2013

Blog: www.Ring0.blog.ir

Author: Ring Zer0

E-Mail:
jmp.ring0@gmail.com

WWW.Ring0.Blog.Ir

Ring0

Jump to Ring0

[What is VirtualKD]

VirtualKD improves kernel debugging performance with VirtualBox and VMWare virtual machines.

سلامی به داغی باگ های 0day !

شاید دوستان اهل فن بگن این کارا چیه!! مقاله و مطلب دادن بنده، بقولی استاد همیشگی گوگل عزیز پس چکاره است؟ (ناگفته نمونه که بهترین استاد همه چیز بلد همین گوگل خودمونه)

تنها هدف بنده تولید محتوا هست، وگرنه همه میدونیم که مطلب بی نهایت هست، مقالات علمی ترو آکادمیک تر بخایین که IEEE و SinceDirect و.... هم وجود داره. فقط یک سرچ نیازه، ولی به زبان فارسی نیست. خیلی ها هم هستند و نمیخوان این چیزا رو یاد بدن هرچند Basic، دلیلشون هم به خودشون مربوط است. درد و دل من زیاده، اگ بشینم و بگم میشه "*داستان دو هزار دو شب RingZer0* "... :دی

خوب بریم سراغ اصل مطلب، VirtualKD ابزاری است که به Kernel Debugging در VM ها سرعت میبخشه (VMWare - VirtualBox)، این ابزار با VirtualBoxبیشتر هماهنگی داره و match هستش. چون خودم همه مدل از vmware استفاده میکنم (workstation,esxi) پس آموزش براساس همین vm خواهد بود.عملیات Debugging توسط پورت com و یا virtual serial سرعت پایینی دارند که سرعتی محدود در حدود 10KB/S هستش، که توسط Virtual KD این سرعت بیشتر میشود، در VirtualBox سرعتی تقریبی معادل 450KB/S و در VMWare سرعتی معادل 150KB/S خواهد بود. VKD ماشین مجازی مون patch و یک pipe ایجاد میکنه که قادر میشیم تا دیباگ رو توسط ابزار استانداردش WinDBG/KD انجام بدیم.

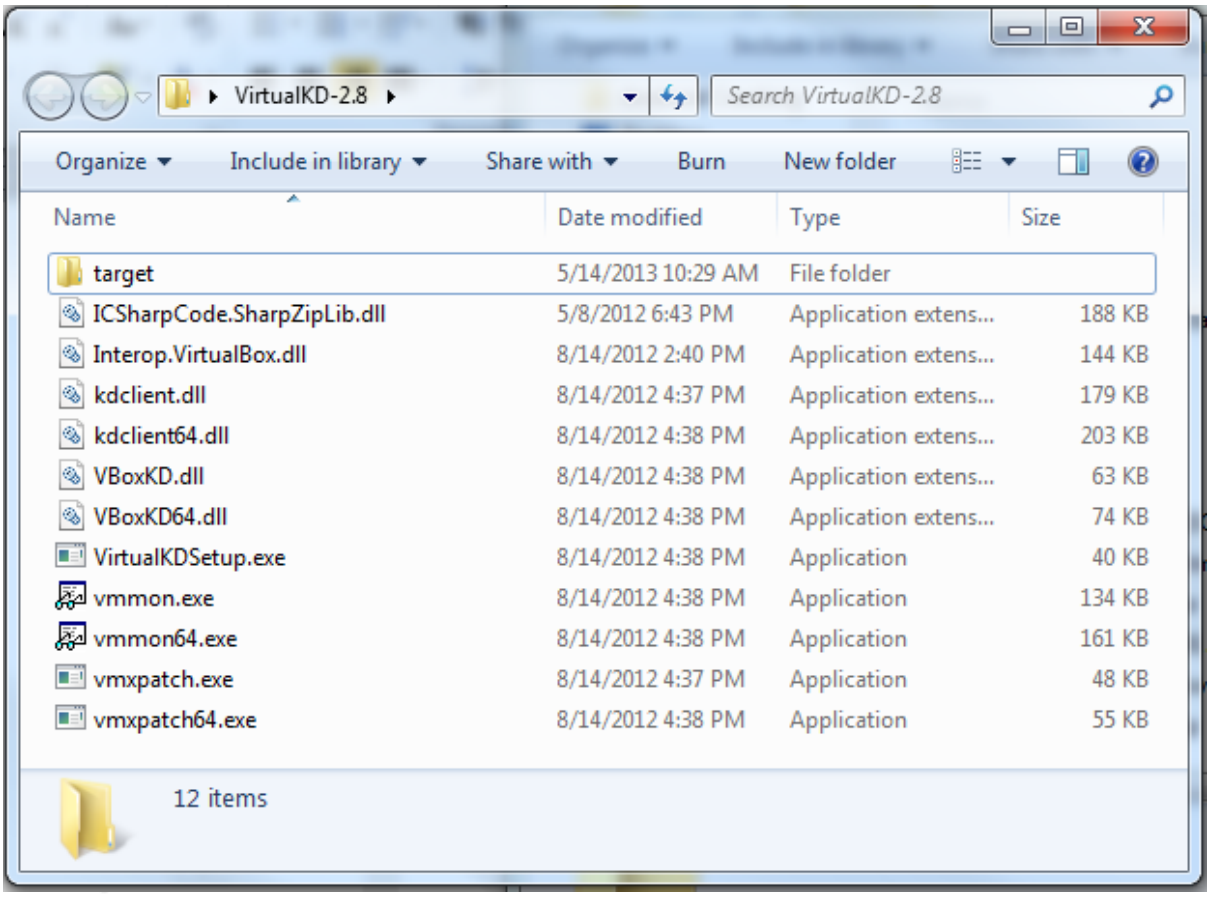
این ابزار ویندوز های x86 و x64 رو پشتیبانی میکنه. برروی سیستم عامل های زیر تست شده:

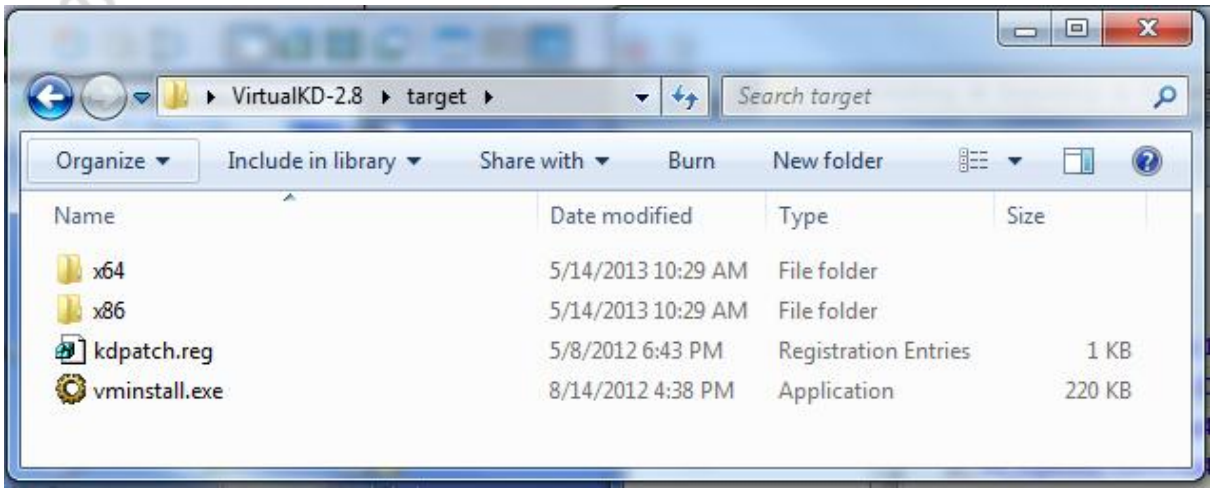
- Windows 7 64-bit
- Windows Vista 32-bit
- Windows Vista 64-bit
- Windows XP 32-bit
- Windows XP 64-bit
- Windows Server 2003 32-bit

وبرروی نسخه های مختلف از VMWare و VirtualBox تست ها انجام شده است که تیم نویسنده اطمینان کامل رو در اجرای ابزار دادن. آخرین نسخه این ابزار رو همیشه از آدرس زیر دانلود کنید:

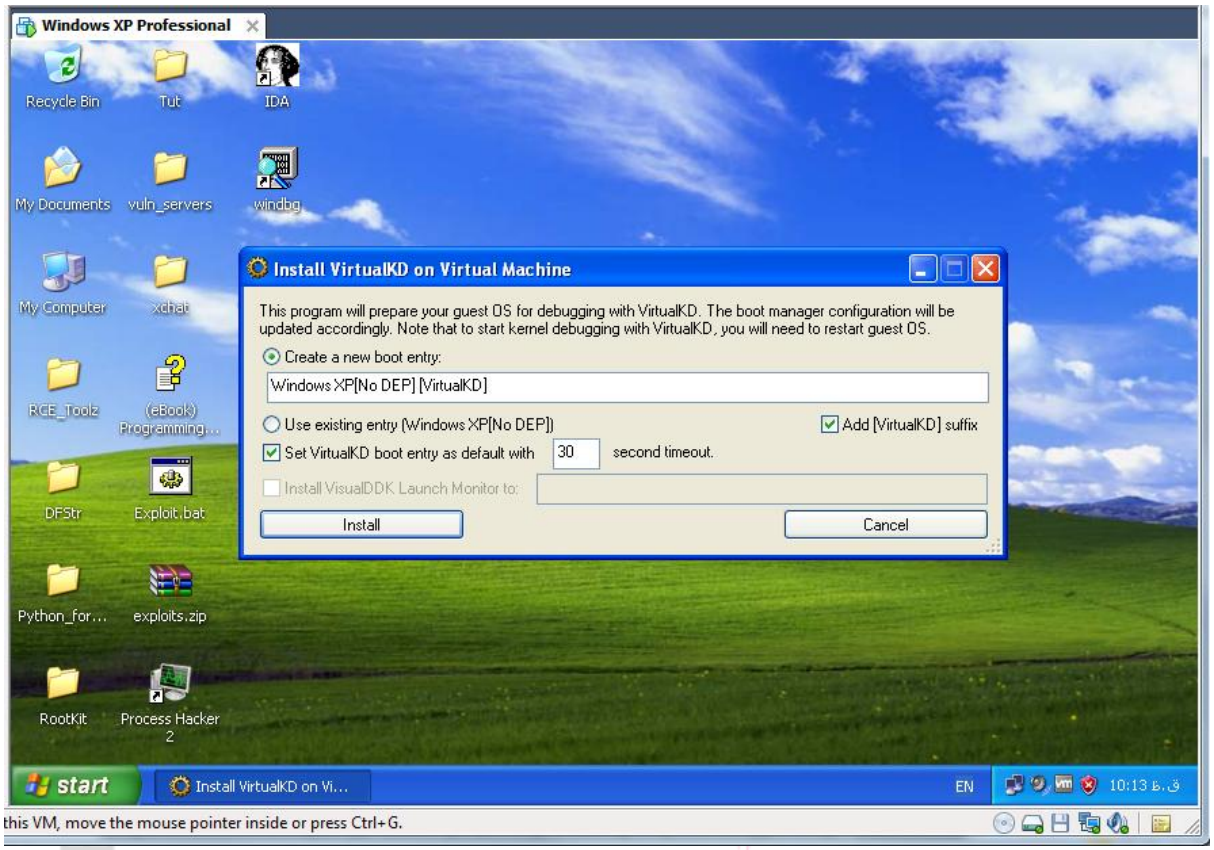
```
www.virtualkd.sysprogs.org/download
```

بعد از دانلود VKD و extract کردن آن فایل های اصلی به شکل زیر خواهد بود، که فایل های درون دایرکتوری target رو کاملا درون سیستم عامل نصب شده در VM کپی کنید.





خوب درون ماشین مجازی vminstall.exe رو اجرا کنید تا پنجره ای به شکل زیر نشان داده بشه که VKD رو در ماشین مجازی بایستی نصب کنیم.

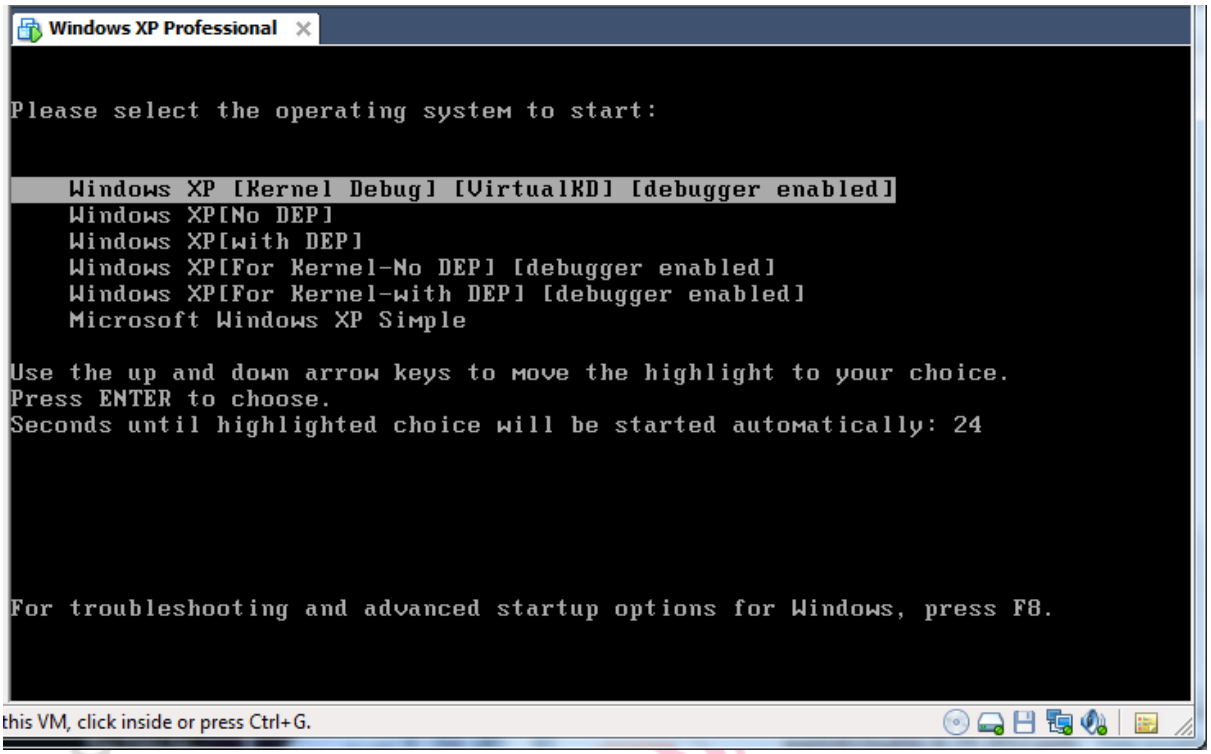


خوب در پنجره بالا که ظاهر خیلی ساده است، دو حالت داره. اولین : کاری به entry های موجود در فایل نداریم و خودمون یک entry جدید میخواهیم ایجاد کنیم و متن مورد نظر رو هم مینویسیم. در حالت دوم اولین entry در فایل رو درنظر بگیره و تغییرات رو اعمال کنه. بعد از تایپ نوشته دلخواه خودم entry زیر به فایل boot.ini ویندوزم اضافه شد.

```
Multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows XP [Kernel
Debug] [VirtualKD]" /baudrate=115200 /DEBUG /DEBUGPORT=bazis
/fastdetect /noexecute=optin
```

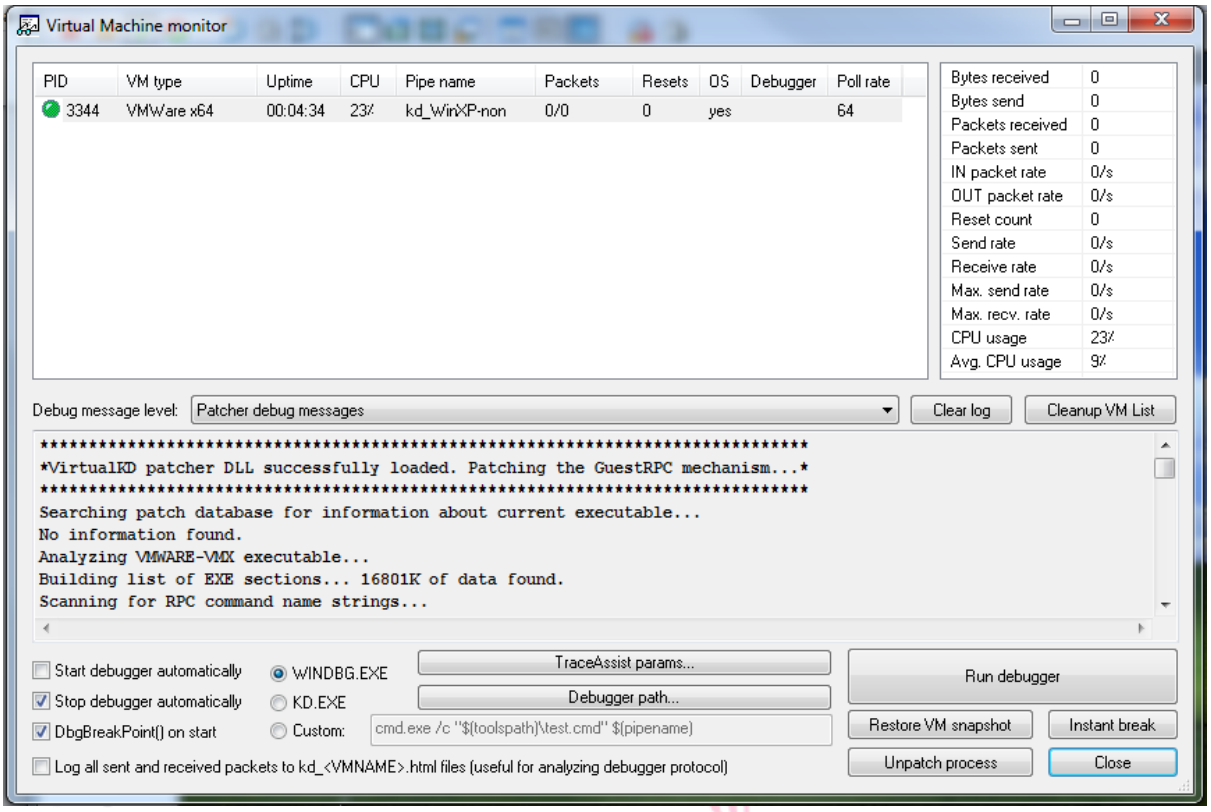
البته نکته قابل ذکر که من قبلا VisualDDK رو نصب کردم، بهمین خاطر گزینه Install VisualDDK غیرفعال هستش و مسیری از من نمیخاد. بعد ازاینکه تنظیمات دلخواه رو انجام دادین و install رو زدین پیغام restart شدن میاد که برای اعمال شدن تنظیمات بایستی انجام بشه، نصب کامل شد. حالا در ویندوز اصلی فایل vmmon بنابر ویندوز خودتون که x86 یا x64 هست اجرا کنید بعد ویندوز مجازی رو بالا بیارین.

همیشه تمامی فایل ها رو run as admin بزنید. بعد از Restart هنگامیکه ویندوز بالا میاد میبینید که entry خودتون به لیست اضافه شده، در تصویر زیر اولین گزینه:

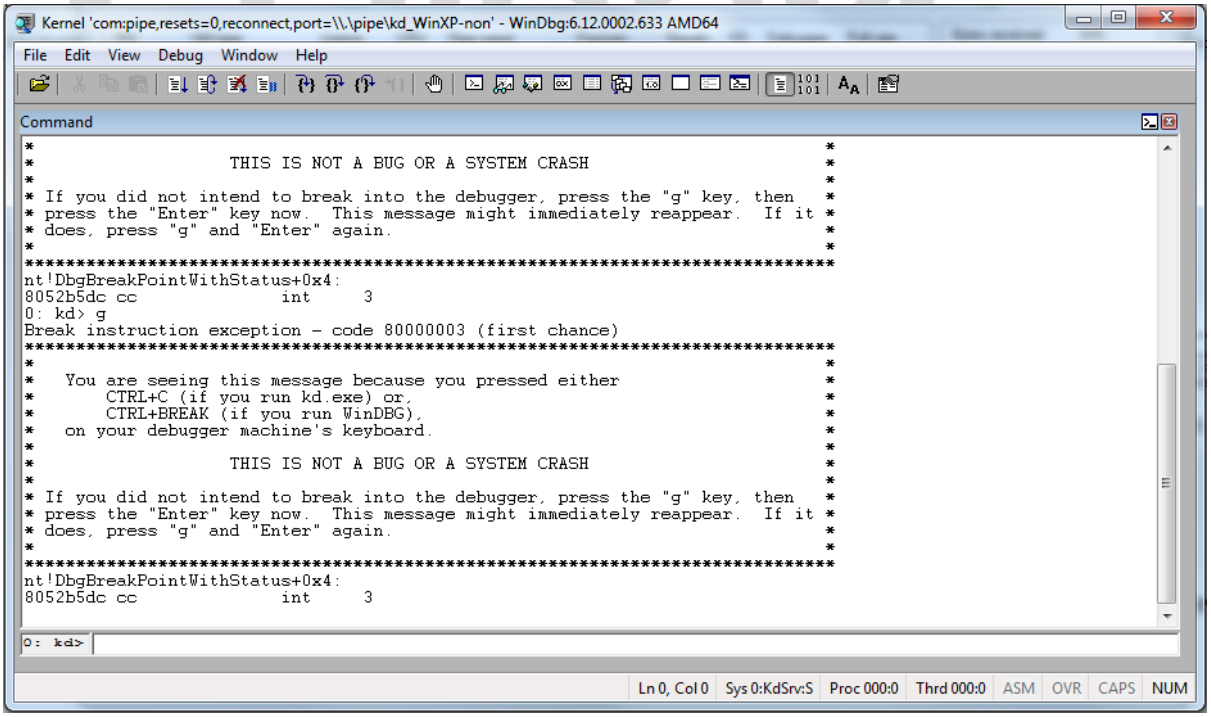


گاهی ممکنه در نصب به مشکل برخورد کنین و نصب با موفقیت کامل انجام نشه، که درصد این اتفاقات خیلی کمه. اگر همچین اتفاقی براتون افتاد بگین تا بعدا نحوه نصب دستی رو هم براتون بگم. یک مشکلی که گاها بوجود میاد در patch هست. اگر مشکلی در بالا اومدن ویندوز داشتین گزینه unpatch process و بعد از اون دوباره گزینه repatch process رو بزنید. خوب در اصل این مشکل نیس!!! وقتی که در مرحله قبل Entry مربوط به VKD رو انتخاب کردید صفحه کاملا سیاه میشه و ادامه بوت انجام نمیشه، چون منتظر میمونه تا دیباگر کانکت بشه و ادامه بوت تحت نظر دیباگر باشه. شما میتونید در این مرحله به اصطلاح هنگ کردن، بعد از شناسایی توسط vmmon دیباگر رو اجرا کنید که پیش فرض ما WinDBG هستش. بعد از اتصال کامل کلید F5 رو فشار بدید تا ادامه بوت اجرا بشه.

خوب ویندوز مجازی که بدرستی run شد باید Vmmon به شکل زیر باشه :



دقت کنید در بخش OS گزینه yes داشته باشه در غیر اینصورت بدین معنی است که درون ماشین مجازی VKD که نصب کردیم به درستی Load نشده و نمیشه debug رو انجام بدیم. بعد از اینکه دیباگر رو اجرا کردیم بخش Debugger هم مقدار yes میگیره.



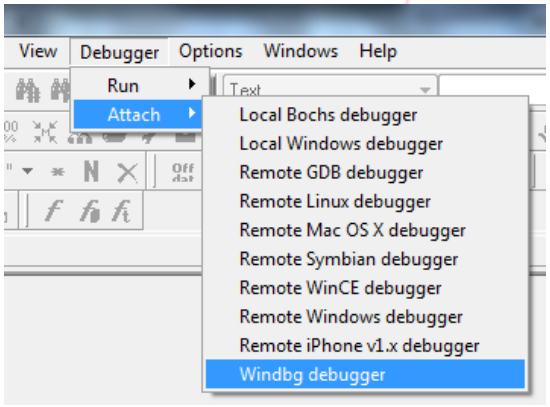
خوب این آموزش تموم شد و وارد مباحث ریز نمیشیم مثلا چطور این اتفاقات رخ میده و اساس کار چیه، هدف استفاده از تولز بود نه آنالیزش.

میتونید بجای WinDBG هم از IDA عزیز استفاده کنید، که این کارها توسط پلاگین WinDBG در IDA انجام میشه. حالا دیباگر اجرا شد و برین عملیات دیباگ رو انجام بدین وهمچنین دعای خیر برای من ...

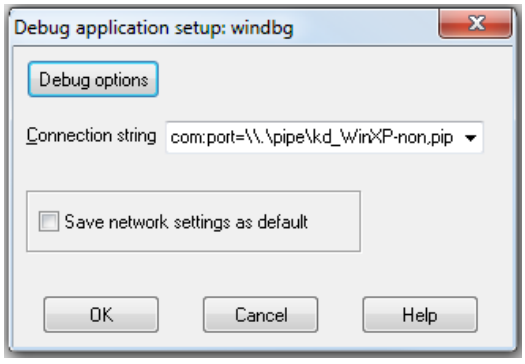
هر 0day زدین هم یادی از من کنید و یک خدابیامرز بگین !!!

حوصله نداشتم آموزش ارتباط با IDA رو بنویسم، ولی بعد از ناهار خوردن تصمیم عوض شد ...

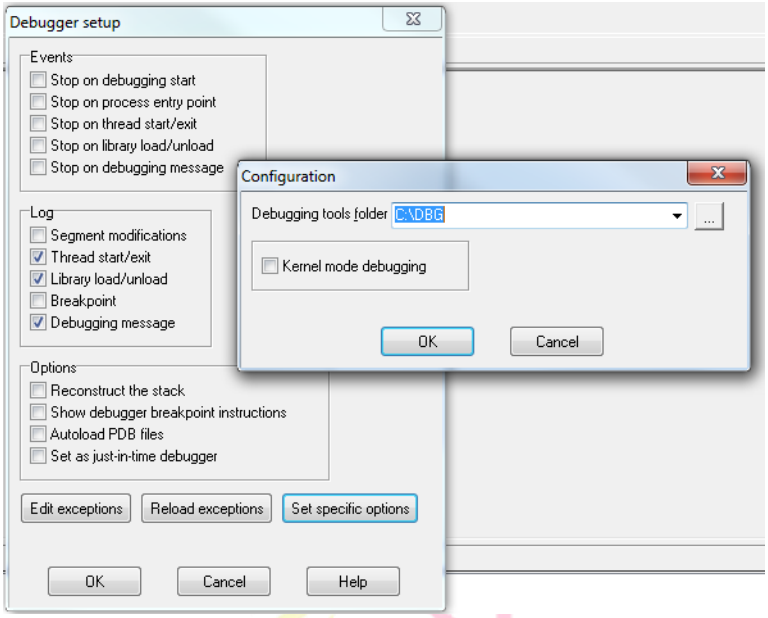
بعد از اجرای IDA به ترتیب براساس منوی زیر عمل کنین:



خوب پنجره زیر رو باید مشاهده کنید، connection string براساس قواعد نوشته زیر هست، فقط شما جای Pipe name که kd_WinXP-non ماشین مجازی من بود، در تصاویر قبل میتونید ببینید شما pipe name خودتون رو بنویسید. یک نکته : این connection string با مبحث دیتابیس یکی نیس، و اصل نیت شونه که جفت رشته اتصال هستند.

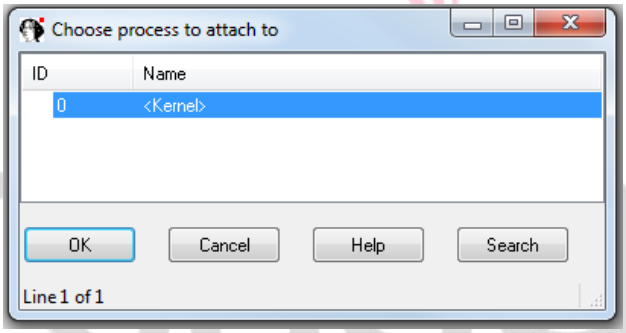


بعد از اون باید برروی Debug options کلیک کنید تا Debugger setup رو مشاهده کنید:



سپس برروی Set specific Option کلیک کنید. توجه کنید debugging tools حتما بایدنسخه x86 باشند.

در ضمن تیک Kernel mode debugging رو هم بزنید. سپس تنها گزینه برای اتچ کردن کرنل هست



اتچ کردین و همه چیز آماده و مهیاست برای دیباگ کردن.

```
nt:8052B5E8 ; ---------------------------------------------------------------------------
nt:8052B5E8
nt:8052B5E8 nt_DbgBreakPointWithStatus:
nt:8052B5E8 mov     eax, [esp+4]
EIP
nt:8052B5EC int     3                               ; Trap to Debugger
nt:8052B5ED retn    4
nt:8052B5ED ; ---------------------------------------------------------------------------
```

یک شمع روشن میتواند هزاران شمع خاموش را روشن کند و ذره ای از نورش کم نشود.