

Mov:

Bu komutla bir registerdan bir registera kopyalama yapılabileceği gibi bir registere sabit bir değer de yazılabilir. Örnekler:

mov ah,5 #ah ye 5 değeri taşınmış yani atanmış.

mov al,bh #al’nin içine bh değeri tarşınıyor.

Cmp:

İki registerdeki değeri ya da bir registerdaki değerle sabit bir değeri kıyaslar. Tek başına bir işe yaramaz. Örnek:

14F7:100 cmp al,bl #al ile bl kıyaslanıyor.

14F7:102 cmp bl,5 #bl ile 5 kıyaslanıyor.

14F7:104 cmp 5,bl #5 değeri başta olduğu için kıyaslıyamıyor

14F7:106 cmp ax,bl #farklı bitlerde oldukları için kıyaslanamıyor

Bu komutlardan ilk ikisi çalışacak. Son ikisiyse çalışmayacak. Çünkü üçüncüsünde ilk argüman sabit bir değer. Sonuncusunda da farklı boyutlardaki yazmaçlar kıyaslanmış.

Push:

Push komutu herhangi bir bilgiyi belleğin stack adı verilen bölümüne kaydetmek için kullanılır.

Pop:

Pop komutu ile de stack üzerinden bilgi okuması gerçekleştirilir.

Add:

Add komutu toplama işlemini gerçekleştirmek için kullanılır.Add konutu ile “kayna” içerisindeki değer “hedef” ile toplanıp tekrar “hedef” register içerisine kaydedilir.

Lea:

Lea komutu ise etkin adresi yüklememizi sağlar.

Test:

Test komutunun çalışma prensibi ve flagları etkileme biçimide dahil olmak üzere And ile aynıdır.

Je:

Kendisinden hemen önce gelen cmp komutuna göre programın akışını belirli bir ofsete yönlendirir.Örnek:

14F7:100 cmp al,bl #al ile bl kıyaslanıyor.

14F7:102 je 10e # je yani al ve bl eşit ise 10e ofsetine yönlendiriyor.eğerki değilse program olduğu gibi devam edecektir.

Xor:

Xor komutu eğer 2 register birbiri ile aynı ise 0,farklı ise 1 değerini döndürür.

Örnek:

1^1=0

1^0=1

0^1=1

0^0=0

Call:

Call komutu fonksiyon çağırmamızı sağlar bu işlemi yaparken bir sonraki işlemin adresini kaydeder fonksiyon tamamlandıktan sonra o adresten program devam eder.

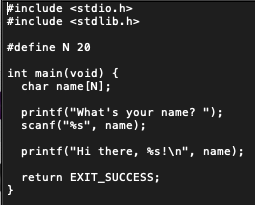
**FUZZİNG**

**Fuzzing,** sisteme beklenmedik, yarı geçerli, sıralı verilerin gönderimi gibi yöntemlerle sistemin iç yapısındaki hataları bulmayı hedefleyen Kapalı-Kutu yazılım test etme yöntemi. Fuzzing için çeşitli test yöntemleri isimlendirilmektedir:

* Olumsuz test yöntemi;
* Protokol mutasyon;
* Güvenilirlik test yöntemi;
* Sözdizimi test yöntemi;
* Hata enjeksiyonu;
* Yağmurlu-gün test yöntemi;
* Kirli test yöntemi.

Fuzzing yöntemlerinin uygulanmasını sağlamak için geliştirilen programlara ise Fuzzer denilmektedir.

Örnek Fuzzing kodu :



Son olarak da Buffer overflow işleminin kısa özeti..