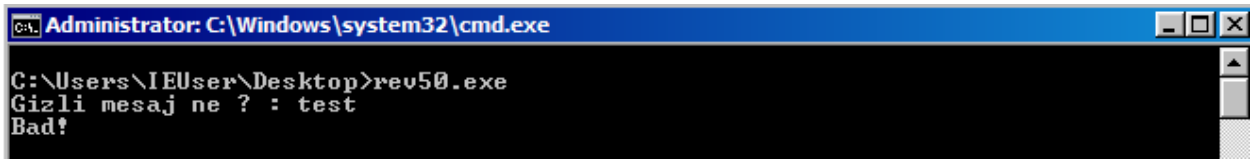
Merhabalar,

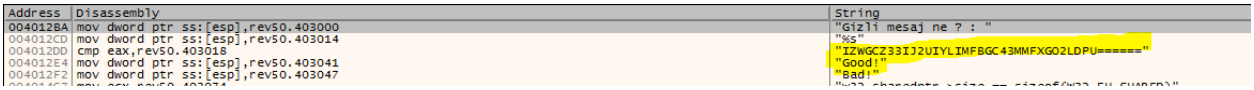
Cybercamp19 kamp son ctf yarışmasında çıkan tersine mühendislik sorularının yapmış olduğum çözümleri şu şekilde;

Program mekaniklerine değinmek amacıyla ilk soru için detaylı anlatımdır.

Rev50.exe
Çalıştıralabilir dosyamızı yürüttüğümüzde bize sorduğu soruya herhangi bir cevapla karşılık verince BAD! Tuzağına düşüyoruz.

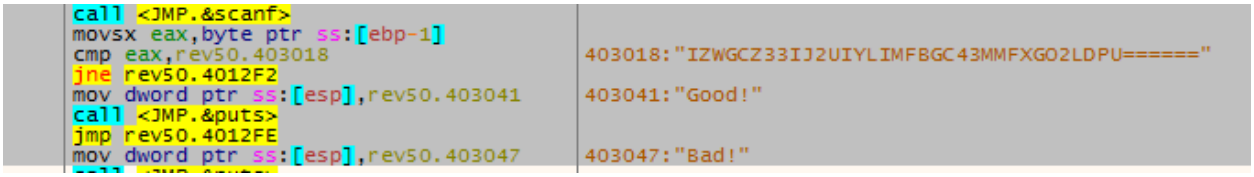


Herhangi bir exe disassemble edebilen bir programla baktığımızda (ben x86WinDbg kullanmak istedim) , programın giriş noktası (Entry point'e) ulaşıyoruz.;main fonksiyonumuz. Bu noktada ki kontrolleri anlamak için öncelikle verilen mesajları bularak başlıyorum. Main fonksiyonun frame'I içerisinde kullanılan stringleri listelemek istiyorum . Eğer stringler bir şekilde saklanmadıysa işimiz oldukça kolay.



Program içerisindeki stringleri bulmak için genellikle "search for > all referenced strings" şeklinde seçeneklerden ulaşabilirsiniz.

Öncelikle "Bad!" mesajını hangi kontrol noktası kullanmış buna bir bakalım: Yine kolay bir şekilde Bad! String'ine tıkladığınız zaman sizi kod akışı içerisinde çağrıldığı fonksiyona götürecektir.



Resimde ki akışa bizi götürdü ve fonksiyona genel olarak baktığımız da bizden scanf() fonksiyonu ile aldığı girdi değerinin ilk karakterini ebp-1 (tüm girdinin tutulduğu stack) 'ten BYTE PTR ile sadece bizim girdimizin sadece ilk karakterini alıp IZWGC.. stringini gösteren data adresi ile karşılaştırıyor. Bu işleme göre programa patch yapmadan asla GOOD mesajına ulaşma şansımız olmayacak. Zaten program bizden onu da istemiyor. Data adresinde bulunan stringi BASE32 decode edince elde ettiğimiz değer puan almak için yeterli olucak.

IZWGCZ33IJ2UIYLIMFBGC43MMFXGO2LDPU

Flag{BuDahaBaslangic}