

برنامج السب سيفن (SUB SEVEN 2.1) :

- برنامج السب سيفن (sub7) برنامج لاخترق الأجهزة، يعتبر أقوى وأسهل برامج الاختراق حتى الآن،
- الباتش فايل الخاص به من أكثر الباتشات انتشارا في الأجهزة
- البرنامج رائع في اختراق الأجهزة الشخصية كالتى في مقاهي الانترنت أو الشبكات الداخلية
- الباتش فايل الخاص به له ميزة الاختفاء بعدما يقوم الضحية بتشغيله.. فيحذف نفسه من جهاز الضحية مباشرة بعد تشغيله لكنه قبل ذلك ينشئ ملفا تشغيليا آخر باسم مختلف يكون وسيطا مابين الهاكر و الضحية تحت امتداد (exe.*).



(برنامج sub7-الشاشة الرئيسية)

- إن خطأ التعامل مع ملف الباتش فايل... هو خطأ قاتل، لذا قمت بتشغيل الباتش فايل.. ثم قام برنامج زون ألامر بسؤالك هل توافق على تشغيله أم لا ثم اخترت الموافقة على تشغيل الباتش فايل عندها ستكون عرضة لاختراقات كثيرة من قبل الهاكرز حتى مع وجود زون ألامر في جهازك.. لذا دوما انتبه لرسائل الزون ألامر وغيره من برامج الحماية..... !!!

- شرح واجهة السب سيفن (SUB7) :

- كيفية الدخول إلى الضحية:

- يجب أولا إرسال الباتش أو السيرفر، ويجب على الضحية فتح الباتش.... ولا يكفي انه استقبله بل يجب عليه فتحه أيضا ومن ثم نفتح ملف السب سيفن وندخل الأي بي (IP) الخاص بالضحية وندخل البورت (المنفذ) وغالبا يكون رقم المنفذ (1243) ومن ثم نضغط على كلمة (connect) اتصال وهذا كل شيء وسوف يتم الإتصال به وتظهر لك رسالة في الأسفل بها التاريخ بالعربي أو الإنكليزي.....!!!

- idle - connected. 22:54.08 - السبت ٢٠٠٣، شباط ١٥ version: 2.1

(الرسالة التي تظهر في الأسفل عند الاتصال بالضحية)

شرح القائمة الرئيسية:

- ١- هنا أدخل رقم الأي بي.....!!!!
- ٢- هنا أدخل رقم البورت(المنفذ) وهو على الأغلب (27374).
- ٣- (connection) اضغط من أجل الاتصال.
- ٤- القائمة (connection) وفيها نجد:
 - ip scanner (باحث الأي بي) وفيه يتم البحث عن ip مصاب بملف باتش عبر النت ،حيث تدخل رقم البدء ورقم الانتهاء من البحث ورقم المنفذ ولكن يجب أن تراعي أن لا يتجاوز ip 255 ...وسوف تظهر نتيجة البحث ضمن قائمة.....!!!!

The screenshot shows a dark-themed interface for an IP scanner. It has two rows of input fields for IP addresses. The first row is labeled 'start ip:' and contains the values 21, 17, 53, and 1. The second row is labeled 'end ip:' and contains the values 21, 17, 55, and 25. To the right of these fields are two buttons: 'scan' and 'stop'. Below the IP fields, there are two more fields: 'port:' with the value 1243 and 'delay:' with the value 4. A small blue icon with a downward arrow is next to the delay field.

(شكل الباحث)

- get pc info (الحصول على معلومات الجهاز كسرعة المعالج والهارد ديسك والذاكرة).
- Get home info (الحصول على معلومات صاحب الجهاز كالعنوان -رقم الهاتف-الايمل)
- Server options (وفيه خيارات الباتش ويمكنك من خلالها وضع باسورد للباتش فايل لكي لا يتمكن أحد غيرك من الدخول- أو إجراء تحديث للباتش بنسخة أحدث- أو إزالة الباتش سيرفر) .
- Ip notify (وفيه اعدادات برامج المحادثة irc-email – icq)
- ٥- keys/massages (الرسائل – المفاتيح) وفيها القائمة التالية:
 - keyboard (لوحة المفاتيح) تتحكم بلوحة مفاتيح الضحية مثل (تعطيلها-التحكم في وظيفة الأزرار)
 - Chat (محادثة)وهي أيقونة مهمة لأنك تستطيع من خلالها التحدث مع الضحية أو أي هاكر ثاني .
 - Matrix (الرحم) حيث تصبح شاشة الضحية كلها لوحة محادثة (مسكين مايقدر يسكرها).
 - Masg manager (إدارة الرسائل)من هنا تستطيع إيهام الضحية بأي نوع من رسائل النظام .
 - Spy (التنصت) حيث يمكنك التنصت على برامج المحادثة (icq-msn-yahoo msn).
 - Icq takeover (الدخول لقائمة محادثات الأي سي كيو).
- ٦- advanced (خيارات متقدمة) وفيها خيارات كثيرا أهمها الباسورد:
 - ftp/http (اعدادات ملقم الانترنت اكسبلورر).
 - Find files (بحث عن الملفات) وذلك ضمن سواقات الضحية.
 - Password (كلمات السر) وهنا يمكنك الحصول على جميع كلمات السر الموجودة في جهاز الضحية (اشترك النت – كلمة المرور للويندوز.....الخ).
 - Open edit (للدخول إلى الريجستري الخاص بالويندوز).
 - App redirect (هذه تفتح لك موجة دوس الموجودة ضمن جهاز المسكين).
 - Port redirect (لتغيير المنافذ الموجودة ضمن الريجستري للضحية).
- ٧- miscellaneous (اختيارات متعددة) نجد في هذه القائمة:

- **file manager** (إدارة ملفات الضحية) حيث يمكنك اختيار أي سواقة لدى الضحية واستعراض البرامج الموجودة ضمنها وتحميل هذه البرامج من أو إلى جهاز الضحية أو تشغيل موجة صوت للضحية، أو حذف، أو طباعة أي ملف أو فتح صورة على جهازه.
- **Windows manager** (تظهر أي برامج تعمل لدى الضحية) ويمكنك إيقاف أي منها.
- **Process manager** (يظهر لك جميع الملفات ذات الامتداد *.exe التي تعمل على جهازه)
- **Text2-speech** (نص ناطق) حيث يمكنك ارسال نص يقرأ أحرفه عند الضحية (الملف غير موجود)
- **Clipboard manager** (يظهر لك ما يكتبه الضحية و الأزرار التي يستخدمها).
- **Irs port** (اعدادات برنامج المير سي) .
- **fun manager** (إدارة المرح) فيها العديد من الأيقونات المسلية :
- **desktop/webcam** (من خلالها تقدر إن ترى سطح مكتب الضحية بكل وضوح أو الكاميرا إذا كانت موصولة وتخزين صورهم في جهازك عن طريق (save) .
- **flip screen** (تمكنك نم العبث بشاشة الضحية فيمكنك قلبها من اليسار اليمين وبالعكس ولن يسطع الضحية إلا أن يغلق جهازه لأن كل شيء قلب في وجهه).....!!!!!!!
- **print** (طباعة) حيث يمكنك كتابة أي نص واستخدام طباعة الضحية لطباعته!!!
- **Browser** (المتصفح) من هنا يمكنك توجيه الضحية إلى أي موقع ترغب به.
- **Resolution** (تمكنك من الإطلاع على اعدادات الشاشة لدى الضحية).
- **Win colors** (التحكم بألوان نظام ويندوز لدى الضحية) .
- **extra fun** (المزيد من المرح) ومن هنا تتمكن من التحكم في سواقة الضحية أو إخفاء سطح المكتب أو إغلاق الشاشة في وجهه والكثير من التسلية.....!!!!!!!
- **screen saver** (شاشة التوقف) تشغيل نص معين كشاشة توقف (الملف غير موجود).
- **Restart win** (إعادة تشغيل) تمكنك من إيقاف التشغيل أو إعادة الإقلاع أو تسجيل الخروج.
- **Mouse** (الفأرة)تحكم كامل باعدادات الفأرة لدى الضحية(الزر اليمين يسار وبالعكس) .
- **Sound** (الصوت) تمكنك من التحكم باعدادات الصوت في جهاز الضحية وميزة أجرة هامة ألا وهي التنتصت علما يدور من حديث عند الضحية عبر المايكروفون الخاص به دون أن يعلم.
- **Time/data** (التحكم في الوقت والتاريخ في جهاز المسكين) .
- **local options** (هذه القائمة حساسة ومهمة جدا ،من خلالها تستطيع الدخول إلى اعدادات البرنامج وتغيرها وأهم شيء هو الايدت) .



- نافذة الايدت (edit) ومن هذه النافذة تستطيع تصنيع ملف باتش على كيفك! EditServer!

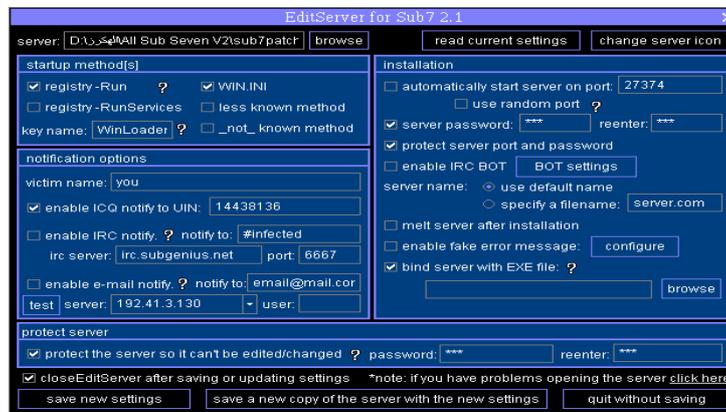
١١- نافذة القراءة(الأيقونات) .

١٢- مستكشف الأبي بي ip+اعدادات القوائم وهذا شكل المستكشف كما في الصورة:



(صورة المستكشف)

١٣- قائمة بأسماء الضحايا وعناوين الأي بي و البورت.



(شكل النافذة)