**KOCAELİ ÜNİVERSİTESİ**

**MÜHENDİSLİK FAKÜLTESİ**

**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

**ARAŞTIRMA PROJESİ**

**KABLOSUZ AĞLARA İZİNSİZ GİRİŞ YAPAN**

**CİHAZLARIN MAKİNE ÖĞRENMESİ YOLU İLE**

**TESPİTİ**

**MUSTAFA KARA**

**5,2 cm**

**MEHMET FATİH ALICI**

ÖZET

Bilgisayar ağlarına yapılan izinsiz girişler ve tehditler, günümüzde oldukça yaygın olarak karşılaşılan güvenlik sorunlarıdır. Bu tür izinsiz girişler, bir kişinin veya bir grup kişinin, bir ağa giriş yapması veya ağdaki bilgiye ulaşması için izin almadan ağa giriş yapmasına denir. Bu tür izinsiz girişler, ağda bulunan bilgilere erişim, ağı kullanıma uygun olmayan yöntemlerle kullanım, ağda bulunan bilgileri değiştirme veya silme gibi faaliyetleri de içerebilir.

Tehditler, bilgisayar ağlarını ve bilgisayarları hedef alan, güvenlik açıklarını kullanarak ağlara ve bilgisayarlara zarar veren saldırılardır. Tehditler, birçok farklı şekilde ortaya çıkabilir ve farklı amaçlar için kullanılabilir. Örneğin, bir hacker, bir ağa izinsiz giriş yaparak, ağdaki bilgilere erişmek isteyebilir. Diğer bir tehdit türü olarak, bir malware (kötü amaçlı yazılım) ağdaki bilgisayarlara bulaşarak, bu bilgisayarları kontrol etmeye çalışabilir. Bu saldırıların arkasında maddi zarar veya elde edilmeye çalışılacak bir kazanç sebebiyle de yapılabilir.

Günümüzde, bilgisayar ağlarına yapılan izinsiz girişler ve tehditlerle mücadele etmek için birçok farklı yöntem ve araç kullanılmaktadır. Örneğin, ağ güvenliğini artırmak için güvenlik duvarı (firewall) ve güvenlik yazılımları (antivirus yazılımları) kullanılabilir. Ayrıca, kullanıcıların ağa giriş yaparken kullandıkları parolaların güçlü olması, ağa izinsiz girişlerin önüne geçebilir. Ayrıca, ağda bulunan bilgisayarların ve diğer cihazların güncel olması, tehditlerden korunmada önemli bir rol oynar.

Bu projede amaç daha spesifik olarak kablosuz ağlara yapılacak izinsiz giriş veya denemeleri yapan cihazları tespit yöntemlerinden biri olan makine öğrenmesi yolu ile veri kümeleri paylaşan sitelerden veya kuruluşlardan bu bilgileri kullanarak analizini sağlayıp sonuca ulaşmak hedeflenmektedir.

**Abstract**

Illegal access to computer networks and threats are common security problems encountered today. Such illegal access refers to a person or group of people accessing or attempting to access a network without permission. This can include accessing information on the network, using the network in an unauthorized manner, altering or deleting information on the network.

Threats are attacks that target computer networks and computers, using vulnerabilities in security to cause harm to networks and computers. Threats can take many forms and can be used for various purposes. For example, a hacker may attempt to illegally access a network to access information on it. Another type of threat is malware, which can infect computers on a network and attempt to control them. These attacks may be carried out for the purpose of causing financial damage or seeking a gain.

There are many methods and tools used to combat illegal access to computer networks and threats. For example, firewall and security software (antivirus software) can be used to increase network security. Strong passwords for users accessing the network can also help prevent illegal access. Keeping computers and other devices on the network up to date is also important in protecting against threats.

This project specifically aims to use machine learning to identify devices attempting illegal access or attempts on wireless networks, using data from data set sharing sites or organizations, and analyzing this information to reach a conclusion.

1. **GİRİŞ**

Kablosuz ağlara yapılan izinsiz girişler, günümüzde yaygın olarak karşılaşılan bir güvenlik sorunudur. Özellikle, kablosuz ağların yaygın kullanılmasıyla birlikte, bu tür izinsiz girişlerin sayısı da artmıştır. Kablosuz ağlara yapılan izinsiz girişler, ağa izinsiz giriş yaparak bilgiye erişme, ağı kullanıma uygun olmayan yöntemlerle kullanma ve ağdaki bilgileri değiştirme veya silme gibi faaliyetleri içerebilir.

Kablosuz ağlara yapılan izinsiz girişler, ağların güvenliğini tehdit eder ve ağdaki bilgilere ve cihazlara zarar verebilir. Bu nedenle, kablosuz ağlara yapılan izinsiz girişlerin önlenmesi ve mücadele edilmesi küresel anlamda şirketler, devletler, özel kurum ve kuruluşlar için gözden geçirilmesi gereken bir sorundur.

**2. KULLANILAN YAYGIN YÖNTEMLER**

Kablosuz ağlara yapılan izinsiz girişlerin tespitini yakalamak için, aşağıdaki yöntemler ve teknolojiler kullanılabilir.

**2.1.1 Güvenlik Duvarı (Firewall)**

Güvenlik duvarı, bir ağın giriş ve çıkışını denetleyen bir araçtır ve izinsiz girişleri engellemek için kullanılır. Güvenlik duvarı, ağ üzerinden gelen ve giden tüm verilere bir filtre uygular ve belirli kurallara uygun olmayan verilere izin vermez. Bu sayede, izinsiz girişler engellenir.

**2.1.2 Güvenlik Yazılımları (Antivirus Yazılımları)**

Güvenlik yazılımları, bilgisayar ve ağları kötü amaçlı yazılımlardan (malware) korur. Bu yazılımlar, bilgisayar ve ağlarda bulunan dosyaları tarar ve kötü amaçlı yazılım tespit ettiklerinde, bunları temizler veya engeller. Böylece, ağ ve bilgisayarların güvenliği sağlanır ve izinsiz girişler engellenir.

**2.1.3 Parola Güçlendirme**

Kullanıcıların ağa giriş yaptıklarında kullandıkları parolaların güçlü olması, izinsiz girişleri önleyebilir. Örneğin, parolaların uzunluğunun artırılması ve parolalarda rakam, sembol ve büyük/küçük harflerin kullanılması, parolaların güçlenmesine yardımcı olabilir.

**2.1.4 İzin Verilen Cihazlar Listesi**

Bir ağın izinsiz girişlerini önlemek için, ağa sadece belirli cihazların girişine izin verilebilir. Bu şekilde, ağa sadece izin verilen cihazlar tarafından erişim sağlanabilir ve diğer cihazların ağa girişine izin verilmez.

**2.1.5 Güncel Sistemler**

Ağda bulunan bilgisayarların ve diğer cihazların güncel olması, tehditlerden korunmada önemli bir rol oynar. Örneğin, bilgisayarlarda ve diğer cihazlarda bulunan işletim sistemlerinin güncel olması ve güvenlik güncellemelerinin yüklü olması, ağ ve bilgisayarların güvenliğini artırır ve izinsiz girişleri engeller. Ayrıca, ağda bulunan cihazların sistem yazılımlarının (örneğin, tarayıcı yazılımları, sürücü yazılımları) güncel olması da aynı şekilde önemlidir.

**2.1.6 İzleme ve Anlık Tespit Sistemleri**

Ağ üzerinde anlık olarak izleme ve tespit sistemleri kullanılabilir. Bu sistemler, ağ üzerinde belirli bir davranışın tespit edildiğinde, anlık olarak uyarı mesajları göndererek izinsiz girişleri önler.

**2.1.7 Makine Öğrenimi (Machine Learning)**

Makine öğrenimi, veri setlerini kullanarak, sistemlerin kendisini öğrenmesine ve bu öğrenmeleri kullanarak, izinsiz girişleri tespit etmesine yardımcı olabilir. Bu teknolojinin kullanımı, izinsiz girişlerin tespit edilmesinde önemli bir rol oynayabilir.

**3.VERİ KÜMESİ**

UNSW-NB15, ağ güvenliği konusunda yapılan bir araştırmada kullanılan bir data setidir. Bu data set, New South Wales Üniversitesi'nden (UNSW) geliştirilmiştir ve ağ girişlerinin tespiti gibi güvenlik sorunlarının çözümünde kullanılmak üzere tasarlandı.

UNSW-NB15 data seti, bir ağa yapılan 9 cinsiyet ayrımı olmayan, 49 başarılı ve başarısız ağ girişini içeren 4.8 milyon kayıt içerir. Bu kayıtlar, ağ girişlerini tespit etmek için kullanılabilecek özellikleri (örneğin, paketlerin zaman damgası, protokol türü, paket boyutu gibi) içerir. UNSW-NB15 data seti, ağ girişlerinin tespiti için kullanılan makine öğrenimi modellerinin eğitimi ve değerlendirilmesinde yaygın olarak kullanılmaktadır.

UNSW-NB15 data seti hakkında daha fazla bilgi için aşağıdaki referansı inceleyebilirsiniz:

Moustafa, N., Ayad, A., ve Guizani, M. (2015). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data). arXiv:1608.02576 [cs.CR]. https://arxiv.org/abs/1608.02576

**3.1 VERİ SETİNİN SINIFLARI**

**3.1.1 İÇERDİĞİ BİLGİLER**

**3.1.2 UYGULANAN İŞLEMLER (?)**

**3.2 MAKİNE ÖĞRENİMİ**

**3.2.1 MAKİNE ÖĞRENİMİ MODELLEMESİ- DETAYLANDIRILMASI**

**3.1.2**

**4. PROJE PLANLAMASI**

**5.YÖNTEM**

**6. İLGİLİ ÇALIŞMALAR**

**7.KAYNAK**