BÖLÜM 2

AĞ GÜVENLİĞİ

ANAHTAR KAVRAMLAR

Ağ Yönetim Cihazları, Güvenlik Açıkları, Ağ Erişim Güvenliği, Saldırı Türleri, Ağ Güvenlik Ekipmanları

ÖĞRENME HEDEFLERİ

1. Bilgisayar ağlarının yönetiminde kullanılan cihazları tanır
2. Ağ cihazlarının zayıf yönlerini açıklar
3. Ağlara yönelik yapılacak saldırıları bilir
4. Ağ cihazlarını yönetmek için erişim yöntemlerini açıklar
5. Anahtarlama saldırılarını açıklar
6. Yönlendirme saldırılarını açıklar
7. Kablosuz ağlardaki zayıflıkları açıklar
8. Güvenlik açıkları için çözüm önerilerini açıklar
9. Ağ güvenliği için kullanılan donanımları bilir

İKİNCİ BÖLÜM

GİRİŞ

Bilgisayar ağları, bilgisayarlar, ağ cihazları ve diğer iletişim aygıtları arasında veri ve kaynak paylaşımını mümkün kılan bağlantılı bir yapıdır. Bu ağlar, bilgisayarların, yazıcıların, dosya sunucularının, internet erişiminin ve diğer kaynakların paylaşılmasını sağlar. Ayrıca, bilgi ve verilerin standartlar dahilinde bir noktadan diğerine iletilmesine olanak tanır.

Bilgisayar ağlarının temel amacı, iletişim ve veri transferi sağlamaktır. Bu ağlar, farklı yerlerdeki kullanıcılar arasında veri ve bilgi paylaşımını kolaylaştırarak işbirliği yapmayı, kaynakları etkili bir şekilde kullanmayı ve iletişimi artırmayı mümkün kılar. Ayrıca, internet gibi geniş çaplı ağlar aracılığıyla dünya genelindeki bilgisayarları birbirine bağlar.

Bilgisayar ağları genellikle kablolu (Ethernet, fiber optik vb.) veya kablosuz (Wi-Fi, Bluetooth vb.) bağlantılar üzerinden gerçekleştirilir. Bu ağlar, farklı büyüklüklerde olabilir; küçük ölçekli yerel alan ağlarından (LAN) büyük ölçekli geniş alan ağlarına (WAN) kadar çeşitli ölçeklerde olabilirler. Ayrıca, bilgisayar ağları farklı tiplerde de olabilir. Örneğin, internet servis sağlayıcıları tarafından sağlanan genel erişimli ağlar, özel şirket ağları veya devlet kurumları için kurulan özel ağlar gibi farklı türlerde ağlar bulunmaktadır.

Bilgisayar ağları, günümüzde bireyler, işletmeler, kurumlar ve kuruluşlar arasında bilgi alışverişini sağlayan kritik bir teknoloji haline gelmiştir. Bilgisayar ağları günlük yaşamda ve endüstriyel alanlarda birçok farklı yerde bulunur. *Evlerde kullanılan Wi-Fi ağı*, bilgisayar ağlarının en yaygın ve temel örneklerinden biridir. Bu ağlar, bilgisayarlar, akıllı telefonlar, tabletler ve diğer cihazlar arasında internet erişimi sağlar. *Yerel Alan Ağları (LAN),* işyerlerindeki bilgisayarlar ve diğer cihazlar, ofis içinde veri paylaşımı ve işbirliği yapabilmek için yerel

ağlar üzerinde bağlanır. *Okul ve Üniversite Ağları*, öğrencilere ve öğretmenlere kaynakları paylaşma, öğrenme yönetim sistemlerine erişim ve online kaynaklara bağlanma olanağı sunan geniş bilgisayar ağlarına sahiptir. *Cep Telefonu Ağları, m*obil telefonlar, cep telefonu baz istasyonlarına bağlanarak ses ve veri iletişimini mümkün kılan kablosuz ağlar üzerinden çalışır. *Kütüphane ve Açık Alanlar,* kamu alanlarındaki bilgisayarlar ve internet erişimi, kullanıcılara ücretsiz veya ücretli olarak hizmet vermek amacıyla kurulmuş ağlara bağlıdır. *Büyük Veri Merkezleri*, büyük teknoloji şirketleri ve araştırma kuruluşları, büyük veri analizi, bulut hizmetleri ve diğer yüksek performanslı hesaplama görevlerini gerçekleştirmek için karmaşık bilgisayar ağları kullanır. *Telekomünikasyon Ağları*, telefon ve internet hizmetleri sağlayan şirketler, dünya genelinde geniş alan ağları kurar ve yönetir. Bu ağlar, kara kabloları, deniz altı kabloları ve uydu bağlantıları gibi farklı teknolojileri içerir.

Bu örnekler, bilgisayar ağlarının geniş bir uygulama yelpazesi olduğunu gösterir. Günlük hayatımızda gerçekleştirdiğimiz birçok dijital işlem ağlar sayesinde sağlanır ve modern yaşamın birçok yönünde kritik bir rol oynar.

1. AĞ CİHAZLARI

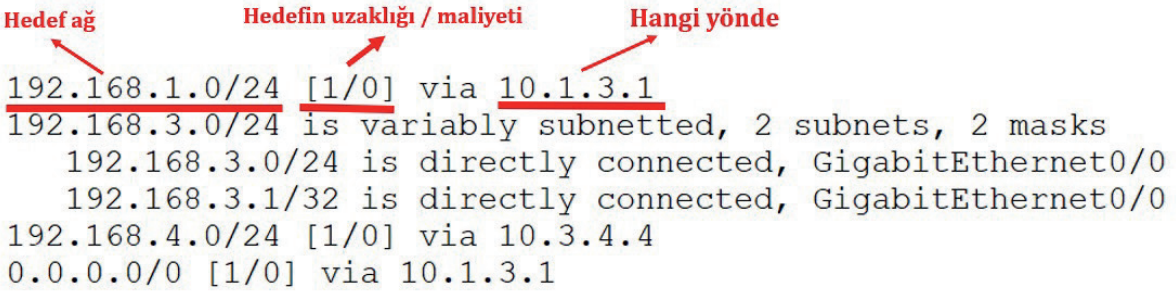
Bilgisayar ağlarında, uç cihazlar ve aracı cihazlar olmak üzere iki tür cihazların varlığından söz edilebilir. Uç cihazlar, verilerin genelde insanlarla etkileşime girdiği, PC, laptop, IP telefon, IP yazıcı, mobil telefon, tablet, sunucu gibi donanımları kapsar. Aracı cihazlar ise, verinin bir uç cihazdan diğerine doğru ve güvenli bir şekilde aktarılmasını sağlayan cihazlardır. Yönlendirici (router), anahtar (switch), kablosuz erişim noktası (Access point) ve güvenlik duvarı (firewall) bu kategoride yer alan cihazlara birer örnektir.

Ağ güvenliği söz konusu olduğunda hem uç cihazların hem de aracı cihazların güvenliğinin sağlanması bir zorunluluktur. Saldırılar ve tehditler sadece son kullanıcıların etkileşim halinde bulunduğu uç cihazlara değil, aracı cihazlara da yapılmaktadır. Bu tür cihazlara yapılan saldırılar, daha geniş bir yüzeyde bir zarara neden olabilir. Bu nedenle güvenlik için öncelikle bu cihazların kullanım amaçları, nasıl çalıştıkları ve çalışma prensipleri incelenmelidir.

Yönlendirici (Router): Yönlendiriciler, farklı ağlar arasında veri paketlerini yönlendirir. İki veya daha fazla ağ arasında veri iletimi sağlar (Şekil 1). IP adreslerini kullanarak paketleri doğru hedefe yönlendirir (Peterson & Davie, 2003).

Şekil 1. Örnel bir yönlendirici cihazının arka panel görüntüsü

Yönlendiriciler, hedef ağlara hangi yolla ulaşılacağını tanımlayan bilgiler barındırır. Bu bilgiler, bir IP paketinin doğru rotaya ulaşılmasını sağlayan ve cihazın belleğinde tutulan ve *yönlendirme tablosu* denen bir tabloda yer alır. Şekil 2'de örneği gösterilen bu tabloda yer alan bilgiler, ağ yöneticisi tarafından elle girilebildiği gibi (statik yönlendirme), yönlendiriciler arasındaki bilgi alışverişi sonucunda otomatik olarak da (dinamik yönlendirme) girilebilir.



Şekil 2. Yönlendirme tablosu örneği

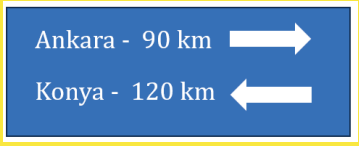
Yönlendirme tablosuna yapılacak bir saldırı sonucunda IP paketleri yanlış yerlere yönlendirilebilir, paketler saldırganların eline geçebilir, bazı durumlarda paketlerin içeriği okunabilir. Böylesi bir durumda, bu tür istismar edilmiş yönlendiriciyi kullanan tüm bilgisayarların ve uç cihazların iletişimine güvenilmez. Uç cihazlarda ne kadar güvenlik sağlanırsa sağlansın, hatalı bir yönlendirme istenmeyen durumlara neden olabilir.

Saldırganlar, yönlendiriciye erişim sağlayarak yönlendirme tablolarını değiştirilebilir, eksik yapılandırılmış dinamik yönlendirme protokollerindeki açıklardan faydalanarak yönlendirme tablosunu bozabilir, iletişimi farklı yere yönlendirebilir, verileri manipüle edebilir (*man in the middle attack*) ve çok farklı amaçlar doğrultusunda zararlı eylemlerini gerçekleştirebilir.

Ev ağı gibi küçük ölçekli ağlarda yönlendiriciler genellikle uç cihazlara IP adresi atama görevini (DHCP sunucu) de yürütürler. Yine yönlendiricilere yapılan bir manipülasyon sonucu, son kullanıcı cihazlarının hatalı IP parametrelerini (ağ geçici adres, DNS gibi) alması sağlanabilir. Benzer şekilde hatalı IP parametrelerine sahip olan bir cihazın güvenli olduğundan bahsedilemez, trafiklerine güvenilemez.

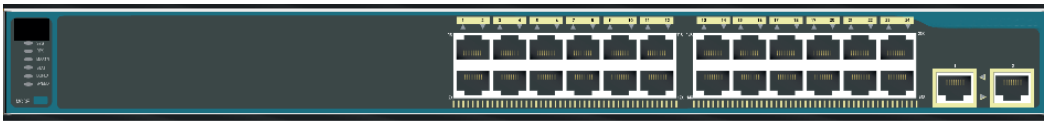
GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Yönlendiricilerin kullandıkları yönlendirme tablosu, karayollarındaki şehirlerin uzaklıklarını ve gidiş yönünü gösteren tabelalara benzetilebilir.



Bir şehirden uzak bir şehre gittiğinizde, kavşaklardaki tabelalara göre hedef şehre nasıl gideceğinizi karar verirsiniz. Yönlendirme tabloları da benzer şekilde kullanılır. IP paketleri yönlendiricilere ulaştıklarında, yönlendiriciler hedef IP adresine göre hangi arayüzden paketi göndereceklerini belirlerler. Bu işlem yol boyunca tüm yönlendiricilerde yapılır.

Anahtar (Switch): Anahtarlar, bilgisayarlar gibi uç cihazlar arasında doğrudan iletişimi sağlayan donanımlardır. Anahtarda yer alan portlara bağlı olan bilgisayarlar arasındaki veri iletimini daha hızlı ve etkili hale getirir (Şekil 3). MAC (media access control) adreslerini kullanarak paketleri doğru portlara yönlendirir (McDonald, 2013).



Şekil 3. Bir anahtarın görünümü

Anahtarlar, MAC tablosu olarak adlandırılan bir tabloyu bellekte tutarlar. Bu tabloda, hangi cihazın hangi porta bağlı olduğu fiziksel MAC adresleri üzerinden tutulur. Ayrıca bu tabloda, bir uç cihazın anahtar üzerindeki mantıksal izole grupların (VLAN) hangisine dahil olduğu bilgisi de yer alır. Bu bilgilerin saldırı sonucunda manipüle edilmesi, o anahtara bağlı olan tüm cihazların güvenliğini etkiler. Anahtarlar ile ilgili diğer bir önemli konu, son kullanıcı cihazlarının altyapı ile ilk temas noktasını oluşturmasıdır. Bu nedenle anahtarlar genelde en zayıf halkalardan biri olarak varsayılır ve tehdit aktörlerinin hedefindedirler. Anahtara yönelik yapılan saldırılar çok geniş bir yelpazede olabildiğinden ayrı bir başlıkta ele alınacaktır.

Modem (Modulator-Demodulator): Modemler, bilgisayar verilerini analog sinyallere dönüştürerek internet hizmet sağlayıcısının ağına gönderebilir ve aynı zamanda gelen analog sinyalleri dijital verilere dönüştürerek bilgisayar tarafından anlaşılabilir hale getirir. Bu, evlerimizdeki cihazların internete bağlanmasını sağlar(Shinder, 2001).

Access Point (AP): Kablosuz ağlarda kullanılan access point'ler (erişim noktaları), kablolu ağa bağlı cihazların kablosuz olarak ağa erişimini sağlar (Şekil 4). Wi-Fi sinyalleri yayarak kablosuz bağlantıları mümkün kılar(KUNDU, 2008).

Şekil 4. Access Point kablosuz bağlantı sağlar

Access Point'ler radyo frekanslarını kullanarak kablosuz iletişim sağladıkları için saldırganlar için potansiyel bir atak yüzeyidir. AP'nin kapsama alanında bulunan her cihaz teorik olarak bu sinyalleri yakalayabilir. Bu durum ciddi bir güvenlik riski oluşturur. Kablosuz ağlara yönelik yapılan saldırılar ayrı bir başlıkta ele alınacaktır.

Firewall (Güvenlik Duvarı): Güvenlik duvarları, ağ trafiğini denetler ve istenmeyen erişimleri, saldırıları veya veri trafiğini engeller. Bilgisayar ağına gelen ve ağdan çıkan verileri kontrol ederek izin verilen trafikleri geçirirken zararlı trafikleri engeller(Miller, n.d.; Stephen et al., 1996).

Bu bölümde kısaca açıklanan cihazlar, bir bilgisayar ağının temel bileşenleridir ve birlikte çalışarak bilgisayarlar arasında iletişimi ve veri paylaşımını mümkün kılarlar. Cihazlar, belirli görevleri yerine getirirken genellikle belirli protokolleri ve standartları esas alırlar, böylece veri iletimi güvenli ve etkili olur.

2. AĞ CİHAZLARINDAKİ ZAFİYETLER

Bir önceki başlıkta özetle açıklanan ağ cihazlarında çeşitli güvenlik açıkları bulunabilir. Bu açıklar kötü niyetli saldırganların ağa erişmesine veya ağdaki verilere zarar vermesine olanak tanır. Bu tür güvenlik açıkları, ağ cihazlarının yazılımında, çalışma prensibinde, yapılandırmasında veya donanımında olabilir. Ağ cihazlarındaki bazı yaygın güvenlik açıkları aşağıda ele alınmıştır.

Yetersiz Parolalar: Varsayılan parolaların değiştirilmemesi veya zayıf parolaların kullanılması, saldırganların kolayca cihazlara erişim sağlamasını mümkün kılar.

Yazılım Güncellemelerinin İhmal Edilmesi: Ağ cihazlarının işletim sistemlerinde veya yazılımında bulunan güvenlik açıklarının zamanında düzeltilmemesi, saldırılara açık kapı bırakabilir.

Zayıf Şifreleme: Kablosuz ağlarda zayıf veya kırılabilir şifreleme algoritmalarının kullanılması, verilerin güvenliğini tehlikeye atabilir.

DoS (Denial of Service) Saldırıları: Ağ cihazlarına yoğun trafiği yönlendirerek veya aşırı hizmet talepleriyle ağ kaynaklarını tüketerek cihazları hizmet dışı bırakma saldırılarıdır.

Fiziksel Erişim: Fiziksel olarak cihazlara erişim sağlanması, cihazlara zarar verme, yazılım değiştirme veya doğrudan verilere erişim sağlama gibi tehditleri beraberinde getirebilir.

Kötü Tasarlanmış Güvenlik Politikaları: Yetersiz güvenlik politikaları veya erişim kontrolü, yetkisiz erişimlere olanak tanıyabilir.

3. AĞ CİHAZLARINA ERİŞİM GÜVENLİĞİ

Ağ cihazlarına yapılandırma amacıyla erişim sağlamak için genellikle bant içi ve bant dışı olarak adlandırılan iki yöntem kullanılır. Bant içi erişimde Telnet, SSH, SNMP, HTTP/s gibi protokoller kullanılırken, bant dışı erişimde cihaza fiziksel olarak konsol kablosu ile erişilir(Odom, 2004). Aşağıda bu erişim yöntemleri açıklanmıştır.

Konsol Bağlantısı: Ağ cihazlarına fiziksel olarak yaklaşarak, seri konsol kablosu aracılığıyla doğrudan konsol portundan erişim sağlanabilir.

SSH (Secure Shell): SSH, güvenli bir şekilde uzaktan erişim sağlamak için kullanılan bir protokoldür. Kullanıcılar, SSH istemcisi kullanarak ağ cihazlarına şifrelenmiş bir bağlantı kurabilirler.

Telnet: Telnet, ağ cihazlarına uzaktan erişim sağlamak için kullanılan bir protokoldür, ancak veriler şifrelenmez ve güvensizdir. Güvenlik açısından önerilmez, ancak bazı eski cihazlarda hala kullanılabilir.

Web Tabanlı Arayüzler: Ağ cihazlarının çoğu, web tarayıcıları üzerinden yapılandırılabilir. Bu yöntem, kullanıcıların cihazlarına tarayıcıları aracılığıyla erişim sağlamalarını sağlar. Ev ağlarında kullanılan ADSL modem router yapılandırmalarında genelde bu yöntem kullanılır.

• Bu erişim yöntemleri kullanılırken, bazı güvenlik riskleriyle karşılaşılabilir.

• Zayıf veya varsayılan parolalar kullanıldığında, saldırganlar erişim sağlamak için brute-force veya şifre tahmini saldırıları gerçekleştirebilirler.

• Cihazlarda güncel olmayan yazılımların kullanılması, bilinen güvenlik açıklarını içerebilir.

• Güvenlik duvarları veya diğer güvenlik önlemleri yanlış yapılandırıldığında, yetkisiz erişim riski artar.

• Kötü amaçlı yazılımlar, ağ cihazlarına bulaşabilir ve saldırganlara uzaktan erişim sağlama imkanı tanır.

• Fiziksel olarak erişim sağlanabilen cihazlar, yetkisiz kişilerin fiziksel erişim sağlaması riskini taşır.

Bu güvenlik risklerini azaltmak ve ağ cihazlarına yapılandırma erişimini güvenli hale getirmek için çeşitli güvenlik çözümleri uygulanabilir. Aşağıda bu çözümler öneriler olarak yer almaktadır.

Güçlü Parolalar ve Kimlik Doğrulama: Güçlü ve karmaşık parolalar kullanın. İki faktörlü kimlik doğrulamayı (2FA) etkinleştirin.

Yazılım Güncellemeleri: Cihazlarınızdaki yazılımları ve işletim sistemlerini düzenli olarak güncelleyin.

Güvenlik Duvarları ve İzinler: Güvenlik duvarlarını doğru şekilde yapılandırarak sadece gerekli portları ve hizmetleri açık bırakın. İzinleri sıkı bir şekilde denetleyin.

Fiziksel Erişimi Kontrolü: Cihazlara fiziksel erişimi kısıtlamak için güvenlik önlemleri alın, örneğin erişim kontrol kartları veya biyometrik kimlik doğrulama sistemi kullanabilirsiniz.

Kötü Amaçlı Yazılım Taraması: Düzenli olarak kötü amaçlı yazılım taramaları yaparak cihazları temiz tutun.

Güvenli İletişim Protokolleri: Uzaktan erişim için SSH gibi güvenli iletişim protokolleri kullanın. Telnet gibi güvensiz protokollerden kaçının.

Bu tedbirler ve öneriler, ağ güvenliğini artırmak için alınabilecek önemli adımlardır. Güvenlik, sürekli bir süreçtir ve değişen tehditlere karşı sürekli olarak güncellenmelidir.

4. AĞ SALDIRILARI

Ağlara yönelik yapılan saldırılar, çeşitli yöntemlerle gerçekleştirilebilir ve genellikle amaçlarına, kullanılan tekniklere ve etkiledikleri bileşenlere göre sınıflandırılırlar.

4.1. Keşif Saldırıları

Keşif (Reconnaissance) saldırıları, bir saldırganın hedef ağ veya sistem hakkında bilgi toplamak için gerçekleştirdiği ön saldırı aşamasıdır(Standard ve diğerleri., 2013). Bu tür ataklar, saldırganın hedef ağın yapılanması, güvenlik zayıflıkları, kullanılan yazılımlar ve sistem yöneticileri gibi bilgilere erişmesine yardımcı olur. Bu bilgiler daha sonra daha sofistike saldırılar planlamak ve gerçekleştirmek için kullanılır. Keşif saldırıları aktif ve pasif olmak üzere iki ana kategoride değerlendirilebilir (Zaripova & Ugli, 2021).

Pasif Keşif: Bu tür keşifte saldırganlar, hedef ağ veya sistemle doğrudan etkileşime girmek yerine kamuya açık kaynaklardan, internet sitelerinden, sosyal medya hesaplarından ve diğer erişilebilir bilgilerden bilgi toplarlar. Bu bilgiler genellikle IP adresleri, alan adları, e-posta adresleri, çalışan bilgileri ve şirket yapısı gibi genel bilgileri içerir.

Aktif Keşif: Bu tür keşifte saldırganlar, doğrudan hedef ağ veya sistemle etkileşime girer. Bu, port taraması, zayıf nokta taraması ve ağ üzerinde gezinme gibi teknikleri içerebilir. Bu saldırılarla saldırganlar, hedef sistemde çalışan servisleri, açık portları ve potansiyel güvenlik açıklarını belirleyebilir.

Keşif saldırıları, ağ güvenliği açısından ciddi bir tehdit oluşturur, çünkü saldırganlar hedef sistemin zayıf noktalarını tespit edip daha sofistike saldırılar planlayabilirler. Bu tür atakları önlemek veya azaltmak için ağ güvenliği uzmanları, güçlü şifreler kullanma, güvenlik yamalarını düzenli olarak uygulama, ağ trafiğini izleme ve güvenlik duvarları gibi güvenlik önlemlerini uygulayarak sistemi koruma stratejileri geliştirirler.

4.2. Erişim Saldırıları

Erişim (Access) atakları, bir saldırganın yetkisiz şekilde bir sistem, ağ veya hizmete erişim sağlama girişimlerini ifade eder. Bu tür saldırılar, sistemlere veya verilere izinsiz erişmeye çalışmak, yetkisiz hakları kullanarak gizli bilgilere ulaşmak veya hedef sistemi kontrol etmeye çalışmak amacıyla gerçekleştirilir. Erişim atakları, çeşitli yöntemlerle gerçekleştirilebilir ve ağ güvenliğini tehdit eden önemli bir kategori olarak kabul edilir. Bazı yaygın erişim atakları aşağıda açıklanmıştır:

Brute Force Saldırıları: Brute force saldırısı, oturum açma bilgilerini veya parolaları doğru kombinasyonu bulana kadar sürekli olarak deneyerek bir sistem veya hesaba yetkisiz erişim sağlamayı amaçlayan bir tür saldırıdır. Bu tür saldırılar, saldırganın genellikle oturum açma formu veya servisi üzerindeki parola deneme sınırını aşmasını engelleyen güvenlik önlemlerine karşı bir yöntemdir. Brute force saldırıları, şifreleme kullanılan sistemlerde şifre kırma amacı taşırlar. Saldırgan, genellikle kullanıcı adı ve parola kombinasyonlarını sürekli olarak deneyerek, doğru kombinasyonu bulana kadar sistemi veya hesabı hedef alır. Bu saldırı türü, çok sayıda farklı kombinasyonu hızlı bir şekilde deneyebilen yazılım veya yazılım araçları kullanılarak gerçekleştirilebilir (Standard ve diğerleri., 2013).

Brute force saldırılarına karşı korunmak için, kullanıcılar karmaşık ve güçlü parolalar kullanmalı, aynı kullanıcı adı ve parola kombinasyonunu farklı hesaplarda kullanmaktan kaçınmalı ve sistem yöneticileri başarısız oturum açma denemelerini tespit edip engellemek için güvenlik önlemleri uygulamalıdır. Bu önlemler, oturum açma denemelerinin belli bir sıklığı veya süresi içinde sınırlanması, güçlü parola politikaları ve çift faktörlü kimlik doğrulama gibi güvenlik önlemlerini içerebilir.

Password Guessing (Parola Tahmini): Saldırgan, kullanıcıların genellikle kullanabileceği parolaları tahmin ederek giriş yapmaya çalışır. Bu tahmin doğru olarak yapıldığında hedefe erişim sağlanır.

Credential Stuffing: Saldırgan, başka bir hizmette sızdırılan kullanıcı adı ve parola kombinasyonlarını kullanarak aynı kullanıcıların diğer hesaplarına girmeye çalışır. İnsanların genelde aynı parolaları birden fazla hesapta kullanma eğiliminden yararlanır.

Session Hijacking (Oturum Kaçırma): Oturum kaçırma, bir kullanıcının oturumunu (session) ele geçirip, yetkisiz erişim sağlama amacı taşıyan bir saldırı türüdür. Bu tür saldırılar, genellikle çerez (cookie) tabanlı oturum yönetimi kullanan web sitelerinde gerçekleşir. Bir kullanıcının oturumunu ele geçirme süreci aşağıda belirtilen yöntemler ile gerçekleşebilir.

• Session Sniffing (Oturumun Ele Geçirilmesi): Saldırgan, ağdaki verileri izleyerek (sniffing) kullanıcının oturum kimliği (session ID veya cookie) gibi bilgileri ele geçirir. Bu bilgi, kullanıcının web sitesine kimlik doğrulamasız erişim sağlayan bir anahtardır.

• Cookie Theft (Çerezlerin Çalınması): Kullanıcının tarayıcısında saklanan çerezler, oturumu koruyan bir tür anahtardır. Eğer saldırgan kullanıcının tarayıcısındaki çerezleri ele geçirebilirse, bu çerezleri kullanarak kullanıcının oturumunu taklit edebilir ve yetkisiz erişim sağlayabilir.

• Cross-Site Request Forgery- CSRF (Çapraz Site İstek Sahteciliği): Saldırgan, kullanıcıyı, oturumu ele geçirilmiş bir siteye yönlendiren ve kullanıcının farkında olmadığı istekleri gönderen zararlı bir siteye yönlendirebilir. Kullanıcı, güvenilir bir sitede oturum açıkken, bu CSRF saldırısı ile oturumu ele geçirilmiş bir siteye istekler gönderebilir.

Saldırgan, ele geçirdiği oturumu kullanarak kullanıcının adına işlem yapabilir, yetkisiz verilere erişebilir veya kullanıcının hesabında zararlı

aktivitelerde bulunabilir. Bu tür saldırılara karşı korunmak için web uygulamaları, güvenli oturum yönetimi protokolleri kullanmalı, oturum kimlikleri (session IDs veya çerezler) güvenli bir şekilde yönetilmeli ve kullanıcı girişleri, güvenlik duvarları ve güvenlik politikaları ile doğrulamalıdır.

Man-in-the-Middle (MITM) Saldırıları: Saldırgan, veri iletişimini dinleyerek veya değiştirerek kullanıcılar arasına girer. Bu şekilde, veri akışını izleyebilir veya manipüle edebilir (Standard ve diğerleri., 2013).

Zero-Day Exploits: Saldırgan, henüz keşfedilmemiş güvenlik açıklarını kullanarak sisteme erişmeye çalışır. Bu, güncellenmemiş yazılımlardan veya sistemlerden yararlanarak gerçekleştirilir.

Privilege Escalation (Ayrıcalık Yükseltme): Saldırgan, düşük düzeydeki bir hesaptan daha yüksek düzeydeki bir hesaba erişim sağlamak için açıklar veya hataları kullanarak sistemi manipüle eder. Privilege escalation genellikle dikey ve yatay olmak üzere iki şekilde gerçekleşir.

• Vertical Privilege Escalation (Dikey Ayrıcalık Yükseltme): Bu tür privilege escalation, kullanıcının kendi hesabındaki izinleri artırmasını içerir. Örneğin, bir kullanıcı normalde sadece sınırlı bir uygulamaya erişim sağlayan bir hesaba sahipse, bu kullanıcı kendisini daha fazla ayrıcalığa sahip bir hesaba yükseltebilir. Bu tür bir hak yükseltme genellikle uygulama veya sistemdeki bir güvenlik açığından kaynaklanır.

• Horizontal Privilege Escalation (Yatay Hak Yükseltme): Bu tür privilege escalation, bir kullanıcının aynı seviyede (örneğin, iki kullanıcı da yönetici düzeyinde) bulunan bir başka kullanıcının hesabına erişim sağlamasını içerir. Bu, genellikle paylaşılan parolalar veya oturum açma bilgileri gibi güvenlik zayıflıklarından kaynaklanır.

Erişim ataklarına karşı korunmak için güçlü parolalar kullanma, çok faktörlü kimlik doğrulama uygulama, sistemleri ve yazılımları düzenli olarak güncelleme, güvenlik yamalarını hızla uygulama ve ağ trafiğini izleme gibi önlemler alınmalıdır.

5. ANAHTARLAMA (SWİTCHİNG) ZAFİYETLERİ

Anahtarlar son kullanıcı cihazlarının kritik altyapı ile ilk temasının sağlandığı noktadır. Bu nedenle anahtarlar ve anahtarlama çoğunlukla bir ağın en zayıf noktalarından biri olarak görülür. Anahtara yönelik yapılan saldırılar çok geniş bir yelpazede yer alır. Bu saldırılar, ağ güvenliği açısından ciddi tehditler oluşturabilir. Aşağıda anahtarlara yönelik yapılan bazı önemli saldırılar yer almaktadır.

MAC Spoofing (MAC Sahteciliği): Saldırgan, ağdaki başka bir cihazın MAC adresini taklit ederek anahtara kendisini meşru bir cihaz olarak tanıtabilir. Bu şekilde, saldırgan meşru bir cihaz gibi davranabilir ve ağ trafiğini izleyebilir veya yönlendirebilir.

MAC Flooding (MAC Seli): Saldırgan, anahtara çok sayıda sahte MAC adresi göndererek MAC adres tablosunu doldurabilir. Bu durumda anahtar, bir hub gibi çalışıp tüm trafikleri herkese gönderebilir. Bu durum anahtarın normal işlevselliğini bozabilir, doğru kullanıcıların ağa erişimini engelleyebilir veya ağdaki trafiği izlemesine olanak tanır.

ARP Spoofing/Poisoning (ARP Sahteciliği): Saldırgan, ARP tablosunu manipüle ederek anahtara sahte IP-MAC adres eşlemeleri gönderebilir. Bu saldırı, saldırganın veri trafiğini yönlendirmesine ve hatta izlemesine olanak tanır.

VLAN Hopping: VLAN hopping saldırıları, switch konfigürasyonu hatalarını veya zayıflıkla-

rını kullanarak bir VLAN'dan diğerine geçmeyi sağlar. Bu, normalde izin verilmeyen trafiği diğer VLAN'lara yönlendirebilir.

Spanning Tree Protocol (STP) Saldırıları: STP, bir ağdaki ikinci katman döngülerini önlemek için kullanılan bir protokoldür. Saldırganlar, STP saldırıları kullanarak anahtarın ağ topolojisini manipüle edebilir veya anahtarı devre dışı bırakabilir. Ağ topolojisi değiştiğinde, yapılan saldırı türüne bağlı olarak saldırgan ağda döngü oluşmasını sağlayarak ağı (dolayısıyla anahtara bağlı olan tüm cihazları) ağ trafiği üretemez hale getirebilir.

DHCP Starvation (DHCP Açlık) Saldırısı : Açlık saldırısı, ağdaki DHCP sunucularını tükenmeye zorlayan bir tür ağ saldırısıdır. DHCP sunucuları, ağdaki cihazlara (bilgisayarlar, telefonlar, tabletler vb.) IP adresi ve diğer ağ yapılandırma bilgilerini dinamik olarak atar. DHCP sunucusu, IP adreslerini bir havuzda tutar ve bu adresleri cihazlara tahsis etmek için kullanır. DHCP Starvation saldırısı, saldırganın ağdaki tüm IP adreslerini talep etmesiyle gerçekleşir. Bu tür bir saldırıda, saldırganlar sahte MAC adresleri (Media Access Control) ile bir dizi DHCP talebi oluşturarak DHCP sunucusunu aşırı yüklemeye çalışır. DHCP sunucusu, her talebe yanıt vererek IP adreslerini tahsis etmeye çalışır, ancak bu sahte talepler nedeniyle gerçek cihazlara IP adresi tahsis edemez. Sonuç olarak, meşru cihazlar ağa bağlanamaz hale gelebilir, çünkü tüm IP adresleri tükenmiştir. DHCP Starvation saldırısı, ağ performansını düşürebilir, ağa erişimi engelleyebilir ve güvenlik açıklarına yol açabilir.

DHCP Spoofing (DHCP Sahteciliği): Saldırgan, ağdaki DHCP sunucusu gibi davranarak IP adresleri dağıtabilir. Bu, saldırganın verileri yönlendirmesine ve izlemesine olanak tanır.

DNS Spoofing (DNS Sahteciliği): Saldırgan, DNS isteklerini yanıtlayarak kullanıcılara yanıltıcı veya zararlı web sitelerine yönlendirebilir. Bu, kullanıcıları phishing (kimlik avı) saldırılarına maruz bırakabilir.

Anahtarlamaya yönelik yapılan saldırıların çözümünde birden çok güvenlik yönteminin birlikte kullanılması gerekebilir. Aşağıda bu çözüm önerilerine kısaca değinilmiştir.

Port Güvenliği: Kullanılmayan portları devre dışı bırakın ve gerekirse port güvenliği ayarlarını yapılandırın.

802.1X Kimlik Doğrulama: Port bazlı kimlik doğrulama kullanarak yalnızca yetkilendirilmiş cihazların ağa bağlanmasını sağlayın.

Güvenli VLAN Konfigürasyonu: VLAN'lara erişimi kontrol etmek için güvenlik politikaları oluşturun.

Güçlü Parola Kullanımı: Switch yönetim arayüzüne güçlü parolalar ve kimlik doğrulama yöntemleri uygulayın.

Yazılım Güncellemeleri: Switch'in işletim sistemini ve yazılımını güncel tutarak güvenlik yamalarını uygulayın.

Güvenlik Duvarları: Ağınıza gelen ve ağdan çıkan trafiği izlemek ve filtrelemek için güvenlik duvarları kullanın.

Bu önlemler, anahtarlara yönelik saldırıları önlemek ve ağ güvenliğini artırmak için alınabilecek temel adımlardır.

5.1. Yönlendirme (Routing) Zafiyetleri

Yönlendirme işlemi Router (yönlendirici) tarafından ağda gerçekleştirilen, IP paketlerin doğru hedefe gitmesini sağlayan bir süreçtir. Daha önce kısaca değinildiği gibi, bu yönlendirme süreci saldırganlar için bir atak vektörü olabilir.

Routing Tablosu Saldırıları: Saldırganlar, router'ın routing tablosunu manipüle ederek trafik yönlendirmeyi değiştirebilir, bu da trafiği yanlış yönlendirebilir veya ele geçirebilir.

Routing Protocol Saldırıları: Routing protokollerin (örneğin, RIP, OSPF, BGP) zayıf güvenlik mekanizmalarını hedef alarak yanıltıcı veya zararlı routing bilgileri gönderme.

IP Spoofing: Saldırganlar, meşru bir kaynaktan geliyormuş gibi görünen sahte IP adreslerini kullanarak router'ı yanıltabilir.

Fragmentation Saldırıları: Saldırganlar, IP paketlerini parçalayarak, trafik akışı sırasında güvenlik duvarlarını aşabilecek şekilde manipüle edebilir.

Bu saldırıların çözümlerinde öncelikle erişim güvenliğinin sağlanması önemlidir. Saldırganın cihaza uzaktan veya fiziksel olarak erişememesi gerekir. Erişim güvenliğinin sağlanmasının ardından çeşitli yöntemlere yönlendirmeye yönelik çözümler geliştirilebilir. Bu çözümler aşağıda özetle gösterilmiştir.

Güvenilir Routing Protokolleri Kullanımı: Kimlik doğrulama ve şifreleme yeteneği olan güvenli yönlendirme protokolleri kullanılmalıdır. Bu protokoller, doğrulama ve güvenlik önlemleri sağlamak için yapılandırılabilir.

Güncel Yazılım ve Firmware Kullanımı: Ağ cihazlarınızın işletim sistemleri, yazılımları ve firmware'leri güncel olmalıdır. Üretici tarafından yayınlanan güvenlik güncellemelerini düzenli olarak kontrol edilmelidir.

Ağ İzleme: Ağ trafiğini izlemek ve anormal durumları tespit etmek için ağ izleme araçları kullanılmalıdır. Bu şekilde potansiyel saldırıları daha hızlı tespit edebilir ve önlem alınabilir.

ARAŞTIRALIM

Kablosuz ağlarda ne gibi güvenlik riskleri vardır? Bu güvenlik riskleri nasıl azaltılabilir? Araştıralım.

5.2. Kablosuz Zafiyetler

Kablosuz ağlara yönelik bir dizi özgün saldırı türü bulunmaktadır. Bu saldırılar, kablosuz iletişimdeki özelliklerden kaynaklanan güvenlik zayıflıklarını hedef alır ve çeşitli teknikler kullanarak kablosuz ağları hedef alabilirler.

Rogue Access Point (Sahte Erişim Noktası): Saldırganlar, sahte bir erişim noktası oluşturarak, kullanıcıları gerçek ağ yerine kendi oluşturdukları ağa yönlendirebilir. Bu şekilde, kullanıcılar verilerini saldırgana açabilirler.

Evil Twin Attack (Kötü İkiz Saldırısı): Saldırgan, gerçek ağa benzeyen sahte bir kablosuz ağ oluşturarak kullanıcıları kandırabilir. Kullanıcılar, kötü amaçlı ağa bağlandıklarında, saldırgan trafiği izleyebilir ve kişisel verileri çalabilir.

Deauthentication (Deauth) Saldırısı: Saldırgan, hedef ağdaki cihazları deaktive edebilir, böylece bu cihazlar ağa erişemeyerek kullanıcıları hizmet dışı bırakır.

Man-in-the-Middle (MITM) Saldırıları: Saldırgan, kablosuz ağ trafiğini dinleyebilir, değiştirebilir veya çalabilir. Bu, şifrelenmemiş ağlarda daha kolay gerçekleştirilebilir.

Packet Sniffing: Saldırganlar, kablosuz ağdaki veri paketlerini dinleyebilir, bu da hassas bilgilerin ele geçirilmesine olanak tanır.

Wi-Fi Jamming: Saldırganlar, radyo frekanslarına müdahale ederek kablosuz sinyali bozabilir, bu da kullanıcıların ağa bağlanmasını engeller.

WPS (Wi-Fi Protected Setup) Saldırıları: WPS, kullanıcıların kolayca kablosuz ağlara bağlanmalarını sağlayan bir özelliktir. Ancak WPS PIN brute-force saldırılarıyla kolayca kırılabilir.

Kablosuz Güvenlik Protokollerine Yönelik Saldırılar: WEP (Wired Equivalent Privacy) ve bazı eski WPA (Wi-Fi Protected Access) protokollerine yönelik saldırılar, güçlü olmayan şifreleme nedeniyle zayıf noktaları hedef alır.

Kablosuz ağlar, doğası gereği radyo frekansları ile veri iletimi yapar, bu da fiziksel erişime dayalı olmayan saldırıların gerçekleştirilebilmesine olanak tanır. Ancak, bu saldırılar yalnızca kablosuz ağları hedef almaz; çoğu durumda, aynı saldırılar kablolu ağlarda da gerçekleştirilebilir. Bu nedenle, güvenlik önlemleri hem kablosuz hem de kablolu ağlarda etkili bir şekilde uygulanmalıdır.

6. AĞ GÜVENLİK DONANIMLARI

Ağ güvenliğini sağlamak için kullanılan çeşitli donanım cihazları bulunmaktadır. Yaygın olarak kullanılan ağ güvenlik donanımlarından bazıları maddeler halinde sıralanmıştır.

Firewall (Güvenlik Duvarı): Firewall, ağdaki veri trafiğini izleyen ve filtreleyen bir güvenlik cihazıdır(Odom, 2004). İzin verilen ve engellenen trafik kurallarına göre trafiği kontrol eder. Paket filtreleme, durumlu paket incelemesi ve proxy gibi hizmetleri sunarlar. Firewall cihazları ağ giriş noktalarında, iç ağlarda ve veri merkezlerinde kullanılır.

Intrusion Detection System (IDS) ve Intrusion Prevention System (IPS): IDS (saldırı tespit sistemleri), ağda anormal aktiviteleri izler ve belirli saldırı desenlerini tanımlar. IPS (saldırı önleme sistemleri) ise saptanan tehditlere otomatik olarak tepki verir, saldırıları durdurur (Zaripova & ugli, 2021). IDS/IPS sistemleri, tıpkı antivirüs yazılımlarında olduğu gibi, daha önce analiz yapılmış saldırıların karakteristik özelliklerinin yer aldığı imza veritabanlarını kullanabilir. Bu tür sistemlere imza tabanlı IDS/IPS sistemleri denir. Daha gelişmiş sistemlerde ise anomali tabanlı saldırı analizi yapılabilir. Buna göre ağın normal davranışı analiz edilir ve bir temel çizgi (baseline) çıkarılır. Sistem, bu temel çizgiden yaşanan sapmalara göre anormal davranışları tespit edebilir. Bunların haricinde davranış bazlı çalışan IPS sistemleri, makine öğrenmesi tabanlı çalışan gelişmiş ve modern IDS/IPS sistemleri de bulunmaktadır.

IDS/IPS sistemleri, trafik izleme, saldırı algılama, saldırı engelleme, anormal davranış algılama gibi fonksiyonları sunarlar. Genelde internet gibi dışarıdan gelen saldırıları karşılamak üzere ağ giriş noktalarında veya iç ağlarda kullanılır.

Virtual Private Network (VPN) Cihazları: Güvenli bir şekilde uzak kullanıcıları veya uzak ofisleri ağa bağlamak için kullanılır. Veriyi şifreler ve güvenli bir şekilde iletimini sağlar. Şifreleme, kimlik doğrulama, güvenli tünel oluşturma gibi fonksiyonları yerine getirir.

Proxy Sunucular: Proxy sunucular, istemci cihazların ve sunucuların ağa erişimini kontrol eder ve izler. İstemci ve sunucular ile internet arasında ara bir nokta oluşturur. Web filtreleme, İnternet erişimi kontrolü, İnternet anonimliği sağlama gibi fonksiyonları sağlar. Kurumsal ağlarda, içeriği filtreleme ve kullanıcı izleme için kullanılır.

Load Balancer (Yük Dengeleyici): Load balancer, gelen ağ trafiğini dengeler ve farklı sunuculara yönlendirerek yükü dağıtır. Bu, hizmet sürekliliği sağlamak ve performansı artırmak için kullanılır. Trafik dengeleme, sunucu yedekleme ve hizmet sürekliliği gibi doğrudan güvenlik ile ilgili olmayan ancak oldukça faydalı fonksiyonları gerçekleştirir. Yük dengeleyiciler, web siteleri, uygulamalar ve veri merkezlerinde yaygın olarak kullanılır.

Distributed Denial of Service (DDoS) Koruma Cihazları: DDoS koruma cihazları, DDoS saldırıla-

rına karşı ağ ve sunucuları korumak için kullanılır. Ağ trafiğini izler, anormal aktiviteleri belirler ve saldırıları filtreler. Trafik analizi, DoS/DDoS saldırı algılama, saldırıları engelleme görevlerini yaparlar.

Web Security Appliance: Web Security Appliance (WSA), ağlarını güvenli tutmak isteyen organizasyonlar için kullanılan bir güvenlik cihazıdır. WSA, web trafiğini izler, filtreler ve güvenlik tehditlerine karşı koruma sağlar. Bu cihaz, kullanıcıların internet üzerinden güvenli bir şekilde gezinmelerini ve web tabanlı tehditlere karşı savunmalarını güçlendirmelerini sağlar.

URL filtreleme, antivirus ve antimalware koruma, SSL izleme ve içerik filtreleme, uygulama denetimi, veri kaybını önleme, gelişmiş tehdit izleme, raporlama ve analiz görevlerini sağlayabilir. Web Security Appliance, kurumsal ağlarda, okullarda, devlet kurumlarında ve diğer organizasyonlarda kullanılan bir güvenlik çözümüdür. Bu tür bir güvenlik cihazı, çalışanları ve ağı web tabanlı tehditlere karşı korumak için önemli bir rol oynar.

e-Mail Security Appliance, organizasyonların e-posta iletilerini korumak için kullanılan bir güvenlik cihazıdır. Bu cihaz, zararlı e-postaları algılamak, istenmeyen içerikleri engellemek, phishing girişimlerini durdurmak ve gizli verilerin sızmasını önlemek gibi görevleri yerine getirir.

NAC, Network Access Control'ün (Ağ Erişim Kontrolü) kısaltmasıdır ve ağ güvenliği yönetiminde kullanılan bir güvenlik çözümüdür. NAC sistemleri, güvenlik politikalarını uygular, ağa erişmeye çalışan cihazları kimlik doğrular ve yetkilendirir ve yalnızca güvenilir ve uyumlu cihazların ağa bağlanmasını sağlar.

• Kimlik doğrulama: NAC çözümleri, ağa erişim sağlamadan önce kullanıcıları ve cihazları kimlik doğrular. Bu kimlik doğrulama süreci, kullanıcı adı ve şifre, dijital sertifikalar veya çok faktörlü kimlik doğrulama gibi çeşitli yöntemleri içerebilir.

• Yetkilendirme: Kimlik doğrulandıktan sonra, NAC sistemleri, kullanıcıya veya cihaza önceden tanımlanmış güvenlik politikalarına dayalı olarak hangi erişim düzeyini vereceğini belirler. Örneğin, çalışanlara, misafirlere veya taşeronlara farklı erişim seviyeleri atanabilir.

• Uyumluluk Kontrolleri: NAC sistemleri, güvenlik politikalarına uygunluğu kontrol etmek için cihazların güvenlik durumunu değerlendirir. Bu, işletim sisteminin ve antivirüs yazılımının güncel olup olmadığını kontrol etmek, güvenlik yamalarının varlığını doğrulamak ve belirli güvenlik yapılandırmalarının olduğundan emin olmak gibi kontrolleri içerebilir.

• Düzeltme: Bir cihazın güvenlik politikalarına uygun olmadığı tespit edilirse, NAC çözümleri, cihazı karantinaya alabilir, onu düzeltme ağına yönlendirebilir veya kullanıcıya cihazlarını güncellemek için talimatlar verebilir.

• İzleme ve Raporlama: NAC sistemleri sürekli olarak ağ aktivitesini izler, bağlı cihazları takip eder ve güvenlik olayları, uyumluluk durumu ve kullanıcı aktiviteleri hakkında raporlar oluşturur. Bu izleme, potansiyel güvenlik tehditlerini ve gerçek zamanlı olarak tespit edilebilecek olan zayıf noktaları belirlemeye yardımcı olur.

NAC, yetkisiz erişimi önleyerek, hassas verileri güvenli hale getirerek ve ağa bağlanan tüm cihazların kuruluşun güvenlik standartlarını karşıladığından emin olarak ağ güvenliğini artırmada önemli bir rol oynar. Özellikle günümüzde çeşitli ve karmaşık ağ ortamlarında, dizüstü bilgisayarlar, akıllı telefonlar, tabletler ve IoT cihazları gibi farklı cihazların güvenli bir şekilde ağa entegre edilmesi gerektiği durumlarda büyük önem taşır.

BÖLÜM ÖZETİ

Bilgisayar ağlarında kullanılan iki tür cihazdan bulunur. Uç cihazlar genellikle insanlarla etkileşim halinde bulunan cihazları içerirken, aracı cihazlar verinin güvenli bir şekilde iletilmesini sağlar. Yönlendiriciler, farklı ağlar arasında veri iletimini yönlendirir. Yönlendirme tablosu, bu iletimi sağlamak için kullanılır ve saldırılara açık olabilir. Anahtarlar, bilgisayarlar arasında doğrudan iletişimi hızlandırır. MAC tablosu, hangi cihazın hangi porta bağlı olduğunu gösterir. Modemler, bilgisayar verilerini analog sinyallere dönüştürerek internete bağlanmayı sağlar. Access point'ler kablosuz ağlara bağlantıyı mümkün kılar, ancak güvenlik riski taşır. Güvenlik duvarları, istenmeyen erişimleri engeller. Bu cihazlar, belirli protokoller ve standartlarla çalışarak veri iletimini güvenli ve etkili bir şekilde sağlarlar. Ağ cihazlarında güvenlik açıkları bulunabilir. Bu açıklar, yetersiz parolalar, yazılım güncellemelerinin ihmal edilmesi, zayıf şifreleme, DoS saldırıları, fiziksel erişim ve kötü tasarlanmış güvenlik politikaları gibi faktörlerden kaynaklanabilir. Ağ cihazlarına erişim güvenliği için konsol bağlantısı, SSH, Telnet, web tabanlı arayüzler ile sağlanır. Bu yöntemler ile ilgili güvenlik riskleri, güçlü parolalar ve kimlik doğrulama, yazılım güncellemeleri, güvenlik duvarları ve izinlerin doğru yapılandırılması, fiziksel erişim kontrolü ve kötü amaçlı yazılım taramaları gibi çözümler ile önlenebilir. Ağ saldırıları, ağ güvenliği için ciddi bir tehdit oluşturur ve bu tür saldırılara karşı korunmak için alınması gereken önlemler büyük önem taşır. Keşif saldırıları, saldırganların hedef ağ veya sistem hakkında bilgi toplamak için yaptığı ön saldırıları ifade eder. Pasif keşif (kamuya açık kaynaklardan bilgi toplama) ve aktif keşif (doğrudan hedef sisteme etkileşimde bulunma) olmak üzere iki türü vardır. Bu tür saldırıları önlemek için güçlü şifreler kullanma, güvenlik yamalarını düzenli olarak uygulama ve ağ trafiğini izleme gibi önlemler alınabilir. Erişim saldırıları, saldırganların yetkisiz şekilde bir sistem, ağ veya hizmete erişim sağlamak için yaptığı girişimleri ifade eder. Bu tür saldırılara karşı güçlü parolalar kullanma, çok faktörlü kimlik doğrulama uygulama ve yazılım güncellemelerini düzenli olarak yapma gibi önlemler alınabilir. Anahtarlamaya yönelik yapılan saldırılar, ağ güvenliğini ciddi şekilde tehdit edebilir. Bu saldırıları önlemek için kullanılmayan portları devre dışı bırakma, 802.1X kimlik doğrulama kullanma, güvenli VLAN konfigürasyonu oluşturma gibi önlemler alınabilir. Yönlendirme işlemi sırasında yapılan saldırılar, ağ trafiğini yanıltabilir veya ele geçirebilir. Bu tür saldırıları önlemek için erişim güvenliğini sağlama, güvenilir routing protokolleri kullanma ve güncel yazılım ve firmware kullanma gibi önlemler alınabilir. Tüm bu önlemler, ağ güvenliğini artırmak ve saldırılara karşı daha güvende olmak için hayati öneme sahiptir. Ancak unutulmamalıdır ki güvenlik, sürekli bir süreçtir ve ağınızdaki tehditler zaman içinde değişebilir, bu nedenle güvenlik önlemlerinizi sürekli güncellemek önemlidir. Ağ güvenliğini sağlamak için kullanılan çeşitli donanım cihazlar kullanılır. Firewall (Güvenlik Duvarı): Ağdaki veri trafiğini izler ve izin verilen ve engellenen trafik kurallarına göre trafiği kontrol eder. Intrusion Detection System (IDS) ve Intrusion Prevention System (IPS): Ağda anormal aktiviteleri izler ve belirli saldırı desenlerini tanımlar. Virtual Private Network (VPN) Cihazları, Uzak kullanıcıları veya uzak ofisleri güvenli bir şekilde ağa bağlamak için kullanılır. Proxy Sunucular, İstemci cihazların ve sunucuların ağa erişimini kontrol eder ve izler. Load Balancer (Yük Dengeleyici), ağ trafiğini dengeler, farklı sunuculara yönlendirir ve hizmet sürekliliği sağlar. Distributed Denial of Service (DDoS) Koruma Cihazları: DDoS saldırılarına karşı ağ ve sunucuları korumak için kullanılır. Web Security Appliance, e-Mail Security Appliance ve Network Access Control (NAC) gibi özel güvenlik cihazları web tabanlı tehditlere karşı koruma sağlamak, zararlı e-postaları algılamak ve ağa güvenli erişimi kontrol etmek gibi özel görevlere yöneliktir.

GÖZDEN GEÇİRELİM

1. **Ağ cihazlarında güvenlik açıkları oluşmasına neden olan yaygın bir durum aşağıdakilerden hangisidir?**
   a) Fiziksel Erişim
   b) SSH Kullanımı
   c) İyi Yapılandırılmış Güvenlik Duvarları
   d) Yazılım Güncellemeleri

2. **Aşağıdaki güvenlik önlemlerinden hangisi kötü amaçlı yazılım taramasını içerir?**
   a) Fiziksel Erişim Kontrolü
   b) Güçlü Parolalar ve Kimlik Doğrulama
   c) Yazılım Güncellemeleri
   d) Kötü Amaçlı Yazılım Taraması

3. **Ağ cihazlarına yapılandırma amacıyla uzaktan erişimde güvenli bir seçenek olarak tavsiye edilen protokol hangisidir?**
   a) Telnet
   b) HTTP
   c) SSH
   d) FTP

4. **Keşif saldırıları hangi iki ana kategoride değerlendirilebilir?**
   a) Pasif ve aktif
   b) Harici ve içsel
   c) Doğrudan ve dolaylı
   d) Fiziksel ve dijital

5. **Brute-force saldırılarına karşı korunmak için aşağıdaki yöntemlerden hangisi etkili olabilir?**
   a) Kısa ve basit şifreler kullanmak
   b) Aynı parolayı farklı hesaplarda kullanmak
   c) Güçlü parolalar kullanmak ve çift faktörlü kimlik doğrulamayı uygulamak
   d) Parolaları kamuya açık kaynaklarda paylaşmak

6. **Man-in-the-Middle (MITM) saldırısı nedir?**
   a) Saldırganın doğrudan sisteme fiziksel erişim sağlaması
   b) Saldırganın kullanıcılar arasında veri iletişimini dinleyerek veya değiştirerek girmesi
   c) Saldırganın sisteme henüz keşfedilmemiş güvenlik açıklarını kullanarak erişim sağlaması
   d) Saldırganın bir kullanıcının oturumunu ele geçirmesi

7. **MAC Spoofing (MAC Sahteciliği) nedir?**
   a) Gerçek bir cihazın MAC adresini taklit ederek anahtara yetkisiz erişim sağlama saldırısıdır.
   b) Saldırganın anahtara çok sayıda sahte MAC adresi göndererek anahtarın normal işlevselliğini bozma saldırısıdır.
   c) Saldırganın ARP tablosunu manipüle ederek sahte IP-MAC adres eşlemeleri gönderme saldırısıdır.
   d) Saldırganın DNS isteklerini yanıtlayarak kullanıcıları yanıltıcı veya zararlı web sitelerine yönlendirme saldırısıdır.

8. **DHCP Starvation (DHCP Açlık) Saldırısı nedir?**
   a) Saldırganın ağdaki tüm IP adreslerini talep ederek DHCP sunucusunu aşırı yüklemeye çalışmasıdır.
   b) Saldırganın sahte IP adresleri kullanarak anahtara yanıltıcı veri yönlendirmesi yapmasıdır.
   c) Saldırganın DNS isteklerini yanıtlayarak kullanıcıları zararlı web sitelerine yönlendirme saldırısıdır.
   d) Saldırganın ağdaki cihazları deaktive etmesi ve kullanıcıları ağa erişimden mahrum bırakmasıdır.

9. **Aşağıdakilerden hangisi kablosuz ağlara yönelik bir saldırı türüdür?**
   a) Brute Force Saldırısı
   b) MAC Spoofing
   c) Rogue Access Point (Sahte Erişim Noktası)
   d) Spanning Tree Protocol (STP) Saldırısı

10. **Aşağıdaki ağ güvenlik cihazlarından hangisi imza verita banına göre yapılan saldırıyı tespit eder ve önler?**
    a) Yönlendirici
    b) Access Point
    c) NAC
    d) IPS

Yanıt Anahtarı: 1A, 2-D, 3-C, 4-A, 5-C, 6-B, 7-A, 8-A, 9-C, 10-D

Kaynakça

KUNDU, S. (2008). *Fundamentals of Computer Networks*. PHI Learning. https://books.google.com.tr/books?id=OMoHmEQHosAC

McDonald, J. C. (2013). *Fundamentals of Digital Switching*. Springer US. https://books.google.com.tr/books?id=haXqBwAAQBAJ

Miller, R. (n.d.). *Computer Networking: Network+ Certification Study Guide for N10-008 Exam 4 Books in 1: Enterprise Network Infrastructure, Network Security \& Network Troubleshooting Fundamentals*. Richie Miller. https://books.google.com.tr/books?id=_BCeEAAAQBAJ

Odom, W. (2004). *Computer Networking First-step*. Cisco Press. https://books.google.com.tr/books?id=-VoXXwpE_YoMC

Peterson, L. L., & Davie, B. S. (2003). *Computer Networks: A Systems Approach*. Elsevier Science. https://books.google.com.tr/books?id=XUkIKfJbFCUC

Shinder, D. L. (2001). *Computer Networking Essentials*. Cisco Press. https://books.google.com.tr/books?id=ZMizSUW7XF4C

Standard, S., Greenlaw, R., Phillips, A., Stahl, D., & Schultz, J. (2013). Network Reconnaissance, Attack, and Defense Laboratories for an Introductory Cyber-Security Course. *ACM Inroads*, *4*(3), 52–64. https://doi.org/10.1145/2505990.2506002

Stephen, T. D., Harrison, T. M., & Stephen, T. (1996). *Computer Networking and Scholarly Communication in the Twenty-First-Century University: An Introduction to Isaac Breuer's Philosophy of Judaism*. State University of New York Press. https://books.google.com.tr/books?id=Jkuen2GW2H8C

Zaripova D.A and Makhmudov Abdukhalil Abdurakhmon ugli 2021. Network security issues and effective protection against network attacks. International Journal on Integrated Education. 4, 2 (Feb. 2021), 79-85. DOI:https://doi.org/10.17605/ijie.v4i2.1204.

Okuma Listesi

S. Çelik and B. Çeliktaş , "Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar", Cyberpolitik Journal, vol. 3, no. 5, pp. 105-132, Jul. 2018

G. Canbek and Ş. Sağıroğlu , "BİLGİSAYAR SİSTEMLERİNE YAPILAN SALDIRILAR VE TÜRLERİ: BİR İNCELEME", Erciyes Üniversitesi Fen Bilimleri Enstitüsü Fen Bilimleri Dergisi, vol. 23, no. 1, pp. 1-12, Feb. 2007

Sağıroğlu, Ş. & Mohammmed, M. (2009). Mobil Ortamlara Yapılan Saldırılar Üzerine Bir İnceleme. TÜBAV Bilim Dergisi , 2 (2) , 138-147.