يعتقد بعض المستخدمين للشبكة العنكبوتية أن الوصول لحالة من الأمان تبعدهم عن أعين الفضوليين يعتبر أمرا صعب المنال ولكن هذا غير حقيقي فالأمان على الإنترنت سهل كسهولة شرب كأس من الماء.

ولتبسيط الفكرة على عزيزنا القارىء نوضح حقيقة الأمان وكيف يمكن انتهاك حرمة المستخدم على الشبكة.عند اتصال جهاز حاسب آلي بالإنترنت أو بأي شبكة أخرى فإن ذلك يعني فتح حوالي65 ألف منفذ Port على تلك الشبكة وهناك نوعان من المنافذ وهما UDP و TCPولكن لا تهتم فهذا التقسيم لا يهمك بأي حال من الأحوال ولكن ما يهمك هو معرفة ما هو المتصل من هذه المنافذ وما هو المغلق ولا يحتوي على اتصال.

عندما يكون منفذا متصلا بالإنترنت فهذا يعني أنه مفتوح وهنا يكمن الخطر فعند وجود أحد المنافذ مفتوحا فهذا يتيح لأعين الفضوليين على الشبكة مراقبة ومعرفة تحركات صاحبه وفي بعض الأحيان اختراقه.

إن وجود أحد المنافذ مفتوحا تختلف خطورته من منفذ لآخر وعلى أقل الأحوال قد يعطي هذا المنفذ معلومات عن شخصيتك أو معلومات عن جهازك واسمه كما يحدث مع منفذ Netbios والذي غالبا ما يكون مفتوحا على الأجهزة التي تعمل بنظام ويندوز.بعض المنافذ معروف عنه أنه خاص بملفات التجسس كمنفذي 1243 و 27374 الخاصين ببرنامج التجسس الشهير سب سفن أو منفذي 2140 و 3150 المعروفين بعملهما لبرنامج ديب ثروت للتجسس.

لسنا نريد إثارة هلع المستخدم والقارئ في زاوية هذا اليوم ولكننا نريد أن نوضح له الطريقة الأمثل للحفاظ على سريته في تجواله على الإنترنت.وكما قلنا سابقا فإن المنفذ المفتوح هو الطريق الرئيسي للنظام لذلك يجب تأمين جميع منافذ الجهاز والتأكد من عملها بشكل سليم وأنها لا تقوم بتسريب أو إتاحةالفرصة للآخرين لكسر حاجز السرية الذي يتمتع به المستخدم في الإنترنت ويجب التنويه بشدة إلى أن أي برنامج يقوم المستخدم بتثبيته وتفعيله للعمل من خلال شبكة الإنترنت فإن هذا البرنامج يقوم بشكل مباشر بفتح أحد المنافذ لكي يتمكن من الاتصال بالنت وعلى سبيل المثال فبرنامج إنترنت اكسبلورر يقوم بفتح المنفذالخاص ببروتوكول HTTP والمشهور أنه الخاص بتصفح المواقع وكذلك برنامج الماسنجروبرامج المحادثات CHAT وغيرها الكثير.

وبالتأكيد عند دخول ملف التجسس والمعروف بسيرفر Server أو باتش Patch لجهازك فإنه يقوم بفتح منفذ يستطيع من خلاله المهاجمون من الدخول لجهازك ويقوم هذاالملف دائما بتحميل نفسه مع بداية عمل الجهاز من وضع الإيقاف لكي يكون موجودا في قائمة عمل الجهاز دائما وأبدا.أعتقد أنك استنتجت مما سبق أن تأمين جهاز ما متصل بشبكة يبدأ عند إقفال المنافذ المتصلة بتلك الشبكة وبفضل شبكة الإنترنت يمكنك الآن التأكد من منافذ جهازك المتصلة بالإنترنت بكل سهولة فكل ما عليك فعله هو الذهاب لأحد المواقع المتخصصة بهذا المجال ويمكنني أن أرشدك لإحداها والذي يتخصص بقياس مدى سرية وقوة جهازك على الشبكة من ناحية المنافذ وهو على العنوان التالي:http// www.grc.com فهذا الموقع كما يظهر من صفحته الرئيسية قام باختبار قوة «الدروع» الخاصة بالأجهزة حوالي 917.911.8 مرة أما البرنامج الذي يمكنك عن طريقه اختبار قوةومتانة دروعك فهو Shields Up وعند الضغط عليه فإنه يقوم بتحميل برنامج صغيربجهازك لكي يتواصل من خلاله مع الموقع ليتسنى له إجراء الاختبار وعندما يكتمل التحميل وبعد تشغيل هذا البريمج تضغط على الزر الوحيد فيه وهو Test My Shields وعندها سينقلك إلى الصفحة الخاصة به في الموقع وهناك البدء بعملية الاختبارعند الضغط على الزر الواضح والمعنون باسم Test My Shields ! وبعدها سينقلك لصفحة تالية وستظهر عليها النتائج وسيعطيك تقريرا عن وضع دروع جهازك ولكن لا تقف هنا بل واصل العملية ففي نفس الصفحة يمكنك مواصلة عمليات الاختبارعن طريق الضغط على الزر الواضح في هذه الصفحة والمعنون ب PROP MY PORTS! والذي سيواصل العملية وسيبدأ في فحص منافذ الخدمات مثل منفذ FTP ومنفذTelnet و SMTP وغيرها وسيوضح لك النتائج أمام كل منفذ على حده وهل هو مغلق أم مفتوح.وبعد الحصول على هذه النتائج تقف أمام احتمالين أولهما أنك راض عن وضع دروعك على الشبكة )بحالة أن تكون جميعها مغلقة closed وتظهر أمامك الحالة تحت النتائج بعبارة Stealth( أو أن الاختبار اكتشف ضعف هذه المنافذ لديك وعليها يجب عليك مراجعة دروعك الإنترنتية والتي تبعد أعين الفضوليين عن الوقوع عليك ويجب عليك أخذ جولة لمعرفة محتويات الموقع ومنها خدمة تعرف باسم Test Leak وهي خاصة باختبار هل برنامج الحماية لديك يقوم بتسريب أي معلومات عن جهازك للمواقع أو المستخدمين وأنصحك بتجربتها وتجدها في الصفحة الرئيسية للموقع.

𝗠𝗮𝗹𝘄𝗮𝗿𝗲 𝗧𝗲𝗮𝗺, [3/21/2022 10:37 PM]

في حالة وجود أحد المنافذ مفتوحا فأول نصيحة تتلقاها هي تثبيت برنامج جدارناري في جهازك وكما نصحت سابقا من خلال هذه الزاوية ونصح غيري من كل المواقع الصحفية والإنترنتية والاجتماعية الأخرى فإنه عليك ببرنامج Alarm Zone فهذا البرنامج المطلب الجماهيري الشعبي الأول على شبكة الإنترنت لغرض الحماية ويكفيك أنه يعتبر أساسيا للهاكرز الذين يمثلون الهاجس الأول المخيف للجميع على الشبكة فجميعهم تقريبا لا يستغنون عنه بأي حال من الأحوال.

ما سبق كان خاصا بمنافذ الخدمات الشهيرة فهذا الفحص لا يقوم بفحص جميع منافذ الجهازوالبالغ عددها حوالي 65 ألف كما ذكرنا سابقا ولكي تتأكد من جميع المنافذأنصحك بأحد برامج فحص المنافذ Scanner Port وإن كان اشهرها Sphere 7th ومن خلال هذا البرنامج يمكنك وضع العنوان الشبكي Address IP الخاص بك ومن ثم بدء عملية فحص المنافذ وسيأتيك البرنامج بأي منفذ يكون مفتوحا وعند معرفةرقم المنفذ يمكنك معرفة البرنامج المشتغل عليه بكل سهولة عن طريق الذهاب لأحد المواقع الأمنية المتخصصة.ويجب عليك أيضا تركيب أحد برامج مكافحة الفيروسات للتأكد من خلو الجهاز من جميع أنواع التروجانات وملفات التجسس والأبواب الخلفية والسكريبتات والخبيثة والتي يستطيع من خلالها المقتحمون للخصوصيات من الوصول للجهاز ويجب أن أنوهأن ليس جميع ملفات التجسس تقوم بفتح منافذ Port اتصال لها بل أن بعضها تقتصر مهمته على مراقبة الضغطات التي يقوم بها المستخدم على لوحة المفاتيح والمعروفةباسم strokes Key ويقوم بعد ذلك بتسجيلها في ملف خاص ليقوم بعد ذلك بإرسالها لصاحبه بواسطة البريد الإلكتروني على عنوان محدد مسبقا والبرامج هذه معروفة باسم loggers Key أو Password Stealers وبلغت خطورة بعض هذه البرامج في أنها تمتلك القدرة على تجنب برامج مكافحة الفيروسات وأشباهها ولهذا يجب تحديث Update برامج مكافحة الفيروسات بشكل مستمر لكي تستطيع التخلص منها دائما وأبدا ويمكن إجراء فحص ضد الفيروسات لجهاز من موقع شركة Micro Trendعلى الإنترنت والواقع تحت العنوان التالي:antivirus. com .www ومن ثم tools free وبعدها call house ومن ثم now scan وسيتم ربط جهازك بالخادم server الشركة المسؤول عن إجراء عمليات الفحص ضد الفيروسات وملفات التجسس .