****

**YILDIZ TECHNICAL UNIVERSITY**

**FACULTY OF ELECTRICAL AND ELECTRONICS**

**SECURITY OF COMPUTER SYSTEMS**

**(BLM4011)**

**\_ \_ \_ \_ \_ \_ \_ \_ LAB REPORT**

20011901 – Muhammet Kayra Bulut  
19011707– Barış Can Yılmaz

kayra.bulut@std.yildiz.edu.tr  
can.yilmaz8@ std.yildiz.edu.tr

**DEPARTMENT OF COMPUTER ENGINEERING**

1. **INTRODUCTION**

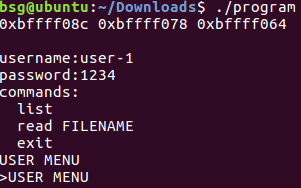
Buffer Overflow saldırısı, kullanıcıdan alınan input değerinin, eğer bu input değerleri statik olarak saklanacaksa, beklenen uzunluktan daha uzun girdi gelmesiyle gerçekleşir. Sistemin arkaplanını bilen bir hacker rahatlıkla sisteme girebilir. Yapması gereken tek şey programın ayırdığı hafıza alanından daha uzun bir input girmektir. Bize verilen örneğe baktığımızda ‘isAdmin’ değeri 4 byte, ‘userName’ değeri 20 byte, ‘password ‘ değeri de 20 byte yer kaplamaktadır. Bu değişkenler statik tanımlandığı için stackte ardışık bir şekilde stackin en büyük adresine karşılık gelen değerde ‘idAdmin’, onun ardından ‘password’ ve ‘username’ değerleri gelmektedir. Bundan dolayı ya ‘userName’ alanına 40 byte’dan daha büyük bir değer ya da ‘password’ alanına 20 byte’dan daha büyük bir değer girildiğinde hacker ‘isAdmin’ değerini istediği şekilde manipüle ederek sisteme yetkisiz giriş sağlayabilmektedir.

1. **METHOD**

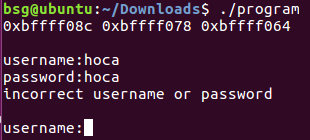
Hacker sisteme girmek için sistemin sistematiğini elde eder ya da çözmeye çalışır. Sonrasında sistemdeki değişkenlerin yapısına ve sistemin hafıza organizasyonuna göre yöntemini belirler. Eğer sistemdeki değişkenler statik ve ardışık tanımlanmışsa sistem Buffer Overflow kullanılarak yapılacak atağa karşı çok savunmasız demektir. Hacker brute-force olarak belli uzunluklarla sisteme erişmeye çalışır. Sonunda hacker sisteme erişir ve dilediği şekilde verileri silme-kopyalama-manipüle etme gibi işlemleri yapabilir. Hacker bununla gözdağı vererek karşılığında para teklif edebilir.

1. **RESULTS**

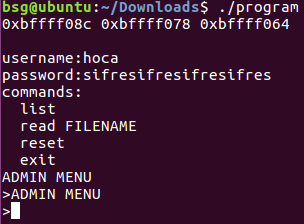
Verilen örnekler için 0xbffff08c ile 0xbffff078 arasında 0x14 byte, yani onluk tabanda 20 byte’lık fark var. Benzer şekilde 0xbffff078 ile 0xbffff064 arasında 0x14 byte, yani onluk tabanda 20 byte’lık fark var.

****

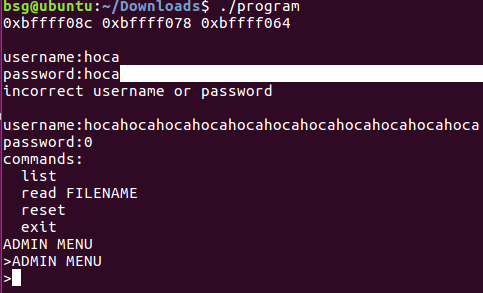
Burada verilen örnek kod için normal şekilde kullanıcı girişi yaptık



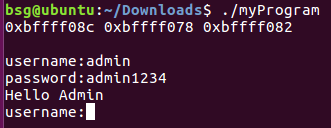
Burada verilen örnek kod için normal şekilde kullanıcı girişi yapamadık



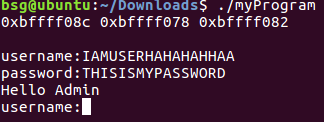
Burada verilen örnek kod için şifreyi uzun girerek buffer overflow yaptık



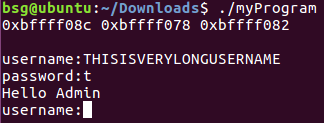
Burada verilen örnek kod için kullanıcı adını uzun girerek buffer overflow yaptık



Burada kendi yazdığımız kod için normal giriş yaptık



Burada kendi yazdığımız kod için şifreyi uzun girerek buffer overflow yaptık



Burada kendi yazdığımız kod için kullanıcı adını uzun girerek buffer overflow yaptık