

**NECMETTİN ERBAKAN ÜNİVERSİTESİ**

**BİLGİ GÜVENLİĞİ DERSİ DÖNEM PROJE ÖNERİSİ**

BAYRAM YARIM

18010011067

Dirty-COW Attack

Öğretici:

Dr. Öğr. Üyesi Alperen Eroğlu

Bilgisayar Mühendisliği Bölümü

KONYA, [2022]

1. **ÖZET**

Dirty-COW 2018 yılından önce oluşturulan tüm Linux çekirdeklerinde bulunan bir güvenlik açığıdır. Bu açıktan dolayı Android cihazları dahil tüm Linux tabanlı işletim sistemlerini, bilgisayarları, cihazları, telefonları etkilemektedir.

Bu projenin amacı Linux çekirdeğinde bulunan bu açıklıktan yararlanarak erişimi olmayan dosyalara erişmek ve üzerlerinde değişiklik yapmaktır.

Bu amaç doğrultusunda Linux işletim sistemi kurmak ve C Programlama dili ile yapılacak uygulama ile belirlenen açıklıktan yararlanarak gerekli işlemleri yapmak ve sonuçları göstermektir.

1. **PROBLEM TANIMI**

Linux çekirdeğinde bulunan bir güvenlik açığıdır. 2018 yılından önce oluşturulmuş sürümlerde bulunan Android cihazlar dahil tüm Linux tabanlı işletim sistemlerini etkileyen bir açıktır. Eski sürümleri kullanan bilgisayarlar, cihazlar, telefonlar vs.. bu açıktan dolayı halen savunması zayıftır.

Probleme gelirsek çekirdeğin bellek yönetiminde gerçekleşen bir durumdan dolayı saldırıya açıktır. Bellek yönetiminde yazma sırasında gerçekleşen bir açıktan dolayı hafızaya erişim sağlanarak dosya üzerinde erişim sağlanmasa dahi bilgileri değiştirerek dosya üzerinde değişiklik yapmaktadır.

1. **YÖNTEM**

Saldırı için Dirty-COW metodu uygulanacaktır. Bu metod ile erişim izni olmayan dosya üzerinde değişiklik yapmak. Uygulama için C programlama dilinden yararlanılacaktır. Yapılan uygulama ile saldırı yöntemi gerçekleştirilecektir.

1. **PROJE İŞ-ZAMAN PLANI**

Proje iş-zaman planında şu adımlar takip edilecektir. Projede içeriğin yapılması için linux işletim sistemi kurmak ve saldırı için gerekli yollar/aşamalar izlenecektir. Kurulan sistemde ilk denemeler için sadece okuma erişim izni olan bir dosya oluşturmaktır. Daha sonraki adımda ise saldırı yapacak kodu yazmak ve derleme aşamasıdır. Derlenen ve çıktısı alınan program ile ilgili dosyaya saldırı düzenlemektir.

1. **SONUÇ**

Sonuç olarak belirtilen veya belirlenen dosyaların içeriğine hafıza üzerinden erişim sağlayarak içeriğini değiştirerek istenilen saldırıları elde etmek istenmektedir.

1. **KAYNAKÇA**

https://seedsecuritylabs.org/Labs\_20.04/Software/Dirty\_COW/

https://seedsecuritylabs.org/Labs\_20.04/Files/Dirty\_COW/Dirty\_COW.pdf

https://en.wikipedia.org/wiki/Dirty\_COW

https://www.youtube.com/watch?v=kEsshExn7aE&t=714s&ab\_channel=LiveOverflow