IDA Pro ile Remote Linux Debugging

written by Mert SARICA | 31 October 2010

Windows bağımlısı biri olarak benim dünyamda Linux, hep sanal makina içinde çalışmaya mahkum olmuştur. Her ne kadar Ubuntu'yu çok seviyor olsamda alışkanlık ve oyunlar nedeniyle Windows kullanmaya uzun bir süre daha devam edeceğim gibi duruyor. Windows üzerinde debug için Ollydbg, Immunity Debugger ve IDA Pro araçlarını sıkça kullanıyorum fakat sistem Linux olunca GDB kullanmak gerçekten grafik arayüzü olmaması nedeniyle can sıkıcı olabiliyor.

Fakat benim gibi sadece tek bir işletim sistemi kullanmıyor sanal makinalardanda faydalanıyorsanız Linux üzerindeki bir programı debug etmek için IDA Pro'nun uzaktan (remote) debug özelliğinden faydalanabilirsiniz. Remote debugging, yerel veya uzaktaki ağ üzerinde yer alan bir sistemde çalışan bir programı kendi sisteminiz üzerinden debug etmenizi sağlar bu sayede örnek olarak uzak sistemde çalışan zararlı bir yazılımı kendi sisteminize zarar vermeden analiz etme imkanınız olmuş olur.

Benim gibi ana sistem olarak Windows 7 kullanıyorsanız ve sisteminizde IDA Pro v5.x yüklü ise şu adımları izleyerek Linux üzerindeki renksiz GDB'ye güzel bir alternatifiniz olabilir :)

Yazının daha kolay anlaşılabilmesi için örnek olarak Linux için hazırlanmış bir crackme programını debug edeceğiz. Crackme, tersine mühendislik becerilerinizi geliştirebilmeniz için internet üzerindeki gönüllüler tarafından kırılmak üzere hazırlanmış programlara verilen isimdir.

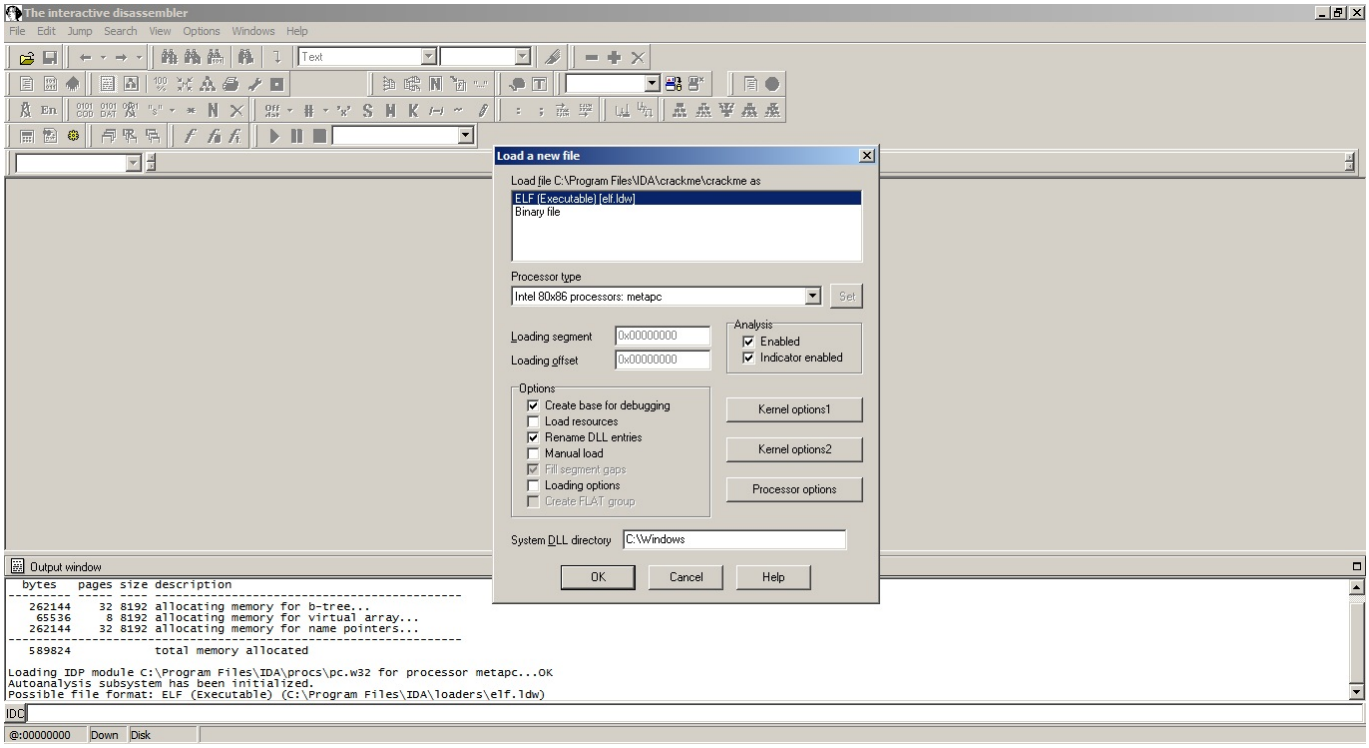
İlk olarak Crackmes.de sitesinden cyrex's Linux CrackMe programını indirelim ve C:\Program Files\IDA\crackme klasörü içine arşivden çıkartılmış halini kopyalayalım.

Öncelikle uzaktan debug etmek için Windows sisteminiz üzerinde ida adında bir kullanıcı yaratmanızı tavsiye ederim. Kullanıcıyı yarattıktan sonra C:\Program Files\IDA klasörünü paylaşıma açalım ve IDA kullanıcısını bu paylaşım üzerinde yetkilendirelim. Daha sonra sanal makina içinde yüklü olan Ubuntu'ya geçerek (evet herkes Ubuntu kullanmalı :p) bulunduğumuz klasör altında ida klasörü yaratalım ve arından smbmount komutu ile az önce yaratmış olduğumuz paylaşıma bağlanarak bu klasör içinde yer alan linux_server

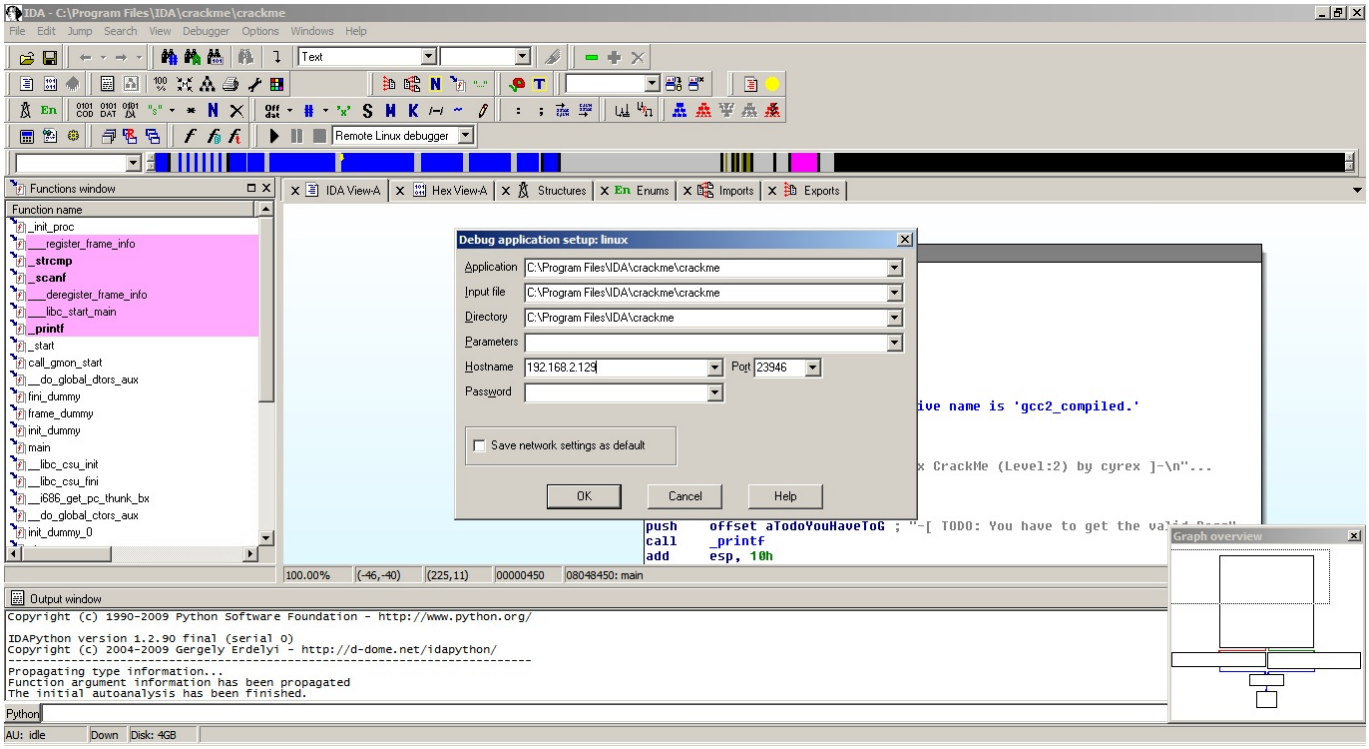
programını çalıştıralım.

```
root@bt:~# mkdir ida
root@bt:~# smbmount //192.168.1.3/ida ida -o username=ida,password=ida,rw
root@bt:~# ls ida
aqDockingManagerB6.bpl  ida_kdstub.dll  license.txt     unins000.dat
cfg                     idacolor.cf     linux_server    unins000.exe
clp.dll                 idag.exe        linux_server64  vcl60.bpl
clp64.dll               idag.ico        loaders         vclx60.bpl
dbgeng.dll              idag64.exe      mac_server      win32_remote.exe
dbghelp.dll             idahelp.chm     mac_server64    win32_remote64.exe
doswin32.rtm            idau.exe        plugins         win64_remotex64.exe
ida.hlp                 idau64.exe      procs           win_fw.dll
ida.int                 idaw.exe        python          wince_remote_arm.dll
ida.key                 idaw64.exe      rtl60.bpl       wingraph32.exe
ida.wll                 idc             sig             xmlrtl60.bpl
ida64.int               ids             symsrv.dll
ida64.wll               iphone_server   til
root@bt:~# ./ida/linux_server
IDA Linux remote debug server(ST). Version 1.10. Copyright HexRays 2004-2009
Listening on port #23946...
```

Daha sonra Windows'a geçerek IDA'yı çalıştıralım ve File menüsünden Open'a basarak C:\Program Files\IDA\crackme klasörü içinde yer alan crackme programını açalım.



Daha sonra üstteki menüden Debugger'ı seçelim ve daha sonra Remote Linux Debugger'ı seçelim. Ardından Debugger menüsünden Start process'i seçelim ve Hostname kısmına sanal makina içinde çalışan Ubuntu sisteminin IP adresini girelim.



IP adresini girdikten sonra ise Debugger menüsünden Start process'i seçerek debug işlemini başlatalım. (Her iki uyarı mesajınıda Yes diyerek geçebiliriz.)

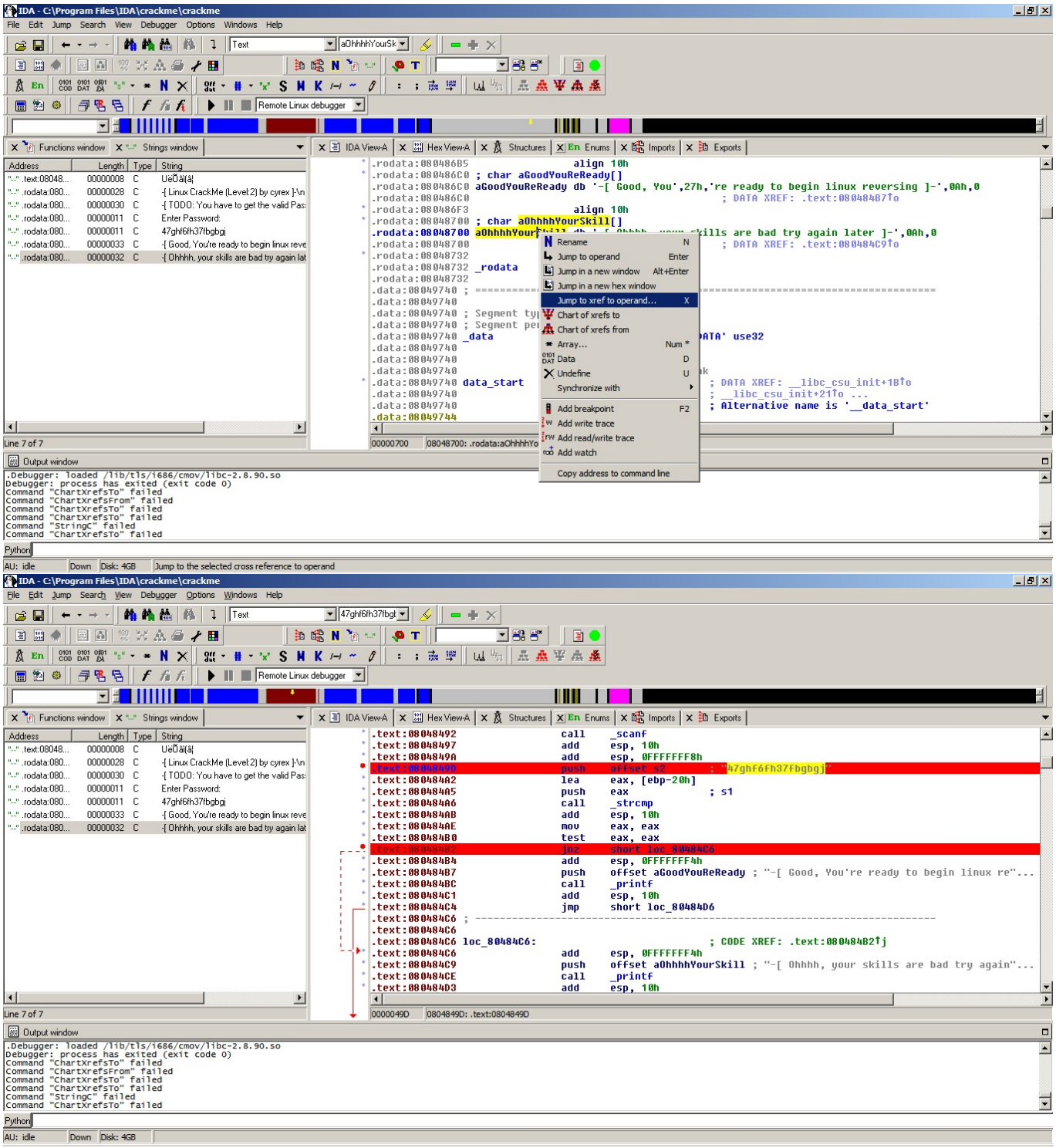
Crackme'yi kırmak için bizden doğru şifreyi bulmamız isteniyor. Debug işlemi başladıktan sonra Ubuntu'ya bakacak olursanız ekranda sizden doğru şifreyi girmenizi istediğini görebilirsiniz. Buraya rastgele bir şifre girdiğimizde (12345) hata mesajı ile karşılaşıyoruz ve debug işlemi sonlanıyor.

```
root@bt:~# mkdir ida
root@bt:~# smbmount //192.168.1.3/ida ida -o username=ida,password=ida,rw
root@bt:~# ./ida/linux_server
IDA Linux remote debug server(ST). Version 1.10. Copyright HexRays 2004-2009
Listening on port #23946...
=============================================================
Accepting incoming connection...
td_ta_new: application not linked with libthread
td_ta_new: application not linked with libthread
-[ Linux CrackMe (Level:2) by cyrex ]-
-[ TODO: You have to get the valid Password ]-
Enter Password: 12345
-[ Ohhhh, your skills are bad try again later ]-
Closing incoming connection...
=============================================================
```

Amacımız doğru şifreyi bulmak olduğu için bunun için IDA'da Shift 12 tuşlarına basarak Strings penceresini açalım ve az önce karşılaştığımız hata mesajının üzerine iki defa basarak program üzerinde bu değişkenin tutulduğu ilgili bölüme gidelim.

Faremizin imlecini char aOhhhhYourSkill[] üzerine getirdikten sonra x tuşuna

basarak bu değişkeni çağıran kod parçasına gidelim.



Bu kodun üzerine hızlıca göz attığımızda kullanıcıdan alınan verinin yani şifrenin strcmp fonksiyonu yardımı ile 47ghf6fh37fbgbg değeri ile karşılaştırıldığını ve doğru olması durumunda Good ile başlayan mesaja aksi durumda Ohhh ile başlayan hata mesajına gittiğimizi görüyoruz ve şifrenin 47ghf6fh37fbgbg olduğunu öğrenmiş oluyoruz ve crackme başarıyla çözülmüş oluyor.

```
root@bt:~# mkdir ida
root@bt:~# smbmount //192.168.1.3/ida ida -o username=ida,password=ida,rw
root@bt:~# ./ida/linux_server
IDA Linux remote debug server(ST). Version 1.10. Copyright HexRays 2004-2009
Listening on port #23946...
=============================================================
Accepting incoming connection...
td_ta_new: application not linked with libthread
td_ta_new: application not linked with libthread
-[ Linux CrackMe (Level:2) by cyrex ]-
-[ TODO: You have to get the valid Password ]-
Enter Password: 12345
-[ Ohhhh, your skills are bad try again later ]-
Closing incoming connection...
=============================================================
Accepting incoming connection...
td_ta_new: application not linked with libthread
td_ta_new: application not linked with libthread
-[ Linux CrackMe (Level:2) by cyrex ]-
-[ TODO: You have to get the valid Password ]-
Enter Password: 47ghf6fh37fbgbgj
-[ Good, You're ready to begin linux reversing ]-
Closing incoming connection...
```

Gördüğünüz üzere Windows üzerinde çalışan IDA ile Linux üzerindeki bir programı debug etmek GDB'nin aksine daha kolay ve eğlenceli olabiliyor.

Bir sonraki yazıda görüşmek dileğiyle herkese iyi haftalar dilerim.

Not: Geçtiğimiz aylarda yayınlanan v6 sürümü ile IDA Pro kullanıcıları Linux ve Mac OS X üzerinde GUI arayüzüne kavuştu.