**الفيروسات آمن المعلومات**

يعني أمن المعلومات إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص آخر دون إذن منك، وان تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى معلوماتك الخاصة.
أنت بالتأكيد لا ترغب أن يكون للآخرين مدخلاً لمعلوماتك الخاصة. ومن الواضح أن معظم الأشخاص يرغبون في الحفاظ على خصوصية معلوماتهم الحساسة مثل كلمات المرور ومعلومات البطاقة الائتمانية وعدم تمكن الآخرين من الوصول إليها، والكثير من الأشخاص لا يدركون بأن بعض المعلومات التي قد تبدو تافهة أو لا معنى لها بالنسبة لهم فإنها قد تعني الكثير لأناس آخرين وخصوصاً إذا ما تم تجميعها مع أجزاء أخرى من المعلومات. فعلى سبيل المثال، يمكن للشركة الراغبة في الحصول على معلومات شخصية عنك للأغراض التسويقية أن تشتري هذه المعلومات من شخص يقوم بتجميعها من خلال الوصول إلى جهاز كمبيوترك بشكل غير شرعي.
ومن المهم كذلك أن تفهم أنك حتى ولو لم تقم بإعطاء معلوماتك لأي شخص عبر الإنترنت، فقد يتمكن بعض الأشخاص من الوصول إلى نظام الكمبيوتر لديك للحصول على المعلومات التي يحتاجونها دون علم أو إذن منك.

**ماهية فيروسات الحاسب:**

الفيروس في حقيقته هو برنامج من برامج الحاسب ولكن تم تصميمه بهدف إلحاق الضرر بنظام الحاسب , وحتى يتحقق ذلك يلزم ان تكون لهذا البرنامج القدرة على ربط نفسه بالبرامج الأخرى وكذلك القدرة على إعادة تكرار نفسه بحيث يتوالد ويتكاثر مما يتيح له فرصة الإنتشار داخل جهاز الحاسب في أكثر من مكان في الذاكرة ليدمر البرامج والبيانات الموجودة في ذاكرة الجهاز.
وتكمن خطورة الفيروس في أنه مثله مثل الفيروس الذي يصيب الجسم الإنساني قادر على الانتقال من جهاز إلى آخر بسرعة كبيرة والسبب في ذلك التقدم الكبير الذي وصلت إليه وسائل الاتصال وشبكات الحاسب مما أدى الى سهولة الاتصال بين أجهزة الحاسب والتي ربما تكون في قارات متباعدة , كما أدى توافق نظم التشغيل واتباعها للمعايير الى زيادة انتشار الفيروسات حيث يستطيع البرنامج الواحد الآن أن يعمل على انواع مختلفة من الحاسبات ونسخ مختلفة من نظم التشغيل, والعامل الثالث الذي أدى الى زيادة انتشار الفيروسات هو قرصنة البرامح التي جعلت نسخ البرامج غير الأصلية موضع التداول بين الكثير من الأجهزة , مما أوجد ثغرة كبيرة تنفذ من خلالها البرامج الملوثة بالفيروسات.
أنواع الفيروسات
تأخذ الفيروسات أشكالا عديدة فقد تشبه الدودة في توالدها وتكاثرها , وقد يتم إدخالها الى النظام لتحدث التخريب المطلوب في توقيت معين أو عند حدوث واقعة معينة. وفيما يلي بعض أشكال الفيروسات :
حصان طراودة:(esroH najorT)
هو جزء صغير من الكود يضاف الى البرمجيات ولا يخدم الوظائف العادية التي صممت من أجلها هذه البرمجيات ولكنه يؤدي عملا تخريبيا للنظام , وتكمن خطورته في أن النظام لا يشعر بوجوده حتى تحين اللحظة المحددة له ليؤدي دوره التخريبي.
**القنابل المنطقية**
(sbmoB cigoL) القنبلة المنطقية هي أحد أنواع حصان طراودة وتصمم بحيث تعمل عند حدوث ظروف معينة أو لدى تنفيذ أمر معين, فقد تصمم بحيث تعمل عند بلوغ عدد الموظفين في الشركة عددا معينا من الموظفين مثلا أو إذا تم رفع إسم المخرب (واضع القنبلة) من كشوف الراتب, وتؤدي القنبلة في هذه الحالة الى تخريب بعض النظم او الى مسح بعض البيانات أو تعطيل النظام عن العمل.
**القنابل الموقوتة**
(sbmoB emiT) القنبلة الموقوته هي نوع خاص من القنابل المنطقية وهي تعمل في ساعة محددة أو في يوم معين كأن تحدث مثلا عندما يوافق اليوم الثالث عشر من الشهر يوم الجمعة.
**باب المصيدة(roodparT)**
هذا الكود يوضع عمدا بحيث يتم- لدى حدوث ظرف معين - تجاوز نظم الحماية والأمن في النظام . ويتم زرع هذا الكود عند تركيب النظام بحيث يعطي المخرب حرية تحديد الوقت الذي يشاء لتخريب النظام فهو يظل كامننا غير مؤذ حتى يقرر المخرب استخدامه , وكمثال على ذلك إقحام كود في في نظام الحماية والأمن يتعرف على شخصية المخرب ويفتح له الابواب دون إجراء الفحوص المعتادة.
**الديدان(smroW)**
الدودة هي عبارة عن كود يسبب أذى للنظام عند استدعائه, وتتميز الدودة بقدرتها على إعادة توليد نفسها , بمعنى أن أي ملف أو جهاز متصل بالشبكة تصل إليه الدودة يتلوث , وتنتقل هذه الدودة إلى ملف آخر أو جهاز آخر في الشبكة وهكذا تنتشر الدودة وتتوالد.
**كيفية عمل الفيروسات**
يقوم من أنشأ أو برمج الفيروس ببرمجة الفيروس ( توجيه الأوامر له) حيث يقوم بتحديد الزمان ومتى يبدأ الفيروس بالنشاط , وعادة ماتعطى فرصة كافية من الوقت حتى يضمن حرية الانتشار دون أن يلفت الانتباه ليتمكن من إصابة أكبر عدد ممكن من الملفات في النظام, تختلف الفيروسات من حيث بدأ المستخدمين والنشاط, فهنالك من يبدأ بتاريخ أو وقت محدد , وهنالك من يبدأالعمل بنشاط بعد تنفيذ آمر معين في البرنامج بالانتشار بعد التكاثر المصاب وهناك بعض من الفيروسات يبدأ بالوصول الى رقم معين من النسخ ثم يقوم بدوره التخريبي.
يقوم الفيروس بعدة أنشطة تخريبية حسب الغرض من إنشاء ذلك الفيروس فهناك ما يقوم بعرض رسالة تحذيرية عن امتلاء الذاكرة أو رسالة تستخف بالمستخدم وهناك أنواع أخرى تقوم بحذف أو تعديل بعض ملفات جهازك وهناك من يقوم بتكرار ونسخ نفسه حتى يشل تماما وهناك أنواع أشد فتكا فتقوم بمسح كل المعلومات من قرصك الصلب .
**طرق الوقاية من الفيروسات**
هناك عدة إجراءات وقائية يعفي تطبيقها المؤسسة من كثير من العواقب الوخيمة التي قد تترتب على الإصابة بالفيروسات مثل:
1- تجهيز عدة نسخ من البرمجيات وحفظها بحيث يمكن استرجاع نسخة نظيفة (غير ملوثة بالفيروس) من البرنامج عند الحاجة.
2- الاحتفاظ بسجل لكل عمليات التعديل في برامج التطبيقات بحيث يتم تسجيل جميع وقائع نقل البرامج المعدلة إلى البيئة الإنتاجية , وبخاصة تلك البرامج المجلوبة من خارج المؤسسة.
3- يجب توعية المستخدمين بعدم تحميل أي برنامج مجلوب من الخارج في حاسباتهم الشخصية, فهذا هو أوسع الأبواب لإدخال الفيروسات إلى النظم والتي عند دخولها ربما تصيب جميع الأقراص وجميع الأجهزة بالشبكة.
والبرامج المجانية التي تنتقل من يد إلى يد أو يتم توزيعها بواسطة مجلات الكمبيوتر المتخصصة يجب دائما الحذر في التعامل معها. حتى تلك البرامج التي تأتي من مصادر لا يرقى إليها الشك يجب فحصها جيدا.
4- عند فحص البرمجيات أو اختبارها قبل السماح بنشرها في المؤسسة للاستخدام العام , يجب ان يتم ذلك على جهاز مستقل غير مرتبط بالشبكة . ويجب أن يتضمن الاختبار البحث عن أي سلوك غير مفهوم في البرنامج كأن يخرج رسائل لا داعي لها على الشاشة مثلا , ولو أن خلو البرنامج من مثل هذا السلوك غير المفهوم لا يعني بالضرورة نظافة البرنامج فالفيروسات تظل كامنة ولا تكشف عن سلوكها إلا في اللحظة المناسبة.
5- تركيب برنامج للتحقق من وجود فيروسات ويفضل ان يكون هذا البرنامج دائم الوجود في الذاكرة , وهذه البرامج تقوم بالتأكد من عدم وجود الفيروسات المعروفة لها, ولذلك فهي تكون عديمة الفائدة في مواجهة الفيروسات الجديدة, وبعض هذه البرامج يقوم بمقارنة محتويات بعض مناطق القرص (الصلب او اللين) أو بعض مناطق الذاكرة بمحتوياتها المتوقعة والمفترض أن توجد بها والإبلاغ عن أي تغيير فيها مما قد ينبئ عن وجود فيروس.
6- ويجب عدم إجازة البرامج للاستخدام العام في المؤسسة إلا بعد اجتيازها بنجاح هذه الاختبارات.
نصائح للمستخدم من أجل تأمين الكمبيوتر الشخصي
1- احتفظ بنسخة احتياطية من البرامج والبيانات مأخوذة على فترات متقاربة.
2- احتفظ بهذه النسخ في مكان آمن بعيدا عن الحاسب الشخصي.
3- احتفظ بسرية كلمة المرور وقم بتغييرها من وقت لآخر.
4- لا تترك البيانات معروضة على الشاشة وتغادر المكان.
5- اغلق الجهاز قبل أن تترك مكانك أمامه.
6- احتفظ لديك بالرقم المتسلسل للجهاز وللقرص الصلب.
7- لا تقم بتحميل أي بيانات شخصية دون التنسيق مع مسؤل أمن المعلومات.
8- عند حدوث مشكلة اتصل فورا بمسؤل مساندة المستفيدين.
9- ضع شريط الحماية أو اغلق فتحة التأمين للأقراص المرنة بعد الانتهاء من استخدامها لمنع الكتابة عليها بشكل غير مقصود.

**مواطن الضعف في شبكة الإنترنت**

تعتبر شبكة الإنترنت عرضة للعيوب والضعف في دفاعاتها. وقد يكون هذا الضعف ناجما عن الأخطاء البرمجية والعيوب في تصميم النظام. ويعود سبب بعض نقاط الضعف إلى الإدخال الخاطئ للبيانات، حيث أن غالبا ما يسمح بتنفيذ الأوامر المباشرة أو عبارات لغة SQL. وأحيانا يخفق المبرمج في التحقق من حجم البيانات المخزنة، حيث يؤدي ذلك إلى فيض من البيانات والذي يسبب فساد المكدس أو مناطق الشجرة الثنائية في الذاكرة.
وغالبا ما تتيح مواطن الضعف للمهاجم إمكانية التحايل على البرنامج بتجاوز فحص إمكانية الوصول أو تنفيذ الأوامر على النظام المضيف لهذا البرنامج.
هناك عدد من نقاط الضعف والتي يكون جهازك أو شبكتك عرضة لها. ومن أكثرها شيوعا هي أخطاء تدقيق صحة إدخال البيانات مثل الأخطاء البرمجية الناجمة عن تنسيق الرموز النصية، والتعامل الخاطئ مع الرموز المتغيرة لغلاف البرنامج ولذلك يتم تفسير هذه الرموز، وإدخال عبارات SQL وتضمين النصوص البرمجية متعارضة-الموقع داخل تطبيقات الويب. ومن نقاط الضعف الشائعة أيضا تحطم المكدس وفيض البيانات في ذاكرة التخزين المؤقت بالإضافة إلى ملفات الروابط الرمزية (Symlinks).

## المشاكل الأمنية

تحدث المشكلة الأمنية عندما يتم اختراق النظام لديك من خلال أحد المهاجمين أو المتسللين (الهاكر) أو الفيروسات أو نوع آخر من أنواع البرامج الخبيثة.
وأكثر الناس المستهدفين في الاختراقات الأمنية هم الأشخاص الذي يقومون بتصفح الإنترنت، حيث يتسبب الاختراق في مشاكل مزعجة مثل تبطئ حركة التصفح وانقطاعه على فترات منتظمة. ويمكن أن يتعذر الدخول إلى البيانات وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم.
وفي حالة وجود أخطاء برمجة أو إعدادات خاطئة في خادم الويب، فمن الجائز أن تسمح بدخول المستخدمين عن بعد غير المصرح لهم إلى الوثائق السرية المحتوية على معلومات شخصية أو الحصول على معلومات حول الجهاز المضيف للخادم مما يسمح بحدوث اختراق للنظام. كما يمكن لهؤلاء الأشخاص تنفيذ أوامر على جهاز الخادم المضيف مما يمكنهم تعديل النظام وإطلاق هجمات إغراقية مما يؤدي إلى تعطل الجهاز مؤقتاً، كما أن الهجمات الإغراقية (DoS) تستهدف إبطا او شل حركة مرور البيانات عبر الشبكة. كما أنه من خلال الهجمات الإغراقية الموزعة (DDoS)، فإن المعتدي يقوم باستخدام عدد من الكمبيوترات التي سيطر عليها للهجوم على كمبيوتر أو كمبيوترات أخرى. ويتم تركيب البرنامج الرئيسي للهجمات الإغراقية الموزعة (DDoS) في أحد أجهزة الكمبيوتر مستخدماً حساباً مسروقاً.
إن التجسس على بيانات الشبكة واعتراض المعلومات التي تنتقل بين الخادم والمستعرض يمكن أن يصبح أمراً ممكناً إذا تركت الشبكة أو الخوادم مفتوحة ونقاط ضعفها مكشوفة.

## الهاكر

الهاكر هو الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي. وقد أصبح هذا المصطلح ذا مغزى سلبي حيث صار يطلق على الشخص الذي يقوم باستغلال النظام من خلال الحصول على دخول غير مصرح به للأنظمة والقيام بعمليات غير مرغوب فيها وغير مشروعة. غير أن هذا المصطلح (هاكر) يمكن أن يطلق على الشخص الذي يستخدم مهاراته لتطوير برمجيات الكمبيوتر وإدارة أنظمة الكمبيوتر وما يتعلق بأمن الكمبيوتر.

## فيروسات الكمبيوتر

فيروسات الكمبيوتر هي الأكثر شيوعاً من بين مشاكل أمن المعلومات التي يتعرض لها الأشخاص والشركات. وفيروس الكمبيوتر هو برنامج غير مرغوب فيه ويدخل إلى الجهاز دون إذن ويقوم بإدخال نسخ من نفسه في برامج الكمبيوتر، والفيروس هو أحد البرامج الخبيثة أو المتطفلة. والبرامج المتطفلة الأخرى تسمى الديدان أو أحصنة طروادة أو برامج الدعاية أو برامج التجسس.
يمكن للبرامج الخبيثة أن تكون فقط للإزعاج من خلال التأثير على استخدامات الكمبيوتر وتبطئيه وتتسبب في حدوث انقطاعات وأعطال في أوقات منتظمة وتؤثر على البرامج والوثائق المختلفة التي قد يرغب المستخدم في الدخول إليها. أما البرامج الخبيثة الأكثر خطورة فيمكن أن تصبح مشكلة أمنية من خلال الحصول على معلوماتك الشخصية من رسائلك الإلكترونية والبيانات الأخرى المخزنة في جهازك.
أما بالنسبة لبرامج الدعاية وبرامج التجسس فهي مزعجة في الغالب وتؤدي إلى ظهور نوافذ دعائية منبثقة على الشاشة. كما أن برامج التجسس تجمع معلوماتك الشخصية وتقدمها إلى جهات أخرى تطلب الحصول عليها لأغراض تجارية.
يمكنك حماية كمبيوترك وحماية نفسك باستخدام برامج مناسبة لمكافحة البرامج الخبيثة غير المرغوب فيها والتي قد تكون نتائجها مدمرة.

## اللصوصية (Phishing)

يستخدم مصطلح (Phishing) للتعبير عن سرقة الهوية، وهو عمل إجرامي، حيث يقوم شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني مدعياً أنه من شركة نظامية ويطلب الحصول من مستلم الرسالة على المعلومات الشخصية مثل تفاصيل الحسابات البنكية وكلمات المرور وتفاصيل البطاقة الائتمانية. وتستخدم المعلومات للدخول إلى الحسابات البنكية عبر الإنترنت والدخول إلى مواقع الشركات التي تطلب البيانات الشخصية للدخول الى الموقع.
هناك برامج لمكافحة اللصوصية Phishing والكشف عن هوية المرسل الحقيقي، وأفضل وسيلة لحماية الشخص من نشر معلوماته الشخصية لمن يطلبها هو أن يكون الشخص متيقظاً وحذراً ولديه الوعي الكافي، فلا يوجد هناك أي بنك معروف أو مؤسسة فعلية يطلبون من عملائهم إرسال معلوماتهم الشخصية عبر البريد الإلكتروني.

## البريد الإلكتروني

يجدر بنا أن نتذكر دائماً إلى أن البريد الإلكتروني لا يضمن الخصوصية، فخصوصيته تشابه خصوصية البطاقة البريدية. ويتنقل البريد الإلكتروني في طريقه إلى المستلم عبر العديد من الخوادم حيث يمكن الوصول إليه من قبل الأشخاص الذين يديرون النظام ومن الأشخاص الذين يتسللون إليه بشكل غير نظامي. والطريقة الوحيدة للتأكد إلى حد ما من خصوصية بريدك الإلكتروني هو تشفيره. انظر الفقرات التالية..

##     كيف تحمي شبكتك ونظامك

عليك بالحذر والحرص الدائمين لحماية نظامك كي لا يكون عرضة للهجمات بسبب نقاط الضعف فيه، ويمكنك تركيب برامج فعالة لجعل استخدام الإنترنت أكثر أماناً لك.

### وسائل الحماية المادية

سنستعرض في الفقرات التالية المزيد من المعلومات حول البرمجيات المختلفة والوسائل المتعلقة بالأنظمة الأخرى للإبقاء على معلوماتك آمنة، لكن علينا أن نتذكر أن ثمة العديد من الطرق الأخرى التي يسلكها المتسللون للوصول إلى معلوماتك. ضع كمبيوترك وخصوصاً الكمبيوتر المحمول دائماً في مكان آمن. قم بحماية كمبيوترك بكلمة مرور ويستحسن أن تطفئه وأنت بعيداً عنه. عليك أن تشك في أي شخص يرغب في الحصول على أي من كلمات المرور الخاصة بك، حتى أولئك الأشخاص الذي يعملون (أو يدعون بأنهم يعملون) في الدعم الفني في شركتك. فإن أرادوا الحصول على كلمة المرور الخاصة بك، قم أنت بطباعتها (إدخالها) بنفسك (بحيث لا يرونها) ولا تبلغها لهم شفوياً أو خطيا. قم بانتظام بتغيير كلمة المرور إذا تصادف أن اطلع عليها أحد غيرك، أو حتى إذا شعرت أن أحد ما تمكن من الوصول إليها. ولا تكتب كلمات المرور الخاصة بك في أي مكان ولكن عليك أن تتذكرها بنفسك.

### التحديثات

حافظ على تحديث جميع برامجك بما في ذلك أحدث نسخة من برنامج التشغيل الذي تستخدمه. وإذا كنت تستخدم التحديث التلقائي الذي يقوم بالبحث يومياً عن التحديثات عند بدء تشغيل الجهاز، فعليك إعادة تشغيل جهازك يومياً.

### جدار النار (Firewall)

يكون جدار الحماية الناري إما برنامجاً أو جهازاً يستخدم لحماية الشبكة والخادم من المتسللين. وتختلف جدران النار حسب احتياجات المستخدم. فإذا استدعت الحاجة إلى وضع جدار النار على عقدة منفردة عاملة على شبكة واحدة فإن جدار النار الشخصي هو الخيار المناسب. وفي حالة وجود حركة مرور داخلة وخارجة من عدد من الشبكات، فيتم استخدام مصافي لجدار النار في الشبكة لتصفية جميع الحركة المرورية. علماً بأن الكثير من الشبكات والخوادم تأتي مع نظام جدار نار افتراضي، ولكن ينبغي التأكد فيما إذا كان يقوم بعمل تصفية فعالة لجميع الأشياء التي تحتاج إليها، فإن لم يكن قادراً على ذلك، فينبغي شراء جدار حماية ناري أقوى منه.

### برامج مراقبة بيانات الشبكة Packet Sniffers

طريقة فعالة لمراقبة الحركة المرورية عبر الشبكة باستخدام أحد برامج مراقبة بيانات الشبكة، حيث يتم من خلاله تجميع البيانات الداخلة والخارجة، وهي طريقة ممكن أن تكون مفيدة في الكشف عن محاولات التسلل عبر الشبكة، وكذلك يمكن استخدامها لتحليل مشاكل الشبكة وتصفية وحجب المحتوى المشكوك فيه من الدخول إلى الشبكة.

### التشفير

التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس. ويجعل التشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن.

## أمن الشبكة اللاسلكية

تنتشر الشبكات اللاسلكية في كل مكان وتنمو بشكل غير طبيعي ولا توجد دلالات على توقف ذلك النمو على المستوى المنظور. وهناك العديد من القضايا الأمنية المصاحبة لهذه الشبكات اللاسلكية، كما أن بإمكان أي شخص الوصول إلى الشبكة اللاسلكية من أي مكان تتوفر فيه الوصلة اللاسلكية. وبالإضافة إلى التدابير الأمنية العامة المتبعة لحماية الشبكات اللاسلكية، فإنه من الضروري اتباع المبادئ العامة البسيطة لتوفير أفضل مستوى من الأمن لشبكتك اللاسلكية.

## التشفير

يتم حماية الشبكة اللاسلكية باستخدام بروتوكول تشفير الشبكات اللاسلكية (WEP). ويعمل هذا البروتوكول بتضمين مفتاح مشترك 64 أو 128 بت بين العملاء ونقطة الدخول، ومن ثم يتم استخدام هذا المفتاح لتشفير وفك تشفير البيانات بينهم، وهذا يوفر قدر كاف من الأمن للشبكات المنزلية. عليك الرجوع إلى الوثائق الخاصة بالأجهزة اللاسلكية لديك لتعرف كيفية تمكين وإعداد بروتوكول التشفير اللاسلكي (WEP) على شبكتك. أما بالنسبة لبيئات الشركات، فيجب اعتبار هذا البروتوكول (WEP) فقط كنقطة بداية للترتيبات الأمنية، وعلى الشركات البحث جدياً في ترقية شبكاتهم اللاسلكية إلى مستوى (WPA) أكثر أماناً.

## التعريف

يكون للأجهزة ومديرو الشبكات أسماء تعريف افتراضية في النظام، ومن السهل كثيراً على الهاكر إيجاد هذه الأسماء، ومن ثم عمل كلمات مرور واسم مستخدم شخصي لك من خلال تعديل أسماء التعريف الافتراضية في النظام. لذا ننصح بإعطاء الأجهزة لديك أسماء لا تكشف عن هوية صاحبها أو أماكنها، ومثال ذلك بدلاً من استخدام عنوانك الفعلي مثل اسم المبنى أو اسم الشركة كأسماء لأجهزتك، يمكنك استخدام أسماء مختلفة مثل "الجبل Mountain" أو "جهازي My Device".

## فحص مواطن الضعف

يمكن أن تكون هناك نقاط ضعف في جميع أنظمة التشغيل مثل الويندوز، ماكنتوش، لينوكس، OpenVMS، وغيرها. ويمكن فحص نقاط الضعف في الشبكة والخوادم من خلال إجراء اختبار خاص عليها يتم من خلاله فحص الخوادم والصفحات الإلكترونية وجدران النار وغير ذلك لمعرفة مدى تعرضها لنقاط الضعف. ويمكن تنزيل برامج فحص نقاط الضعف من الإنترنت.