الفصل السابع :
أدوات الجريمة

لكي يتمكن المجرم في الإنترنت من تحقيق هدفه يجب أن يكون لديه بعض الأسلحة أو الأدوات التي تساعده على ذلك. وسيتطرق هذا الفصل إلى بعض الأدوات التي يستخدمها المجرمون في الإنترنت. فقد يحتاج المجرم لبعض الأدوات ويستغني عن بعضها الآخر اعتماداً على نوع الجريمة التي ينوي ارتكابها، وبناء على نوعية المجرم أيضا.

يكون الغرض من بعض هذه الأدوات هو الاستعداد لتنفيذ الجريمة، ويكون الهدف من بعضها الآخر هو القيام بتنفيذ الجريمة، أما القسم الأخير فيكون الغرض منه مسح آثار الجريمة. ونظراً لانتماء بعض الأدوات إلى أكثر من قسم، فلن يتم عرضها بناءً على هذا التقسيم، بل ستعرض واحداً تلو الآخر مع شرح الفائدة من كل سلاح.

وسيرد في هذا الفصل والفصول القادمة استخدام مصطلحي (المجرم) و(المخترق) بشكل متبادل، حيث إن المجرم في أغلب هذه الحالات يقوم بجريمته عن طريق الاختراق.

٧-١ تقنيات الشبكات

يعد هذا السلاح المعرفي من أهم الأدوات لمجرمي الإنترنت. ويمثل المعرفة بعلم شبكات الحاسب وكيفية عملها ومعرفة بروتوكولاتها. وهذا القسم مرتبط بشكل أو بآخر بجميع الأقسام الأخرى من أقسام أدوات المجرمين. قد لا يحتاج المجرم للإلمام بعلم الشبكات في بعض الأحيان. ولكن في أحيان أخرى كثيرة سيحتاج المجرم لمعرفة كيفية عمل الأداة لكي يتمكن من استخدامه، وهذا ينطبق غالباً على الجرائم الكبيرة التي تستهدف شركات كبيرة ذات شبكات محصنة. وكما أن الأداة تستخدم من قبل المجرمين، فإنها أيضاً تستخدم من قبل من يريد الدفاع عن نفسه أو شبكته.

٧-٢ فاحصات المنافذ

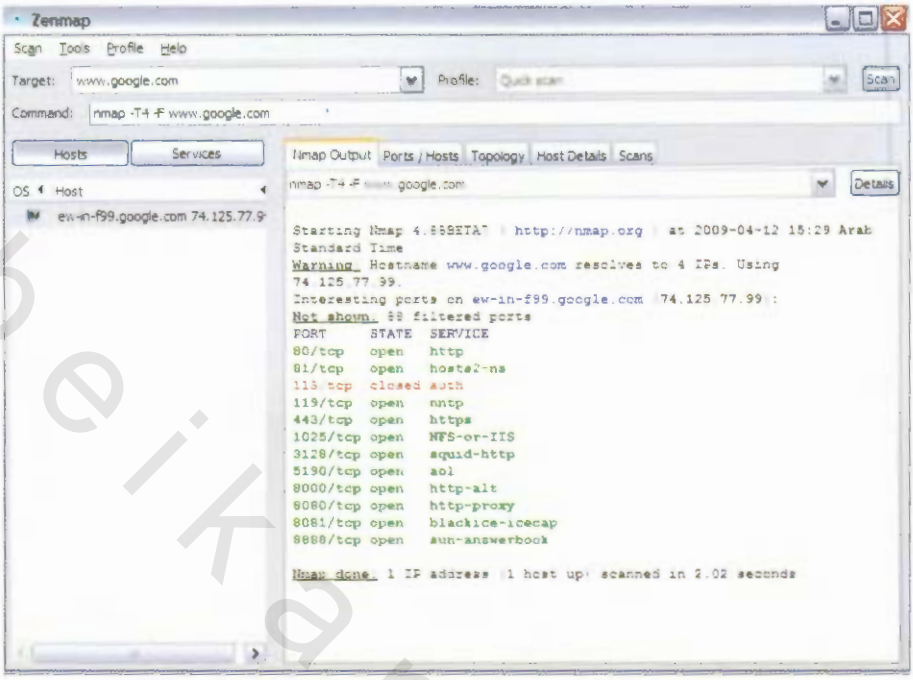
هذه النوعية من الأدوات هي برامج تقوم بفحص جهاز أو مجموعة من الأجهزة، وتقوم بتحديد المنافذ المفتوحة في تلك الأجهزة. ووجود منفذ مفتوح في الجهاز يعني أنه مستعد لقبول اتصال من جهاز آخر على ذلك المنفذ. ويتم تعريف المنفذ بتحديد رقم معين، وهذا الرقم في الغالب يمكن ربطه بتطبيق من تطبيقات الحاسب، فمثلا؛ مزودات الويب في الغالب تكون على المنفذ رقم ٨٠، ومزودات نقل الملفات (FTP) تكون على المنفذ ٢١، ويوضح الجدول ٧-١ بعض المنافذ والتطبيقات المقابلة لها. وفائدة هذه البرامج بالنسبة للمستخدم هي أنها تقوم بإعطائه معلومات مبدئية عن الجهاز الذي يرغب في اختراقه، أو أنها تساعده على تحديد الجهاز الذي يريد اختراقه. فمثلاً، ما الفائدة من تجربة البرامج التي تقوم باختراق مزودات الويب على جهاز، ما لم يكن ذلك الجهاز محتوياً على خادم ويب في الأصل. وكذلك أيضاً فإن المجرم قد يرغب في تحديد الأجهزة التي تحتوي على مزود نقل ملفات لكي يحاول اختراقها، ففي هذه الحالة يمكنه

استخدام برامج فاحصات المنافذ لكي تقوم بفحص عدد من الأجهزة وإعطائه قائمة بالأجهزة والمنافذ المفتوحة في كل جهاز.

المنفذ	التطبيق المستخدم
٨٠	مزودات الويب Web Servers
٢١	مزودات نقل الملفات FTP
٢٥	مزودات نقل البريد SMTP Servers
١١٠	مزودات استقبال البريد POP3 Server
١٣٩	تطبيق مشاركة الملفات في ويندوز Windows File Sharing
٥٣	مزود الأسماء DNS Servers

جدول ٧-١: بعض المنافذ والتطبيقات المقابلة لها.

والقيام بعملية فحص المنافذ يتطلب عادةً محاولة إنشاء اتصال بين الجهاز الفاحص والمفحوص، مما يعني أن الجهاز المفحوص سيلاحظ محاولة الاتصال، وفي بعض الشبكات المحصنة، فإن هذا سيقرع ناقوس الخطر للمشرف على الشبكة مبيناً وجود من يقوم بجمع المعلومات عن الشبكة. لهذا فإن بعض برامج فحص المنافذ المتقدمة تقوم بالقيام بفحص الجهاز الضحية بطريقة خفية ومن أشهر هذه البرامج برنامج (www.nmap.com)

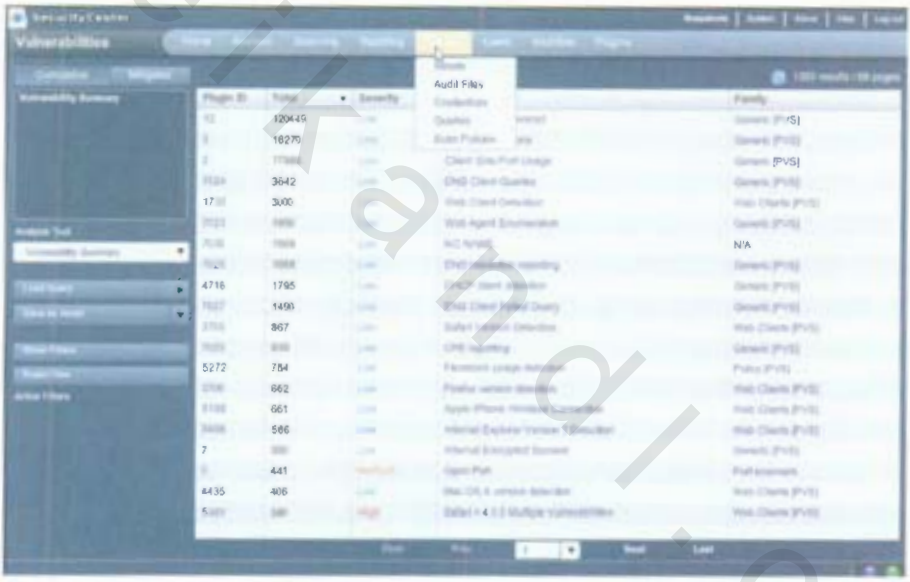


شكل٧-١: لقطة من برنامج nmap لفحص المنافذ من (www.insecure.org)

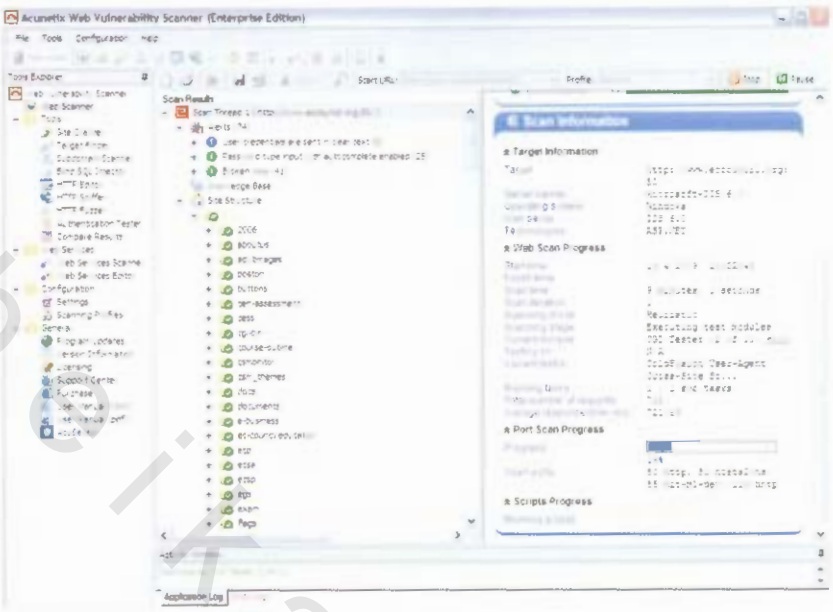
٧-٣ برامج تحديد الثغرات

إن برامج تحديد الثغرات هي مشابهة في الهدف لبرامج فاحصات المنافذ، ولكنها أعقد وأكثر تقدماً منها. فهي مزودة ببعض الثغرات الموجودة في بعض التطبيقات، التي تستخدمها لكي تقوم بفحص جهاز أو مجموعة من الأجهزة لتحديد الثغرات الأمنية الموجودة بها، ومعرفة بعض المعلومات المفصلة عنها. وطريقة عمل هذه البرامج تقوم أولاً على فحص المنافذ وعند وجود منفذ مفتوح في الجهاز الضحية، فإن البرنامج يقوم بتجربة الثغرات المشهورة المرتبطة بهذا المنفذ، ومن ثم إعطاء المخترق تقريراً كاملاً عن الجهاز أو (الأجهزة) الضحية، ويحتوي التقرير على المنافذ المفتوحة والتطبيقات المرتبطة بها، وعدد الثغرات الموجودة في هذه الأجهزة.

وهذا بالتأكيد يعطي معلومات أكثر من تلك التي تعطيها برامج فاحصات المنافذ. فمثلاً؛ برامج فاحصات المنافذ تقوم بإخبار المخترق بأن الجهاز يحتوي على منفذ مفتوح على الرقم ٨٠. بينما برامج تحديد الثغرات تخبر المخترق بأن الجهاز يحتوي على منفذ ٨٠ مفتوح، وأن الجهاز من نوع ويندوز٧ وهو محتوٍ على الإصدار ٧،٥ من برنامج Internet Information Services (IIS) وأنه تمت تجربة ثغرة (Buffer overflow) بنجاح، بينما فشلت تجربة الوصول للقرص الصلب.



شكل ٧-٢ صورة لأحد برامج مسح الثغرات



شكل ٧-٢ صورة لأحد برامج فحص الثغرات لتطبيقات الويب.

وتساعد مثل هذه البرامج على حفظ وقت المتطفل، وذلك بتجربة كل الثغرات المعروفة آليًا ودون الحاجة لتدخله. وهي أيضا تساعده على جمع المعلومات عن الجهاز الضحية، وهي المرحلة الأولى من مراحل الاختراق (سيتم الحديث عن ذلك في الفصل التالي)

على الرغم من أن هذه البرامج تساعد المجرم بشكل كبير، إلا أنها لا تغنيه بشكل كامل، حيث يتم اكتشاف الثغرات بشكل دائم ومستمر، وقد لا تحتوي هذه البرامج على آخر ما تم اكتشافه من الثغرات، التي تعد من أخطر الثغرات حيث يغفل المشرفون على الشبكات أو يتأخرون عن تحديثها. لذا فقد يحتاج المخترق للقيام بذلك بشكل يدوي أو باستخدام برامج أخرى مستقلة.

وعلى الرغم من أن هذه البرامج تستخدم في الغالب من المتطفلين والمجرمين. إلا أنه يمكن استخدامها من قبل المشرفين على الشبكات لتحديد الثغرات الموجودة في شبكاتهم قبل أن

يحددها المجرمون، وهذا أحد التطبيقات المقترحة لتلك النوعية من البرامج.

٧-٤ البرامج المتنصتة

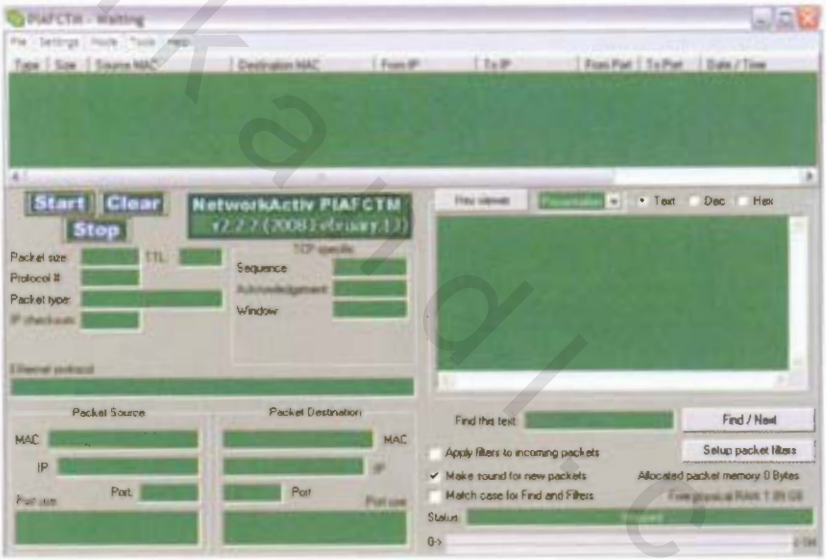
وهذه النوعية من البرامج هي اسم على مسمّى، حيث يستخدمها المخترق عند ارتباطه بشبكة معينة لكي تقوم بالتقاط كل البيانات التي يتم تبادلها في تلك الشبكة. وهذه البيانات قد تكون بيانات غير مهمة، مثل صفحة الأخبار التي قام أحد المستخدمين بزيارتها، ولكنها في أحيان أخرى كثيرة قد تكون مهمة جداً، مثل كلمة السر الخاصة بالبريد الإلكتروني، أو رقم البطاقة الائتمانية.

وتعمل هذه البرامج ضمن بعض أنظمة الشبكات، إذ إن البيانات المرسلة من جهاز إلى جهاز آخر يتم إرسالها لجميع الأجهزة في تلك الشبكة، وتقوم جميع الأجهزة بتجاهلها، ما عدا الجهاز الذي أرسلت له تلك البيانات حيث يقوم باستقبالها. وهذه البرامج تقوم بوضع كرت الشبكة في وضع التنصت الذي يمكّن الكرت من استقبال جميع البيانات، سواء كانت موجهة له أو لغيره.

ولكن لكي يتمكن المخترق من استخدام هذه البرامج، فلابد له أن يكون مرتبطاً بالشبكة التي يريد اختراقها، ليتمكن من التنصت على البيانات المارة خلال تلك الشبكة. مع العلم بأن معظم الشبكات الحديثة تقوم بوضع ما يسمى بالمقسم، وهو جهاز يسمح بنقل البيانات مباشرة من الجهاز المرسل إلى الجهاز المستقبل دون أن تراها الأجهزة الأخرى، بعكس الموزع الذي يقوم بوضع البيانات على وسيط مشترك بين كل الأجهزة المرتبطة به بحيث تستقبلها جميع الأجهزة المرتبطة بهذا الوسيط المشترك. وإذ يظن بعضهم أن المقسم يبطل عمل البرامج المتنصتة إلا أن هناك العديد من الوسائل التي تمكّن مثل هذه البرامج من العمل على المقسم، مثل ما يسمى بـ (ARP Cache Poisoning) ، وكذلك (Switch Port Stealing)

وأيضا (CAM Table Flooding).

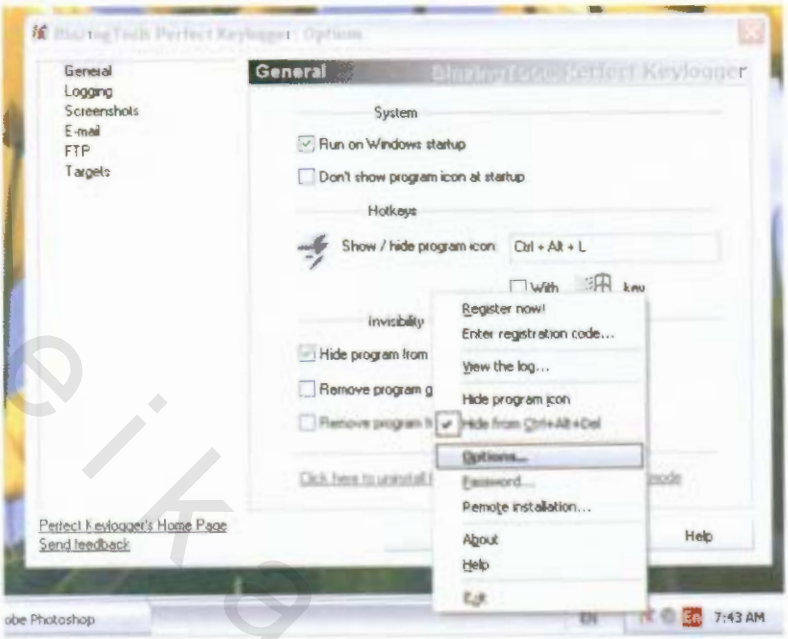
ولعل ظهور تقنية الشبكات اللاسلكية زادت من خطورة هذه النوعية من البرامج، حيث إنه في السابق كان لابد للشخص من الارتباط بالشبكة بشكل سلكي، أي إنه لابد له من الوجود في مقر الشبكة وربط جهازه بالموزع. أما مع ظهور الشبكات اللاسلكية فإنه يكفي المتطفل أو المجرم أن يكون ضمن نطاق بث جهاز نقطة الاتصال التي تعمل كوسيط مشترك بين الأجهزة في الشبكة لكي يتمكن من التقاط البيانات المارة في الشبكة. وهذا يعني أنه بإمكانه أن يكون داخل سيارته في مواقف المبنى لكي يتمكن من الارتباط بالشبكة.



شكل ٧-٣ : لقطة لبرنامج (NetworkActiv) الذي يقوم بالتنصت

٧-٥ تسجيل لوحة المفاتيح

هذه النوعية من الأدوات تقوم بتسجيل كل ما يقوم المستخدم بكتابته على لوحة المفاتيح، وحفظه لكي يقوم المخترق بالاطلاع عليه فيما بعد. وتوجد هذه النوعية من الأدوات على نوعين، أحدهما برامج يتم تركيبها في الجهاز، والآخر هو عتاد يتم وصله في الجهاز بين سلك لوحة المفاتيح والمنفذ الخاص بها في الجهاز. والفرق بينهما هو أن البرامج تعمل عندما يعمل نظام التشغيل، وهي بذلك لا تستطيع تخزين ما يكتبه المستخدم قبل الدخول لنظام التشغيل، مثل كلمة السر الخاصة بـ(BIOS) ولكنها في نفس الوقت تتميز بسعة عالية، حيث تقوم بتخزين كل ما يكتبه المستخدم حتى تنفذ المساحة في قرصه الصلب. أما بالنسبة لنوعية العتاد، فميزتها أنها تعمل بمجرد تشغيل الجهاز، فهي لا تعتمد على نظام التشغيل، بل هي قطعة مستقلة بذاتها، ولكنها في الوقت نفسه ذات مساحة محدودة، ويتطلب المخترق من الوصول الفيزيائي للجهاز لكي يقوم بفكها أو تركيبها، بعكس البرامج التي يمكن تركيبها عن بعد. وغالب البرامج من هذه النوعية تعمل بحيث لا يستطيع المستخدم رؤيتها ضمن قائمة البرامج العاملة في النظام عندما يضغط على Alt+Ctrl+Del . انظر الشكل ٧-٤.



شكل ٧-٤: برنامج Perfect Key logger

(ويظهر فيها خيار إخفاء البرنامج من الظهور في قائمة البرامج العاملة)

٧-٦ برامج التروجان (حصان طروادة)

أغلبنا يعرف قصة حصان طروادة الشهير، الذي كان يبدو في ظاهره كالهدية، ولكنه كان يحتوي على جنود الجيش، الذين ما أن دخل الحصان إلى وسط المدينة حتى قاموا بالخروج من الحصان واحتلوا المدينة.

برامج أحصنة طروادة، التي درج الناس على تسميتها بـ (التروجان) نسبة إلى كلمة Trojan الإنجليزية التي تعني طروادة، تعمل بنفس الطريقة، فهي برامج ترسل للمستخدم على أنها برنامج

مفيد أو لعبة أو غيرها من البرامج التي يرغب المستخدم بها، وما أن يقوم المستخدم بتشغيلها حتى تقوم تلك البرامج بفتح منفذ في جهاز المستخدم، وانتظار المخترق لكي يقوم بإرسال الأوامر لها. وإكمالا لخداع المستخدم الضحية، فإن البرامج الحاملة للتروجان تعمل في الغالب، وذلك حتى لا يشك المستخدم في الحيلة.

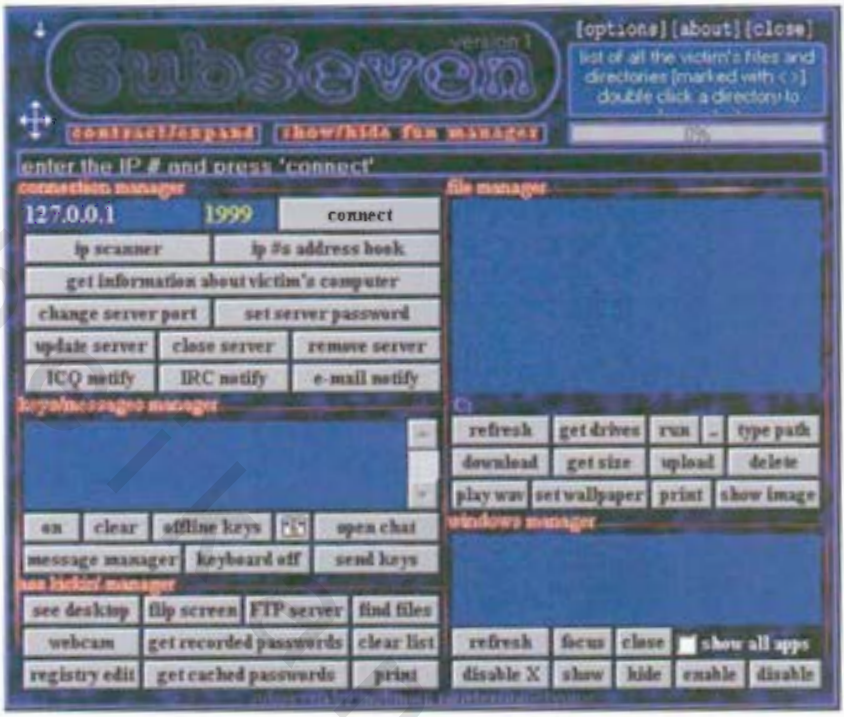
وبرامج أحصنة طروادة الشهيرة تنقسم لأربعة أقسام:

أولاً: البرنامج الحامل، وهو البرنامج الذي يقوم بخداع المستخدم حتى لا يشك في الأمر. وهذا البرنامج قد يكون أي نوع من البرامج بدءًا من الألعاب وحتى برامج معالجة الكلمات أو تحميل الأفلام، وغيرها.

ثانيًا: البرنامج الخادم، وهذا البرنامج يكون ملحقاً في البرنامج الحامل بشكل خفي، بحيث ما إن يقوم المستخدم بتشغيل البرنامج الحامل حتى يقوم البرنامج الخادم بتركيب نفسه بحيث يعمل بشكل دائم، وكذلك أيضاً فإنه يقوم بفتح منفذ قام المخترق بتحديده مسبقاً، ويبدأ في الاستماع انتظاراً لأوامر المخترق.

ثالثاً: البرنامج العميل، وهو برنامج موجود لدى المخترق، ويسمح له بالاتصال بأي جهاز ضحية، وإصدار الأوامر التي تتراوح من فتح باب مشغل القرص المدمج CD إلى عرض الملفات في جهاز الضحية وسحبها، أو رؤية ما هو خلف الكاميرا في حالة وجود كاميرا. وبعض البرامج أيضا تسمح بوضع رسالة على شاشة الضحية.

رابعاً: برامج الدمج، وهذه البرامج وظيفتها هي دمج برنامج الخادم بالبرنامج الحامل ليصبحا برنامجاً واحداً، وذلك لخداع المستخدم.



شكل ٧-٥: لقطة لبرنامج SubSeven Client

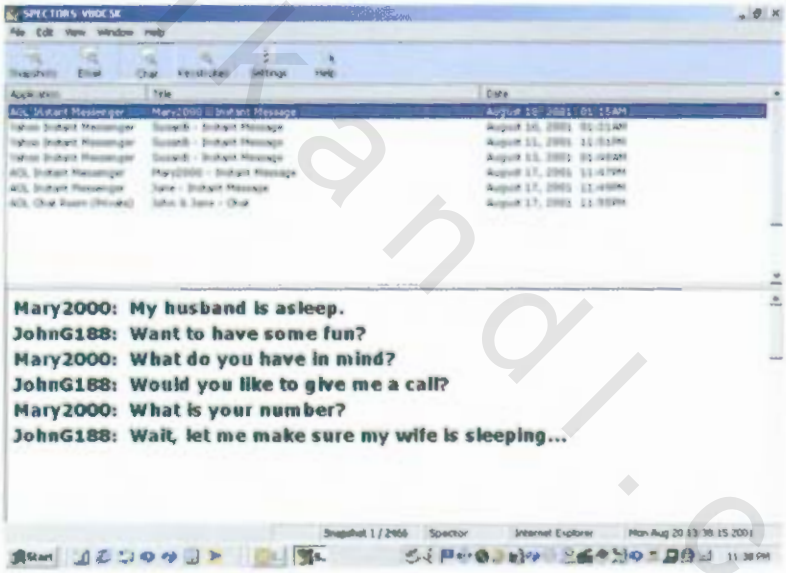
٧-٧ برامج التجسس

هذه البرامج، كما هو مسماها، تقوم بالتجسس على جهاز المستخدم، وذلك بتسجيل كل ما يقوم به، سواء أكان نص محادثة أو عنوان موقع أو بريداً إلكترونياً. وهي تختلف عن برامج تسجيل لوحة المفاتيح في كونها تقوم بتفصيل كل شيء على حدة، فهي تعطي المخترق تقريراً كاملاً ومبوباً بكل ما قام المستخدم الضحية بعمله، مفصلاً على قائمة من الرسائل التي استقبلها، والمواقع التي زارها ونصوص المحادثة التي قام بها. وهذه البرامج أيضاً تقوم بعمل لقطة

لمحتوى الشاشة بشكل متكرر وإلحاق ذلك بالتقرير الذي يستلمه المخترق.

وتعمل هذه البرامج أيضا بالنظام الخفي، حيث لا يتمكن المستخدم من معرفة عملها. ويحتوي أغلبها على الخيار الذي يسمح لها بإرسال هذا التقرير بالبريد الإلكتروني إلى من قام بتركيبها لكي يطلع عليه أينما كان.

والتطبيق الشائع لهذه البرامج هو ما يقوم به الأزواج من مراقبة زوجاتهم أو العكس لكشف خيانتهم. ولقد وجدت الكثير من قضايا الطلاق التي استندت على تقارير هذه البرامج كدليل أساسي فيها.



شكل ٧-٦: لقطة لخاصية تسجيل نصوص المحادثة في برنامج Spector

٧-٨ برامج تعطيل الخدمة

الغرض الرئيس من هذه البرامج هو تعطيل الجهاز الخادم (المزود) والمغار عليه عن تقديم خدماته للمستخدمين والأجهزة الأخرى المستحقة للخدمة. وفكرة عمل هذه البرامج هي إرسال العديد من الطلبات للخادم الضحية، بحيث يعتقد الجهاز الخادم بأن هذه الطلبات هي طلبات حقيقية ويحاول القيام بخدمتها، مما يجعله مشغولاً عن خدمة الطلبات التي يقدمها المستخدمون العاديون والمستحقون للخدمة. ويطلق على هذه النوعية من الهجمات، هجمات تعطيل الخدمة (DoS) ، وهناك نوعية أخرى يتم تنفيذها بشكل موزع، حيث تقوم مجموعة كبيرة من الأجهزة بالقيام بهذه النوعية من الهجوم في وقت واحد وهذه النوعية يطلق عليها الهجمات الموزعة لتعطيل الخدمة (DDoS) ولعل آخر هجمة شهيرة هذا القبيل هو ما حدث لموقع ويكيليكس المتخصص في نشر الوثائق السرية، فحين ملأ هذا الموقع الدنيا وشغل الناس بأخباره وتسريباته، انشغلت جهة ما بتجهيز جيش كبير وإعداد العدة لغزو الموقع وتدميره، ففتحت عليه سيلا جارفًا من الرسائل الإلكترونية مما أدى إلى تضعضع الموقع وتوقفه عدة مرات، والطريف في الأمر أن جنود هذا الجيش العظيم أصغر من أن تُرى، وأخفى من تلمس أو تحس، وتعرف بين المختصين بـ(البوت)، وهي برامج يتم تنزيلها وتركيبها بصور مختلفة على الأجهزة المصابة كأشباح رقمية، وتدار عن بعد بواسطة خادم التحكم والسيطرة (C2S). وتصبح أجهزة المستخدمين أداة للآخرين بغير علم أصحابها، وتشكل مجاميعها شبكة تقوم بهجمات تسمى الهجوم الموزع لتعطيل الخدمة، ويصنف هجوم (البوت نت) على موقع ويكيليكس على أنه من أعلى الهجمات خطورة نظرًا لحجم البيانات الكبير التي تعدت ١٠ غيغا في الثانية (١٠ Gbps). وقد حدث إغلاق الموقع في نهاية ٢٠١٠م، وتكررت الهجمات عليه ثانية، وكان آخرها ٢٠١١/٨/٣٠م، عند أعلن موقع ويكيليكس تعرضه لهجوم إلكتروني بعد انتقادات وجهت إليه لنشره آلاف الوثائق الدبلوماسية الأميركية الجديدة. ومن أشهر برامج الهجمات الموزعة لتعطيل الخدمة أيضاً،

برنامج (Trinoo)، وبرنامج TFN (Tribal Flood Network).

٧-٩ إخفاء الهوية

عند اكتشاف أي هجمة على موقع من المواقع، فإن المشرفين عليه سيقومون بتتبع مصدر الهجمة لمقاضاته. ولهذا فإن المخترقين في الغالب يلجؤون لإخفاء هوياتهم، وذلك بطريقتين:

الأولى: اختراق أجهزة وسيطة والسيطرة عليها ومسح آثارهم من تلك الأجهزة، ومن ثم استخدام هذه الأجهزة للقيام بالاختراق. ففي هذه الحالة وعند تتبع مصدر الهجمة، فإن الأثر سينتهي عند تلك الأجهزة ولن تصل للمخترق.

الثانية: استخدام بعض البرامج التي تقوم بإخفاء الهوية، وهي تعمل ذلك بكونها أجهزة وسيطة بين المستخدم وبين ما يطلبه، ويكون هناك غالبا نوع من التشفير والعشوائية لضمان عدم إمكانية تتبع المستخدم. ولكن هذه البرامج أصلاً وضعت لمن يخشون على خصوصيتهم في الإنترنت ولم توضع للمخترقين. لذا فإنه نادراً ما تستخدم للقيام بعمليات الاختراق، بل يلجأ المخترقون للقيام بذلك باستخدام النوع الأول. ولعل أشهر البرامج من هذه النوعية هو برنامج (Freedom) من شركة (Zero-Knowledge) التي قامت بإغلاق خدمتها بعد فترة وجيزة. وكذلك برنامج (JAP) الذي يمكن الحصول عليه من الموقع الألماني http://www.anon-online.de

٧-١٠ برامج التشفير وفك التشفير

هذه النوعية من البرامج يكون هدفها فك تشفير البيانات الخاصة بالمستخدم، سواء كانت هذه البيانات عبارة عن ملفات مشفرة، أو أنها كانت بيانات مشفرة تمر بالشبكة بين جهاز المستخدم وجهاز آخر.

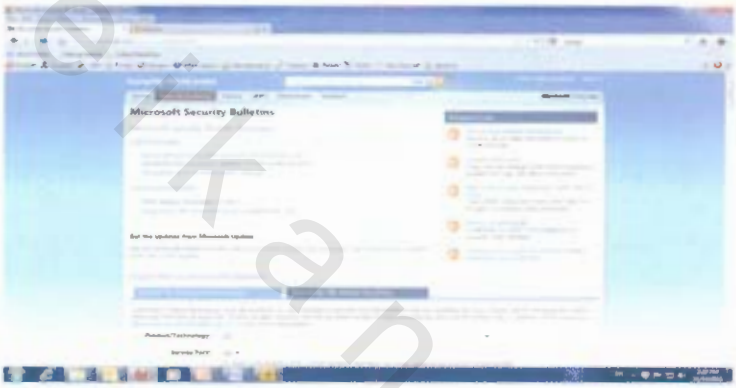
تقنيات التشفير الموجودة حالياً لا تضمن عدم إمكانية كسر الشفرة، ولكنها تضمن أن ذلك سيستغرق وقتاً طويلاً تصبح البيانات بعده عديمة الفائدة. فبعض تقنيات التشفير المعتمدة على المفتاح العام والمفتاح الخاص قد تتطلب مئات السنين لفكها.

ولكن الجهات الاستخباراتية المنتمية للدول تمتلك من القدرة الحاسوبية ما يمكنها من القيام بذلك في فترات قصيرة جداً. ويوجد في الإنترنت العديد من المشاريع التي تستخدم القدرة الحاسوبية لأجهزة ملايين المستخدمين، لكي تقوم بفك تشفير بيانات معينة. ولقد قامت شركة (RSA) الشهيرة بوضع مسابقات ذات جوائز تقدر بعشرات الآلاف من الدولارات، لمن يقوم بكسر بيانات قامت بتشفيرها ووضعها على موقعها. ولقد تم فعلاً كسر بعض هذه البيانات، ومازال بعضها الآخر سليماً لم يتم فك تشفيره إلى الآن.

٧-١١ نشرات الثغرات الجديدة

يتوفر في الإنترنت الكثير من المواقع والقوائم البريدية التي تقوم بنشر أحدث الثغرات التي تم اكتشافها سواء كان ذلك على مستوى الأجهزة أو أنظمة التشغيل أو التطبيقات المختلفة. وتوفر هذه المعلومات على المجرم عناء البحث ومحاولة فتح ثغرة في النظام الذي يحاول اختراقه. كما أن حصول المجرم على هذه المعلومات قبل أن يحصل عليها المشرف على الشبكة، يمكنه من استخدام هذه الثغرات للقيام بجريمته سواء كانت حصوله على معلومات محمية أو قيامه بتخريبها.

للحد من فعاليه هذا السلاح فإن معظم البرامج وأنظمة التشغيل تقوم دورياً بالاتصال بموقع الشركة المنتجة للبرنامج، والحصول على التحديثات التي تقوم بإصلاح هذه الثغرات. ولكنها تبقى مسؤولية المشرف على الجهاز أو الشبكة أن يتأكد من حدوث ذلك. انظر الشكل المرفق.



شكل ٧-٧: لقطة لموقع الأمن من شركة مايكروسوفت الذي يعرض آخر الثغرات التي تم اكتشافها ويوفر البرامج اللازمة لإصلاحها.