**BİLGİ SİSTEMLERİ VE GÜVENLİĞİ**

**BİREYSEL RAPOR**

**170541047- Mert ÇEVİK**

Bilgi Sistemleri ve Güvenliği dersi kapsamında bizden istenilen zafiyet tarama konusunda Grup-1 içerisinde yapılan iş bölümünde ben ve takım arkadaşlarıma Grup-1 içerisinde Nessus Zafiyet tarama aracı ile çalışma yapma görevi düştü. Bu görev için takım arkadaşlarım olan Ece Doğan ve Abdullah Günan ile birlikte görev dağılımı yapıp başarılı bir çalışma ortaya çıkarmak yol haritamızı hazırladık.

**GRUP İçerisinde Yer Aldığım Görevler:**

**1)Araştırma**

Araştırma konularını belirleyerek konular üzerinde görev dağılımında bulunduk ve araştırma aşamasına başladık. Araştırma süreci içerisinde elde ettiğimiz bulguları ortak olarak kullanmış olduğumuz sanal görüşme ortamı olan Discord uygulaması içerisinde topladık ve araştırmalarımız üzerinde toplantılar yaparak fikir alış-verişinde bulunduk.

**2)Zafiyet Tarama**

Zafiyet tarama için öncelikle Kali işletim sistemini Windows bilgisayarımıza kurmak adımını gerçekleştirdik. Kali işletim sisteminin başarılı bir şekilde kurulmasından sonra Nessus Zafiyet tarama aracını başarılı bir şekilde yüklemek için araştırmalarımızı yapıp konsol üzerinden başarılı bir şekilde yükleme işlemini tamamladık. Ardından uygun host kullanarak programı açtık ve zafiyet tarama programını keşfetmeye ve bu süreçte nasıl başarılı bir tarama işlemi yapabileceğimizi öğrenmek için yol haritası belirledik.

Üzerinde zafiyet tarama çalışması yapmak için hocamızın önerdiği 3 farklı Ticaret ve Sanayi Odası içerisinde Muş TSO’yu seçtik ve ardından kendilerine ait <https://www.mustso.org.tr/> sitesi içerisinde sistem taramalarımızı başlattık.

Tarama sürecinde site üzerinde Basic Network, Advanced ve Malware taramalarını kullanarak sistemde açık olup olmadığını bulmaya çalıştık. Çalışmalarımız neticesinde sisteme ait 1’i yüksek 3’ü orta derecede sistem açıkları ile karşılaştık. Elde ettiğimiz bu verileri değerlendirip bir rapor haline getirdik.

**3)Raporlama**

Muş TSO’ya ait sistemde Nessus zafiyet tarama aracı ile yaptığımız tarama sonuçlarını risk durumuna göre sıralayarak bu açıklar üzerinde çeşitli araştırmalar yaptık. Bu araştırmalarımız sonucunda sistemde bulunan bu zafiyetlerin neden kaynaklandığını ve nasıl önlemler alınarak düzeltilebileceğini rapor haline getirdik. Bu raporu hem Grup-1 içerisinde hemde Grup 1-2-4 Nessus gruplarının birleşerek oluşturduğu rapora ekledik.

**4)Sunum**

Nessus zafiyet tarama aracı ile Muş TSO’ya ait resmi web sitesinde yapmış olduğumuz zafiyet tarama işlemine ait bilgileri rapor haline getirerek <https://debsis.firat.edu.tr> platformunda canlı ders içeriğinde sunum olarak paylaştık. Ardından ekip olarak GitHub hesaplarımızda dönem içerisindeki grup çalışmalarımıza ait görüntüleri, araştırma aşamalarını ve düzenlediğimiz son raporu paylaştık.