****

**YILDIZ TECHNICAL UNIVERSITY**

**FACULTY OF ELECTRICAL AND ELECTRONICS**

**SECURITY OF COMPUTER SYSTEMS**

**(BLM4011)**

**LAB-3 BUFFER OVERFLOW**

**LAB REPORT**

20011701 – Muhammet Ali ŞEN  
20011045– Muhammed Ali LALE

ali.sen@std.yildiz.edu.tr  
ali.lale@ std.yildiz.edu.tr

**DEPARTMENT OF COMPUTER ENGINEERING**

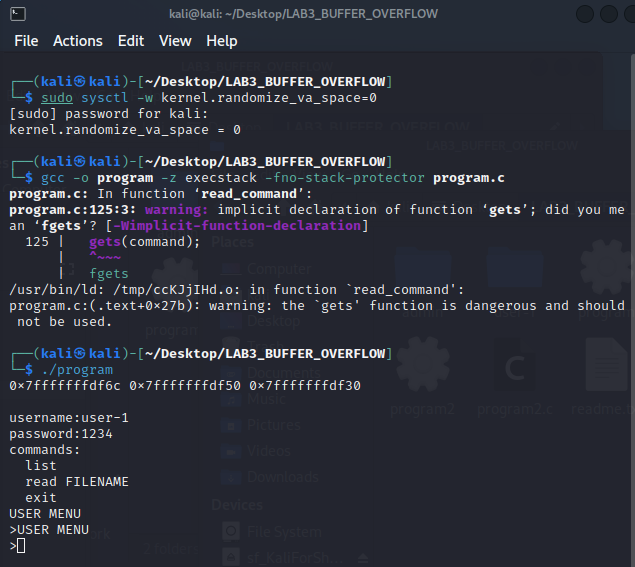
1. **GİRİŞ**

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. **METOD**

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. **SONUCLAR**

Verilen örnekler için 0x7fffffffdf6c ile 0x7fffffffdf50 arasında 0x14 byte, yani onluk tabanda 20 byte’lık fark var. Benzer şekilde 0x7fffffffdf50 ile 0xbfffffffdf30 arasında 0x14 byte, yani onluk tabanda 20 byte’lık fark var.

Burada verilen örnek kod için normal şekilde kullanıcı girişi yaptık. Akabinde hatalı kullanıcı adı ve şifre ile giriş yapılamadı.

Graphical user interface, text

Description automatically generated

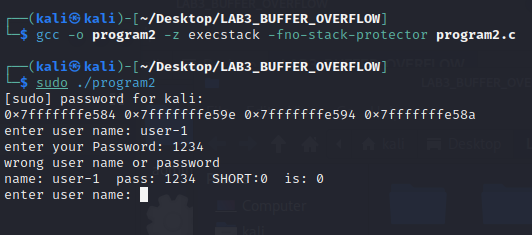
Graphical user interface, text, website

Description automatically generatedGraphical user interface, text

Description automatically generated

Kullanıcı adını 20+20 = 40 karakterden fazla girdiğimizde veya password’u 20 karakterden fazla girdiğimizde stack de yer alan admin hesabına ulaşabiliyoruz.

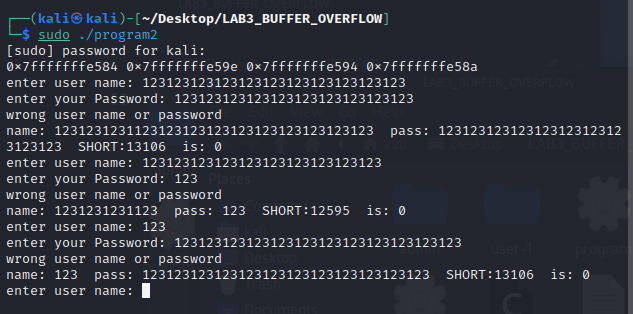
****

****Kendi yazdığımız kodda admine stack den ulaşılmaması için en alta yerleştirdik.

**Text

Description automatically generated**Ayrıca şifreyi hatalı girince yine giriş yapılamadığını gördük

Şifre doğru girildiğinde admin paneline ulaşılabilmektedir.

****

Şifre ve/veya Kullanıcı adı kendisine ayrılan stack belleğinden fazla girilse bile admin bölgesine ulaşılamamaktır. Ayrıca Şifre ve Kullanıcı adında belirli bir karakter sayısını aşmamaya zorlanarak da yine admin stack bölgesine erişimi engellenebilir.