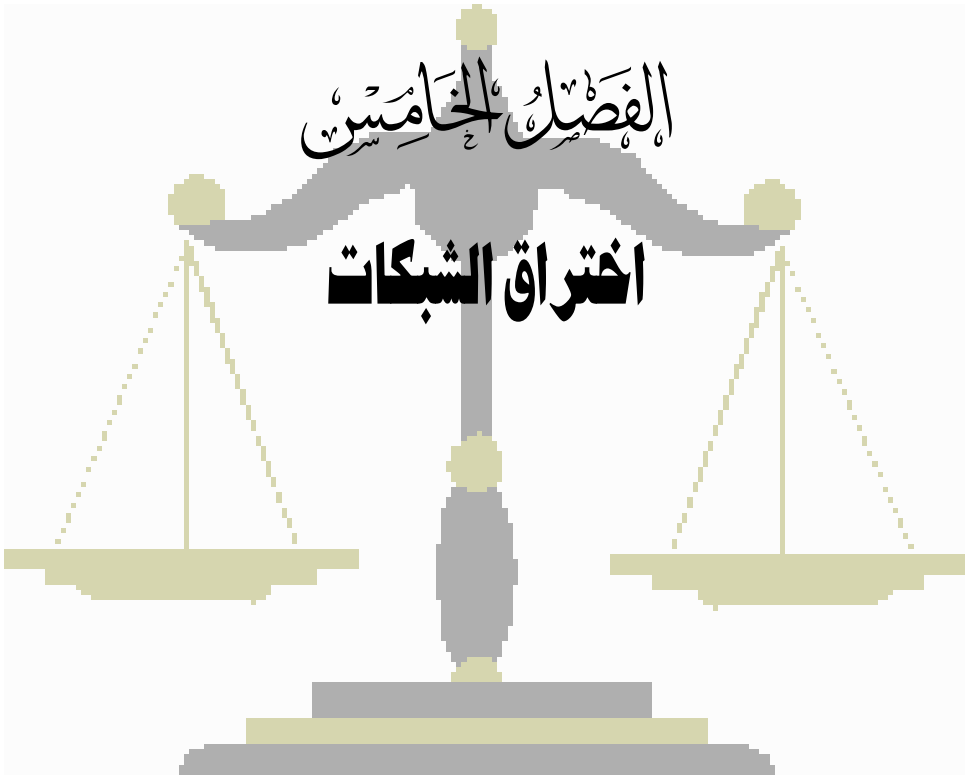

الفصل الخامس

اختراق الشبكات

الاختراق بشكل عام "هو القدرة على الوصول لهدف بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف" وحينما نتكلم عن الاختراق بشكل عام فنقصد بذلك القدرة المخترق على الدخول إلى جهاز شخص ما بغض النظر عن الأضرار التي قد يحدثها فحينما يستطيع الدخول إلى جهاز آخر فهو مخترق **Hacker** إما عندما يقوم بحذف ملف أو تشغيل آخر أو جلب ثالث فهو مخرب **Cracker** .

وهو الدخول على أجهزة الآخرين عنوة ودون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قدي حدثها سواء بأجهزتهم الشخصية أو بنفسيتهم عند سرية ملفات تخصهم وحدهم فما الفرق هنا بين المخترق للأجهزة الشخصية والمقتحم للبيوت الآمنة المطمئنة[1] .

أسباب الاختراق ودوافعه:

لم تنتشر هذه الظاهرة لمجرد العبث وان كان العبث وقضاء وقت الفراغ من ابرز العوامل التي ساعدت على تطورها وبروزها إلى عالم الوجود وقد أجمل المؤلفين الدوافع الرئيسية للاختراق في ثلاث نقاط على النحو التالي :

١. الدافع السياسي أو العسكري:

مما لاشك فيه أن التطور العلمي والفني أديا إلى الاعتماد بشكل شبه كامل على أنظمة الكمبيوتر في اغلب الاحيتاجات التقنية والمعلوماتية فمنذ الحرب الباردة

(١) موقع الجمعية المصرية لمكافحة جرائم الإنترنت والمعلومات محمد محمد الألفي اختراق الشبكات .

والصراع المعلوماتي والتجسس بين الدولتين العظمى على أشده ومع بروز مناطق جديدة للصراع في العالم وتغير الطبيعة المعلوماتية للأنظمة والدول أصبح الاعتماد كليا على الحاسب الآلي وعن طريقه أصبح الاختراق من اجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية .

٢ـ الدافع التجاري:

من المعروف أن الشركات التجارية الكبرى تعيش هي أيضا فيما بينها حربا مستعرة وقد بينت الدراسات الحديثة أن عدداً من كبريات الشركات التجارية يجرى علها أكثر من خمسين محاولة للاختراق لشبكاتها كل يوم .

٣ـ الدافع الفردي:

بدأت أولى محاولات الاختراق الفردي بين طلاب الجامعات في الولايات المتحدة كنوع من التباهي بالنجاح في اختراق الأجهزة شخصية لأصدقائهم ومعارفهم ما لبثت أن تحولت تلك الظاهرة إلى تحدى فيما بينهم في اختراق الأنظمة بالشركات ثم بمواقع الإنترنت ولا يقتصر الدافع على الأفراد فقط بل توجد مجموعات ونقابات أشبه ما تكون بالأندية وليست بذات أهداف تجارية.بعض الأفراد بشركات كبرى بالولايات المتحدة الأمريكية ممن كانوا يعملون مبرمجين ومحللي نظم تم تسريحهم من أعمالهم للفائض الزائد بالعمالة فصبوا جم غضبهم على أنظمة شركاتهم السابقة مقتحميها ومخربين لكل ما يقع عليه أيديهم من معلومات حساسة بقصد الانتقام .

أنواع الاختراق:

يمكن تقسيم الاختراق من حيث الطريقة المستخدمة إلى ثلاثة أنواع :

١ـ اختراق المزودات والأجهزة الرئيسية للشركات والمؤسسات أو الجهات الحكومية وذلك باختراق الجدران النارية التي عادة توضع لحمايتها وغالبا ما يتم ذلك باستخدام المحاكاة **Spoofing** وهو المصطلح الذي يطلق على عملية انتحال

شخصية للدخول إلى النظام حيث أن حزم الـ IP تحتوى على عناوين للمرسل والمرسل إليه وهذه العناوين ينظر إليها على أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة ومن خلال طريقة تعرف بمسارات المصدر Routing Source فإن حزم الـ IP قد تم إعطائها شكلا تبدو معه وكأنها قادمة من كمبيوتر معين بينما هي في حقيقة الأمر ليست قادمة منه وعلى ذلك فعن النظام إذا وثق بهوية عنوان مصدر الحزمة فإنه يكون بذلك قد حوكر (خدع) وهذه الطريقة في ذاتها التي نجح بها مخترقي الهوت ميل في الولوج إلى معلومات النظام قبل شهرين .

٢ـ اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات وهى طريقة للآسف شائعة لسذاجة أصحاب الأجهزة الشخصية من جانب ولسهولة تعلم برامج الاختراق وتعددها من جانب آخر .

٣ـ التعرض للبيانات أثناء انتقالها والتعرف على شفرتها أن كانت مشفرة وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكية ATMوفى هذا السياق نحذر هنا من أمرين لا يتم الاهتمام بهما بشكل جدي وهما عدم الكشف عن أرقام بطاقات الائتمان لمواقع التجارة الإلكترونية إلا بعد التأكد بالتزام تلك المواقع بمبدأ الأمان . أما الأمر الثاني فبقدر ما هو ذو أهمية أمنية عالية إلا انه لا يؤخذ مأخذ الجدية فالبعض عندما يستخدم بطاقات السحب الآلي من مكائن البنوك النقدية ATMلا ينظر خروج السند الصغير المرفق بعملية السحب أو انه يلقى به في اقرب سلة مهملات دون أن يكلف نفسه عناء تمزيقه جيداً . ولو نظرنا إلى ذلك المستند سنجد أرقاما تتكون من عدة خانات طويلة هي بالنسبة لنا ليست بذات أهمية ولكننا لو أدركنا بان تلك الأرقام ما هي في حقيقة الأمر إلا انعكاس للشريط الممغنط الظاهر بالجهة الخلفية لبطاقة ATMوهذا الشريط هو حلقة الوصل بيننا وبين رصيدنا بالبنك الذي من خلاله تتم عملية السحب النقدي لأدركنا أهمية التخلص من المستند الصغير بطريقة مضمونة ونقصد بالضمان هنا عدم تركها لهاكرز محترف يمكنه

استخراج رقم الحساب البنكي بل والتعرف على الأرقام السرية للبطاقة البنكية ATM .

آثار الاختراق:

١ـ تغيير الصفحة الرئيسية لموقع الويب كما حدث لموقع فلسطيني مختص بالقدس حيث غير بعض الشباب الإسرائيلي الصور الخاصة بالقدس إلى صور تتعلق بالديانة اليهودية بعد عملية اختراق مخطط لها .

٢ـ السطو على خدمات مادية أو أي معلومات ذات مكاسب مادية كأرقام بطاقات الائتمان والأرقام السرية الخاصة ببطاقات ATM .

٣ـ اقتناص كلمات السر التي يستخدمها الشخص للحصول على خدمات مختلفة كالدخول إلى الإنترنت حيث يلاحظ الضحية أن ساعاته تنتهي دون أن يستخدمها وكذلك انتحال شخصية في منتديات الحوار كما حدث للأخت الدانة بهذه الساحة . والآن وبعد هذه العجالة هل فكرتم بخطورة الاختراق ؟ هل خطر على أحدكم بأن جهازه قد اخترق ؟؟ وكيف له أن يعرف ذلك قبل أن يبدأ التخلص من ملفات التجسس ؟

ميكانيكية الاختراق:

يعتمد الاختراق على السيطرة عن بعد Remote وهى لا تتم إلا بوجود عاملين مهمين الأول البرنامج المسيطر ويعرف بالعميل Client والثاني الخادم Serverالذي يقوم بتسهيل عملية الاختراق ذاتها .

وبعبارة أخرى لابد من توفر برنامج على كل من جهازي المخترق والضحية ففي جهاز الضحية يوجد برنامج الخادم وفى جهاز المخترق يوجد برنامج العميل . تختلف طرق اختراق الأجهزة والنظم باختلاف وسائل الاختراق ، ولكنها جميعا تعتمد على فكرة توفر اتصال عن بعد جهازي الضحية والذي يزرع به الخادم (server) الخاص بالمخترق ، وجهاز المخترق على الطرف الآخر حيث يوجد برنامج المستفيد أو

العميل : **Client** وهناك ثلاث طرق شائعة لتنفيذ ذلك :

عن طريق ملفات أحصنة طروادة : **Trojan** لتحقيق نظرية الاختراق لابد من توفر برنامج تجسسي يتم إرساله وزرعه من قبل المستفيد في جهاز الضحية ويعرف بالملف اللاصق ويسمى (الصامت) أحيانا وهو ملف باتش **Patch** صغير الحجم مهمته الأساسية المبيت بجهاز الضحية (الخادم) وهو حلقة الوصل بينه وبين المخترق (المستفيد) .

كيفية الإرسال والاستقبال:

تقوم الفكرة هنا على إرسال ملف باتش صغير يسمى هذا الملف باسم حصان طروادة لأنه يقوم الحصان الخشبي الشهير في الأسطورة المعروفة الذي ترك أمام الحصن وحين ادخله الناس خرج من داخله الغزاة فتمكنوا من السيطرة والاستيلاء على الحصن . ملفنا الصغير الفتاك هذا ربما يكون أكثر خبثا من الحصان الخشبي بالرواية لأنه حالما يدخل لجهاز الضحية يغير من هيئته فلو فرضنا بان اسمه **mark.Exe** وحذرنا منه صديق فإننا سنجده يحمل اسما آخر بعد يوم أو يومين .لهذا السبب تكمن خطورة أحصنة طروادة فهي من جانب تدخل للأجهزة في صمت وهدوء ويصعب اكتشافها من جانب آخر في حالة عدم وجود برنامج جيد مضاد للفيروسات .

لا تعتبر أحصنة طروادة فيروسات وان كانت برامج مضادات الفيروسات تعتبرها كذلك فهي بالمقام الأول ملفات تجسس ويمكن أن يسيطر من خلالها المستفيد سيطرة تامة على جهاز الضحية عن بعد وتكمن خطورتها في كونها لا تصدر أية علامات تدل على وجودها بجهاز الخادم .

كيفية الإرسال:

تتم عملية إرسال برامج التجسس بعدة طرق من اشهرها البريد الإلكتروني حيث يقوم الضحية بفتح المرفقات ضمن رسالة غير معروفة المصدر فيجد به برنامج الباتش

المرسل فيظنه برنامجا مفيد ا إلا فيفتحه أو انه يفتحه من عامل الفضول ليجده لا يعمل بعد فتحه فيتجاهله ظنا بأنه معطوب ويهمل الموضوع بينما في ذلك الوقت يكون المخترق قد وضعه قدمه الأولى بداخل الجهاز يقوم بعض الأشخاص بحذف الملف مباشرة عند اكتشافهم بأنه لا يعمل ولكن يكون قد فات الأوان لان ملف الباتش من هذا النوع يعمل فورا بعد فتحه وان تم حذفه كما سنرى فيما بعد .

هناك طرق أخرى لزرع أحصنة طروادة غير البريد الإلكتروني كانتقاله عبر المحادثة من خلال الـ ICQ وكذلك عن طريق إنزال بعض البرامج من أحد المواقع الغير موثوق بها . كذلك يمكن إعادة تكوين حصان طروادة من خلال الهاكرز الموجودة ببرامج معالجات النصوص .

كيفية الاستقبال:

(عند زرع ملف الباتش في جهاز الضحية) الخادم (فانه يقوم مباشرة بالاتجاه إلى ملف تسجيل النظام Registry لأنه يؤدى ثلاثة أمور رئيسية في كل مرة يتم فيها تشغيل الجهاز :

١ـ فتح بوابة أو منفذ ليتم من خلالها الاتصال .

٢ـ تحديث نفسه وجمع المعلومات المحدثة بجهاز الضحية استعدادا لإرسالها للمخترق فيما بعد .

٣ـ تحديث بيانات المخترق (المستفيد) في الطرف الأخر .

تكون المهمة الرئيسية لملف الباتش فور زرعه مباشرة فتح منفذ اتصال داخل الجهاز المصاب تمكن برامج المستفيد (برامج الاختراقات)من النفوذ .

كما انه يقوم بعملية التجسس بتسجيل كل ما يحدث بجهاز الضحية أو انه يقوم بعمل أشياء أخرى حسب ما يطلبه منه المستفيد كتحريك الماوس أو فتح باب محرك السي دي وكل ذلك يتم عن بعد .

بوابات الاتصال:

يتم الاتصال بين الجهاز عبر بوابات **ports** أو منافذ اتصال وقد يظن البعض بأنها منافذ مادية في أماكنه رؤيتها كمنافذ الطابعة والفارة ولكنها في واقع الأمر جزء من الذاكرة له عنوان معين يتعرف عليه الجهاز بأنه منطقة اتصال يتم عبره إرسال واستقبال البيانات ويمكن استخدام عدد كبير من المنافذ للاتصال وعددها يزيد عن **65000** يميز كل منفذ عن الآخر رقمه فمثلا المنفذ رقم **1001** يمكن إجراء اتصال عن طريقه وفية نفس اللحظة يتم استخدام المنفذ رقم **2001** لإجراء اتصال آخر .

التواصل:

قلنا بأنه المخترق قد تمكن من وضع قدمه الأولى بداخل الجهاز الضحية بعد زرع ملف الباتش به ورغم خطورة وجود هذا الملف بجهاز الضحية فانه يبقى في حالة خمول طالما لم يطلب منه المخترق التحرك فهو مجرد خادم ينفذ ما يصدر له من أوامر ولكن بدونه لا يتمكن المخترق من السيطرة على جهاز الضحية عن بعد، وحتى يتم له ذلك، فان على المخترق بناء حلقة وصل متينة بينه وبين الخادم عن طريق برامج خاصة تعرف ببرامج الاختراق من جانب آخر تبقى أحصنة طروادة عديمة الفائدة أن لم يتمكن المخترق من التعامل معها وهى تفقد ميزتها الخطرة حالما يتم اكتشافها والتخلص منها كما أوضحت بالحلقة الدراسية السابقة، وهناك عامل ممتاز يساهم في تحقيق هذه الميزة فبرامج مضادات الفيروسات الجيدة تكتشف ملفات الباتش .

كيف يتم الاختراق:

اختراق الأجهزة كاختراق أي شيء آخر له طرق وأسس يستطيع من خلالها المخترق التطفل على أجهزة الآخرين عن طريق معرفة الثغرات الموجودة في هذا النظام وغالبا ما تكون هذه الثغرات في المنافذ **PORTS** الخاصة بالجهاز وهذه المنافذ وصفها بأبسط شكل على أنها بوابات للجهاز الإنترنت على سبيل المثال: المنفذ **80** غالبا ما يكون مخصصا ليوفر الخدمة لكي يتم دخول المستخدم الإنترنت وفى بعض الأوقات

يكون المنفذ رقمه 8080 وهناك طرق عديدة للاختراق ابسطها التي يمكن للمبتدئين استخدامها هي البرامج التي تعتمد على نظام (الزبون /الخادم /CLIENT SERVER) حيث يحتوى على ملفين أحدهما SERVER يرسل إلى الجهاز المصاب والآخر CLIENT يتم تشغيله من قبل المخترق يصبح الكمبيوتر عرضه للاختراق حيث يتم فتح أحد المنافذ PORTS وغالبا ما يكون البورت 12345 أو 12346وبذلك يستطيع الاختراق ببرنامج مخصص لذلك كبرنامج NET BUS أو NET SPHEREأو BACK ORIFICE ويفعل ما يحلو له .كما يستطيع أشخاص آخرون (إضافة إلى من وضع الملف في جهازك) فعل نفس الشيء بك حينما يقومون بعمل مسح للبورتات PORT SCANNINGفيجدون البورت لديك مفتوح من هذه الطريقة التي ذكرتها هي ابسط أشكال الاختراق . فهناك طرق عديدة للاختراق بدون إرسال ملفات لدرجة أن جمعية المقتنصين بأمريكا ابتكرت طريقة للاختراق متطورة للغاية يتم اختراقك عن طريق حزم البيانات التي تتدفق مع الاتصالات الهاتفية عبر إنترنت فيتم اعتراض تلك البيانات والتحكم في جهازك[١] .

أفضل طريقة للحماية من الاختراقات والقرصنة:

أولاً: يجب التأكد من عدم وجود تروجان بجهازك ، والتروجان هو خادم يسمح للمخترق بالتحكم الكامل في جهازك ويتم زرعه بجهازك عن طريق المخترق وذلك بإرساله إليك عن طريق البريد الإلكتروني مثلا أو عن طريق برامج الدردشة الفورية مثل ICQأو عن طريق قرص مرن ، أو يقوم أنت بزرعه في جهازك عن طريق الخطأ بسبب عبثك في برامج الاختراق فتقوم بفك التروجان في جهازك بدلا من أن ترسله إلى الجهاز المراد اختراقه ، لذلك أنصحك عدم تحميل البرامج نهائيا و ولكي نتأكد إذا كان جهازك به تروجان أم لا . هناك طرق عدية برنامج هو في ملف السجل REGISTRY الخاصة بالوندوز لأهمية REGISTRY ولفتادى حذفك الملفات عن طريق الخطأ سوف نبحث عن

(١) موقع www.khayma.com دراسة شاملة عن الاختراق من الموقع عن " تعريف الاختراق وأسبابه ودوافعه و ميكانيكية الاختراق والتواصل والإرسال " .

الترجان بطريقة آمنة وذلك باستخدام برامج باحثة . الذي يعد أفضل برنامج هو **cleaner** .

ثانيًا : قم بعمل بحث عن التروجان بالضغط على زر بحث وبعد الانتهاء من البحث على قرصك الصلب . سيخبرك برنامج أن كان يوجد لديك تروجان مزروع بجهازك وسيعطيك خيار حذفه أو علامة إذا انتهى البحث وظهرت نافذة صغيرة مكتوب بها **scan complete** فهذا معناه أن جهازك خال ونظيف من التروجان .

ثالثًا : قم بتحديث البرنامج المكافح للفيروس لديك دائما فبرنامج الفيروسات يقوم أحيانا بكشف التروجان عند فتحه عن طريق تحديث البرنامج الموجود على جهازك لان عمل **update** باستمرار من على الإنترنت . فيكون قد تم وضع إصدار آخر لهذه البرامج المكافحة للفيروسات والتروجان من على الموقع الخاص ببرنامج المكافحة ومد ذلك أيضا بأحدث الأسماء الفيروسات والتروجان الذي أنضمك دائما بعمل **update** للبرنامج الخاص بك باستمرار .

رابعًا : استقبل الملفات أو البرامج أو الصور من أشخاص من تثق بهم فقط . وان تفعل ذلك فعلى الأقل لا تقم بفتحها إلا بعد انقطاعك عند الانتهاء وبعد فتحها جميعا قم بعملية بحث عن التروجان بواسطة برنامج **cleaner** على قرصك الصلب للتأكد من خلوه من التروجان فالتروجان له خاصية الذوبان في النظام علما بان حجمه يتراوح من **50** إلى **150** كيلو بايت حسب نوعيته وإصداره .

خامسًا : إذا الملفات التي تأتيك عن طريق البريد الإلكتروني فإذا كان الملف المرسل إليك شخص لا تثق به ومن نوع **die**أو **exe**فلا تسبقه أبدا ويفضل أن يكون رقمك السري مكونا من حروف وأرقام[1] .

---

(١) موقع **www.websy.net** موضوع الحماية من الاختراق .