيات الخبيثة الأخرى تصبح طريقة غير كافية أو فعالة يومًا بعد يوم (الدفاع عن طريق التوقيع هي طريقة لتحديد البرمجيات الخبيثة حيث ترتبط ببرنامج الحماية من الفيروسات والذي بدوره يحوي على ملف يجمع البرمجيات الخبيثة المنتشرة وتوقيع كلاً منها). وبالمقابل فبرنامجًا واحدًا من البرامج المضادة للفيروسات يستقبل أكثر من ٢٠٠ ألف من الطلبات التي تحوي برامجًا خبيثة كل شهر. فبهذا المعدل يجب على منتجي البرامج المضادة للفايروسات أن تصدر تحديثاً كل ١٠ دقائق لإبقاء حواسيب مستخدميها محمية.

أغلب الهجمات الآن هي هجمات موزعة بدلًا من أن تكون من مصدر واحد: المهاجمون الآن يمكنهم استخدام آلاف الحواسيب في المهاجمة ضد حاسوب واحد أو شبكة. هذا الأسلوب في الهجوم يجعل أمر تحديد وحجب مصدر هجوم واحد مستحيلًا.

إرباك المستخدم: تزداد الطلبات على المستخدم باتخاذ قرارات أمنية صعبة فيما يتعلق بأنظمة الأجهزة الخاصة بهم، وأحياناً تدعم هذه الطلبات بمعلومات قليلة جدًا لا تمكن المستخدم ذو المعرفة البسيطة بالقرارات الأصح للاتخاذ. ومن هذه الأسئلة الشائعة على سبيل المثال "هل تسمح لهذا الموقع بتثبيت برامج إضافية؟" وغالباً ما يلجأ المستخدمين للسماح لتسهيل وتسريع عملية بحثهم دون أدنى معرفة بالبرمجيات المضافة وأهدافها.

أسئلة ونقاش(٢):

س١: ماهي العوائق التي تواجه أمن المعلومات؟

س٢: برأيك أي تلك العوائق تشكل الخطر الأكبر على أمن المعلومات؟

من المهاجمون؟

يقف خلف الهجمات على الحاسوب أنواع مختلفة من المهاجمين، وبشكل عام يقسم هؤلاء المهاجمين لفئات عدة، وتشمل تلك الفئات كلاً من: القراصنة، أطفال النصوص البرمجية، الجواسيس، الموظفون، مجرمو الإنترنت، وإرهابيو الإنترنت.

القراصنة (Hackers): على الرغم من أن "القراصنة (أو الهاكر)" مصطلح شائع الاستخدام، إلا أن خبراء الحاسوب وغيرهم دائمًا ما يناقشون تعريفه. فالبعض يستخدمون مصطلح القراصنة كمصطلح عام لأي شخص يحاول اقتحام أو خرق أمن الحاسوب والشبكات بشكل غير قانوني. وهنا يكون مصطلح "القراصنة" مرادفًا لمصطلح "المهاجمين". والبعض الآخر يستخدمون مصطلح "القراصنة" بشكل دقيق أكثر يقصدون به الشخص الذي يستخدم مهارات الحاسوب المتقدمة لمهاجمة الأنظمة لفضح العيوب الأمنية فقط. وعلى الرغم من أن اختراق نظام الحاسوب لشخص آخر هو أمر غير أخلاقي، إلا أن البعض منهم يعتقد بأن فعلته أخلاقية طالما أنه لم يسرق البيانات ولم يقم بالتخريب أو يفصح عن أي معلومات سرية. هؤلاء المتسللين من القراصنة (الذين يحبون تسمية أنفسهم بأصحاب القبعات البيضاء) يدّعون أن تحسين الأمن هو دافعهم ويكون ذلك عن طريق السعي لإيجاد الثغرات وإثبات الخلل في الأنظمة ليتم إصلاحها. من الممكن على كل حال استغلال الثغرات الأمنية بطرق تختلف عن مهاجمة نظام الحاسوب بغير إذن مالكه. وأن معظم المتخصصين في مجال أمن المعلومات لا يشيرون لأنفسهم كونهم قراصنة (أو هاكرز). إذًا بشكل عام، استخدام مصطلح القراصنة يستخدم بشكل أوسع وأكثر قبولًا للإشارة إلى مهاجمي الأنظمة بشكل غير أخلاقي.

أطفال النصوص البرمجية (Script Kiddies): أطفال النصوص البرمجية يهدفون لاقتحام نظام الحاسوب لإحداث الأضرار فقط. ففي حين أن القراصنة يتمتعون بمعرفة ومهارات حاسوبية عالية، إلى أن أطفال النصوص البرمجية ليس لديهم أدنى حد من المهارات. فهم يقومون بأداء أعمالهم عن طريق تنزيل واستخدام برمجيات قرصنة آلية مزود بواجهة سهلة الاستخدام لاقتحام أجهزة الحاسوب. ومع أن أطفال النصوص البرمجية ليس لديهم مهارات فنية للقرصنة، إلى أنهم في بعض الأحيان يصبحون أكثر خطورة من القراصنة. فهم غالبًا يتمتعون بأوقات فراغ طويلة جدًا والتي عادةً ما يقضونها في مهاجمة أنظمة الحاسوب. بالإضافة إلى أن نجاحهم في استخدام النصوص البرمجية لاقتحام الحاسوب يأجج رغبتهم في خلق المزيد من الأضرار. ولأنهم لا يتمتعون بمعرفة واسعة ولا يفهمون التكنولوجيا فهم عادةً ما يستهدفون أجهزة الحاسوب بشكل عشوائي مسببين أضرار لشريحة كبيرة من المستخدمين.

الجواسيس (Spies): جواسيس الحاسوب هم أشخاص مؤجرين لاقتحام الحاسوب وسرقة المعلومات. فهم لا يبحثون بشكل عشوائي عن أجهزة حاسوب غير مؤمنة ويقومون باختراقها كالقراصنة وأطفال النصوص البرمجية. على عكس ذلك فالجواسيس يتم توظيفهم لاستهداف حاسوب معين أو نظام يحوي معلومات حساسة. هدف الجواسيس هو اقتحام هذا الحاسوب أو النظام وسرقة المعلومات دون لفت الأنتباه لهم. والجواسيس كالقراصنة يتمتعون بقدرات حاسوبية ممتازة.

الموظفون (Employees): إحدى أكبر المخأوف التي تشكل خطراً على الشركات تكون من مصدر غير متوقع ألا وهم موظفيها. لماذا قد يخترق أحد الموظفين أنظمة حواسيب الشركة التي يعمل لديها؟ أحياناً قد يود الموظف إظهار الثغرات الأمنية ونقاط الضعف الموجودة في النظام للشركة. وفي أحيانًا أخرى يكون الموظفون مستائين من الشركة لسبب ما فينون الأنتقام منها عن طريق خرقهم لآمنةا. أما البعض الآخر فتكون غايتهم المال، حيث تتقدم شركة منافسة بعرض مبلغ مادي ضخم للموظف مقابل سرقته لمعلومات الشركة التي يعمل لديها. وفي بعض الأحيان يتم ابتزاز الموظف لكي يقوم بسرقة المعلومات من رب علمه. بالإضافة لعدم مبالاة الموظفين في بعض الأحيان حيث يقومون بترك أجهزة الحاسوب مفتوحة من غير تأمين فيتسبب ذلك بسرقة المعلومات.

مجرمو الإنترنت (Cybercriminals): هناك جيل جديد من مهاجمي الحاسوب المعروفين باسم مجرمي الإنترنت. يعمل مجرمي الإنترنت كشبكة متسعة ومترابطة من المهاجمين، سارقي الهوية، والمحتالين الماليين. مجرمي الإنترنت يشكلون خطراً كبيراً فلديهم دوافع كثيرة للغاية. فالخطورة عليهم أقل، والمردود المادي لهم أفضل، وهم عنادين أكثر من القراصنة فلديهم الإصرار لإكمال ما قد بدأوا به مهما واجهتهم عواقب أمنية عالية. يلتقي مجرمي الإنترنت في المنتديات والتجمعات التي لها أسماء مثل DarkMarket.org وtheftservices.com. والغرض من هذه الاجتماعات هو المعلومات التجارية وتنسيق الهجمات في جميع أنحاء العالم. بدلًا من مهاجمة نظام أجهزة الحاسوب لاستعراض المهارات التقنية كالقراصنة، مجرمي الإنترنت يهاجمون ولديهم هدف محددًا أكثر ويمكن تلخيصه في كلمة واحدة: المال. هذا الاختلاف يجعل المهاجمين الجدد أكثر خطورة، وهجماتهم تصبح أكثر تهديدًا. فهجماتهم تستهدف الشبكات المالية، والوصول غير المصرح به للمعلومات. كما تعرف سرقات المعلومات الشخصية عادةً بجرائم الإنترنت. وغالبًا ما تنقسم جرائم الإنترنت المالية إلى فئتين. الأولى تتم عن طريق استخدام بيانات بطاقات الائتمان المسروقة أو معلومات الحسابات المالية على الإنترنت كحسابات PayPal أو باستخدام أرقام الضمان الاجتماعي. في حال كشفت هذه المعلومات لأحد المجرمين فهو عادة ما يقوم بنشرها في مواقع مجرمي الإنترنت الخاصة ويعرضها للبيع على البقية. وعادة ما يتم الإعلان عن هذه المعلومات بطرق لا تختلف كثيراً عن طرق الإعلانات المعتادة. أما الفئة الأخرى فهي تشمل إرسال ملايين الرسائل التسويقية غير المرغوب بها للبريد الإلكتروني، كالتسويق للأدوية المزيفة، برامج مقرصنة، بضائع مقلدة أو مواد إباحية. ويقدر إجمالي أرباح مجرمي الإنترنت من تلك الرسائل غير المرغوب بها (أو ما تسمى Spam) بـ ٣٠ مليون دولار سنوياً. جرائم

الإنترنت سواءَ كانت بالتجارة بأرقام بطاقات الائتمان والمعلومات المالية الخاصة أو بالرسائل التسويقية غير المرغوب بها فهي قد سادت بشكل كبير ومخيف وفقًا لما يقولوه الكثير من الخبراء الأمنين.

إرهابيو الإنترنت (Cyberterrorist): يخشى العديد من الخبراء الأمنين أن هجمات الإرهابيين ستتحول لهجمات تستهدف البنية التحتية للحاسوب والشبكات وذلك لخلق حالة من الذعر لدى المواطنين. لدى المعروفين باسم إرهابيي الإنترنت دوافع قد تكون دينية أو للدفاع عن مبادئهم ومعتقداتهم. يسرد تقرير وزعه معهد لدراسات التقنيات الأمنية ثلاثة أهداف لهجوم إلكتروني:

- لتشويه المعلومات الإلكترونية (مثل مواقع ويب) ونشر المعلومات المضللة والدعاية.
- لحرمان مستخدمي الحاسوب والشبكات الشرعيين من الوصول للخدمة.
- لارتكاب عمليات اقتحام غير المصرح بها في النظم والشبكات التي قد تؤدي إلى انقطاع التيار الكهربائي عن البنية التحتية لأنظمة حساسة وبالتالي تتسبب في فساد البيانات أو حذفها.

ويعتبر الإرهابيون السيبرانية أحيانا المهاجمين الذين ينبغي أن يخشى منهم أكثر من غيرهم، لأنه يكاد يكون من المستحيل التنبؤ متى أو أين يحدث هجوم. وخلافا للقراصنة الذين التحقيق مستمر معهم في أنظمة أو إنشاء الهجمات، يمكن أن الإرهابيين السيبرانية يكونون غير نشطين لعدة سنوات ثم يضربون فجأة الشبكة بطريقة جديدة. ويمكن أن تشمل أهدافها مجموعة صغيرة من أجهزة الحاسوب أو الشبكات التي يمكن أن تؤثر على أكبر عدد من المستخدمين، مثل أجهزة الحاسوب التي تتحكم في شبكة الطاقة الكهربائية للدولة أو المنطقة. هجوم معزول يمكن أن يتسبب في انقطاع الكهرباء التي يمكن أن تؤثر على عشرات الملايين من الناس. أحيانًا يعتبر إرهابيي الإنترنت أكثر مجرمي الإنترنت الذي يجب علينا الخوف منهم. لأنه يكاد أن يكون من المستحيل التنبؤ متى أو أين يحدث هجوم. [٣]

حالة دراسية (١):

يتم توزيع المتدربين إلى مجموعات، ومن ثم تقوم كل مجموعة بالعمل على الحالة الدراسية التالية:

أحمد يعمل في مستشفى في مدينة الرياض، وفي يوم عمل شاق ازدادت فيه أعداد المرضى والمصابين في غرف الطوارئ وتعطل نظام المستشفى، أمر أحمد المختصين أن يجدوا السبب خلف تلك الأعطال، سواءَ كان انقطاع في الشبكة أو خلل في قاعدة البيانات.. إلخ. بعد مرور ساعات قليلة جاء عبدالله مدير مركز أمن المعلومات في المستشفى للأستاذ أحمد ليخبره أن ما حصل اليوم كان بسبب خلل في النظام نفسه. بعدها أخبر عبدالله الأستاذ أحمد بأنه سيقوم بالبحث عن سبب هذا العطل. أجرى الأستاذ عبدالله تحقيقًا نتج عنه تقريرًا مفصلًا مفاده أن العطل لم يكن بسبب خطأ اعتيادي في النظام بل كان هناك متسبب! وأفادت التحريات بعد التحقق من سجلات دخول النظام أن موظفًا

كان قد استقال منذ أشهر لأسباب مجهولة هو من كان متصلًا في ذلك الوقت. وهو من قام بتنفيذ بعض الأوامر التي كان من شأنها تعطيل النظام في ذلك الوقت.

برأيك ماهي الأسباب التي قادت ذاك الموظف المستقيل للقيام بهذا العمل؟ وعلى ضوء تلك الأسباب حدد أيًا من **أصناف المهاجمين** قد ينتمي إليه هذا الموظف؟

الهجمات وتقنيات الدفاع

الهجمات: على الرغم من أن هناك مجموعة واسعة ومتنوعة من الهجمات التي يمكن إطلاقها على جهاز الحاسوب أو الشبكة، دائمًا ما تستخدم نفس الخطوات الأساسية في معظم الهجمات. حماية أجهزة الحاسوب من خطوات الهجوم تلك تدعو إلى خمسة مبادئ أمنية أساسية.

خطوات الهجوم: هناك مجموعة متنوعة من الهجمات. أحد الأساليب لتصنيف هذه الهجمات يكون عن طريق الخمس خطوات التي تشكل الهجوم، وتلك الخطوات هي:

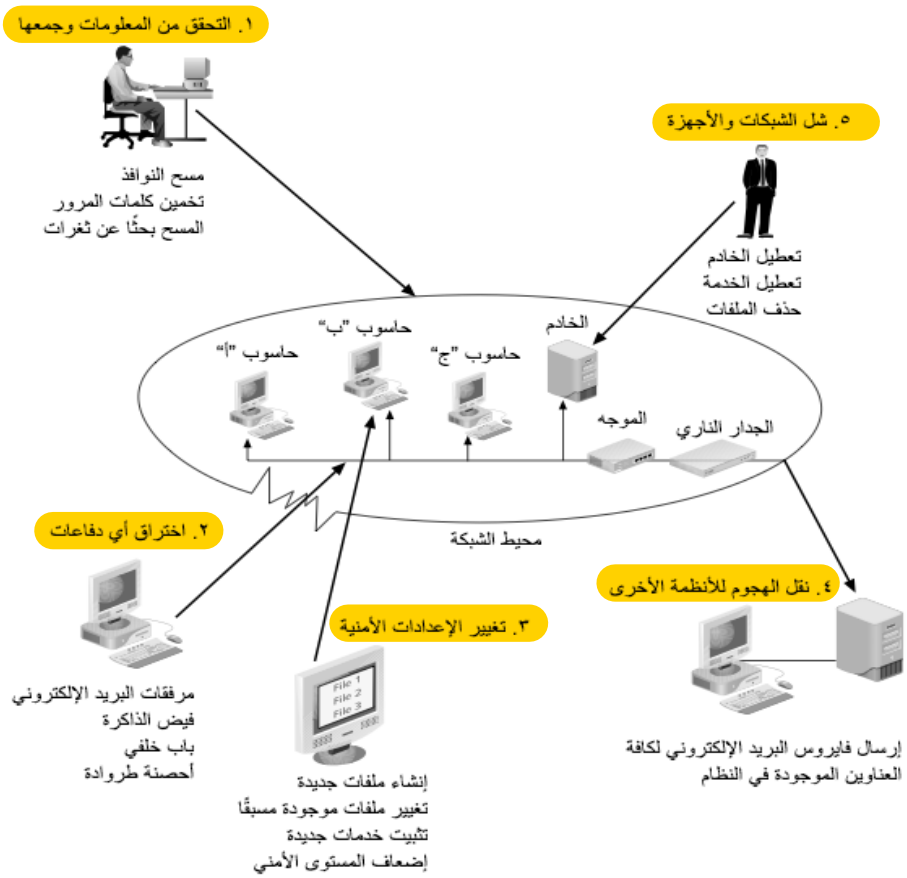
١-**التحقق من المعلومات وجمعها:** أول خطوة في الهجوم هي فحص النظام أو الشبكة للحصول على أي معلومات ممكن استخدامها لبدء الهجوم. هذا النوع من "الاستطلاع" ضروري لإيجاد المعلومات، كنوع الجهاز المستخدم، أو نوع إصدار البرمجيات أو نظم التشغيل، أو حتى المعلومات الشخصية عن المستخدمين، والتي يمكن استخدامها في الخطوة التالية. وتشمل الإجراءات التي تتم في هذه المرحلة الاتصال بالشبكة لتحديد ما إذا كان النظام يستجيب لمحاولات الاتصالات الخارجية، ومسح المنافذ لرؤية أي المنافذ قد تكون مفتوحة، وتخمين كلمات المرور.

٢-**اختراق أي دفاعات:** في حين تحدد النظام المراد الهجوم عليه، وتمت عملية جمع المعلومات المطلوبة عنه، الخطوة التالية هي إطلاق الهجوم لاختراق الدفاعات. وتأتي هذه الهجمات بأشكال متنوعة كالتلاعب بكلمات المرور أو كسرها.

٣-**تغيير الإعدادات الأمنية:** تغيير الإعدادات الأمنية هي الخطوة القادمة بعد اختراق النظام. هذه الخطوة تساعد المهاجمين على سهولة إعادة الدخول للنظام المخترق. تُعرف أيضاً باسم أدوت تصعيد الامتيازات، هناك العديد من البرامج التي تساعد على إنجاز هذه المهمة.

٤-**نقل الهجوم إلى الأنظمة الأخرى:** ريثما يتم اختراق النظام أو الشبكة، يستخدمهما المهاجم كقاعدة يبدأ منها هجماته على الأجهزة والشبكات الأخرى. باستخدام نفس الطرق والوسائل لجمع المعلومات عنها ومن ثم توجيه الهجمات عليها.

٥-**شل الشبكات والأجهزة:** إذا ما اختار المهاجم إلحاق الضرر بتخريب أو تدمير أنظمة الأجهزة أو الشبكات، قد يقوم بالحذف أو التعديل على الملفات، سرقة معلومات قيمة وخاصة، أو إطلاق الهجمات التي تعمل على تعطيل الجهاز أو الخدمة.



الشكل 4-١ : خطوات الهجوم

الدفاع ضد الهجمات: على الرغم من أن الدفاعات المتعددة قد تكون ضرورية للصمود ضد الهجمات، لكن تلك الدفاعات يجب أن تكون قائمة على خمسة مبادئ أمنية أساسية، ألا وهي حماية النظام من خلال كلٍ من: إنشاء الطبقات (Layering)، المحدودية (Limiting)، التنوع(Diversity)، الغموض(Obscurity)، والبساطة(Simplicity). سنتناول في هذا الموضوع كلًا من تلك المبادئ التي توفر الأساس لبناء نظام أمن على حدة.

إنشاء الطبقات (Layering): يجب أن ينشأ أمن المعلومات على شكل طبقات، فطريقة دفاع واحدة قد تكون سهلة بتحايل أحد المهاجمين. لذلك يجب أن ننشئ نظام أمني يتكون من طبقات، مما يجعل وجود مهاجم لديه القدرة والأدوات لخرق جميع تلك الطبقات أمر غير مرجح. لذا فتقنية الطبقات مفيدة جدًا لمقاومة شريحة كبيرة من المهاجمين فالأمن الطبقي يوفر أكبر قدر من الحماية الشاملة.

المحدودية (Limiting): بطبيعة الحال، عند الحد من الوصول للمعلومات فإن احتمالية الخطر الذي يهددها يصبح أقل. يجب أن يسمح للأشخاص المعنيين فقط بالوصول للمعلومات. بالإضافة إلى أن الوصول نفسه يجب أن يُحد على المعلومات والبيانات التي يحتاجها فقط ذلك المستخدم. على سبيل المثال، الوصول لقاعدة بيانات الموارد البشرية في منظمة أو شركة معينة يجب أن يقتصر على الموظفين المختصين والمعتمدين، ومديري الإدارات، ونواب الرئيس فقط. كمثال آخر، الموظف التقني مكلف بإجراء نسخة احتياطية يومياً لقاعدة البيانات، لكنه ليس مخول لعرض تلك البيانات كالرواتب وغيرها لأنها ليست من شأن عمله.

بعض الطرق للحد من وصول هي القائمة على التكنولوجيا (مثل تعيين أذونات الملف بحيث يمكن للمستخدم القراءة فقط ولكن ليس التعديل على ملف)، في حين أن البعض الآخر إجرائي (حظر موظف من إزالة وثيقة حساسة من المبنى). والمفتاح هو أن الوصول يجب أن تقتصر على الحد الأدنى.

التنوع (Diversity): التنوع يرتبط ارتباطًا وثيقًا بالطبقات، بما أنه من المهم لحماية البيانات أن يكون النظام الأمني متشكلًا من طبقات، كذلك يجب أن تكون تلك الطبقات مختلفة أو متنوعة، حيث إذا تمكن المهاجم من اختراق طبقة واحدة، لن يستطيع اختراق الطبقات التي تليها بنفس التقنية. باستخدام طبقات متنوعة من الدفاع يعني أن كسر طبقة الأمان واحدة لا تخترق النظام برمته. ويمكن تحقيق التنوع بطرق عدة. على سبيل المثال، بعض المنظمات تستخدم المنتجات الأمنية التي تقدمها مختلف البائعين. على سبيل المثال، بعض المنظمات تستخدم المنتجات الأمنية التي يقدمها منتجين مختلفين. فالمهاجم الذي يستطيع كسر الحواجز الأمنية للعلامة التجارية -أ-سيصعب عليه كسر الحواجز الأمنية للعلامات التجارية -أ- و -ب- فهما على الأغلب يستخدمان تقنيات مختلفة كليا.

الغموض (Obscurity): يجب علينا ألا نفصح عن أنواع أجهزة الحاسوب التي نستخدمها، أنظمة التشغيل، البرمجيات، أو نوع الاتصال بالشبكة. فيكون من السهل على المهاجم الذي يعرف هذا النوع من المعلومات أن يحدد نقاط الضعف في النظام الأمني للمستخدم وثغراته وبالتالي يسهل الهجوم عليه. وبالمقابل إن لم تكن تلك المعلومات مكشوفة فإن المهاجم سيستغرق وقتًا وجهدًا أكبر في محاولة إيجادها، وفي حالات عدة كثيراً ما ينصرف المهاجم لمحاولة إيجاد جهاز حاسوب أو شبكة أخرى بنظام أمني أضعف. لذلك التكتم عن المعلومات والغموض بالنظام الأمني وسيلة مهمة جدًا

البساطة (Simplicity): لأن الهجمات يمكن أن تأتي من مجموعة متنوعة من المصادر وبطرق عديدة، فأمن المعلومات بطبيعته أمراً معقدًا. والأمور بشكلٍ عام يزداد فهمها صعوبة كلما ازدادت تعقيداتها. والأنظمة المعقدة تعطي الكثير من الفرص لتجري بها الأمور على غير ما يرام. باختصار، يمكن للأنظمة المعقدة أن تصبح حليفة للمهاجم أو تؤدي ما هو في صالحه. وعادة ماتكون أنظمة أمن المعلومات المعقدة في الحاسوب والشبكات صعبة في الفهم والاستكشاف وصعبة في اكتساب ثقة المستخدم. لذلك يجب أن تكون أنظمة أمن المعلومات بسيطة قدر الإمكان لمستخدميها ومن يعمل عليها من الداخل. لكن حين تكون أنظمة أمن المعلومات بسيطة، قد تكون في الوقت نفسه سهلة للاختراق

من المهاجمين. ولكي يكون النظام بسيطًا من الداخل ومعقدًا من الخارج فهذا أمر من الصعب تحقيقه في الغالب ولكن الفائدة المرجوة منه ضخمة جدًا.

حالة دراسية (٢):

يتم توزيع المتدربين إلى مجموعات، ومن ثم تقوم كل مجموعة بالعمل على الحالة الدراسية التالية:

في شركة (أ. أ. م) كان هنالك ثغرات أمنية في النظام الخاص بإدارة الشركة. مما أدى الشركة لاتخاذ قرار تعيين مدير جديد لمركز أمن المعلومات. أحمد، المدير الجديد يحاول جاهدًا السعي والبحث عن تلك الثغرات وسدها. حينها وجد أن المدير السابق كان قد اشترط استخدام كلمة مرور قوية للدخول إلى النظام. علم أحمد آن ذاك أن كلمة المرور القوية وحدها لم تكن كافية لحفظ المستوى الأمني للنظام. فكان عليه أن يتخذ إجراءات ليزيد من أمن المعلومات في النظام.

اقترح أنت ومجموعة من زملائك إجراءات أمنية تساعد أحمد لرفع مستوى الأمن آخذين **تقنيات الدفاع** بعين الاعتبار.

المخاطر التي تهدد الأنظمة

إحدى أهم الصعوبات التي تواجه تأمين أنظمة الأجهزة الشخصية هي أن الشخص لديه معظم الصلاحيات-وفي أغلب الحالات كل الصلاحيات- للتحكم في النظام. فحين يكون المستخدم مدرك ويعي أهمية الأمن المعلوماتي قد يتخذ الإجراءات اللازمة للتأكد من أن معلوماته الرقمية في مأمن، لكن عندما يعتقد المستخدم أن تأمين المعلومات الرقمية هو شيء مكلف ومزعج أو لم يكن على دراية بالإجراءات التي يجب اتخاذها للحفاظ على أمن وسلامة النظام، سيكون النظام عرضة للهجمات حينها. مما يعني أن المستخدم هو العامل الأساسي والأكثر تأثيراً على المستوى الأمني لأنظمة الأجهزة الشخصية.

أثبتت الدراسات أن معظم المستخدمين لا يقومون بالإجراءات الأمنية الكافية للحفاظ على سلامة أنظمة حواسيبهم. وفقًا لدراسات شركة Secunia وهي إحدى الشركات المسوقة لمنتجات أمنية رقمية أن أكثر من ٩٥٪ من الأجهزة الشخصية المتصلة بالإنترنت تحوي على الأقل تطبيقًا واحدًا غير أمن. وأن ثلثي هذه الأجهزة تحوي على ستة تطبيقات غير آمنة إضافية أو أكثر، وأن ٤٢٪ منهم قد نصبوا إحدى عشر تطبيقًا غير أمن على الأقل. دائمًا ما يعرف بأن الأجهزة الشخصية ضعيفة أمنيًا، وذلك يعود بشكل كبير لعدم مبالاة المستخدمين أو جهلهم بأهمية تفعيل أمن المعلومات والحفاظ عليه. مما جعل من الحواسيب الشخصية هدفًا رئيسيًا يقصده المهاجمون. [٤]

ويتناول هذا الموضوع التهديدات والمخاطر التي تواجه أنظمة الحاسب اليوم. حيث أننا سنتعرف على الهجمات التي تصيب برمجيات الأنظمة.

الهجمات على برمجيات الأنظمة: البرمجيات الخبيثة(Malware) هي برمجيات تدخل لنظام الحاسب بدون علم المستخدم أو إذنه. البرمجيات الخبيثة(Malware) هي مصطلح عام يشير إلى مجموعة واسعة من البرمجيات المدمرة أو المزعجة. وهنالك طريقة واحدة لتصنيف البرمجيات الخبيثة وهي عن طريق هدفها الأساسي، فلدينا ثلاثة أهداف أساسية لتلك البرمجيات ألا وهي ألحاق الضرر بالنظام، إخفاء النشاطات الخبيثة من برمجيات أخرى أو لتحقيق الأرباح من النشاطات التي يقوم بها.

البرمجيات الخبيثة ضارة: نوعين من البرمجيات الخبيثة هدفها الأساسي هو إلحاق الضرر بنظام الحاسب الآلي وهما الفيروسات والديدان. وهي أيضاً من أقدم أنواع البرمجيات الخبيثة للتأثير على أنظمة الحاسوب الشخصية.

الفيروسات: بدأ ظهور الفيروسات في السبعينات من القرن الميلادي الماضي، وكانت بداياته بسيطة جدًا، ولم تكن على مستوى الخطورة التدميرية الحاصلة في عصرنا الحاضر. تعتبر الفيروسات هي أكبر فئات البرامج الضارة من ناحية عدد الأشكال المعروفة، ومن ناحية أثرها على بيئة الحاسب الآلي. ولذلك فإن كلمة "فيروسات" تميل لأن تكون مرادفًا في ذهن العامة لكل أنواع البرامج غير السوية أو الشرعية.

وسبب تسمية فيروسات الحاسب الآلي بهذا الاسم هو تشابهها الكبير مع الفيروسات التي تصيب الإنسان .فإن فيروس الحاسب الآلي يبدأ بالعدوى، أي انتقالها من جهاز إلى جهاز آخر، ثم مرحلة الحضانة أو الركود، ثم بعد ذلك يبدأ بالعمل والتكاثر (نسخ نفسه)، ثم تظهر أعراضه، ثم يظهر بعد ذلك الخراب والدمار الذي يسببه، سواءَ كان كبيرًا أو صغيرًا.

فيروس الحاسب الآلي هو برنامج يعد لينسخ نفسه وينتشر ذاتيًا دون علم وتعاون مع المالك أو المستخدم للجهاز ولم يتم التوصل بعد لتعريف موحد للفيروسات متفق عليه من كافة الباحثين. والتعريف العام هو أن الفيروس برنامج يقوم بتعديل البرامج الأخرى لكي تحتوي على نسخة معدلة من نفسها. ورغم أن هذا التعريف يصف جل الفيروسات، وأن كثيرًا من الباحثين مازالوا يصرون على استخدامه، إلا أنه يقتصر على البرامج التي تقحم نفسها بنفسها في البرامج الأخرى فقط. وهو بذلك يهمل كثيرًا من الفيروسات التي تقحم نفسها في الملفات التي ليست برامج بطبيعتها، كالوثائق مثلًا. وعليه يمكن تعريف الفيروسات بصورة عامة بأنها البرامج التي تقوم بإقحام نفسها بنفسها في مادة أخرى قد تكون برنامجًا أو قرصًا أو وثيقة أو رسالة بريد إلكتروني أو نظام حاسب آلي أو أي صيغة معلوماتية. ولدى كثير من الناس انطباع بأن أي شيء لا يسير على مايرام في الحاسب الآلي يكون: سببه فيروس. ابتداء من فشل القرص الصلب وحتى أخطاء الاستخدام. والحقيقة أنه ليس بالضرورة أن ينتج عن الفيروس ضررًا ما. فقد يتم بناء الفيروسات لكي تكون وسيلة نقش إلكتروني لعلامة تخلد أسم مصممه في العالم. وفي بعض الأحيان يتم عرض اسم مصمم الفيروس في أي مناسبة مع عنوانه ورقم هاتفه، واسم الشركة التي ينتمي إليها، من أجل الشهرة فقط بدون إلحاق أي ضرر. [٤]

خصائص الفيروسات: لا تحدث فيروسات الحاسب الآلي أو تنتج طبيعية، وإنما هي برامج يكتبها مبرمجون. وكذلك فهي لا تظهر من خلال بعض التطورات الإلكترونية فقط، وإنما تكتب بصورة متعمدة عن طريق أناس متخصصين. وتبقى الفيروسات مختبئة داخل البرنامج المصاب؛ لتبدأ بالعمل والتكاثر والأنتشار. أي أنها لا تبدأ بعملها حتى تتم استثارتها من قبل المستخدم. هناك عدة خصائص لفيروسات الحاسب الآلي تميزها عن غيرها من البرامج الضارة، وتساعدها على الأنتشار وإصابة أجهزة الحاسب الآلي الأخرى دون علم مستخدميها، وهي:

التخفي: ويعني القدرة على الارتباط ببرامج أو ملفات أخرى تبدو سليمة ومألوفة للمستخدم، بحيث يلحق الفيروس نفسه بالملف المصاب خفية ليصبح جزءًا منه. ومن أشهر طرق تخفي الفيروسات ما يلي:

- التخفي في مرفقات البريد الإلكتروني.
- التخفي في الملفات التي يتم تحميلها من مواقع الإنترنت، خاصة تلك التي تقوم بتشغيل ملفات الصوتيات والفيديو وتبادلها.
- التخفي وراء الروابط والأوامر الموجودة في صفحات الإنترنت والبريد الإلكتروني.
- التخفي وراء روابط وملفات الإعلانات والبريد الدعائي.
- التخفي مع البرامج المنسوخة بشكل غير قانوني.

التضاعف: ويعني ذلك أن ينسخ الفيروس نفسه عدة نسخ تصل في بعض الأحيان إلى ملايين النسخ، بمعنى أنه يتكاثر ليصيب أكبر قدر ممكن من الملفات والبرامج داخل نفس جهاز الحاسب الآلي أو داخل الأجهزة الأخرى المرتبطة به. وتبدأ عملية التضاعف عندما يتم تحميل برنامج الفيروس إلى ذاكرة الحاسب الآلي ويقوم المعالج المركزي بتنفيذه.

الأنتشار: ويعني أنتقال الفيروس من جهاز إلى آخر عبر شبكات الحاسب الآلي أو وسائط التخزين المختلفة. ومعنى ذلك أن لدى الفيروس القدرة على نقل نفسه عند استثارته، كتشغيل أمر النسخ، أو عند اكتشاف اتصال الحاسب الآلي المصاب بحاسب آلي آخر. ومن أشهر طرق أنتشار الفيروسات مايلي:

- تحميل ملفات مصابة من مواقع شبكة الإنترنت أو زيارة مواقع تقوم بنشر الفيروسات بشكل تلقائي.
- فتح مرفقات بريد إلكتروني مصابة.
- أن يقوم المستخدم بنسخ ملفات مصابة دون علمه، وتخزينها على وسائط تخزين خارجية تنتشر معها، أو يقوم بإرسالها عبر الشبكة "كاستخدام المجلدات المشتركة"، فتنتشر عبرها.
- أن يقوم الفيروس بنسخ نفسه، ثم إرفاق تلك النسخة مع أي ملف آخر عند استثارته.

أنواع الفيروسات: ثمة أنواع كثيرة جدًا من الفيروسات ولكن ما يهمنا هنا هو الأنواع "أو المجموعات" الرئيسة الأكثر أنتشاراً، التي يشكل كل نوع منها مجموعة من الفيروسات لها نفس البنية وتقوم بمهام متشابهة إلى حد كبير، وهذه الأنواع هي:

فيروسات قطاع بدء التشغيل (الأقلاع): يوجد لكل نظام تشغيل قطاع في قرص التخزين الصلب، مخصص لبدء عملية التشغيل (الأقلاع). وعادة ما يكون هذا القطاع هو القطاع الأول (Track ٠)، وعند وجود أي خلل فيه فإن الحاسب الآلي لن يستطيع البدء بالتشغيل. وفيروسات قطاع بدء التشغيل (viruses boot sector) هي الفيروسات التي تصيب قطاع بدء التشغيل في قرص التخزين الصلب. وتكمن خطورة هذا النوع من الفيروسات في إصابتها لمكان مهم جدًا يتم من خلاله توجيه

الجهاز لتنفيذ البرامج التي يتم من خلالها استكمال تجهيز جهاز الحاسب الآلي للعمل. وبدلًا من ذلك يقوم الفيروس بتوجيه الحاسب الآلي لتنفيذ الكود الخاص بالفيروس، وبالتالي يفشل الجهاز في عملية الأقلاع ولا يمكنه العمل.

فيروسات الملفات (File infecting viruses)**:** هي الفيروسات التي تصيب الملفات بشتى أنواعها فيمكن أن تصيب ملفات نظام التشغيل كملف (command.com) في نظام الويندوز أو أي ملف آخر. وعادة ما ينتج عن هذه الفيروسات زيادة في أحجام الملفات.

الفيروسات الجزئية الكبيرة (viruses macro)**:** تستخدم فيروسات الجزئية الكبيرة البرمجة الجزئية الخاصة بتطبيق معين، مثل معالج الكلمات، للبدء بنشاطها. وتضرب هذه النوعية من الفيروسات ملفات البيانات (مثل ملفات برامج وورد واكسل واكسس)، تظل ساكنة أو مقيمة في التطبيق نفسه عن طريق إصابة حقل التهيئة الخاص به. وعلى الرغم من أن الفيروسات الجزئية الكبيرة تصيب ملفات البيانات، إلى أنها عموماً لا تعد من فيروسات الملفات. والسبب في ذلك أن فيروسات الملفات قد تصيب البرامج وملفات البيانات، بينما لا تصيب فيروسات الجزئية الكبيرة إلا ملفات البيانات فقط.

فيروسات البريد الإلكتروني: هي الفيروسات التي تنتقل بواسطة البريد الإلكتروني. فبإضافة بعض الوظائف (عن طريق الفيروس) لبرنامج مقدم خدمة البريد الإلكتروني القياسي (مثل أوتلوك (Outlook)) أصبح للفيروسات إمكانية الأنتشار عبر العالم خلال ساعات فقط، بدلًا من شهور. ومن أشهر فيروسات البريد الإلكتروني ماليسا (Melissa). وماليسا ليس أول فيروس بريد إلكتروني، بل أول فيروس بريد إلكتروني انتشر بنجاح بصورة شرسة هو فيروس كيرستما اكسك (Christma exec). ولكن فيروس ماليسا هو أول فيروسات البريد الإلكتروني السريعة التكاثر والأنتشار، وكذلك الأول الذي صار معروفًا لشريحة واسعة من عامة الناس. ويعتبر ماليسا من الفيروسات الجزئية الكبيرة، فبالإضافة إلى أنه فيروس بريد إلكتروني، إلا أنه يمكن أن يرسل نفسه ذاتيا في شكل وثيقة مصابة بالفيروس.

ديدان الحاسب الآلي: دودة الحاسب الآلي (Computer Worm) هي عبارة عن برنامج مستقل بذاته، وله ملف خاص به. فالدودة تعتبر برنامجاً تطبيقياً متكاملاً يمكن أن يعمل لوحده، ولا يحتاج لأن يضيف نفسه لملف آخر، كما هي الحال في الفيروسات. ويمكن للدودة أيضاً أن تعمل بمفردها وتحمّل نفسها في ذاكرة الحاسب الآلي. وتبدأ بالعمل بشكل آلي.

ومن الفوارق الأصلية، هي أن الديدان تستخدم الشبكات وروابط الاتصالات لكي تنتشر، وهي خلافاً للفيروسات لا تلتحم مباشره بالملفات القابلة للتنفيذ. وتصيب الديدان أجهزة الحاسب الآلي المرتبطة بشبكات الحاسب الآلي المصابة دون أن تدخّل المستخدم أو قيامه باستثارتها كفتح ملف معين أو تشغيل برنامج، كما هي الحال في الفيروسات. فقد تنتقل إلى الجهاز بمجرد تصفح بعض مواقع الإنترنت، أو بمجرد فتح بريد إلكتروني (إذا لم يكن الجهاز محمياً ببرنامج حماية محدّث). تستخدم كلمتا دودة وفيروس بالترادف، حيث كان يعتقد أن الفرق الفني بينهما غير ضروري لمعظم المستخدمين. وأصل مصطلح برنامج "دودة" يتواءم فنياً مع طرق أنتشار الديدان في الوقت الحاضر. فنجد أن برنامج الدودة يتكون من أجزاء (رأس وجسم كما في الدودة الطبيعية) تعمل في أجهزة حاسب متفرقة، تتواصل فيما بينهما عبر الشبكة، فيمكن أن تجد رأس البرنامج في جهاز، وذيله في جهاز آخر بعيداً.

لم تضع دودة الإنترنت يونيكس موريس (UNIX/Morris) الإنترنت عامة والبريد الإلكتروني خاصة في حالة شبه توقف فقط، بل لقد استطاعت تشغيل الإصدارات الحديثة لنظام يونيكس وترويجها في منصات أقراص صلبة محددة. وخلال هذه العاصفة البريدية، تأثرت الكثير من الأجهزة بالفصل بين البريد الإلكتروني وقائمة توزيع البريد، وتم فقد بعض رسائل البريد نهائياً. ومعظم البريد تم تأخيره، وفي بعض الأحوال تم توجيهه نحو طرق أقل كفاءة؛ مما تسبب في فقده أو تأخيره. وفي الحالات الأخرى التي تأثرت في الأجهزة الرئيسية بالمشكلة كانت ببساطة أبطأ في نقل البريد. وكذلك توقفت في بعض الأجهزة الأخرى برامج نقل البريد، وخرجت من الخدمة مع تأخير ملحوظ في إرسال البريد. ومن المفارقة في هذه العاصفة، أن البريد الإلكتروني يشكل الوسيلة الأساسية التي يحاول مختلف الأطراف التعامل مع المشكلة من خلاله، وكانوا يحاولون استخدامه للتواصل فيما بينهم؛ مما زاد الأمر سوءاً. وعند دخول رأس الدودة إلى النظام، يتم تغذيته بالبرنامج الرئيسي، (الجسم)، من الموقع الذي تمت إصابته مسبقاً. وتم استخدام برنامجين (رأس وجسم)، أحدهما في الموقع المصاب، والآخر في الموقع المستضيف (الجديد). وإذا لم يستطع أي من البرنامجين العمل، تزيل الدودة نفسها بنفسها، وإن كان المستضيف الجديد غير مناسب، فإن الدودة ستبحث عن مستضيفين آخرين وتوصيلات أخرى. [١]

طرق أنتشار الديدان: من أهم خصائص الديدان هي قدرتها على الأنتشار والتكاثر عبر الاتصال بشبكات الحاسب الآلي. ومن أهم الطرق التي تنتشر بها الديدان ما يلي:

- مرفقات البريد الإلكتروني.
- التحميل التلقائي عند زيارة بعض مواقع الإنترنت التي من خلالها تنتشر الديدان، أو عند استخدام أحد الارتباطات داخل البريد الإلكتروني.
- التسلل عبر الثغرات الأمنية في أنظمة التشغيل أو برامج الحماية.

أضرار الديدان: لا تقل أضرار الديدان عن الفيروسات من ناحية التلف، أو فقد البيانات التي تسببها. ومن أهم أضرار الديدان ما يلي:

- تتيح للمهاجم أن يستخدم الحاسب الآلي المصاب لمهاجمة أجهزة أخرى، أو مواقع الإنترنت، أو إرسال بريد إلكتروني، أو تحميل برامج ضارة إليه.
- يمكن من خلالها فتح باب خلفي (Back Door) في الجهاز المصاب، حيث يمكن التحكم به من خلال ذلك الباب.
- يمكن للديدان أن تنسخ نفسها، وترسل نسخة إلى كل بريد إلكتروني في عناوين البريد المخزنة في جهاز الحاسب الآلي المصاب.

البرمجيات الخبيثة لإخفاء البرامج الضارة: هناك أنواع عدة من البرمجيات الخبيثة هدفها الأساسي هو إخفاء ظهورها ونشاطاتها عن المستخدم، على عكس البرمجيات الخبيثة الضارة التي تهدف لتخريب وتدمير الأنظمة مثل الفيروسات والديدان. برمجيات الإخفاء تشمل أحصنة طروادة، وتقنية التحكم الخفي في الحاسوب (RootKit)، والقنابل المنطقية، وتصعيد الامتيازات.

أحصنة طروادة (Trojan Horses): وفقا للأسطورة القديمة، فاز الإغريق بحرب طروادة عن طريق إخفاء الجنود في حصان خشبي كبير مجوف قدم كهدية لمدينة طروادة. فحينما أُدخل الحصان إلى المدينة المحصنة، زحف الجنود من الحصان أثناء الليل وهاجموا المدافعين المطمئنين. حصان طروادة الحاسوبي هو برنامج قد أعلن بأنه يقوم بأداء نشاط معين لكنه في الحقيقة يقوم بنشاط آخر، وفي بعض الأحيان يقوم بأداء كلًا من النشاطين المعلن عنه والخبيث. على سبيل المثال، قد يقوم مستخدم بتنزيل برنامج قد أعلن بأنه تقويم مجاني للتاريخ الهجري. لكن عندما تم تشغيله فإنه بالإضافة لتثبيت التقويم الهجري قام بمسح الجهاز باحثًا عن أرقام بطاقات الائتمان وكلمات المرور، فيرتبط عن طريق الشبكة بنظام عن بعد ليرسل له تلك المعلومات. إذاً فبرامج حصان طروادة هي برامج قابلة للتنفيذ وتحوي عادة على أوامر برمجية خبيثة خفية.

تقنية التحكم الخفي في الحاسوب (RootKit): تقنية التحكم الخفي في الحاسوب (RootKit) هي مجموعة من الأدوات البرمجية التي يستخدمها المهاجم لاختراق نظام جهاز الحاسوب، أو للحصول على امتيازات خاصة لأداء وظائف غير مصرح بها، ومن ثم إخفاء كل آثار وجودها. تعمل تقنية التحكم الخفي في الحاسوب عن طريق استبدال أوامر نظام التشغيل بإصدار محدث من الأوامر والذي صمم خصيصًا لتجاهل النشاطات الخبيثة وبالتالي عدم القدرة على كشفها. على سبيل المثال، مضاد الفيروسات في جهاز الحاسوب مكلف بفحص ملفات في مجلدات معينة، وهذا التكليف عادة ما يكون بأمر من نظام التشغيل، هنا تعمل تقنية التحكم الخفي في الحاسوب على تحديث تلك الأوامر بحيث تجعل مضاد الفيروسات يتجاهل المجلدات التي تحوي ملفات خبيثة. فمضاد الفيروسات يأخذ بأوامر نظام التشغيل على أنها أوامر تعزز أمن الحاسوب فلا يستطيع التفرقة بين

الأوامر المعززة لأمن الحاسوب والعكس. وهذا ما قد نتج عنه مشكلة رئيسة، وهي أن المستخدمين لم يعودوا يثقوا بأجهزتهم وأنظمتها. أما عن تحديد واكتشاف وجود تقنية التحكم الخفي في الحاسوب فهو أمر صعب. مع أن هنالك برامج متاحة للتحقق من وجود تلك التقنية في الحاسوب، لكن ومع ذلك بعض من البرامج التي تستخدم تلك التقنية تستطيع إخفاء نفسها عن البرامج التي تسعى لكشفها أيضاً.

القنابل المنطقية (Logical Bombs): القنبلة المنطقية هي برنامج أو جزء من برنامج يظل خامدًا حتى يتم تشغيله بواسطة حدث منطقي محدد، كوصول التقويم في جهاز الحاسوب لتاريخ محدد مسبقًا، أو عند انخفاض المستوى الوظيفي لموظف ما تحت رتبة معينة. في حين تم تشغيل البرنامج فسيقوم بعدة نشاطات خبيثة. على سبيل المثال، القنبلة المنطقية قد تكون مزروعة في نظام الرواتب للشركة من قبل موظف، ويكون قد صممها بحيث تبدأ نشاطاتها بعد ثلاثة أشهر من إزالة اسمه من القائمة (وذلك يعني أنه استقال أو قامت الشركة بطرده).

تصعيد الامتيازات (Privilege Escalation): أنظمة التشغيل والعديد من التطبيقات لديها القدرة على تقييد امتيازات المستخدم في الوصول إلى مهام محددة. وتصعيد الامتيازات هو عادة ما يكون استغلال من المهاجم لثغرة ما في النظام ومن ثم الحصول على صلاحيات وامتيازات ليست من حقه. وهنالك نوعان من تصعيد الامتيازات، أما الأول فهو يختص بمستخدم يتمتع بامتيازات قليلة فيستغل ثغرة النظام ويقوم بتصعيد تلك الامتيازات للحصول على الخصائص والصلاحيات التي يتمتع بها المستخدمين الذين يتمتعون برتب أعلى. والثاني هو أن يحاول المستخدم الذي لديه امتيازات محدودة تصعيد امتيازاته للوصول لحساب مستخدم آخر محدود الامتيازات أيضاً لكن امتيازاته مختلفة عن امتيازات الأول فيود الجمع بينهما.

برمجيات خبيثة من أجل الربح: وهناك فئتان من البرمجيات الخبيثة هي التي تهدف إلى تحقيق الربح للمهاجمين. وتشمل الرسائل غير المرغوب بها، وبرامج التجسس.

الرسائل غير المرغوب بها (Spam): تستمر أعداد الرسائل المزعجة وغير المرغوب بها بالتصاعد في عالم الإنترنت وخاصة البريد الإلكتروني، فالدراسات تشير أن واحدًا من كل اثنا عشر بريدًا إلكترونيا هو بريد إعلاني غير مرغوب به. إن الرسائل غير المرغوب بها تخفض الإنتاجية بشكل كبير، فهنالك ١١% من العاملين يتلقون أكثر من ٥٠ رسالة غير مرغوب بها في اليوم، ويقضون نصف ساعة على الأقل لحذفها. والدراسات تشير أن الرسائل غير المرغوب بها تكلف المنظمات الأمريكية ٨٧٤$ لكل موظف في السنة وتلك التكلفة ناجمة عن خفض الإنتاجية التي سببتها تلك الرسائل. ويعود سبب تضخم أعداد تلك الرسائل للأرباح المرتفعة التي يجنيها المرسلون، فإرسال مليون بريد مخادع للإعلان

عن منتجات مغشوشة على سبيل المثال لن يكلف المرسل الشيء الكثير لكنه بالمقابل سيعود عليه بأرباح هائلة حتى وإن كانت نسبة المستجيبين له ضئيلة.

برامج التجسس (Spyware): برنامج التجسس ليس بفيروس ولكن فعله أقوى وأخطر من الفيروسات والديدان وغيرها من البرمجيات الخبيثة سواء كانت ملحقة بالضرر أو لإخفائه. فبالرغم من عدم تسببه في تلف البيانات، إلا أنه يفعل فعله من وراء الكواليس بكل هدوء، ودون علم المستخدم، ويقوم بنقل المعلومات لمالكه. وبرنامج التجسس هو عبارة عن خدعة ماكرة، مثله في ذلك مثل الفيروس، ولكنه عموماً أقل شهرة.

وحالياً تقحم برامج التجسس في مئات من برامج المشاركة المعروفة، بل وصل الحد لأنتاج البرامج التجارية من هذه الفئة. وحسب التقديرات فإن نحو ١٥٪ من أجهزة الحاسب المحمولة و٢١٪ من أجهزة الحاسب المكتبية مصابة ببرامج تجسس. ويوضح تقرير معهد أمن الحاسب الآلي أن ١٢٪ من عينة الدراسة تعرضوا لسرقة كلمات المرور، وأن ٩٪ تعرضوا لاحتيال مالي، وأن ٨٪ تعرضوا لاستغلال الشبكات اللاسلكية.

وعلى الرغم من الجدل الذي يكتنف تعريف برنامج التجسس الدقيق، إلا أنه في النهاية كائن (إلكتروني) يتجسس عليك. ونتيجة لذلك يتركز الجانب المهم من موضوع برنامج التجسس عادةً حول مسألة الخصوصية. تعرف برامج التجسس بأنها برامج تقوم سراً بالحصول على معلومات عن المستخدم عن طريق الربط بالإنترنت، وخاصة بدعاوى دعائية وإعلانية. وعادة ما يتم تضمين برامج التجسس في شكل مكونات مجانية خفية، أو برامج مشاركة يمكن تنزيلها من شبكة الإنترنت. وبمجرد تثبيت برنامج التجسس يبدأ بمراقبة حركة المستخدم، وينقل المعلومات من وراء الكواليس لجهة أخرى.

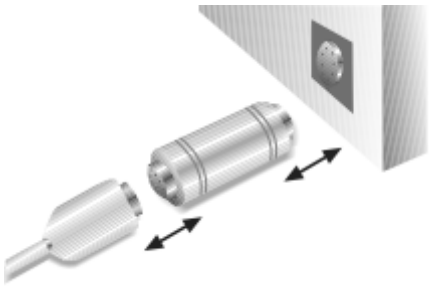
يستخدم المهاجمون أدوات عدة للتجسس، لكن أشهر أداتان هما:

برمجيات الإعلانات (Adware): وهي برمجيات من شأنها أن توفر محتوى الإعلان بطريقة غير متوقعة وغير مرغوب فيه من قبل المستخدم. وعادة ما تعرض تلك البرمجيات لافتات الإعلانات، والإعلانات المنبثقة، أو تفتح نوافذ متصفح ويب جديدة في حين اتصال المستخدم بالإنترنت. وغالباً ما يقأوم المستخدمين برمجيات الإعلانات للأسباب التالية:

- برمجيات الإعلانات قد تعرض محتوى غير مرغوب فيه، مثل مواقع القمار أو المواد الإباحية.
- تكرار الإعلانات المنبثقة قد يعيق إنتاجية المستخدم.
- الإعلانات المنبثقة يمكن لها أن تبطئ من أداء الجهاز وقد تتسبب بخسارة أو تلف البيانات أيضاً.
- يمكن للإعلانات غير المرغوب فيها أن تكون مصدراً للإزعاج.

يمكن أن تشكل برمجيات الإعلانات خطراً أمنياً أيضاً. فالعديد من تلك البرمجيات تعمل على تتبع نشاطات المستخدم. فتقوم بمراقبة وتعقب جميع نشاطات المستخدم على الإنترنت ومن ثم تقوم بإرسال سجل من هذه النشاطات لطرف ثالث دون إذن المستخدم أو حتى معرفته. على سبيل المثال، يمكن لبرمجيات الإعلانات تتبع مستخدم يقوم بزيارة مواقع لبيع السيارات على الإنترنت ومن ثم يبحث عن نوع محدد منها. عند إذن ستصنف تلك البرمجيات هذا المستخدم على أنه مستخدم يرغب في شراء سيارة جديدة، فتجمع معلوماته وتبيعها لشركات الإعلان عن سيارات للبيع.

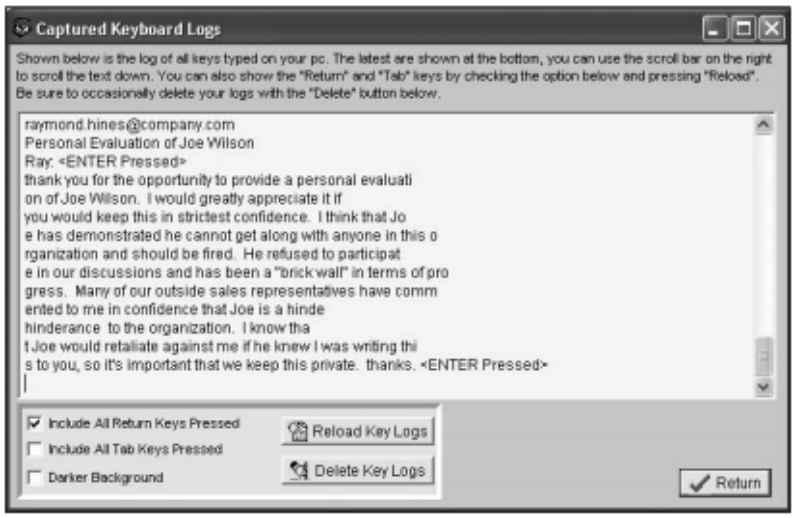
مسجل المفاتيح (Keyloggers): ومسجل المفاتيح إما أن يكون جهاز صغير أو برنامج يراقب كل ضغطة زر يقوم المستخدم بإدخالها من لوحة المفاتيح. كل ما يكتبه المستخدم يتم جمعه وتخزينه في ملف نصي. وتلك المعلومات يمكن الوصول إليها لاحقًا عن طريق مهاجم أو يتم إرسالها لطرف ثالث بشكل سري. بعدها سيتمكن المهاجم من البحث عن معلومات تفيده في ذاك النص ككلمات المرور أو أرقام البطاقات الائتمانية أو معلومات شخصية. إذا كان مسجل المفاتيح المستخدم عبارة عن جهاز فيكون بين موصل لوحة المفاتيح ومنفذ لوحة المفاتيح في الحاسوب كما يظهر في الصورة المبينة في الأسفل:



الشكل 5-1: الجهاز المسجل للمفاتيح

يصعب اكتشاف الجهاز المسجل للمفاتيح حيث أنه صغير الحجم وشكله شبيه بالرأس الموصل للوحة المفاتيح، ودائمًا ما يكون منصب من الجهة الخلفية للحاسوب. وغالبًا ما يرجع المهاجم ليزيله بعد ما يحصل على المعلومات اللازمة للهجوم.

أما البرنامج المسجل للمفاتيح فهو برنامج يقوم بالتقاط الإدخالات من لوحة المفاتيح بدون إذن المستخدم أو لفت أنتباهه كما يظهر في الصورة المبينة في الأسفل. البرنامج المسجل للمفاتيح لا يحتاج وصول مادي للحاسوب فهو عادة ما يُنصب في الجهاز باستخدام برمجيات خبيثة كالفيروسات أو أحصنة طروادة. وعادةً ما تتمكن تلك البرامج من إخفاء نفسها عن المستخدم حتى وإن قام بالبحث عنها.



الشكل 6-١: البرنامج المسجل للمفاتيح

حالة دراسية (٣):

يتم توزيع المتدربين إلى مجموعات، ومن ثم تقوم كل مجموعة بالعمل على الحالة الدراسية التالية:

أشترك ثلاثة زملاء يدرسون في معهد الإدارة (تركي، فهد، خالد) في مشروع لمادة البرمجة. كان كلًا منهم يعمل على حاسوبه في المكتبة. اشتكى فهد من نشاط خبيث يقوم به حاسوبه، وأنه قد بدأ بملاحظته بعدما قام بتنزيل وتثبيت برمجيات خاصة بالتصميم من إحدى مواقع المنتديات في شبكة الإنترنت. أضاف خالد متسائلًا عن نشاط خبيث قام به حاسوبه هو الآخر لكنه تعجب أن النشاط الخبيث قد بدأ بعد أسابيع عدة لم يتصل خالد فيها بشبكة الإنترنت ولم يقم بتشغيل أي قرص مدمج أو قابل للإزالة على جهازه خلال هذه الفترة. داخلهما تركي وتحدث عن الأنتشار الكبير للبرمجيات الخبيثة في الوقت الحالي. وذكر أنه للتو استلم حاسوبه من قسم الصيانة لإصابته ببرمجية خبيثة تمنعه من بدء تشغيل حاسوبه.

من خلال ما تعلمته في **أنواع البرمجيات الخبيثة**، حاول تصنيف البرمجيات التي أصابت أجهزة كلًا من تركي، فهد، وخالد مع ذكرك للأسباب التي استندت عليها.

اليوم الأول - الجلسة التدريبية الثانية

حماية الأنظمة

تدعيم أمن نظام التشغيل:

تحديث نظام التشغيل:

نظام التشغيل يتكون من عدد كبير من برامج الحاسوب التي تتكون من مئات الآلاف من الأوامر وربما تصل إلى أكثر من مليون أمر لذلك يمكن ملاحظة أن مجلد نظام التشغيل على حاسبك يشغل مساحة كبيرة من وحدة التخزين. نظراً للعدد الكبير من البرامج التي يتكون منها نظام التشغيل ولتشعب عملياتها فإن الشركات المنتجة لها كانت في الماضي تنتج إصدار جديد كل بضعة أشهر لكي تعالج المشكلات التي توجد في أوامر النظام ولكي تضيف مزيداً من الخصائص. الطريقة السابقة لم تعد تصلح مع نظم التشغيل الحديثة فالشركات المنتجة لها قد تحتاج إلى تحديث وتطوير برامجها كل يوم.

قدمت شبكة الإنترنت حلاً لتحديث نظم التشغيل حيث أتاحت للشركات المنتجة لها طريقة سهلة وسريعة لكي يستطيع المستخدم تحديث النظام الذي يتعامل معه على حاسوبه. باستخدام هذه الطريقة لم تعد الشركات تسعى إلى إصدار نسخة جديدة من نظم التشغيل كل بضعة أشهر فنظام التشغيل يمكن أن يعيش لسنوات طويلة طالما تتمكن الشركات المنتجة لها من علاج المشكلات التي تظهر به ومن تقديم خدمات جديدة عن طريق مواقعها على شبكة الإنترنت. [٣]

الهدف من تحديث نظام التشغيل هو: ـ

- ـ علاج الثغرات الأمنية التي يمكن أن ينفذ منها الفيروسات والبرامج الضارة بالحاسب.
- ـ علاج بعض مشكلات البرامج المكونة للنظام والتي من الممكن أن تسبب مشكلات للمستخدم مثل توقف الحاسب عن العمل بطريقة غير طبيعية.
- ـ إضافة خصائص جديدة على الحاسوب.

تكوين حماية لنظام التشغيل (Protection Configuring Operating System):

ولأن نظام التشغيل هو الجوهر لنظام الحاسوب فمن المهم جداً حمايته. تتخذ أغلب المنظمات أربعة مناهج لتكوين حماية نظام التشغيل:

١-السياسة الأمنية (Security Policy): يبتدأ الأمن مع منظمة تحدد أولاً الإجراءات اللازمة فيما يجب اتخاذه لإنشاء بيئة آمنة والحفاظ عليها. فيتم تسجيل المعلومات رسمياً في السياسة الأمنية (Security Policy). وهو عبارة عن ملف أو سلسلة من الملفات التي تحدد بوضوح آليات الدفاع

التي تستخدمها المنظمة من أجل الحفاظ على معلومات آمنة. وسنستعرض لاحقًا بعضًا من السياسات الأمنية المتبعة في معهد الإدارة.

٢-التكوين الأساسي (Configuration Bassline): بعدما تم تكوين السياسة الأمنية (Security Policy)، يتم إنشاء التكوين الأساسي(Configuration Bassline) وهو عبارة عن إعدادات تكوين نظام التشغيل الذي يستخدم لكل حاسوب في المنظمة. حيث إن السياسة الأمنية (Security Policy) تحدد ما يجب حمايته، والتكوين الأساسي (Configuration Bassline) هي الإعدادات لتكوين نظام التشغيل التي فرضت كيفيته السياسة التي يتم تطبيقها، يشتمل التكوين الأساسي على السيطرة على الخدمات، الصلاحيات على الملفات، صلاحيات التسجيل وغيرها.

٣-قالب الأمان (Security Templet): هو التكوين الأساسي لكل حاسوب، ويمكن أن يتم إنشاء قالب أمان واحد من خلاله يمكن تكوين مجموعة من إعدادات الأمان للتكوين الأساسي ويمكن استيرادها إلى أنظمة الحاسوب التي ينطبق عليها.

٤-النشر(Deployment): الخطوة الأخيرة نشر قالب الأمان (Security Templet) وهناك طريقتان للنشر لأجهزة مايكروسوفت ويندوز. الطريقة الأولى يمكن نشر قالب الأمان (Security Templet) يدوياً لكل حاسوب من قبل المسؤول باستخدام الأوامر الكتابية أو باستخدام برنامج(Snap-in). الطريقة الثانية هي باستخدام نهج المجموعة (Group Policies) هي خاصية في مايكروسوفت ويندوز توفر تكوين وإدارة مركزية للأجهزة الحاسوب والمستخدمين عن بعد الذين يستخدمون خدمة الدليل من مايكروسوفت تعرف بالدليل النشط (Active Directory).

وهذه الخطوات الأربع تجعل مهمة إدارة أمن نظام التشغيل للأجهزة الحاسوب في المنظمات أسهل.

منع الهجمات التي تستهدف متصفح الويب:

من المهم حماية النظام من الهجمات التي تأتي من خلال متصفح الويب وتشمل هذه الهجمات:

ملفات تعريف الارتباط (Cookie): يمكن للخادم أن يخزن معلومات المستخدم الشخصية في ملف داخل الحاسوب المحلي للمستخدم واسترجاع هذه المعلومات في وقت لاحق هذا ما يسمى بملفات تعريف الارتباط (Cookie). وهناك نوعان: الأول ملف تعريف الارتباط من الطرف الأول (First Party Cookie) يتم إنشاءه من قبل الموقع الذي تمت زيارته من قبل المستخدم وذلك عند زيارة أي موقع يتم حفظ ملف تعريف الارتباط في القرص الصلب للحاسوب. وكلما رجع المستخدم لصفحة الموقع يمكن لملف تعريف الارتباط الذي أنشئ من قبل الموقع أن يعرف تفضيلات المستخدم. النوع الثاني هو ملف تعريف الارتباط من طرف ثالث (Third Party Cookie) لا يتم إنشاءه من قبل الموقع وإنما يحاول الموقع الوصول لملف تعريف الارتباط الذي أنشئ من قبل موقع آخر. في كلتا الحالتين لا توجد مخاطر أمنية عالية من ملف تعريف الارتباط لأنه لا يحتوي على معلومات شخصية مثل اسم المستخدم وعنوان البريد وإنما هي تستخدم لتتبع عادات التصفح والشراء للمستخدم مثل المنظمات التسويقية تقوم بتتبع عادات التصفح والشراء للعملاء في الموقع.

للدفاع ضد ملفات تعريف الارتباط (Cookie): للاحتياط من ملفات الارتباط يمكننا الدفاع ضدها عن طريق تعطيلها أو حذفها بمجرد إنشاؤها.

جافا سكريبت (JavaScript): هي لغة برمجة نصية يتم تفسيرها إلى لغة يفهمها الحاسوب وتُقيم هذه اللغة في داخل ملفات(HTML). إذا كان هناك مواقع تستخدم جافا سكريبت(JavaScript) فإن ملفات(HTML) مع برمجة الجافا سكريبت تنزل في حاسوب المستخدم بعد ذلك يقوم المتصفح بتنفيذ برمجة باستخدام مترجم جافا. وبسبب ذلك فإن زيارة موقع يقوم بتنزيل تلقائي لبرنامج على الحاسوب من الممكن أن يسبب مخاطر. لكن للجافا سكريبت محدودية حيث إنه:

- لا يمكن للجافا سكريبت أن يدعم إمكانيات معينة. تشغيل الجافا سكريبت ليس له القدرة على القراءة، الكتابة، الحذف، أو فهرسة الملفات على الحاسوب.
- ليس له القدرة على الربط الشبكي بحيث لا يمكن تأسيس اتصال مباشر مع الأجهزة المتصلة بنفس الشبكة.

للدفاع ضد الجافا سكريبت (JavaScript) يمكن تعطيلها في صفحة المستعرض.

مضادات الفيروسات Virus countermeasures: يقصد بها البرمجيات التي تستخدم لمكافحة البرامج المصممة خصيصاً للإضرار بنظام الحاسب الآلي وتسميتها بمضادات الفيروسات لا يجعلها قاصرة على مكافحة الفيروسات فقط بل هو اصطلاح يطلق على هذا النوع من البرمجيات. وفي كثير من الأحيان يطلق على كل البرامج الضارة اسم فيروس بغض النظر عما إذا كان فيروس فعلاً أو دودة أو أحصنة طروادة أو أي نوع آخر من أنواع البرمجيات الضارة.

هناك سباق مستمر بين مطوري البرامج الضارة وبرامج مضادات الفيروسات، فكلما وجد برنامج فعال لمكافحة الفيروسات الحالية، يتم أنتاج نوع جديد من الفيروسات لا يعالجها البرنامج الحالي.

العلاج الناجح للفيروسات هو منعها أو عدم السماح لها بالدخول لنظام الحاسب إلا أن تحقيق ذلك يعد من الصعوبة بمكان ولكن إذا حدثت الإصابة بالفيروس فهناك إجراءات يمكن اتخاذها في مواجهة الفيروس أو لمعالجته وتقليل عواقبه هي عبارة عن خيارات يتم اختيار الأنسب منها والذي يوفر أعلى حماية وأقل تكلفة. تتلخص أهداف مضادات الحماية من الفيروسات في الآتي:

الاكتشاف Detection: هو تحديد حدوث الإصابة بالفيروس وتحديد مكانه.

التعرف على الفيروس Identification: عند اكتشاف الإصابة تأتي مرحلة التعرف على نوع الفيروس الذي سبب الإصابة وذلك من خلال علامات معينة في كود الفيروس أو بسلوكه الذي يقوم به في النظام.

إزالة الفيروس Virus Removal: بعد التعرف على نوع الفيروس تتم إزالته من الملف المصاب وإرجاع الملف إلى وضعه الأصلي وتَعَقُّب كل النسخ الأخرى من الفيروس للحد من أنتشاره مرة أخرى. إذا أسفرت مرحلة الاكتشاف عن وجود فيروس لم يتم التعرف على نوعه يجب اللجوء

لخيار التخلص discard من البرنامج المصاب ثم إعادة تركيبه مرة أخرى باستخدام النسخ الاحتياطية. هناك سباق سريع في تصميم وتطوير الفيروسات ومضادات الفيروسات، وبعكس الأنواع القديمة من المضادات، التي كانت بسيطة، فان تعقيدا كبيراً قد طرأ على مضادات الفيروسات نسبة لتعقيد الفيروسات التي تعالجها.

أسئلة ونقاش(٣):

س١: على ماذا يشتمل حماية الأنظمة؟

س٢: ماأهداف تحديث نظام التشغيل؟

س٣: ما أهداف مضادات الحماية من الفيروسات؟

تثبيت برامج الحاسوب المهمة للحماية

أولًا تثبيت مكافحة الفيروسات:

تمرين عملي(١):

يقوم المتدرب بتثبيت برنامج مكافحة الفيروسات "Avast" الإصدار المجاني على جهاز الحاسب.
يمكن الحصول على البرنامج من خلال الرابط التالي:

http://files.avast.com/iavs9x/avast_free_antivirus_setup_online.exe

*قد تستغرق عملية التثبيت من ٦ إلى ١٠ دقائق

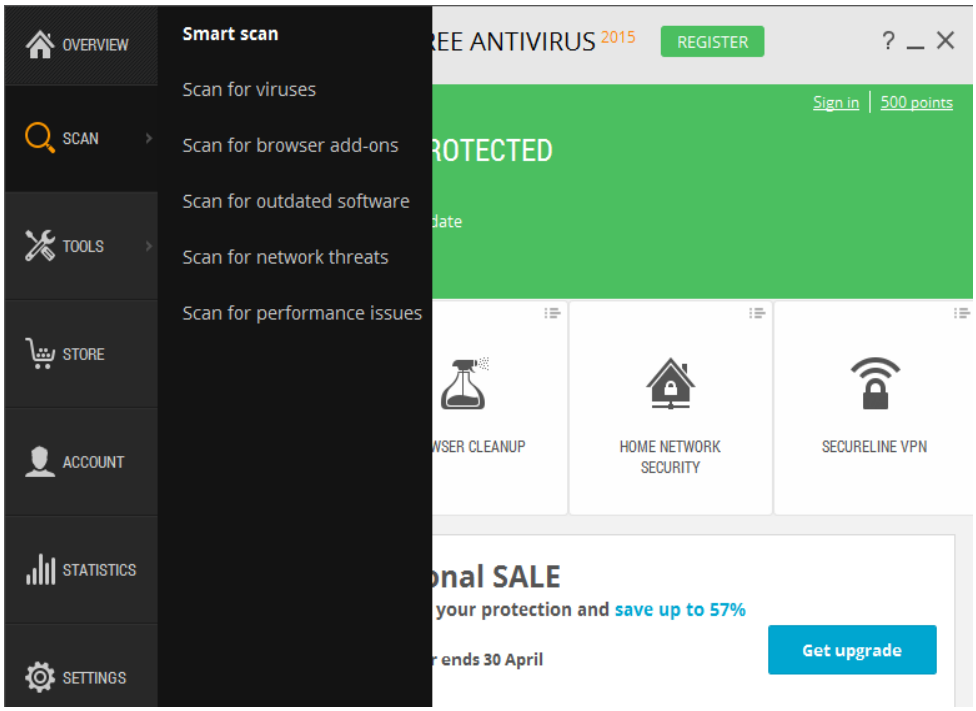
يقوم المتدرب بعد ذلك بضبط الإعدادات التالية:

- التحكم بطرق تفحص الجهاز.
- التحكم بإعدادات اللغة.
- إعداد درع ملف النظام.
- إعداد درع البريد الإلكتروني.
- إعداد تحديث برنامج الحماية.

بعد عملية تثبيت مكافح الفيروسات "Avast" سيصبح شكل الشاشة الرئيسية للبرنامج كما في الشكل:

الشكل 7-١: الشاشة الرئيسية لبرنامج Avast

أولاً: التحكم بطرق تفحص الجهاز: ١-اضغط على أيقونة "Scan" وستظهر لك أنواع طرق التفحص المتاحة في البرنامج كما في الشكل التالي:



الشكل 8-١: أنواع طرق التفحص المتاحة في برنامج Avast

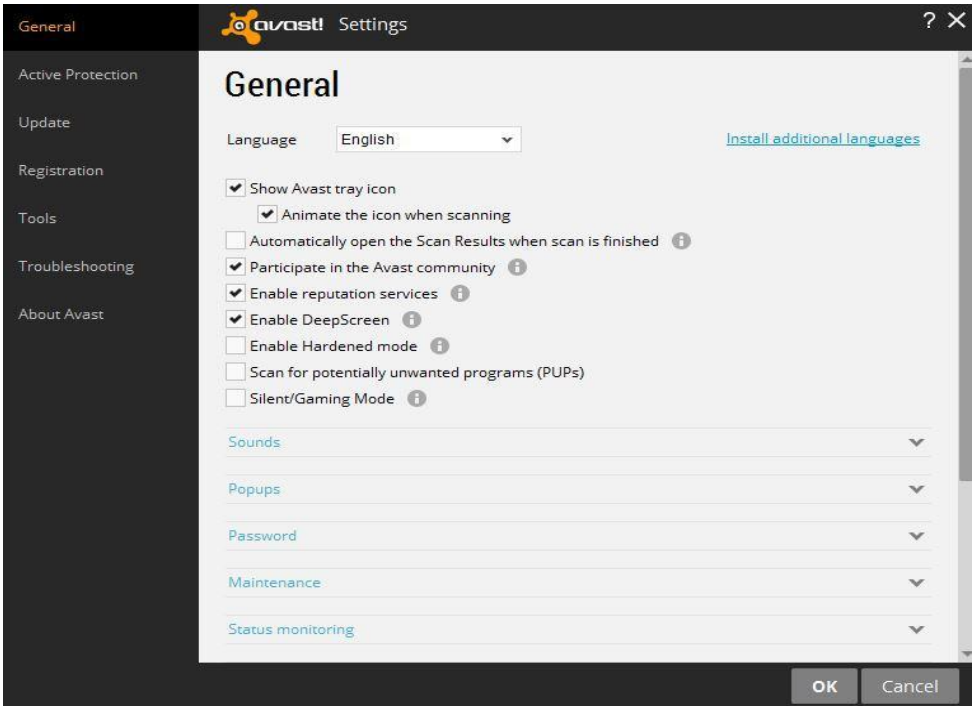
٢-قم باختيار "Scan for Viruses" وستظهر لك الطرق المتاحة لعملية تفحص الجهاز من الفيروسات كما في الشكل التالي:

الشكل 9-١: الطرق المتاحة لعملية فحص الفيروسات في برنامج Avast

يتيح لك البرنامج عدة طرق لتفحص الجهاز، إما تفحص سريع، كامل، الوسائط القابلة للإزالة أو ملف محدد. قم باختيار إحدى هذه الطرق.

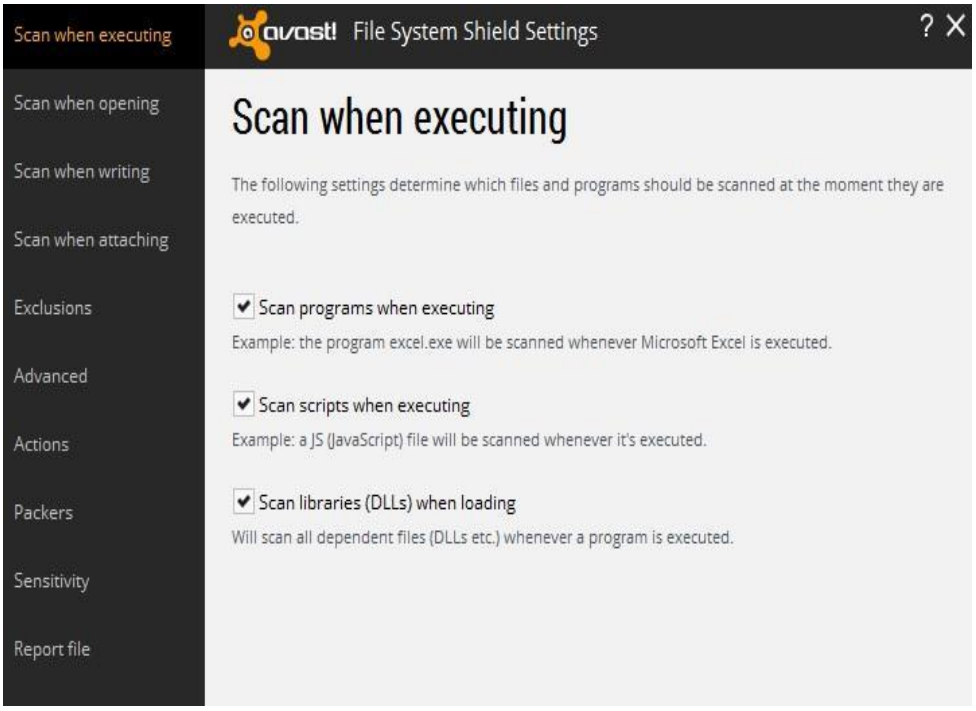
ثانياً: التحكم بإعدادات اللغة:

١. اضغط على "Sitting" ومن "General" ستظهر لك خيارات التحكم في اللغة كما في الشكل التالي:



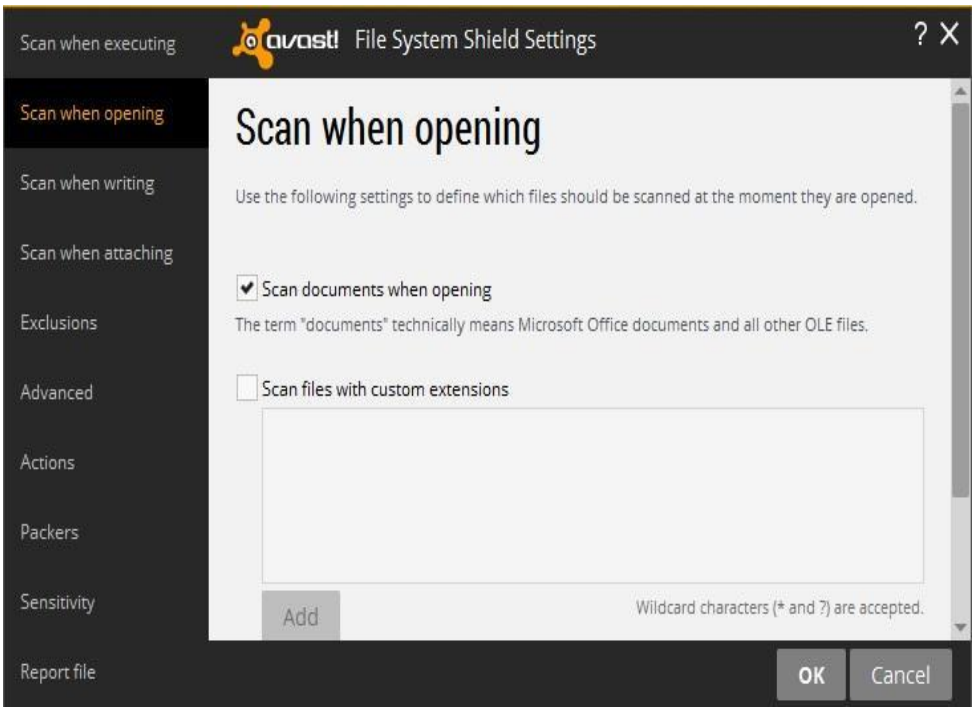
الشكل 10-١: خيارات التحكم في اللغة في برنامج Avast

ثالثاً: إعدادات درع ملفات النظام: ١-اضغط على "Sitting" ومن ثم "Active Protection" ومن "File System Shield" اضغط على "Customize" وستظهر لك الشاشة التالية:



الشكل 11-١: شاشة تحديد أنواع الملفات التنفيذية التي يجب فحصها من قبل Avast

٢. تأكد من تفعيل "Scan Documents when opening" بالضغط على خيار "Scan When opening" كما في الشكل (١٢-١):

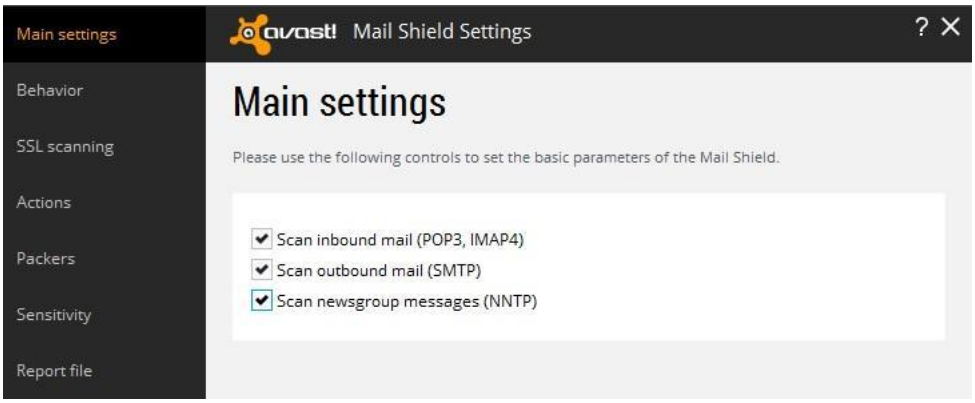


الشكل 12-١: خيارات فحص الملفات عند فتحها في برنامج Avast

٣. قم باستعراض بقية الخيارات المتاحة لضبط إعدادات درع ملف النظام

رابعاً: إعداد درع البريد الإلكتروني:

١. اضغط على "Sitting" ومن ثم "Active Protection" ومن "Email Shield" اضغط على "Customize" وستظهر لك الشاشة كما في الشكل (١٣-١):

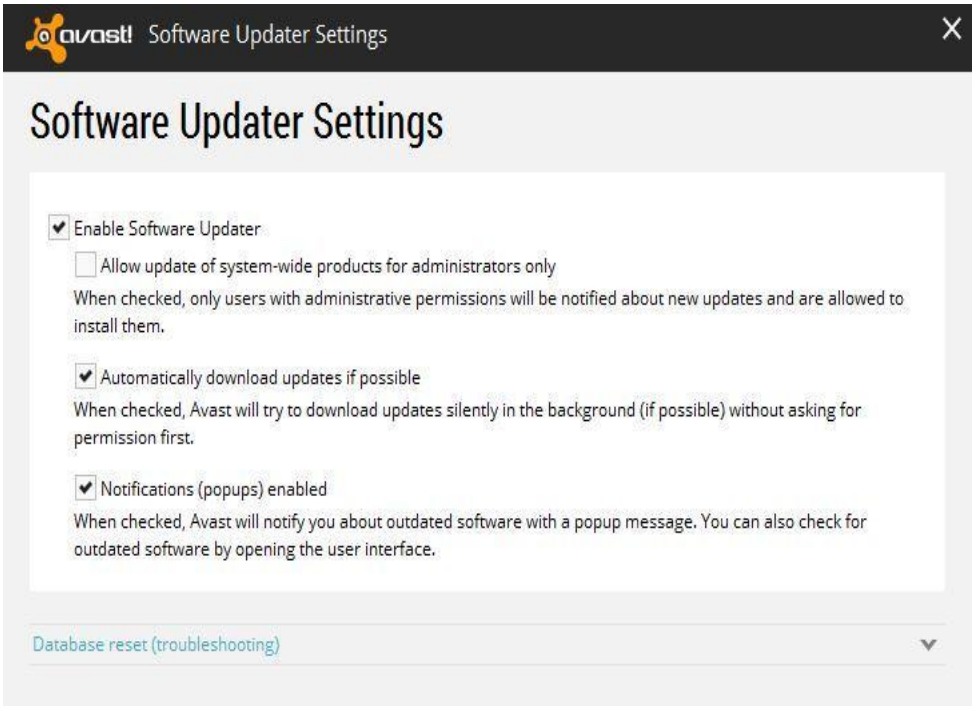


الشكل 13-١: الإعدادات الرئيسية في درع البريد الإلكتروني في برنامج Avast

٢. تأكد من اختيار جميع البروتوكولات الخاصة بالبريد الإلكتروني والتي تعني بأن البرنامج سيقوم بتفحص جميع الرسائل الصادرة والواردة إلى جهازك

خامساً: إعداد تحديث برنامج الحماية

١. اضغط على "Sitting" ومن ثم "Tools" ومن "Software Updater" اضغط على "Customize" وستظهر لك الشاشة كما في الشكل (١٤-١):



الشكل 14-1: شاشة إعدادات تحديثات برنامج Avast

٢. تأكد من تفعيل خيار "Automatically download update if possible" حيث يتيح لك هذا الخيار تحديث برنامج مكافحة الفيروسات آلي وبالتالي تتأكد من احتواء قاعدة بياناته على أحدث الفيروسات ليقوم بعملية اكتشافها في حالة إصابتها لجهازك.

*__ملاحظة:__ هنالك العديد من برامج مكافحة الفيروسات على الإنترنت. وهناك العديد منها بمقابل مادي. غالباً ما ينقص برامج مكافحه الفيروسات المجانية العديد من الخصائص المفيدة والتي من الممكن أن تسبب ثغره للمهاجمين للوصول لجهازك. فعلى سبيل المثال لا توفر العديد من برامج المكافحة المجانية خدمة تفحص رسائل البريد الإلكتروني أو رسائل الدردشات والتي من الممكن من خلالها إصابة جهازك ببعض الفيروسات. كذلك غالباً ما تطلب منك هذه البرامج تشغيل عملية تفحص الجهاز يدوياً وفي المقابل توفر مكافحة الفيروسات المدفوعة جدولة تفحص الجهاز بشكل آلي. كما أن هناك العديد من برامج مكافحة الفيروسات المجانية في الإنترنت والتي تظهر في الإعلانات المنبثقة يكون هدفها هو إيهام الشخص بإصابة جهازه بفيروس وبعد تثبيتها بجهاز الضحية يصب النظام بفيروس يجعله بطيئاً.

ثانياً: تثبيت مكافح البرمجيات الضارة Malwarebyte:

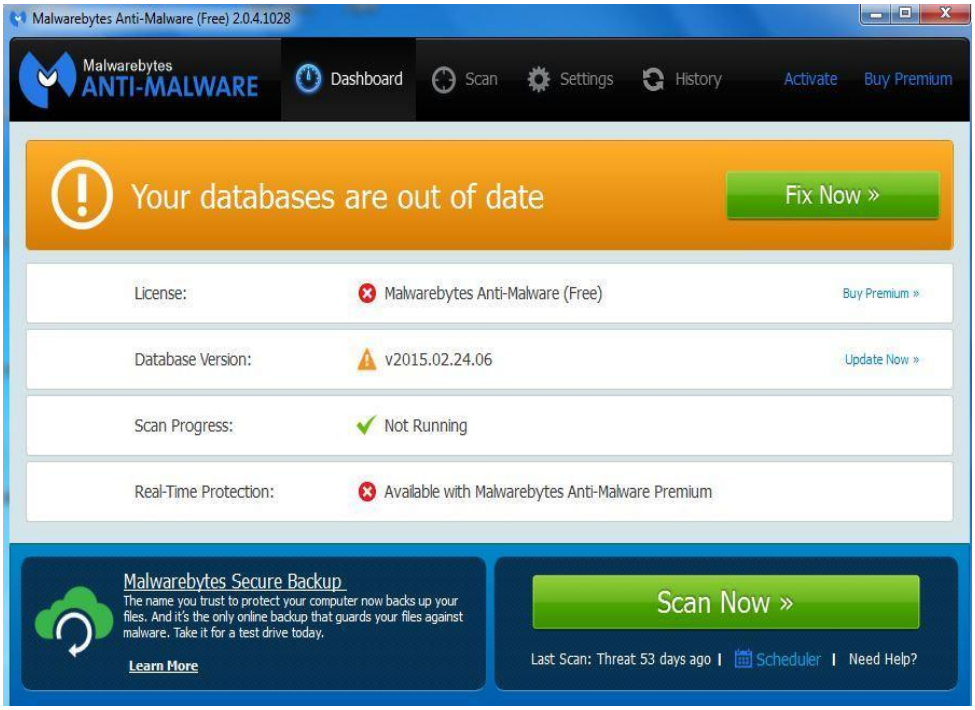
يعمل هذا البرنامج على كشف أغلب التهديدات الحديثة تقريباً، والتي لا تستطيع أغلب برامج مضادة الفيروسات المعروفة كشفها. يستخدم هذا البرنامج طرق سريعة وفي المقابل لا يستخدم الكثير من موارد النظام، والمهم في هذا البرنامج بالإضافة على قدرته في البحث عن الفيروسات المخبأة في الجهاز بكفاءة عالية، خفة البرنامج على الجهاز المثبت عليه وعدم تعارضه مع أي برنامج حماية مثبت مسبقا بالجهاز بمعنى أنه يمكن تثبيته مع برنامج الحماية المثبت على جهازك مسبقاً.

تمرين عملي(٢):

طريقة التثبيت:

١. قم بالدخول على الموقع https://www.malwarebytes.org/، ومن ثم تحميل النسخة المجانية وثبيتها.

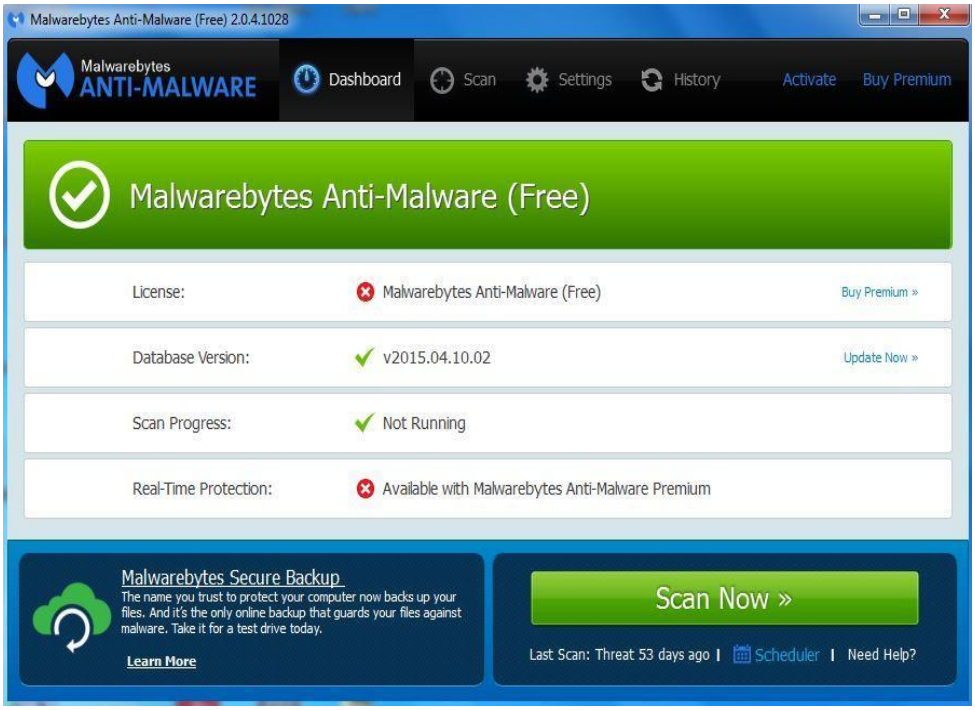
بعد عملية التحميل والتثبيت ستظهر لك الشاشة الرئيسية للبرنامج كما في الشكل (١٥-١):



الشكل 15-١: الشاشة الرئيسية لبرنامج Malwarebytes

يلاحظ في القائمة العليا لهذه الشاشة عدة خيارات منها عملية المسح للجهاز، الضبط، التاريخ، تفعيل البرنامج.

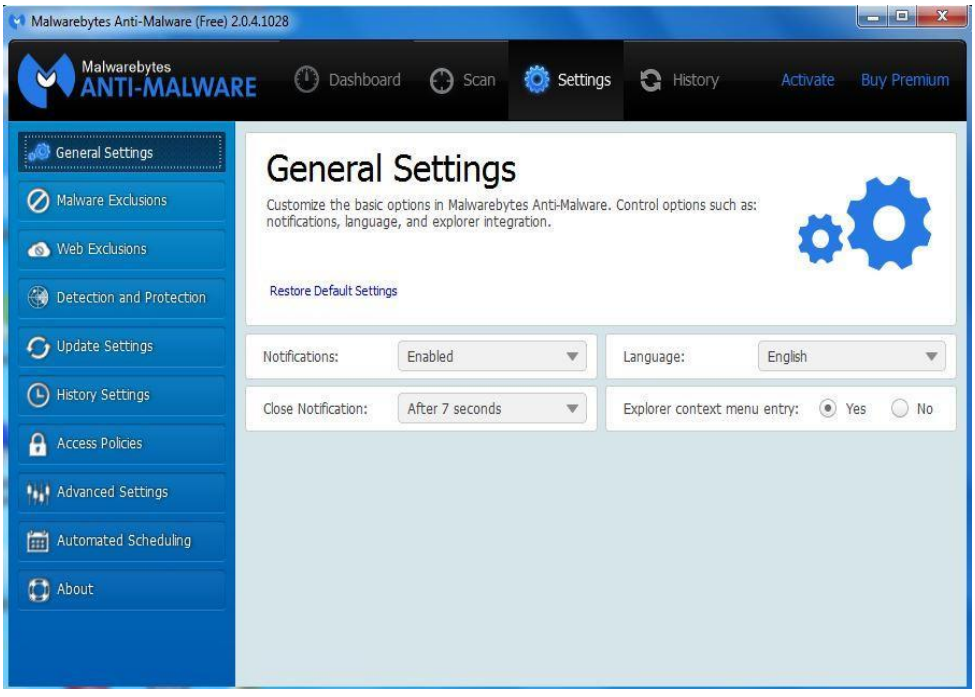
٢. قم باختيار Fix now كما هو موجود في الشكل (١٥-١)، وسيقوم البرنامج بتحديث قاعدة البيانات الخاصة به والتي ستساعد على كشف أحدث البرمجيات الخبيثة كما في الشكل (١٦-١):



الشكل 16-١: الشاشة الرئيسية لبرنامج Malwarebytes بعد التحديث

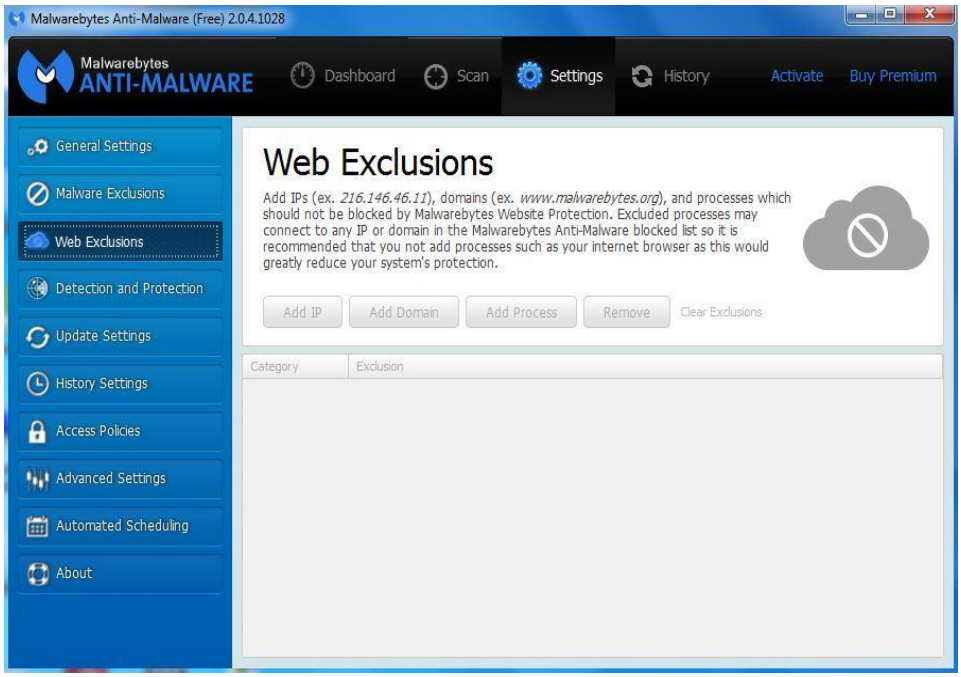
٣. بعد عملية التحديث قم بالضغط على خيار settings للمرور على ضبط إعدادات البرنامج حيث يتيح لك هذا الخيار ضبط العناصر التالية:

- اختيار اللغة المناسبة والسماح بالتنبيه عن البرمجيات الضارة كما في الشكل (١٧-١):



الشكل 17-١: شاشة الإعدادات العامة لبرنامج Malwarebytes

- إضافة استثناءات لبعض المواقع. كما هو معلوم تقوم بعض المواقع بالوصول إلى بعض المصادر الحساسة في جهازك. يقوم هذا البرنامج بمنع هذه المواقع وبالتالي سيقوم بحجب هذه المواقع عن جهازك. تقوم بعض المواقع المعروفة والمملوكة لشركات كبيرة موثوقة كشركة مايكروسوفت بالوصول لبعض العناصر لجهازك، فإذا قام هذا البرنامج بحجب هذا الموقع عنك، يمكنك عندئذ إضافته كاستثناء لتتمكن من تصفحه. تتم عملية الاستثناء بإضافة عنوان الموقع أو رقمه كما في الشكل (١٨-١):

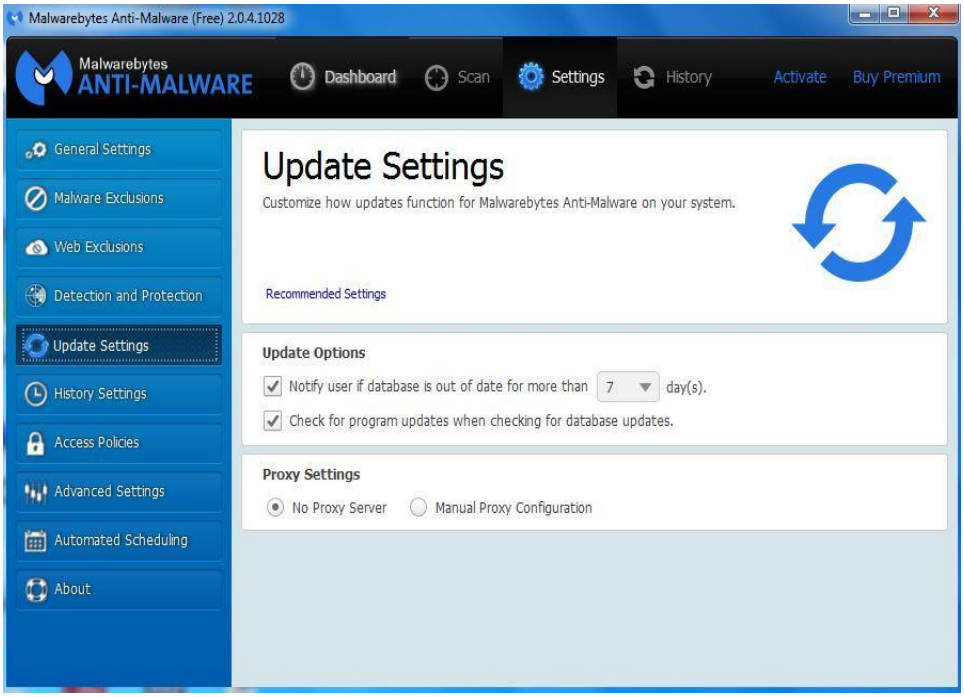


الشكل 18-١: شاشة إضافة استثناءات صفحات الويب المحجوبة في برنامج Malwarebytes

- الكشف والحماية: حيث تتيح لك هذه الخاصية اختيار البرمجيات التي تريد الكشف عنها والحماية منها مثل الجذور الخفية (Rootkit) وهي عبارة عن مجموعة أدوات برمجيات تمكن المستخدمين غير المصرح لهم للسيطرة على نظام الحاسوب دون أن يتم كشفها.

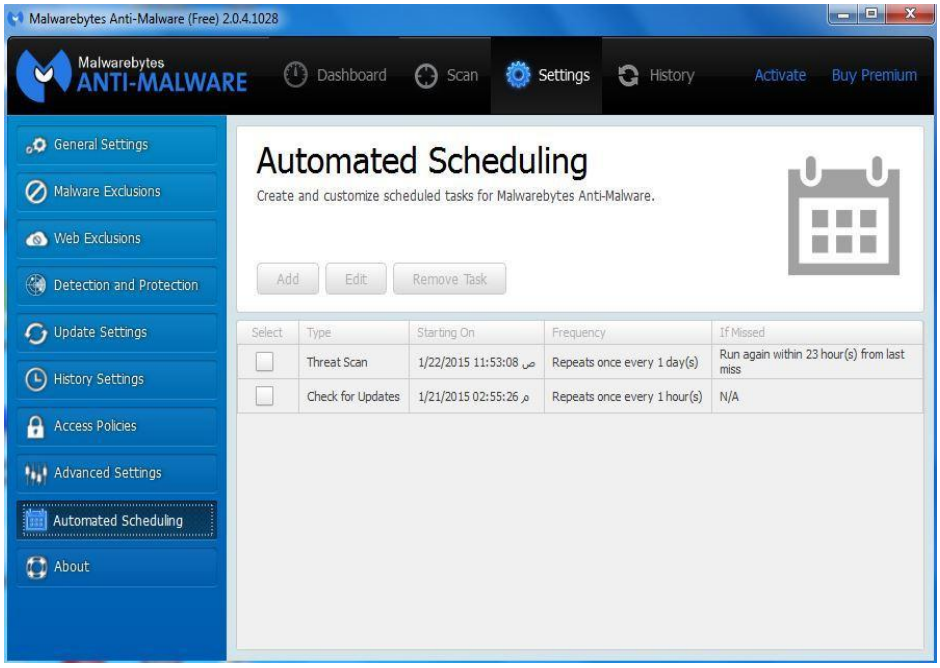
الشكل 19-١: شاشة الكشف والحماية في برنامج Malwarebytes

- إعدادات التحديث حيث تتيح لك اختيار التنبيه لوجود تحديث جديد للبرنامج كما في الشكل (٢٠-١):



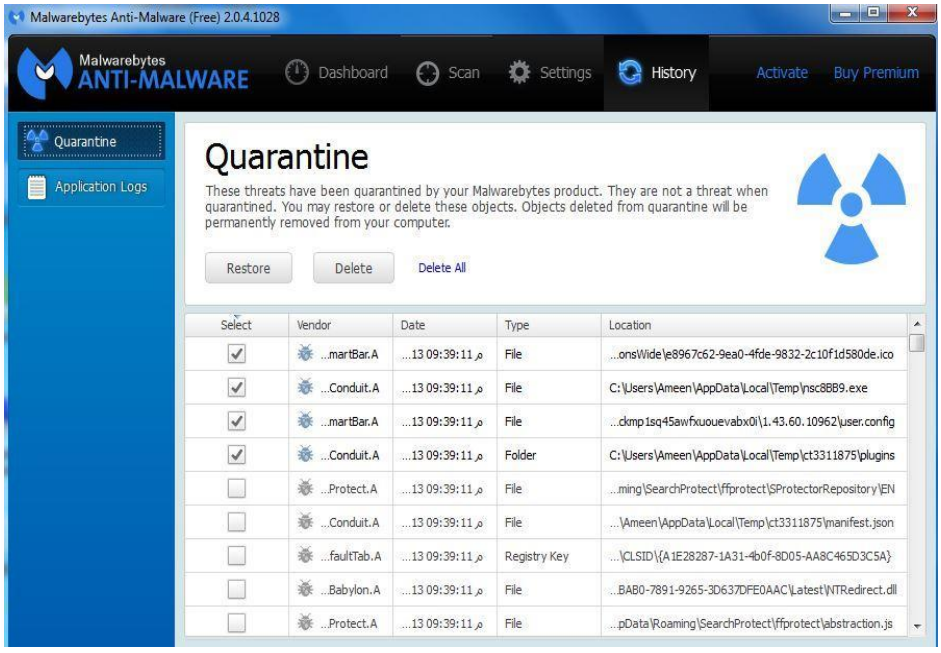
الشكل 20-١: شاشة إعدادات التحديثات في برنامج Malwarebytes

- الجدولة الأوتوماتيكية لعملية المسح: حيث يمكن عمل جدول زمني محدد يقوم فيه البرنامج بعملية مسح كامل للبرمجيات الخبيثة في جهازك كما في الشكل (٢١-١):



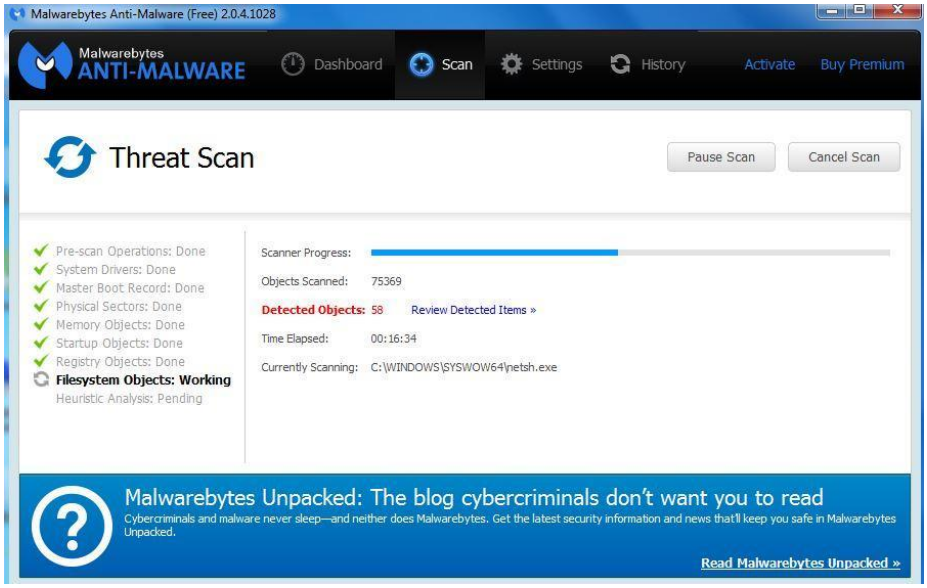
الشكل 21-١: شاشة جدولة عملية المسح في برنامج Malwarebytes

٤. في الواجهة الرئيسية للبرنامج يمكنك اختيار History حيث سيقوم البرنامج باستعراض جميع التهديدات التي تم كشفها في جهازك من قبل مع إمكانية حذفها كما في الشكل (٢٢-١):



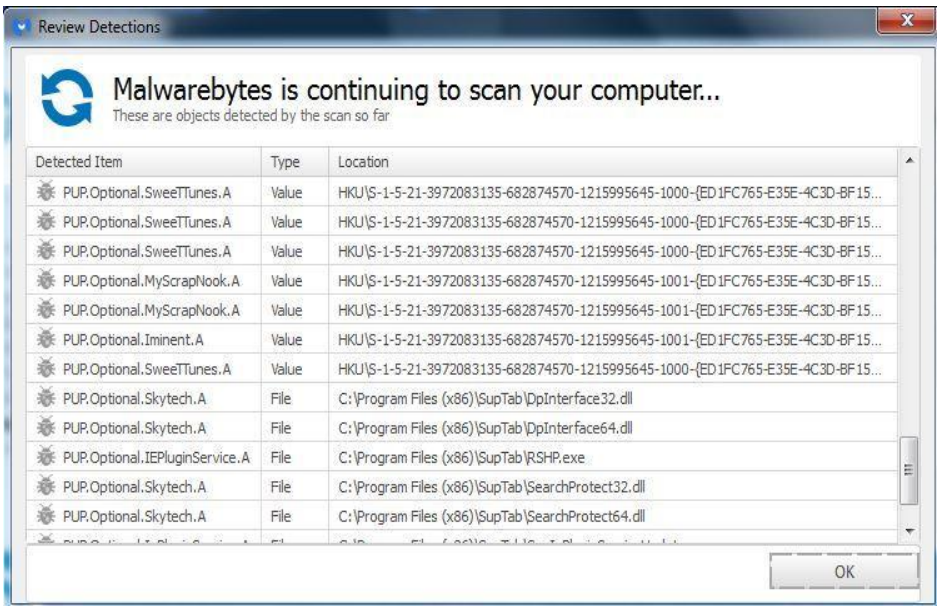
الشكل 22-١: سجل التهديدات التي تم كشفها من قبل Malwarebytes

٥. من الشاشة الرئيسية عند الضغط على خيار Scan سيقوم البرنامج ببدء عملية المسح للكشف عن البرمجيات الخبيثة والتهديدات التي من الممكن أن تصيب جهازك. وقد يستغرق هذا المسح مدة تزيد على ٣٠ دقيقة بناء على عدد الملفات الموجودة في جهازك كما في الشكل (٢٣-١):



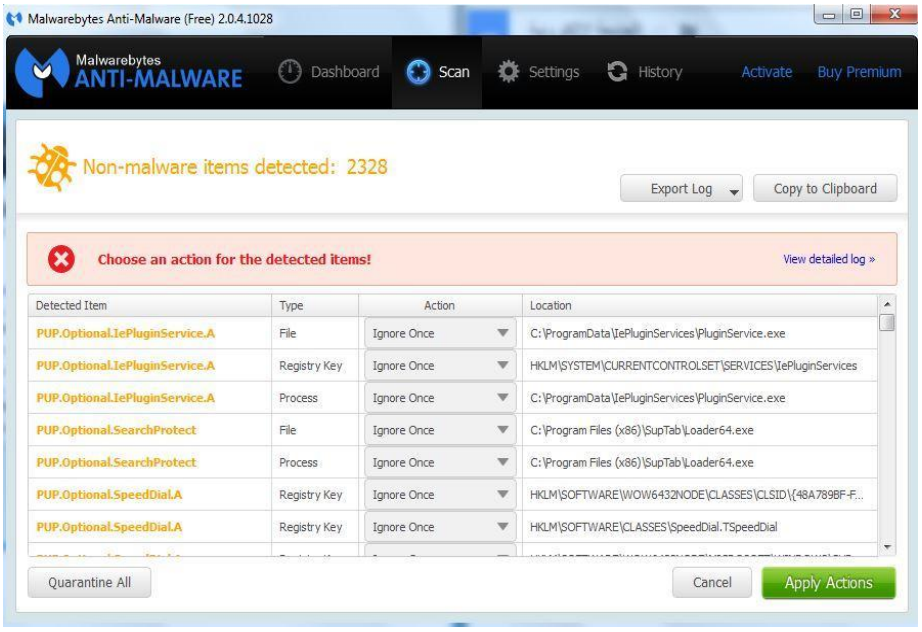
الشكل 23-١: شاشة المسح بحثاً عن التهديدات في برنامج Malwarebytes

يوضح هذا الشكل كمية ملفات الأنظمة الهائلة التي يقوم هذا البرنامج بفحصها، حيث يقوم بفحص جميع ملفات الأنظمة الموجودة في جهازك ومن ثم الكشف عن العناصر المهددة لجهازك كما هي ظاهرة باللون الأحمر detected object، فبعد الضغط عليها سيظهر لك العناصر التي تم كشفها ومع مواقعها كما في الشكل(٢٤-١):



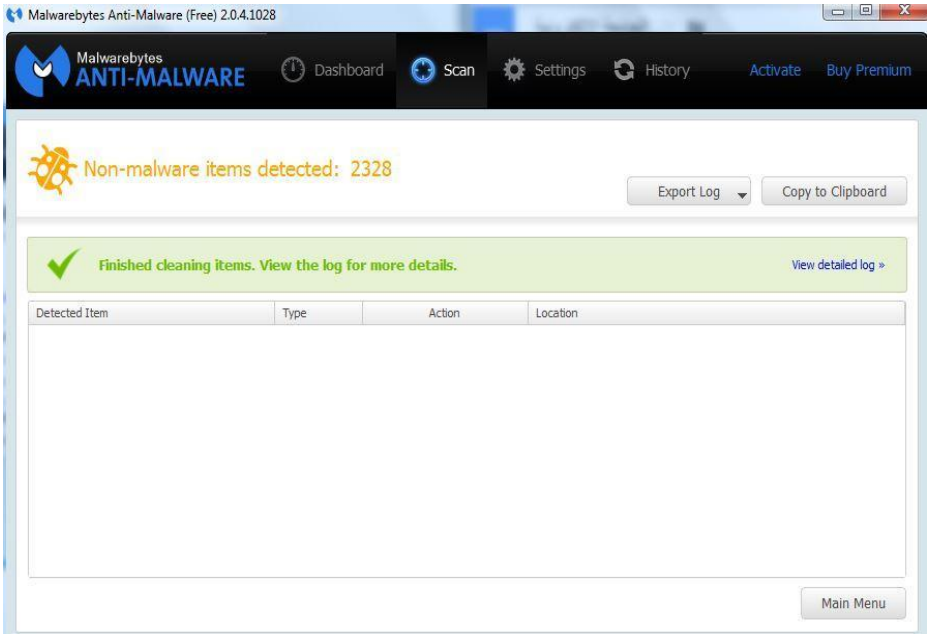
الشكل 24-١: الملفات التي يقوم Malwarebytes بفحصها

٦. بعد اكتمال عملية المسح قم باختيار "Quarantine all" لتتم عملية التنقيح لجهازك كما في الشكل (٢٥-١):



الشكل 25-١ : شاشة تظهر الملفات التي قد تشكل تهديداً والإجراءات التي يمكن للمستخدم اتخاذها في Malwarebytes

عندئذ ستظهر لك رسالة بأنه تم تنظيف جهازك من جميع التهديدات كما في الشكل (٢٦-١):



الشكل 26-١: رسالة تفيد بأن Malwarebytes قام بمسح جميع الملفات التي تشكل تهديد للنظام

ومن ثم ستظهر لك رسالة تفيد أنه تم حذف العناصر المحددة من جهازك وأن جهازك يحتاج إلى إعادة التشغيل كما في الشكل (٢٧-١):

الشكل 27-١: رسالة من برنامج Malwarebytes تطلب إعادة التشغيل

وبذلك قمت بتنظيف جهازك وإزالة جميع التهديدات التي من الممكن أن تصيب جهازك وتأثر على عمله أو تسمح للبعض بالوصول غير المشروع لجهازك. يفضل القيام بعملية المسح على جهازك بشكل أسبوعي على الأقل لتتم عملية إزالة جميع التهديدات بشكل دوري.

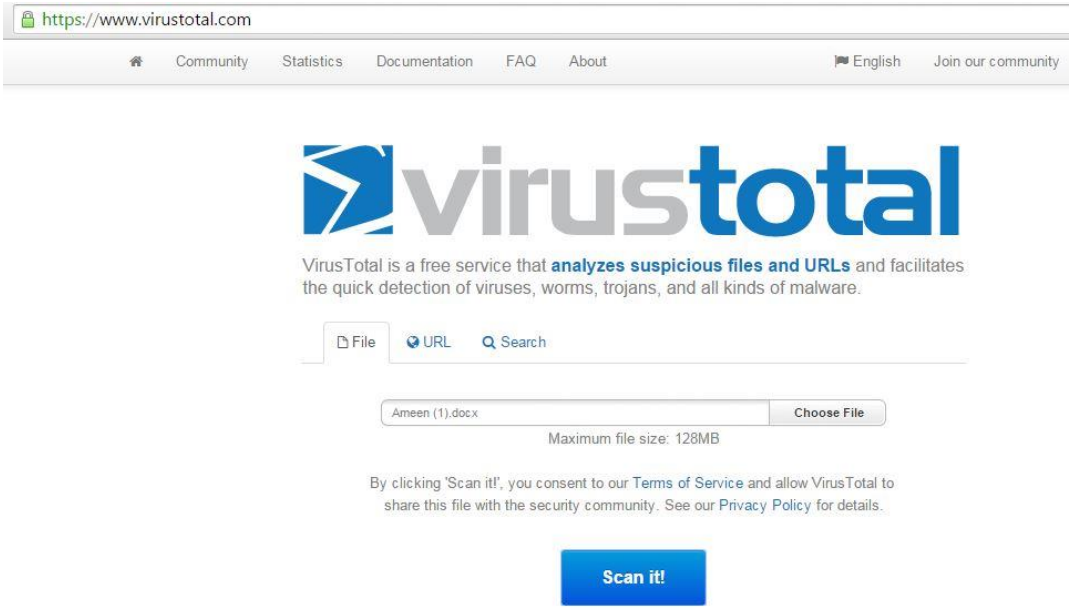
استخدام بعض مواقع الإنترنت لفحص ملف معين في الجهاز:

تتيح الكثير من مواقع الإنترنت إمكانية تفحص ملف معين وتوضيح ما إذا كان الملف يحتوي على فيروس معين أم لا مثل موقع Virus Total. تقوم العديد من برامج مكافحة الفيروسات المحدثة في وقتنا الحاضر بالكشف عن هذه الملفات أثناء تنزيلها أو تشغيلها. لكن قد تقوم باستخدام جهاز لا يوجد فيه برنامج حماية محدث فمن الأفضل فحص هذا الملف إذا كان مجهول المصدر. يتيح لك الموقع استعراضا لنتائج هذا الفحص بعد تمريره على عدة شركات حماية مثل Microsoft، Mcafee إلخ..

تمرين عملي(٣):

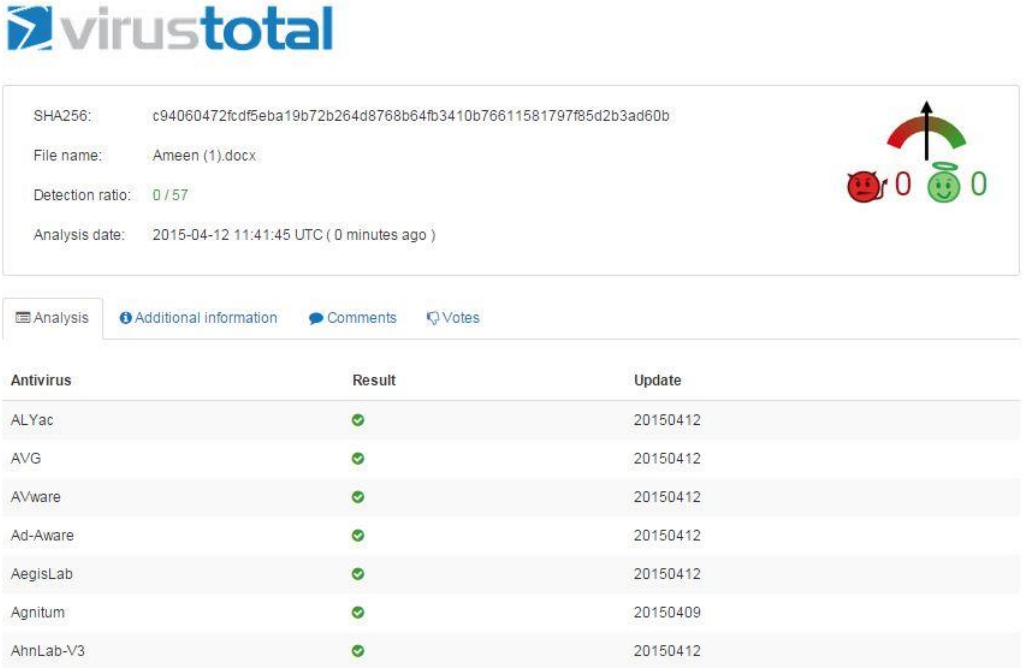
١-قم بالدخول على موقع https://www.virustotal.com/

٢-من الخيار choose file في الصفحة الرئيسية، قم باختيار الملف المراد تفحصه من جهازك كما في الشكل (٢٨-١):



الشكل ٢٨-١: الصفحة الرئيسية لموقع VirusTotal

بعد ذلك قم باختيار Scan it كما هو ظاهر في الشكل السابق، عندئذ سيبدأ الموقع تفحص الملف من عدة شركات حماية معروفه ويظهر لك النتائج التالية:



الشكل ٢٩-١: نتيجة فحص الملف باستخدام موقع VirusTotal

سيظهر لك الموقع نتائج الفحص لهذا الملف لأكثر من ٥٠ تطبيق حماية مستخدم في أمن الأجهزة.

الإعدادات الدورية للحفاظ على سلامة الجهاز

إذا كنت تتصل بأنترنت أو تسمح للآخرين باستخدام الحاسوب أو تشارك الملفات مع آخرين، ينبغي اتخاذ خطوات لحماية الحاسوب من التعرض للضرر. لماذا؟ نظرا لوجود مجرمي الحاسوب (يطلق عليهم أحيانًا المتطفلين) الذين يهاجمون أجهزة الحاسوب الخاصة بالآخرين. يمكن لهؤلاء الأشخاص مهاجمة الحاسوب مباشرةً بالتسلل إلى جهاز الحاسوب من خلال الإنترنت وسرقة المعلومات الشخصية أو يمكنهم مهاجمة أجهزة الحاسوب بطريقة غير مباشرة بإنشاء برامج ضارة تلحق الضرر بالحاسوب.

ولكن، يمكنك حماية جهازك من خلال اتخاذ بعض التدابير الوقائية البسيطة، والتأكد من إعداداتها بشكل دوري لأنها قد تتغير بعد تمكن بعض البرمجيات الضارة من جهازك.

*ملاحظة قم باستخدام نظام التشغيل ويندوز ٨

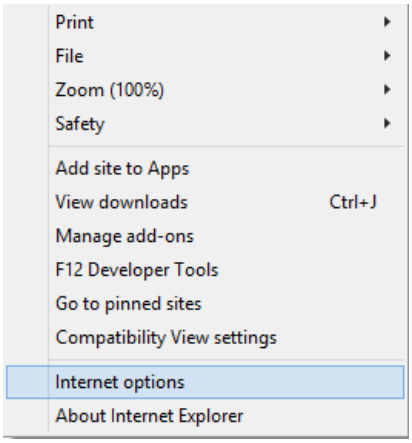
لضبط الإعدادات الدورية لجهازك قم بتنفيذ التطبيق التالي على نظام تشغيل ويندوز ٨:

تمرين عملي(٤):

*ملاحظة يتم استخدام نظام التشغيل ويندوز ٨ لإتمام هذا التدريب

أولاً: تأكد من إعدادات الأمان لمتصفح الإنترنت من خلال الخطوات التالية:

١. من سطح المكتب اضغط على متصفح الإنترنت "Internet Explorer".
٢. اضغط على أيقونة الأدوات "Tools" ومن ثم خيارات الإنترنت "Internet Options" كما في الشكل (٣٠-١):

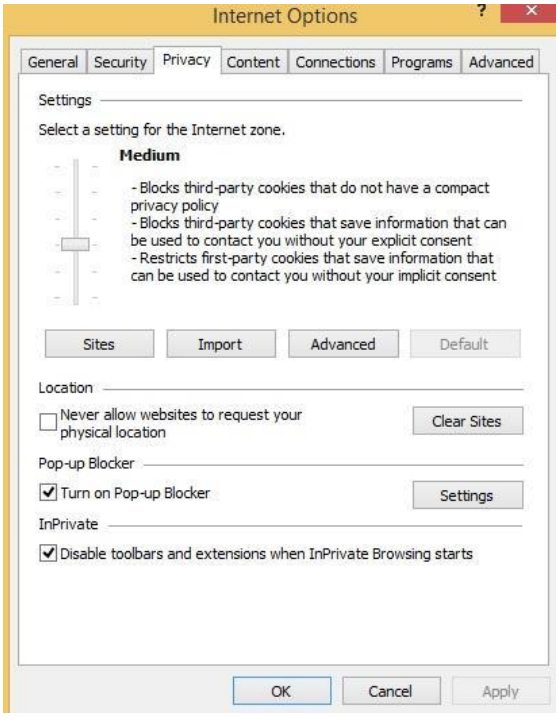


الشكل ٣٠-١: قائمة أدوات متصفح الإنترنت إكسبلورر

٣. من الخيار عام "General"، بإمكانك حذف "Browsing History".

٤. من الخيار أمان "Security"، لاحظ بأن بإمكانك ضبط إعدادات مناطق الأمان. حيث يتيح لك هذا الخيارات عدة مناطق يعتبر خيار "Medium-high" الأفضل.

٥. من الخيار "Privacy"، قم بتشغيل أداة حظر الصفحات المنبثقة "Pop-up Blocker" كما في الشكل(٣١-١):



الشكل 31-1: تبويب الخصوصية في خيارات الإنترنت في متصفح الإنترنت إكسبلورر

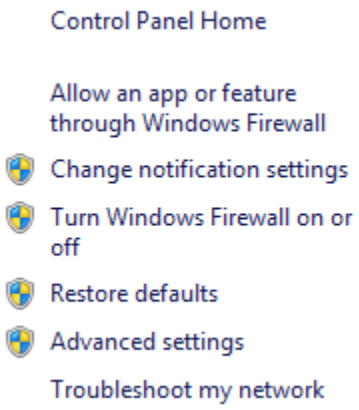
ثانياً: تأكد من تفعيل الجدار الناري "Windows Firewall"

الجدار الناري لويندوز هو عبارة عن برنامج يقوم بتفحص البيانات القادمة من الإنترنت أو الشبكة المحلية ومن ثم يقرر ما إذا كانت هذه بيانات جيدة أو سيئة للنظام. إذا اعتبر هذه البيانات سليمة، فإنه سيسمح لها بالمرور من خلال الجدار الناري. أما إذا كانت ضارة فأنه سيقوم بحجبها ولن تستطيع الوصول إلى الجهاز.

تمرين عملي(٥):

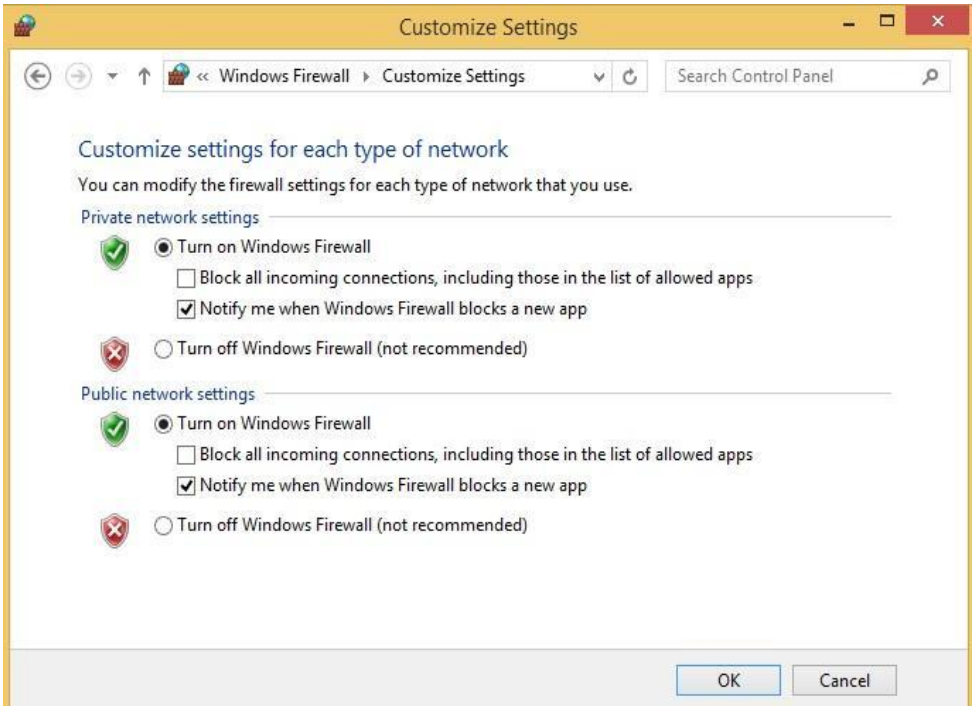
لتفعيل الجدار الناري قم بتطبيق الخطوات التالية:

١. من إبدأ "Start" قم باختيار لوحة التحكم "Control Panel" ومن ثم "System security" ومن ثم قم باختيار "Windows Firewall" ومن ثم اختر " Turn Windows Firewall On or off" كما في الشكل (٣٢-١):



الشكل 32-١: تفعيل الجدار الناري من لوحة تحكم النظام

٢. تأكد من أن إعدادات الجدار الناري على وضع التشغيل "on" كما في الشكل (٣٣-١):



الشكل 33-١: إعدادات الجدار الناري في نظام التشغيل ويندوز

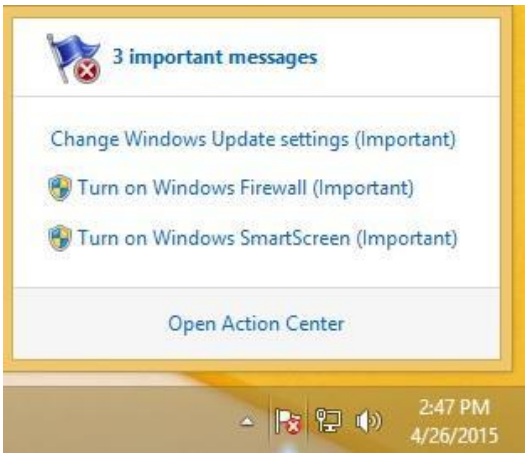
ثالثاً: تأكد من التنبيهات الموجودة في "Action Center" باستمرار

يحاول نظام تشغيل ويندوز ٨ جاهداً الاهتمام بأمان جهازك وبياناتك. ستقوم أداة "Action Center" والموجودة في ويندوز بإرسال تنبيهات إليك في حالة وجود مشكلة في أمان جهازك. تطلق هذه الأداة تنبيه في حالة أنك لم تقم بِضبط إعدادات الأمان المناسبة مثل برنامج حماية فيروسات غير مُحدَث، جدار ناري لا يعمل وغير مُحدَث. تلخص هذه الأداة العديد من الإعدادات الأمان حيث يمكن حل العديد من المشكلات من خلالها.

تمرين عملي(٦):

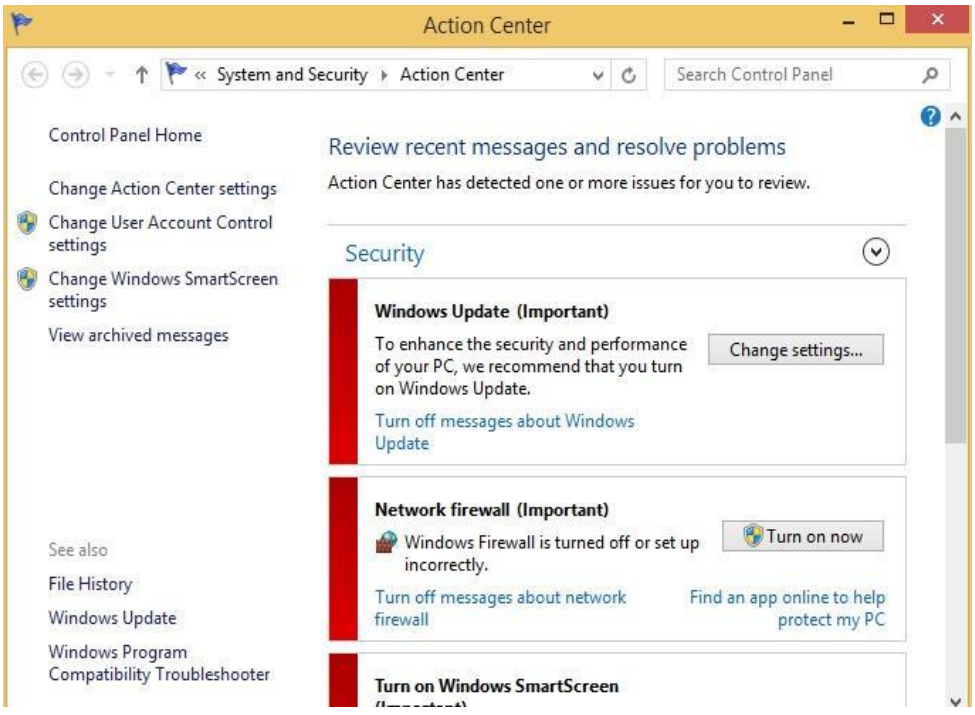
للتأكد من التنبيهات الموجودة في "Action Center" قم بتطبيق الخطوات التالية:

١. من سطح المكتب، من خلال شريط الأدوات قم باختيار "Action Center" كما في الشكل(٣٤-١):



الشكل 34-١: مركز التنبيهات في نظام التشغيل ويندوز

٢. لاحظ وجود العديد من التنبيهات الخاصة بأمان ويندوز، قم باختيار " Open Action Center" لحل هذه المشكلات في الإعدادات كما في الشكل (٣٥-١):



الشكل 35-١: مركز الإجراءات في نظام التشغيل ويندوز

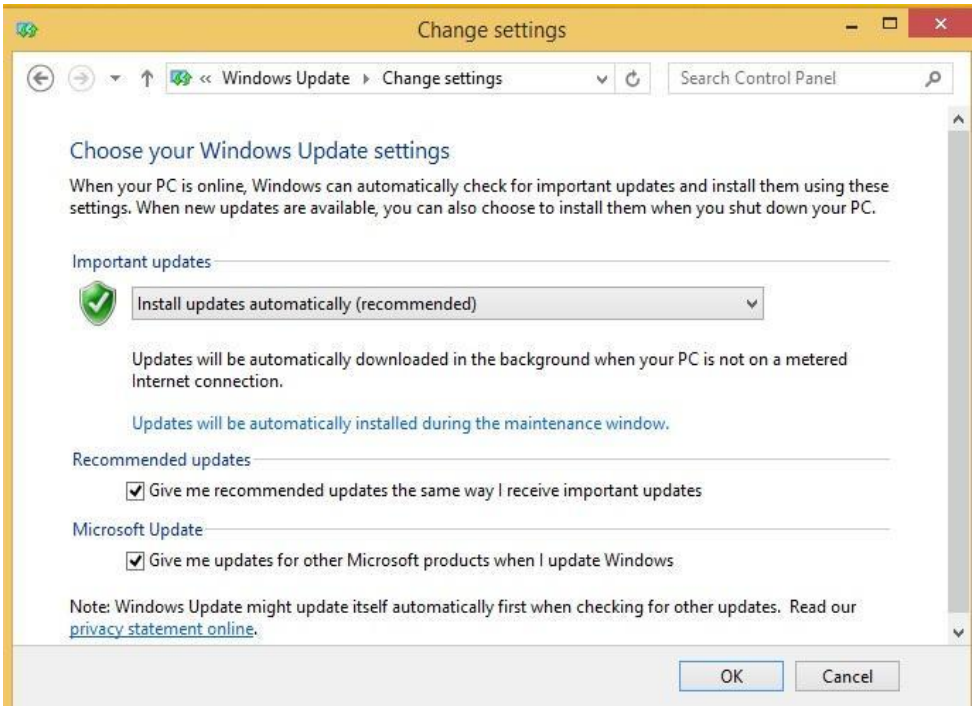
٣. نلاحظ وجود العديد من التنبيهات الخاصة بالنظام الأول خاص بتحديث ويندوز والآخر خاص بإعدادات الجدار الناري، قم بالدخول على هذه التنبيهات ومن ثم حلها. اضبط إعدادات الجدار الناري ليكون بوضع التشغيل.

رابعاً: تأكد من ضبط تحديث نظام التشغيل على الوضع الآلي:

تمرين عملي(٧):

تأكد من ضبط تحديث نظام التشغيل على الوضع الآلي بتطبيق الخطوات التالية:

١. من ابدأ "Start" قم باختيار لوحة التحكم "Control Panel" ومن ثم "System security" ومن ثم قم باختيار "Windows Update" ومن ثم اختر " Turn Automatic Windows update On or off":



الشكل 36-1: ضبط تحديث نظام التشغيل ويندوز

٢. تأكد من اختيار "Install update automatically" كما في الشكل (٣٦-١).

خامساً: استخدم "Windows Defender":

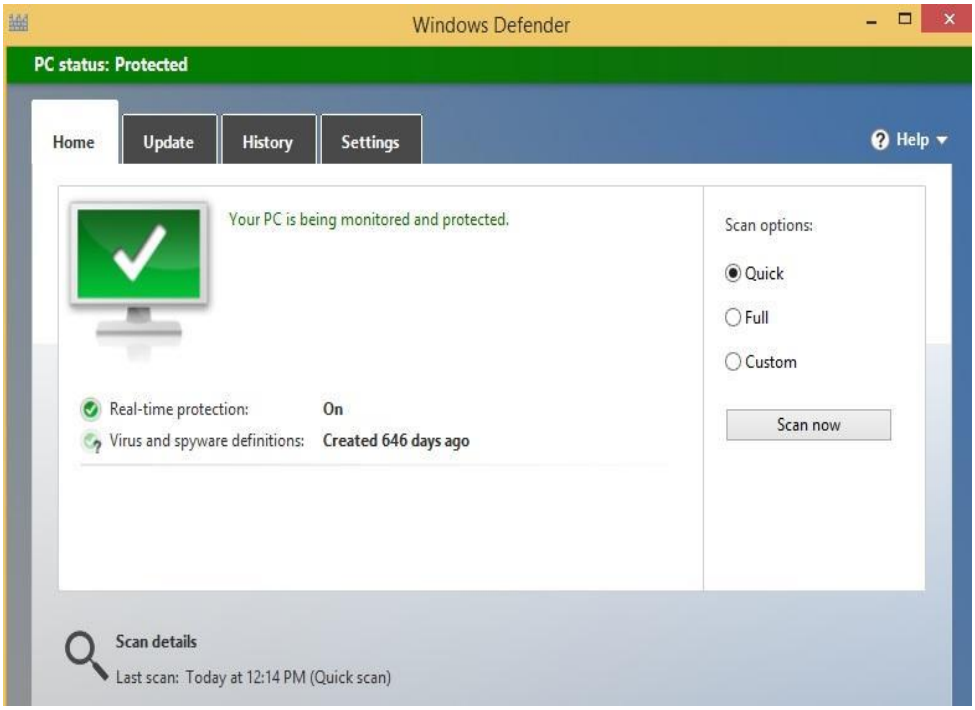
يتيح لك نظام تشغيل ويندوز إمكانية الدفاع عن أغلب تهديدات الإنترنت من خلال " Windows Defender". يعمل هذا النظام بوضع التشغيل بشكل آلي، ولكن إذا اعتقدت أن جهازك تعرض لهجوم معين من خلال الإنترنت (ديدان، برمجيات ضارة، إلخ..) يمكنك تشغيل عملية التفحص يدوياً لهذا النظام. حيث سيتمكن هذا النظام من التخلص من هذا الهجوم.

تمرين عملي(٨):

للتشغيل اليدوي ل "Windows Defender" قم بتطبيق الخطوات التالية:

*ملاحظة:

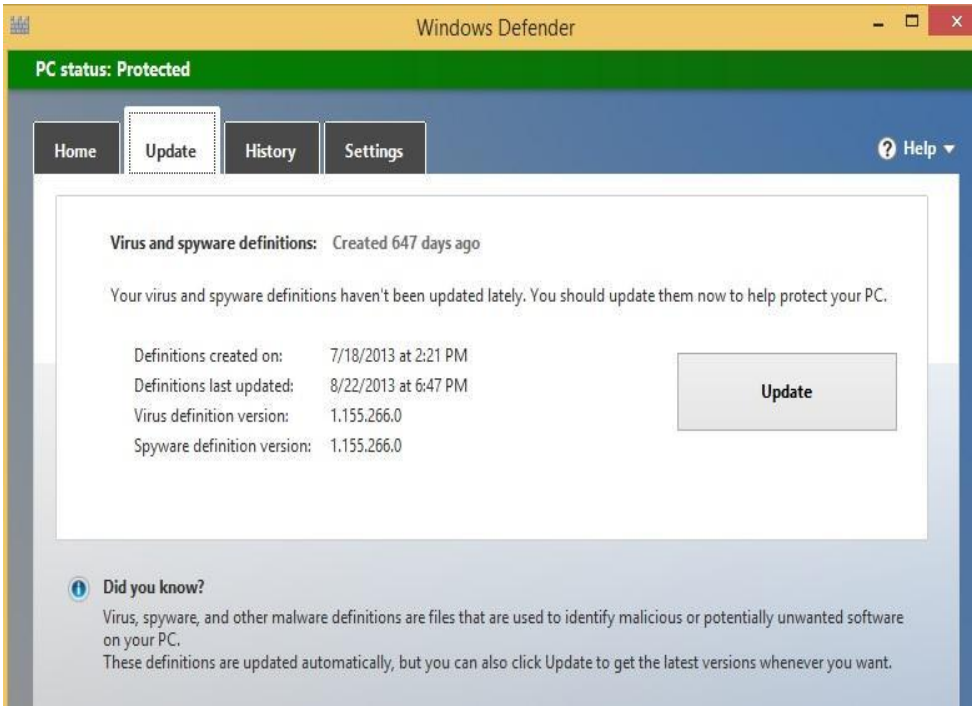
١. من ابدأ "Start" من بحث "Windows Defender"، ستظهر لك الشاشة الرئيسية كما في الشكل (٣٧-١):



الشكل 37-١: الشاشة الرئيسية لبرنامج Windows Defender

٢. قم باختيار نمط التفحص، حيث يتيح لك "Windows Defender" ثلاثة أنواع من طرق التفحص.

٣. تأكد من تحديث "Windows Defender" من خلال اختيار "Update" كما في الشكل (٣٨-١):



الشكل 38-١: تحديث برنامج Windows Defender

سادساً: تثبيت برنامج تنظيف ملفات التسجيل "Ccleaner":

يعتبر هذا البرنامج من البرامج القادرة على تسريع أداء الحاسوب. حيث يستخدم للتخلص من ملفات زائدة استقرت في التسجيل(Registry) كذكرى لبرامج قام المستخدم بحذفها لكنها لم تنظف وراءها بشكل كامل. بالإضافة إلى أن البرنامج يقوم بالعديد من الأوامر التي تقوم بإصلاح النظام. حيث يقوم بعملية فحص على الرجستري ويقوم أيضاً بمسح الصور وملفات الفلاش والصفحات المؤقتة من المتصفح. يُنصح بتثبيت هذا البرنامج، عندئذ لا أحد يستطيع معرفة إلى أين وصل المستخدم في تصفح الإنترنت، ويساعد على حذف ملفات لا حاجَة لها وتشغل حجما في القرص الصلب.

خصائص البرنامج:

- تسريع الجهاز
- تسريع الإنترنت وإصلاح مشكلات الاتصال الشائعة وأخطاء DNS وتحسين التصفح.
- تنظيف الجهاز على أجهزة Windows،MAC .
- حماية الخصوصية على الإنترنت بحذف ملفات التتبع والكوكيز وحذف السجل عند إنهاء الصفحة.
- إزالة تثبيت البرامج بسهولة وقوة عن طريق حذف الملفات التي تتركها البرامج أو قيم ملفات التسجيل إذا ما تم إزالتها بالطريقة الاعتيادية الخاصة بنظام الويندوز.
- حذف الملفات الضارة التي تؤثر سلباً على أداء وسرعة جهازك.
- إصلاح أخطاء نسخ الويندوز الشائعة والتي تلاحظ بكثرة عند استخدام النسخ غير الأصلية.

- صيانة الجهاز بطريقة سريعة دون الحاجة إلى خبرة ومراكز صيانة.
- إزالة الملفات الخاملة والتي تستهلك مساحات من القرص الصلب دون أدنى فائدة منها.
- إصلاح ملفات التسجيل (Registry) وذلك بحذف القيم غير المستخدمة.

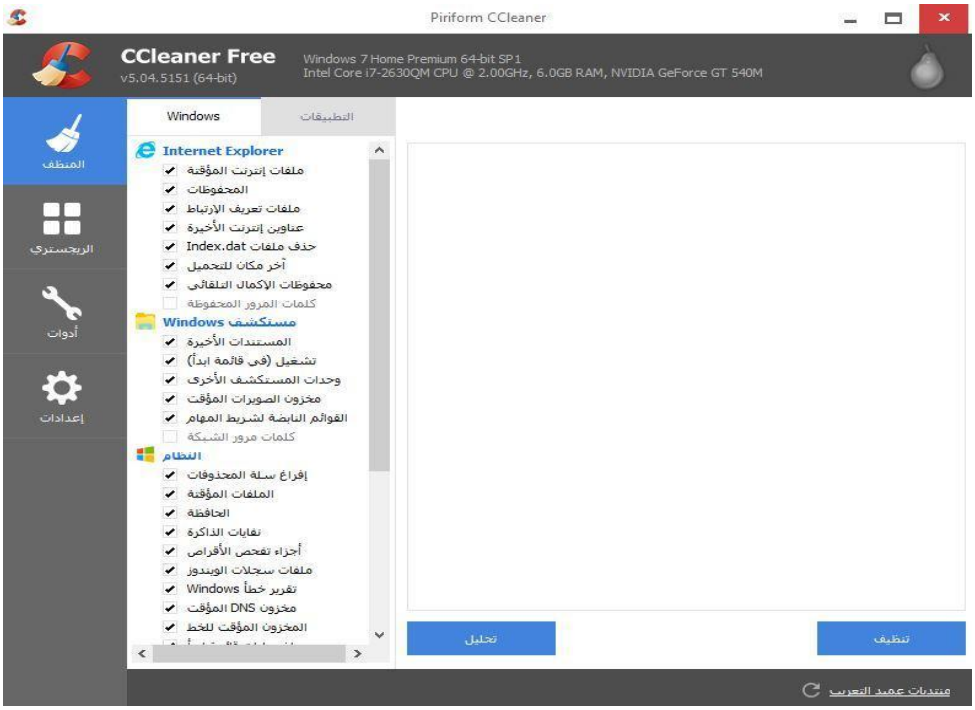
تمرين عملي(٩):

لتثبيت البرنامج، قم بتطبيق الخطوات التالية:

١. يمكن الحصول على نسخة مجانية من البرنامج عن طريق البحث في جوجل "CCleaner" أو عن طريق الرابط التالي:

https://www.piriform.com/ccleaner/download

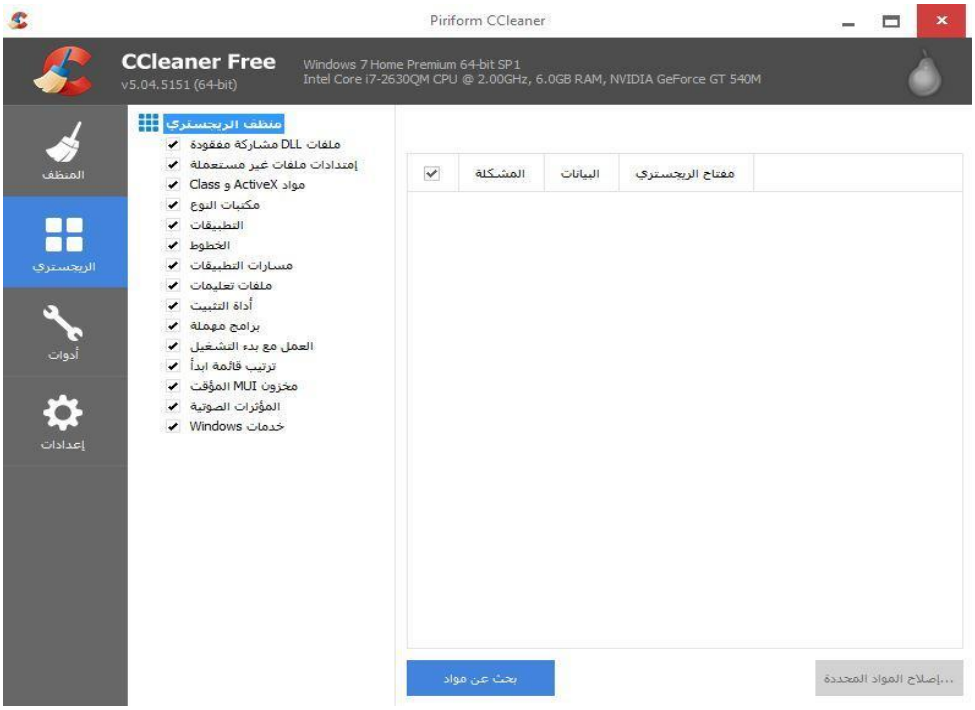
بعدها ستظهر لك الواجهة الرئيسية للبرنامج كما في الشكل (٣٩-١):



الشكل 39-١: الشاشة الرئيسية لبرنامج Ccleaner

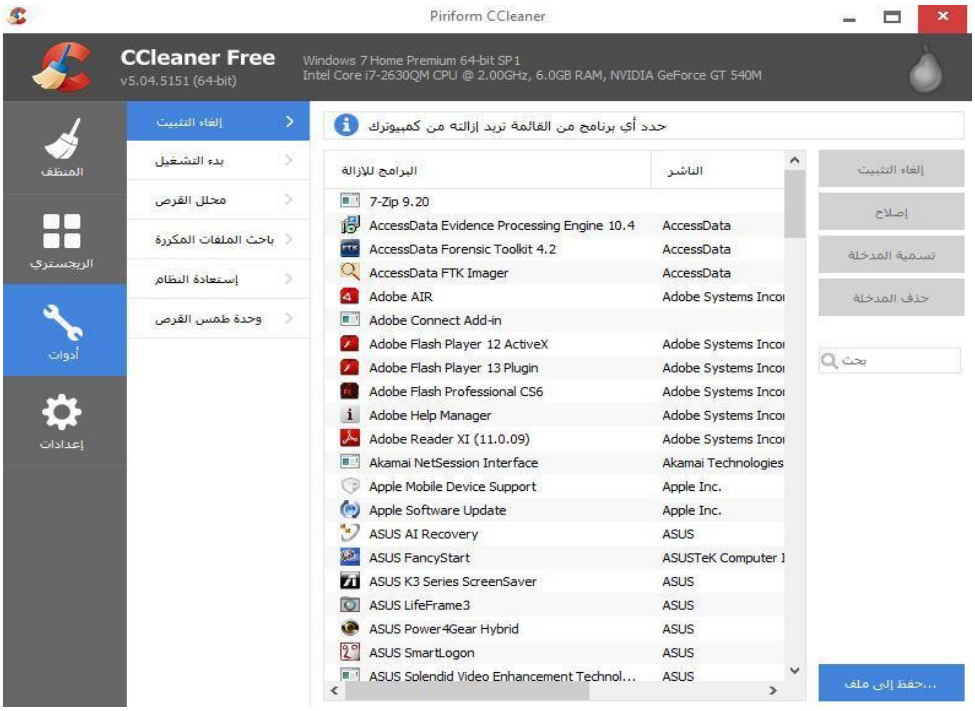
تتيح هذه الواجهة اختيار الملفات المراد فحصها إما للتطبيقات المثبتة على الجهاز أو ملفات نظام التشغيل ويندوز

٢. كما يمكنك استعراض وتحليل ملفات النظام وإصلاحها عن طريق اختيار الرجستري كما في الشكل (٤٠-١):



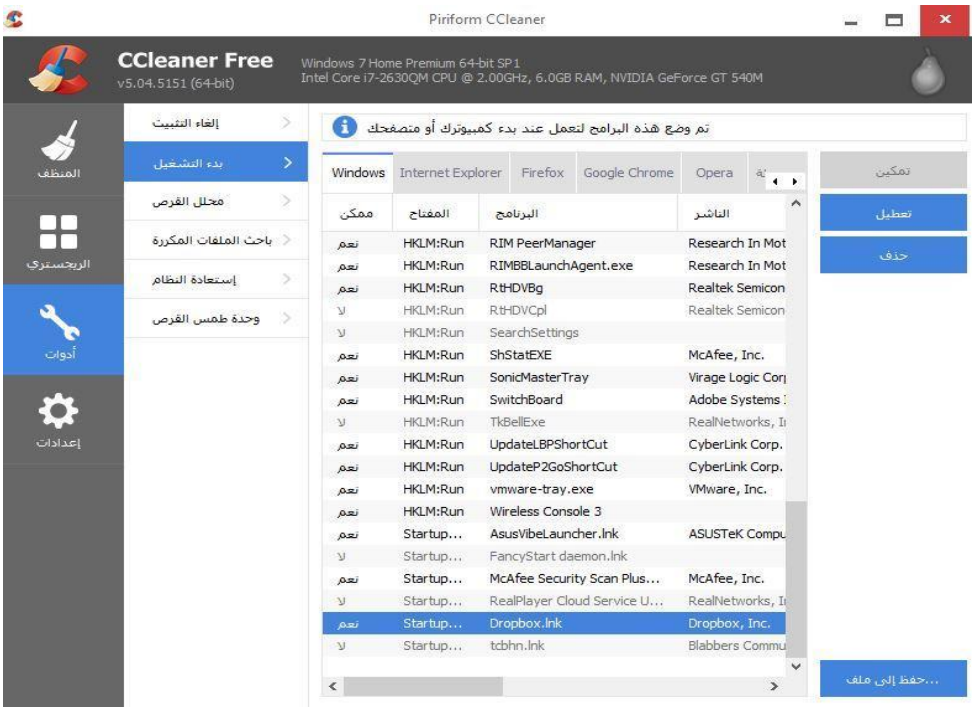
الشكل 40-١: شاشة استعراض ملفات النظام في برنامج Ccleaner

٣. من خيار الأدوات يمكنك استعراض العديد من الخدمات كإلغاء تثبيت البرامج التي لا يستطيع نظام التشغيل حذفها من تطبيق إزالة البرامج في لوحة التحكم



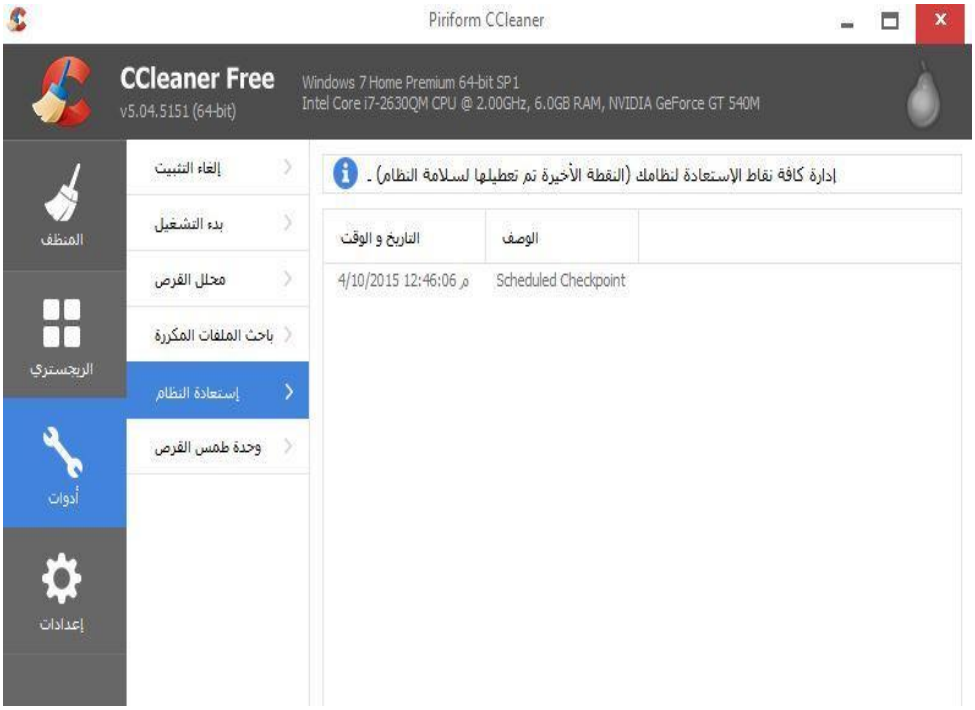
الشكل 41-١: الأدوات في برنامج Ccleaner

٤. يمكنك بالتحكم بالبرامج والملفات التي تعمل مع بدء التشغيل في النظام كما في الشكل (٤٢-١):



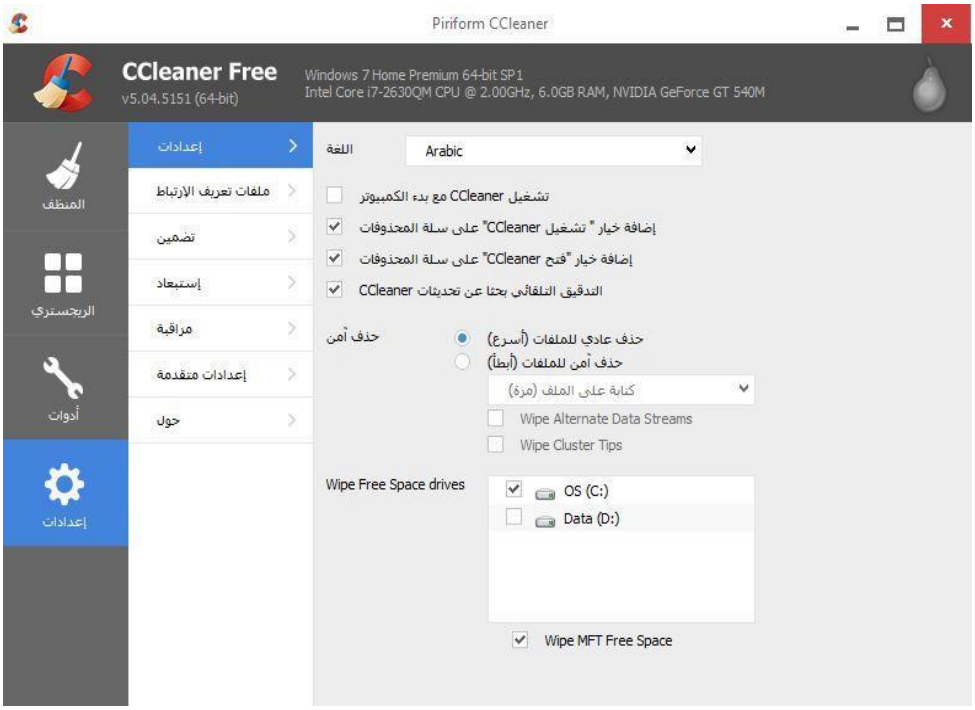
الشكل 42-١: التحكم في البرامج وملفات النظام التي تعمل مع بدء التشغيل من خلال برنامج Ccleaner

كما يتيح البرنامج إمكانية استعادة ملفات النظام في حالات حدوث خلل كما في الشكل (٤١-١):



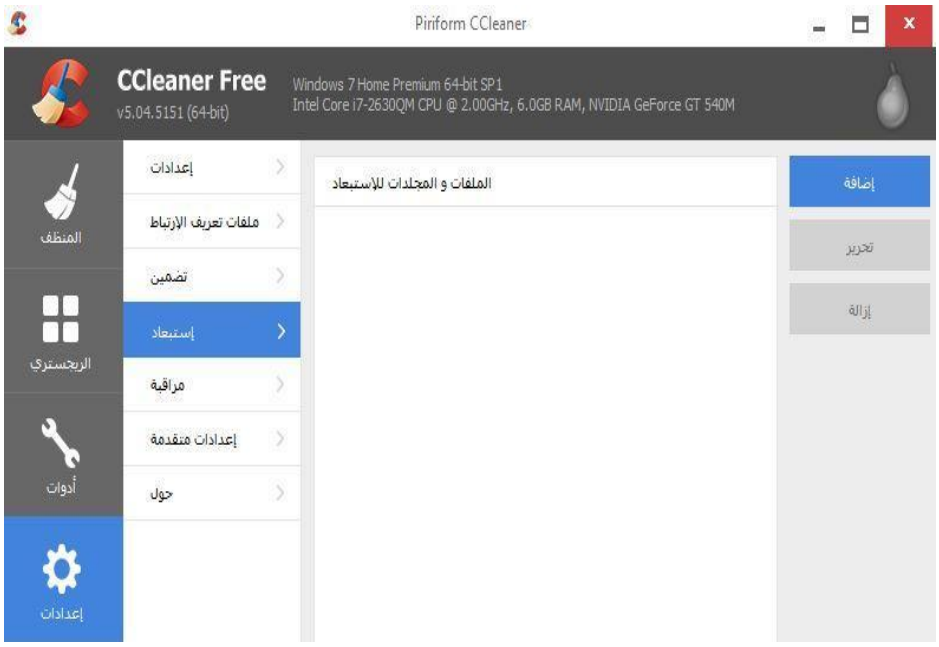
الشكل 43-١: استعادة ملفات النظام من خلال برنامج Ccleaner

ومن خيار الإعدادات يمكنك التحكم بإعدادات البرنامج كاللغة وخيارات تشغيل البرنامج كما في الشكل:



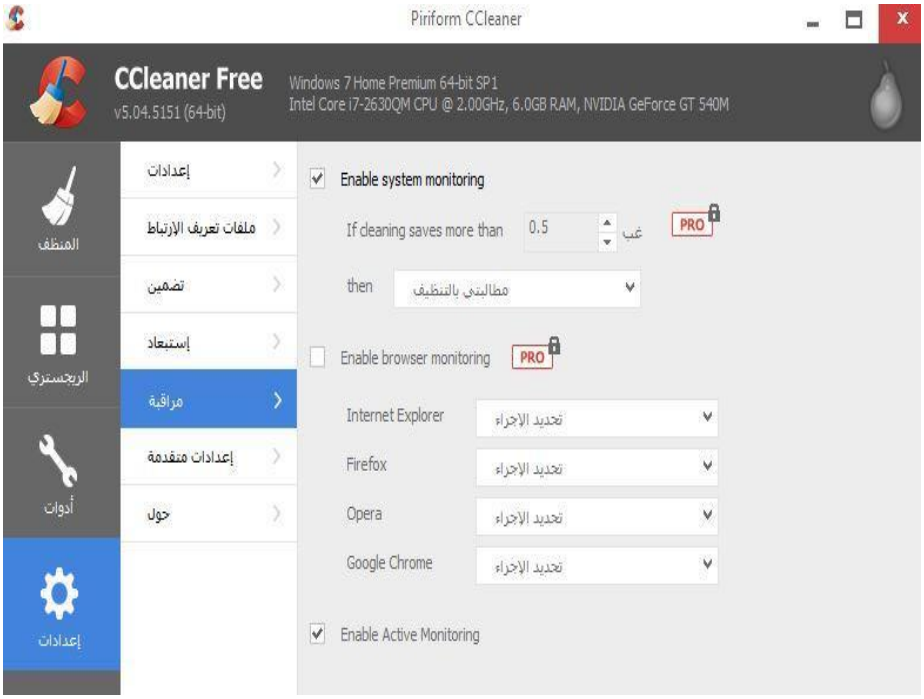
الشكل 44-١: الإعدادات العامة في برنامج Ccleaner

٥. يمكنك خيار استبعاد من تحديد بعض المجلدات في جهازك التي تستثنيها من عمل التنظيف كما في الشكل (٤٥-١):



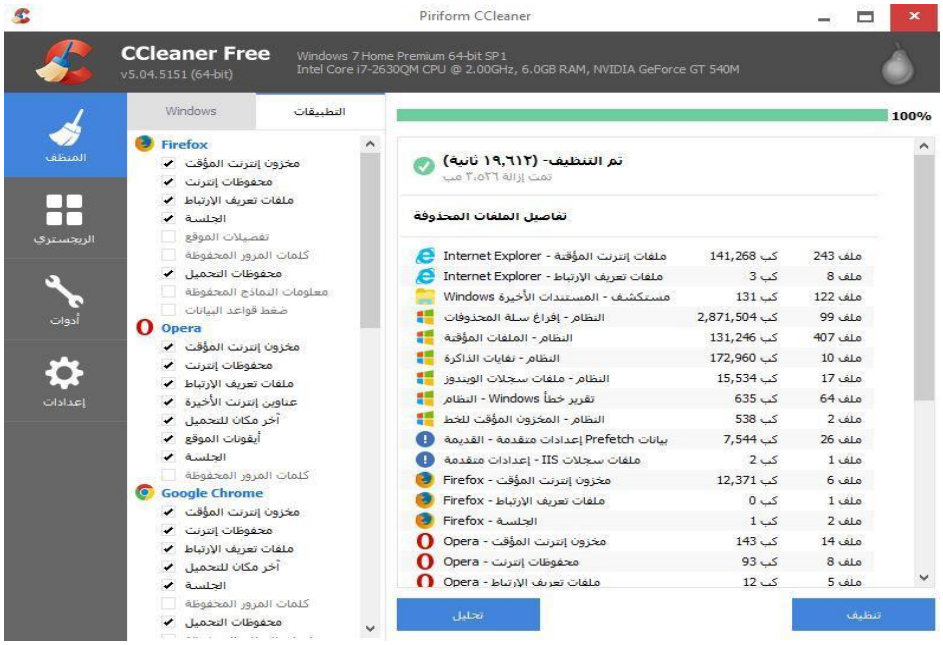
الشكل 45-١: خيار الاستبعاد للمجلدات في برنامج Ccleaner

كذلك يمكن اختيار مراقبة لضبط إعدادات المراقبة الدورية لجهازك



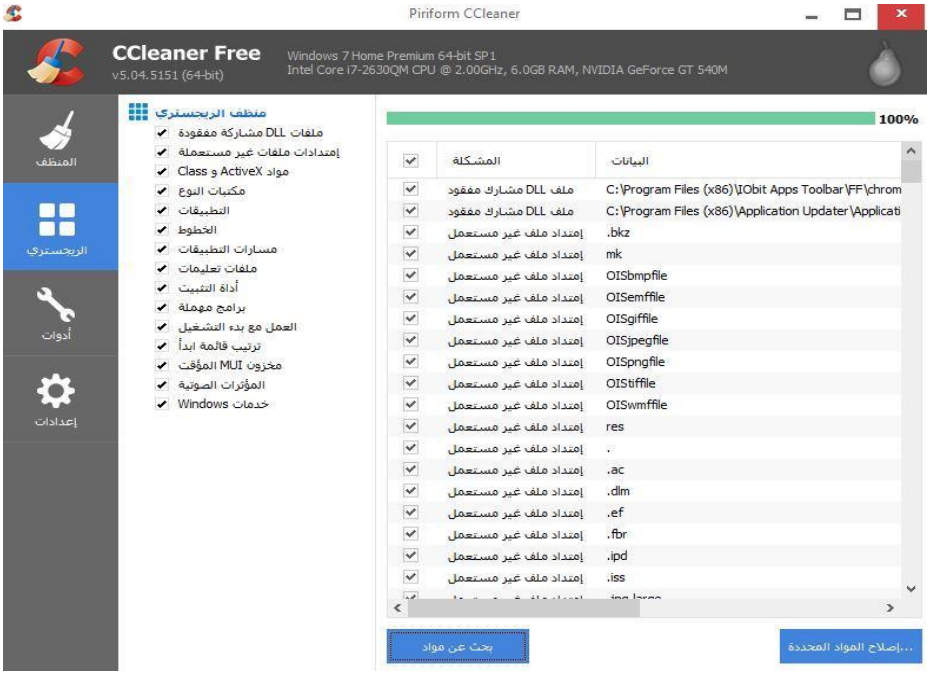
الشكل 46-1: خيار المراقبة من خلال برنامج Ccleaner

٦. الآن بعد الإلمام بالخصائص التي يتيحها هذا البرنامج اذهب إلى واجهة البرنامج الرئيسية وقم باختيار تحليل ومن ثم تنظيف للقيام بإزالة الملفات الخاملة في جهازك كما في الشكل(٤٧-١):



الشكل 47-1: خيار التنظيف في برنامج Ccleaner

٧. بعد ذلك اذهب لخيار الرجيستري ومن ثم اختر بحث عن المواد ليقوم البرنامج بالبحث عن المشكلات في ملفات التسجيل(Registry) ومن ثم إصلاحها كما في الشكل (٤٨-١):



الشكل 48-١: البحث عن مشكلات في ملفات النظام من خلال برنامج Ccleaner

٨. كما يتيح البرنامج عمل نسخة احتياطية لملفات التسجيل(Registry) كما في الشكل) ٤٩-١):

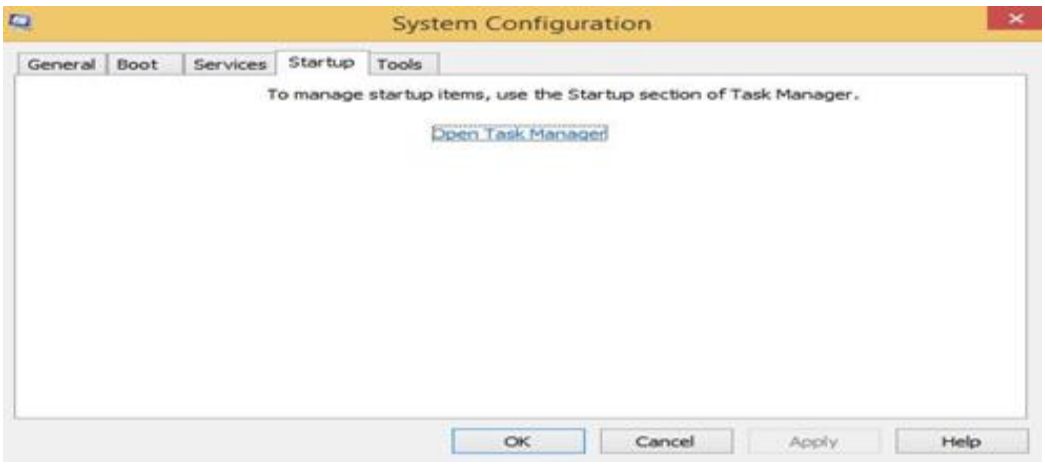
الشكل 49-١: النسخ الاحتياطي في برنامج Ccleaner

سابعاً: التأكد من برامج بدء التشغيل:

معظم مستخدمي الكمبيوتر يعانون من بطأ في الأقلاع، وخاصة عند تركيب برامج مثل RealPlayer و Skype وغيرها، وربما تكون هناك برامج تعمل في الخفاء مثل برامج القرصنة. يفضل دائمًا تفقد البرامج التي تعمل مع تشغيل الجهاز بشكل آلي بدون أي أمر من المستخدم، من أجل تسريع أقلاعه، والتأكد من خلو نظام التشغيل من برامج مجهولة المصدر تعمل بدون علمك مع بدء التشغيل. الطريقة في التحكم بهذه البرامج كالتالي:

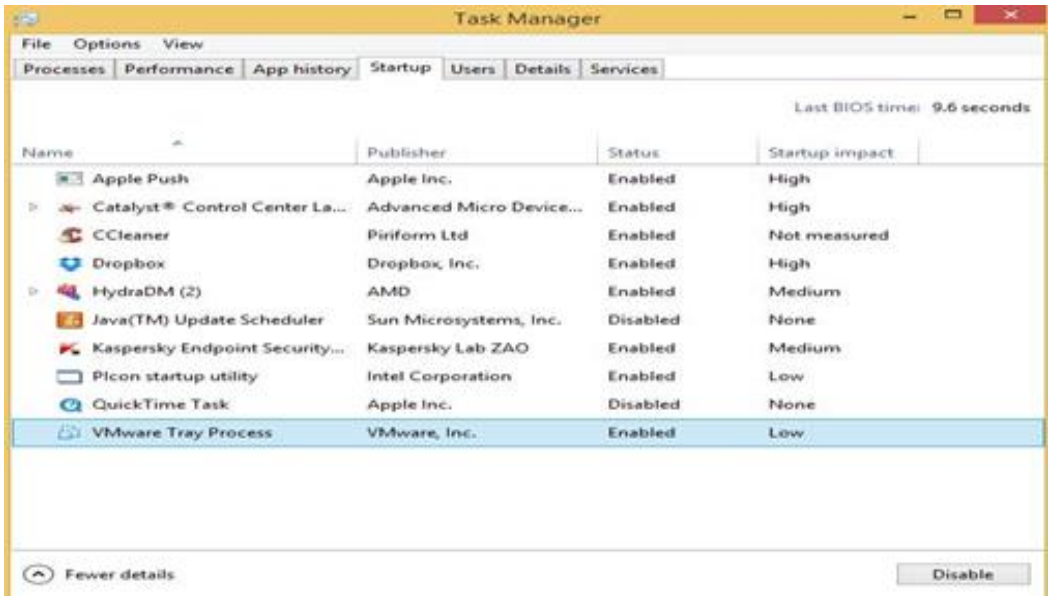
تمرين عملي(١٠):

١-قم بفتح نافذة التشغيل بالضغط على (علامة الويندوز+ r) اكتب Msconfig عندها ستظهر لك الشاشة كما في الشكل (٥٠-١):



الشكل ٥٠-١: نافذة التشغيل في نظام ويندوز

٢-من القائمة العلوية، اختر Startup ومن ثم Open Task Manager:



الشكل ٥١-١: مدير المهام في نظام التشغيل ويندوز

عندها ستظهر لك قائمة البرامج التي تعمل مع بدأ تشغل النظام مباشرة. لاحظ وجود معلومات عن كل برنامج تشتمل على مصدرة وحالته ومدى تأثيره على النظام.

قم بتفحص هذه البرامج وتأكد من إذا كنت تحتاجها أثناء بدء التشغيل أم لا. من الممكن أن تجد في جهازك بعض البرامج التي تعمل مع بدء التشغيل ومصدرها مجهول ولا تعرف ماهي وظيفة هذا البرنامج. كل ما عليك هو اختيار هذا البرنامج ثم اضغط على Disable، عندها سيلغى هذا البرنامج

من قائمة البرامج التي تعمل مع بدء التشغيل. يتطلب عليك بعد ذلك البحث عن هذا البرنامج والتأكد من وظائفه ومصدره.

مناقشة: بعد تطبيق الخطوات السابقة قم باستعراض البرامج الموجودة في قائمة بدء التشغيل ثم أجب عن الأسئلة التالية:

- ما هو عمل هذه البرامج؟
- هل يوجد برنامج مجهول المصدر ولا تعرف وظيفته؟ ما هو اسم هذا البرنامج؟
- ناقش مع مدربك هذه البرامج وتعرف ما إذا كانت برامج ضارة أو تؤثر على عمل الجهاز.

ثامناً: التأكد من التخلص من ملفاتك الخاصة:

الكثير منا يحتفظ بملفات مهمة دائما على حاسوبه الشخصي وهذه الملفات قد تحتوي بعض من الخصوصيات والأمور المهمة التي يجب ألا يطلع عليها أحد. وقد تلجأ في بعض الأحيان للتخلص من هذه الملفات عن طريق حذفها من الحاسوب ومن على مساحة القرص الصلب، لكن للأسف الكثير لا يعلم أنه فعليا لم يتخلص من هذه الملفات المهمة بعد حذفها ومن الممكن أن يتم استعادتها مرة أخرى حتى بعد عملية فورمات كاملة للقرص الصلب

كيف يتم هذا؟ لنتخيل أن الملفات كأنها صفحات في كتاب، عندما تقوم بحذف ملف فإنك تقوم بحذف صفحة من الكتاب ولكنها تبقى خارج الكتاب لذلك فإن الصفحة مازالت موجودة ولكنها غير معروفة في أي مكان كانت موجودة في الكتاب. هذا المكان هنا هو بمثابة "sector" فالقرص الصلب لا يعرف شيء يسمى ملفات ولكنه يتعامل مع "sectors" فقط وهي أجزاء صغيرة من البيانات غالبا تكون ٥١٢ بايت ونظام الملفات مثل نظام NTFS مهمته هو ترجمة هذه الـ sectors لملفات حتى يستطيع التعامل معها نظام التشغيل.

نظام الملفات يعمل على بناء جدول للملفات، هذا الجدول يحتوي في كل صف على اسم الملف ومكان sector الخاص به على القرص الصلب. لذلك عندما تقوم بحذف ملف ما من نظام التشغيل فكل ما تم حذفه هو معلومات هذا الملف من ملفات ونقوم بترك فراغ في الجدول لملف آخر.

قد يستخدم نظام التشغيل هذا المكان في الجدول لاحقا وقد لا يستخدمه في حالة عدم استخدامه والكتابة عليه مرة أخرى بمعلومات جديدة فمازالت عملية استعادة الملفات ممكنة وذلك عن طريق بعض البرامج المتخصصة والمبرمجة من قبل خبراء في هذا المجال مثل برنامج testdisk أو Recuva المجاني والذي سنقوم باستخدامه في وقت لاحق في هذه الحقيبة.

الآن فأن وسيلة حذف الملفات بالطريقة التقليدية من نظام التشغيل هي غير آمنة وتعرض ملفاتك للخطر واحتمالية استرجاع الملفات واستعادتها مرة أخرى. لذلك يجب عليك حذفها بشكل كامل والحذف هنا بشكل كامل يطلق عليه shredding أو wiping.

تمرين عملي(١١):

طريقة حذف الملفات بصورة نهائية:

طريقة التخلص وحذف الملفات نهائيا وبشكل أمن من القرص الصلب هي عن طريق إعادة الكتابة على نفس sector بمعلومات أخرى تحل محل القديمة. بمعنى أنك تقوم بعمل إعادة كتابع على موقع البيانات القديمة بأخرى جديدة. فهذا يجعل من استعادة الملفات القديمة مرة أخرى عملية مستحيلة. هنالك العديد من البرامج التي تقدم هذه خاصية حذف الملفات بشكل كامل وبالتالي يستحيل استعادتها. من ضمن تلك البرامج "Eraser"

تطبيق استخدام برنامج "Eraser":

١-قم بتحميل وتثبيت برنامج "Eraser" عن طريق البحث عنه باستخدام جوجل أو عن طريق الرابط التالي: http://eraser.heidi.ie/download.php

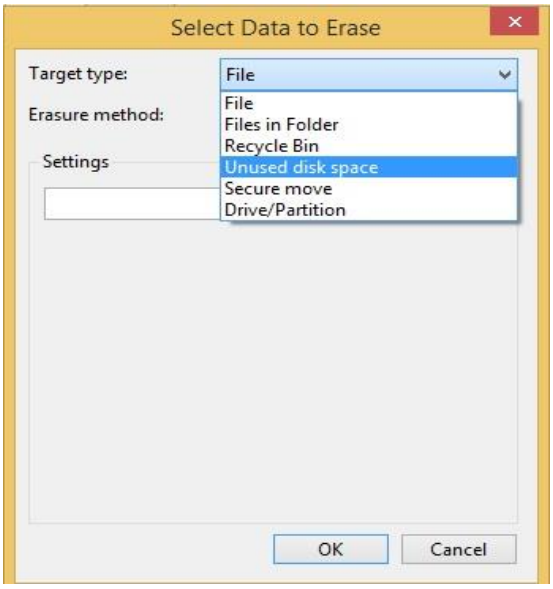
٢-بعد عملية التثبيت، قم بالضغط بزر الفأرة الأيمن على الملف المراد حذفه نهائياً وسيظهر لك خيار "Eraser" كما في الشكل (٥٢-١):

الشكل ٥٢-١: خيارات تثبيت برنامج Eraser

عندها سيقوم البرنامج بحذف الملف بشكل نهائي من الجهاز.

*ملاحظة: يتيح هذا البرنامج خاصية "Unused disk space" حيث تقوم هذه الخاصة بحذف المساحة الفارغة من جهازك والتي سبق أن تم التخزين عليها. تستخدم هذه الخاصية لحذف الملفات التي حُذفت بشكل عادي في السابق ويخشى المستخدم إمكانية استرجاعها. لكن هذه العملية قد تأخذَ وقت طويل عند تنفيذها لأنها تقوم بإعادة الكتابة على جميع المساحات الفارغة في الذاكرة. ينصح باستخدام هذه الطريقة قبل بيع جهازك الخاص أو التخلص منه.

يمكن الوصول إلى هذه الخاصية من شاشة البرنامج الرئيسة "Erase Schedule" ومن ثم " New Task"، بعد ذلك "Add date"، ومن ثم "Task Type" عندها ستظهر لك الشاشة التالية:



الشكل ٥٣-١: خيار تنظيف المساحة الغير مستخدمة في اجهاز

قم باختيار "Unused Disk Space" ومن ثم "OK"

اليوم الأول - الجلسة التدريبية الثالثة

أمن المعلومات للأجهزة النقالة

أصبحت الأجهزة النقالة كالهواتف الذكية والأجهزة اللوحية من أكثر التقنيات التي نستخدمها في حياتنا اليومية. كثرة الإقبال على مثل هذه الأجهزة أدى إلى إنشاء الكثير من التطبيقات لهذه الأجهزة النقالة. هذه التطبيقات تتيح لنا الاستفادة من العديد من الخدمات المقدمة من قبل المطورين كالتواصل فوراً مع الآخرين، التدريب على مهارات معينه أو فقط من أجل التسلية. [١]

الأجهزة النقالة لازالت تمثل مصدر قلق على كثير من مسؤولي أمن المعلومات في الشركات والمنضمات الحكومية. هذا القلق سببه كمية المعلومات الهائلة الخارجة من سيطرة مسؤول أمن المعلومات في المؤسسة بمجرد مرورها من خلال الأجهزة النقالة. كثرة امتلاك هذه الأجهزة عند الأفراد في وقتنا الحاضر أدت إلى زيادة كبيرة للتهديدات الأمنية في الكثير من المؤسسات. مما لا شك فيه أن هذه التهديدات تضع على عاتق المؤسسة مهمة حماية المعلومات من هذه التهديدات بشكل متنامي مع كثرة استخدام الأفراد لهذه الهواتف. هذا وتكلف المؤسسات مبالغ باهضة في ضل التزايد المتنامي لتطبيقات الهواتف النقالة التي يستخدمها الكثير من الأفراد بدون النظر إلى الصلاحيات التي يصل إليها التطبيق بمجرد قبول شروط تثبيته. في دراسة حديثة أجريت عام ٢٠١٤ للتحقق من نمو استخدام الهواتف النقالة في المؤسسات وتأثيراتها في كل من الولايات المتحدة الأمريكية وبريطانيا وألمانيا وأستراليا وجدت ما يلي:

١-عدد الأجهزة النقالة المتصلة بشبكات المؤسسات في تزايد مستمر:

٧٥% من المؤسسات تسمح بالأجهزة الشخصية للاتصال بشبكات الشركات، بزيادة من ٦٧% في عام ٢٠١٣ و٦٥% في عام ٢٠١٣.

٢ -حوادث أمن الأجهزة النقالة للشبكة في تزايد مما يؤدي إلى زيادة تكاليف إصلاحها:

- ٨٢% من خبراء أمن المعلومات يتوقعون زيادة حوادث أمن الأجهزة النقالة في هذه السنة.
- ٩٨% لديهم قلق من تأثير الحوادث الأمنية للأجهزة النقالة.
- ٩٥% يواجهون تحديات مع الأمان مع تزايد استخدام الأجهزة النقالة.
- ٦٤% يقولون إن تكاليف إصلاح ما تسببه حوادث الأجهزة النقالة للشبكة في تزايد.
- ٤٢% من المديرين التنفيذيين يقولون أن التأثيرات الضارة لاستخدام الأجهزة النقالة تكلف أكثر من ٢٥٠٠٠٠ دولار.

٣ -سلوك الموظف وطريقة استخدامه للأجهزة النقالة عامل مهم في أمن المعلومات:

٨٧% يقولون إن إهمال الموظف يمثل تهديد أكبر من مجرمي الإنترنت، ارتفاعاً من ٧٢% عام ٢٠١٢

أفعال الموظفين تمثل التأثير الأكبر على ثغرات البيانات المتنقلة.

٩٢% يقولون إن سلوكيات الموظف قد جعلت فرق في منع الخروقات الأمنية رفيعة المستوى.

هذا الدراسة تبين مدى الخطر الكبير على أمن المعلومات في المؤسسات الحكومية والشركات. بناء على ذلك لا بد من نشر الوعي بين المستخدمين لهذه الأجهزة النقالة من أجل الحد من هذه الأخطار. من أجل ذلك لابد من اتباع هذه الخطوات:

تأكد دائماً من أنك تحصل على التطبيقات من مصدر موثوق وأمن: بإمكان أي شخص عمل تطبيق ونشره في الإنترنت، لذلك يجب الحذر من مصادر هذه التطبيقات والتأكد منها قبل تثبيتها على جهازك. يقوم الكثير من مطوري تطبيقات الهاتف بإنشاء ونشر تطبيقات تبدو مفيدة للمستخدمين لكنها في الحقيقة مؤذية. حيث بمجرد قيامك بتثبيت هذه التطبيقات يمكن لهؤلاء المطورين السيطرة على جهازك النقال والوصول إلى جهات الاتصال الخاصة بك، قراءة رسائل البريد الإلكتروني وقد تصل أحياناً إلى الاستماع لمحادثاتك الصوتية. فلذلك التأكد من مصدر التطبيق واستعراض وجهات النظر عنه يقلل من فرصة تثبيت تطبيق مؤذي على جهازك.

على سبيل المثال أجهزة الآبل مثل الآي فون والآيباد بإمكانها الحصول على تطبيقات معروفة المصدر من خلال متجر أبل للتطبيقات. فدائماً المتجر يحرص على أن تكون التطبيقات الموجودة فيه من مصدر معروف مع وجود شروط معينه لإضافة تطبيقك عليه مثل عرض الصلاحيات التي سيقوم التطبيق بالوصول إليها أثناء التثبيت. مما يعني أنه سيمكنك من معرفة صلاحيات الوصول لهذا البرنامج قبل قبول تثبيته. رغم ذلك قد لا يستطيع متجر أبل من اكتشاف جميع البرامج المؤذية لكثرة التطبيقات المرفوعة عليه، لكن تحرص أبل على إزالة البرنامج المؤذي بسرعة من متجرها إذا تم اكتشافه.

على الجانب الآخر الأجهزة النقالة التي تعمل بنظام الأندرويد تسلك منهجاً مختلفاً من ناحية الأمان. فهذه الأجهزة تعطيك مرونة أكثر من ناحية تحميل التطبيقات من مواقع متعددة على شبكة الإنترنت يصعب حصرها. لكن هذه المرونة من الممكن أن تمثل تهديداً حقيقياً لجهازك النقال فلابد أن تتحمل مسؤولية هذه التطبيقات لأن بعضها قد يكون مطعماً بالفيروسات أو يأخذ الصلاحيات بمجرد تثبيته بدون أخذ إذن منك. علماً بأن شركة جوجل المطور لنظام أندرويد قد وضعت متجراً مشابهاً لفكرة متجر أبل يسمى جوجل بلي. حيث أن التطبيقات التي توجد فيه قد تمت مراجعتها بشكل أساسي. فلذلك من الأفضل إذا كنت من مقتني الأندرويد تحميل التطبيقات من المتجر الخاص به فقط.

ولتجنب المخاطر بشكل أكبر تجنب تثبيت التطبيقات الجديدة والتي لم يقم بتثبيتها إلا عددا قليل من الناس، فلا بد من التأكد أولاً من التعليقات التي كتبت عن هذا التطبيق. فغالباً كلما مضى وقت أطول للتطبيق في المتجر دل على الأرجح أنه موثوق به. كذلك تجنب اختراق نظام التشغيل الخاص بك من أجل تثبيت التطبيقات غير المعتمدة أو الحصول عليها بشكل مجاني لأنه يؤدي إلى تعطيل الكثير من الضوابط الأمنية في جهازك. [١]

تأكد من الصلاحيات التي يستطيع التطبيق الوصول إليها: بعد تثبيت التطبيق من مصدر موثوق، يجب التأكد بعد ذلك من إعداده بأمان وأنه يحمي خصوصياتك. تتطلب أغلب البرامج صلاحيات معينه في جهازك كالوصول إلى ألبوم الصور، الكاميرا أو الرسائل النصية. فلابد من التفكير قبل إعطاء الصلاحيات هل يحتاج هذا التطبيق الوصول إلى هذه الصلاحية فعلاً من أجل القيام بعملها؟ فعلى سبيل المثال تطلب تطبيقات الخرائط المختلفة الوصول إلى معرفة موقعك، فمن غير الممكن لهذه البرامج العمل بكفاءة دون الحصول على هذه الصلاحية. مثال آخر تتطلب بعض برامج المحادثة الفورية الوصول إلى أرقام دليل الهاتف في جهازك النقال من أجل معرفة الأشخاص الذين يمتلكون نفس التطبيق للدردشة معهم. على الجانب الآخر تتطلب بعض البرامج صلاحية الوصول إلى الرسائل النصية على الرغم من عدم حاجتها لذلك فلابد من تعطيل هذه الصلاحية من الإعدادات أو حذف التطبيق.

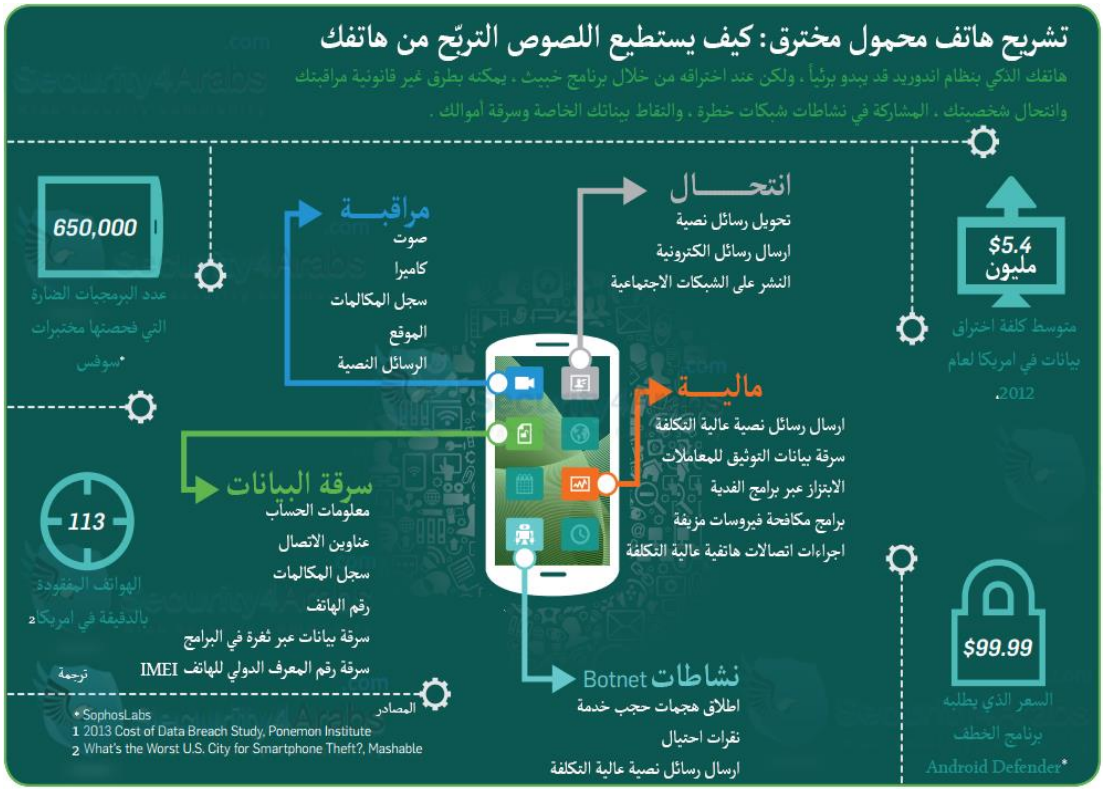
تأكد من تحديث التطبيق: تطبيقات الأجهزة النقالة شأنها كشأن أنظمة التشغيل وتطبيقات أجهزة الحاسوب الشخصية. فمجرمو الإنترنت دائماً ما يبحثون عن بعض الثغرات في التطبيقات من أجل الوصول إلى بعض المعلومات المهمة في الجهاز النقال أو من أجل التحكم الكامل به. على الجانب الآخر يسعى العديد من مطوري التطبيقات على إنشاء تحديثات مستمرة للتطبيقات من أجل إصلاح تلك الثغرات. أغلب التطبيقات تتيح لك بوجود خيار التحديث الآلي لها مما يساعد على إغلاق هذه الثغرات وإضافة الكثير من الخصائص بشكل دوري. فمن الأفضل تفعيل هذا الخيار أو التأكد يدوياً بشكل أسبوعي من التحديثات المتاحة لتطبيقات جهازك النقال. ومع ذلك تأكد دائماً بأن هذه التحديثات لم تضف صلاحيات ليس لها علاقة بعمل التطبيق على جهازك. [٢]

الخطوات الأساسية لتأمين جهازك النقال:

- قم بتفعيل خصائص الحماية في جهازك النقال، حيث تتيح أغلب الأجهزة على خصائص معينه للحماية. يجب عليك الاطلاع عليها ومعرفتها ومن ثم استخدامها.
- يجب إضافة رقم (PIN) لجهازك النقال، عندئذ لن يستطيع المتلصصين من حولك الوصول إلى محتويات جهازك النقال بدون معرفة هذا الرقم السري.
- قم بتثبيت برامج مكافحة الفيروسات والبرمجيات الضارة على جهازك النقال من مزود موثوق خصوصاً إذا كنت من مستخدمي نظام أندرويد.
- إذا قمت بتفعيل خاصية البلوتوث على جهازك النقال، فأحرص على أن تكون مشغلة في وضع مخفي بحث لا يستطيع أن يراه الآخرون. هذا سيجعل عملية اكتشافه من قبل المخترقين المحيطين بك أكثر صعوبة. حيث يصعب على المخترقين معرفة عنوان البلوتوث إذا كان في هذا الوضع.

- عند استخدامك لشبكة لاسلكية، أحرص على أن تكون هذه الشبكة مشفرة ومن مصدر موثوق. سواء كانت هذه الشبكة خاصة أو مقدمة من شركة تجارية كما في المطارات وبعض الأماكن العامة.
- استخدم خاصية (Remote wipe) إذا كان جهازك النقال يحتوي على هذه الخدمة. وهي خاصية تسمح لك بمسح كافة بياناتك وحماية معلوماتك الشخصية عن بعد في حالة فقدت أو تمت سرقة جهازك النقال.

الجهاز المخترق وطريق استخدامه: لمعرفة أهمية حماية الجهاز النقال والمعلومات والصلاحيات التي يمكن للمخترق الحصول عليها، الشكل (٥٤-١) من تقرير شركة سوفس يوضح إمكانيات المخترقين بعد الوصول إلى جهازك النقال:



الشكل 54-١: تشريح هاتف محمول مخترق

كيف تتم عملية اختراق جهاز الضحية: هناك عدّة طرق يمكن المخترقون استخدامها لاختراق هواتف الضحايا، أسهلها هو متابعة أشهر البرامج في السوق ومن ثم تحميلها والتعديل عليها لزرع برامج خبيثة فيها ومن ثم طرحها مجددا في السوق الرئيسي أو الأسواق الأخرى. في حالة الحكومات أو غيرها من المنظمات الإجرامية يمكن أن يتم عبر إنشاء شركات وهمية تقوم بإصدار برامج مغرية يقوم المستخدمون العاديون بتحميلها ومن ثم إعطاء صلاحيات لها ولهم على هواتفهم. أما الطرق الأخرى للاختراق فتكون عبر استغلال ثغرة في نظام التشغيل نفسه أو في أحد البرامج الشرعية أو

تحويل المستخدمين إلى صفحات ويب وهمية لسرقة صلاحياتهم. الشكل (٥٥-١) يظهر كيف يقوم مطور خبيث بسرقة برنامج شرعي ومن ثم زرع برمجيته فيها ورفعها إلى سوق البرامج:

الشكل55 -١: كيف يقوم مبرمج خبيث بسرقة برنامج شرعي

أسئلة ونقاش(٤):

س١: برأيك لماذا أمن المعلومات في الأجهزة النقالة أمر مهم؟

س٢: ما الخطوات المهمة للحد من الأخطار التي تهدد الأجهزة النقالة؟

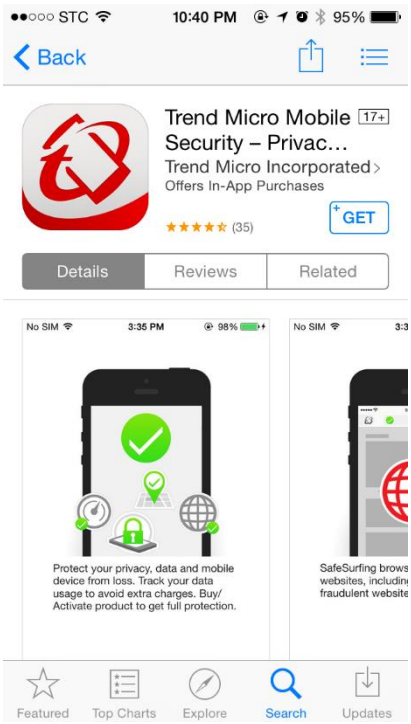
س٣: كيف تتم عملية الاختراق في الأجهزة النقالة؟

برامج الحماية الخاصة بالأجهزة النقالة: تصفح مختلف مواقع الإنترنت عن طريق الأجهزة النقالة والوصول إلى مواقع التواصل الاجتماعي والمواقع السياسية والاقتصادية والرياضية وأيضاً تحميل بعض الملفات والصور والأفلام وغير ذلك من خلال شبكة الإنترنت، يؤدي بدون أدنى شك للتعرض لخطر الفيروسات أو إمكانية سرقه جميع بياناتك. يعتبر الجهاز النقال معرض للضرر بالعديد من الأشكال، لذلك يجب عليك تحميل برنامج حماية على جهازك النقال لكي يقوم بمنع وصول أي نوع من أنواع الفيروسات لجهازك والتأكد من خلو المواقع من فيروسات قد تضر جهازك.

تمرين عملي(١٢):

- **تطبيق استخدام برامج حماية على الجهاز النقال:**

1-يقوم المتدربون من خلال نظام iso الخاص بأجهزتهم النقالة تثبيت برنامج "Trend Micro Mobile Security" عن طريق متجر أبل كما في الشكل (٥٦-١):

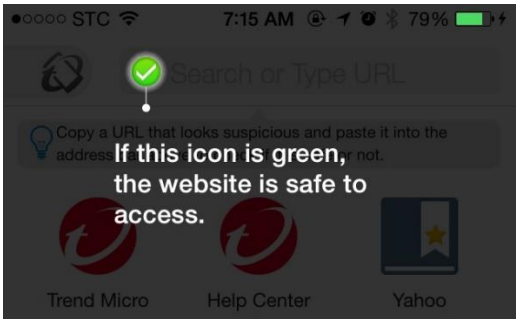


الشكل 56-١: برنامج Trend Micro Mobile Security في متجر أبل

*ملاحظة يقوم مستخدمي نظام الأندرويد بتحميل برنامج Avast وتطبيق نفس الخطوات الأساسية لاستخدام برامج الحماية.

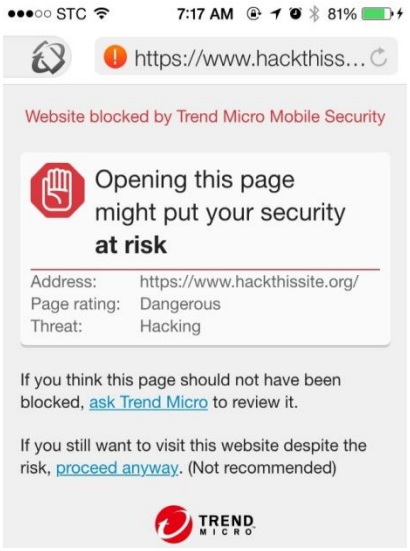
2-بعد عملية التثبيت قم بفتح البرنامج ومن ثم السماح للجهاز بإرسال التنبيهات.

3-سيظهر لك البرنامج علامة خضراء اللون في أعلى المتصفح في حالة أن الموقع سليم من الفيروسات والبرمجيات الضارة كما في الشكل (٥٧-١):



الشكل 57-1: تنبيه بأن البرنامج خالي من الفيروسات

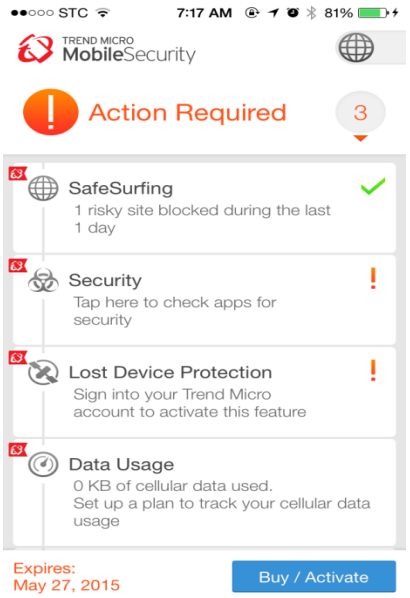
4-قم بتجربة هذا المتصفح من خلال الدخول على بعض المواقع التي من الممكن أن تحتوي على برمجيات خبيثة مثل "www.hackthissite.org" ستلاحظ أن البرنامج قام بحجب هذه الصفحة وإظهار تنبيه أن هذا الموقع من الممكن أن يضع أمن جهازك النقال في خطر كما في الشكل (٥٨-١):



الشكل 58-1: تنبيه أن الموقع قد يضع أمن جهازك النقال في خطر

-

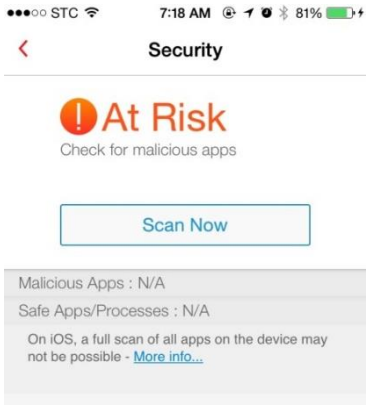
5-قم بالضغط على أعلى الأيقونة في يسار الشاشة وستظهر لك الخيارات التي يقدمها لك البرنامج من التصفح الأمن، وتفحص تطبيقاتك، وإمكانية البحث عن جهازك في حالة فقدانه وعمل نسخة احتياطية لجهات الاتصال. الشكل (٥٩-١) يوضح هذه الخصائص:



الشكل 59-١: خيارات إجراءات الأمان في تطبيق Mobile Security

-

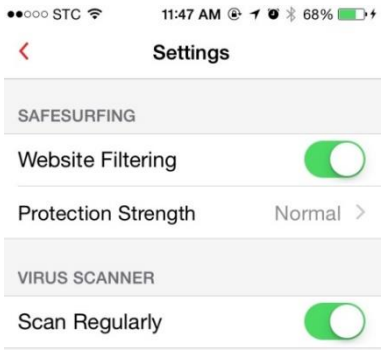
6-اضغط على "Security" ومن ثم اضغط على "Scan" ومن ثم قم بالموافقة على إعطاء الصلاحيات للوصول إلى تطبيقاتك، عندها سيبدأ البرنامج بتفحص تطبيقاتك كما في الشكل (٥٤-١) والشكل (٦٠-١):



الشكل 60-١: إجراء المسح في تطبيق Mobile Security

الشكل 61-١: نتيجة المسح باستخدام Mobile Security

7-بعد ذلك قم بالعودة للقائمة الرئيسية ومن ثم اختيار "Sitting"، ومن ثم قم بالتأكد من ضبط الإعدادات التالية كما في الشكل (٦٢-١):



الشكل 62-١: الإعدادات في تطبيق Mobile Security

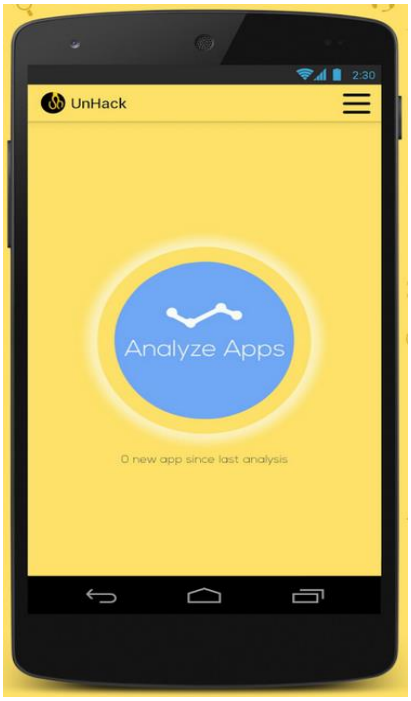
8-من القائمة الرئيسية اضغط على "Backup and Restore" وسيظهر لك الخيار الذي يمكنك من عمل نسخة احتياطية لجهات اتصالك واستعادة من خلال حسابك في البرنامج في أي وقت كما في الشكل (٦٣-١):

الشكل 63-١: النسخ الاحتياطي في تطبيق Mobile Security

تمرين عملي(١٣):

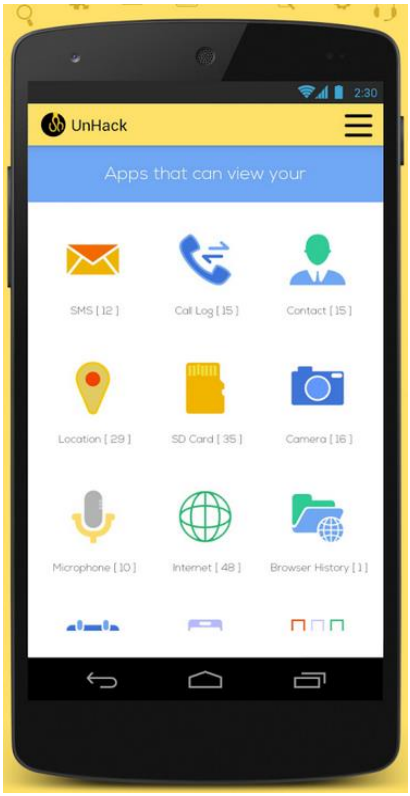
يتم توزيع المتدربين إلى مجموعات ومن ثم يطلب من أحد الأعضاء القيام بتثبيت التطبيق التالي على جهازه النقال.

-قم بتحميل تطبيق unhack على نظام الأندرويد الخاص بك وبعد التثبيت قم بالضغط على أيقونة Analyze Apps كما في الشكل (٦٤-١):



الشكل 64-١: تطبيق Unhack

ستظهر لك عدد البرامج التي تستطيع الوصول إلى ملفات معينة في جهازك كالرسائل ودليل الهاتف كما في الشكل(٦٥-١):



الشكل 65-١: الشاشة الرئيسية لتطبيق Unhack

تأكد من الصلاحيات التي يتمتع بها كل تطبيق في جهازك. أختر ثلاثة تطبيقات ومن ثم ناقش مع مجموعتك النقاط التالية:

- ماهي الصلاحيات التي يستطيع كل تطبيق الوصول إليها؟
- هل تلك التطبيقات فعلاً تحتاج لكل الصلاحيات المعطاة لها أم لا؟
- ماذا يمكن أن يعرف عنك مطور التطبيق من خلال هذه الصلاحيات؟
- هل تغيرت نظرتك عن هذا التطبيق بسبب وصوله لصلاحيات لا يحتاجها وترى أنه من الأجدر إزالته من جهازك؟

معهد الإدارة العامة
INSTITUTE OF PUBLIC ADMINISTRATION

شرائح اليوم التدريبي الأول

مقدمة في أمن المعلومات

- أهم الأهداف المقصودة في الجرائم:
  ١. المعلومات: يشمل ذلك سرقة أو تغيير أو حذف المعلومات.
  ٢. الأجهزة: ويشمل ذلك تعطيلها أو تخريبها.
  ٣. الأشخاص أو الجهات: تهدف فئة كبيرة من الجرائم على شبكة الإنترنت أشخاص أو جهات بشكل مباشر كالتهديد أو الإبتزاز.

بعض جرائم الإنترنت التي تؤدي إلى إتلاف المعلومات

١. صناعة ونشر الفيروسات
٢. الإختراقات
٣. تعطيل الأجهزة
٤. انتحال الشخصية
٥. المضايقة والملاحقة
٦. التغرير والإستدراج
٧. التشهير وتشويه السمعة
٨. النصب والإحتيال

جرائم الإنترنت التي تؤدي إلى إتلاف المعلومات

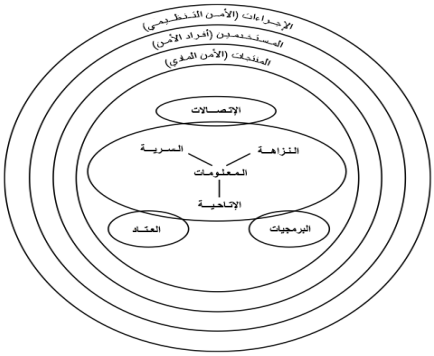
٩- الهجوم
- هجوم التنصت على الرسائل
- هجوم الإيقاف (Dos)
- هجوم تعديل محتوى الرسالة
- الهجوم المفبرك أو المزور لطلب معلومات معينه

الخصائص الأساسية لأمن المعلومات والتي يجب حمايتها

أولاً: سريَّة المعلومات (confidentiality)

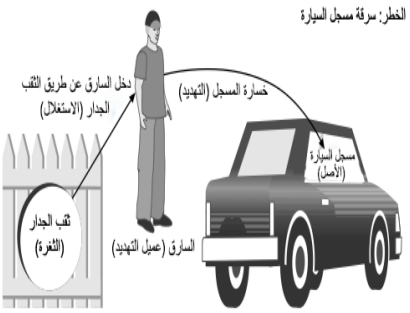
ثانياً:سلامة المعلومات ونزاهتها (Data Integrity)

ثالثاً: التوافرللخدمات و المعلومات (Availability)



مصطلحات أمن المعلومات

- الأصول (Asset)
- التهديد (Threat)
- عميل التهديد (Threat Agent)
- الثغرات (Vulnerability)
- الإستغلال (Exploiting)
- الخطر (Risk)



الصعوبات التي تواجه الدفاع ضد الهجمات

١. سرعة الهجمات
٢. تقدم وتطور الهجمات
٣. سهولة أدوات الهجوم
٤. اكتشاف الثغرات واستغلالها بشكل سريع٥- التأخير في تطوير منتجات الحماية
٥. أغلب الهجمات حالياً هجمات موزعه بدلا من كونها من مصدر واحد
٦. إرباك المستخدمين

من هم المهاجمين

- القراصنة (Hackers)
- أطفال النصوص البرمجية (Script Kiddies)
- الجواسيس (Spies)
- الموظفين (Employees)
- مجرمين الإنترنت (CyberCriminals)
- إرهابيين الإنترنت (CyberTerrorist)

حالة دراسية

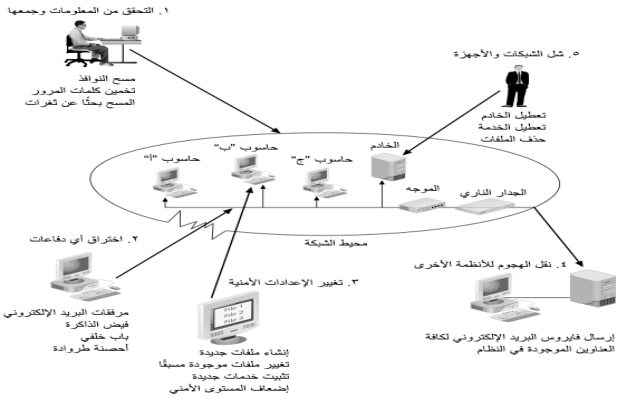
حالة دراسية(١):

أحمد يعمل في مستشفى في مدينة الرياض، وفي يوم عمل شاق ازدادت فيه أعداد المرضى والمصابين في غرف الطوارئ تعطل نظام المستشفى، أمر أحمد المختصين أن يجدوا السبب خلف تلك الأعطال، سواءًا كان انقطاع في الشبكة أو خلل في قاعدة البيانات.. الخ. بعد مرور ساعات قليلة جاء عبدالله مدير مركز أمن المعلومات في المستشفى للأستاذ أحمد ليخبره أن ما حصل اليوم كان بسبب خلل في النظام نفسه. بعدها أخبر عبدالله الأستاذ أحمد بأنه سيقوم بالبحث عن سبب هذا العطل. أجرى الأستاذ عبدالله تحقيقًا نتج عنه تقريرًا مفصلًا مفاده أن العطل لم يكن بسبب خطأ اعتيادي في النظام بل كان هناك متسبب! وأفادت التحريات بعد التحقق من سجلات دخول النظام أن موظفًا كان قد استقال منذ أشهر لأسباب مجهولة هو من كان متصلًا في ذلك الوقت. وهو من قام بتنفيذ بعض الأوامر التي كان من شأنها تعطيل النظام في ذلك الوقت.

❖ **برأيك ماهي الأسباب التي قادت ذاك الموظف المستقيل للقيام بهذا العمل؟ وعلى ضوء تلك الأسباب حدد أيًا من أصناف المهاجمين قد ينتمي إليه هذا الموظف؟**

الهجمات وتقنيات الدفاع

- **خطوات الهجوم:**



الدفاع ضد الهجمات

- إنشاء الطبقات (Layering)
- المحدودية (Limiting)
- التنوع (Diversity)
- الغموض (Obscurity)
- البساطة (Simplicity)

الدفاع ضد الهجمات

- **حالة دراسية(٢):**

في شركة (أ. أ. م) كان هنالك ثغرات أمنية في النظام الخاص بإدارة الشركة. مما أدى الشركة لاتخاذ قرار تعيين مدير جديد لمركز أمن المعلومات. أحمد، المدير الجديد يحاول جاهدًا سعيًا للبحث عن تلك الثغرات وسدها. حينها وجد أن المدير السابق كان قد اشترط استخدام كلمة مرور قوية للدخول إلى النظام. علم أحمد آن ذاك أن كلمة المرور القوية وحدها لم تكن كافية لحفظ المستوى الأمني للنظام. فكان عليه أن يتخذ إجراءات ليزيد من أمن المعلومات في النظام.

❖اقترح أنت ومجموعة من زملائك إجراءات أمنية تساعد أحمد لرفع مستوى الأمن آخذين تقنيات الدفاع بعين الاعتبار.

المخاطري التي تهدد الأنظمة

١- الفيروسات
٢- ديدان الحاسب
٣-أحصنة الطروادة
٤- التحكم الخفي في الحاسوب
٥- القنابل المنطقية
٦- تصعيد الامتيازات

أنواع البرمجيات الخبيثة

حالة دراسية(٣):

أشترك ثلاثة زملاء يدرسون في معهد الإدارة (تركي، فهد، خالد) في مشروع لمادة البرمجة. كان كلًا منهم يعمل على حاسوبه في المكتبة. اشتكى فهد من نشاط خبيث يقوم به حاسوبه، وأنه قد بدأ بملاحظته بعدما قام بتنزيل وتثبيت برمجيات خاصة بالتصميم من إحدى مواقع المنتديات في شبكة الإنترنت. أضاف خالد متسائلًا عن نشاط خبيث قام به حاسوبه هو الآخر لكنه تعجب أن النشاط الخبيث قد بدأ بعد أسابيع عدة لم يتصل خالد فيها بشبكة الإنترنت ولم يقم بتشغيل أي قرص مدمج أو قابل للإزالة على جهازه خلال هذه الفترة. داخلهما تركي وتحدث عن الانتشار الكبير للبرمجيات الخبيثة في الوقت الحالي. وذكر أنه للتو استلم حاسوبه من قسم الصيانة لإصابته ببرمجية خبيثة تمنعه من بدء تشغيل حاسوبه.

❖من خلال ما تعلمته في أنواع البرمجيات الخبيثة، حاول تصنيف البرمجيات التي أصابت أجهزة كلًا من تركي، فهد، وخالد مع ذكرك للأسباب التي استندت عليها

حماية الأنظمة

- تحديث نظام التشغيل
- تكوين حماية لنظام التشغيل من خلال:
  - السياسات الأمنية
  - التكوين الأساسي
  - قالب الأمان
  - النشر
- منع الهجمات على متصفح الويب
- مضادات الفيروسات

تطبيق حماية الأنظمة

تمرين عملي:

١) أولاً تثبيت مكافحة الفيروسات: Avast
٢) تثبيت مكافح البرمجيات الضارة Malwarebyte
٣) استخدام بعض مواقع الكشف عن الملفات Virustotal.com

الإعدادات الدورية للحفاظ على سلامة الجهاز

تمرين عملي:

١) أولاً: تأكد من إعدادات الأمان لمتصفح الإنترنت
٢) ثانياً: تأكد من تفعيل الجدار الناري Windows Firewall
٣) ثالثاً: تأكد من التنبيهات الموجودة في Action Center بإستمرار
٤) رابعاً: تأكد ضبط تحديث نظام التشغيل على الوضع الآلي
٥) خامساً: استخدم Windows Defender
٦) سادساً: تثبيت برنامج تنظيف ملفات التسجيل Ccleaner
٧) سابعاً: التأكد من برامج بدء التشغيل
٨) ثامناً: التأكد من التخلص من ملفاتك الخاصة بشكل Eraser

أمن المعلومات للأجهزة النقالة

- الازدياد الهائل في استخدام الأجهزة النقالة في الشركات والمؤسسات.
- سلوك الموظف وطريقة إستخدامه وعلاقته بأمن المعلومات.
- أخطار إستخدام الأجهزة النقالة على المؤسسات.
- الخطوات الأساسية لتأمين جهازك النقال.

برامج حماية الأجهزة النقالة

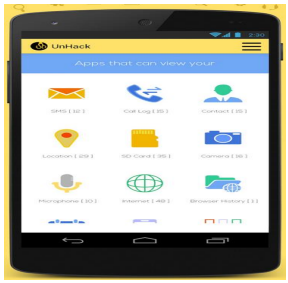
تطبيق عملي:

تثبيت برنامج "Trend Micro Mobile Security" على أجهزة الآيفون

*ملاحظة يقوم مستخدمي نظام الأندرويد بتحميل برنامج Avast وتطبيق نفس الخطوات الأساسية لاستخدام برامج الحماية

أمن الهواتف النقالة

- **نشاط:** يتم توزيع المتدربين إلى مجموعات ومن ثم يطلب من أحد الأعضاء القيام بتثبيت التطبيق التالي على جهازه النقال
- قم بتحميل تطبيق unhack على نظام الأندرويد الخاص بك وبعد التثبيت قم بالضغط على أيقونة Analyze Apps كما في الشكل



أمن الهواتف النقالة

- تأكد من الصلاحيات التي يتمتع بها كل تطبيق في جهازك. أختر ثلاثة تطبيقات ومن ثم ناقش مع مجموعتك النقاط التالية:
  - ماهي الصلاحيات التي يستطيع كل تطبيق الوصول إليها؟
  - هل تلك التطبيقات فعلاً تحتاج لكل الصلاحيات المعطاة لها أم لا؟
  - ماذا يمكن أن يعرف عنك مطور التطبيق من خلال هذه الصلاحيات؟
  - هل تغيرت نظرتك عن هذا التطبيق بسبب وصولة لصلاحيات لا يحتاجها وترى أنه من الأجدر إزالته من جهازك؟

أساسيات أمن المعلومات ١

معهد الإدارة العامة
INSTITUTE OF PUBLIC ADMINISTRATION

اليوم التدريبي الثاني

اليوم التدريبي الثاني

الجلسة	الموضوع التدريبي	الزمن	الهدف السلوكي
الأولى	❖ السياسات الأمنية لأنظمة المعلومات. ❖ ثغرات الشبكات والهجمات عليها. ❖ الدفاع عن الشبكات.	٩٠د	❖ التعرف على السياسات الأمنية لأنظمة المعلومات. ❖ التعرف على ثغرات الشبكات بأنواعها وطرق الهجمات عليها. ❖ التعرف على الأساليب المختلفة للدفاع عن الشبكات.
الثانية	❖ مقدمة في التشفير.	٩٠د	❖ التعرف على التشفير، ماهيته وأهميته. ❖ التمييز بين نوعي التشفير، المتماثل والغير متماثل. ❖ تطبيق بعض من تقنيات التشفير. ❖ استخدام تطبيقات التشفير على جهاز الحاسب.
الثالثة	❖ تطبيقات التشفير.	١٢٠د	❖ التعرف على الشهادات الرقمية والبنية التحتية للمفتاح العمومي للتشفير. ❖ التعرف على أساليب إدارة المفاتيح. ❖ مناقشة الحالات الفردية للمتدربين

اليوم الثاني - الجلسة التدريبية الأولى
سياسات أمن المعلومات

للحصول على بيئة آمنة، فإن على إدارة المنشأة أولاً فهم القوانين والأنظمة المتعلقة بأمن المعلومات ثم البدء في تطبيقها من أعلى مستوى إداري في المنشأة إلى أقل مستوى تنفيذي فيها. ومن ذلك معرفة ما يجب حمايته، ومن يتعامل معه لضمان أن المنشأة تسير وفق برنامج عام يتضمن الالتزام التام بقوانين أمن المعلومات وأخلاقياتها.

فمن المعروف أنه كلما كان هناك إجراءات أكثر تفصيلاً ودقة كلما كان معرفة من يخالف وأين ومتى تقع المخالفة أسهل. لذلك يجب أن يشتمل برنامج أمن المعلومات على:

السياسيات الأمنية (Security Policies)، وبرامج التدريب والتوعية (Awareness and Training) المنظمة والمحققة لأمن المعلومات في المنشأة. [٤]

السياسة الأمنية (Security Policy):

السياسة الأمنية هي الوثيقة الرسمية للمنشأة التي تصدرها الإدارة العليا للمنشأة (أو اللجنة المختصة بذلك)، والتي تنص على دور أمن المعلومات في المنشأة. ويمكن تعريفها بشكل أدق بأنها: " الطريقة أو الخطوات المكتوبة التي يتم تحديدها من قبل الإدارة العليا للمنشأة لتحديد كيفية أداء الأعمال ذات العلاقة بأمن المعلومات وكيف تتم معالجة أي نشاط يخص المعلومة أو الأنظمة والأشخاص المعالجين لها ". وتعتبر السياسة الأمنية هي حجر الزاوية للتخطيط لأمن المعلومات، والتي يمكن الانطلاق منها لتطبيق خطة متكاملة لأمن المعلومات على أرض الواقع.

أهمية السياسة الأمنية:

يمكن تلخيص أهمية السياسة الأمنية في النقاط التالية، التي يمكن اعتبارها إجابة عن السؤال:

لماذا يجب أن يكون هناك سياسة أمنية؟

- تحديد موارد المنشأة الرئيسة، التي تعتبر ذات قيمة كبيرة للمنشأة؛ لأن المقصود هو حمايتها.
- بموجب السياسة الأمنية يتم تحويل فريق أمن المعلومات لممارسة مهامه.
- تشكل مرجعاً رئيساً وموحداً للرجوع إليه عند تعارض المهام الخاصة بأمن المعلومات مع بعضها، أو مع غيرها، أو عند عدم قبولها أو عدم تطبيقها.
- تحدد أهداف المنشأة المتعلقة بأمن المعلومات.
- توضح مسؤوليات الموظفين وتحددها، فيما يخص معالجة المعلومات.
- تساعد في منع حدوث المفاجآت في الإجراءات أو الطلبات أو أحداث العمل اليومية.
- تحدد نطاق عمل فريق أمن المعلومات ومهامه.

- توضح مسؤوليات الاستجابة للأحداث التي تقع والتي تخص أمن المعلومات.
- توضح استجابة المنشأة ومسؤوليتها تجاه القوانين والمعايير العامة والخاصة.

أنواع السياسات الأمنية:

مما لا شك فيه فإنه يجب أن يكون هناك سياسة أمنية عامة للمنشأة، تعني بعموميات أمن المعلومات، وتوثق رؤية المنشأة وأهدافها، وآليات تحقيق تلك الأهداف.

١-السياسة الأمنية العامة:

السياسة الأمنية العامة هي السياسية التي تعتمد على رؤية المنشأة وأهدافها العامة، وتحدد توجهاتها ونطاق الأعمال الخاصة بأمن المعلومات فيها. وتبدأ السياسة الأمنية العامة بتحديد برنامج أمن المعلومات وأهدافه، ثم تنتقل إلى منح الصلاحيات وتحديد المسؤوليات اللازمة لتنفيذه، وتنتهي بوضع الآليات والطرق التي تضمن فرض البرنامج وتطبيقه على أرض الواقع. [٥]

وللسياسة الأمنية العامة معايير ومميزات يجب فهمها وتطبيقها، وهي:

- أن يتم إنشاء السياسة الأمنية وتطبيقها وفق أهداف المنشأة العامة، بل يجب أن تكون أهداف المنشأة هي المحرك لها وتحت مظلتها. وبعبارة أخرى: يجب ألا تتعارض السياسة الأمنية مع أهداف المنشأة.
- يجب أن تكون سهلة الفهم واضحة المعاني ومرجعاً أساساً لموظفي المنشأة وإداريها كافة.
- يجب أن تعد بطريقة يتم فيها تضمين أمن المعلومات في جميع إجراءات المنشأة وأقسامها.
- يجب أن تعد بالاستناد إلى القوانين والتشريعات والقواعد المطبقة على المنشأة (من الحكومة أو الجهات التشريعية)، وأن تدعمها.
- يجب أن تتم مراجعتها وتحديثها دورياً، وعند إضافة أو حذف نشاط أو قسم من أقسام المنشأة، أوعند دمج المنشأة مع غيرها، أو عند تغيير مرجعيتها أو ملكيتها.
- أن يتم إصدار وتحديث السياسة الأمنية على شكل إصدارات أو طبعات مؤرخة، مثل: الطبعة الأولى، الطبعة الثانية، .. وهكذا.
- أن يكون لدى الوحدات والأشخاص المطبقة عليهم السياسة الأمنية إمكانية الوصول إلى الأجزاء التي يحتاجون إليها بسهولة، ولا يشترط عليهم قراءة باقي أجزاء السياسة.
- أن تكون قابلة للتطبيق لعدة سنوات، بحيث يمكن الاستفادة منها على المدى القريب والمتوسط، وأن تكون لديها القدرة على استيعاب المتغيرات خلال تلك الفترة.

- استخدام لغة سهلة ومحددة المعاني، والبعد عن استخدام الألفاظ التي تحتمل أكثر من معنى أو لا تكون محددة، مثل " ربما " أو " من الأفضل " أو " يحسن "، وكذلك البعد عن الألفاظ التي لا تكون معروفة لغالبية الناس، حتى وإن كانت محددة.
- غالباً ما تكون السياسة الأمنية العامة ثابتة قليلة تكرار التحديث.

محتوى وثيقة السياسة الأمنية العامة:

يجب أن تحتوي وثيقة السياسة العامة على البنود التالية (على الأقل):

١-الإجراءات اللازم اتخاذها فيما يخص أمن المعلومات وموارد المنشأة لدى تعيين موظف جديد، أو عند إنهاء خدمات موظف حالي.

٢-تحديد صلاحيات المستخدمين وتقسيمهم إلى مجموعات، وتحديد صلاحيات كل مجموعة.

٣-وضع الشروط والقيود اللازمة لكلمات المرور لضمان أمن حسابات المستخدمين وحمايتها.

٤-تحديد متى يجب إيقاف حساب المستخدم، ومنعه من الدخول على شبكة، المنشأة أو تعطيل حسابه لفترة محدودة، ومتى يجب إعادة تفعليه.

٥-تحديد المستخدمين أو المجموعات الذين يسمح لهم بتركيب أجهزة أو برامج إضافية على أجهزتهم.

٦-الإجراءات اللازم إتباعها والشروط اللازم استيفائها قبل توصيل أي جهاز جديد بشبكة المنشأة.

٧-إجراءات أمن المعلومات التي يجب تطبيقها على الشبكة بشكل عام، وعلى كل جهاز على حدة، كقفل منافذ الاتصال وتفعيل التحديث التلقائي لأنظمة التشغيل والبرامج وتحديد الأوقات المناسبة لذلك.

٨-الإجراءات اللازم إتباعها لحماية شبكة المنشأة من الفيروسات.

٩-شروط وقيود استخدام شبكة الإنترنت وإجراءات الاتصال بها.

١٠-الإجراءات اللازم اتخاذها للحصول على بريد إلكتروني وشروط وقيود استخدامه.

١١-آلية النسخ الاحتياطي وتحديد مسؤوليات وصلاحيات عمل ذلك.

ويمكن القول بأنه لا توجد سياسة أمنية تغطي كافة جوانب أمن المعلومات في جميع إجراءات المنشأة. فلابد من وضع طريقة مناسبة للتعديل أو الإضافة على السياسة الأمنية، وترك مجال لذلك وفق ضوابط وشروط محددة، ويجب مراعاة إمكانية مراجعة السياسة الأمنية، والتعديل فيها مع مرور الزمن أثناء التطبيق.

٢-السياسة الأمنية الموضوعية:

السياسة الأمنية الموضوعية (أو التخصصية) هي سياسة أمنية متخصصة في موضوع أو تخصص معين بشكل تفصيلي أكثر من السياسة الأمنية العامة. ويتم إعداد مثل هذه السياسات عندما تظهر الحاجة للتركيز على تخصص أو إجراء أو قسم معين لأهميته، أو لكثرة التفاصيل فيه التي يجب أن يكون الموظفون على اطلاع عليها وعلم بها.

وللسياسة الأمنية الموضوعية معايير ومميزات يجب فهمها وتطبيقها، وهي:

- أنها تركز على تقنية محددة (كالبريد الإلكتروني مثلاً).
- تحتاج إلى التحديث بشكل مستمر وبتكرار أكثر من السياسة العامة.
- يجب أن تحتوي على النصوص اللازمة لتحديد موقف المنشأة من موضوعات محددة، مثل السماح للموظفين باستخدام شبكة الإنترنت داخل المنشأة.

ومن الأمثلة على الموضوعات التي قد تكون لها سياسات أمنية تخصصية مستقلة ما يلي:

- استخدام البريد الإلكتروني.
- سياسة تصنيف البيانات من حيث السرية.
- سياسة تأمين الشبكة.
- سياسة الاستخدام المقبول للأنترنت.
- سياسة كلمة المرور.

مثال:

١. العنوان: سياسة كلمة المرور لجميع مستخدمي الشبكة الداخلية لمعهد الإدارة العامة.

٢.الرقم:IPA-SecPol-009 .

٣. المؤلف: مركز الحاسب الآلي بمعهد الإدارة العامة، إدارة أمن المعلومات.

٤. تاريخ النشر: ١٤٣١/١/١ معهد الإدارة العامة.

٥. النطاق: تطبق هذه السياسة على جميع مستخدمي الشبكة الداخلية لمعهد الإدارة العامة، هذه السياسة لا تطبق على مستخدمي الشبكات الأخرى الخاضعة لمعهد الإدارة العامة.

٦. نص السياسة:

طول كلمة السر وتشكيلها:

- أقصر طول لكلمة السر هو ثمانية رموز.
- استخدام كلتا حالتي الأحرف العلوية والسفلية (حساسية الحالة).
- استخدام رقم واحد أو أكثر.
- استخدام أحرف خاصة.
- حظر كلمات موجودة في القاموس أو المعلومات الشخصية للمستخدم.

مدة كلمة السر:

- تعتبر كلمة السر غير صالحة للاستخدام بعد مرور ١٨٠ يوماً على أول استخدام لها.
- يجب على أي مستخدم أن يقوم بتغيير كلمة السر قبل مرور ١٨٠ يوماً على أول استخدام لكلمة المرور.

ممارسات شائعة في بناء كلمة السر:

- يمنع مشاركة حساب حاسوب.
- يمنع استخدام نفس كلمة السر لأكثر من حساب واحد لنفس الشخص.
- يمنع إفشاء كلمة السر لأحد، بما في ذلك الأشخاص الذين يدعون أنهم من خدمة
- العملاء أو الأمن.
- يمنع كتابة كلمة السر.
- يمنع تمرير كلمة المرور عبر الهاتف أو البريد الإلكتروني أو الرسائل الفورية.
- الحرص على تسجيل الخروج قبل مغادرة حاسوب غير مراقب.
- تغيير كلمات المرور كلما كان هناك اشتباه أن تكون كلمات المرور قد تعرضت لما يثير
- الشبهة.
- كلمة السر لنظام التشغيل وكلمات السر لتطبيقات يجب أن تكون مختلفة.
- وينبغي أن تكون كلمة المرور مكونة من أرقام وحروف.
- جعل كلمات السر تبدو عشوائية تماما ولكن من السهل تذكرها.

٧. العقوبات:

في حال مخالفة المستخدم للسياسة الأمنية المتعلقة بكلمات السر الواردة في هذه الوثيقة فإن المستخدم قد يكون عرضه لفقدان الامتيازات الخاصة باستخدام الحاسوب.

٨. الراعي: اللجنة العليا لتقنيات المعلومات.

تمرين(١):

يتم تقسيم المتدربين إلى مجموعات.كل مجموعة تقوم بعمل سياسة أمن المعلومات الخاصة بالاستخدام المقبول للأنترنت.

الحل المقترح:

١. العنوان: سياسة الاستخدام المقبول للأنترنت لجميع مستخدمي الشبكة الداخلية لمعهد الإدارة العامة.

٢. الرقم:IPA-SecPol-009
٣. المؤلف: مركز الحاسب الآلي بمعهد الإدارة العامة. إدارة أمن المعلومات.
٤. تاريخ النشر: ١٤٣١/١/١هـ
٥. النطاق: تطبق هذه السياسة على جميع مستخدمي الشبكة الداخلية لمعهد الإدارة العامة. هذه السياسة لا تطبق على مستخدمي الشبكات الأخرى الخاضعة لمعهد الإدارة العامة.
٦. نص السياسة.
٧. العقوبات: في حال مخالفة المستخدم للسياسة الأمنية المتعلقة بالاستخدام المقبول للأنترنت الواردة في هذه الوثيقة فإن المستخدم قد يكون عرضة لفقدان الامتيازات الخاصة بالحاسوب.
٨. الراعي: اللجنة العليا لتقنيات المعلومات.

أسئلة ونقاش(٥):

س١: ما السياسات الأمنية وما أنواعها؟

س٢: برأيك ما أهمية السياسات الأمنية؟

س٣: على ماذا تشتمل السياسات الأمنية؟

ثغرات الشبكات والهجمات عليها

الثغرات في الشبكات:

ثغرات متعلقة بالوسائط:

مراقبة الشبكة وحركة المرور داخلها يعتبر من أهم المهام التي يقوم بها مسؤول الشبكة مما يساعد في اكتشاف وتحديد المشكلات داخل الشبكة والعمل على حلها في مرحلة مبكرة. وتتم مراقبة الشبكة عبر طريقتين:

- **باستخدام مبدل الشبكة المدعم بمنفذ مطابق للأصل "المطابق للمنفذ الرئيسي"(Switch mirroring with port)** :حيث يقوم جهاز الحاسوب المخوّل الموصول إلى المنفذ المطابق للأصل بمراقبة حركة المرور في الشبكة، ويقوم البروتوكول المخصص بفك شفرة وتحليل جميع المعلومات المارة في الشبكة، مما يسمح للمسؤول بإعداد المبدل لإعادة توزيع حركة المرور في بعض أو جميع منافذ الشبكة إلى منافذ مراقبة أخرى معينة في المبدل.
- **تثبيت نقطة عبور اختبارية للشبكة ((Network TAP (Test Access Point):** يتم تثبيت نقطة العبور الإضافية كجهاز منفصل بين جهازين آخرين للشبكة مثل المبدل أو جدار الحماية أو الموجّه، مما يسمح بمراقبة حركة المرور داخل الشبكة.

كما تسمح هذه الطرق للمسؤولين بمراقبة حركة المرور في الشبكة لغايات مشروعة، فإنها أيضاً يمكن أن تكون وسيلة للمهاجم لتلقي واعتراض حركة المرور في الشبكة وبالتالي الوصول إلى معلومات غير مخوّل له الاطلاع عليها. عادة لا يكون بمقدور المهاجم تثبيت جهاز لاعتراض الشبكة إلا أنه باستطاعته الوصول إلى الشبكة السلكية بطرق أخرى مثل:

- السقف المعلق (false ceiling) يستخدم في معظم المباني عوضا عن الأسقف الصلبة لتسهيل تمديد الأسلاك داخل المبنى، مما قد يتيح فرصة للمهاجم بالوصول إلى أحد هذه الأسلاك وتوصيل سلك RJ٤٥ الخاص به.
- الأسلاك المكشوفة داخل أو خارج المبنى توفر للمهاجم ثغرة دخول سهلة.
- موصلات RJ٤٥ غير المحمية (RJ45 jacks) قد تتواجد في عدة مكاتب أو غرف فارغة داخل المبنى.

عندها باستطاعة المهاجم أن يستغل الشبكة لصالحه باستخدام أحد الأساليب التالية:

- فيضان المبدل (switch flooding): يقوم المهاجم بغمر جدول عناوين المبدل بعناوين MAC زائفة مما يؤدي لجعل المبدل يقوم بعمل الموزع(hub) ويرسل حزم المعلومات في الشبكة إلى جميع الأجهزة عوضًا عن إرسالها إلى الجهاز المحدد.

- أنتحال عناوين MAC: يقوم المهاجم المستخدم لجهاز "أ" بالتظاهر أنه المستخدم لجهاز "ب "بواسطة إرسال عنوان MAC الخاص بجهاز "أ" إلى المبدل متظاهراً أنه العنوان الخاص به.
- إعادة توجيه شبكة وهمية: عندما يكون الجهازان على اتصال بواسطة شبكة وهمية (logical network) يجب على جهاز "أ" أن يرسل طلب التواصل مع جهاز "ب "من خلال الموجّه(router). يمكن للمهاجم من جهاز "ج" أن يقوم بإرسال شبكة وهمية زائفة إلى جهاز "أ" مدعياً أنه من الضروري إرسال حزم المعلومات الخاصة بجهاز "ب "إلى الجهاز "ج".
- إعلانات الموجّه (router advertisements): عادة ما يقوم الموجّه بإرسال إعلان إلى باقي الأجهزة بشكل روتيني بهدف الإخبار عن وجوده واتصاله. ويستخدم المهاجم هذه الطريقة حيث يقوم بإرسال إعلانات زائفة إلى جميع الأجهزة المتصلة متظاهراً بأنه الجهاز الموجّه وبالتالي تقوم الأجهزة بإرسال حزم المعلومات إلى جهاز المهاجم.
- إعادة توجيه جهاز وهمي: يقوم المهاجم بالتظاهر بكونه جهاز شبكة صالح عن طريق إرسال إشارات إعادة توجيه جهاز وهمي إلى المبدل.

ثغرات أجهزة الحاسوب الشبكية:

بعض أهم الثغرات في الأجهزة الحاسوبية:

كلمة المرور الضعيفة: كلمة المرور عبارة عن توليفة من الأرقام والحروف التي تعرّف عن المستخدم وتؤكد مصادقة بيأنته لإعطائه الصلاحيات المخولة.

خصائص كلمة المرور الضعيفة:

- أن تكون من الكلمات المتعارف عليها ككلمة مرور.
- عدم تغيير كلمة المرور إلا عند الضرورة.
- أن تكون كلمة المرور قصيرة.
- أن تحتوي على بيانات أو معلومات المستخدم الشخصية.
- أن تستخدم كلمة المرور نفسها لجميع حسابات المستخدم.
- تدوين كلمة المرور على ورقة جانبية، مما قد يؤدي إلى اطلاع شخص غير مخول له على كلمة المرور.

ملاحظة: في حين يجب أن تكون كلمة المرور طويلة ومعقدة مع التأكد بعدم تدوينها جانباً، قد يسبب ذلك صعوبة في حفظ كلمة المرور عن ظهر قلب.

أحد الطرق التي تساعد على زيادة حماية المستخدم هي أن تبرمج كلمة المرور على أنتهاء صلاحيتها خلال فترة معينة من الزمن مما يتطلب إعادة إدخال كلمة مرور جديدة.

الحساب الافتراضي: هو الحساب الذي يتم إنشاؤه تلقائيًا من قبل الجهاز بدلًا من المستخدم المسؤول والذي يساعد في إنشاء الإعدادات الأولية وتثبيت البرامج بسهولة. ومن المفترض أن تحذف هذه الحسابات الافتراضية بعد الأنتهاء من التثبيت وإنشاء الإعدادات، إلا إنها غالبًا ما تترك من دون أن تحذف مما يجعل الحسابات الافتراضية الهدف الأول الذي يستخدمه المهاجم عند البحث على ثغرات.

الباب الخلفي: عبارة عن حساب ينشأ بسرية والذي يسمح بالوصول إلى الجهاز عن بعد دون دراية المستخدم أو إذنه ويكون من الصعب اكتشاف وجوده. ويمكن إنشاء الباب الخلفي عن طريقين:

- أن يصاب جهاز الشبكة بفيروس أو ديدان الحاسوب أو حصان طروادة بواسطة المهاجم.
- أن ينشأ أحد مبرمجي البرامج باب خلفي في الجهاز.

تصعيد الامتيازات: قد تتواجد بعض الثغرات في برامج أجهزة الشبكة التي قد تمكن المستخدم من تصعيد الامتيازات والصلاحيات الخاصة به والحصول على صلاحيات أو معلومات غير مخول له الوصول لها. على سبيل المثال، من الممكن للمستخدم الحاصل على إذن (القراءة فقط) التلاعب بالبرنامج بواسطة إدخال رابط خاص مما يسمح له بالحصول على إذن إداري يتضمن (القراءة والكتابة).

أنواع الهجمات:

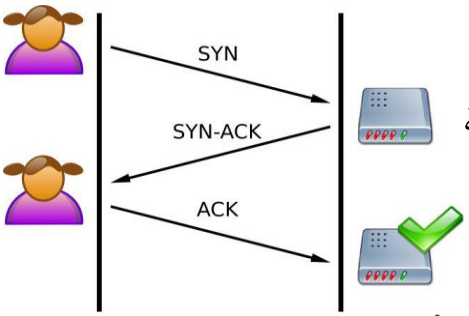
- تعطيل الخدمة (Denial of service DoS)
- التحايل (Spoofing)
- رجل في المنتصف (Man-in-the-middle)
- هجمات الإعادة (Replay attacks)

تعطيل الخدمة (Denial of service DoS):

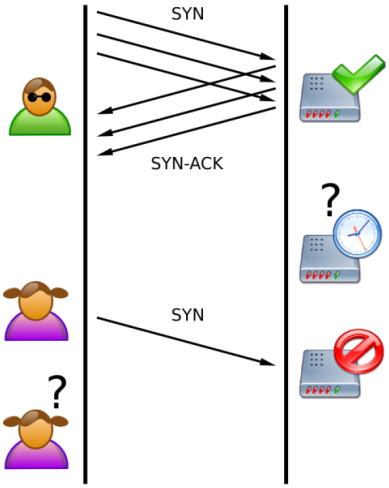
أسلوب الهجوم بواسطة تعطيل الخدمة يهدف بصفة عامة إلى استنفاذ جميع مصادر الشبكة مما يؤدي إلى عدم استطاعة الشبكة أو الأجهزة المتصلة بها الرد على الطلبات المتبادلة. وينقسم إلى ثلاثة أنواع:

هجوم فيضان التزامن (SYN flood attack): يقوم المهاجم بغمر المحول أو الجهاز المسؤول عن الشبكة بإشارات طلب تزامن SYN متابعته وبالتالي يرد جهاز الشبكة بإشعار استلام(SYN-ACK) منتظرا التأكيد(ACK) والمعلومات المطلوبة من المهاجم الذي بدوره يتجاهل الرد تاركًا الجهاز في حالة أنتظار مؤدياً إلى تعطيل الشبكة لعدم استطاعتها على التجاوب مع الأجهزة الأخرى.

تعطيل الخدمة الموزعة (Distributed denial of service DDoS): يختلف عن هجمات تعطيل الخدمة العادي حيث يقوم هذا النوع من الهجمات باستخدام عدد كبير من أجهزة الحاسوب (الزومبي) في شبكة الروبوتات (botnet) لإغراق جهاز الشبكة بإشارات الطلب، بدلاً من استخدام



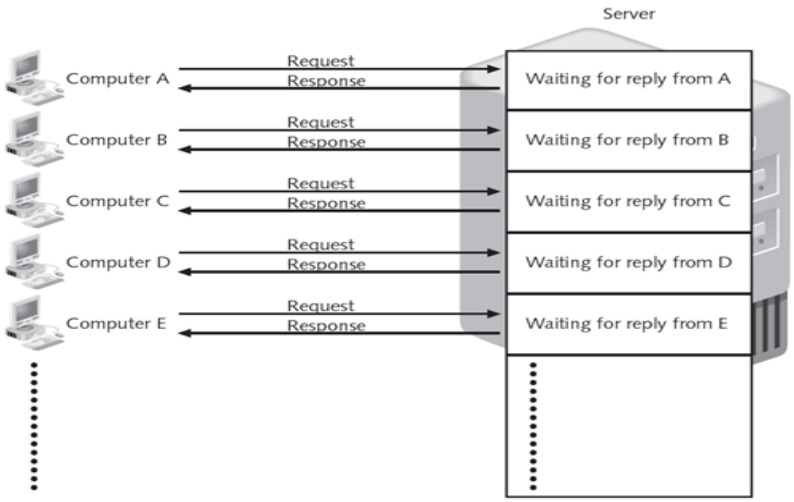
الشكل 67-٢: الاتصال في الحالة السليمة بين الخادم والمستخدم.



الشكل 66-٢: الاتصال في حالة فيضان الهجوم على الخادم.

جهاز حاسوب واحد فقط. مما يجعله من الصعب تحديد وإيقاف مصدر الهجوم.

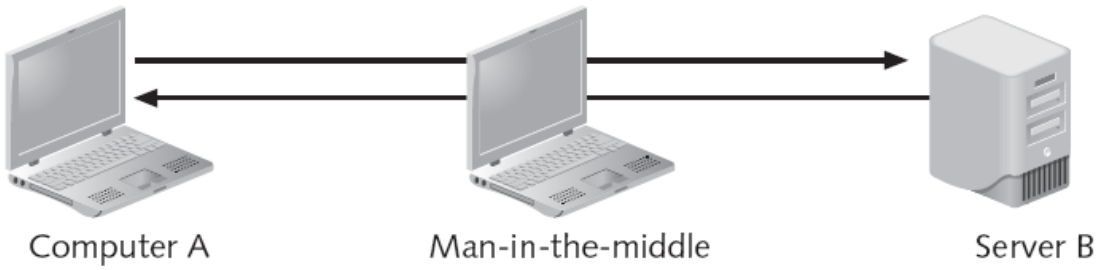
تعطيل الخدمة اللاسلكية (Wireless DoS): هجمات تعطيل الخدمة لا تقتصر على الشبكة السلكية فقط، بل يمكن أن تتم في الشبكة اللاسلكية أيضاً. حيث يقوم المهاجم بإغراق ترددات الراديو في الشبكة اللاسلكية بترددات راديو مغناطيسية مشوشة لتمنع باقي الأجهزة في الشبكة من التواصل مع بعضها البعض. إلا أن هذا النوع من الهجمات غير مستخدم بكثرة نظرا لتعقيد المعدات المسؤولة عن إرسال الإشارات الراديومغناطيسية وغلاء أسعارها، وأيضاً لسهولة تعقب هذه الأجهزة نظرا لضرورة وجودها في مسافة قريبة نسبيا من محوّل الشبكة اللاسلكية وبالتالي سهولة الإمساك بالمهاجم.



الشكل 68-2: هجوم تعطيل الخدمة الموزعة DDoS

التحايل (Spoofing)**:** هجمات التحايل هي عبارة عن أنتحال شخصية أحد أو جهاز ما بواسطة إظهار معلومات خاطئة أو مزورة، إما ليتمكن المهاجم من تنفيذ أعمال غير قانونية باعتباره مستخدم قانوني، أو ليتمكن من الدخول إلى شبكة غير مخوّل له الدخول إليها، أو لخداع مستخدمين آخرين بغرض الحصول على معلوماتهم السرية.

رجل في المنتصف (Man in the middle)**:** يكون المهاجم بدور الرجل في المنتصف عندما يكون هناك اتصال بين جهازين حاسوبيين ويوجد المهاجم في المنتصف بين الطرفين دون علم أي منهما، حيث يظن الجهاز الأول أنه يرسل إلى الجهاز الثاني، في حين أن الجهاز الأول يرسل إلى المهاجم الذي بدوره يمرر الرسالة إلى الجهاز الثاني. وينقسم إلى نوعين: فعّال وغير فعّال.
في النوع الفعّال يقوم المهاجم بتلقي الرسالة من الجهاز الأول ثم إرسالها إلى الجهاز الثاني بعد التغيير في محتويات الرسالة، أما في النوع غير الفعّال يقوم المهاجم بالاطلاع على الرسالة ثم إعادة إرسالها دون تغيير محتواها.



الشكل 69-٢: هجوم الرجل في المنتصف

إعادة الإرسال (Replay): هجوم إعادة الإرسال يشبه في أسلوبه هجوم الرجل في المنتصف غير الفعّال حيث يقوم المهاجم بالاطلاع على الرسالة المرسلة، غير أنه في هجوم إعادة الإرسال يقوم المهاجم بالاحتفاظ بنسخة من الرسالة قبل إعادة إرسالها لاستخدامها لاحقا.

طرق الهجمات على الشبكة:

مثل ما أن هناك أنواع عدة للهجمات على الشبكة فهناك أيضاً طرق مختلفة للهجمات على الشبكة، أما الهجمات التي تعتمد على البروتوكولات أو الشبكات اللاسلكية أو غيرها من الطرق الأخرى والتي لن يتم التطرق إليها حالياً، فسنكتفي بالتعرف على بعض من هجمات البروتوكولات والتي تنقسم إلى طرق عدة:

البروتوكولات المهملة (Antiquated protocols): أحد أكثر البروتوكولات شيوعاً هو بروتوكول TCP/IP والذي مع مرور الزمن قد مر بالعديد من التحديثات التي تعالج مسائل أمنية ونقاط الضعف. أحد الأمثلة للبروتوكولات المحدثة هو بروتوكول SNMP والذي يستخدم لتبادل المعلومات الإدارية بين معدات وأجهزة الشبكة. قد تستخدم بعض الشركات والمؤسسات البروتوكولات غير المحدثة والتي تحتوي على العديد من الثغرات الأمنية مما يزيد من خطر التعرض للهجوم.

هجمات DNS: الهجمات على أنظمة أسماء النطاقات أو كما يعرف (Domain Name System DNS) وهو النظام الذي يقوم بترجمة أسماء النطاقات (أي روابط المواقع) من كلمات إلى أرقام تعرف باسم (IP Address) وتنقسم إلى قسمين: الأول تسميم الـ DNS والثاني تحويل الـ DNS.

- تسميم الـ DNS: ويتم عن طريق استبدأل عنوان الـ IP الخاص بأحد المواقع بآخر مزور بحيث عندما يقوم أحد المستخدمين بإدخال اسم رمزي أو رابط موقع يتم تحويله إلى الموقع الاحتيالي.
- تحويل الـ DNS: باستطاعة المهاجم رسم خريطة تفصيلية لأحد الشركات ومعرفة عناوين الأجهزة داخلها إن كانت متصلة بالـ DNS.

أسئلة ونقاش(٦):

س١: ما أنواع الثغرات؟

س٢: ما خصائص كلمة المرور الضعيفة؟

س٣: اذكر أنواع الهجمات؟ وما أكثرها أنتشاراً برأيك؟

الدفاع عن الشبكات

تصميم شبكة آمنة:

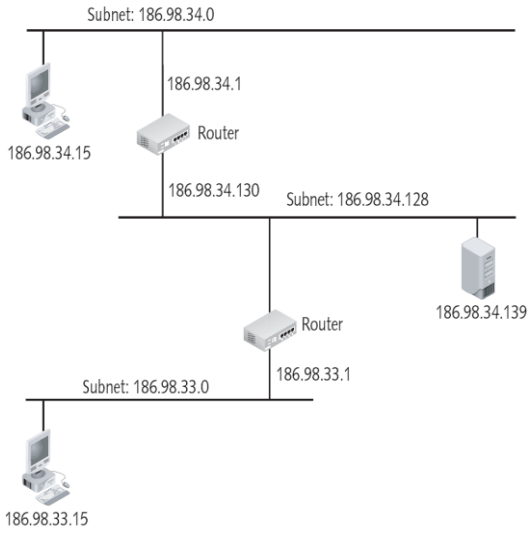
أحد أكثر الأخطاء شيوعًا في أمن الشبكات هو محاولة سد الثغرات في شبكة ضعيفة تم تصميمها وتنفيذها بسوء وركاكة. في حين أن تأمين الشبكة يعتمد بشكل أساسي على التصميم الشبكة، ويتضمن تقنيات الشبكة الآمنة وأجهزة الأمن الخاصة بالشبكة. بعض العناصر المهمة لتصميم شبكة آمنة تتضمن: الشبكات الفرعية(Subnetting)، الشبكات المحلية الافتراضية (Virtual LANs)، وضع منطقة منزوعة السلاح (Demilitarized zone DMZ).[٣]

الشبكات الفرعية Subnetting:

ينقسم عنوان الـIP إلى قسمين، جزء يسمى بعنوان الشبكة (network address) والآخر يسمى بمضيف الشبكة (host address) وتتم العنونة بطريقتين:

- العنونة الصنفية (Classful addressing): حيث يكون الانقسام بين جزء عنوان الشبكة وجزء عنوان المضيف في عنوان الـIP .
- العنونة بالشبكات الفرعية(Subnetting): تسمح هذه الطريقة في العنونة بأن يتم الانقسام في عنوان الـIP في أي مكان، ويمكن تقسيم الشبكة أساسًا إلى ثلاثة أقسام: شبكة، شبكة فرعية، ومضيف. كل شبكة تحتوي على عدة شبكات فرعية، وكل شبكة فرعية تحتوي على عدة مضيفين. من مزايا الشبكة الفرعية أنها عند تقسيم الشبكة إلى عدة شبكات فرعية تزداد نسبة الأمن والحماية خصوصًا عند احتياج عزل مجموعة من المضافين في شبكة فرعية خاصة. على سبيل المثال، يمكن تقسيم الشبكة في أحد الشركات الكبيرة إلى عدة شبكات فرعية، واحدة خاصة بقسم التوظيف وواحدة لقسم الأبحاث

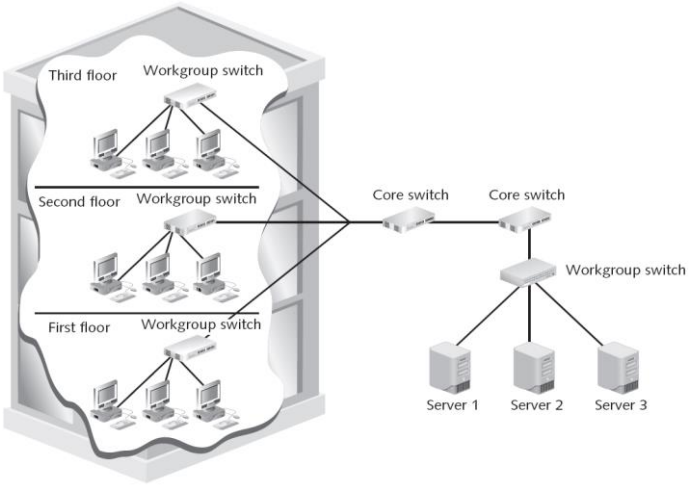
وواحدة لقسم المالية، بالتالي يكون لكل قسم شبكة فرعية خاصة. وهذا أيضاً قد يساعد في إخفاء تخطيط الشبكة الداخلية للشركة عن المهاجمين.



الشكل 70-٢: الشبكات الفرعية
Subnetting

الشبكات المحلية الافتراضية (Virtual LANs):

تقوم على أساس تقسيم الشبكة إلى سلمٍ هرمي. وتقوم الشبكة الافتراضية (VLAN) على أساس تجميع المستخدمين في شبكة واحدة منطقيا وليس فعليا حتى وإن كان المستخدمون متصلين بمبدلات مختلفة. تتكون الشبكة الافتراضية من مبدلات أساسية وهي التي تقع على قمة الهرم السلّمي للشبكة وتقوم بنقل حركة المرور بين المبدلات، ومبدلات المجموعة والتي تتصل مباشرة مع أجهزة المستخدمين في الشبكة. ويجب أن تكون سرعة المبدلات الأساسية أسرع من مبدلات المجموعة بما أن



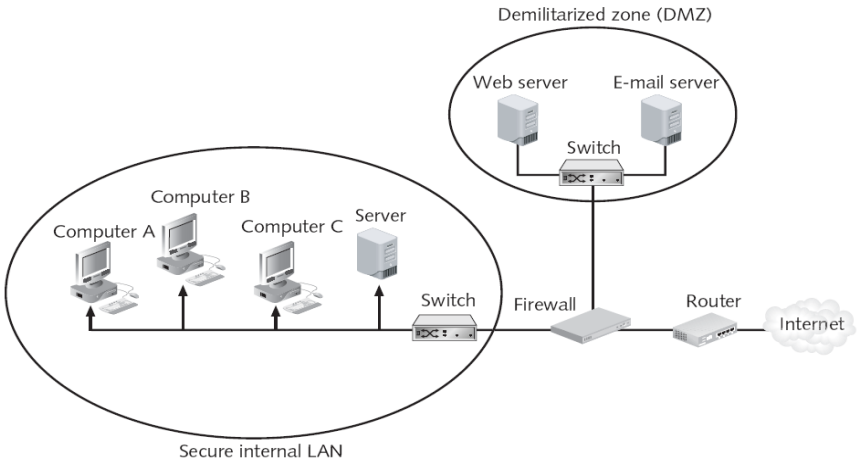
الشكل 71-٢: الشبكات المحلية الافتراضية VLANs

وظيفتها تنظيم حركة المرور بينها. من مزايا الشبكات المحلية الافتراضية أنها تسهل من حركة مرور المعلومات وتوفر نفس درجة الحماية التي توفرها الشبكات الفرعية المذكورة سابقًا، كما أن الشبكة الافتراضية يمكن أن تكون معزولة في حال وجود معلومات حساسة أو خاصة بحيث يتم الاتصال بين أجهزة هذه المجموعة فقط.

المنطقة منزوعة السلاح (Demilitarized zone DMZ):

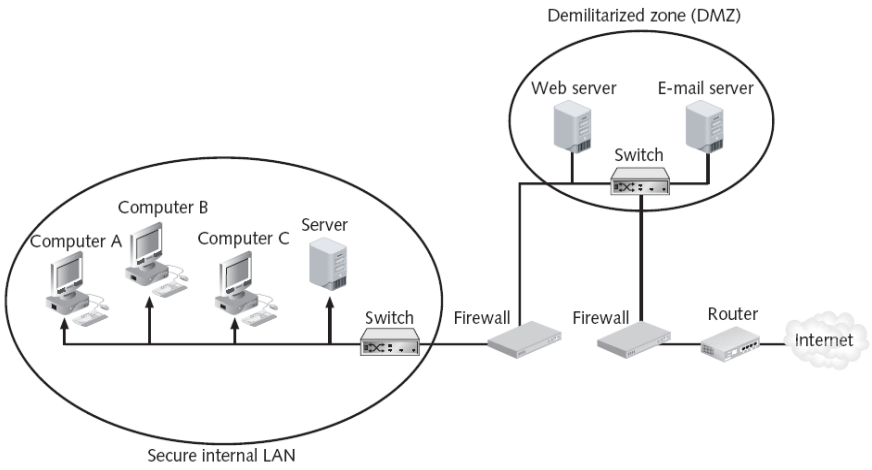
المنطقة المنزوعة السلاح DMZ هي عبارة عن شبكة منفصلة تقع خارج محيط الشبكة المؤمنة حيث يمكن للمستخدمين الوصول إلى الـ DMZ ولكن بدون الوصول إلى الشبكة المؤمنة. وهناك طريقتين لإعداد هذه المنطقة:

- إما بواسطة جدار ناري واحد وثلاث واجهات للشبكة: الإنترنت، DMZ، شبكة LAN داخلية آمنة. لكن هذه الطريقة توفر ما يسمى بنقطة فشل واحدة، أي أن فشل أي من هذه الواجهات الثلاث في توفير الحماية فإن الشبكة ستتعرض للخطر.



الشكل 72-٢: المنطقة منزوعة السلاح باستخدام جدار ناري واحد

- أو بواسطة تثبيت جدارين ناريين عوضا عن واحد، حيث إن فشل أحدهما فإن الآخر لا يزال في وضع الحماية. يتوضح المفهوم أكثر عند الاطلاع على الشكل (٧٣-٢):



الشكل 73-٢: المنطقة منزوعة السلاح باستخدام جدارين ناريين

تطبيق أجهزة أمن الشبكات:

هناك العديد من الأجهزة الخاصة التي يمكن استخدامها لحماية الشبكة من المهاجمين مثل:

- الجدار الناري (Firewalls).
- خادم البروكسي (Proxy servers).
- المصيدة (Honeypots).

الجدار الناري (Firewalls): أحد الطرق التي تساعد على حماية الشبكة هي تصفية حزم المعلومات والبيانات عند وصولها إلى الشبكة ويتم ذلك باستخدام الجدار الناري أو جدار الحماية، والذي يقوم بالعمل كحارس البوابة حيث يتم السماح لحزم البيانات غير الضارة بالدخول إلى الشبكة ومنع حزم البيانات الضارة أو الخبيثة من الدخول إلى الشبكة. ويمكن للجدار الناري أن يتواجد بصورة برنامج أو كجهاز مستقل. ويعمل الجدار الناري على أساس القوانين حيث يقرر اتخاذ ردة الفعل عند تلقي الحزمة إما بالسماح لها بالمرور(Allow) أو المنع(Block) أو إحالة الأمر إلى المستخدم لاتخاذ القرار(Prompt).

هناك نوعان من الجدار الناري:

- جدار ناري شخصي: والذي تحسنت وظائفه مؤخراً حيث أصبح من الإمكان تصفية البيانات الداخلة والخارجة من وإلى الشبكة، والذي يساعد في حماية المستخدم من البرامج الخبيثة التي

تحاول الأنتشار والتواصل مع الأجهزة الأخرى. وتعتمد كفاءة الجدار الناري الشخصي على كفاءة نظام التشغيل الخاص بالجهاز.

- جهاز الجدار الناري المستقل: الذي يعمل على نظام التشغيل الخاص به وعادة ما يكون موقعه خارج حدود الشبكة الآمنة كخط دفاع أمامي أول مما يوفر حماية للشبكة الداخلية من المهاجمين خارج الشبكة. لكن في بعض الأحيان قد تشكل أخطاء المستخدمين أنفسهم داخل الشبكة خطراً على أجهزة الخوادم مما يتطلب في هذه الحالة وضع جهازي جدار ناري أحدهم خارج الشبكة لحمايتها من الخارج والآخر داخل الشبكة ليعزل أجهزة الخوادم عن باقي المستخدمين. أحد مساوئ جهاز الجدار الناري أنه مكلف مادياً. [٣]

خادم البروكسي (Proxy servers): هو نظام أو برنامج تطبيقي يتلقى طلبات المستخدم في الشبكة الداخلية ويقوم بمعالجة هذا الطلب نيابة عن المستخدم. مثلاً إذا طلب المستخدم صفحة أو ملف من موقع معين يتلقى خادم البروكسي الطلب أولاً ويتحقق ما إذا كانت الصفحة متواجدة من بحث مسبق لنفس الصفحة في الذاكرة المؤقتة في البروكسي حينها يقوم بتحويلها للمستخدم، أما إذا لم تتواجد الصفحة في الذاكرة المؤقتة فإن خادم البروكسي يتواصل مع الشبكة الخارجية مستخدماً عنوان الـIP الخاص به لطلب الصفحة. والهدف من ذلك هو إخفاء عنوان الـIP الخاص بالمستخدمين داخل الشبكة. وللبروكسي صلاحية تغيير طلب المستخدم أو استجابة الخادم لمنع عرض المواقع غير المصرح لها أو الممنوعة.

المصيدة (Honeypots): جهاز مستقل يهدف إلى خداع المهاجمين للوقوع في الفخ، وهو جهاز حاسوبي غالباً ما يقع في المنطقة منزوعة السلاح(DMZ) محمل ببرامج وبيانات تبدو وكأنها أصلية إلا أنها في الحقيقة تقليد لملفات بيانات حقيقة. وتهدف المصيدة إلى عدة أغراض:

- تصرف أنتباه المهاجم عن أجهزة الخوادم الحقيقة.
- تساعد في التحذير المبكر من الهجمات الجديدة.
- تساعد في دراسة تقنيات وأساليب المهاجمين.

مرشحات محتوى الإنترنت (Internet Content Filter): تقوم عملية تصفية محتوى الإنترنت على أساس مراقبة حركة المرور في الإنترنت وحجب مواقع الويب المختارة مسبقًا والتي تكون إما مصابة بالفيروسات أو مواقع القرصنة أو مواقع لأغراض إباحية، والتي من الممكن أن تكون أيضاً على هيئة برامج تنفيذ أو ملفات سمعية أو مرئية. لا يتم عرض صفحة الويب أو الملفات إلا إذا تطابقت مع قوانين التصفية حيث يتم حجب أو منع الصفحات بناءً على العنوان URL أو بمطابقة الكلمات المفتاحية.

أسئلة ونقاش(٧):

س١: ما سبل الدفاع عن الشبكات؟

س٢: ما الجدار الناري وما أنواعه؟

تطبيقات:

الجدار الناري:

في أنظمة التشغيل، يعتبر الهدف الأساسي للجدار الناري هو حجب الاتصالات الواردة غير المرغوب فيها. الجدران النارية تستطيع حجب أنواع مختلفة من الاتصالات بذكاء كبير. على سبيل المثال تستطيع السماح بالوصول إلى ملفات الشبكة التشاركية والخدمات الأخرى عندما يكون كمبيوترك المحول متصل بشبكة المنزل الخاصة بك، ولكن لا يسمح بالوصول إليها عندما تكون متصل بشبكة لاسلكية في مكان عام.

يساعد الجدار الناري على حجب الاتصالات التي من المحتمل أن تحتوي على خدمات قابلة للتعرض إلى هجوم والتحكم بالوصول إلى خدمات الشبكة مثل خدمات مشاركة الملفات. تلك الخدمات لا بد أن تكون قابلة للوصول من خلال شبكة موثوقة وإلا سيتم حجبها من قبل الجدار الناري.

الجدار الناري الخاص بويندوز ٨:

مع بداية نظام ويندوز أكس بي، كان النظام الذي يتصل بشكل مباشر بالإنترنت، أحياناً يصاب بعد دقائق ببعض الديدان التي تنتشر من خلال الشبكة مثل "Blaster Worm" والتي تحاول الاتصال بشكل مباشر بجميع الأشخاص المتصلين بالشبكة. سبب ذلك لأن الأجهزة في ذلك الوقت لا تحتوي على جدار ناري وبالتالي تسمح لهذا النوع مع الديدان بالوصول إلى النظام والتمكن منه. وفي النسخة المحدثة من نظام ويندوز تمت ترقية نظام التشغيل ويندوز ليحتوي على جدار ناري مفعل بشكل آلي. بذلك حتى وإن كانت بعض برمجيات نظام ويندوز معرضة لمثل هذه الديدان، سيكون من الصعب إصابتها لجهاز الكمبيوتر لأن الجدار الناري يقوم بحجب جميع مثل هذه الاتصالات الواردة على النظام.

يعتبر حالياً الجدار الناري الخاص بويندوز ٨ من أفضل الجدران النارية التي من الممكن أن تتعامل مع جهاز الكمبيوتر. حيث تفوق هذا الجدار الناري والمرفق مع نظام التشغيل على العديد من البرمجيات الخاصة بالجدار الناري والمتاحة في السوق. حيث يوفر هذا الجدار الناري أفضل تكامل مع نظام التشغيل. فعندما تقوم بالاتصال مع شبكة جديدة، يقوم نظام التشغيل بسؤالك لوضع وصف لهذا الاتصال، مثل هل تريد تشغيل مشاركة الملفات في هذه الشبكة أم لا، بناء على ذلك الخيار، جدار الحماية سيقوم بشكل آلي بضبط القواعد وتطبيق الاستثناء لتلك الشبكة. عدد قليل من تطبيقات الجدران النارية في السوق التي توفر هذه الخاصية، وأغلب تلك التطبيقات تطلب منك ضبط إعدادات الوثوق بشكل يدوي.

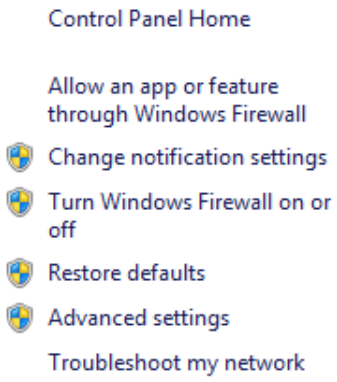
كما يحتوي الجدار الناري الخاص بويندوز على قائمة كبيرة بالقواعد الافتراضية بعمليات الاتصالات، تُطبيق هذه الإعدادات آلياً بمجرد اختيارك لنمط الاتصال بالشبكة. فلا يتطلب هذا الجدار الناري الكثير من العمل من قبل المستخدم إنما يعمل بصمت من أجل حمايته. كما يعتبر سهل الضبط للمستخدمين المبتدئين والمتقدمين على حد سواء.

تطبيق استخدام الجدار الناري الخاص بويندوز ٨:

تمرين عملي(١٤):

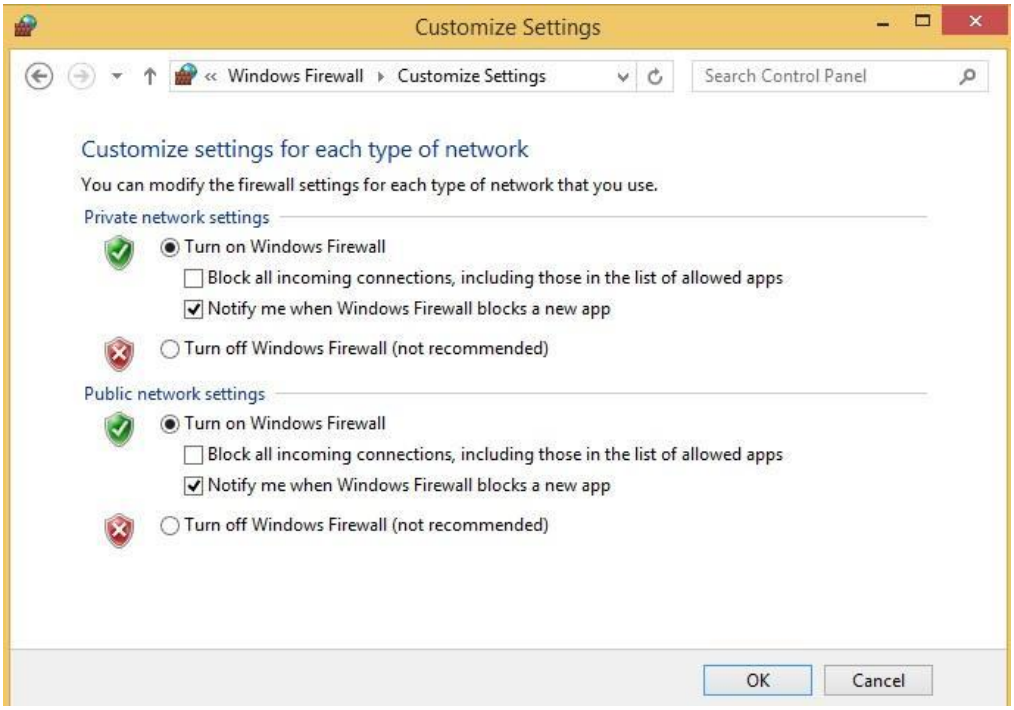
أولاً: قم بتفعيل الجدار الناري

١. اضغط على إبدأ "Start" بزر الفأرة الأيمن ومن ثم قم باختيار لوحة التحكم " Control Panel" ومن ثم "System security" ومن ثم قم باختيار "Windows Firewall" ومن ثم اختر "Turn Windows Firewall On or off" كما في الشكل(٧٤-٢):



الشكل 74-٢: خيارات لوحة التحكم في نظام التشغيل ويندوز

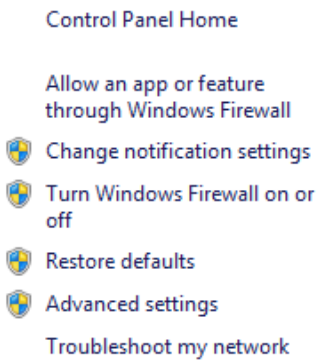
٢. تأكد من أن إعدادات الجدار الناري على وضع التشغيل "on" كما في الشكل (٧٥-٢):



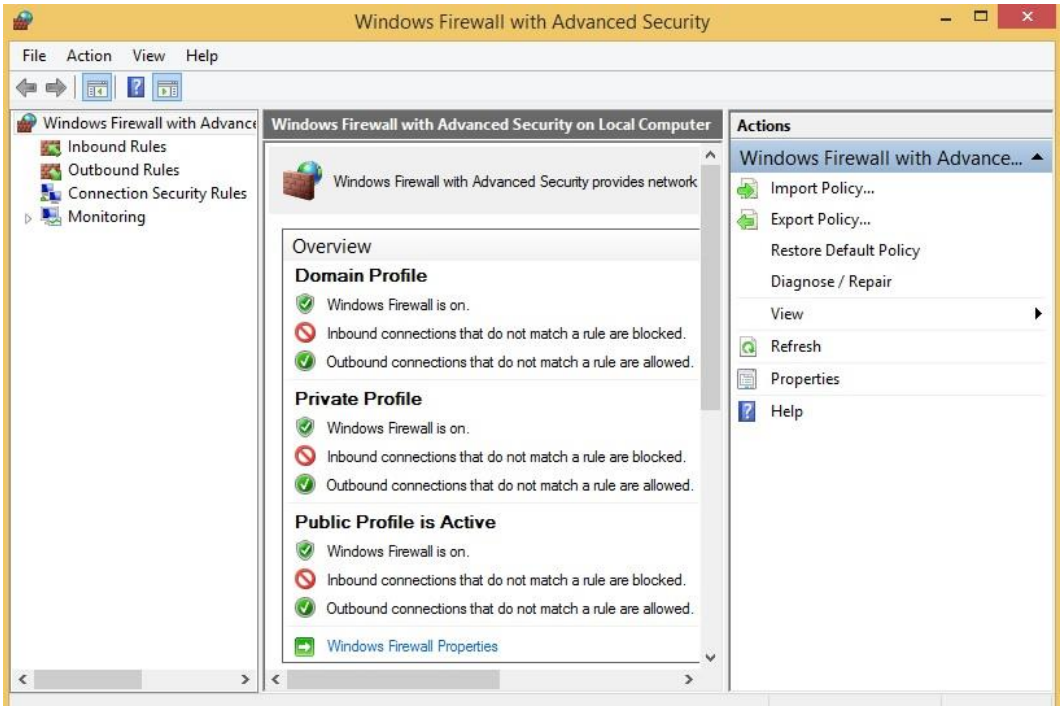
الشكل 75-٢: إعدادات الجدار الناري في نظام التشغيل ويندوز

ثانياً: الوصول للواجهة الرئيسة للتحكم بقواعد الجدار الناري:

١-إضغط على إبدأ "Start" بزر الفأرة الأيمن ومن ثم قم باختيار لوحة التحكم "Control Panel" ومن ثم "System security" ومن ثم قم باختيار "Windows Firewall" ومن ثم اختر "Advance Sittings" كما في الشكل (٧٦-٢):



الشكل 76-٢: خيارات لوحة التحكم في نظام التشغيل ويندوز



الشكل 77-٢: الخيارات المتقدمة في الجدار الناري لنظام التشغيل ويندوز

يستخدم الجدار الناري ثلاثة مظاهر مختلفة "Profiles" كما في الشكل (٧٧-٢)

الأول: مظهر النطاق " Domain Profile" والذي يُستخدم عندما يكون جهازك متصل بنطاق

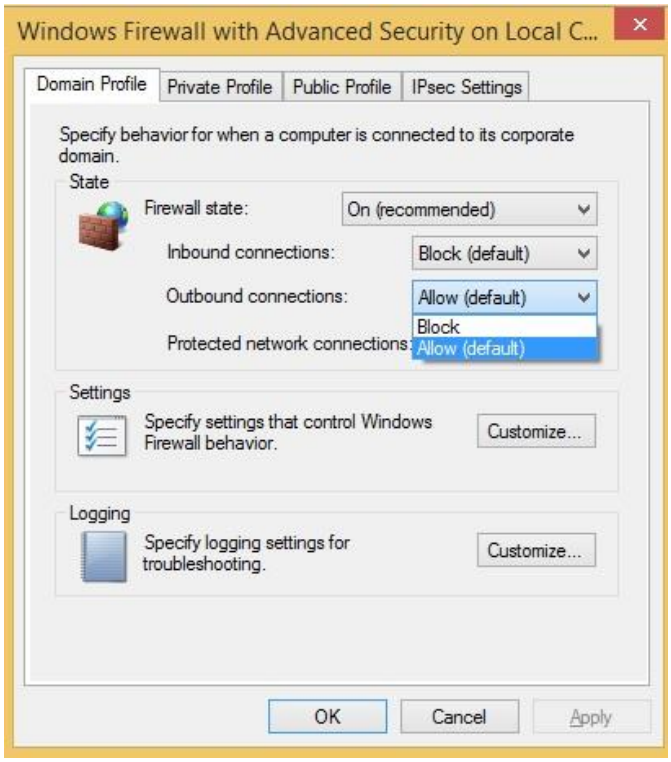
الثاني: مظهر خاص "Private Profile" والذي يُستخدم عند الاتصال بشبكة خاصة مثل شبكة المنزل.

الثالث: مظهر عام "Public Profile" والذي يُستخدم عند الاتصال بشبكة عامة مثل نقاط الوصول العامة "Wi-fi Access point" أو الاتصال المباشرة بالإنترنت.

لذلك دائماً ما يقوم نظام ويندوز بسؤالك عند الاتصال للمرة الأولى بشبكة ما، لتحديد نوع هذه الشبكة وبناء عليه سيتم تطبيق القواعد الافتراضية المستخدمة لمثل هذا النوع من الشبكات.

كما يمكن لجهاز الكمبيوتر أن يُستخدم مظاهر متعددة "Multiple Profiles"، بناء على الحالة. على سبيل المثال الكمبيوتر المحول الخاص بالعمل من الممكن أن يعمل على مظهر النطاق " Domain Profile" عند الاتصال بالنطاق في العمل، وأن يعمل كذلك على المظهر الخاص "Private Profile" عند الاتصال بشبكة المنزل.

٣-من الشكل السابق اضغط على خيار "Windows Firewall Properties" لتكوين والتحكم بالمظاهر "Profiles" كما في الشكل(٧٨-٢):



الشكل 78-٢: خصائص الجدار الناري في نظام التشغيل ويندوز

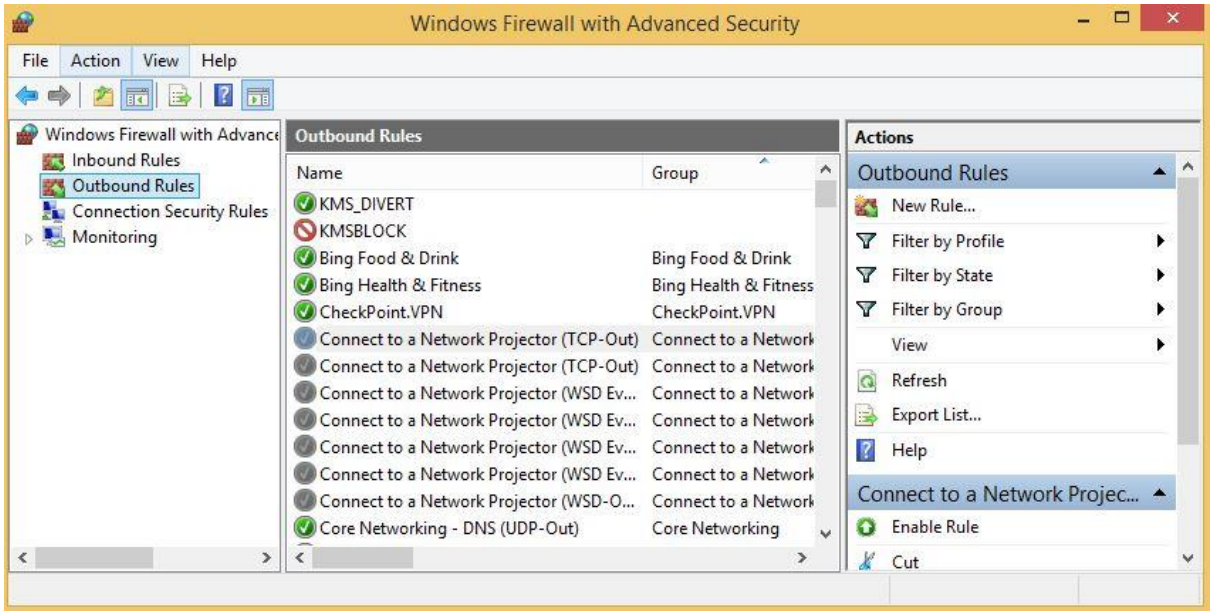
تحتوي خصائص الجدار الناري على تفرع مختلف لكل مظهر "Profile". يقوم نظام ويندوز بحجب الاتصالات الواردة والسماح بالاتصالات الخارجة بشكل افتراضي في جميع المظاهر "Profiles"، ولكن تستطيع حجب جميع الاتصالات الخارجة وإنشاء قواعد خاصة للسماح بنوع معين فقط من الاتصالات الخارجة. يعتبر هذا الإعداد خاص بكل مظهر، حيث يمكنك إضافة قائمة مسموح بها فقط شبكة محددة.

إذا قمت بحجب جميع الاتصالات الخارجة، لن تستلم تنبيه عندما يحجب أحد البرامج وإنما اتصال الشبكة سيفشل بدون أي تنبيهات.

ثالثاً: إنشاء قواعد معينة للجدار الناري

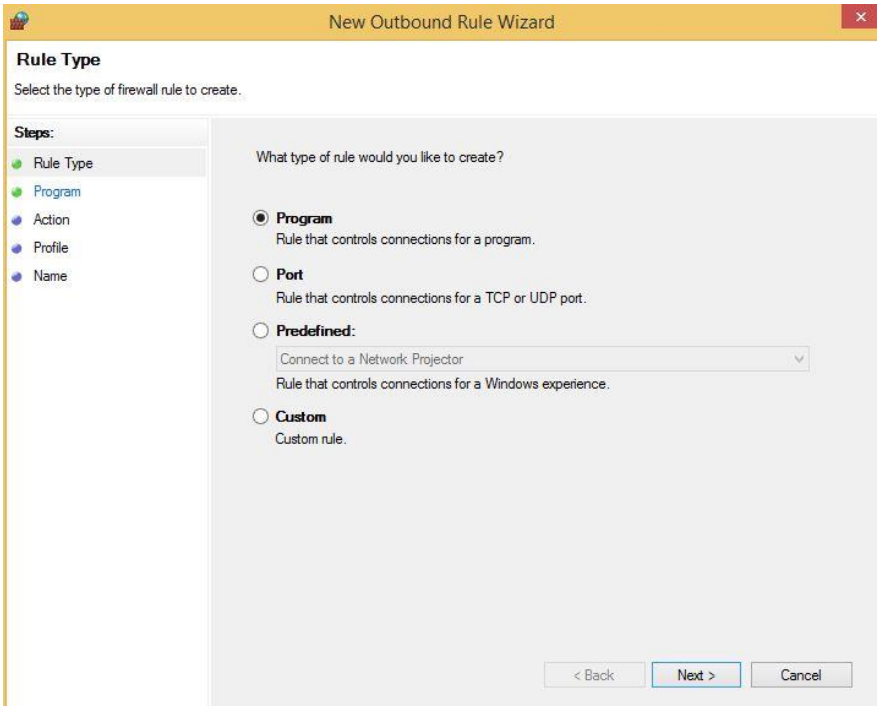
لإنشاء قاعدة معينة في الجدار الناري اتبع الخطوات التالية:

١-اذهب إلى الواجهة الرئيسية للضبط المتقدم للجدار الناري ومن ثم اختر "Outbound Rules" كما في الشكل (٧٩-٢):



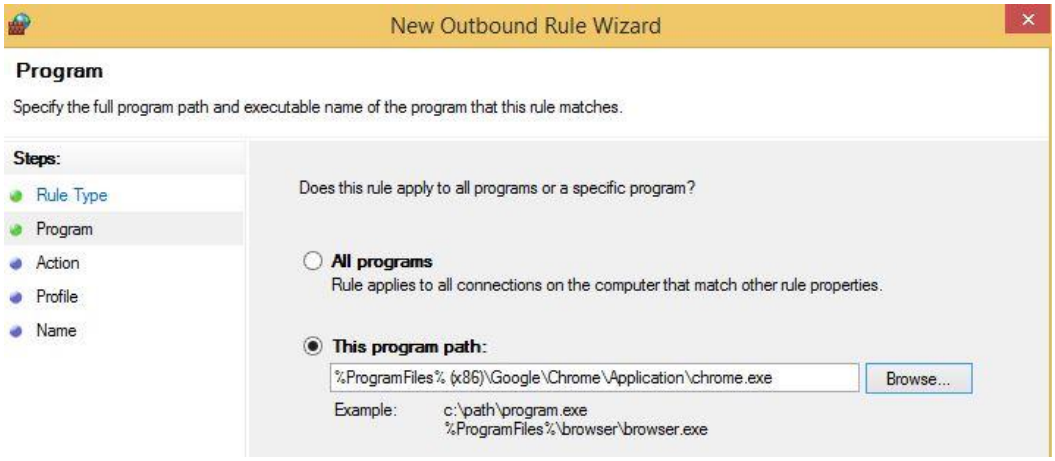
الشكل 79-٢: الخيارات المتقدمة في الجدار الناري لنظام التشغيل ويندوز

٢-من أعلى القائمة في اليمين من الشكل السابق اختر "New Rule" عندها ستظهر لك الشاشة كما في الشكل(٨٠-٢):



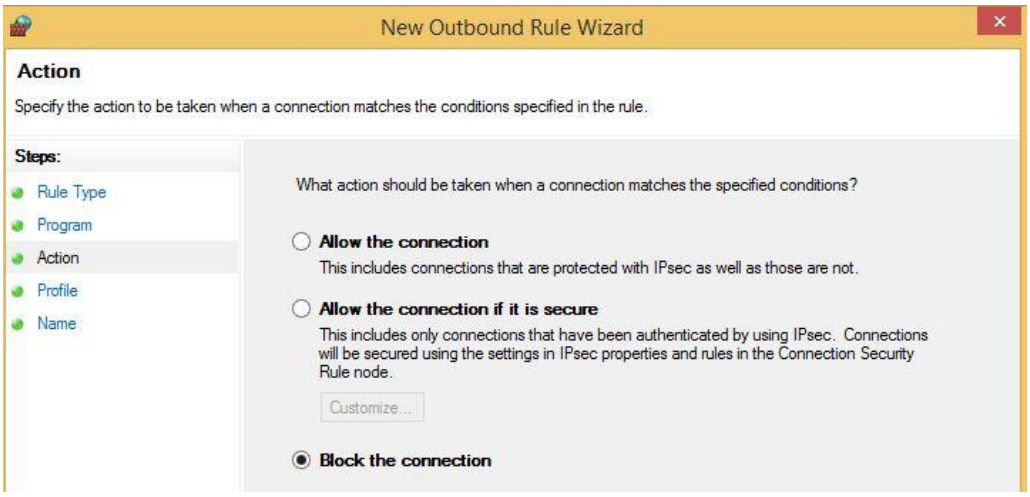
الشكل 80-٢: نوع القاعدة المنشأة للجدار الناري في نظام التشغيل ويندوز

٣-الشاشة السابقة "شكل(٨٠-٢)" توضح أربعة أنواع من القواعد التي من الممكن أن تطبقها وهي "Program، Port، Predefined، Custom "، قم باختيار "Program" ومن ثم "Next". عندها ستظهر لك الشاشة كما في الشكل (٨١-٢):



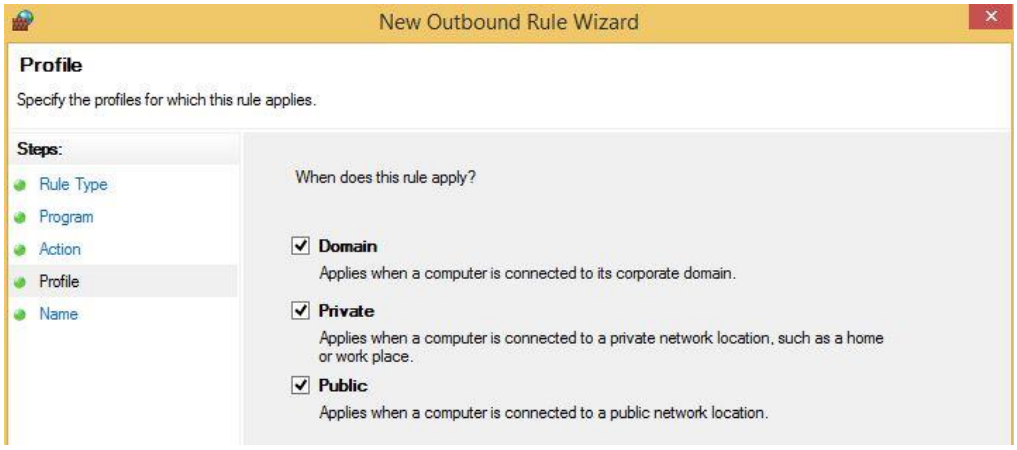
الشكل 81-٢: خيارات تطبيق قاعدة الجدار الناري في نظام التشغيل ويندوز

٤-من الشاشة السابقة من "Browse" قم بتحديد مسار البرنامج الذي تريد حجب الاتصالات الخارجة منه. في مثالنا هذا قمنا باختيار المتصفح "Google Chrome" ومن ثم اضغط على "Next".



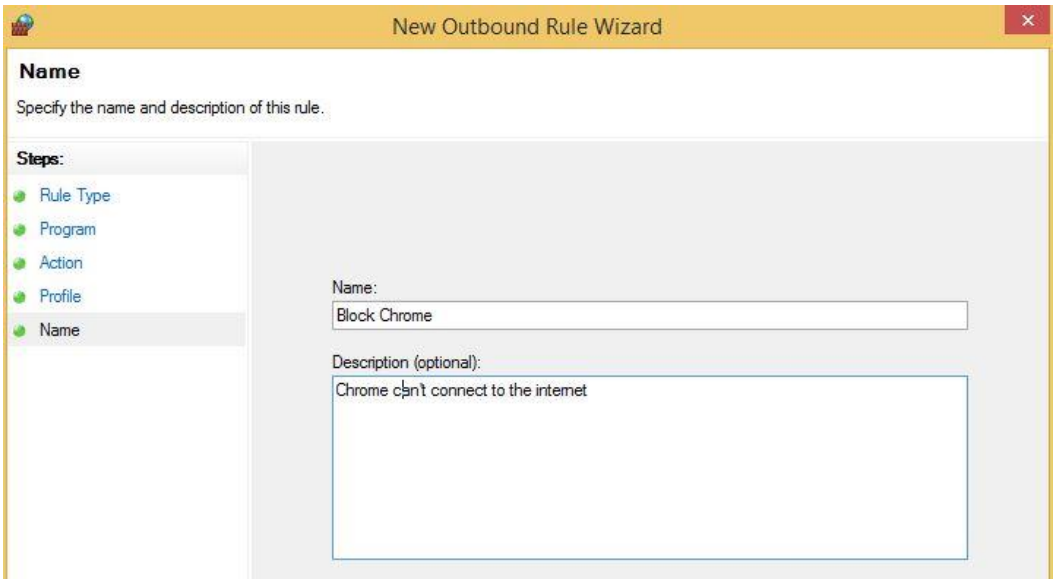
الشكل 82-٢: خيارات الإجراء المتخذ من الجدار الناري في حال تطبيق القاعدة

٥-من الشاشة السابقة "شكل(٨٢-٢)" قم باختيار نوع القاعدة التي تريد تطبيقها، في مثالنا هذا سنستخدم خيار الحجب "Block the connection" ومن ثم "Next".



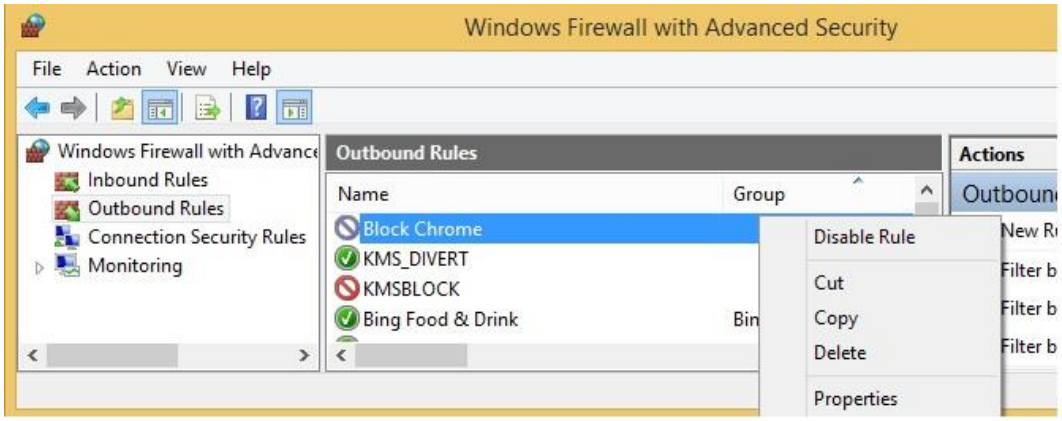
الشكل 83-٢: خيارات تحديد الحالات التي تنطبق عليها قواعد الجدار الناري

٦-بعد ذلك قم باختيار المظاهر التي تريد تطبيق هذه القاعدة عليها، في مثالنا الحالي سنختار جميع المظاهر "Profiles" ومن ثم اختر "Next".



الشكل 84-٢: تسمية القاعدة المنشأة في الجدار الناري

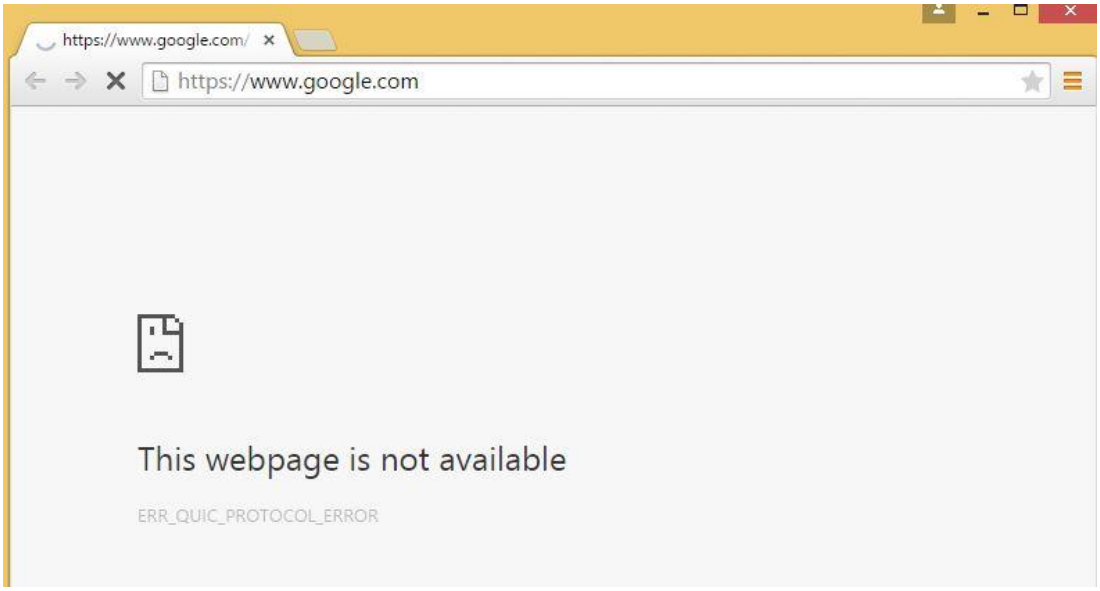
٧-في الشاشة السابقة "شكل(٨٤-٢)" قم بتسمية هذه القاعدة وإضافة وصف لها ومن ثم اختر "Next".



الشكل 85-٢: القاعدة بعد الإضافة للجدار الناري

عندها ستظهر لك هذه القاعدة في الشاشة الرئيسية للضبط المتقدم للجدار الناري. حيث يمكنك تعطيل هذه القاعدة أو حذفها عن طريق الضغط عليها بزر الفأرة الأيمن.

٨-قم بتجربة فاعلية هذه القاعدة بالدخول على متصفح "Google Chrome" والموجود على جهازك والدخول على أي صفحة أنترنت، عندها ستظهر لك الشاشة التالية والتي تفيد بعدم إمكانية وصول هذا البرنامج للأنترنت:



الشكل 86-٢: نتيجة تطبيق قاعدة الجدار الناري

٩-قم بحذف هذه القاعدة من الجدار الناري كما شُرِح في الخطوات السابقة.

اليوم الثاني – الجلسة التدريبية الثانية

مقدمة في التشفير

عُرِفت التعمية بأنها: تحويل نص واضح أو مقروء إلى نص غير واضح، أو نص معمى، بطريقة تستطيع بواسطتها الأطراف المتعارف عليها فقط أن تحل التعمية وتحول النص غير الواضح أو المعمى إلى النص المقروء". ويمكن من ذلك استخلاص تعريف التشفير التالي: "التشفير هو العملية التي من خلالها يتم تغيير البيانات وجعلها في شكل غير مفهوم أو غير مقروء (أي تعميتها)، بحيث لا يستطيع إرجاعها إلى وضعها الأصلي إلا الشخص أو الأشخاص المصرح لهم فقط، الذين لديهم الأدوات اللازمة لذلك". [١]

ويتألف التشفير من عمليتين أساسيتين هما: التشفير، وفك التشفير. وحسب نوعية التشفير، فإنه يمكن استخدام مفتاح تشفير أو أكثر لإتمام هاتين العمليتين. وعموماً، فهناك مصطلحات أساسية، وهي:

- **النص الصريح** (Plain Text): وهو الرسالة أو (البيانات) الأصلية قبل إجراء أي عملية عليها.
- **النص المشفر** (Cipher Text): يطق على الرسالة المشفرة بعد أن تشفر.
- **التشفير** (Encryption): تحويل الرسالة من نص صريح إلى نص مشفر.
- **فك التشفير** (Decryption): استرجاع النص الصريح من النص المشفر.
- **خوارزمية التشفير** (Encryption Algorithm): مجموعة الخطوات والعمليات الرياضية التي يتم إتباعها لتحويل النص الصريح إلى نص مشفر.
- **خوارزمية فك التشفير** (Decryption Algorithm): وهي الخوارزمية العكسية لخوارزمية التشفير لاسترجاع النص الصريح من النص المشفر.
- **تحليل الشفرة** (Cryptanalysis): ويطلق عليها أيضاً (كسر الشيفرة): وتعني التقنيات المستخدمة لفك تشفير رسالة بطريقة غير شرعية، أي كسر تشفيرها بواسطة طرف غير مصرح له، ولا يعرف المفاتيح اللازمة لذلك.
- **المفتاح السري** (Key): وهو عبارة عن قيمة غير معتمدة على الرسالة يتم اختيارها من قبل نظام التشفير أو المستخدم.

وقبل أن نبدأ في استعراض عمليات التشفير، يحسن بنا أن نتعرف على أنواع التشفير وتقسيماته، حيث يوجد نوعان رئيسان من التشفير، هما:

- التشفير المتناظر (Symmetric Encryption).
- التشفير غير المتناظر، أو ما يسمى بالتشفير باستخدام المفتاح العام (Public key Encryption).

وفيما يلي نستعرض هذين النوعين، والفروق بينهما، والحاجة لكل منهما:

التشفير المتناظر:

هو نظام تشفير يستخدم مفتاحاً متناظراً لدى كل من المرسل والمستقبل، بحيث يُستخدم نفس المفتاح في عمليتي التشفير وفك التشفير.

وتتم عمليتا التشفير وفك التشفير باستخدام التالي:

- **عملية التشفير:** يتم تشفير الرسالة الأصلية باستخدام خوارزمية التشفير والمفتاح السري المشترك للحصول على رسالة مشفرة.
- **عملية فك التشفير:** يتم فك تشفير الرسالة المشفرة باستخدام خوارزمية فك التشفير والمفتاح السري المشترك للحصول على الرسالة الأصلية.

إن نظام التشفير المتناظر يتكون من خمسة مكونات رئيسية، هي:

- **النص الصريح:** وهو النص أو الرسالة الأصلية المقروءة التي يتم إدخالها إلى خوارزمية التشفير.
- **خوارزمية التشفير:** وهي الطريقة التي تشتمل على مجموعة الخطوات التي يتم تنفيذها على النص الصريح لأنتاج النص المشفر باستخدام المفتاح السري. وتتكون مدخلات خوارزمية التشفير من النص الصريح، والمفتاح السري ومخرجاتها من النص المشفر، ومن أشهر خوارزميات التشفير المتناظر خوارزمية تشفير البيانات القياسي الثلاثي ((Triple Data Encryption Standard(3DES)) وخوارزمية التشفير القياسي المتقدم ((Advanced Encryption Standard (AES)).
- **المفتاح السري:** وهو المفتاح الذي يتم إدخاله إلى خوارزمية التشفير (بالإضافة إلى النص الصريح) لأنتاج النص المشفر. وهو عبارة عن قيمة يتم اختيارها من قبل المستخدم أو إنتاجها من قبل النظام (مستحسن)، وهي نفس القيمة التي تستخدم للتشفير وفك التشفير. وفي كل مرة يتم اختيار مفتاح مختلف يتم أنتاج نص مشفر مختلف، حتى ولو كان لنفس النص الصريح.
- **النص المشفر:** وهو الرسالة التي تنتجها خوارزمية التشفير من كل من النص الصريح والمفتاح السري.
- **خوارزمية فك التشفير:** وهي نفس خوارزمية التشفير ولكن تعمل بشكل عكسي لها. وتتكون مدخلات خوارزمية فك التشفير من النص المشفر والمفتاح السري، ومخرجاتها من النص الصريح.

في هذا النوع من التشفير، يجب توزيع مفتاح التشفير بين الأطراف المرسلة والمستقبلة بطريقة آمنة جداً. ويمكن لعملية التوزيع هذه أن تتم بشكل تقليدي (عن طريق قنوات آمنة غير إلكترونية) أو

بأنتاج هذه المفاتيح بطريقة آلية آمنة ضمن نظام التشفير، بحيث يتم أنتاج نفس المفتاح عند المرسل والمستقبل.

وللحصول على نظام تشفير متناظر آمن. فإنه يجب تحقيق الشرطين التاليين:

استخدام خوارزمية تشفير (وفك تشفير) قوية: والخوارزمية القوية هي التي لا يمكن إرجاع النصوص المشفرة المنتجة منها إلى نصوص صريحة، حتى ولو كانت الخوارزمية نفسها معروفة عند من يحاول فك التشفير (المعتدي). وعموماً فإن خوارزمية التشفير القوية هي التي يكون المعتدي عليها غير قادر على فك تشفير النص المشفر أو اكتشاف المفاتيح السرية، حتى ولو توفر لدية عدد من النصوص الصريحة والنصوص المشفرة المقابلة لها.

يجب توزيع المفتاح على كل من المرسل والمستقبل بشكل آمن: وأن يبقى هذا المفتاح سرياً بينهما. فلو حصل أحد على المفتاح السري فإنه يصبح بإمكانه فك تشفير الرسائل المشفرة باستخدام خوارزمية التشفير التي عادة ما تكون معروفة عند الجميع.

إن قوة التشفير (سواء كان متناظر، أو غير متناظر) تكمن في سرية المفتاح السري وقوته، وليس في إبقاء خوارزمية التشفير سرية. فمن المعروف ألا تبقى الخوارزمية سرية وأن تكون معروفة حتى يمكن تطويرها من حين لآخر. وللحصول على مفاتيح سر قوية فإنه يمكن إتباع التالي:

- أنتاج المفاتيح السرية بشكل آلي من قبل النظام، وليس من قبل المستخدم.
- استخدام مفاتيح سرية عشوائية مختلفة لكل عملية إرسال مختلفة.
- استخدام مفاتيح سرية طويلة لا تقل عن ٢٥٦ بت (Bit)
- استخدام مفاتيح سرية في صيغتها الثنائية (١،٠) فقط وليس في صيغتها المعتادة (الحروف والأرقام المعتادة)

وكمثال بسيط على التشفير المتناظر، سوف نجري عملية تشفير وفك تشفير باستخدام خوارزمية تبديل مواقع الحروف. يتخلص عمل هذه الخوارزمية في أنها تستبدل الحرف المراد تشفيره بحرف آخر من الأحرف التي تليه في الترتيب الهجائي بناء على مفتاح سري، هو عبارة عن رقم موقع الحرف البديل في الترتيب الهجائي. وبذلك يستبدل الحرف (أ) بالحرف (ث) كونه الحرف الثالث بعد الحرف (أ). ويوضح الجدول أدناه "جدول(١)" كل حرف من الحروف الهجائية والحرف المشفر الذي يقابله باستخدام هذه الخوارزمية. ولفك تشفير أي حرف يتم تطبيق خوارزمية عكسية لخوارزمية التشفير وهي استبدأل الحرف المراد فك تشفيره الحرف (ث) هو الحرف (أ). ويمكن استخدام الجدول ذاته لكلا العمليتين التشفير وفك التشفير.

النص الصريح	أ	ب	ت	ث	ج	ح	خ	د	ذ	ر	ز	س	ش	ص

النص المشفر	ث ج ح خ د ذ ر ز س ش ص ض ط ظ
النص الصريح	ض ط ظ ع غ ف ق ك ل م ن هـ و ي
النص المشفر	ع غ ف ق ك ل م ن هـ و ي أ ب ت

جدول1 : الحروف المستخدمة في خوارزمية التشفير.

ويتكون هذا النظام البسيط من المكونات الأساسية التالية:

- **النص الصريح:** أي كلمة أو جملة في اللغة العربية.
- **خوارزمية التشفير:** استبدأل الحرف بالحرف الثالث الذي يليه في الترتيب الهجائي.
- **المفتاح السري للتشفير:** (3+)
- **النص المشفر:** أي كلمة أو جملة في اللغة العربية.
- **خوارزمية فك التشفير:** استبدأل الحرف بالحرف الثالث الذي يسبقه في الترتيب الأبجدي.
- **المفتاح السري لفك التشفير:** (3-)

لاحظ أن مفتاح التشفير وفك التشفير هو نفس الرقم ولكن بإشارة تختلف حسب الحالة. ففي حالة التشفير نقوم بإضافة المفتاح (الرقم ٣) لترتيب (موقع) الحرف المراد تشفيره، وفي حالة فك التشفير نقوم بطرح المفتاح (الرقم ٣) من ترتيب الحرف المراد فك تشفيره. وفي حالة تشفير حرف من الأحرف الثلاثة الأخيرة في الترتيب الهجائي، فإنه يتم استبدالها بالأحرف في بداية الترتيب الهجائي، انظر الجدول (١) ويتم حساب موقع (ترتيب) الحرف بطريقة الجمع القياسي للقياس (٢٨). فمثلاً، ترتيب الحرف (أ) هو (٠)، وبالتالي يمكن تشفيره إلى الحرف الذي ترتيبه:٠+٣=٣ قياس ٢٨=٣، وهو الحرف (ث)، ومثال آخر: ترتيب الحرف (و) هو (٢٦)، وبالتالي يمكن تشفيره إلى الحرف الذي ترتيبه: ٢٦+٣=٢٩ قياس ٢٨=١، وهو الحرف (ب). لاحظ أ ترتيب الحروف يبدأ بالرقم (٠) للحرف (أ) وينتهي بالرقم (٢٨) للحرف (ي).

وبتشفير الجملة " أمن المعلومات" باستخدام النظام أعلاه فإنه يتم الحصول على النص المشفر " ثوي ثهوقهبوثح"، كما يمكن الحصول على الجملة (أمن المعلومات) مرة أخرى بفك تشفير النص المشفر "ثوي ثهوقهبوثح"، باستخدام نفس النظام. إن نظام التشفير المتناظر باستخدام خوارزمية تبديل الحروف فقط يعتبر نظام تشفير ضعيفاً جداً. والسبب في ذلك أنه يمكن كسره بسهولة عن طريق تجريب جميع الاحتمالات لكل حرف والتي لا تتعدى (٢٨) احتمالاً، حتى يتم العثور على نصوص مقروءة ذات معنى واضح.

وتجدر الإشارة إلى أن أنظمة التشفير المتناظر المعاصرة، كنظام التشفير القياسي المتقدم ((AES، تعتبر أنظمة آمنة ولم يتم كسرها حتى الآن، وهي تعتمد على خوارزميات تشفير معقدة روعي

فيها احتمالات الهجوم عليها وسدها. والشكل (٣-٤) يوضح مقطعاً من ملف نصي (نص صريح) والنص المشفر المقابل له باستخدام خوارزمية التشفير القياسي المتقدم (AES)، وبمفتاح بطول (٢٥٦) بت.

التشفير غير المتناظر (التشفير باستخدام المفتاح العام):

خلال عدة سنوات من البحث العلمي المستمر تم تطوير التشفير المتناظر حتى تم أنتاج نظام التشفير القياسي المتقدم (AES)، الذي يعتبر أمناً لنقل بيانات مشفره بمفتاح بطول لا يقل عن ٢٥٦ بتاً. ولكن المشكلة الأساسية التي توجد في نظام التشفير المتناظر هي كيفية الحصول على نفس المفتاح لكل من المرسل والمستقبل، أو ما يسمى بمشكلة توزيع المفاتيح، ولحل هذه المشكلة تم تطوير التشفير باستخدام المفتاح العام.

قدم التشفير باستخدام المفتاح العام طريقة جديدة تختلف تماماً عن التشفير المتناظر؛ فهو تشفير غير متناظر، أي لا يوجد مفتاح سري مشترك بين المرسل والمستقبل منذ البداية، وإنما يتم استخدام مفتاحين منفصلين يستخدم أحدهما للتشفير، والآخر (وهو مرتبط بالأول) لفك التشفير. في هذا النوع من التشفير، يولّد كل مستخدم زوجاً من المفاتيح مرتبطين بعضهما ببعض (بطريقة رياضية معقدة لا تسمح بكشف أي منهما إذا تم معرفة الآخر) أحدهما عام ويوضع في سجل (مجلد) عام يمكن الاطلاع عليه من قبل جميع المستخدمين، والآخر خاص ويعتبر مفتاحاً سرياً خاصاً بالمستخدم ويجب ألا يطلع عليه الآخرين. ثم بعد ذلك تتم عمليتا التشفير وفك التشفير.

عملية التشفير: يتم تشفير الرسالة الأصلية باستخدام خوارزمية التشفير والمفتاح العام للمستقبل للحصول على رسالة مشفرة. لاحظ أنه يمكن للمرسل الحصول على المفتاح العام للمستقبل؛ لأنه علني (مشاع).

عملية فك التشفير: يتم فك تشفير الرسالة المشفرة باستخدام خوارزمية فك التشفير والمفتاح الخاص (السري) للمستقبل؛ للحصول على الرسالة الأصلية. وبهذه الطريقة لن يستطيع أي شخص آخر فك تشفير الرسالة؛ لأنه لا يملك المفتاح الخاص للمستقبل.

يتكون نظام التشفير غير المتناظر من ستة مكونات رئيسية، هي:

النص الصريح: وهو النص أو الرسالة الأصلية المقروءة التي يتم إدخالها إلى خوارزمية التشفير.

خوارزمية التشفير: وهي الطريقة التي تشتمل على مجموعة الخطوات التي تنفذها على النص الصريح لأنتاج النص المشفر باستخدام المفتاح العام للمستقبل. وتكون مدخلات خوارزمية التشفير هي النص الصريح والمفتاح العام للمستقبل، ومخرجاتها هي النص المشفر. ومن أشهر خوارزميات التشفير بالمفتاح

العام خوارزمية آر إس ايه (RSA)، وخوارزمية التشفير بالمنحنى البيضأوي (الإهليليجي)

المفتاح العام (Public Key): وهو مفتاح عام (مشاع) بحيث يكون لكل طرف مفتاح عام يستخدم لتشفير أي رسالة ترسل إليه. ويمكن لأي شخص الاطلاع على المفتاح العام

واستخدامه في تشفير البيانات المرسلة إلى صاحب ذلك المفتاح العام. ويتم فك تشفير الرسالة المشفرة عن طريق المفتاح الخاص بالمستقبل - صاحب المفتاح العام الذي تم التشفير به.

المفتاح الخاص (Private Key): وهو عبارة عن مفتاح خاص سري، بحيث يكون لكل طرف مفتاح خاص سري خاص به يتم استخدامه لفك تشفير الرسائل الواردة إليه. ويكون هذا المفتاح مرتبطاً بالمفتاح العام الخاص بنفس الشخص.

النص المشفر: وهو عبارة عن الرسالة التي تنتجها خوارزمية التشفير من كل من النص الصريح والمفتاح العام للمرسل إليه.

خوارزمية فك التشفير: وهي مجموعة الخطوات التي يتم تنفيذها على النص المشفر لأنتاج النص الصريح، باستخدام المفتاح السري الخاص للمستقبل. وتكون مدخلات خوارزمية فك التشفير هي النص المشفر والمفتاح السري للمستقبل، ومخرجاتها هي النص الصريح.

ويجب أن يملك جميع المشتركين في نظام التشفير غير المتناظر حق الوصول إلى المفاتيح العامة واستخدامها في التشفير. ويتم توليد المفاتيح الخاصة محلياً لدى كل مستخدم (بشكل آلي) وبالتالي فليس هناك حاجة إلى توزيع المفاتيح كما هي الحال في التشفير المتناظر. ويمكن لأي مستخدم تغيير مفتاحه الخاص في أي وقت شريطة أنتاج المفتاح العام الموافق له، ووضعه في السجل المشترك (العام)، بحيث يطلع عليه جميع المستخدمين. [١]

وللحصول على نظام تشفير آمن باستخدام المفتاح العام، فإنه يجب تحقيق الشرطين التاليين:

استخدام خوارزمية قوية: بحيث يكون من غير الممكن حسابياً تحديد المفتاح السري الخاص بالمرسل إليه بمجرد معرفة هذه الخوارزمية والمفتاح العام (مفتاح التشفير).

يجب أن تبقى المفاتيح الخاصة سرية: وأن يتم إنتاجها بطريقة عشوائية وبطول لا يقل عن ٥١٢ بتاً. ولا يكاد يخلو بلد من نظام متكامل للتشفير غير المتناظر يسمى البنية التحتية للمفاتيح العامة (Public Key Infrastructure (PKI)). يستخدم هذا النظام كعنصر رئيس بشكل منفرد أو بالتكامل مع بعض عناصر أمن المعلومات الأخرى؛ لتحقيق الأهداف الرئيسية التالية للمشتركين فيه:

- السرية (أو الخصوصية): يمكّن هذه النظام (نظام PKI) المستخدمين من تبادل المعلومات بشكل لا يمكن الآخرين من قراءة المعلومات المتبادلة أو فهم طبيعتها.
- التحقق من الهوية: يوفر ذلك إمكانية إثبات هوية الشخص أو الجهة المستخدمة لهذا النظام بصفة قطعية.

- سلامة المعلومة وتكاملها: يوفر إمكانية اكتشاف أي تغيير أو حذف أو إضافة للمعلومة المتبادلة، أو لجزء منها.
- إجراء عملية التصديق الرقمي (أو التوقيع الإلكتروني): يوفر إمكانية توقيع الوثائق إلكترونياً، وكذلك إمكانية التثبت من مصداقية (صحة) التوقيع الإلكتروني لدى استقبال الرسالة التي سبق توقيعها إلكترونياً.

ومن الأمثلة على أنظمة التشفير غير المتناظر: نظام آر إس أيه (RSA)، ونظام التشفير بالمنحنى البيضأوي ((Elliptic Curve Cryptosystem (ECC)).

مقارنة بين التشفير المتناظر وغير المتناظر:

بعد أن استعرضنا أنظمة التشفير المتناظر وغير المتناظر؛ وتعرفنا على أشهر أساليبهما وأنظمتها المطبقة حديثاً، يحسن بنا الآن أن نقارن بينهما. فلكل من نظام التشفير المتناظر وغير المتناظر خصائصه التي تميزه، وتجعله مناسباً لتطبيقات محددة لا تصلح مع الآخر. ويلخص الجدول(٢) المميزات المهمة لكل منهما، والتي توضح أيضاً الفروق بينهما.

التشفير غير المتناظر	التشفير المتناظر
يتم استخدام نفس الخوارزمية للتشفير وفك التشفير.	يتم استخدام نفس المفتاح عند المرسل، والمستقبل ونفس الخوارزمية لكل من عملية التشفير وفك التشفير.
يستخدم زوج من المفاتيح أحدهما عام يطلع عليه الآخرون، والآخر سري خاص بكل مستخدم (ليس نفس المفتاح عند المرسل والمستقبل).	يجب إن يتم توزيع المفتاح السري بطريقة آمنة.
لا يحتاج إلى عملية توزيع المفاتيح.	يحتاج إلى عملية توزيع آمنة للمفاتيح السرية.

جدول2: الفرق بين التشفير المتناظر وغير المتناظر.

بعض أساليب التشفير

للتشفير أساليب عدة سنستعرض منها أسلوبين فقط:

شفرات الانتقال (Transposition Ciphers): تتضمن الشفرات الانتقالية تغيير النمط الاعتيادي للأحرف الموجودة في النص الصريح للعبارة (الرسالـة). تتـم عملية تغيير نمط أحرف الرسالة الصريحة من خلال عمليـة مزج أحرف النص الصريح وفـق طريقة متفق عليها ومحددة بأسلوب ما. إن الطرق التي يمكنها تغيير نمط أحرف النص الصريح تشمل مثلا عكس العبـارة الأصلية، نماذج هندسيـة معينة، إبدال السلك والإبدال العمودي.

الانتقال العمودي (Columnar Transposition): إن التشفير بطريقة الانتقال العمودي تتطلب إزاحة أعمدة الرسالة النص الصريح والمرتبة أصلا بشكل مستطيل.

مثال: لنأخذ النص الصريح التالي:

SHIP EQUIPMENT ON THE FOURTH OF JULY

في البداية يجب اتخاذ القرار بخصوص عدد الصفوف والأعمدة للمستطيل المطلوب استخدامه لأي رسالة. إن الرسالة أعلاه مكونة من ٣٠ حرفا حيث بالإمكان إن تأخذ الأشكال الهندسية التالية: 2 x 15 ,10 x 3 5 x 6 , 6 x 5 أما في حالة عدد أحرف النص الصريح لا تتكون الأشكال المذكورة ، مثلا إذا كان عدد الأحرف ٢٩ فيمكن إضافة حرف ملغي مثل حرف x إلى النص الصريح أو يمكن إضافة فراغ لإكمال عدد الأحرف ليكون ٣٠ حرفا .

عند الرغبة في كتابة النص المذكور أعلاه بشكل ٦ صفوف و٥ أعمدة فانه يمكن الحصول على النص المشفر كما يلي:

أرقام الأعمدة	١	٢	٣	٤	٥
النص المشفر	S	U	T	F	O
	H	I	O	O	F
	I	P	N	U	J
	P	M	T	R	U
	E	E	H	T	L
	Q	N	E	H	Y

إن النص المشفر المكون بهذه الطريقة يمكن قراءته بسهولة حيث لا يوفر أية طريقة أمنية مذكورة. ولغرض زيادة الأمنية فإنه يمكن تبديل أو إزاحة الأعمدة في المستطيل المكون من 6x5 حيث يمكن الحصول على إبدال عمودي مناسب. فعلى سبيل المثال يمكن تغيير مواضع الأعمدة ١٢٣٤٥ إلى

المواضع ٣٤٥٢١ والتي تعتبر واحدا من مجموع ١٢٠ احتمالا للترتيب. إن عدد الاحتمالات للإبدالات العمودية (C) هو (!C). لذلك في حالة عدد الأعمدة يساوي ٥ يحسب كآلاتي: 5!= 5 x 4 x 3 x 2 x 1 = 120

سيكون الناتج في هذه الحالة كما يلي:

أرقام الأعمدة	3	5	4	2	1
النص المشفر	T	O	F	U	S
	O	F	O	I	H
	N	J	U	P	I
	T	U	R	M	P
	H	L	T	E	E
	E	Y	H	N	Q

يمكن الحصول على النص المشفر بعدة أساليب لتحسين أمنية النص الصريح حيث يمكن اختيار أو قراءة النص المشفر على هيئة مجاميع من ٥ أحرف من السطور الأفقية للمستطيل أعلاه وبذلك نحصل على النتيجة التالية:

النص الصريح SHIP EQUIPMENT ON THE FOURTH OF JULY

النص المشفر TOFUS OFOIH NJUPI TURMP HLTEE EYHNQ

أو يمكن الحصول على النص المشفر بأخذ الحروف من المستطيل من الأعمدة المكونة له، حيث سنحصل على النتيجة التالية:

النص الصريح SHIP EQUIPMENT ON THE FOURTH OF JULY

النص المشفر TONTH EOFJU LYFOU RTHUI PMENS HIPEQ

إن النصوص المشفرة عموديا لايمكن قراءاتها بسهولة بدون معرفة قارئ النص المشفر ببعض المعلومات حول الطريقة التي تم استخدامها في التشفير. لذلك على مستلم النص المشفر معرفة المعلومات التالية :

- على مستلم النص المشفر معرفة الأسلوب الذي تم فيه تكوين النص من الشكل الهندسي هل تم مثلا بالأسلوب الأفقي أو العمودي أو القطري أو أية طريقة أخرى.
- يجب على مستلم النص معرفة عدد صفوف وأعمدة المستطيل.

- يجب معرفة المفتاح. ويقصد بالمفتاح كيف تعيد ترتيب أعمدة المستطيل وفق مفتاح رقمي معين مثلا ١ ٢ ٥ ٤ ٢ حيث يجب معرفة هذا المفتاح من قبل كل من المرسل والمستقبل.

تمرين(٢):

يقوم كل متدرب بفك التشفير عن النص التالي:

STTSW EOYEE @ICCL INOUC PFURO AORIM

علماً بأن خوارزمية فك التشفير:

التشفير بطريقة الانتقال العمودي للنص والمكون من مستطيل يحتوي على ٦ صفوف و٥ للنص المشفر والمأخوذ بالأسلوب الأفقي

كما أن مفتاح ترتيب الأعمدة هو ١ ٣ ٤ ٢ ٥

تمرين(٣):

يقوم كل متدرب باستخدام طريقة الانتقال العمودي للتشفير، من خلال تشفير نص رسالة ومن ثم عرض النص المُشفر مع خوارزمية فك التشفير على زميل ليقوم بفك شفرة الرسالة.

الإحلال التخطيطي(Diagraphic Substitution):

في الإحلال التخطيطي يتم تجزئة النص الصريح إلى أزواج من الحروف ، ويتم استبدأل كل زوج بزوج تعويضي من النص المشفر . أحد اشهر أنظمة التشفير التخطيطي تم بناؤه في القرن التاسع عشر من قبل شارلس ويتستون (Charles Wheatstone). هذا النظام يدعى (شفرة بليفير Playfair Cipher). سميت بهذا الاسم نسبة إلى اللورد ليون بليفير (Lord Lyon Playfair) الذي دعم استخدامه من قبل الوزارة الخارجية البريطانية (British Foreign Office).

هذه الشفرة تستخدم مربعا أبعاده (5 x 5) يحتوي على الأحرف الأبجدية . توضع الأبجدية في مثل هذا المربع باتجاه عقرب الساعة كما يأتي :

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

في هذا المربع بالذات ، تم حذف الحرف (Z) . في مربع آخر يمكن دمج الحرفين (I) و (J) في خلية واحدة لكي يضاف حرف (Z) .

إن قواعد التشفير يمكن إن تأخذ عدة أشكال . أحد هذه القواعد موضحة أدناه :

- إذا كان الحرفان للزوج من نفس الصف ، فتكون مكافئاتهما للنص المشفر هما الحرفان الواقعان إلى يمينهما مباشرة ، مثال على ذلك :

النص الصريح : AC النص المشفر : BD

عندما يكون حرف النص الصريح في آخر الصف ، نقوم بتعويض الحرف الموجود في النهاية المعاكسة لنفس الصف ، مثال على ذلك :

النص الصريح : ST النص المشفر : TP

النص الصريح : KO النص المشفر : LK

- إذا كان الحرفان في نفس العمود فتكون مكافئاتهما للنص المشفر هما الحرفان الواقعان مباشرة تحت كل منهما ، مثال على ذلك :

النص الصريح : JO النص المشفر : OT

النص الصريح : YE النص المشفر : EI

إذا كان الحرفان في الزاويتين المتقابلتين لمستطيل وهمي ، متعاكسين قطريا ، فتكون مكافئاتهما هما الحرفان في القطر المعاكس . تبدأ عملية الإحلال بأول حرف من النص الصريح ، ويعوض حرف النص المشفر في نفس النص ، مثال على ذلك :

النص الصريح : EK النص المشفر : AO

النص الصريح : SE النص المشفر : TD

لتطبيق قواعد التشفير على نص ما بهذه الطريقة، نقوم بتقسيم النص إلى أجزاء كل جزء مكون من حرفين. بعد ذلك نرى هل الحرفان متشابهان أم لا، إذا كانا كذلك نفصل بينهما بحرف X. أيضاً في حال كانت نهاية النصل الأصلي عبارة عن جزء بحرف واحد، نضيف له الحرف X

مثال تطبيق قواعد تشفير (Playfair) للرسالة (USE PLAN TODAY) نحصل على :

النص الصريح US EP LA NT OD AY

النص المشفر XP AT KB OS NE EU

ولفك التشفير، نقوم بالعملية العكسية. ففي التشفير قمنا بالذهاب إلى الخانة السفلى في حال كان الحرفان في نفس العمود والذهاب إلى الخانة اليمنى في حال كان الحرفان في نفس الصف، أما لفك التشفير، نذهب للخانة الأعلى في حال كان الحرفان في نفس العمود والخانة اليسرى في حال كان الحرفان في نفس الصف.

كما بالإمكان كتابة مصفوفة التشفير والمكونة من مربع أبعاده (5 x 5) من خلال جملة التشفير (مفتاح التشفير).

مثال: من خلال الشفرة التالية:

Since by man came death

يتم كتابة المصفوفة الخاصة بالتشفير من خلال تكوين مربع أبعاده (5 x 5) ومن ثم تعبئة الخانة الأولى بالحرف الأول من جملة التشفير وهو S والخانة الثانية بالحرف الثاني وهو I وهكذا، ويشترط عدم تكرار الحرف الذي سبق وأن ظهر في المصفوفة. وفي حال أنتهت جملة التشفير نكمل الخانات الباقية بباقي الحرف غير الموجودة في المصفوفة. انظر إلى المصفوفة التالية:

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

بعد ذلك يتم استخدام هذه المصفوفة كمفتاح لتشفير النصوص بنفس الطريقة السابقة.

تمرين(٤):

يقوم كل متدرب باستخدام شفرة بليفر (The Playfair Cipher) بفك التشفير عن النص التالي:

ZN QS PY HL NO GC

علما بأن مصفوفة التشفير هي:

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

تمرين(٥):

يقوم كل متدرب باستخدام شفرة بليفير لتشفير نص رسالة ومن ثم عرض النص المُشفر مع المصفوفة (مفتاح التشفير) على زميل ليقوم بفك شفرة الرسالة.

استخدام بعض تطبيقات التشفير: تشفير البيانات والملفات هو من الأهمية بمكان خاصة في الوقت الحاضر. لهذا هناك مجموعة من البرامج والأدوات المختلفة التي يمكنك استخدامها من أجل ضمان الحماية المناسبة والقصوى لبياناتك الخاصة. سنتطرق في هذه الحقيبة لتشفير ٣ أنواع أساسية من البيانات وهي:

- تشفير الملفات والمجلدات.
- تشفير رسائل البريد الإلكتروني.
- تشفير الأقراص الصلبة والقابلة للإزالة.

أسئلة ونقاش(٨):

س١: ما التشفير وما مصطلحاته الرئيسة؟

س٢: ما مكونات التشفير المتناظر والتشفير غير المتناظر؟

س٣: ما الفرق بين التشفير المتناظر وغير المتناظر؟

تمرين عملي(١٥):

أولاً تشفير الملفات والمجلدات:

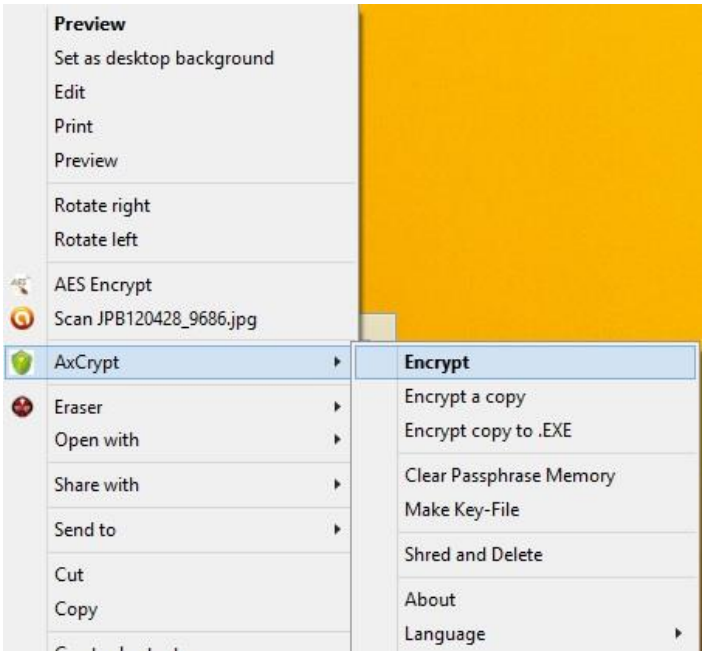
هناك العديد من البرامج التي تتيح لك إمكانية تشفير الملفات والمجلدات وحماية الوصول إليها إلا بمعرفة الرمز السري المستخدم أثناء عملية التشفير. أحد هذه البرامج "Axcryp".

لتشفير الملفات والمجلدات قم بتطبيق الخطوات التالية:

١-قم بتحميل وثبيت برنامج "Axcryp" من خلال البحث عنه في جوجل أو عن طريق الرابط التالي:

http://www.axantum.com/Download/AxCrypt-1.7.3156.0-Setup.exe

٢-بعد عملية الثبيت اضغط بزر الفأرة الأيمن على إحدى الملفات المراد تشفيره ومن ثم اختر "Axcrypt" عندها ستظهر لك القائمة التالية:



الشكل 87-٢: خيارات برنامج AxCrypt

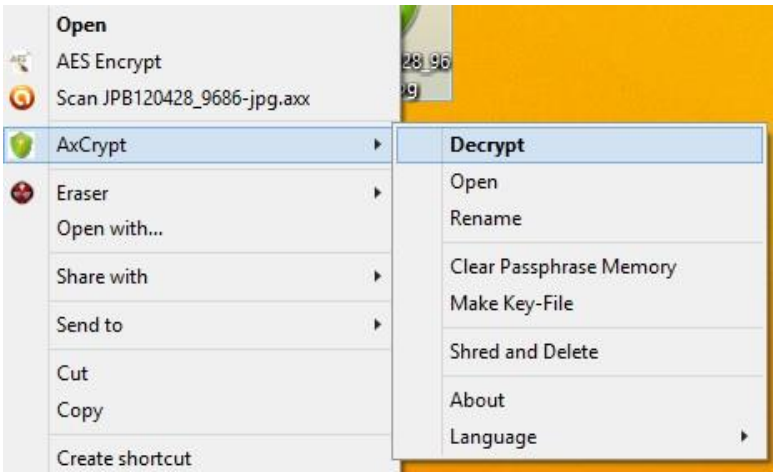
٣-اضغط على خيار "Encrypt" ليتم تشفير الملف الأساسي أو "Encrypt a copy" ليتم تشفير نسخة من الملف، عندها سيطلب منك البرنامج إدخال رقم سري وتأكيده ليتم تشفير الملف ولن تستطيع فك هذا التشفير إلا بمعرفة هذا الرقم السري كما في الشكل (٨٨-٢):

الشكل 88-٢: الرقم السري للتشفير في برنامج AxCrypt

عندها ستظهر لك أيقونة الملف المشفر بهذا الشكل(89-٢):

الشكل 89-٢: أيقونة الملف المشفر.

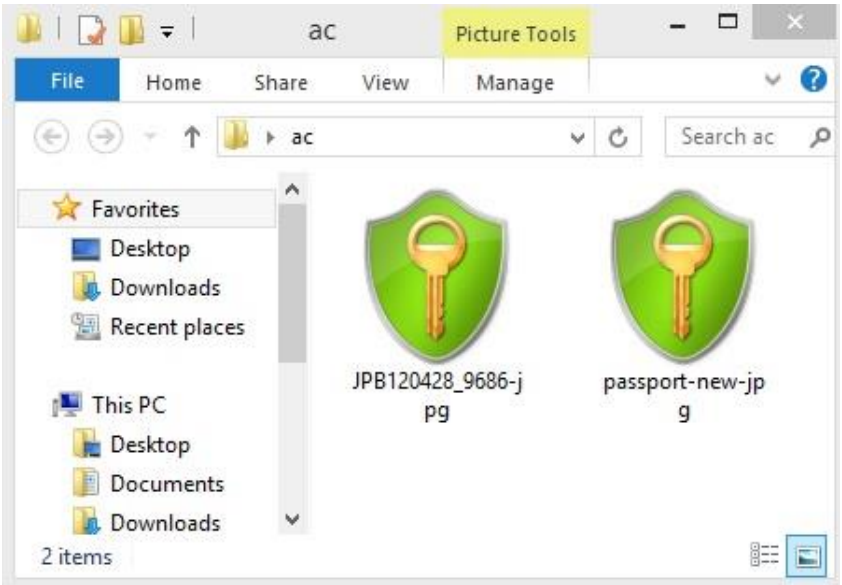
٤-اضغط بزر الفأرة الأيمن على الملف المشفر ومن ثم اختار "Axcrypt" وستظهر لك القائمة التالية "شكل(٩٠-٢)":



الشكل ٩٠-٢: خيارات برنامج AxCrypt

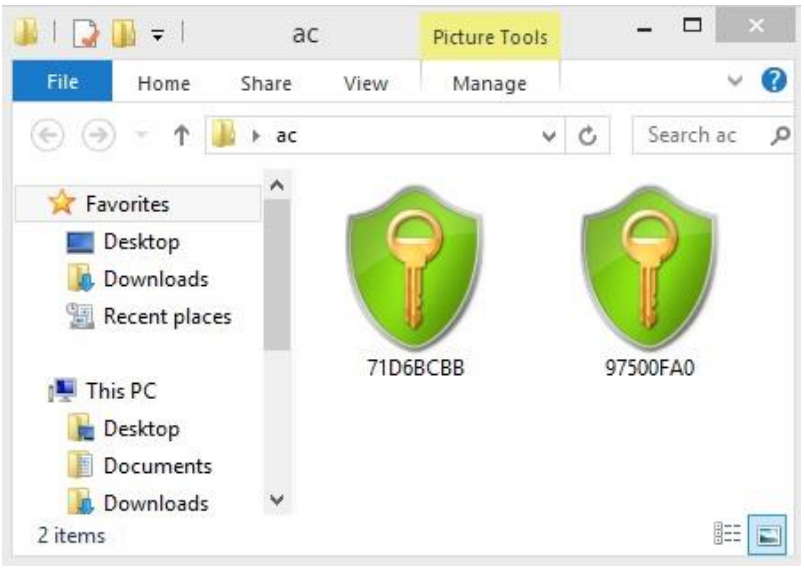
حيث يتيح لك خيار "Decrypt" فك التشـــفير عن الملف بشـــكل كامل وجعله مفتوحٍ أما خيار "Open" سـيتيح لك فتح الملف بعد إدخال الرقم السرـي وعند إغلاقه سـيكون الملف مشـفر مرة أخرى.

٥-كما يمكن هذا البرنامج من تشـــفير جميع الملفات في مجلد واحد، اضـــغط بزر الفأرة الأيمن على المجلد المراد تشفير ملفاته ومن ثم اختر "Axcrypt" ومن ثم "Encrypt" وقم بإدخال الرقم السري. عندها ستظهر لك جميع الملفات في ذلك المجلد بهذا الشكل(٩١-٢):



الشكل ٩١-٢: الملفات المشفرة باستخدام برنامج AxCrypt

٦-كما يمكنك تغيير اسم هذه المجلدات بعد تشفيرها لتكون غير واضحة لأي شخص يستطيع الوصول إليها عن طريق الضغط بزر الفأرة الأيمن على المجلد ومن ثم اختيار "Axcrypt" ومن ثم "Rename"، عندها ستظهر لك جميع الملفات في المجلد باسم عشوائي كما في الشكل(92-٢):



الشكل 92-٢: الملفات المشفرة بعد تغيير أسماءها باستخدام برنامج AxCrypt

كما أن هذه الملفات ترجع إلى اسمها الأصلي بعد عملية فك التشفير.

ثانياً تشفير رسائل البريد الإلكتروني:

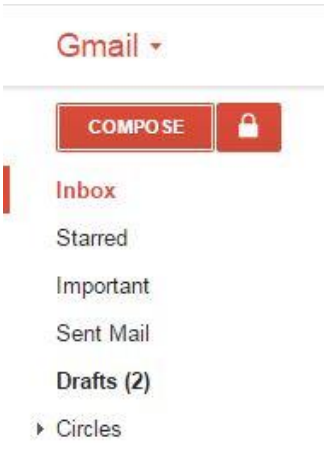
تتيح لك بعض خوادم البريد الإلكتروني إمكانية تشفير النص المرسل من خلالها بحيث لا يستطيع المستلم قراءة الرسالة إلا بعد معرفة الرقم السري الخاص بالتشفير. تفيد هذه العملية في حفظ رسائل البريد الإلكتروني المعرضة للاعتراض ومن ثم الوصول غير المشروع لها. تقدم "Gmail" هذه الخدمة عن طريق تحميل أداة خاصة بالتشفير وعند تثبيتها في المتصفح الخاص بك سيكون بإمكانك إرسال رسائل بريد إلكتروني ذات محتوى مشفر.

تمرين عملي(١٦):

١-قم بتحميل وتثبيت أداة "Streak Secure Gmail" عن طريق تثبيتها في متصفح "Google Chrome" من خلال الرابط التالي:

https://www.streak.com/securegmail

٢-قم بالدخول على حساب "Gmail" الخاص بك عن طريق متصفح "Google Chrome" ومن علبة البريد ستجد خاصية مضافة بعد عملية التثبيت على شكل قفل كما في الشكل (93-٢):



الشكل 93-٢: خيارات بريد Gmail

٣-قم بالضغط على أيقونة القفل عندها ستظهر لك المساحة الخاصة بكتابة رسالة مشفرة كما في الشكل(94-٢):

الشكل 94-٢: المساحة الخاصة بكتابة رسالة مشفرة في Gmail

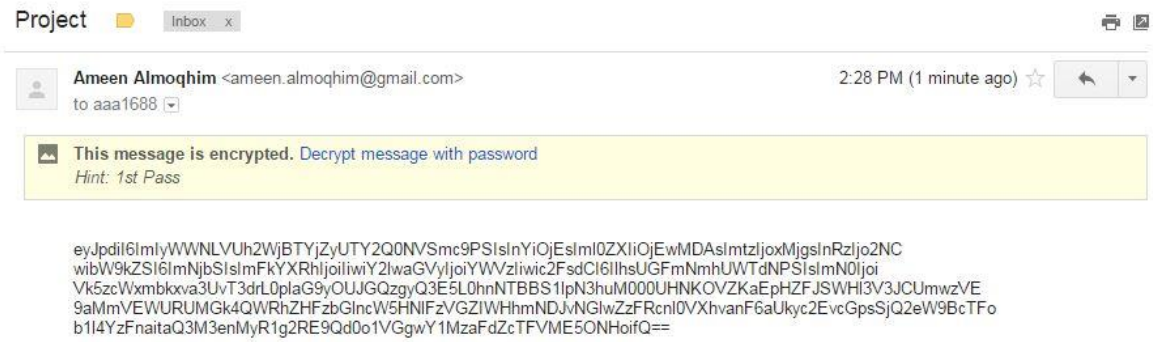
٤-قم بإضافة مستلم للرسالة (لابد أن يكون مزود خدمة البريد الإلكتروني للمستلم من شركة "Gmail")، ومن ثم قم بكتابة النص الذي تريد تشفيره ومن ثم اضغط على "Send Encrypted".

٥-عندها سيطلب التطبيق إدخال الرقم السري الذي من خلاله سيتم الكشف عن الرسالة المشفرة، وكذلك التلميح المستخدم لمعرفة الكلمة السرية كما في الشكل (95-٢):

الشكل 95-٢: الرقم السري لتشفير البريد المرسل عن طريق Gmail

قم بإدخال الرقم السري الخاص بتشفير الرسالة والتلميح ومن ثم اضغط على "Send & Encrypt".

٦-بعد ذلك قم بالدخول على البريد الإلكتروني للمستقبل، عندها ستظهر الرسالة المشفرة في البريد الوارد بهذا الشكل:



الشكل 96-٢: البريد الإلكتروني بعد التشفير في Gmail

٧-قم بالضغط على "Decrypt message with password" ومن ثم ادخل الرقم السري للتشفير. عندها سيتم فك التشفير عن هذه الرسالة وعرضها بمحتواها الأصلي كما في الشكل التالي:

الشكل 97-٢: البريد الإلكتروني بعد فك التشفير في Gmail

تشفير النصوص باستخدام بعض مواقع الإنترنت:

تتيح بعض مواقع الإنترنت إمكانية تشفير نص معين ومن ثم إعطاء رقم سري خاص بالنص المشفر. كل ما عليك هو نسخ النص المشفر ومن ثم إرساله إلى المستقبل. عند وصول النص المشفر إلى المستقبل كل ما عليه هو الدخول على نفس الموقع ومن ثم لصق النص المشفر وإدخال الرقم السري الخاص بالتشفير. من الأمثلة على هذه المواقع:

/https://www.infoencrypt.com

تمرين عملي(١٧):

يقوم المتدرب بالدخول على "/https://www.infoencrypt.com" وكتابة نص مشفر، ومن ثم إرساله لمتدرب آخر ويقوم بفك الشفرة عن هذا النص باستخدام الرقم السري المستخدم للتشفير.

ثالثاً: تشفير الأقراص الصلبة الثابتة والقابلة للإزالة:

أصبحت الأقراص القابلة للإزالة وبطاقات التخزين الخاصة بالهواتف من بين أكثر وسائل التخزين استعمالًا بين المستخدمين، وذلك يرجع لحجمها الصغير وقدرتها على تخزين كم هائل من المعلومات. وبما أننا في كثير من الأحيان نقوم بتخزين معلومات حساسة كالصور الشخصية والملفات والوثائق المهمة، فلابد أن نكون شديدي الحذر من أن تقع هذه الملفات في يد أشخاص لا نرغب باطلاعهم عليها. كما نعلم تعتبر الأقراص القابلة للإزالة عرضة للضياع أكثر من غيرها، لهذا السبب بالتحديد يتوجب عليك تشفير محتويات هذا القرص فلا يستطيع أي شخص الوصول إليها إلا بمعرفة الرقم السري الخاص بالتشفير، وبهذه الطريقة يمكنك نقل بياناتك ومعلوماتك بأمان. كما أن الأقراص الصلبة الثابتة قد يتم الوصول إليها من خلال سرقتها بالكامل من جهازك والوصول إلى البيانات المخزنة فيها بكل سهولة إن لم تكن مشفرة. يوجد العديد من البرامج التي تتيح لك إمكانية تشفير الأقراص الصلبة الثابتة والأقراص القابلة للإزالة بإضافة رقم سري خاص بالتشفير، عندها سيتطلب منك هذا البرنامج إدخال الرقم السري في كل مرة تحاول الوصول إلى هذا القرص القابل للإزالة. كما تتيح بعض البرامج إمكانية تشفير جميع البيانات الجديدة بشكل تلقائي ويتم استعراضها في الجهاز عن طريق إدخال الرقم السري الخاص بالتشفير مره واحدة. حيث تتيح هذه الطريقة تأمين القرص الصلب الثابت من إمكانية الوصول غير المشروع للبيانات إذا تمت سرقته بالكامل.

من المزايا التي تقدمها برامج التشفير، إمكانية حماية القرص القابل للإزالة بتكوين جزء مشفر ومحمي منه. كذلك تقوم بإضافة ملف تنفيذي خاص بالبرنامج الذي قام بالتشفير على القرص القابل للإزالة "USB" وبذلك تستطيع استعراض الملفات المشفرة والمخفية من أي جهاز حتى وإن لم يكن هذا البرنامج مثبت فيه. كل ما تحتاجه هو إدخال الرقم السري الخاص بالتشفير.

تمرين عملي(١٨):

تطبيق استخدام برنامج تشفير الأقراص القابلة للإزالة:

يقوم هذا البرنامج بحماية قرص "USB" برقم سري عن طريق إضافة جزء مخفي ومشفري عليه. إذا كنت تملك العديد من الملفات السرية والخاصة بك على قرص "USB"، يتيح لك هذا البرنامج حمايتها بإضافة جزء مخفي لك ومشفر برقم سري. كما يتيح لك هذا البرنامج إضافة أداة فك التشفير داخل قرص "USB" مما يساعدك على استخدامه على أي جهاز كمبيوتر.

١-قم بتحميل وتثبيت برنامج "Rohos mini drive" عن طريق البحث في جوجل أو من خلال الرابط التالي:

http://www.rohos.com/rohos_mini.exe

٢-بعد عملية التثبيت ستظهر لك الشاشة التالية من البرنامج:

الشكل 98-٢: الصفحة الرئيسية لبرنامج Rohos mini drive

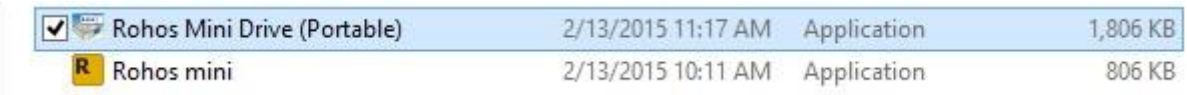
٣-قم بتوصيل القرص القابل للإزالة الخاص بك "USB" ومن ثم اضغط على "Encrypt USB drive" عندها ستظهر لك الشاشة التالية:

الشكل 99-٢: تشفير قرص USB باستخدام برنامج Rohos Mini Drive

٤-قم باختيار رمز القرص القابل للإزالة من خيار "Change" ومن ثم قم بإدخال الرقم السري الخاص بالجزء الذي سيتم تخصيصه وتشفيره في القرص الخاص بك. كما هو ملاحظ سيتم تخصيص ٥٠٠ ميجابايت كمساحة تخزينية قابلة للتشفير في القرص الخاص بك. يمكنك زيادة هذه المساحة حتى ٥٠٠٠ ميجا في النسخة المجانية من خلال الضغط على "Change" ومن ثم قم بزيادة هذه المساحة. بعد إدخال الرقم السري سيبدأ البرنامج بإنشاء جزء مشفر في القرص الخاص بك، عندا ستظهر لك الرسالة التالية:

الشكل 100-٢: رسالة تنويه بإتمام عملية التشفير

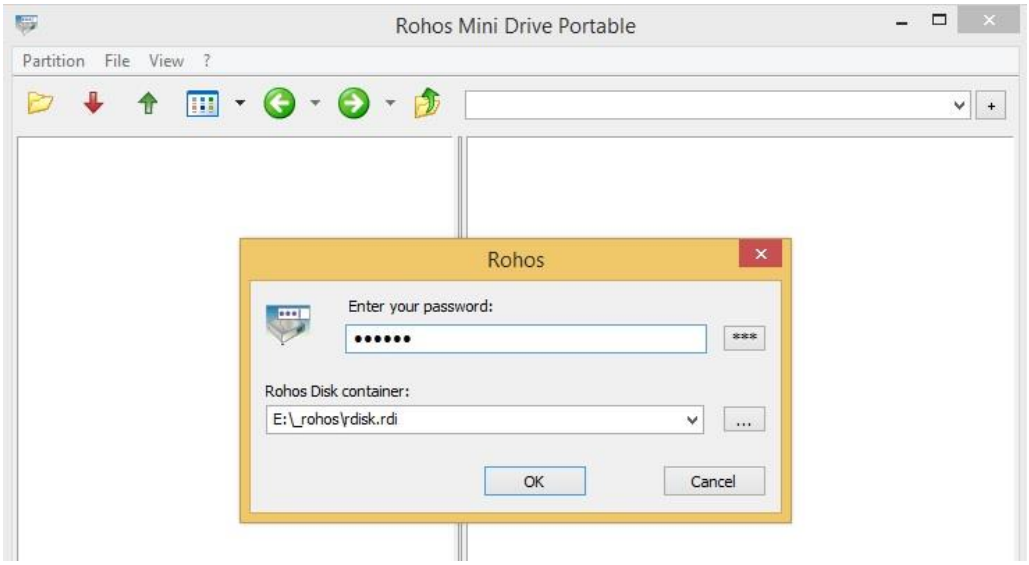
٥-اذهب إلى القرص القابل للإزالة، وقم باستعراض الملفات فيه، ستجد الملفين التاليين تم إنشاؤهما كما في الشكل:



الشكل 101-٢: الملفات في القرص USBبعد تشفيره باستخدام برنامج Rohos Mini Drive

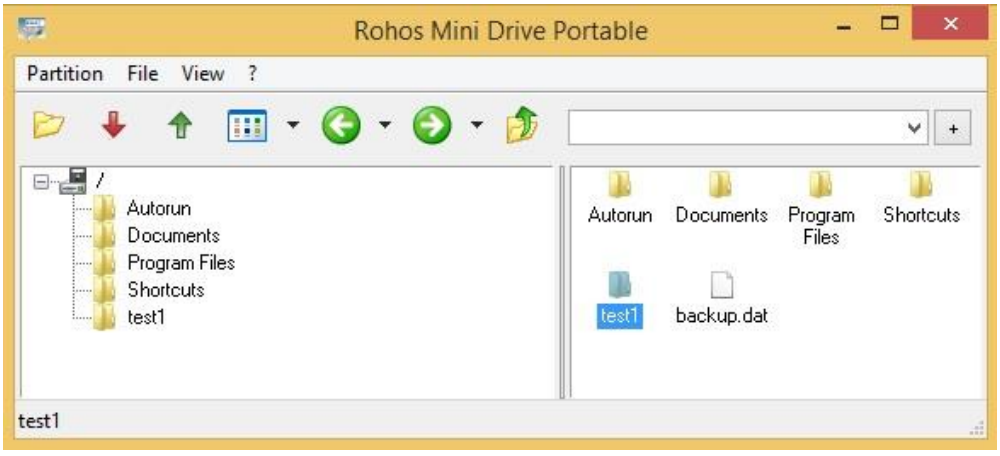
قام البرنامج بإضافة ملف تنفيذي في القرص الخاص بك، حيث سيمكنك هذه الملف التنفيذي من استعراض ملفاتك المشفرة في الأجهزة التي لا تملك فيها صلاحيات مدير النظام.

٦-اضغط على الملف الأول عندها، سيطلب منك البرنامج إدخال الرقم السري الخاص بالجزء المشفر من القرص كما في الشكل (102-٢):



الشكل 102-٢: الرقم السري لفك الملفات المشفرة باستخدام برنامج Rohos Mini Drive

٧-بعد إدخال الرقم السري، سيستعرض لك البرنامج المساحة التخزينية المشفرة الخاصة بالقرص القابل للإزالة، حيث يمكنك إضافة فيه أي ملف تريد تشفيره. قم بإضافة مجلد على سطح المكتب باسم "Test1" ومن ثم انسخ ذلك المجلد في المساحة التخزينية المشفرة كما في الشكل(103-٢):



الشكل 103-٢: المساحة التخزينية المشفرة الخاصة بالقرص USB في برنامج Rohos mini drive

٨-قم بإزالة القرص الخاص بك من جهاز الكمبيوتر، ومن ثم وصل القرص في جهاز آخر وحاول استعراض الملف المشفر كما في الخطوة السابقة.

اليوم الثاني – الجلسة التدريبية الثالثة
تطبيقات التشفير
شهادات التعريف الرقمية وبنية المفتاح العمومي

البنية التحتية للمفاتيح هي مجموعة من الأجهزة والبرامج والأشخاص والسياسات والإجراءات اللازمة لإنشاء وإدارة وتوزيع واستخدام وتخزين، وإلغاء الشهادات الرقمية.

في التشفير، البنية التحتية للمفاتيح العامة هي الترتيب الذي يربط المفاتيح العامة مع هوية المستخدم عن طريق سلطة تصديق الشهادات الرقمية. وسلطة تصديق الشهادات الرقمية (CA) هي الكيان الذي يقوم بمنح الشهادات الرقمية. ويجب أن تكون هوية المستخدم فريدة من نوعها في نطاق سلطة التصديق الرقمي. الربط بين هوية المستخدم والشهادة الرقمية يتم من خلال ربط عملية التسجيل والإصدار؛ إذ يمكن، اعتماداً على مستوى الضمان والربط، القيام به من قبل البرامج في سلطة تصديق الشهادات الرقمية، أو تحت إشراف الموظفين.

سلطات التصديق الرقمي التجارية تقوم بفرض رسوم مالية على تقديم خدمة التصديق لعملائها، من أمثلة **سلطات التصديق الرقمي التجارية:**

- Entrust
- VeriSign
- idenTrust
- goDaddy
- Comodo

من أمثلة الشركات التي تقدم برمجيات لإدارة إصدار الشهادات الرقمية:

- Microsoft
- Entrust
- Comodo
- VeriSign

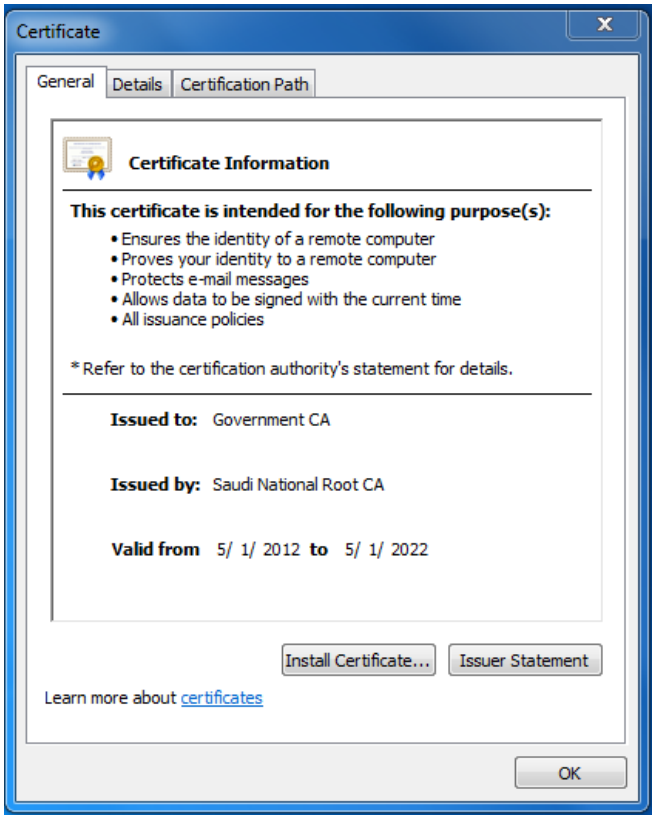
مكونات البنية التحتية للمفاتيح العامة PKI:

- **سلطة التصديق:** تمثل المرجعية في الثقة في البنية التحتية للمفتاح العام وتوفر الخدمات التي تصادق على هوية الأفراد، والحواسيب، والكيانات الأخرى في الشبكة.

- **سلطة التسجيل:** تقوم سلطة التسجيل بوظائف: التحقق الشخصي من هوية ووثائق مقدم طلب الشهادة الرقمية.
- **الشهادة الرقمية:** بنية البيانات المعرفة في المعيار X.٥٠٩ موقعة رقمياً من قبل سلطة التصديق ويتم فيها ربط هوية حامل شهادة (أو الخدمة) بالمفتاح العام.
- **قاعدة بيانات (مجلد نشط) لحفظ الشهادات الرقمية.**
- **نظام إدارة الشهادات الرقمية.**
- **بروتوكول**Simple Certificate Enrollment and Revocation : يقوم هذا البروتوكول بنقل طلبات تسجيل الشهادات الرقمية وطلبات الحصول على قائمة الشهادات الملغاة بين سلطة التصديق والمستخدم، يتم النقل عبر شبكة الإنترنت.
- **قائمة الشهادات الرقمية الملغاة:** قائمة شهادات المفتاح العام الملغية، يتم إصدار تلك القائمة والتوقيع عليها رقمياً بواسطة هيئة التصديق.
- **التنظيم الإداري:** ويشتمل على تحديد الأشخاص ووظائفهم داخل وحدة البنية التحتية للمفاتيح العامة مثل:
  - تحديد مدير لنظام البنية التحتية للمفاتيح العامة يقوم بتهيئة وصيانة النظام.
  - تحديد مسئول للشهادات الرقمية للتحقق من صحة طلبات الشهادات الرقمية وإصدار الشهادات الرقمية.
  - تحديد مدقق سجلات النظام يقوم بتدقيق الأخطاء والتحذيرات التي يقوم النظام بحفظها في سجلات التدقيق (Audit Logs).
- **التنظيم القانوني:** ويشتمل على السياسات والتشريعات التي تنظم تشغيل واستخدام البنية التحتية للمفاتيح العامة.

مثال: الشهادة الرقمية لمركز التصديق الحكومي للمركز الوطني للتصديق الرقمي في المملكة العربية السعودية. يمكن الحصول على هذه الشهادة الرقمية بالذهاب إلى مركز التصديق الحكومي أو عن طريق هذا الرابط:

http://www.ncdc.gov.sa/certs/gcasha256.crt

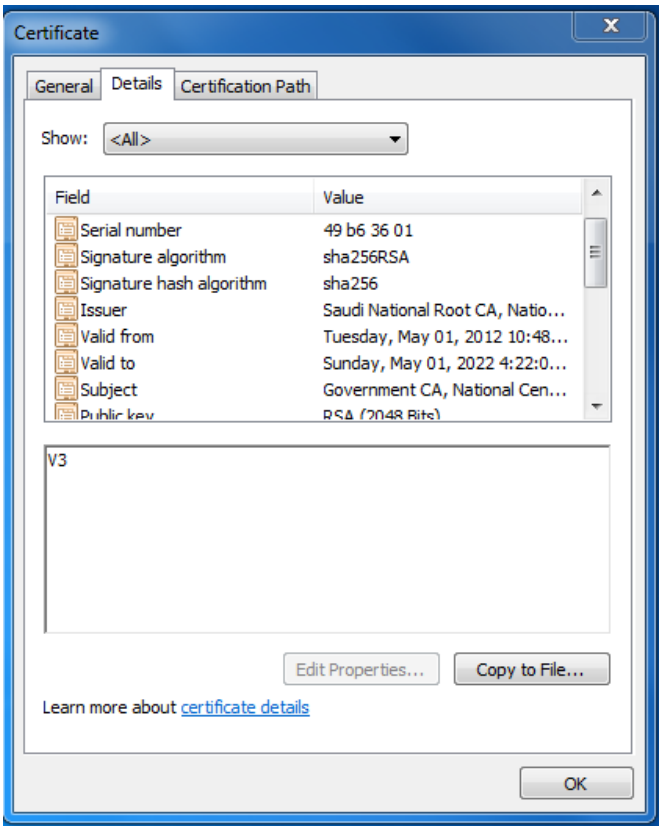


الشكل 104-٢: الشهادة الرقمية لمركز التصديق الحكومي في المملكة العربية السعودية

الحقول المهمة في الشهادة الرقمية:

- **"Issued to"**: ويعني أن هذه الشهادة أصدرت لمركز التصديق الحكومي.
- **"Issued by"**: ويظهر أن هذه الشهادة أصدرت من قبل مركز التصديق الجذري الوطني السعودي.
- **"Valid from"**: ويعني أن هذه الشهادة صالحة من التاريخ الموضح في هذا الحقل.
- **"Valid to"**: ويعني أن هذه الشهادة صالحة حتى التاريخ الموضح في هذا الحقل.

تفاصيل الشهادة الرقمية:



الشكل 105-٢: تفاصيل الشهادة الرقمية لمركز التصديق الحكومي في المملكة العربية السعودية

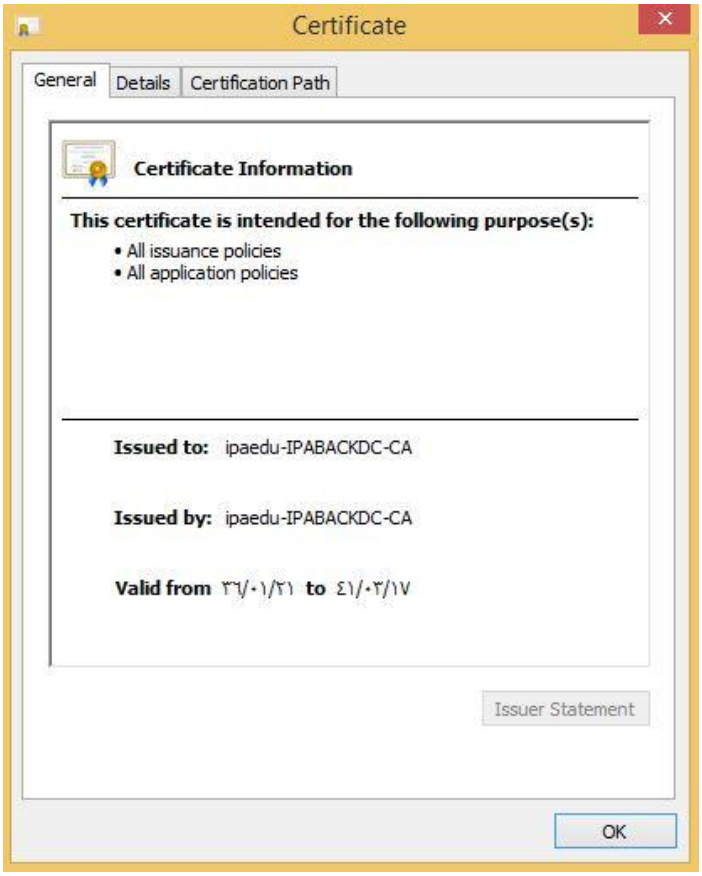
الحقول المهمة في تفاصيل الشهادة الرقمية:

- **"Signature algorithm"**: ويعني أن هذه الشهادة تم توقيعها بواسطة خوارزمية RSA
- **"Signature hash algorithm"**: ويظهر أن خوارزمية الاختزال من نوع SHA1
- **"Subject"**: ويظهر أن صاحب هذه الشهادة هو المركز الوطني للتصديق الحكومي.

تمرين عملي(١٩):

الشهادة الرقمية لمعهد الإدارة:

لكي نستعرض الشهادة الرقمية لمعهد الإدارة اذهب لصفحة الإعدادات (**Settings**) من متصفحك (**Internet Explorer**) ومن ثم توجه لخيارات الإنترنت (**Internet Options**) > المحتوى (**Content**) > الشهادات (**Certificates**) > خادم سلطة التصديق الوسيط (**Intermediate Certification Authorities**) > بعدها نقوم باختيار شهادة معهد الإدارة الرقمية.

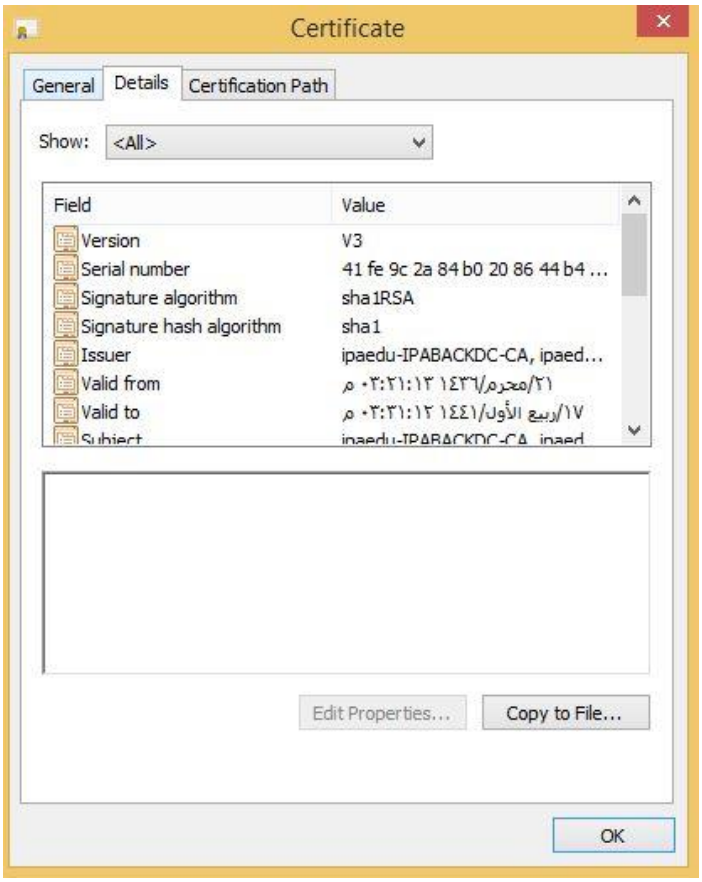


الشكل 106-٢: شهادة معهد الإدارة الرقمية.

الحقول المهمة في الشهادة الرقمية:

- **"Issued to"**: ويعني أن هذه الشهادة أصدرت لمعهد الإدارة.
- **"Issued by"**: ويعني أن هذه الشهادة أصدرت من قبل معهد الإدارة للتصديق الرقمي.
- **"Valid from"**: ويعني أن هذه الشهادة صالحة من التاريخ الموضح في هذا الحقل.
- **"Valid to"**: ويعني أن هذه الشهادة صالحة حتى التاريخ الموضح في هذا الحقل.

تفاصيل الشهادة الرقمية:

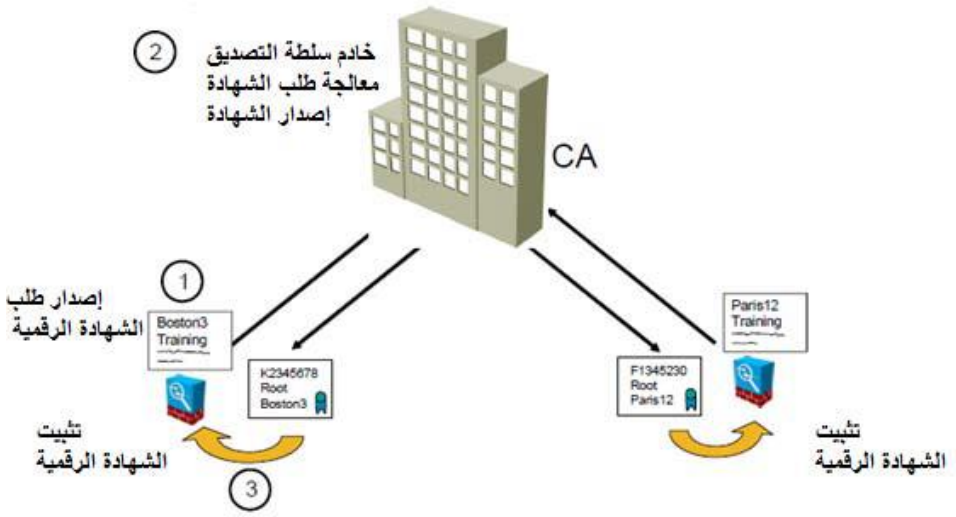


الشكل 107-٣: تفاصيل شهادة معهد الإدارة الرقمية.

الحقول المهمة في تفاصيل الشهادة الرقمية:

- **"Signature algorithm"**: ويعني أن هذه الشهادة تم توقيعها بواسطة خوارزمية RSA
- **"Signature hash algorithm"**: ويظهر أن خوارزمية الاختزال من نوع SHA1
- **"Subject"**: ويظهر أن صاحب هذه الشهادة هو معهد الإدارة.

عملية تسجيل الشهادة الرقمية:



الشكل 108-٢: عملية تسجيل الشهادة الرقمية.

المصطلح المستخدم لوصف العملية التي يتم بواسطتها حصول المستخدم على الشهادة الرقمية يشار إليه بتسجيل الشهادة الرقمية.

يلزم المستخدم أن يتقدم بطلب الحصول على الشهادة الرقمية، هذا الطلب له شكل خاص.

الطلب يجب أن يحتوي على المفتاح العام وهوية طالب الشهادة الرقمية، وبعد التأكد من هوية طالب الشهادة الرقمية يتم منحة الشهادة.

معيار PKCS # ١٠، معيار طلب الشهادة الرقمية؛ عادة ما يكون الشكل المستخدم لتقديم طلبات الشهادة الرقمية. وتشمل المعلومات في طلب تسجيل الشهادة **PKCS** # ١٠ التالي:

- المفتاح العام لطالب الشهادة الرقمية ويجب أن يوقع من قبل سلطة توثيق الشهادات الرقمية.
- الاسم المميز لطالب الشهادة الرقمية.
- التوقيع الرقمي وهو عبارة عن القيمة المختزلة للطلب موقعة بواسطة المفتاح الخاص لطالب الشهادة الرقمية.
- خوارزمية الاختزال المستخدمة في إنشاء التوقيع الرقمي الذي تم إنشاؤه في الخطوة ٣. عندما يريد المستخدم الحصول على شهادة تصديق لمفتاحه العام من سلطة تصديق، عليه الحصول على شهادة التصديق الخاصة بسلطة التصديق أولاً.

عندما تتلقى سلطة التوثيق طلب الشهادة الرقمية، تقوم سلطة التوثيق بعمل التالي:

- فك شفرة التوقيع الرقمي في طلب الشهادة باستخدام المفتاح العمومي في الطلب.
- حساب القيمة المختزلة للطلب باستخدام دالة الاختزال المستخدمة من قبل طالب الشهادة الرقمية.

- هوية الطالب أو المستخدم الذي قدم طلب الحصول على الشهادة الرقمية يتم التحقق منها من خلال حساب القيمة المختزلة للطلب ومقارنتها بالقيمة الناتجة عن فك شفرة التوقيع الرقمي في طلب الشهادة باستخدام المفتاح العمومي في الطلب.
- تقوم سلطة التوثيق بتوقيع المفتاح العام للمستخدم.
- ويتم إضافة توقيع سلطة التوقيع إلى شهادة X.٥٠٩
- تقدم الشهادة إلى المستخدم الذي طلب الحصول على الشهادة

يقوم المستخدم بنشر نسخ من شهادة X.٥٠٩ إلى الكيانات التي يمكن أن تستخدمها لتشفير البيانات التي سيتم إرسالها إلى المستخدم. أيضاً يمكن استخدام شهادة X٥٠٩ للتحقق من صحة التوقيعات.

هذه الكيانات تستطيع التحقق من هوية المستخدم صاحب الشهادة X.٥٠٩ من خلال التحقق من توقيعه باستخدام المفتاح العام للمستخدم والموجود في شهادته الرقمية. يتم التحقق من صحة الشهادة الرقمية من خلال التحقق من التوقيع الرقمي للشهادة والذي يتم إضافته من قبل سلطة التوثيق.

أنواع الشهادات الرقمية بناءَ على طبيعة الاستخدام:

- شهادة رقمية تستخدم لتصديق المفتاح العام المخصص للتشفير.
- شهادة رقمية تستخدم لتصديق المفتاح العام المخصص للتحقق من التواقيع الرقمية.

أسئلة ونقاش(٩):

س١: ما مكونات البنية التحتية للمفاتيح العمومية؟

س٢: كيف تتم عملية تسجيل الشهادات الرقمية؟

س٣: ما أنواع الشهادات الرقمية؟

إدارة مفاتيح التشفير

لأن مفاتيح التشفير تشكل الركيزة الأساسية لنظم البنية التحتية للمفاتيح فمن المهم أن تدار بعناية. وتشمل إدارة مفاتيح التشفير تخزينها، واستخدامها، والتعامل مع إجراءاتها.

تخزين المفاتيح:

تخزين المفاتيح في نظام البنية التحتية هو أمر مهم. من الممكن تخزين المفاتيح العامة عن طريق تضمينها داخل الشهادات الرقمية، في حين أن المفاتيح الخاصة تخزن على النظام المحلي للمستخدم. لكن من عيوب سبل التخزين المرتكزة على البرمجيات إمكانية تعرضها للهجمات: نقاط الضعف في نظام التشغيل العميل على سبيل المثال، يمكن أن يعرض المفاتيح للمهاجمين. تخزين المفاتيح في عتاد هو بديل للتخزين القائم على البرمجيات. يمكن استخدام أجهزة خوادم سلطة التصديق لتخزين المفاتيح العامة. ويمكن تخزين المفاتيح الخاصة على البطاقات الذكية أو جهاز الشفرة الأمنية. [٣]

استخدام المفاتيح:

إذا كانت هناك حاجة إلى رفع المستوى الأمني حيث أن زوج واحدًا من مفتاح عام وخاص لم يكن كافيًا، يمكننا إنشاء زوجان من المفاتيح المزدوجة. بحيث يستخدم الأول في تشفير المعلومات وينسخ مفتاحها العمومي في مكان آخر كالشهادة الرقمية على سبيل المثال، أما الزوج الثاني فيستخدم للتوقيعات الرقمية فقط ولا يتم إجراء النسخ الاحتياطي للمفتاح العمومي في هذا الزوج. حيث أنه في حال سرق المهاجم مفتاح التشفير العمومي لا يزال غير قادرًا على إجراء توقيعًا رقميًا للوثيقة.

إجراءات التعامل مع المفاتيح:

يوجد إجراءات معينة تساعد على ضمان التعامل مع المفاتيح بالشكل السليم. وتشمل هذه الإجراءات[٣]:

التأمين: ويشير هذا المصطلح لإدارة المفاتيح من خلال طرف ثالث لحفظها، كسلطة التصديق على سبيل المثال. في تأمين المفتاح يُقسم المفتاح الخاص لنصفين ويشفر كلًا منهما على حده. ومن ثم يتم إرسال القسمين للطرف الثالث والذي بدوره يقوم بتخزين كل قسم في مكان مختلف. بعد ذلك يمكن للمستخدم استرداد كلًا من القسمين ودمجهما بعد فك شفرتيهما ليتمكن من استخدام المفتاح مجددًا. هذا الإجراء المتبع لتأمين المفتاح يضمن للمستخدمين عدم ضياع المفاتيح الخاصة لهم. لكن العيب في هذا النظام أن المفتاح الخاص يكون عرضة للهجوم بعد فك شفرة القسمين ودمجهما.

أنتهاء الصلاحية: لدى المفاتيح تواريخ أنتهاء الصلاحية. وهذا يمنع المهاجم الذين قام بسرقة مفتاح خاص من أن يكون قادراً على فك تشفير الرسائل لفترة غير محددة من الزمن. بعض النظم تضع للمفاتيح فترة زمنية افتراضية معينة لتنتهي صلاحية المفاتيح بعدها.

التجديد: بدلًا من ترك المفاتيح حتى تنتهي صلاحيتها يمكننا إنشاء مفاتيح جديدة أو تجديد المفاتيح الحالية. في حالة تجديد المفاتيح الحالية تستخدم المفاتيح العمومية والخاصة الأصلية ولا يشترط تغييرها. لكن الاستمرار في تجديد صلاحية المفاتيح الأصلية يجعلها عرضة للسرقة وسوء الاستخدام مع مرور الوقت.

الإبطال: بما أن جميع المفاتيح لها تاريخ صلاحية وينتهي خلال فترة زمنية معينة، قد نحتاج لإبطال المفتاح قبل مجيء تاريخ أنتهاءه في بعض الحالات كما في حالة استقالة الموظف فنحن بحاجة لإبطال المفتاح الخاص الذي بحوزته. ولا يمكن إعادة المفاتيح التي أبطلت صلاحيتها أبدًا.

الاستعادة: هناك تقنيات مختلفة يمكن استخدامها لاستعادة المفاتيح، فبعض سلطات التصديق لديها نظام مضمن لاسترداد المفاتيح الخاصة وهو نظام مسؤول عن استرداد المفاتيح أو الشهادات الرقمية التالفة.

التعليق: الإبطال هو إيقاف دائم للمفتاح، لكننا قد نحتاج إيقاف المفتاح لفترة زمنية ومن ثم إعادة صلاحية المفتاح وهذا ما يسمى بالتعليق.

التدمير: في هذه الحالة يدمر كلًا من المفاتيح العمومية والخاصة جنبًا إلى جنب مع بيانات هوية المستخدم لدى سلطات التصديق الرقيمة.

أسئلة ونقاش(١٠):

س١: ما السبل الممكنة لتخزين المفاتيح؟

س٢: اذكر الإجراءات اللازمة للتعامل مع المفاتيح مع ذكر مثال يحقق الحاجة إلى استخدام تلك الإجراءات؟

معهد الإدارة العامة
INSTITUTE OF PUBLIC ADMINISTRATION

شرائح اليوم التدريبي الثاني

سياسات أمن المعلومات

- **السياسة الأمنية Security Policy**
  - **السياسة الأمنية العامة**
  - **السياسة الأمنية الموضوعية:**
    - استخدام البريد الإلكتروني.
    - سياسة تصنيف البيانات من حيث السرية.
    - سياسة تأمين الشبكة.
    - سياسة الاستخدام المقبول للإنترنت.
    - سياسة كلمة المرور.

السياسة الأمنية الموضوعية

- **تطبيق**

يتم تقسيم المتدربين إلى مجموعات.كل مجموعة تقوم بعمل سياسة أمن المعلومات الخاصة بالاستخدام المقبول للإنترنت.

ثغرات الشبكات و الهجمات عليها

١- ثغرات متعلقة بالوسائط

٢- ثغرات أجهزة الحاسوب:

- كلمة المرور الضعيفة
- الحساب الافتراضي
- الباب الخلفي
- تصعيد الامتيازات

أنواع هجمات الشبكات

- تعطيل الخدمة Denial of service DoS
- التحايل Spoofing
- رجل في المنتصف Man-in-the-middle
- هجمات الإعادة Replay attacks

ثغرات الشبكات و الهجمات عليها

١- ثغرات متعلقة بالوسائط

٢- ثغرات أجهزة الحاسوب:

- كلمة المرور الضعيفة
- الحساب الافتراضي
- الباب الخلفي
- تصعيد الامتيازات

أنواع هجمات الشبكات

- تعطيل الخدمة Denial of service DoS
- التحايل Spoofing
- رجل في المنتصف Man-in-the-middle
- هجمات الإعادة Replay attacks

دفاعات الشبكة

- **تصميم شبكة آمنة:**
  - الشبكات الفرعية Subnetting
  - الشبكات المحلية الافتراضية Virtual LANs
  - منطقة منزوعة السلاح Demilitarized zone DMZ

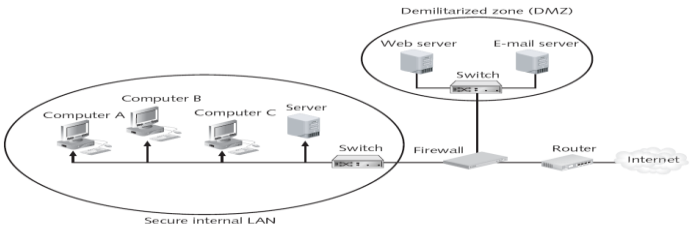


Figure 5-4 Demilitarized zone (DMZ) with single firewall

تطبيق أجهزة أمن الشبكات

- الجدار الناري Firewalls
- خادم البروكسي Proxy servers
- المصيدة Honeypots

استخدام الجدار الناري windows 8

تطبيق عملي:

- خطوات التفعيل
- إنشاء قواعد جديدة

التشفير

يتكون من عمليتين أساسيتين هما:

- التشفير
- فك التشفير

مصطلحات التشفير:

- النص الصريح Plain Text
- النص المشفر Cipher Text
- التشفير Encryption
- فك التشفير Decryption
- خوارزمية فك التشفير
- تحليل الشفرة (كسر الشفرة)
- المفتاح السري (Key)

أنواع التشفير

١- التشفير المتناظر: هو نظام تشفير يستخدم مفتاحاً متناظراً لدى كل من المرسل والمستقبل، بحيث يُستخدم نفس المفتاح في عمليتي التشفير وفك التشفير.

٢- التشفير غير المتناظر:

- لا يوجد مفتاح سري مشترك بين المرسل والمستقبل منذ البداية، وإنما يتم استخدام مفتاحين منفصلين يستخدم أحدهما للتشفير، والآخر (مرتبط بالأول) لفك التشفير.
- يولّد كل مستخدم زوجاً من المفاتيح مرتبطين بعضهما ببعض (بطريقة رياضية معقدة لا تسمح بكشف أي منهما إذا تم معرفة الآخر) أحدهما عام ويوضع في سجل (مجلد) عام يمكن الاطلاع عليه من قبل جميع المستخدمين، والآخر خاص ويعتبر مفتاحاً سرياً خاصاً بالمستخدم ويجب ألا يطلع عليه الآخرين.

مقارنة بين التشفير المتناظر وغير المتناظر

التشفير غير المتناظر	التشفير المتناظر
١- يتم استخدام نفس الخوارزمية للتشفير وفك التشفير. ٢- يستخدم زوج من المفاتيح أحدهما عام يطلع عليه الآخرون، والآخر سري خاص بكل مستخدم (ليس نفس المفتاح عند المرسل والمستقبل). ٣- لا يحتاج إلى عملية توزيع المفاتيح.	١- يتم استخدام نفس المفتاح عند المرسل، والمستقبل ونفس الخوارزمية لكل من عملية التشفير وفك التشفير. ٢- يجب إن يتم توزيع المفتاح السري بطريقة آمنة. ٣- يحتاج إلى عملية توزيع آمنة للمفاتيح السرية.

بعض أساليب التشفير

- **الانتقال العمودي (Columnar Transposition) :**إن التشفير بطريقة الانتقال العمودي تتطلب إزاحة أعمدة الرسالة النص الصريح والمرتبة أصلا بشكل مستطيل.
- **الاحلال التخطيطي(Diagraphic Substitution):** مثل شفرة بليفير Playfair Cipher

---

بعض أساليب التشفير

تدريب ١ :

يقوم كل متدرب بفك التشفير عن النص التالي:

STTSW EOYEE @ICCL INOUC PFURO AORIM

علماً بأن خوارزمية فك التشفير:

التشفير بطريقة الانتقال العمودي للنص والمكون من مستطيل يحتوي على ٦ صفوف و ٥ للنص المشفر والمأخوذ بالأسلوب الأفقي

كما أن مفتاح ترتيب الأعمدة هو ١ ٣ ٤ ٢ ٥

تدريب ٢ :

يقوم كل متدرب باستخدام طريقة الانتقال العمودي للتشفير، من خلال تشفير نص رسالة ومن ثم عرض النص المُشفر مع خوارزمية فك التشفير على زميل ليقوم بفك شفرة الرسالة.

شفرة بليفير Playfair Cipher

تدريب ٣:

يقوم كل متدرب باستخدام شفرة بليفر (The Playfair Cipher) بفك التشفير عن النص التالي:

ZN QS PY HL NO GC

علماً بأن مصفوفة التشفير هي

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

تدريب ٤:

يقوم كل متدرب باستخدام شفرة بليفير لتشفير نص رسالة ومن ثم عرض النص المُشفر مع المصفوفة (مفتاح التشفير) على زميل ليقوم بفك شفرة الرسالة.

تطبيقات التشفير

تطبيقات عملية على التشفير:

- تشفير رسائل Gmail
- استخدام مواقع التشفير مثل Infoencryp
- تشفير الملفات والمجلدات باستخدام Axcrypt
- تشفير Rohos mini drives USB

شهادات التعريف الرقمية وبنية المفتاح العمومي PKI

البنية التحتية للمفاتيح هي مجموعة من الأجهزة والبرامج والأشخاص والسياسات والإجراءات اللازمة لإنشاء وإدارة وتوزيع واستخدام وتخزين، وإلغاء الشهادات الرقمية.

في التشفير، البنية التحتية للمفاتيح العامة هي الترتيب الذي يربط المفاتيح العامة مع هوية المستخدم عن طريق سلطة تصديق الشهادات الرقمية. وسلطة تصديق الشهادات الرقمية (CA) هي الكيان الذي يقوم بمنح الشهادات الرقمية.

أمثلة على بعض سلطات التصديق الرقمي التجارية	أمثلة على شركات تقدم برمجيات لإدارة إصدار الشهادات الرقمية
Entrust	Microsoft
VeriSign	Entrust
idenTrust	Comodo
Comodo	VeriSign

معهد الإدارة العامة
INSTITUTE OF PUBLIC ADMINISTRATION

اليوم التدريبي الثالث

اليوم التدريبي الثالث

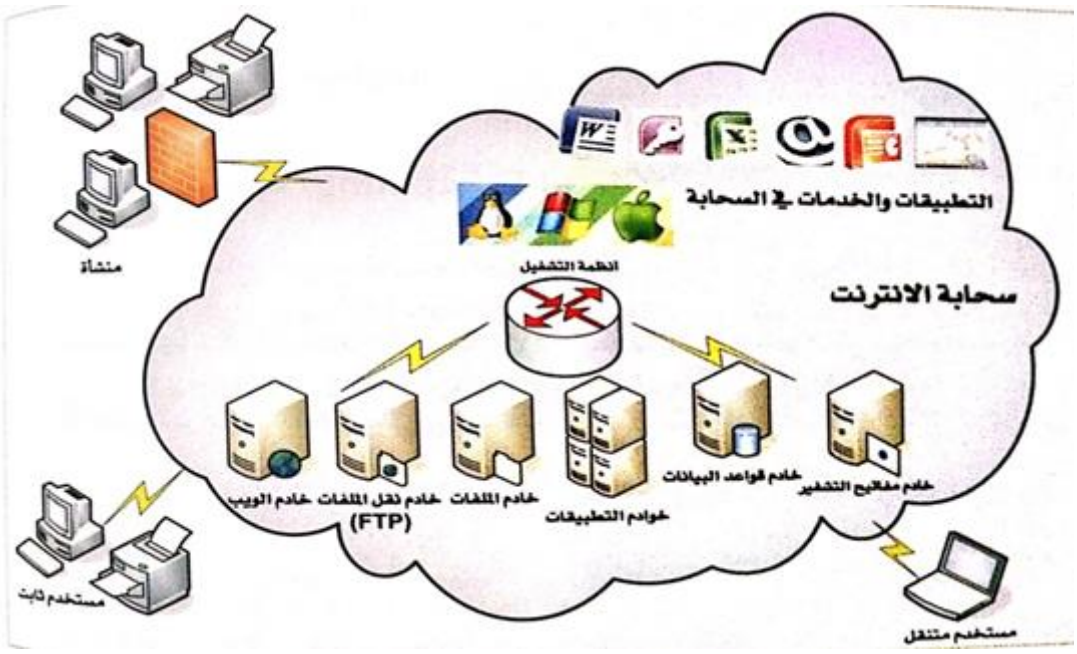
الجلسة	الموضوع التدريبي	الزمن	الهدف السلوكي
الأولى	❖ الأمن والحوسبة السحابية. ❖ أساسيات التحكم في الوصول.	٩٠د	❖ التعرف على الحوسبة السحابية واستخداماتها. ❖ التعرف على أمن المعلومات في الحوسبة السحابية. ❖ التعرف على التحكم في الوصول والتمييز بين طرقه.
الثانية	❖ المصادقة. ❖ تقييم الثغرات.	٩٠د	❖ التعرف على ماهية التصديق وطرق تفويضها. ❖ التعرف على المخاطر وكيفية تخفيف أضرارها وإدارتها. ❖ التعرف على الثغرات وإمكانية تحديدها في بيئة أمن المعلومات.
الثالثة	❖ استمرارية العمل.	١٢٠د	❖ التعرف على كيفية التحكم بالمخاطر البيئية. ❖ تطبيق الإجراءات اللازمة لاسترداد البيانات في حالة حدوث الكوارث. ❖ مناقشة الحالات الفردية للمتدربين

اليوم الثالث - الجلسة التدريبية الأولى

الأمن والحوسبة السحابية

الكثير منا يحتاج إلى تركيب أنظمة التشغيل والبرامج التطبيقية على جهازه الخاص لاستخدامها في أعماله اليومية الرقمية، كإعداد الوثائق، وكتابة الخطابات، وإرسال واستقبال البريد الإلكتروني، وتصفح الإنترنت والتواصل مع الآخرين. والسؤال المطروح هنا هو: لماذا يضطر المستخدم إلى شراء هذه الأنظمة والبرامج والخدمات وتملكها بشكل دائما وتحديثها وصيأنتها على الرغم من أنه لا يحتاجها كل الأوقات وقد لا يحتاج الكثير من أجزائها وإمكانياتها المتقدمة التي يدفع ثمنها ولا يستخدمها؟ والجواب عن هذا السؤال هو: استخدام تقنية الحوسبة السحابية. فالحوسبة السحابية، تشبه الإنترنت بأنها سحابة توجد بها جميع تلك الأنظمة والبرامج والخدمات، وكل ما يحتاجه المستخدم هو الأخذ منها بالقدر الذي تحتاج إليه فقط، تاركًا مهمة التطوير والتحديث والصيانة لمقدمي خدمة السحابة. [٤]

وبشكل عام يمكن تعريف الحوسبة السحابية بأنها: "تقديم الأنظمة والبرامج والعمليات الرقمية المختلفة كخدمات عبر الإنترنت، وليس كمنتجات (Products) مستقلة يلزم تواجدها لدى المستخدم"، انظر للشكل(١٠٣-٣):



الشكل 109-٣: الحوسبة السحابية

ويمكن تشبيه خدمات الحوسبة السحابية بخدمات تقديم الطاقة الكهربائية، حيث يمكن للمستفيد الحصول على الطاقة مباشرة دون الاكتراث بطريقة توليدها، ومن أين تأتي، ومن يديرها ويقوم على صيأنتها.

وتدعم تقنية الحوسبة السحابية حرية التنقل للمستخدم (حول العالم)، مع استمراره في أداء أعماله الإلكترونية من أي مكان، في ظل وجود جميع ما يحتاج إليه من أجهزة وأنظمة وبرامج وخدمات في

السحابة، كما أنها طريقة مثلى للتخلص من إدارة تلك المكونات وصيأنتها والتركيز على عمله الأساسي.

المفهوم الأساسي للحوسبة السحابية:

على عكس ما تحتاجه الحوسبة التقليدية التي نستخدمها من وجود كل البيانات والبرامج والتطبيقات التي تستعمل وينشئها المستخدم على أجهزته الخاصة، فإن " الحوسبة السحابية " تقوم على عدم الحاجة إلى مستخدم لتخزين أي من بياناته على أجهزته الخاصة وعدم حاجته إلى برامج متنوعة أو معقدة ربما يحتاج لبعض منها فقط، لذا كل ما يستخدم وما يحدث من عمليات ومن البرامج ووصوله إلى ملفاته وبياناته المخزنة على حاسبات عبر الشبكات بعيدة عنه. وقد انتشرت في السنوات القليلة الماضية مصطلحات كثيرة ترتبط بالحوسبة السحابية وبعدة أشكال مختلفة، فهناك خدمات التخزين السحابية، الموسيقى السحابية والتطبيقات السحابية بل وحتى أنظمة التشغيل السحابية. [٥]

طبقات الحوسبة السحابية:

تصنف خدمات الحوسبة السحابية في شركة ما إلى ثلاثة تصنيفات (طبقات) فوق بعضها البعض كالتالي (من الأسفل للأعلى):

البنية التحتية كخدمة (Infrastructure as a Service IaaS): في هذه الطبقة يتم توفير أجهزة الشركة كخدمة للمستخدم، بحيث يمكن أن يستأجر موارد الشركة من أجهزة خادم، أجهزة تخزين... إلخ عن بعد بدون الحاجة إلى شراء، إدارة، وصيانة أجهزته الخاصة والتي غالبا ما تكون تكلفتها عالية. تقوم الشركة المستضيفة بالتعامل مع كل هذه الأشياء بدون الحاجة إلى تدخل العميل. مثال على ذلك شركات استضافة المواقع.

منصة العمل كخدمة (Platform as a Service Paas): هذه الطبقة توفر منصة عمل لتطبيقات المستخدم شاملة الأجهزة التي يحتاجها في تطوير البرمجيات بالإضافة إلى التطبيقات الأساسية المطلوبة في عملية البرمجة مثل الخوادم الافتراضية وأنظمة التشغيل. توفر هذه الطبقة على المستخدم تكلفة تأسيس الأجهزة بالإضافة إلى تكلفة شراء التطبيقات الأساسية التي يحتاجها في عمله. مثال على ذلك Google app engine و Microsoft Azure.

التطبيق كخدمة (Software as a Service Saas): الكثير منا يتعامل مع مخرجات هذا الطبقة يوميا بشكل أو بآخر. هي البرمجيات التي يتعامل معها المستخدم عن طريق الإنترنت، مثل"DropBox"، مستندات جوجل، وغيرها، حيث لا دخل للمستخدم في الأجهزة التي تديرها، ولا البرمجيات التي بنيت عليها، ولكن يتعامل مع الناتج النهائي لتلك التطبيقات.

أنواع الحوسبة السحابية:

- **السحابة الخاصة (Private Cloud Computing):** هي بنية تحتية يستأجرها عميل واحد وتعمل لحسابه الخاص تحت سيطرته الكاملة على البيانات، والأمن، وجودة الخدمة.
- **السحابة العامة (Public Cloud Computing):** هي بنية تحتية توفر موارد الحوسبة بشكل حيوي عبر الإنترنت لعدة عملاء، وعادة تكون تطبيقات العملاء المختلفين مختلطة معا على خوادم السحابة.
- **السحابة الهجينة (Hybrid Cloud Computing):** تجمع نماذج سحابية عامة وخاصة متعددة. والسحب الهجينة تعرض العملية المعقدة لتحديد كيفية توزيع التطبيقات عبر كلاً من السحابة الخاصة والعامة.

الأمن في الحوسبة السحابية:

يثير موضوع أمن معلومات السحب الإلكترونية الكثير من الجدل، فالبعض يرى أن المعلومات لا تكون آمنة إلا عند إدارتها في شبكة داخلية، والبعض الآخر يرى أن السحب الإلكترونية تستطيع توفير الأمن اللازم لضمان حفظ المعلومات وسلامتها. يمكن القول إن مشكلات أمن المعلومات في السحب الإلكترونية تأتي من جهتين: موفر الخدمة والعميل، لكن الحمل الأكبر دائما يقع على عاتق موفر الخدمة، فهو الملزم بتوفير بنية تحتية قوية وأدوات ومستودعات تخزين آمنة، خصوصا إذا ما كان سيأخذ مقابلاً ماديا عليها.

يعمد موفرو الخدمة عادة إلى التركيز على الأوجه التالية من أجل ضمان حفظ المعلومات على السحابة الإلكترونية:

الشكل 110-٣: الأمن في الحوسبة السحابية

حماية البيانات: ضمن هذا النطاق العريض يمكن القول بأن أساسيات معالجة البيانات وتخزينها تبقى هي الأولوية، بالإضافة لتعريف الأصول الموجودة وتوقع الهجمات المحتملة، فمن جهة العميل عند القيام بأي عملية معالجة وتخزين للبيانات ينبغي عليه التأكد من جودة اتصاله بالإنترنت وأنه قام فعلا بتخزين الملف على الشبكة وأن معلومات حسابه لا يعلمها أحد سواه، ومن جهة موفر الخدمة فإنه سيحرص دائما على حفظ معلوماتك وعدم تسربها إجمالا بمنع دخول أي طرف ثالث في الحساب. [٤]

نظام إدارة الهوية: وهو نظام معلومات يهدف إلى التحقق من هوية المستخدم والتأكد من أنه الصاحب الحقيقي للحساب، ولزيادة الحماية يمكن أن يكون موجودا بشكل أفضل من طرف العميل (الموظف) في منشأة تعمل على السحب الإلكترونية.

الأمن المادي: ويأتي من جانب مزود الخدمة، حيث يجب عليه التأكد من جودة الشبكة والتطبيقات والخوادم التي يستعملها وعدم وجود أي ثغرات أمنية بها، ويمكنه دائما عمل ذلك عن طريق اختبار الاختراق (PenetrationTest) والذي يفحص جميع الأجهزة والأنظمة ومتعلقاتها بهدف اكتشاف ما بها من نقاط ضعف وثغرات يمكن أن يستغلها أي مخترق من أجل الحصول على المعلومات.

أمن التطبيقات: في السحب الإلكترونية التي تقوم بتوفير أدوات معالجة البيانات والأدوات البرمجية التي تساعد المستخدم على تطوير أي كود برمجي وتجربته ينبغي أن تكون هذه الأدوات دائما على قدر عالي من الكفاءة، حيث يجب أن يتميز أداءها بالسلاسة وعدم حفظ البيانات غير المهمة وتشتيت المستخدم بما لا ينفع، حيث يمكن لهذه الأدوات أن تكون أداة في تسرب أي بيانات مهمة للمستخدم.

الخصوصية: تبقى هي السمة الأبرز التي يجب أن يحرص كل مزود للخدمة على توفير السياسات والإجراءات المناسبة التي تصاحبها لما في ذلك من حفظ لحقوق العميل ومزود الخدمة، كما أنها تعطي إجمالا رسالة واضحة عن احترافية وقوة مزود الخدمة وعدم تهاونه في الاحتياط من محاولات العابثين.

مثال على الخصائص الأمنية التي يوفرها أحد مزودي الخدمة السحابية "AWS":

يعتبر مزود خدمات الإنترنت أمازون "AWS" إحدى الشركات الأولى والأساسية في تقديم خدمات الحوسبة السحابية والتي بدأت في هذا المجال عام ٢٠٠٦. تقدم هذه الشركة العديد من الخصائص الأمنية التي تضمن للمستخدم توفير بيئة أمنية جيدة للحوسبة السحابية. من الأمثلة على تلك الخدمات الأمنية:

أمن الشبكات: حيث توفر أمازون عدة خيارات لأمان الشبكة للمساعدة في المحافظة على مواردك الحاسوبية والاتصالات بشكل آمن كما تريد من خلال:

- وصول آمن للشبكة من خلال استخدام "HTTPS Access".
- استخدام جدار ناري مدمج "Built in firewall" مع إمكانية التحكم الكامل.
- أنتقال البيانات بين الخادم والعميل يكون مشفر بشكل كامل حيث يدعم كل من تشفير"SSL/TLS".
- إمكانية استخدام "VLAN"، حيث يمكن تقسيم الاتصال إلى عدة اتصالات منطقية للسماح لك بالدخول باستخدام كل من بيئتي "Private and Public IP" للسحابة الخاصة بك.

التحكم في الوصول: حيث يُسمح فقط للمخولين من مستخدمين، عملاء وتطبيقات بالوصول إلى موارد الحوسبة السحابية الخاصة بك عن طريق ضبط سياسات التحكم بالوصول، حسابات المستخدمين الفردية والاعتمادات الفريدة. يتم ذلك من خلال العديد من الخصائص منها:

- طلب المصادقة: من خلال واجهة تطبيق البرنامج حيث يتم طلب المصادقة في كل عملية والتوقيع عليه رقمياً باستخدام دالة تجزئة التشفير ومفتاح الوصول السري الخاص بك.
- توفير أداة "IMA Identify and Access Management " والتي تتيح لك التحكم الكامل في مستويات الوصول للمستخدمين والأنظمة في موارد بيئتك السحابية.
- إمكانية إعطاء الصلاحيات المؤقتة من خلال إعطاء بعض الصلاحيات لبعض المستخدمين الذين عادة ليس لهم صلاحيات الوصول لموارد بيئتك السحابية.

المتابعة والتسجيل: من خلال توفير العديد من الأدوات التي تساعدك على تتبع وحفظ مسار مواردك السحابية، بحيث يكون لديك الرؤية الفورية لجميع العمليات لأنشطة المستخدمين والتطبيقات الخاصة بك. يتم ذلك من خلال الخصائص التالية:

- تحديد الأصول وطرق الربط وذلك من خلال خدمة "Config Service" والتي تتيح لك اكتشاف فوري لجميع موارد بيئتك السحابية وطرق ربط كل منها.
- سجلات الأمان والتي تقوم بتسجيل جميع نشاطات المستخدم في بيئتك.
- مراقبة الموارد والتطبيقات من خلال إمكانية رصد لأداء الموارد في البيئة السحابية.
- التحديد الآلي للثغرات الأمنية من خلال إعطاء تنبيهات آلية مثلاً عند وجود ضعف في سياسات كلمات المرور.

النسخ الاحتياطي والمتماثل: في كثير من الحالات يقوم مزود الخدمة في الحوسبة السحابية بتقديم النسخ الاحتياطي بشكل آلي وفي البعض منها تستطيع اختيار وربط خيارات متعددة للنسخ الاحتياطي.

تشفير البيانات: حيث يتم استخدام التشفير كلما كان ذلك ممكن، وإتاحته للعملاء لاستخدامه

كذلك. كما أن هناك لوائح أمنية لتشفير البيانات يجب أن يقوم العملاء بإتباعها.

أسئلة ونقاش(١١):

س١: ما الحوسبة السحابية؟

س٢: اذكر أنواع الحوسبة السحابية؟

س٣: كيف يمكننا تحقيق الأمن في الحوسبة السحابية؟

أساسيات التحكم في الوصول

ما التحكم في الوصول؟

وهو عبارة عن إجراءات وقوانين تتخذ للحفاظ على سلامة الموارد في النظام أو الشبكة، مثل السماح لبعض المستخدمين للوصول لبيانات معينة وعدم السماح لمستخدم آخر من الوصول إليها.

وذلك يكون بسبب اختلاف المناصب بالنسبة للمستخدمين واختلاف الحاجة لكل مستخدم للاستفادة من النظام وبياناته وموارده لئلا يستطلع بعض المستخدمين على البيانات أو يقومون باستخدام موارد ليست لهم أحقية في استخدامها أو الاطلاع عليها. ويحقق التحكم في الوصول إما بشكل فيزيائي كاستخدام الأبواب والأسقف والأجهزة، أو بشكل منطقي كاستخدام البرمجيات والسياسات الأمنية الموضوعة. [٣]

أهم مصطلحات التحكم في الوصول:

- **الهوية (identification):** وهي عبارة عن رموز أو أرقام أو شهادة تثبت الهوية، مثل أوراق اعتمادية لإثبات الهوية.
- **التحقق من الهوية أو المصادقة (Authentication):** وهو عملية التحقق من هوية المستخدم والمصادقة على صحة ما يثبت هويته واعتمادها.
- **الترخيص والتفويض (Authorization):** إعطاء الإذن والسماح للمستخدم المثبتة هويته بإكمال المهمة المراد عملها.
- **الوصول (Access):** ويمنح المستخدم الوصول أو العبور لإنجاز مهمته.

التحكم في الوصول منطقيًا: يمكننا تحقيق التحكم في الوصول بشكل منطقي عن طريق قائمة التحكم في الوصول وقيود الحسابات.

قائمة التحكم في الوصول (ACL):

هي قائمة بالصلاحيات المخصصة للفاعل(subject) للقيام بعمليات محددة(operation) على المفعول به (object). عندما يقوم الفاعل بطلب تنفيذ عملية ما، يقوم النظام بالاطلاع على قائمة التحكم في الوصول للمصادقة على الصلاحيات المسموحة لهذا الفاعل.

قيود الحساب:

قيود لحظة الاستخدام: قيود توضع على المستخدم عند دخوله النظام لاستخدامه. وقد تكون هذه القيود للنظام المستخدم من قبل مجموعات أو حتى الاستخدام الفردي.

صلاحية أنتهاء الحساب: الحسابات التي قد تسبب مشكلة في أمن المعلومات:

- الحساب اليتيم: وهو الحساب الذي يتركه الموظف لدى الشركة التي كان يعمل لديها.
- الحساب الساكن: وهو الحساب الذي لم يستخدم لفترة طويلة من الزمن.

توصيات للتعامل مع الحساب اليتيم والحساب الساكن:

- مراقبة الحسابات لمعرفة الحسابات التي لم تستخدم لفترة أو ترك أصحابها العمل.
- وضع تاريخ صلاحية أنتهاء للحسابات، بحيث تلغى فورا عند أنتهاء مدة صلاحيتها.

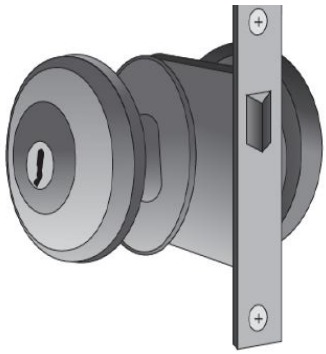
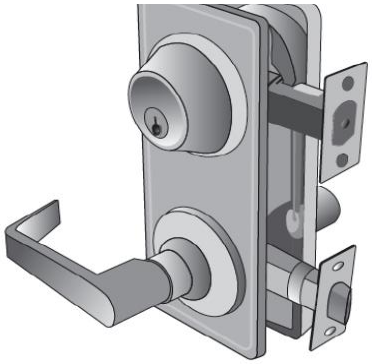
نماذج التحكم في الوصول:

- **إلزامية**(MAC Mandatory Access Control): هو الأقل مرونة بين النماذج، تستخدمه الجهات التي تريد تحقيق أعلى درجات الأمان. مثل: وزارات الدفاع وغيرها من الوزارات الأمنية.
- **تقديرية** (DAC Discretionary Access Control): هو الأكثر مرونة بين النماذج حيث يعطي تحكم كلي للمستخدمين، مثل: نظام التشغيل الذي يحوي على صفحة إعداد لصلاحيات المستخدمين يقوم بوضعها صاحب الجهاز.
- **مبنية على قوانين ثابتة** (R-BAC Role Based Access Control): تستخدم لوضع أدوار معينة ومن ثم يتم إسناد المستخدمين المحددين تحت هذه الأدوار، وذلك لاختصار الوقت بدلًا من وضع صلاحيات لكل مستخدم. مثال: البوابة الإلكترونية للجامعات، حيث يتم إسناد دور "طالب" لكل الطلاب ودور "عضو هيئة تدريس" لأعضاء هيئة التدريس، فكل مستخدم على حسب دوره يقوم بالدخول على الحساب المناسب له والذي يتيح له صلاحيات معينة.
- **مبنية على قوانين ديناميكية** (RB-BAC Rule Based Access Control): وهو نموذج مشابه للنموذج السابق، ولكن يستخدم أكثر من نظام لإنشاء وإسناد الأدوار حيث يصبح بشكل ديناميكي.

التحكم في الوصول فيزيائياً:

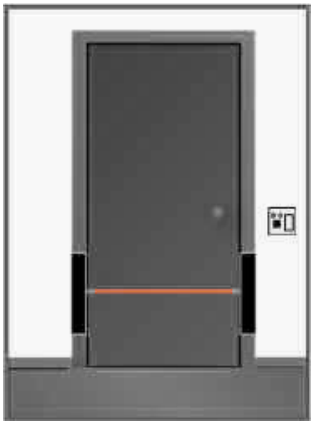
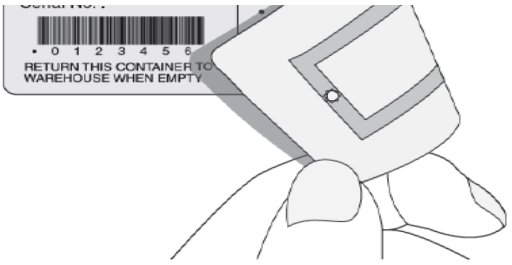
يتم حماية الممتلكات التي تحوي معلومات مهمة عن طريق حمايتها فيزيائيًا بمواد وأقفال معينة. ويشمل التحكم في الوصول المادي أمن الحاسوب، أمن أبواب الدخول، والمراقبة بالفيديو، وسجلات الدخول.

ونأخذ على سبيل المثال أمن الأبواب:

 الشكل 111-٣: الأبواب المزودة بأقفال مفتاحية.	١-الأبواب المزودة بأقفال مفتاحية: هو يعتبر الحد الأدنى من الحماية لأنه يمكن فتحه بسهولة بواسطة أي قطعة بلاستيكية مثل بطاقة صراف وغيرها.
 الشكل 112-٣: الأبواب المزودة بأقفال مفتاحية مزدوجة.	٢-الأبواب المزودة بأقفال مفتاحية مزدوجة: تمت إضافة قطعة معدنية صلبة للباب لزيادة الحماية عن النوع السابق، لذلك يعتبر أصعب للاختراق عن النوع السابق.

توصيات للحماية عند استخدام الأقفال المفتاحية:

- تغيير القفل فور ضياع المفتاح.
- التحقق وفحص الأقفال والمفاتيح دورياً.
- الاحتفاظ بسجل لمن لديهم المفتاح ومن يمكن أن يستخدمه.
- متابعة مشكلات الأقفال والمفاتيح.
- المفتاح الرئيسي يجب ألا يتم نسخه.

 الشكل 113-٣: الأقفال التي تستخدم الشفرات.	٣-الأقفال التي تستخدم الشفرات: ○ بديل أفضل للأقفال التقليدية. ○ أرقام تسلسلية ممزوجة لفتح الباب. ○ يمكن برمجتها لتفتح في فترات محددة ومن ثم تنتهي صلاحيتها. ○ تحتفظ بسجل بأوقات فتح الباب وبأي رمز ويعود ذلك لأي شخص.
 الشكل 114-٣: أجهزة استشعار الدخول.	٤-أجهزة استشعار الدخول: أجهزة استشعار تستخدم الأشعة الحمراء وتوضع على المدخل للتنبيه حينما يقوم بعبورها شخص ما. وغالبا ما تستخدم جنبا إلى جنب مع الأقفال السابقة "الأقفال التي تستخدم الشفرات".
 	٤-شارة التعريف: وهي هوية إلكترونية مثل بطاقة ممغنطة يحملها الموظف حيث تحوي بيأنته فتسمح له بفتح بعض الأبواب المصرح له بالدخول اليها.

جدول 3: الوصول المادي عن طريق الأبواب وتطورها الأمني.

حالة دراسية (٤):

يتم توزيع المتدربين إلى مجموعات، ومن ثم تقوم كل مجموعة بالعمل على الحالة الدراسية التالية:

علي يعمل محقق في هيئة التحقيق والادعاء العام، كان قد حقق علي في جريمة قتل واستند في تلك القضية على أدلة كسلاح الجريمة وعليه بصمات القاتل، لباس المجرم وعليه بقع من دماء القتيل.إلخ. بعد أسابيع من إصدار الحكم، قرر المتهم هو ومحاميه الطعن في الحكم وطلب إعادة المحاكمة. بطبيعة الحال رفع طلب إعادة المحاكمة وجهز فريق تحقيق وقاضي جديد. فكر فريق التحقيق الجديد بالتحقق من الأدلة مجددًا، فاتجه الفريق لغرفة الأدلة الجنائية. كانت الصدمة أن الرقم المرجعي للدليل كان يعود لشيء يبعد كل البعد عن الأدلة في القضية! حينها رفع محضر للتحقيق مع المحققين المصرح لهم بالدخول إلى غرفة الأدلة الجنائية لمعرفة ما حصل، وأنتهى ذلك المحضر بلا فائدة مرجوة أو دليل إدانة سواء للمحققين أو المجرم. فكاميرات المراقبة قد أظهرت دخول وخروج العديد من المحققين لبوابة غرفة الأدلة، لكن جميع ردودهم كانت تبرر أن ذلك كان لتفحص أدلة في قضايا أخرى. لم تستطع الهيئة حينها اتخاذ أي إجراء. لكنها قررت تدعيم المستوى الأمني المادي لغرفة الأدلة الجنائية.

صمم أنت ومجموعة من زملائك نظامًا أمنياً **ماديًا** متكاملاً لحماية الأدلة.

أسئلة ونقاش(١٢):

س١: ما التحكم في الوصول وما أهم مصطلحاته؟

س٢: ما أنواع التحكم في الوصول؟

اليوم الثالث – الجلسة التدريبية الثانية

المصادقة

والمصادقة هي التحقق من هوية الشخص وأنه الشخص المعني لا غيره. فإن التحقق من الهوية هو التحقق من أن المستخدم للنظام هو بالفعل من ادعى أنه ذلك المستخدم وفي حال نقل المعلومات فإنه يجب التحقق من هوية المرسل لضمان أن المعلومات قادمة من مصدرها الحقيقي، وكذلك يجب التحقق من هوية المستلم لضمان أن المعلومة ذاهبة إلى وجهتها الصحيحة. [٤]

- **يمكننا تحقيق المصادقة بثلاثة طرق:**
  - ماذا تعلم؟ (كلمة المرور).
  - ماذا لديك؟ (جهاز الشفرة الرقمية / البطاقة الذكية).
  - من أنت؟ (معياري / سلوكي).

الشكل 116-٣: طرق المصادقة.

ماذا تعرف؟

كما يحدث عند تسجيل دخول المستخدم إلى النظام:

• يتم سؤال المستخدم لتحديد شخصه:

-يدخل اسم المستخدم

• يتم طلب المصادقة عن طريق ما يعرفه " كلمات المرور هي النوع الأكثر شيوعا من التوثيق":
- يدخل كلمة المرور

الهجوم عن طريق كلمة المرور:

الهندسة الاجتماعية: وهو حين يقوم المهاجمون بتجميع بيانات عن الشخص المراد الهجوم على حسابه، ويتم تجميع تلك المعلومات عن طريق الشبكات الاجتماعية مثلًا.

الالتقاط: ويكون عن طريق استخدام بعض الأدوات لالتقاط كلمة السر لاختراق الحسابات، مثل: مسجل المفاتيح(Keylogger)، ومحلل البروتوكول (Protocol Analyzer).

إعادة الضبط: حين يقوم المهاجم بالوصول إلى الجهاز ماديًا ومن ثم يعمل على الدخول لنظام تشغيله لإعادة ضبط كلمة المرور ليمكنه الدخول في أوقات أخرى وعن بعد.

التخمين: وهو حينما يقوم المهاجم بتخمين كلمة المرور، ويكون التخمين سهلًا على المهاجم في حال استخدم صاحب الحساب كلمة مرور قصيرة أو سهلة التخمين. وهناك نوعان للهجوم باستخدام التخمين:

- **الأول: الهجوم القسري** (Brute force attack): حيث يقوم المهاجم بمحاولة تخمين كل مزيج ممكن أن يشتبه بكونه كلمة المرور، ويعتبر هذا النوع بطيئًا حيث أنه يستغرق وقتا للتخمين.
- **الثاني: الهجوم باستخدام القاموس** (Dictionary attack): يقوم المهاجم بأخذ كلمات مرور متوقعه ودارجة من قاموس قد قام بتجميعه مهاجمون سابقون ومن ثم يعمل على تجريبها ككلمة مرور لذلك المستخدم حتى يحصل على كلمة المرور الصحيحة.

كلمات السر الضعيفة:

- الكلمات القصيرة.
- سهلة التخمين.
- المرتبطة بشيء يخص المستخدم مثل: تاريخ ميلاده.
- عندما يستخدم المستخدم نفس كلمة السر لأكثر من حساب.
- عدم تغيير كلمة السر لوقت طويل.

لتكون كلمات المرور القوية:

- يجب عدم استخدام كلمات مرور دارجة ويكثر استخدامها.
- يجب عدم استخدام تواريخ الميلاد أو أسماء العائلة أو أية معلومات شخصية.

- عدم تكرار الحروف أو الرموز أو الأرقام بكلمة المرور أو استخدام تسلسل معين.
- عدم استخدام كلمات مرور قصيرة أو سهلة.

إدارة كلمات المرور:

- تغيير كلمة المرور كل فترة.
- عدم إعادة استخدام كلمة مرور قديمة سبق استخدامها.
- عدم كتابة كلمة المرور في مكان ما للتذكير.
- استخدام كلمة مرور خاصة بكل حساب وعدم استخدام نفس كلمة المرور لكل الحسابات.
- عدم ضبط الجهاز ليدخل للحساب تلقائياً.
- عدم إدخال كلمة المرور في جهاز للاستخدام العام.
- عدم إدخال كلمات المرور حينما يكون الاتصال غير أمن بالشبكة.

ماذا لديك؟

جهاز الشفرة الرقمية (token)**:** وهو جهاز صغير مع نافذة للعرض، متزامن مع خادم المصادقة. ويتم إنشاء شفرته من خوارزمية معينة يحددها خادم المصادقة وتتغير الشفرة كل ٣٠ إلى ٦٠ ثانية.

الشكل 117-٣: جهاز الشفرة الرقمية.

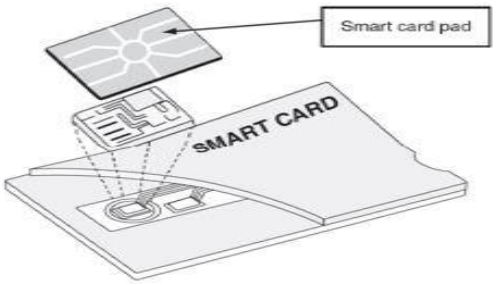
طريقة إدخال كلمة المرور باستخدام جهاز الشفرة الرقمية:

- يدخل اسم المستخدم ومن ثم يدخل الشفرة المعروضة على شاشة الجهاز.
- يبحث خادم المصادقة عن الخوارزمية المرتبطة مع هذا المستخدم، يولد الشفرة الخاصة به.
- يقارن الشفرة الناتجة مع الشفرة التي أدخلها المستخدم.
- في حال كانتا متطابقتان، تمت المصادقة.

ميزات استخدام جهاز الشفرة الرقمية:

- الشفرة التي يتم إنشائها تستخدم مرة واحدة فقط.
- لا يمكن تخمين الشفرة بواسطة المهاجم.
- إذا تمت سرقة الشفرة حين استخدامها فلن يكون ذلك ضاراً حيث أنها لن تكون صالحة للاستخدام مجدداً.

البطاقة الذكية: هي بطاقة ذكية لديها شريحة تحوي خطا ممغنطًا عليها وهو بدوره يحوي معلومات المستخدم التي تقوم بتعريفه.

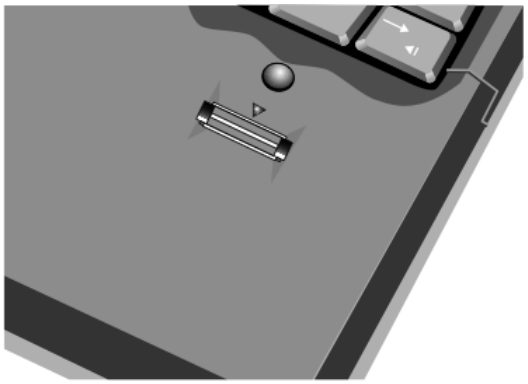


الشكل 118-٣: البطاقة الذكية.

من أنت؟

- **معياري:**

عن طريق استخدام معايير مميزة للشخص (كبصمة اليد، بصمة العين، وتقاسيم الوجه) وأكثر الأنواع شيوعًا هو التعرف على بصمات اليد.



الشكل 119-٣: جهاز البصمة.

مساوئ استخدام المعايير:

- تكلفة الأجهزة المستخدمة لمعرفة المعايير المميزة لكل شخص غالبًا ما تكون باهظة.
- أحيانا تكون القراءات الناتجة عن تلك الأجهزة خاطئة.

- **معايير سلوكية:**

انتقالات ضربات المفاتيح: لكل شخص حركات انتقالية مميزة في استخدام لوحة المفاتيح، مثل الوقت المستغرق بين ضغطة المفتاح والأخرى وهو ما يسمى زمن السكون (Dwell time)، وأيضاً انتقاله بين مفتاح وآخر وهو ما يسمى زمن الانتقال (Flight time).

الشكل 120-٣: انتقالات ضربات المفاتيح.

التعرف على الصوت: لكل شخص صوت مميز وطريقة لغوية مميزة في النطق يمكن من خلالها التعرف على الشخص وإتمام المصادقة.

بصمة آثار الحاسوب: وهو مكان تواجد الحاسوب ومن أين تم تسجيل الدخول، هل من بلد معين أو مدينة معينة:

- تعتمد على أنماط الدخول.
- الموقع الجغرافي.
- وقت الدخول خلال اليوم.
- مزود خدمة الإنترنت.
- التكوين الأساسي للجهاز (نظام التشغيل على سبيل المثال).

المصادقة عن بعد

تستخدم للتثبت من المستخدمين لدخول الشبكات، حيث يقوم المستخدم بإرسال طلب إلى خادم المصادقة عن بعد (RAS) لطلب دخول إلى شبكة معينة واستخدام مصادرها، عن طريق إرفاق شهادة للوصول مع الطلب إلى السيرفر، يقوم السيرفر بالتحقق من الشهادة ومصادقتها عن طريق بروتوكولات معينة ويقوم بالرد إما بـ:

- رفض الوصول.
- قبول الوصول.
- طلب معلومات إضافية من المستخدم.

وتعتبر الشبكات الخاصة الافتراضية الوسيلة الأكثر استخداماً للمصادقة عن بعد:

الشبكة الخاصة الافتراضية (VPN):

قبل استغلال شبكة الإنترنت في إيجاد خطوط اتصال خاصة بالمنشآت، كانت الطريقة المثلى للحصول على خطوط اتصال لنقل البيانات هي استخدام الخطوط المستأجرة (Leased Lines). وهذه الخطوط لا تتوفر بسرعات عالية، وتعتبر تكلفتها عالية جداً مقارنة بتكلفة الاتصال بشبكة الإنترنت.

وعندما انتشر استخدام شبكة الإنترنت، ظهرت إمكانية استخدام هذه الشبكة كنأقل للمعلومات الخاصة بالمنشآت. وظهرت فكرة إنشاء خطوط خاصة على هذه الشبكة العملاقة، أو ما يسمى بالشبكة الخاصة الافتراضية (VPN)Virtual Private Network)). فقد تحتاج بعض المنشآت إلى إيجاد طريقة مناسبة لربط فروعها بعضها ببعض. ومن الخيارات المطروحة استخدام شبكة الإنترنت؛ لما تتميز به من انخفاض التكلفة، وإمكانية ربط الفروع حتى ولو كانت منتشرة في أكثر من قارة. ولكن السؤال الذي يُطرح هنا: هل يمكن الحصول على خطوط اتصال تظهر كأنها خاصة بالمنشأة رغم أنها في حقيقتها مبنية على شبكة الإنترنت، وتتميز بالديمومة والأمان؟ والجواب هو استخدام الشبكة الخاصة الافتراضية. [١]

ماهية الشبكة الخاصة الافتراضية وطريقة عملها:

إن أفضل طريقة لتعريف الشبكة الخاصة الافتراضية هي تحليل كل كلمة بشكل منفصل. وعلى هذا، عرف بيد جولي الشبكة الخاصة الافتراضية (VPN) بأنها: " شبكة خاصة مبنية ضمن إطار بنية الشبكة العامة، مثل شبكة الإنترنت العالمية".

ويعرفها آخرون بأنها: " الشبكة التي تسمح لشبكتين خاصتين أو أكثر بالارتباط بعضها مع بعض من خلال شبكة عامة يمكن الوصول إليها". وتعتبر الميزة الأساسية للشبكة الخاصة الافتراضية هي

استخدامها للشبكات العامة، مثل الإنترنت أكثر من استخدامها للخطوط الخاصة المؤجرة أو العالية الكلفة.

تقوم فكرة الشبكات الخاصة الافتراضية على إنشاء خطوط اتصال على شبكة الإنترنت (أو شبكة عامة كشبكة (Multi-Protocol Label Switching (MPLS) تظهر كأنها خاصة بالمنشأة وتعمل كشبكة نقل بيانات منفصلة تماماً. ويمكن أن تخدم فروع المنشأة في مناطق جغرافية متباعدة، سواءَ كانت داخل البلاد أم على مستوى العالم، بحيث تكون خاصة بالمنشأة، ولا يستطيع أحد أو طرف آخر استخدامها رغم أنها في حقيقة الأمر مبنية على شبكة الإنترنت.

ويقوم عمل الشبكة الخاصة الافتراضية على بناء "نفق" (VPN Tunnel) خاص بين فروع المنشأة، يتم تبادل المعلومات من خلال هذا النفق. والنفق هو آلية لتغليف البيانات الخاصة بالمنشأة، وجعلها تسير في مسار محدد (نفق) ضمن شبكة الإنترنت، بحيث تكون هذه البيانات غير مرئية من قبل الغير.

وتتكون الشبكة الخاصة الافتراضية من ثلاثة مكونات رئيسية هي:

- جهاز البوابة (Gateway) الذي يربط طرفي النفق بالفروع.
- النفق الذي تنقل من خلاله البيانات، ويشمل البرمجيات والبروتوكولات اللازمة.
- جدار النار لحجب البيانات غير المرغوب فيها عن المرور خلال النفق.

مميزات الشبكات الخاصة الافتراضية وعيوبها:

تتلخص مميزات الشبكات الخاصة الافتراضية فيما يلي:

- إمكانية التوسع المستقبلي بسهولة (Scalability)
- سهولة إضافة المستخدمين وحذفهم.
- قليلة الكلفة مقارنة بالخطوط المستأجرة.
- إمكانية التعديل والنقل للشبكة، وسهولة إضافة الفروع وحذفها (Mobility).
- تحقيق حد مقبول من أمن المعلومات، من خلال توفير الخصوصية للخطوط، مقارنة بالإنترنت.

وتتخلص عيوبها فيما يلي:

- تحتاج إلى تطبيق معايير أمنية أكثر صرامة.
- مازال هناك بعض المعايير لم تصل إلى الدرجة القياسية عالمياً.
- يتأثر أداؤها بمدى بالضغط الحاصل على شبكة الإنترنت، والذي لا يمكن التنبؤ به.

أمن الشبكات الخاصة الافتراضية:

لقد حلت الشبكات الافتراضية الخاصة مشكلة إيجاد خطوط اتصال لنقل البيانات، تكون زهيدة الثمن، وتغطي أي مكان في العالم تقريباً. وكذلك فإنها تضمن جزءاً من الخصوصية لهذه الخطوط، فلا يمكن استخدامها من قبل الآخرين. ولكن، طالما أن الحامل الحقيقي لهذه البيانات هي شبكة الإنترنت، فإنها تعتبر طريقة غير آمنة لنقل البيانات، ويجب توفير الحماية اللازمة.

وتوفير الحماية اللازمة يعني ضمان تغطية جميع جوانب أمن المعلومات، من خلال تحقيق عناصر أمن المعلومات، كالتالي:

- **التحقق من الهوية:** ضمان أن المرسلين والمستقبلين هم من يصرحون عن أنفسهم بالفعل، فيمكن أداء التحقق من الهوية من خلال تأكيد أن الطرف الآخر لدية المعرفة، أو لديه بعض المعلومات المشتركة، أو المفتاح السري الفريد.
- **السرية (أو الخصوصية):** أن يستطيع الأطراف المخولون بأن يدخلوا إلى حركة الشبكة الخاصة الافتراضية، ويتبادلوا المعلومات بشكل سري لا يمكن أن يطلع عليها غيرهم. ويمكن تحقيق الخصوصية من خلال تطبيق التشفير.
- **سلامة البيانات تكاملها:** ألا تستطيع حركة الشبكة الخاصة الافتراضية التغيير في البيانات دون كشفها، فيمكن تحقيق سلامة البيانات تكاملها من خلال تطبيق البصمة الرقمية.
- **عدم الإنكار:** ألا يمكن للمستقبلين والمرسلين فيما بعد أن ينكروا علاقتهم بما تم عمله. ويمكن تحقيق ذلك من خلال استخدام التصديق (التوقيع) الرقمي، فعند وضع إجراءات عدم الإنكار لا يمكن للمستقبل أن ينكر استلام المعاملة، ولا يستطيع المرسل أن ينكر إرسالها.

أسئلة ونقاش(١٣):

س١: ما المصادقة؟

س٢: كيف يمكننا تحقيق المصادقة؟

س٣: ما أبرز طرق المصادقة عن بعد؟

تقييم الثغرات

إدارة المخاطر، وتقييم، والتخفيف من آثارها

أحد أهم ممتلكات أي منشاة هي البيانات الخاصة بها، فبدون هذه البيانات لا يمكن للمنشآت أن تعمل. ولكن أهمية هذه البيانات قلل من شأنها بشكل عام، فينبغي النظر لها كأحد الممتلكات الأخرى مثل المباني، الأوراق المالية، الموظفين وغيرها. ولنقوم بحماية تلك البيانات فأول خطوة تبدأ بفهم المخاطر وإدارتها. [٣]

ما المخاطر؟

في أمن المعلومات، المخاطر هي احتمال أن عميل التهديد يستغل الثغرة. بشكل عام المخاطر يمكن أن تعرف كحدث أو حالة يمكن أن تحدث، وفي حالة حدوثها فإن تأثيرها دائمًا ما يكون سلبي.

تعريف إدارة المخاطر:

هو منهج منظم وهيكلي لإدارة احتمال الخسائر المتعلقة بما هو يشكل تهديداً. هذه التهديدات قد تكون من قبل المهاجمين، البيئة، خلل في التقنية أو عوامل أخرى. فإن هدف إدارة المخاطر هو التقليل من المخاطر التي قد تصيب الممتلكات.

خطوات في إدارة المخاطر:

١-تعريف الممتلكات: هي عمليات لحصر وإدارة هذه العناصر فإن لكل منشأة عدد مختلف من الممتلكات مثل:

- **البيانات** (Data): تنطوي على كل المعلومات المستخدمة والمنقولة من قبل المنشأة مثل قاعدة البيانات للموظفين وسجل المخزون وما إلى ذلك.
- **الأجهزة**(Hardware): مثل الحواسيب المكتبية، الخوادم، نقاط الوصول اللاسلكية، معدات الشبكة.
- **الموظفين**(Personnel): مثل الموظفين، العملاء، شركاء العمل، المقاولين، الباعة.
- **الممتلكات المادية** (Physical Assets): مثل المباني، السيارات، وغيرها من المعدات غير الحاسوبية.
- **البرمجيات**(Software): مثل برامج التطبيقات، نظم التشغيل، البرامج الأمنية.

كما أن العديد من المنشآت تقوم بإسناد قيمة رقمية لكل ممتلك (مثل رقم ٥ كونها قيمة للغاية، و١ كونها أقل قيمة). أما بالنسبة للعوامل التي ينبغي النظر لها أثناء تحديد القيمة النسبية فهي:

مدى أهمية الممتلكات في تحقيق أهداف المنشأة؟

- مدى صعوبة استبداله؟
- كم هي تكلفة حمايته؟
- كيفية استبداله بسرعة؟
- كم هي التكلفة لاستبداله؟
- ما هو الأثر السلبي على المنظمة إذا كانت هذه الممتلكات غير متاحة؟

٢-**تعريف التهديد** (Threat Identification): عميل التهديد هو أي شخص أو شيء له السلطة لتنفيذ تهديد ضد أحد الممتلكات. عميل التهديد لا يقتصر على المهاجمين فقط، بل أيضاً الكوارث الطبيعية مثل الحريق، أو الظروف المناخية القاسية.

نماذج التهديد (Threat Modeling): بناء سيناريو لأنواع التهديدات التي يمكن أن تواجهه الممتلكات. وهدفها يكون من أجل فهمٍ أفضل. على سبيل المثال من هم المهاجمين؟ لماذا يهاجمون؟ ونوع الهجمات التي يمكن أن تحصل. وهناك أداة تستعمل للمساعدة في بناء نماذج التهديد وهي بناء شجرة الهجوم (Attack Tree). فهي تصور للهجمات الممكنة أن تحدث ضد الممتلكات.

٣-**تقييم الثغرات** (Vulnerability Appraisal): ماهي نقاط الضعف الأمنية التي قد تعرض الممتلكات لهذه المخاطر. تحديد الثغرات وتقييمها يعتمد غالباً على خلفية وخبرة المُقيم.

٤-**تقييم المخاطر** (Risk Assessment):

تحديد الأضرار التي ستنجم عن الهجوم في حال استغلال الثغرات وخطورتها على المنشأة. تصنف كل ثغرة ممكنه بإحدى التصنيفات التالية:

- لا تأثير: فالخطر التي قد تتسبب به هذه الثغرة لا يمكن أن يؤثر على المنشأة.
- تأثير بسيط: هذه الثغرة قد ينتج عنها فترات محدودة من الإزعاج لا أكثر.
- مهم: هذه الثغرة يمكن أن ينتج عنها فقدان إنتاجية الموظفين أو تتسبب بزيادة النفقات.
- رئيسي: للثغرة تأثير سلبي على العائدات.
- كارثي: تصنف بعض الثغرات كأمر كارثي وهي كالتي تتسبب بإحداث وقف العمل للمنشأة.

٥-تخفيف المخاطر (Risk Mitigation):

يعد تخفيف المخاطر وتصنيفها آخر خطوة. وهي تحديد ما يجب فعله تجاه هذه المخاطر ومن المهم أن ندرك أن الضعف الأمني لا يمكن القضاء عليه بشكل كامل.

المنشآت لديها خيارات متشابهة عند مواجهة الخطر وما يجب فعله:

- تقليص الخطر (Diminish the Risk).
- نقل الخطر (Transfer the Risk).
- تقبل الخطر (Accept the Risk).

حالة دراسية (٥):

يتم توزيع المتدربين إلى مجموعات، ومن ثم تقوم كل مجموعة بالعمل على الحالة الدراسية التالية:

قررت شركة (م. ن. م) للتقنية ومقرها في الولاية الأمريكية واشنطن، بافتتاح فرع جديد للشركة في ولاية ألاباما لحاجة العمل الملحة. لكن هذه الولاية قد عُرفت بكثرة الأعاصير المدمرة. فكلف مدير الشركة قسم إدارة المخاطر بوضع خطة متكاملة لإدارة المخاطر في حال افتتح الفرع.

من خلال ما تعلمته في جزئية **إدارة المخاطر**، قم أنت ومجموعة من زملائك بتشكيل الخطة الإدارية لهذه الشركة من خلال الخطوات المتخذة لإدارة المخاطر.

تحديد الثغرات

تحديد الثغرات من خلال تقييمها يحدد نقاط الضعف الأمنية الحالية التي يمكن أن تعرض الأصول للتهديد.

البحث عن الثغرات (vulnerability scanning):

يستخدم من قبل المنشأة لتحديد ثغرات النظام التي ينبغي معالجتها من أجل زيادة المستوى الأمني. وهناك بعض الأدوات المستخدمة للبحث عن الثغرات:

ماسح المنافذ (port scanner): عادة ما تستخدم المنشأة برنامج يعرف بماسح المنافذ (port scanner) ليبحث في النظام عن ثغرات المنافذ الذي يمكن استغلالها في الهجوم. وهناك ثلاث حالات للمنفذ:

- مفتوح: المنفذ المفتوح يعني أن هناك تطبيق أو عملية مسندة لهذا المنفذ وتصغي إليه.
- مغلق: المنفذ المغلق يعني أنه لا توجد عملية تصغي لهذا المنفذ.
- محظور: المنفذ المحظور يعني أن النظام المستضيف لا يقوم بالرد على أي استعلامات لهذا المنفذ.

مخططون الشبكة (network mappers): هي أدوات برمجية يمكن أن تحدد جميع الأنظمة المرتبطة بالشبكة. وتستخدم عادة من قبل مسؤولي الشبكة لمعرفة ماهي الأجهزة المتصلة بالشبكة وتحديد الأجهزة غير المصرح بها التي أرفقت من قبل الموظفين أو المهاجمين. أيضاً تستخدم من قبل المهاجمين لتحديد الأنظمة التي تكون مرتبطة بالشبكة حتى يقوم بمهاجمة هذه الأنظمة.

محلل البروتوكول (protocol analyzers): حركة المرور في الشبكة يمكن عرضها من قبل جهاز محلل بروتوكول مستقل أو جهاز الحاسوب يقوم بتشغيل برنامج محلل البروتوكول. محلل البروتوكول في الأغلب يستخدم من قبل مسؤولي الشبكة لمراقبة الشبكة. الاستخدامات الشائعة تشمل:

- استكشاف أخطاء وإصلاح الشبكة (network troubleshooting): محلل البروتوكول يمكن اكتشاف وتشخيص مشكلات الشبكة.
- توصيف حركة مرور الشبكة (network traffic characterization): محلل البروتوكول يمكن استخدامه لرسم صورة لنوع الشبكة وكيفية حركة المرور فيها.

- تحليل الأمن (Security analysis): هجمات تعطيل الخدمة وأنواع أخرى من الهجمات يمكن الكشف عنها عن طريق فحص حركة مرور الشبكة.

ماسحات الثغرات (vulnerability scanners): هو مصطلح عام يشير إلى مجموعة من المنتجات التي تبحث عن الثغرات في الشبكات أو الأنظمة. فالمنشأة تهدف لتحديد الثغرات وتنبيه مسؤولي الشبكة لهذه المشكلات. ماسحات الثغرات قادرة أيضاً على:

- التنبيه عند إضافة نظام جديد للشبكة.
- الكشف عندما يكون هناك تطبيق تم تخريبه أو اختراقه.
- تعقب أي الأنظمة التي تتواصل مع الأنظمة الداخلية الأخرى.
- الحفاظ على سجل جميع جلسات الشبكة التفاعلية.

كسر كلمات السر (password crackers): لأن كلمات السر أكثر من يخل في الأمن ويتسبب في أمن ضعيف فهي التركيز المتكرر للهجمات. فالمنشأة قادرة على اختبار قوة الكلمات السرية عن طريق استخدام برامج كسر كلمات السر، فالمهاجمين بالمثل يستخدمون هذا البرنامج لكسر كلمات المستخدم السرية. ففي حال كانت المنشأة قادرة على كسرها فالمهاجم سيكون كذلك بالمقابل.

اختبار الاختراق (penetration testing): هي طريقة لتقييم أمن نظام الحاسوب أو الشبكة من خلال محاكاة هجومًا ضارًا بدلًا من الاكتفاء بالبحث عن الثغرات. فالاختبار يتضمن تحليلًا أكثر نشاطًا لثغرات النظام. ويُأخذ الاختبار من موقع مهاجم محتمل ويمكن في الواقع الاستفادة من الثغرات الأمنية التي تم اكتشافها.

تطبيقات:

أولا: استخدام أدوات الكشف عن نقاط ضعف تطبيقات الويب:

هنالك العديد من الأدوات المجانية والتجارية التي تستخدم لهذا الغرض. في هذا التطبيق سنقوم باستخدام أداة "IronWASP" وهي اختصار لاسم " Iron Web application Advanced Security testing Platform" وهي أداة مجانية مفتوحة المصدر تُستخدم لفحص الأمان في تطبيقات الويب بشكل متقدم. تتيح لك هذه الأداة إمكانية إجراء عدة أنواع من الاختبارات على تطبيق ويب معين عن طريق إضافة رابط موقع الويب الذي تريد فحصه. ومن ثم إجراء فحص لهذا الموقع وتوليد تقرير مفصل عن نقاط الضعف والتي من الممكن أن تكون مصدر خطر يستغلها المهاجمون لإلحاق أضرار بهذا الموقع من تعطيل أو وصول غير مشروع لبعض البيانات فيه.

تمرين عملي(٢٠):

١-قم بتحميل أداة "IronWASP" عن طريق البحث عنها من خلال جوجل أو عن طريق الرابط التالي:

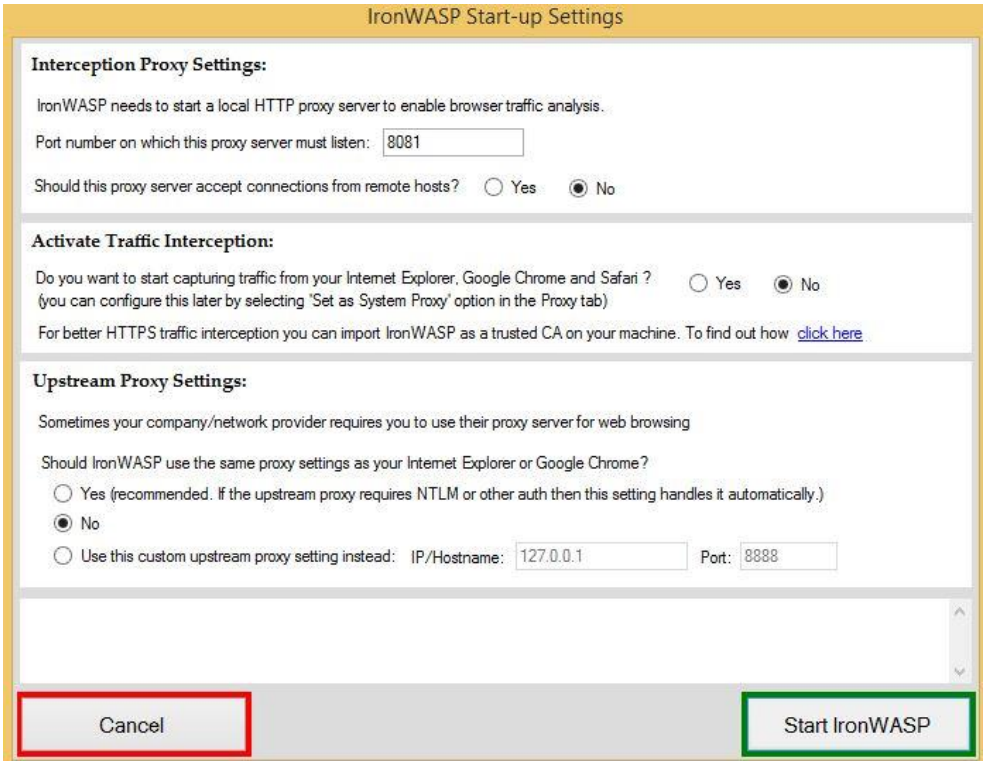
https://ironwasp.org/ironwasp.zip لنظام ويندوز

https://ironwasp.org/download.html لأنظمة تشغيل مختلفة

٢-بعد التحميل، قم بفك الضغط عن الملف ومن ثم قم بفتح الملف التنفيذي للأداة باسم "IronWASP.exe"

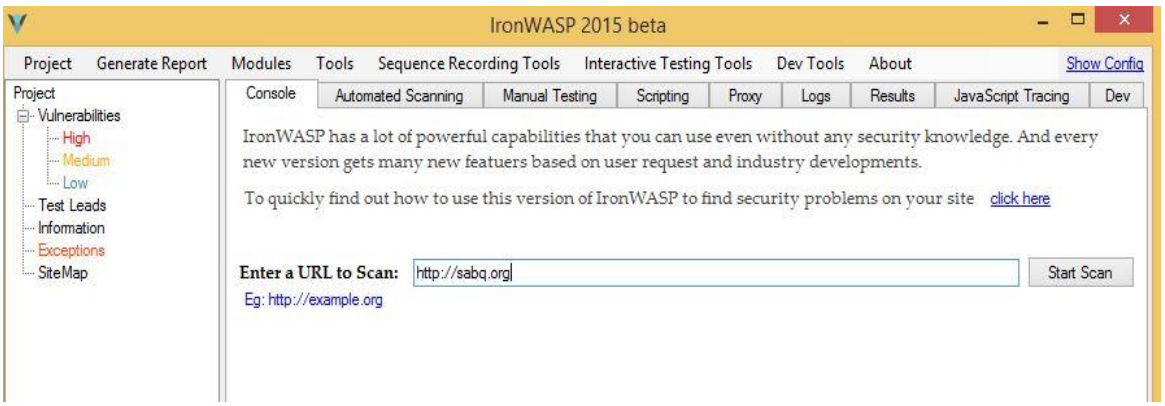
الشكل 121-٣: الملف التنفيذي للبرنامج IronWASP

٣-عندها ستظهر لك شاشة ضبط البرنامج الرئيسة كما في الشكل(١٢٢-٣):



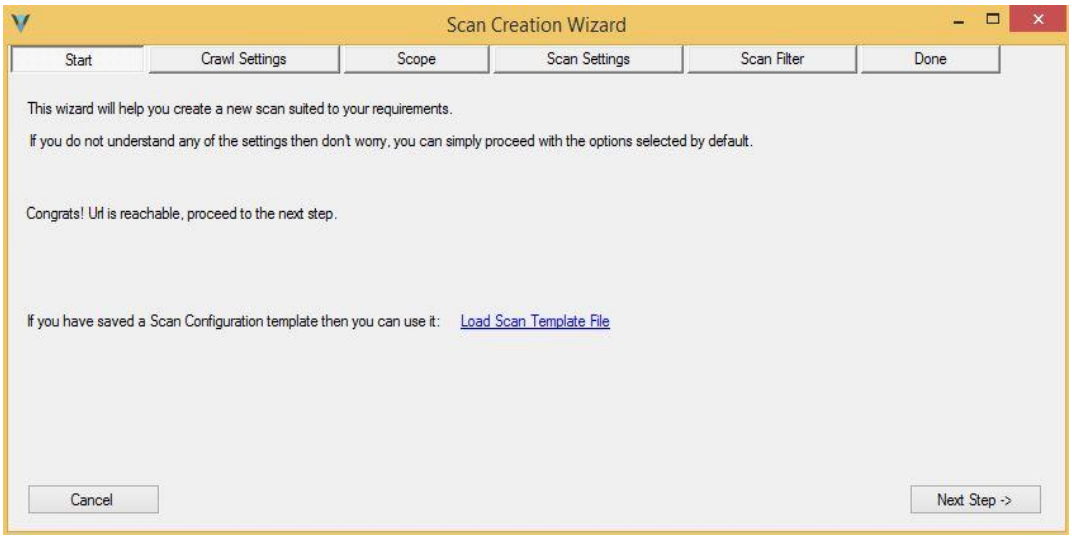
الشكل 122-٣: خيارات الضبط في برنامج IronWASP

٤-اضغط على "Start IronWASP" عندها ستظهر لك الشاشة الرئيسية للبرنامج:



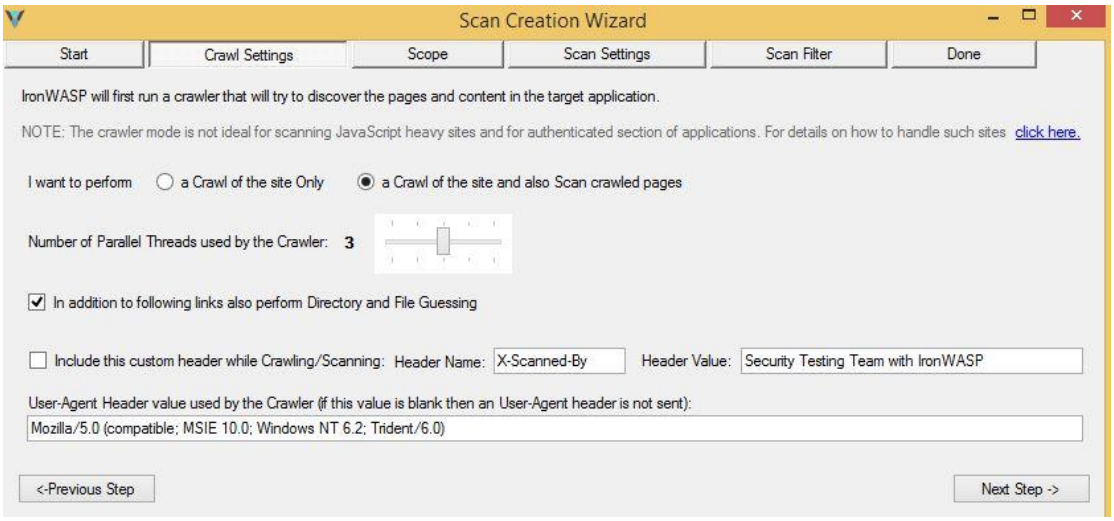
الشكل123 -٣: الشاشة الرئيسية لبرنامج IronWASP.

٥-في المكان المخصص لرابط الموقع "Enter a URL to Scan"، قم بإدخال رابط المؤسسة التي تعمل لديها أو أي موقع تريد تفحص نقاط ضعفه ومن ثم اضغط "Start Scan"



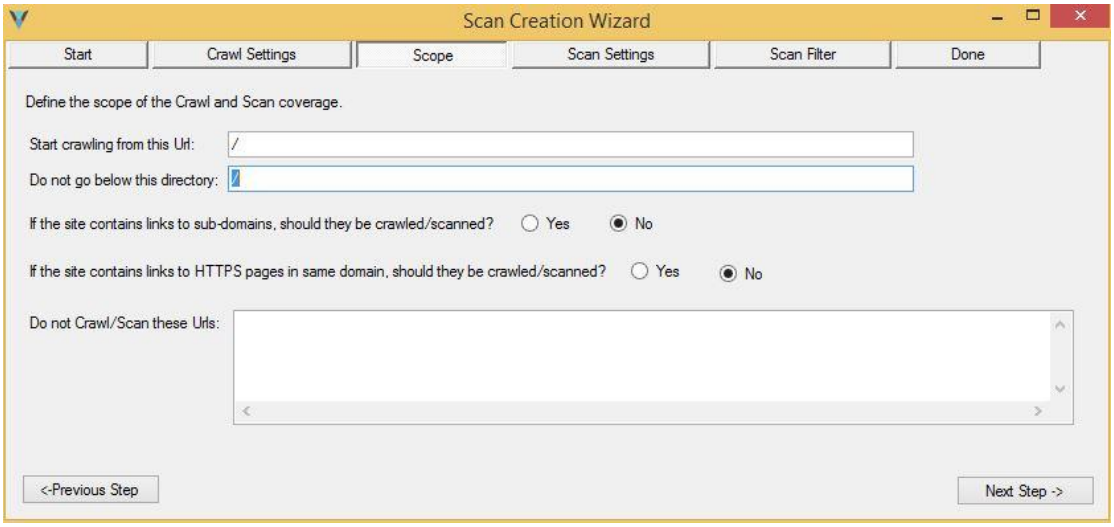
الشكل 124-٣: شاشة الفحص لموقع في IronWASP

٦-عندها ستظهر لك الشاشة التأكيدية بأن الأداة استطاعت الوصول إلى الرابط المُعطى، عندها اضغط على "Next Step".



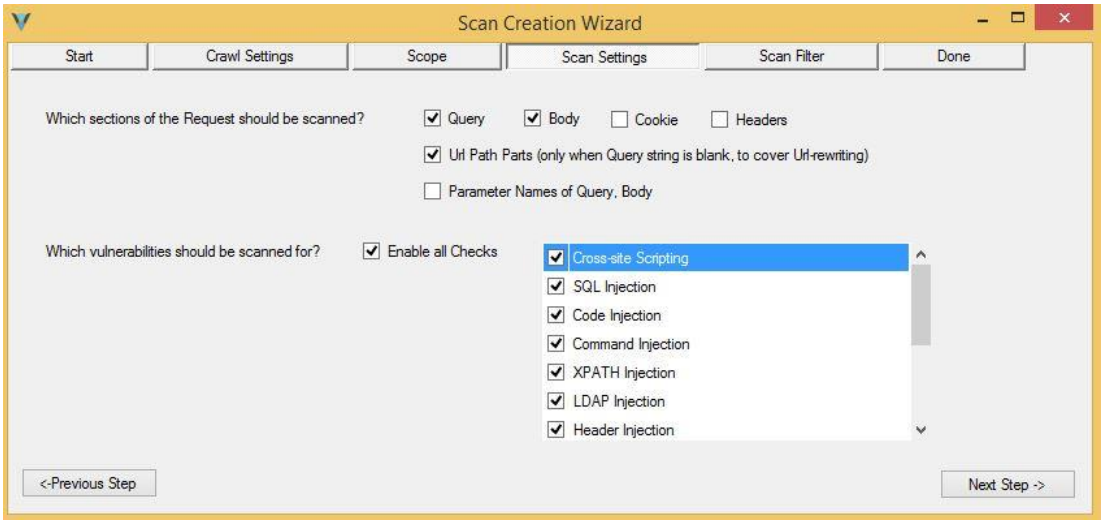
الشكل 125-٣: الشاشة التأكيدية للوصول لرابط الموقع لفحصه في برنامجIronWASP

٧-ستظهر لك الشاشة الرئيسية لإعدادات تفحص الموقع "Crawl Setting"، قم بالضغط على "Next Step".



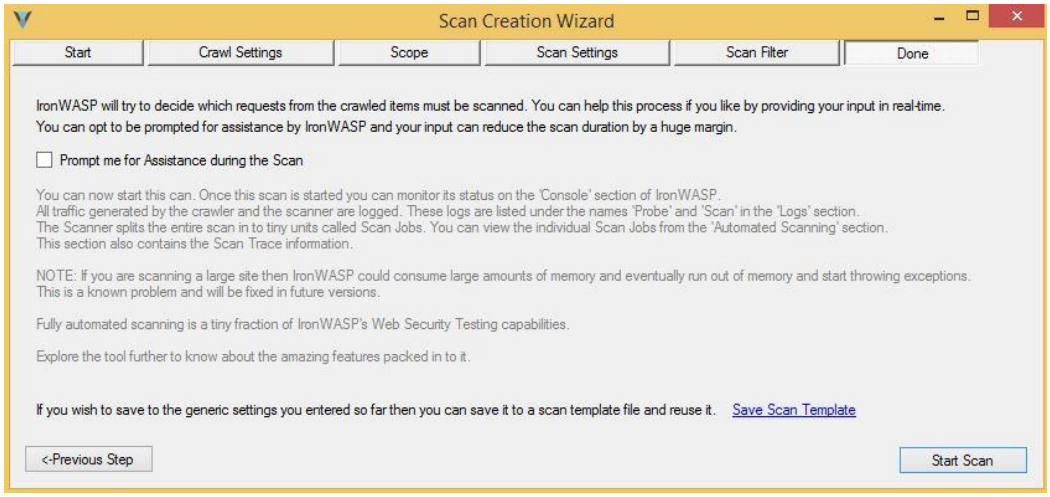
الشكل 126-٣: الشاشة الرئيسية لإعدادات تفحص الموقع عن طريق برنامج IronWASP

٨-عندها سيظهر لك المدى الذي تريد تفحصه للرابط، قم باختيار "Next Step".



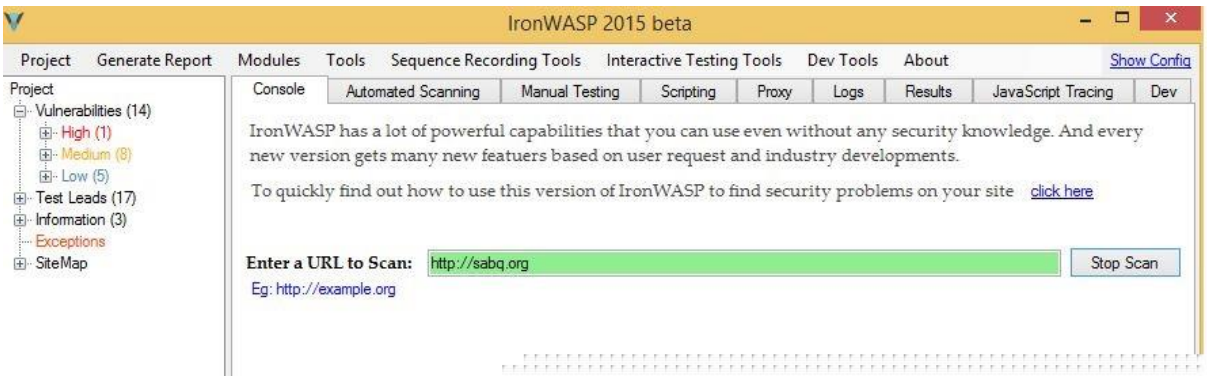
الشكل 127-٣: خيارات الفحص للموقع في برنامج IronWASP

٩-بعد ذلك قم باختيار إعدادات التفحص، حيث يمكنك في هذه الخطوة تحديد نقاط ضعف محددة للموقع المراد فحصه، قم باختيار "Enable all Checks" لتحديد جميع نقاط الضعف ومن ثم اضغط على "Next Step".



الشكل 128-٣: اكتمال خيارات فحص الموقع من خلال برنامج IronWASP

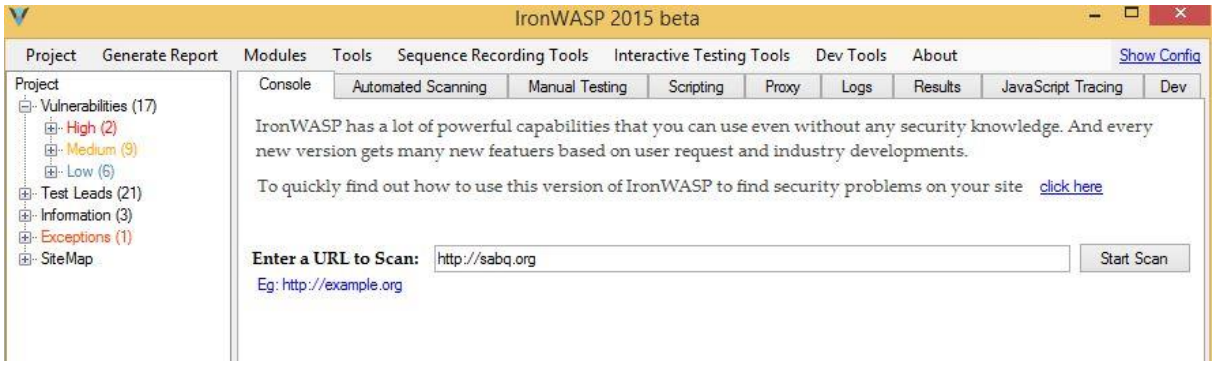
١٠-في آخر خطوة من إعدادات الفحص، قم باختيار "Start Scan"، ليتم البدء في اختبار الموقع.



الشكل 129-٣: خيارات البدء في تفحص الموقع من خلال برنامج IronWASP

عندها ستبدأ الأداة بتفحص الموقع وقد يستغرق هذا الفحص عدة دقائق بناءً على حجم الموقع المراد فحصه.

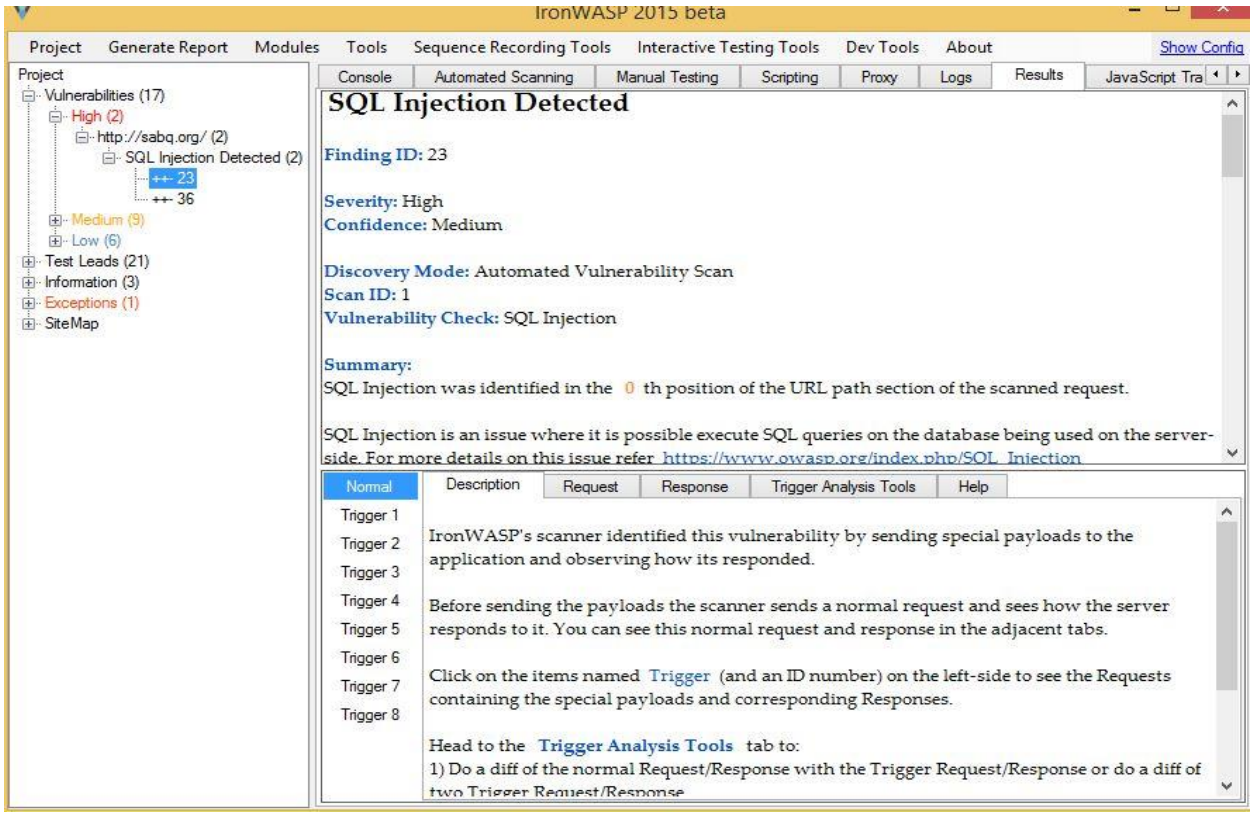
١١-يمكنك الانتظار حتى تنتهي الأداة من فحص كامل الموقع، كما بالإمكان الضغط على "Scan Stop"، ليتم استعراض نقاط الضعف التي اكتشفتها الأداة حتى الآن.



الشكل 130-٣: نتيجة الفحص في برنامج IronWASP

من القائمة في يسار الشاشة، يمكن ملاحظة عدد نقاط الضعف التي تمكنت الأداة من إيجادها وهي ١٧. كما نلاحظ وجود ٣ تقييمات رئيسية للثغرات أو نقاط الضعف وهي عالي، متوسط، منخفض. نجد من هذا الفحص أن الأداة تمكنت من إيجاد ثغرتين عالية الخطورة، و٩ ثغرات متوسطة الخطورة، و٦ ثغرات منخفضة الخطورة.

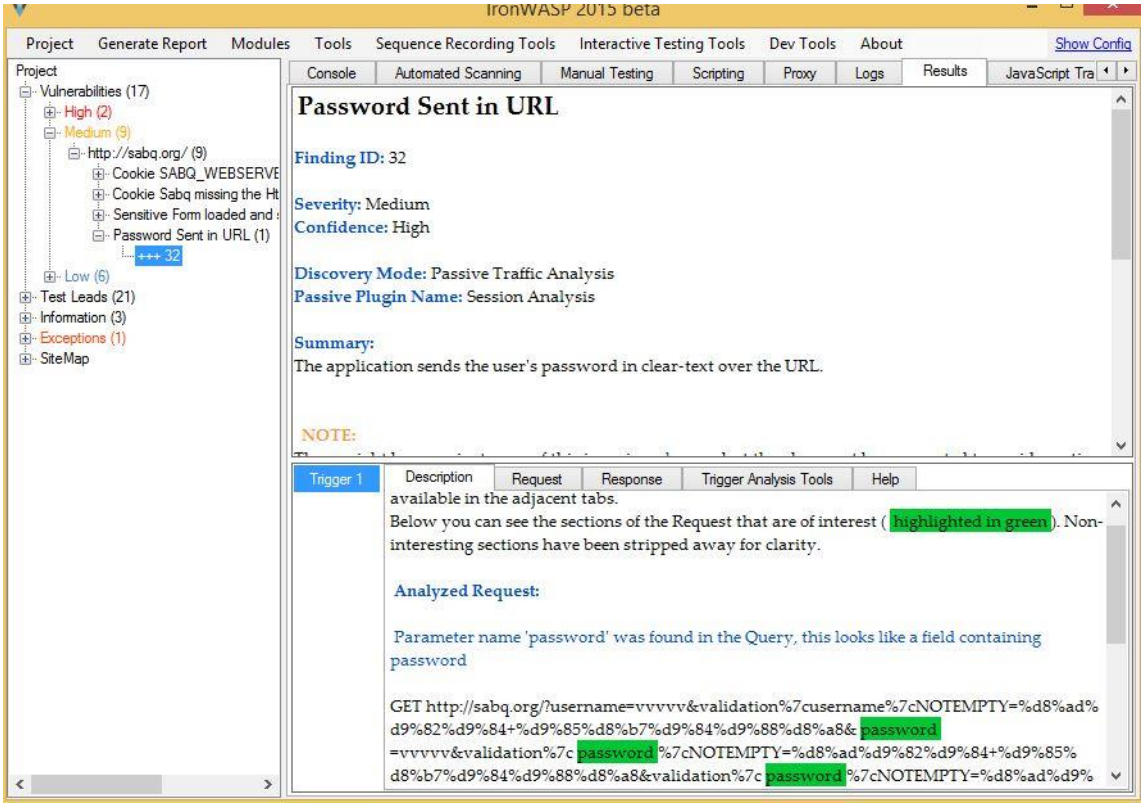
١٢-قم بالضغط على أحد أنواع نقاط الضعف، حيث بالإمكان استعراض تفصيلها كما في الشكل التالي:



الشكل 131-٣ تفاصيل نتيجة الفحص في برنامج IronWASP

نلاحظ عند الضغط على نقطة الضعف، تتيح لك الأداة استعراض وصف لنوع نقطة الضعف والإجراء المتبع لذلك. في الشكل السابق تصنف الثغرة على أنها من نوع "SQL Injection" كما تتيح لك استعراض الطرق التي من خلالها تم اكتشاف هذه الثغرة من خلال استعراض "Trigger".

١٣-قم باستعراض نقاط الضعف المتوسطة الخطورة في الموقع من خلال الضغط على "Medium"، عندها ستظهر لك أنواع نقاط الضعف متوسطة الخطورة، قم باختيار إحداها لعرض محتواها كما في الشكل (٣-١٣٢):



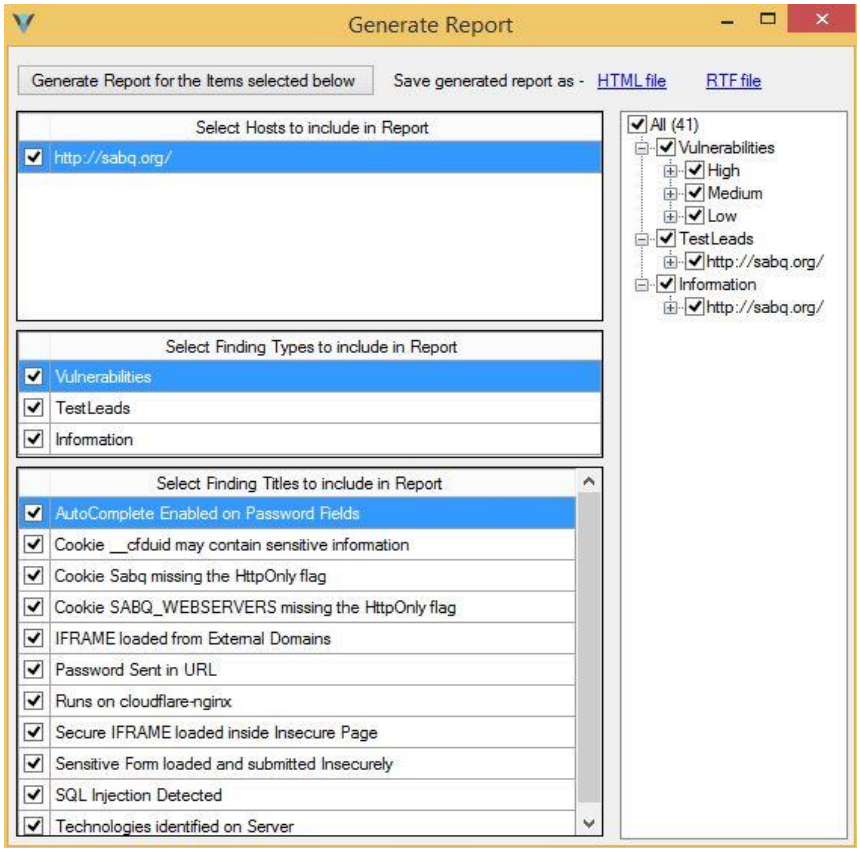
الشكل 132-٣: نقاط الضعف المتوسطة الخطورة في الموقع بعد الفحص خلال برنامج IronWASP

كما نلاحظ وصف هذه الثغرة وهي وجود كلمة "Password" في بعض روابط الموقع والتي من الممكن أن تكون هدف للمهاجمين.

١٤-من القائمة في الشاشة الرئيسية قم باستعراض بعض الأدوات وأنماط البحث التي توفرها هذه الأداة، على سبيل المثال توفر هذه الأداة عدة أنماط من الفحص لنقاط الضعف كما في الشكل (١٣٣-٣):

الشكل 133-٣: الأدوات وأنماط البحث التي توفرها IronWASP

١٥-كما تمكنك هذه الأداة من استعراض وحفظ تقرير للموقع الذي تم فحصه. اضغط على زر " Generate Report" والموجود في أعلى الشاشة الرئيسية.

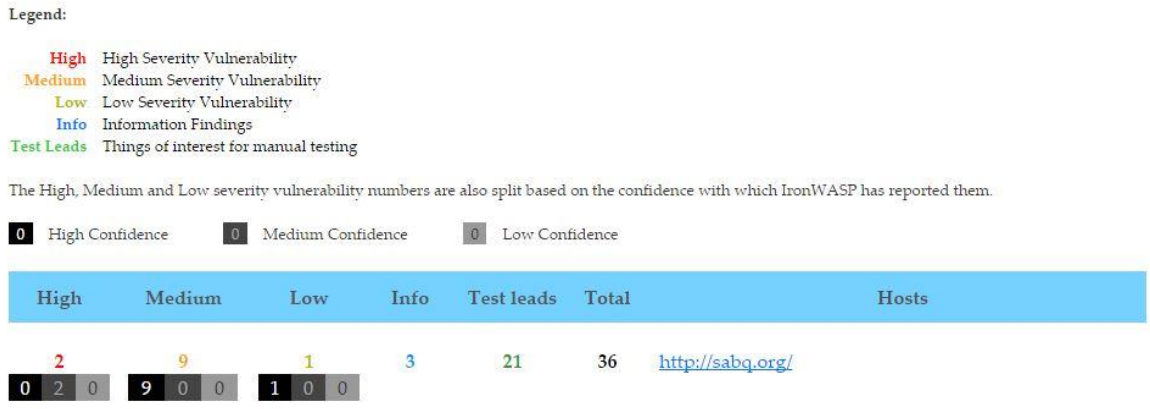


الشكل 134-٣: استعراض وحفظ تقرير للموقع الذي تم فحصه عن طريق برنامج IronWASP

تمكنك هذه الأداة من اختيار العناصر التي تريد عرضها في التقرير.

١٦-اضغط على "Generate Report for the Items Selected below"، ومن ثم اختر طريقة حفظ التقرير "HTML file".

١٧-قم باستعراض ملف التقرير الذي تم حفظه.



الشكل 135-٣: استعراض ملف التقرير التي تم حفظه عن طريق IronWASP

الشاشة السابقة شكل(١٣٥-٣) تظهر لك جزئية من التقرير الذي تم إنتاجه حيث يتم تقسيم النتائج بشكل مُنظم.

ثانياً: استخدام أدوات الكشف عن المنافذ وثغرات الشبكة:

هنالك العديد من الأدوات المجانية والتجارية التي تستخدم لهذا الغرض. في هذا التطبيق سنقوم باستخدام أداة NMAP وهي اختصار Network Mapper حيث يُستخدم لفحص الشبكات والأجهزة الفردية وذلك لتقييمها. البرنامج هو أداة قوية جدا ويستخدمه جميع المخترقون باختلاف أنواعهم. كما يستخدمه أيضاً خبراء الحماية ومحللي الشبكات والذين يهدفون إلى اكتشاف الثغرات والأخطاء لتفادي أي عملية اختراق للشبكة والأجهزة.

يُستخدم هذا البرنامج الكشف عن الأجهزة العاملة ونوع نظام التشغيل المستخدم وإصداره والبرامج العاملة والمنافذ التي تستخدمها والخدمات التي تعمل بالجهاز. كما أن له القدرة على كشف نوع الجدار الناري المستخدم والعناوين الفيزيائية "Mac Addresses" للأجهزة المرتبطة بالشبكة. يُعتبرهذا البرنامج من أهم البرامج لمدير الشبكة حيث يمكن من خلاله الكشف عن المنافذ المفتوحة والمغلقة في الخوادم مما يسمح بمتابعتها وما يجري فيها ومعرفة الأخطار والثغرات التي من الممكن أن تصيب الشبكة.

يعتبر هذا البرنامج ضخم وقد تم تأليف كتب كاملة عنه وذلك لاحتوائه على الكثير من الخيارات والمميزات المتقدمة ولدية القدرة على دعم عدة أنظمة تشغيل. كما أنه في نفس الوقت يعتبر سهل الاستخدام لاحتوائه على خيارات بسيطة عملية بالإضافة لوجود واجهة رسومية لدية تدعى "Zenmap". سنقوم في هذا التطبيق بإجراء تقييم بسيط لمعرفة بعض المنافذ المفتوحة للخوادم الشبكة.

تمرين عملي(٢١):

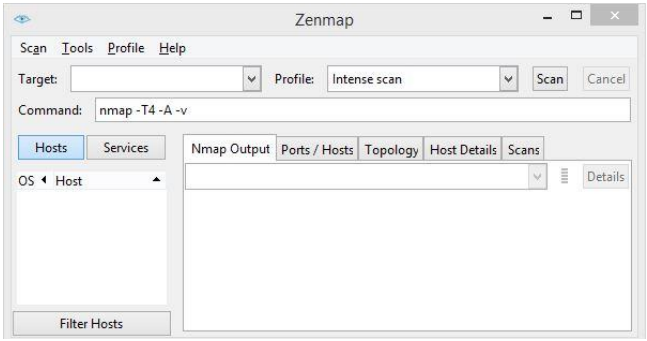
١-قم بتحميل "Nmap" وتثبيته من خلال البحث عنها في محرك جوجل أو من خلال الرابط التالي:

https://nmap.org/download.html#windows

ولتحميل البرنامج لأنظمة تشغيل مختلفة يمكنك استخدام هذا الرابط:

https://nmap.org/download.html

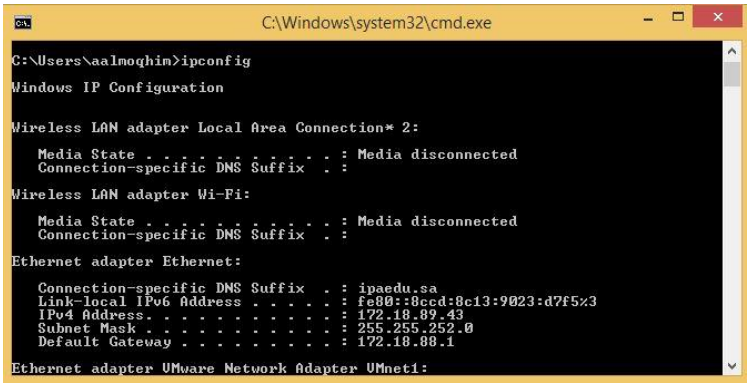
٢-بعد تثبيت البرنامج، قم بفتح واجهة البرنامج الرئيسية الرسومية "Zenmap" كما في الشكل (١٣٦-٣):



الشكل 136-٣: الواجهة الرئيسية لبرنامج Zenmap

تتيح لك هذه الشاشة اختيار عنوان الجهاز الذي تريد عمل مسح عليه لمعرفة الأجهزة المرتبطة به أو اختبار حالة المنافذ فيه من خلال خانة "Target" في أعلى يسار الشاشة. كما أن هذه البرنامج يتيح لك العديد من أنواع المسح للهدف المراد اختباره من خلال "Profile" فعند الضغط على هذا الخيار يمكنك هذا البرنامج من العديد من أنواع المسح مثل " Intense Scan,Slow Comprehensive scan".

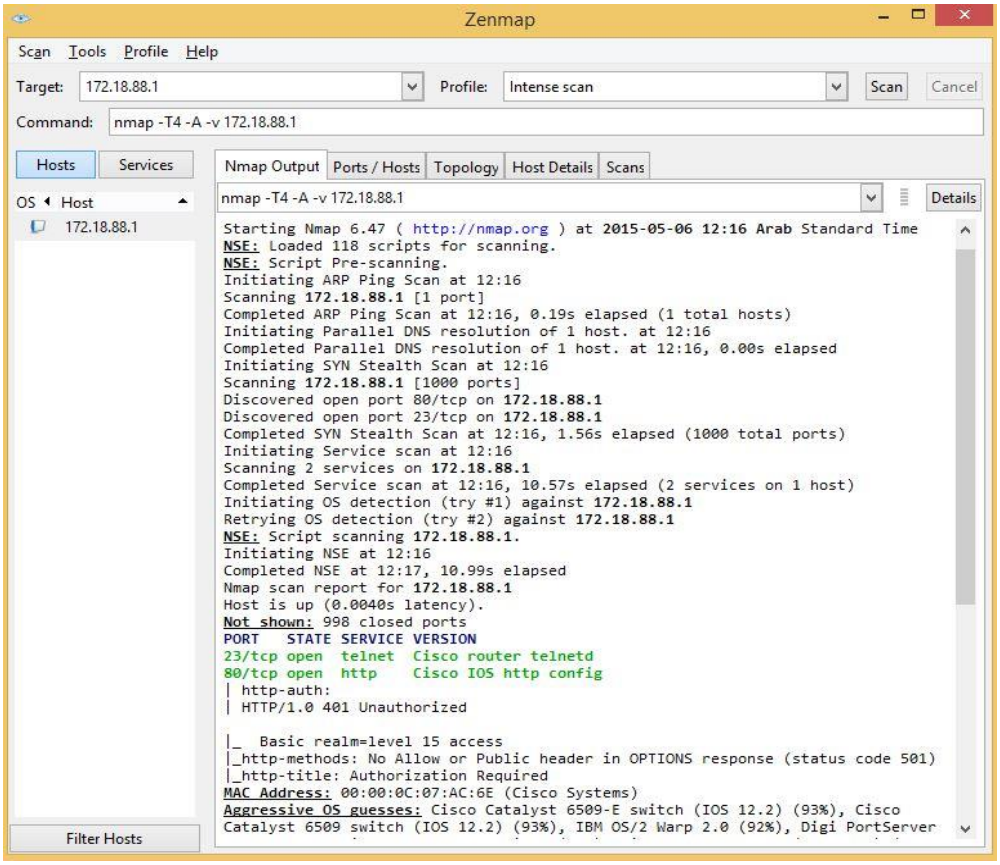
٣-قم بالحصول على عنوان البوابة الافتراضية في الشبكة التي تعمل عليها "Default Gateway" من خلال موجه الأوامر Cmd عن طريق ابدأ "Start" وفي مربع البحث اكتب "Cmd"، بعدها قم بكتابة الأمر "ipconfig" في موجه الأوامر كما في الشكل (١٣٧-٣):



الشكل 137-٣: شاشة الأوامر في نظام التشغيل ويندوز

نلاحظ هنا عنوان البوابة الافتراضية هو ١٧٢,١٨,٨٨,١

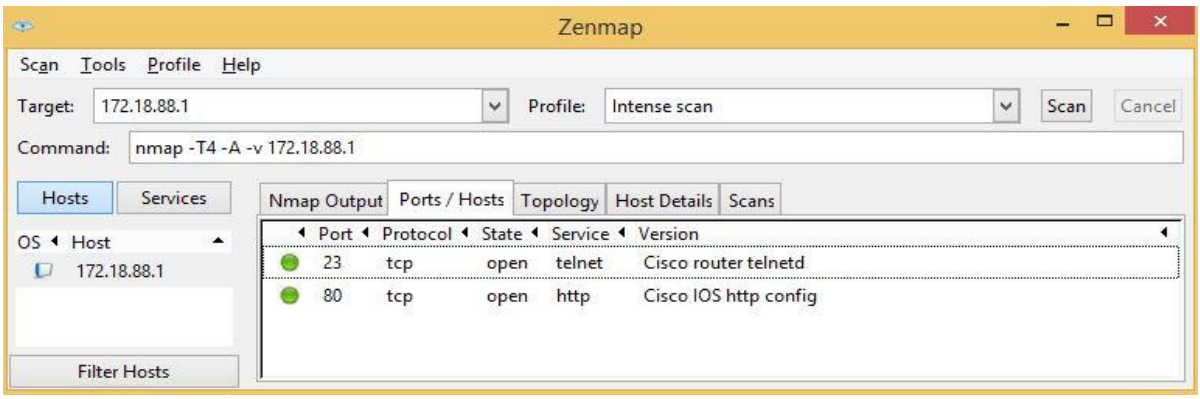
٤-ارجع إلى الشاشة الرئيسية الخاصة ببرنامج Nmap وقم بكتابة عنوان البوابة الافتراضية لجهازك في مربع "Target" ومن ثم اختر نوع المسح "Intense Scan"، ثم اضغط على "Scan" كما في الشكل(١٣٨-٣):



الشكل 138-٣: خيارات نوع المسح في برنامج Zenmap

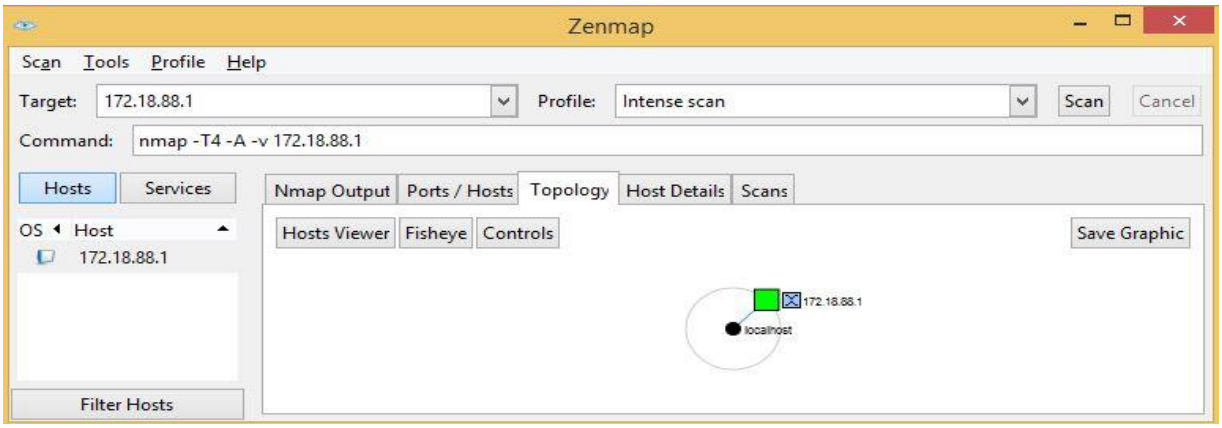
نلاحظ أنه في الشاشة السابقة أن البرنامج استطاع عمل مسح لمعلومات للبوابة الافتراضية لهذه الشبكة من خلال الوصول إلى أسماء الأجهزة المستخدمة والعنوان الفيزيائي والمنافذ المفتوحة. يمكنك استعراض معلومات أكثر ومفصلة عن جميع الأجهزة المرتبط بالبوابة الافتراضية من خلال اختيار نوع المسح "Slow Comprehensive Scan" لكن هذا المسح قد يستغرق وقتاً طويلاً بناء على حجم الشبكة التي تعمل عليها.

٥-من الشاشة الرئيسية للبرنامج اضغط على "Ports/Hosts" للحصول على حالة المنافذ في الشبكة الخاصة بك والخدمات التي تقدمها كما في الشكل(١٣٩-٣):



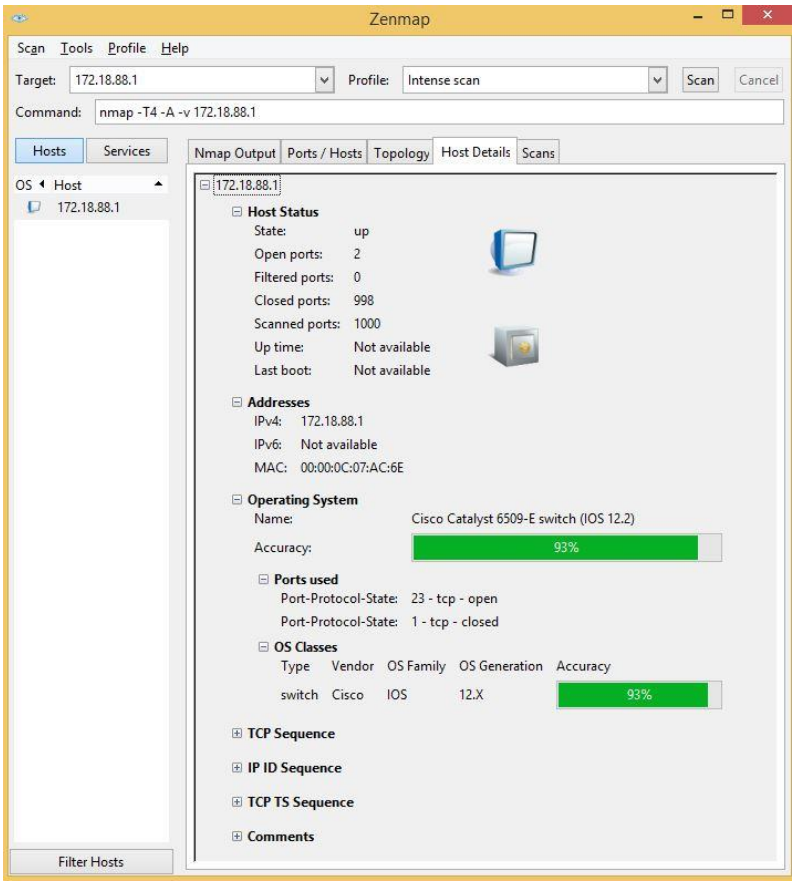
الشكل 139-٣: استعراض حالة المنافذ في الشبكة الخاصة بك والخدمات التي تقدمها عن طريق برنامج Zenmap.

٦-كما يمكنك استعراض طريقة الربط المستخدمة بين جهازك والهدف المُختبر من خلال اختيار "Topology" كما في الشكل(١٤٠-٣):



الشكل 140-٣ : استعراض طريقة الربط المستخدمة بين جهازك والهدف المُختبر عن طريق Zenmap.

٧-يمكنك استعراض تفاصيل المضيف من خلال الضغط على"Host Details" كما في الشكل(١٤١-٣):



الشكل 141-٣: استعراض تفاصيل المضيف عن طريق برنامج Zenmap

نلاحظ فيه وجود جميع معلومات المضيف والحالة وعدد المنافذ المفتوحة والمغلقة فيه. كما يحتوي على نوع نظام التشغيل المستخدم والعنوان الفيزيائي لهذا الجهاز.

٨-قم بعملية فحص لبعض الأجهزة الموجودة في الشبكة التي تعمل عليها مثل "DHCP Server، DNS Server". يمكنك الحصول على عناوين هذه الأجهزة من خلال كتابة الأمر "ipconfig /all" في موجه الأوامر Cmd. ومن ثم ناقش مع مدربك المعلومات التي حصلت عليها.

ملاحظة يمكن إجراء هذا الفحص على الشبكة الداخلية الخاصة بك في المنزل. حيث سيقوم البرنامج بعرض حالة المنافذ الخاصة بك وإمكانية استعراض الأجهزة المرتبطة بشبكتك الداخلية وعناوينها الفيزيائية من خلال استخدام نوع المسح "Intense Scan". يمكنك هذا البرنامج من مراقبة منافذ الجهاز الذي تعمل عليه ومعرفة المخاطر التي من الممكن أن تصيبك من خلال حالة هذه المنافذ والأجهزة المرتبطة بشبكتك والتي من الممكن أن تكون ارتباطها من غير علمك.

اليوم الثالث - الجلسة التدريبية الثالثة
استمرارية العمل
التحكم بالمخاطر البيئية

هناك الكثير من العوامل التي تعرض سلامة الحاسوب الشخصي للخطر والتي يمكن تصنيفها إلى:

الحرارة العالية: الحاسوب الشخصي شأنه شأن الأجهزة الكهربائية الأخرى، فيه الكثير من القطع التي تولد حرارة أثناء عملية التشغيل مما يؤدي إلى ارتفاع درجة الحرارة داخل الحاسوب بمعدلات أعلى من البيئة المحيطة له، لذا يتم تجهيز الحاسوب بمراوح داخلية تعمل مع بداية التشغيل، لغرض تقليل درجة الحرارة للمعدل المقبول، من خلال دفع الهواء الساخن الناتج عن ارتفاع درجة حرارة القطع والبطاقات الموجودة داخل علبة الحاسوب. وسحب تيار هواء بارد من المحيط الخارجي من خلال فتحات التهوية الموجودة في الأغطية الخارجية للعلبة. إلا أن ارتفاع درجة الحرارة الخارجية إلى أكثر من المعدلات الموصى بها (١٦-٣٣) درجة مئوية، قد يؤدي إلى تضرر الحاسوب، وعليه يجب اتخاذ الإجراءات الآتية للمحافظة على الحاسوب:

- التأكد من وضع الحاسوب في المواضع التي تسمح للهواء بالمرور إلى داخل علبة الحاسوب من خلال فتحات التهوية.
- تجنب تشغيل الحاسوب عندما ترتفع درجة حرارة الغرفة إلى أكثر من (٣٣) درجة، في حال تعطلت أجهزة التكيف.
- الفحص المستمر للمراوح الداخلية والتأكد من عملها بشكل صحيح. خاصة المروحة المخصصة للمعالج ومجهز القدرة.
- تجنب وضع أجهزة تولد طاقة حرارية بالقرب من الحاسوب المستخدم. فضلا عن تجنب وضعه في مكان تصل إليه أشعة الشمس بشكل مباشر.
- ولزيادة الأمان نقوم بإضافة بطاقات أو دارات متحسسة للحرارة تركب داخل الحاسوب وتطلق إشارة إنذار عند ارتفاع درجة الحرارة لحد معين خارج الحد المسموح به.

الغبار: يتألف الغبار من ذرات رمل صغيرة، ويسبب عدة مشكلات للمكونات الداخلية للحاسوب الشخصي، مع ملاحظة أن تشغيل الحاسوب، سيؤدي إلى وجود شحنة كهربائية تولد مجال مغناطيسي يؤدي إلى جذب الغبار والأتربة إلى داخل علبة الحاسوب، فضلا عن أن عمل المراوح الداخلية يؤدي إلى تكوين تيار هواء يسحب معه الغبار إلى داخل علبة الحاسوب. إن هذا الغبار يمكن أن يؤدي إلى:

- تراكم ذرات الغبار على الدارات داخل الحاسوب مما يؤدي إلى تشكيل طبقة عازلة حرارياً وهذا يقلل من تبديد الحاسوب للحرارة الناتجة.
- يسد الغبار منطقة امتصاص الهواء في وحدة الإمداد بالطاقة والقرص الصلب.

- يسد الغبار بين رأس القراءة والكتابة وبين القرص في مشغل الأقراص المرنة.

ولتجنب هذه المشكلات يراعى وضع الحاسوب في الغرف والقاعات التي يتم تكيفها باستخدام أجهزة التكيف، ولا يتم فيها فتح النوافذ لمنع دخول الغبار. كما يفضل وضع الحواسيب في مؤسسات المعلومات في القاعات التي لا يستخدم السجاد (والموكيت) في تغطية أرضيتها. ومن المفيد دائما تنظيف الحواسيب باستخدام أجهزة نفخ الهواء كل سنة مرة على الأقل. [٢]

المجال المغناطيسي: معظم الأجهزة الكهربائية تولد مجال مغناطيسي عند تشغيلها، ولكن بحدود قليلة نسبيا، لكن في حال تعرض الحاسوب الشخصي إلى مجال مغناطيسي عالي، فإن المكونات الممغنطة فيه مثل القرص الصلب أو الأقراص المرنة قد تتأثر، ويتم فقد المعلومات المخزنة عليها. وهو ضرر قد يحدث في حال تمرير الأقراص المرنة أو أجهزة الحاسوب الشخصي (المحمول) خاصة في أجهزة فحص الأمتعة في المطارات والمناطق الحساسة الأخرى. لذا يفضل دائما استخدام الأقراص الليزرية في تخزين نسخ من البيانات والمعلومات، في حال وجود تنفيذ عملية فحص الأجهزة في الأماكن المشار إليها.

تذبذب الطاقة: يعتبر مقبس الطاقة الجداري مصدراً لكثير من المشكلات التي يمكن أن تؤثر في المكونات المادية للحواسيب، إذ تصنف تأثيرات مصدر الطاقة إلى:

- المشكلات الناتجة عن ازدياد الجهد وانخفاض الجهد (تذبذب التيار). إن انخفاض الجهد يؤدي إلى زيادة التيار المستهلك وهذا بدوره يؤدي إلى زيادة القواطع الكهربائية والتوصيلات مما يؤدي إلى ارتفاع حرارة وحدة الإمداد بالطاقة وكذلك الرقائق ويمكن حل هذه المشكلة بالاستعانة بأجهزة تنظيم الكهرباء.
- المشكلات الناتجة عن غياب الجهد نهائياً. والتي تؤدي إلى توقف التشغيل في بعض المكونات، واستمراره في مكونات أخرى.
- المشكلات الناتجة عن العبور. العبور هو عبارة عن تغير طفيف في الطاقة لا يمكن أنه يكرر نفسه مرة أخرى ويأتي على شكل انخفاض في الجهد أو ارتفاع في الجهد فإذا امتلك العبور ترددا كافياً عطل مكثفات الحماية وعناصر أخرى لوحدة الإمداد بالطاقة كما أن الجهد يؤدي إلى نفس الأضرار وتعطيل رقائق الحاسوب التي قد يتسبب بها تشغيل الطاقة أو اندفاع الطاقة.
- المشكلات الناتجة عن عملية تفريغ الكهرباء الساكنة. جسم الإنسان قابل أن يشحن بشحنة ساكنة وقد تصل إلى حوالي ٥٠ ألف فولت ويكفي ٢٠٠ فولت لإفساد الرقائق الإلكترونية لذلك قبل البدء بأي عملية صيانة يجب تفريغ الشحنة التي تحملها بواسطة لمس أشياء معدنية ويمكن تجنب مشكلة الكهرباء من خلال زيادة رطوبة الجو بواسطة أجهزة زيادة الرطوبة. أو زيادة رطوبة الجو عن طريق اقتناء نباتات الزينة وأحواض السمك.

عوامل التآكل: يعد الماء والأملاح من المواد الخطرة على الحاسوب ويجب تجنيب الحاسوب الأشياء التالية:

- انسكاب الماء أو أي سوائل أخرى غير مقصودة.
- الترشيح الناتج عن تسرب المياه الرطبة إلى داخل الحاسوب.
- فيضان المياه ودخول الماء إلى الحاسوب.
- ويعد التآكل عمل آخر من عوامل الأضرار بالأجهزة نتيجة تراكم الأملاح بسبب تعرق جسم الإنسان، وتراكم الأحماض الكبريتية الناتجة عن النقل بواسطة الطائرات.
- إن المشكلة الكبرى التي نتعرض لها هي أكسدة نقاط الدارات وبالتالي تفقد وظيفتها في وصل الدارات ببعضها، وبالتالي تعطل الحاسوب.

لهذا السبب، يجب توخي الحذر عند التعامل مع بطاقات الدارات وعدم لمس أقطابها خوفاً من تأثير الأملاح الناتجة عن التعرق. [١]

البيئة المناسبة لعمل الحاسوب:

يجب ملاحظة بعض الأمور لجعل البيئة المحيطة بالحاسوب مناسبة للتشغيل، وتحقق مستوى أمان مناسب للحفاظ على الجهاز ومن هذه الأمور:

- تأكد من تأمين شروط حماية الطاقة الكهربائية. وذلك بعدم ربط الحاسوب مباشرة إلى مصدر طاقة، وإنما يفضل استخدام جهاز حماية UPS.
- يفضل عدم مشاركة الحاسوب لأي جهاز كهربائي آخر على نفس مصدر الطاقة.
- لا يفضل تشغل محركات ضخمة على نفس خط الطاقة الذي يغذي الحاسوب.
- إبعاد الحاسوب عن مصادر الضجيج.
- حافظ على مستوى معتدل لدرجة حرارة الغرفة.
- يساعد إبقاء الحاسوب في حالة عمل دائم على ضبط حرارة الحاسوب الداخلية بشكل جيد.
- تأكد من عدم وجود أي مصدر للاهتزاز على نفس الطاولة. التي يوجد عليها الحاسوب.
- الحرص على تعميم إجراءات السلامة تلك على جميع العاملين في مؤسسات المعلومات الذين يستخدمون الحاسوب.

النسخ الاحتياطي وحماية الملفات

في مجال تكنولوجيا المعلومات. النسخ الاحتياطي أو عملية النسخ الاحتياطي تشير إلى صنع نسخ من البيانات بحيث يمكن استخدام هذه النسخ لاستعادة البيانات الأصلية في حال تم فقد البيانات الأصلية. يقابل هذه العملية عملية الاسترجاع والتي يتم فيها استعادة البيانات إلى موقعها في الأنظمة. [٤]

أهمية النسخ الاحتياطي:

يؤدي النسخ الاحتياطي دوراً مهماً في الأحوال التالية:

١. تحقيق متطلبات الأعمال داخل المنشأة.
٢. الحماية من فشل الأجهزة.
٣. التعافي من الكوارث.
٤. الحماية من فشل التطبيقات.
٥. الحماية من أخطاء للمستخدمين.
٦. المتطلبات القانونية وتشمل عادة الشروط القانونية التي تفرضها الوكالات التنظيمية الحكومية. وعادة ما تشمل هذه المتطلبات الاحتفاظ بالبيانات لأنواع معينة من البيانات لفترات محددة.

وسائط التخزين:

١-الشريط المغناطيسي:

الشريط المغناطيسي اعتبر لفترة طويلة الوسيلة الأكثر شيوعاً لتخزين البيانات. والنسخ الاحتياطي، والأرشفة، وتبادل البيانات. يتميز الشريط المغناطيسي الذي يدعم معيار LTO-5 بقدرة على تخزين كمية كبيرة من البيانات تصل إلى ٣ تيرابايت مع إمكانية تشفير البيانات بواسطة محرك الشريط المغناطيسي. الشريط المغناطيسي يمكن أن يدعم خاصية WORM أي اكتب مرة واحدة واقرأ العديد من المرات. هذه الخاصية مهمة عند أرشفة البيانات.

٢-القرص الثابت الخارجي:

يعتبر حلاً مناسباً للحفظ الاحتياطي للبيانات للأفراد عند حال الرغبة في الحفظ الاحتياطي لملفات الصوت والصورة ذات الأحجام العالية وكذلك الحفظ الاحتياطي للأقراص الصلبة، كذلك يعتبر القرص الثابت الخارجي حلاً مناسباً لأعمال الحفظ الاحتياطي في المنشآت الصغيرة.

الأقراص المدمجة:

تعتبر حلاً مناسباً للحفظ الاحتياطي للبيانات المستخدمين ذات الحجم المحدود والذي يتناسب مع السعة التخزينية للقرص المدمج.

تقنيات الحفظ:

تؤدي تقنيات الحفظ دوراً بارزاً في تسهيل عملية الحفظ الاحتياطي للمؤسسات الكبيرة. كذلك تعتبر هذه التقنيات ذات فاعلية عالية في عملية الاسترجاع. **من أمثلة هذه التقنيات:**

١-المخازن **المتصلة مباشرة** (Directly Attached Storage—DAS):

وهو عبارة عن نظام تخزين رقمي يرتبط مباشرة بمقلم أو محطة عمل. بدون أن تكون هنالك شبكة تخزين بينهما. البروتوكولات الرئيسية المستخدمة للربط تشمل: SCSI SATA.ATA.FiberChannel

٢-شبكة **منطقة التخزين** (Storage Area Network SAN):

تُعرّف بأنها شبكة الغرض الأساسي منها هو نقل البيانات بين أنظمة الكمبيوتر وعناصر التخزين. تتكون شبكة منطقة التخزين من البنية التحتية للاتصالات، التي تقدم اتصالات فعلية، وطبقة الإدارة، والتي تنظم الاتصالات، وعناصر التخزين، وأنظمة الكمبيوتر بحيث يتم نقل البيانات بشكل آمن وسليم. عناصر التخزين في شبكة منطقة التخزين تشمل الأقراص الصلبة والأشرطة المغناطيسية.

البروتوكولات الرئيسية المستخدمة للربط تشمل: ATA over Ethernet iFCP ISCSI FC over Ethernet

أنماط النسخ الاحتياطي:

١-النسخ الاحتياطي الكامل:

يتم فيه أخذ نسخة احتياطية كاملة من كل ملف على نظام الملفات، سواء كان هذا الملف قد تغير أم لا. أخذ نسخة احتياطية كاملة يستغرق وقتاً أطول لإنجاز ذلك ويتطلب معظم مساحة التخزين على وسائط النسخ الاحتياطي، ولكنه يوفر استعادة أسرع.

٢-نسخ احتياطي تزايدي:

وفيه يتم أخذ نسخة احتياطية من كل ملف على نظام الملفات التي قد تغيرت منذ آخر نسخ احتياطي.

٣-النسخ الاحتياطي التفاضلي (أو التفاوتي):

وفيه يتم أخذ نسخة احتياطية من كل ملف على نظام الملفات التي قد تغيرت منذ النسخ الاحتياطي الكامل الأخير. إذا قمت بإجراء نسخة احتياطية كاملة يوم الجمعة والتفاضلية كل ليلة. وتعطل النظام يوم الثلاثاء. فسوف تحتاج فقط إلى استعادة النسخة الاحتياطية الكاملة الخاصة بيوم الجمعة، والنسخة الاحتياطية التفاضلية الخاصة بيوم الاثنين. وفي المقابل، إذا قمت بإجراء نسخة احتياطية كاملة يوم الجمعة ونسخ احتياطي تزايدي كل ليلة، فإذا تعطل النظام يوم الثلاثاء، فسوف تحتاج إلى استعادة النسخ الاحتياطي الكامل الخاص بيوم الجمعة إلى جانب النسخ الاحتياطية التزايدية الخاصة بأيام السبت، الأحد، والاثنين.

وينبغي إجراء النسخ الاحتياطي التفاضلي يومياً على الأنظمة الإنتاجية.

أساليب عمل النسخ الاحتياطي:

١-النسخ الاحتياطي الكامل دائماً:

في كل مرة يتم عمل النسخ الاحتياطي لملفات المشروع يتم عمل النسخ الاحتياطي لجميع الملفات، سواء تغير بعضها أم لا. هذا النهج جيد عندما لا يشمل المشروع كميات كبيرة جدّا من البيانات.

٢-نسخ احتياطي كامل + نسخ تزايدي:

ويتم فيه إنشاء نسخة احتياطية كاملة مرة واحدة في الشهر، أو مرة واحدة في الأسبوع، أو عند تحقيق نقطة مهمة في العمل. لجميع أعمال النسخ الاحتياطي التالية يتم استخدام النمط التزايدي، ليتم الحصول على نسخ احتياطية للملفات فقط التي تغيرت منذ النسخ الاحتياطي الأخير. يعتبر هذا الأسلوب مناسباً للمشاريع التي تتضمن العديد من الملفات وتستلزم إجراء نسخ احتياطي لكل الملفات في كل مرة. يتميز هذا الأسلوب بأنه سريع ويستغرق وقتاً أقل لعمل نسخ احتياطي تزايدي. كذلك يتميز بأنه يأخذ مساحة أقل على وسائط التخزين. لاستعادة جميع الملفات، يجب استعادة النسخ الاحتياطي الكامل الأخير، وجميع النسخ الاحتياطية الإضافية.

٣-نسخ احتياطي كامل + نسخ التفاضلي:

هو أسلوب وسيط بين الأسلوبين السابقين. النسخ التفاضلي يشمل جميع ملفات المشروع التي تم تغييرها منذ النسخ الاحتياطي الكامل الأخير. يتميز هذا الأسلوب بأنه يستغرق وقتاً ومساحة أقل من "النسخ الاحتياطي الكامل دائماً"، ولكن أكثر من "نسخ احتياطي كامل + نسخ تزايدي". ولاستعادة البيانات يتم استعادة آخر نسخة احتياطية كاملة وآخر نسخة احتياطية تفاضلية.

أسئلة ونقاش(١٤):

س١: اذكر العوامل التي تعرض سلامة الحاسوب الشخص للخطر؟

س٢: ما البيئة المناسبة لعمل الحاسوب؟

النسخ الاحتياطي لنظام ويندوز ٨

ملاحظة: يتم استخدام نظام التشغيل ويندوز٨ لإتمام هذا التدريب.

يقوم برنامج "النسخ الاحتياطي والاستعادة" في نظام ويندوز بعمل نسخة كاملة من نظام التشغيل تشمل البرامج وإعدادات النظام والملفات. يمكن استخدام هذه النسخة في حالة وحدوث خلل أو كارثه لنظام التشغيل؛ عندها ستتمكن من استعادة جميع بيانات الجهاز.

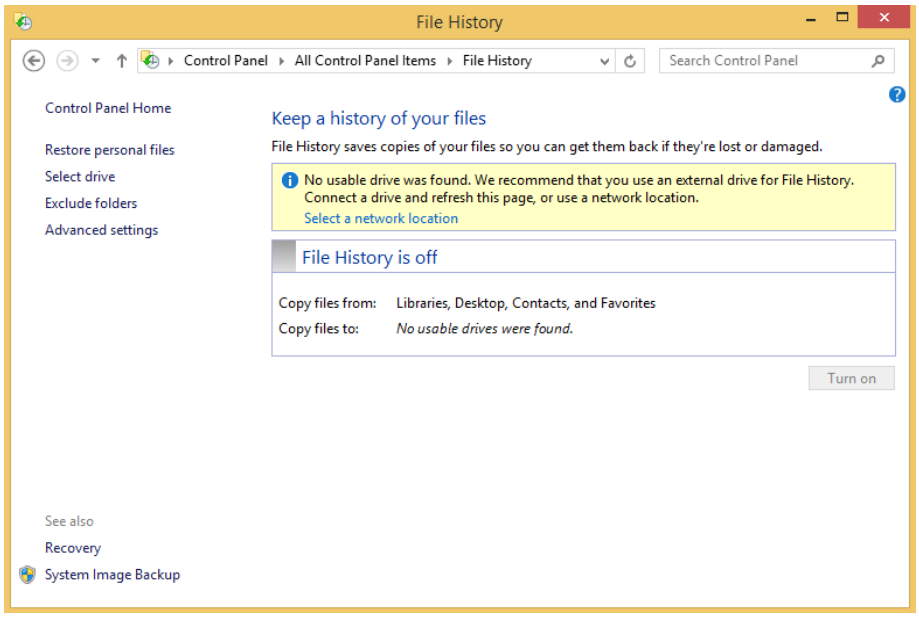
تمرين عملي(٢٢):

لعمل نسخة احتياطية للبرامج، إعدادات النظام والملفات اتبع الخطوات التالية:

١-من قائمة إبدأ اضغط على لوحة التحكم ومن ثم Strat, Control Panel, File History

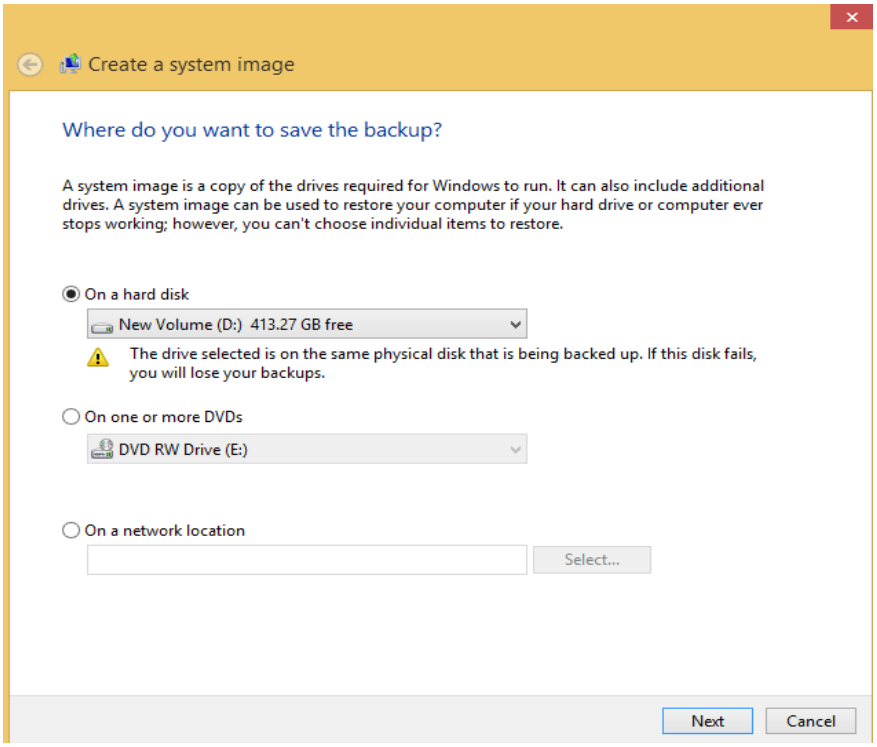
اضغط على Strat – Control Panel – File History

ستظهر لك الشاشة التالية:



الشكل142 -٣: إعدادات ملفات النظام في ويندوز.

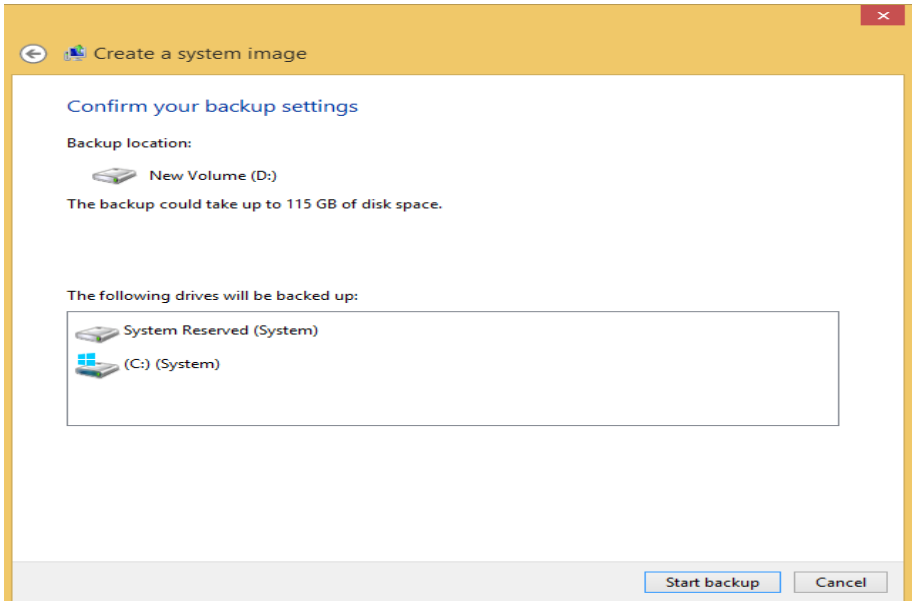
٢-من أسفل الشاشة قم باختيار System Image fileعندها ستظهر لك شاشة اختيار مكان حفظ النسخة الاحتياطية كما في الشكل (١٤٣-٣):



الشكل 143-٣: شاشة اختيار مكان حفظ النسخة الاحتياطية.

- كما هو ملاحظ في الشكل السابق توجد رسالتين من نظام التشغيل عند إنشاء نسخة احتياطية. الأولى تفيد بأن هذه النسخة يمكن استخدامها لاستعادة جهاز الكمبيوتر في حالة توقف القرص الصلب أو جهاز الكمبيوتر عن العمل، ولكن لن تستطيع اختيار عناصر محددة للاستعادة.
- الثانية عند اختيار القرص D "وهو جزء من القرص الفعلي الموجودة في الجهاز"، هذا القرص موجود بنفس القرص الفعلي للجهاز ففي حالة إصابة القرص الفعلي لهذا الجهاز ستفقد النسخة الاحتياطية المحفوظة أيضاً.
- فمن الأفضل حفظ النسخة الاحتياطية على قرص خارجي كما هو متاح في الخيار الثاني

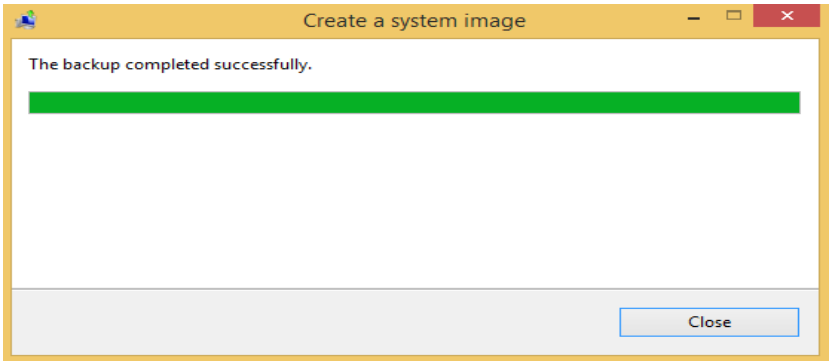
١- قم باختيار الخيار الأول كما في الشكل (١٤٣-٣) بالضغط على Next عندها ستظهر لك رسالة تظهر لك حجم النسخة الاحتياطية والسواقات التي سيتم عمل نسخة احتياطية لها، قم باختيار Start Backup كما في الشكل (١٤٤-٣):



الشكل 144-٣: شاشة إعدادات النسخة الاحتياطية.

عندها سيبدأ النظام عمل نسخة احتياطه، وقد تستغرق هذه العملية مدة زمنية طويلة بناء على عدد الملفات الموجودة على جهازك.

ستظهر لك الرسالة التالية تفيد بأن عملية النسخ الاحتياطي تمت بنجاح كما في الشكل (١٤٥-٣):



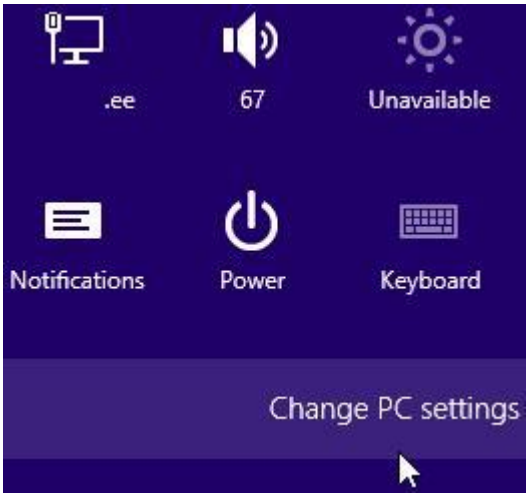
الشكل 145-٣: رسالة تنويه باكتمال النسخ الاحتياطي بنجاح.

استرجاع نسخة احتياطية:

تمرين عملي(٢٣):

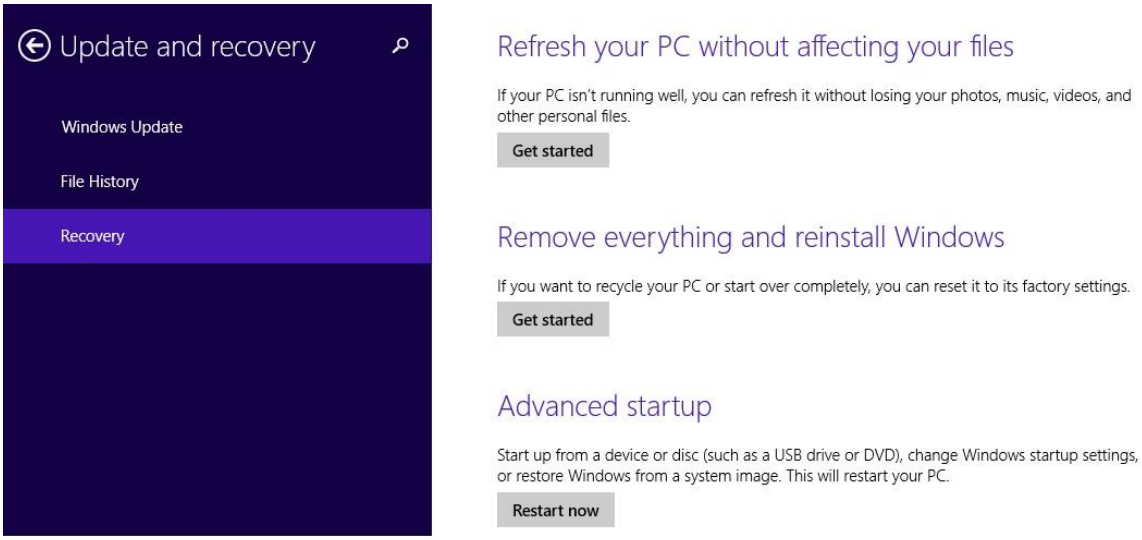
لعمل استرجاع لنسخة احتياطية اتبع الخطوات التالية:

١- اضغط على مفتاحي علامة الويندوز في الكيبورد + I في نفس الوقت، وستظهر لك القائمة التالية:



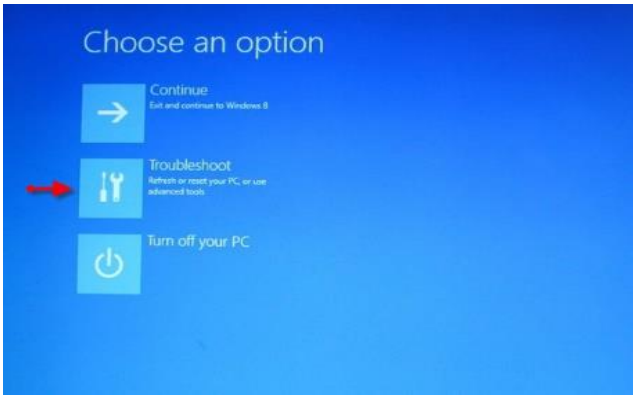
الشكل 146-٣: إعدادات نظام الويندوز الأساسية.

٢- قم باختيار Change PC Sitting - Update and recovery – Recovery، ستظهر لك الشاشة التالية:



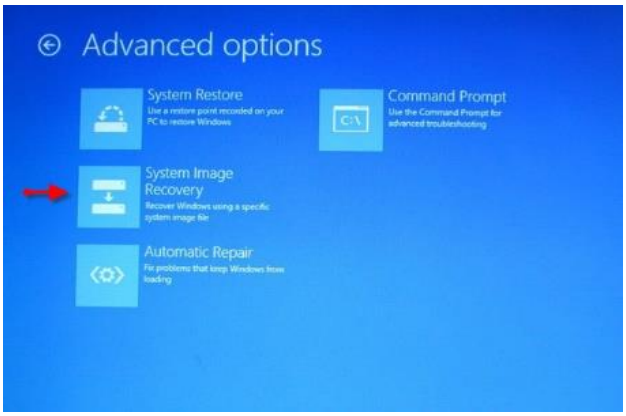
الشكل147 -٣: شاشة التحديث والاستعادة في نظام التشغيل ويندوز.

٣- من Advance Startup اختر Restart now ومن ثم اتبع الخطوات التالية:



الشكل 148-٣: خيارات النظام بعد النسخة الاحتياطية في نظام ويندوز

الشكل 149-٣: خيارات النظام المتقدمة في استعادة النسخة الاحتياطية لنظام التشغيل ويندوز



الشكل 150-٣: استعادة النسخة الاحتياطية للنظام ويندوز

٤- عندها سيطلب نظام التشغيل الرقم السري لحساب مدير النظام، ادخل الرقم السري للحساب ومن ثم Continue عندها ستظهر لك شاشة اختيار مكان النسخة الاحتياطية، قم بإدخال القرص الخاص بالنسخة الاحتياطية ومن ثم سيبدأ النظام باسترجاع النسخة الاحتياطية المأخوذة سابقاً:

** **ملاحظة** يتوقف المتدرب عند خطوة ادخل الرقم السري لحساب مدير النظام، بناء على نظام المعامل في معهد الإدارة.

استعادة الملفات المحذوفة

يمكن تعريف استعادة البيانات Data Recovery بأنها عملية استعادة البيانات المحذوفة أو غير القابلة للوصول (القراءة) من وسط تخزين إلكتروني مثل الأقراص الصلبة، وسائط قابلة للنقل.

مفهوم فقد البيانات: يعتبر مفهوم فقد البيانات (Data loss) من الأكثر سوءَ في الفهم، ومعظم البيانات المفقودة هي ليست مفقودة بتاتاً، ولكنها ببساطة لا يمكن للمستخدم الوصول إليها. وإن ٩٥% من البيانات يمكن استعادته عند استخدام التقنيات والأدوات المناسبة والتي شهدت تطوراً ملحوظاً في السنوات الأخيرة، متناسباً مع تطور وسائط تخزين البيانات. وسواء كنت تخزن ملفاتك على القرص الصلب، القرص اللين، أو أي واسطة تخزين خارجية، فإن طريقة تخزين البيانات هي نفسها جوهرياً، لذلك عند التكلم عن استعادة البيانات من القرص الصلب فهذا يعني معظم وسائط التخزين الأخرى.

قد تفقد البيانات بسبب المشكلات المتعلقة بالوصول إلى البيانات من البرامج أو منطقياً، لنلقي نظرة عن كيفية تخزين القرص الصلب للبيانات وما هي المشكلات التي يمكن استعادة البيانات التي فقدت بسببها:

قطاعات، عناقيد وملفات تخزين: عندما تقوم بشراء قرص صلب جديد فهو غالباً ما يكون قد خضع لعملية تهيئة منخفضة المستوى Low level format الغاية منها تقسيم المساحة الممغنطة على القرص إلى مناطق صغيرة وهي ما يعرف بالقطاعات Sectors. ولغرض الفعالية تقوم أنظمة التشغيل (مثل Windows) بجمع القطاعات بما يسمى العناقيد Clusters والذي هو عبارة عن أصغر مساحة للتخزين يمكن لنظام التشغيل التعامل معها. إذا قمت بحفظ ملف صغير جداً على حاسبك، فسوف يوضع على عنقود واحد من قرصك الصلب، لكن الأمور بالحقيقة أكثر تعقيداً فالملف الواحد قد لا يوضع على عناقيد مستمرة، بل على أقسام مختلفة من القرص الصلب، وهو ما يسمى الملف المبعثر Fragmented File والتي قد تسبب بطأ في حاسبك حيث يستغرق وقتا أطول ليرسل الذراع الميكانيكية إلى هذه الأقسام المختلفة على القرص من أجل القراءة. لذلك يجب إزالة البعثرة حيث إن الملف المبعثر يقلل من إمكانية استعادته. العناقيد التي تستخدم في حفظ البيانات تسمى العناقيد الموزعة Allocated Clusters وغير المستخدمة تسمى Unallocated Clusters، ولكي يجد الحاسب ملفاً محدداً يستخدم ما يسمى جدول توضع الملفات File Allocation Table اختصاراً FAT (وأحياناً يسمى Master File Table MFT)، حيث يحتوي هذا الجدول على أسماء الملفات، أرقام عناقيدها، وحجمها. ويقوم نظام التشغيل باستخدام هذه المعلومات لإيجاد الملفات المطلوبة (لاحظ أن هذه المعلومات تخزن بشكل منفصل عن الملف لذلك يمكن استعادتها).

ما الذي يحدث عندم ا نحذف ملفاً ما: عندما تحدد ملفاً ما وتضغط على زر الحذف في نظام ويندوز يتم إرساله إلى سلة المحذوفات، والتي هي عبارة عن مكان آخر للحفظ وعند إفراغ محتويات السلة أو عندما لا يمر الحذف عبر هذه السلة (Shift+Del) يقوم نظام التشغيل بتعليم اسم الملف في FAT بعلامة خاصة تجعل الحاسب يعتقد أن مكان الملف المحذوف فارغ ويمكن التخزين فوق عناقيده، أي أن نظام التشغيل لا يقوم بمسح المكان الحقيقي للعناقيد المستخدمة في حفظ الملف

المحذوف. الملف المحذوف لازال في مكانه، ولكن نظام التشغيل لا يعرف بوجوده، وهذا هو مفهوم استعادة البيانات أي البحث عن البيانات الموجودة على القرص الصلب والتي لا يستطيع نظام التشغيل إيجادها، إذا كانت العناقيد التي تحتوي هذه البيانات معطوبة أو مخربة فيزيائياً فإن استعادتها شبه مستحيل. وطالما لم تستخدم هذه العناقيد في حفظ ملف جديد فإنه من الممكن استعادتها، وذلك قد يكون من الأفضل استخدام حاسب آخر عند استعادة بيانات القرص الصلب. وهناك العديد من البرامج التي تساعد في الاستعادة وتظهر لك نسبة إمكانية نجاح هذه العملية كما يلي ضعيف – وسط – جيد، وذلك بعد البحث عن FAT السابق والتأكد من سجلاته ومعرفة العناقيد التي يجب استخدامها للاستعادة، وفحص فيما إذا كان ملف جديد قد حفظ فوقه. لكن برامج الاستعادة الجديدة يكون فيها خيار تجاهل FATوالبحث في العناقيد كلها لمحاولة إيجاد أي ملفات قابلة للاستعادة، وهنا نحتاج لمعرفة نوع الملفات التي سنبحث عنها. معظم أنواع الملفات لها ترويسة وتذييل تختلف عن الملفات الأخرى، هذا يعني أنك إذا نظرت إلى ملف Word على سبيل المثال، فإن الأحرف الأولى والأخيرة هي نفسها لكل ملفات Word، لذلك تستطيع برامج الاستعادة البحث داخل القرص لتحديد الملفات عن طريق ترويستها وتذييلها.

الاستعادة من قرص صلب تمت تهيئته: عندما تقوم بتشغيل أمر التهيئة Format فأنك ببساطة تحذف الدليل الجذري وFAT، عندما تقوم برامج الاستعادة بالبحث عن الأدلة المحذوفة والتي هي في الحقيقة تحفظ على شكل ملفات، وعندما تجدها تقوم باستعادتها ثم تستعيد الملفات الأخرى، كما يمكن استخدام طريقة البحث عن الترويسة والتذييل هنا أيضاً. [٢]

تطبيقات استعادة الملفات المحذوفة

يوجد العديد من البرامج التي تتيح لك استرجاع الملفات المحذوفة من الذاكرة سواء كان الحذف بالعمد أو عن طريقة الخطأ. غالباً ما تستطيع هذه البرامج في استرجاع أغلب الملفات المحذوفة، ولكن قد تفشل بعض هذه البرامج في استرجاع اسم الملف. فعلى سبيل المثال إذا قمت بحذف ملف فيديو تحت اسم Mytrip؛ من الممكن أن تجد اسمه عبارة عن أرقام ولكن بنفس الحجم والمحتوى. سنستعرض بعض التطبيقات المستخدمة لهذا الغرض.

تمرين عملي(٢٤):

برنامج Recuva:

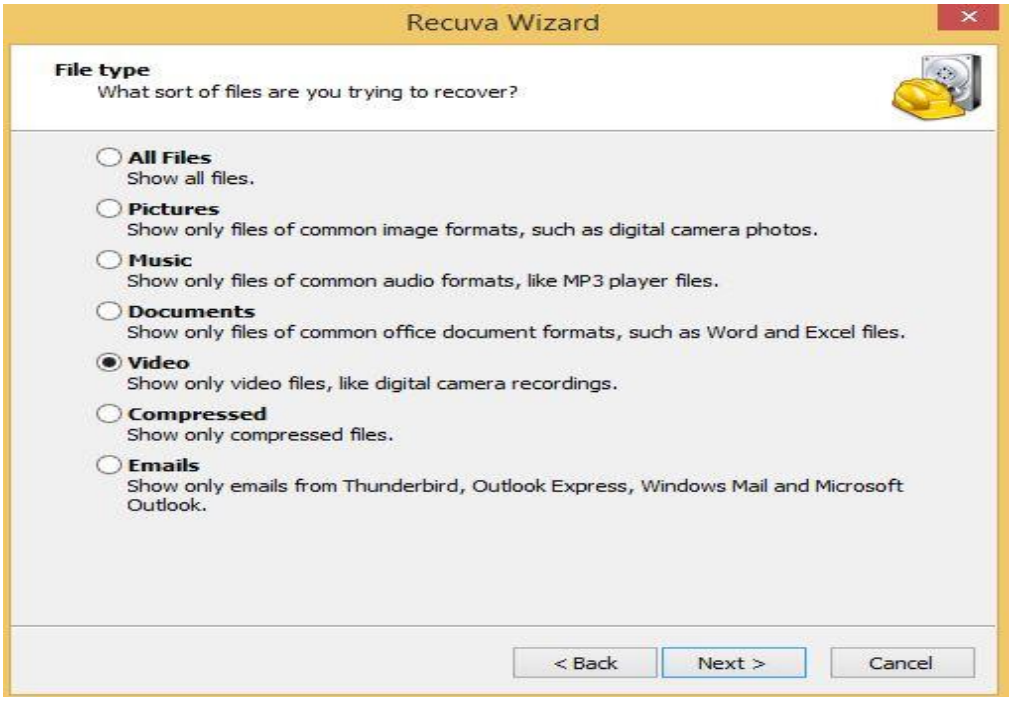
1- قم بتحميل البرنامج من محرك البحث أو من خلال الرابط التالي:

http://download.piriform.com/rcsetup151.exe

2- قم بعملية تثبيت البرنامج وعند الانتهاء ستظهر لك الشاشة التالية:

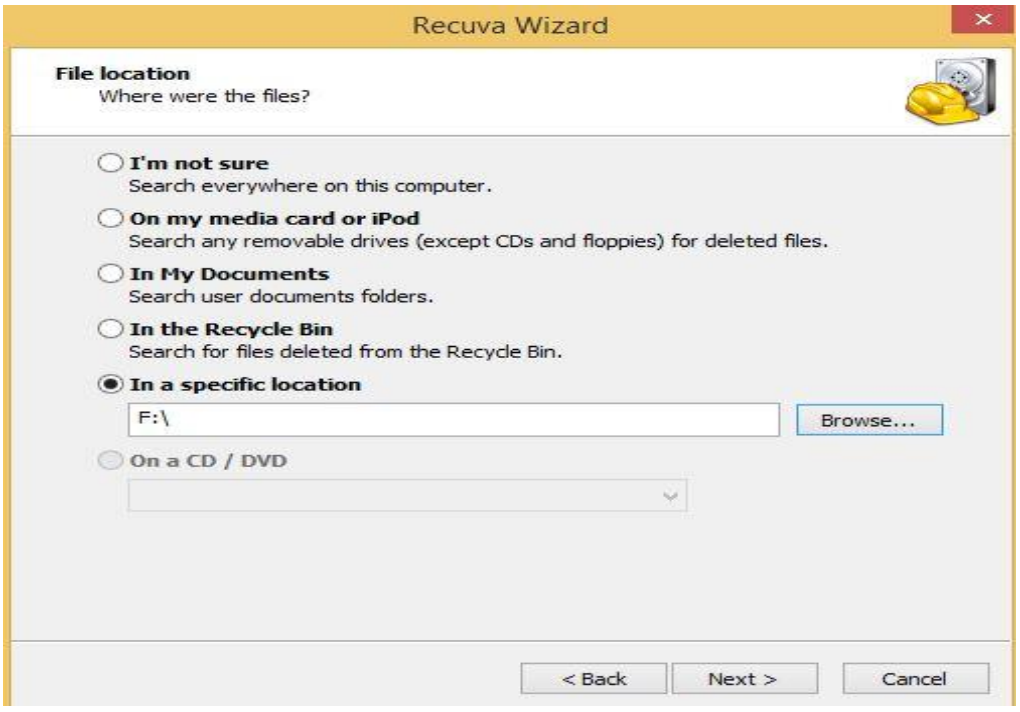
الشكل 151-٣: الواجهة الترحيبية لبرنامج Recuva Wizard

3- قم باختيار التالي "Next" عندها ستظهر لك الشاشة التالية:



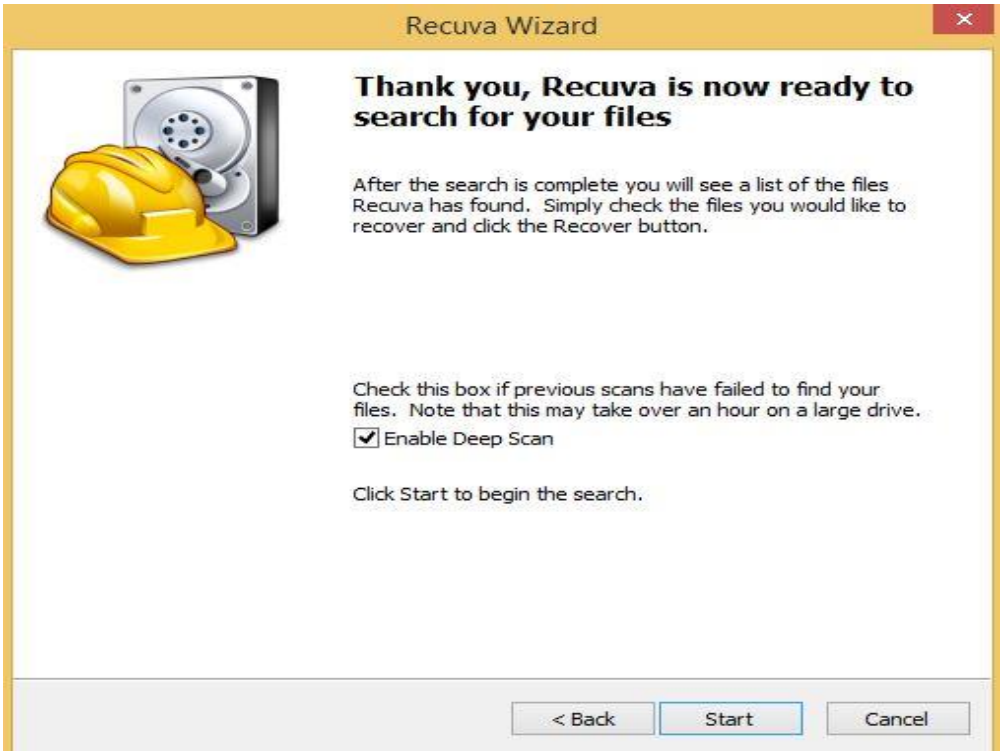
الشكل 152-٣: اختيار نوع الملف المراد باسترجاعه

٤-من هذه الشاشة، قم باختيار نوع الملف التي تريد استرجاعه



الشكل 153-٣: اختيار مكان الملف المراد استرجاعه

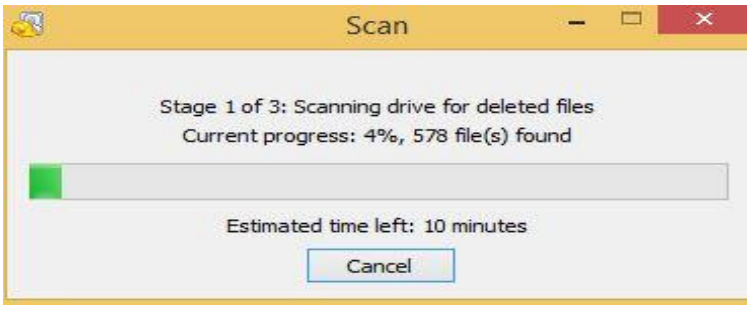
5- ومن ثم، قم باختيار مكان الملف المراد استرجاعه.



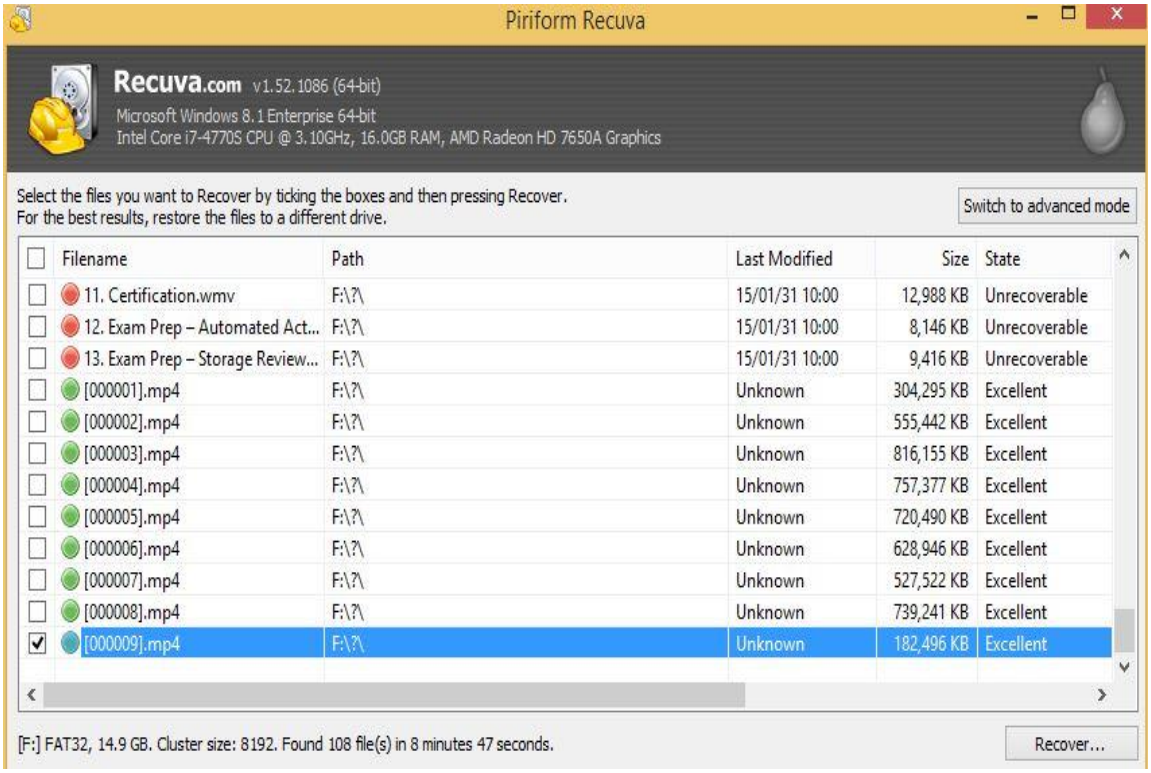
الشكل 154-٣: خيارات نوع الفحص المراد تطبيقه في البحث.

6- قم باختيار Deep Scan حيث يستغرق هذا النمط وقت أطول في عملية البحث عن الملفات المحذوفة ولكن يعطي نتائج أفضل.

اضغط على Start عندها سيبدأ البرنامج عملية البحث ويظهر الوقت المتبقي لعملية المسح كما في الشكل التالي:

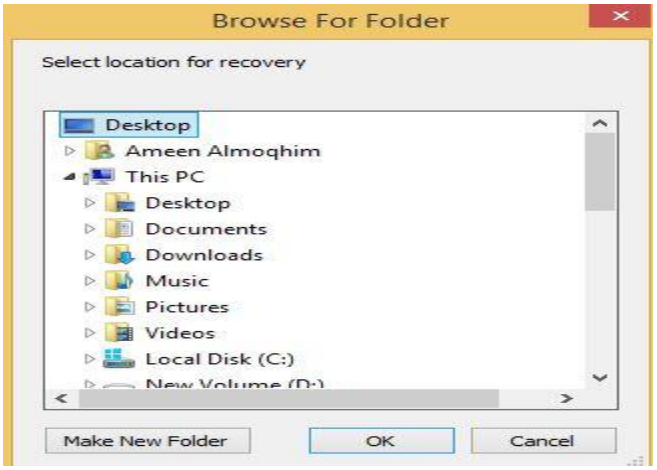


الشكل 155-٣: شاشة البحث عن الملفات المحذوفة.



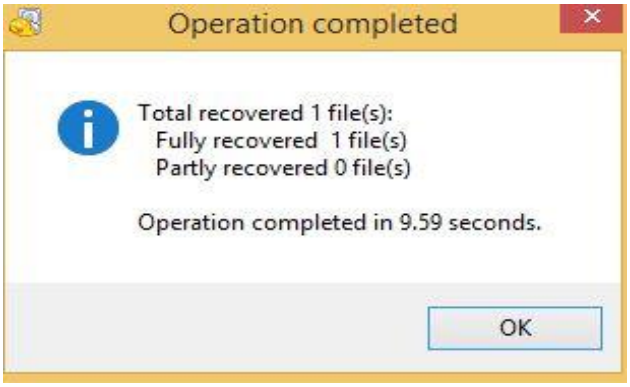
الشكل 156-٣: الملفات المحذوفة وإمكانية استرجاعها.

7- عندها ستظهر لك الملفات المحذوفة من الذاكرة المحددة سابقاً. نلاحظ وجود اسم الملف وامتداده والحجم وحالته، تستطيع فقط استرجاع الملفات التي حالتهExcellent . قم بتحديد الملف المراد استرجاعه ومن ثم اختر Recover:



الشكل 157-٣: تحديد الملف المراد استرجاعه

8- قم باختيار مكان حفظ الملف المُسترجع (يفضل اختيار مكان غير مكان الملف الأساسي المُسترجع).



الشكل 158-٣: اختيار كطان حفظ الملف المسترجع

أخيراً ستظهر لك رسالة تفيد بأنه تمت عملية الاسترجاع بنجاح والوقت المُستغرق لذلك.

برنامج EaseUS Data Recovery:

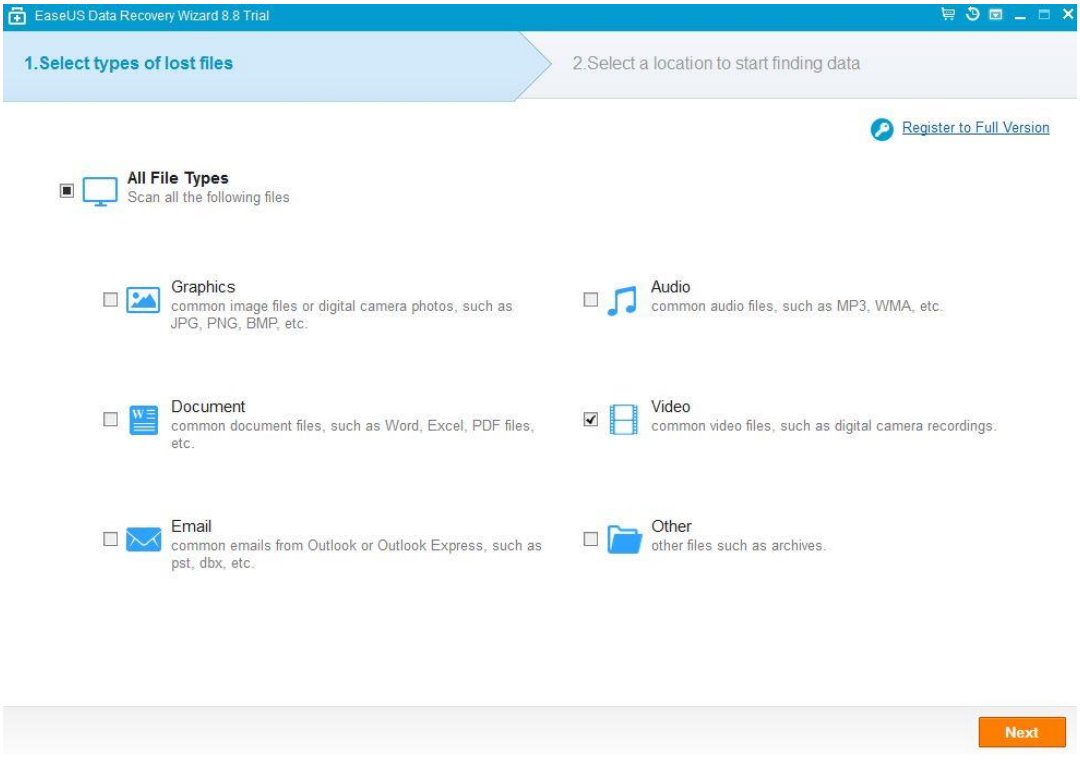
يعمل هذ البرنامج بكفاءة ودقة عالية مقارنة مع البرنامج السابق. حيث يتيح هذا البرنامج استعراض الملفات المحذوفة بكامل اسمها ومرتبة في مجلداتها السابقة. لكن يعتبر هذا البرنامج غير مجاني ويتطلب وجود نسخة كاملة لعملية الاسترجاع.

تمرين عملي(٢٥):

1- قم بتحميل النسخة التجريبية لهذا البرنامج محرك البحث أو من خلال الرابط التالي:

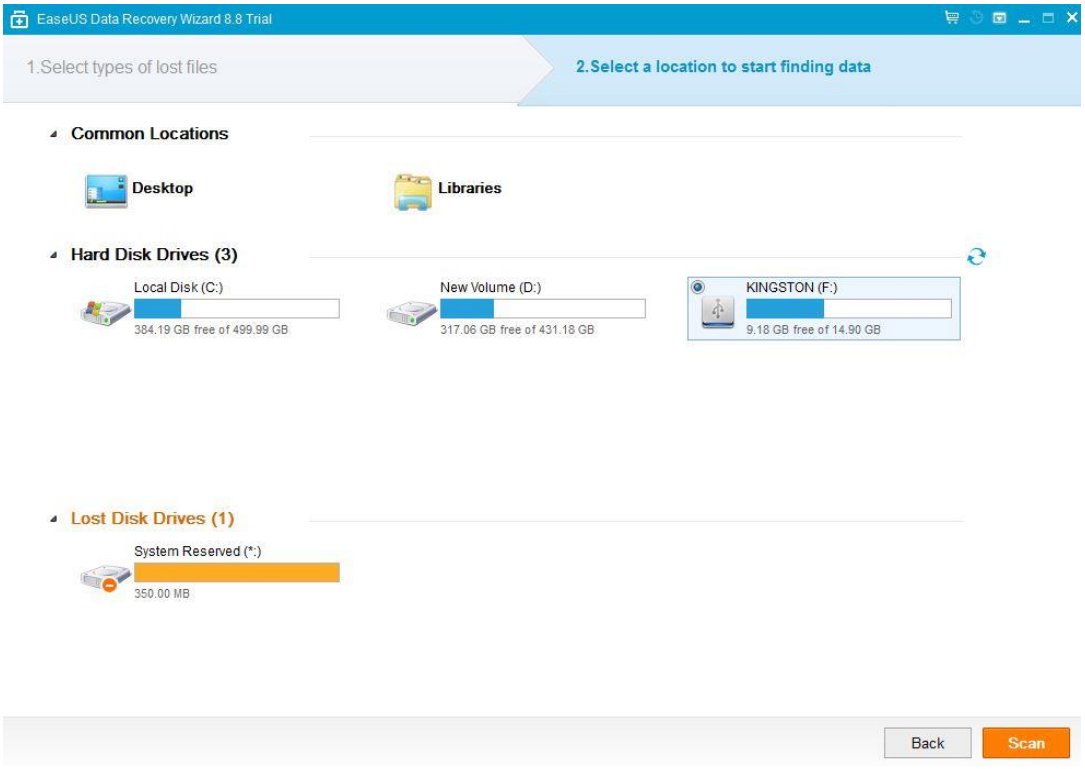
http://download.easeus.com/ad/drw_trial.exe

2- بعد عملية التثبيت وتشغيل البرنامج ستظهر لك الشاشة التالية:



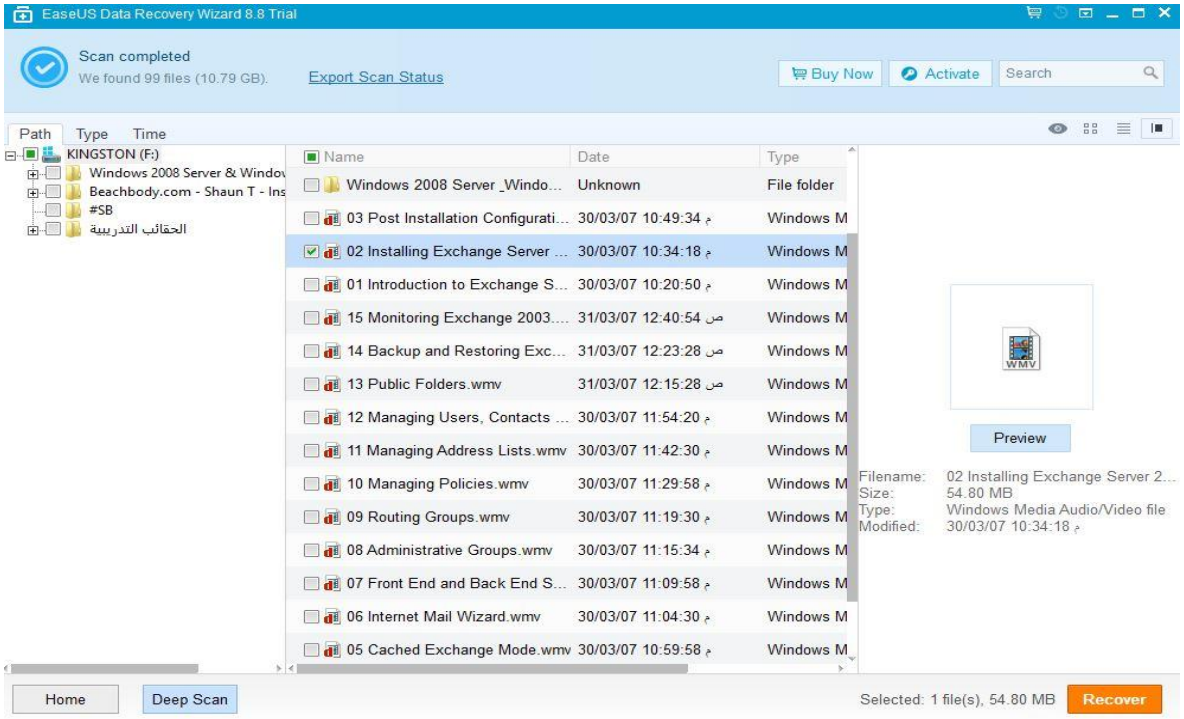
الشكل 159-٣: الشاشة الرئيسية لبرنامج EaseUS

3- قم باختيار نوع الملف المفقود ومن ثم اضغط على Next



الشكل 160-٣: اختيار نوع الملف المفقود لاسترجاعه عن طريق برنامج EaseUS

٤-ومن ثم قم باختيار القرص الذي تريد استرجاع الملف المفقود منه واضغط على Scan



الشكل 161-٣: اختيار القرص الذي تريد استرجاع الملف المفقود منه .

5- بعد عدة دقائق سيَظهر لك البرنامج الملفات التي يمكن استرجاعها بكامل الاسم والحجم. قم باختيار الملف المطلوب استرجاعه ومن ثم اضغط على Recover.

يتيح لك كذلك هذا البرنامج خيار البحث العميق Deep Scan حيث يمكن للبرنامج استرجاع ملفات أكثر تم فقدها أو حذفها في السابق.

معهد الإدارة العامة
INSTITUTE OF PUBLIC ADMINISTRATION

شرائح اليوم التدريبي الثالث

طبقات وأنواع الحوسبة السحابية

الطبقات:

- البنية التحتية كخدمة Infrastructure as a Service IaaS
- منصة العمل كخدمة Platform as a Service Paas
- التطبيق كخدمة Software as a Service Saas

الأنواع:

- السحابة الخاصة Private Cloud Computing
- السحابة العامة Public Cloud Computing
- السحابة الهجينة Hybrid Cloud Computing

الأمن في الحوسبة السحابية

الأمن من قبل مزودي خدمة الحوسبة السحابية:

- أمن الشبكات: من خلال توفير HTTPS Access، جدار ناري مدمج، SSL/TLS
- التحكم في الوصول: مثل طلب مصادقة في كل عملية والتوقيع عليه رقميا باستخدم دالة تشفير، توفير أداة IMA للتحكم في مستويات الوصول، وإمكانية إعطاء الصلاحيات المؤقته
- المتابعة والتسجيل: من خلال سجلات الأمان، مراقبة الموارد وأدائها، التحديد الآلي للثغرات الأمنية
- النسخ الاحتياطي: من خلال تقديمة بشكل آلي
- تشفير البيانات: وجود لوائح أمنية للتشفير يجيب على العميل استخدامها

التحكم في الوصول

وهو عبارة عن إجراءات وقوانين تتخذ للحفاظ على سلامة الموارد في النظام أو الشبكة، مثل السماح لبعض المستخدمين للوصول لبيانات معينة وعدم السماح لمستخدم آخر من الوصول إليها.

مصطلحات التحكم في الوصول:

- الهوية Identification وهي عبارة عن رموز أو أرقام أو شهادة تثبت الهوية، مثل أوراق اعتمادية لإثبات الهوية.
- التحقق من الهوية أو المصادقة Authentication وهو عملية التحقق من هوية المستخدم والمصادقة على صحة ما يثبت هويته واعتمادها.
- الترخيص والتفويض Authorization إعطاء الإذن والسماح للمستخدم المثبتة هويته بإكمال المهمة المراد عملها.
- الوصول Access ويمنح المستخدم الوصول أو العبور لإنجاز مهمته.

أنواع التحكم في الوصول

١- التحكم في الوصول منطقياً

يمكننا تحقيق التحكم في الوصول بشكل منطقي عن طريق قائمة التحكم في الوصول وقيود الحسابات

- **قائمة التحكم في الوصول ACL** هي قائمة بالصلاحيات المخصصة للفاعل subject للقيام بعمليات محددة operation على المفعول به object.

٢- التحكم في الوصول فيزيائياً

نماذج التحكم في الوصول

- إلزامية MAC
- تقديرية DAC
- مبينة على قواعد ثابته R-BAC
- مبنية على قوانين ديناميكية RB-BAC

المصادقة وطرق تحقيق المصادقة

- ماذا تعلم؟ (كلمة المرور)
- ماذا لديك؟ (جهاز الشفرة الرقمية / البطاقة الذكية)
- من انت؟ (معياري / سلوكي)

التحكم بالوصول

حالة دراسية:

علي يعمل محقق في هيئة التحقيق والإدعاء العام، كان قد حقق علي في جريمة قتل واستند في تلك القضية على أدلة كسلاح الجريمة وعليه بصمات القاتل، لباس المجرم وعليه بقع من دماء القتيل.الخ. بعد أسابيع من إصدار الحكم، قرر المتهم هو ومحاميه الطعن في الحكم وطلب إعادة المحاكمة. بطبيعة الحال رفع طلب إعادة المحاكمة وجهز فريق تحقيق وقاضي جديد. فكر فريق التحقيق الجديد بالتحقق من الأدلة مجددًا، فاتجه الفريق لغرفة الأدلة الجنائية. كانت الصدمة أن الرقم المرجعي للدليل كان يعود لشيء يبعد كل البعد عن الأدلة في القضية! حينها رفع محضر للتحقيق مع المحققين الصرح لهم بالدخول إلى غرفة الأدلة الجنائية لمعرفة ماحصل، وانتهى ذلك المحضر بلا فائدة مرجوة أو دليل إدانة سواءً للمحققين أو المجرم. فكاميرات المراقبة قد أظهرت دخول وخروج العديد من المحققين لبوابة غرفة الأدلة، لكن جميع ردودهم كانت تبرر أن ذلك كان لتفحص أدلة في قضايا أخرى. لم تستطع الهيئة حينها اتخاذ أي إجراء. لكنها قررت تدعيم المستوى الأمني المادي لغرفة الأدلة الجنائية.

❖**صمم أنت ومجموعة من زملائك نظامًا أمنياً ماديًا متكاملاً لحماية الأدلة.**

إدارة المخاطر، وتقييم، والتخفيف من آثارها

تعريف إدارة المخاطر :

هو منهج منظم وهيكلي لإدارة احتمال الخسائر المتعلقة بما هو يشكل تهديداً. هذه التهديدات قد تكون من قبل المهاجمين، البيئة، خلل في التقنية أو عوامل اخرى. فإن هدف إدارة المخاطر هي التقليل من مخاطر التي قد تصيب الممتلكات.

خطوات إدارة المخاطر:

١- تعريف الممتلكات

٢- تعريف التهديد

٣- تقييم الثغرات

٤- تقييم المخاطر

٥- تخفيف المخاطر

إدارة المخاطر

- **حالة دراسية:**

قررت شركة (م. ن. م) للتقنية ومقرها في الولاية الأمريكية واشنطن، بافتتاح فرع جديد للشركة في ولاية ألاباما لحاجة العمل الملحة. لكن هذه الولاية قد عُرفت بكثرة الأعاصير المدمرة. فكلف مدير الشركة قسم إدارة المخاطر بوضع خطة متكاملة لإدارة المخاطر في حال افتتح الفرع.

❖من خلال ماتعلمته في جزئية إدارة المخاطر، قم أنت ومجموعة من زملائك بتشكيل الخطة الإدارية لهذه الشركة من خلال الخطوات المتخذة لإدارة المخاطر.

تحديد الثغرات

- البحث عن الثغرات
- مسح المنافذ
- مخططون الشبكات Network Mappers مثل Nmap
- محلل البروتوكولات Protocol Analyzer
- ماسحات الثغرات مثل IronWSAP
- كسر كلمات السر
- اختبار الإختراق

التحكم بالمخاطر البيئية

- **المخاطر البيئية:**

١- الحرارة العالية

٢- الغبار

٣- المجال المغناطيسي

٤- تذبذب الطاقة

٥- عوامل التآكل

النسخ الإحتياطي وإسترداد البيانات

- النسخ الإحتياطي
  - النسخ الإحتياطي التزايدي
  - النسخ الإحتياطي المتغير

تطبيق عملي:

- تطبيق النسخ الاحتياطي على نظام ويندوز ٨
- استعادة الملفات المحذوفة باستخدام برنامج Recuva

المراجع:

[١] ذيب بن عايض القحطاني:"المدخل إلى أمن المعلومات"، مطابع الحميضي، السعودية، الرياض. ٢٠١٢.

[٢] لورنس م. أوليفا: "أمن تقنية المعلومات"، المنظمة العربية للترجمة لبنان، بيروت. ٢٠١١.

[٣] Ciampa, Mark D. Security + Guide to Network Security Fundamentals. Boston N.p., 2012. Print

[٤] Kim, David , and Michael G.Solomon. Fundamentals of Information System Security. Burlington: Jones & Bartlett Learning, 2014. Print.

[٥] Vacca, John R. Cyber Security and IT Infrastructure Protection. Amsterdam: Syngress, 2013. Print.