GAZİ ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ

BM402 BİLGİSAYAR AĞLARI

Gamze Aksu

171180005

ÖDEV-3

MART 2022

İÇİNDEKİLER

Sayfa

1. PROTOKOL SALDIRILARI

1.1. DNS (Domain Name System)

DNS protokolü verilen bir alan adından IP adresini öğrenmek için kullanılan bir protokoldür. Basitçe bir çözümleyici denilebilir. IP adreslerini akılda tutmak zor olduğu için alan adları kullanılır. Ancak bilgisayarlar birbirleriyle iletişim kurabilmek için IP adreslerine ihtiyaç duyarlar. Biz de IP adreslerini ezbere bilmediğimiz için bir çözümleyiciye olan ihtiyaç ortaya çıkmaktadır. DNS protokolü de bu ihtiyaca cevap verir. [1]

1.1.1. DNS Saldırıları

DNS kullanılabilirlik için tasarlanmış bir protokoldür. Aslında sağlam olmasına rağmen güvenlik için tasarlanmamıştır. Bu yüzden güvenlik açıkları bulunmaktadır. Bu güvenlik açıklarını kullanarak saldırganlar kurbanlarına çeşitli saldırılarda bulunurlar. DNS saldırı türleri arasında şunlar bulunmaktadır. [2]

- Sıfırıncı Gün Saldırısı: DNS protokolünde daha önceden açıklanmamış bilinmeyen bir güvenlik açığı ile saldırı yapılmasına denir.
- Önbellek Zehirlenmesi: DNS sunucunun önbelleği bozularak gerçekleştirilir. DNS sunucunda bulunan normal IP adresi değiştirilir ve yerine kötü bir sitenin IP adresi yazılır. DNS sorgusu sonucunda kötü amaçlı site ziyaret edildiğinde bu sitede saldırganın amacı ne ise gerçekleştirebilir. Önbellek zehirlenmesi saldırısı aynı zamanda DNS zehirlenmesi saldırısı olarak da bilinmektedir.
- DoS: Bir DNS sunucusuna farklı IP adresleri ile bir alan adının DNS sorgusunun gönderilmesi ile yapılır. DNS sunucusuna çok fazla sorgu gönderildiği için sunucu hizmet veremez duruma gelir.
- DDoS: DoS saldırısının farklı noktalarda dağıtılmış olarak yapılmasına denir. Bir botnet kullanılarak yapılabilir.
- DNS Amplification: Saldırgan bir kurbanın IP adresini kullanarak bir DNS sunucusuna çok fazla sorgu gönderir. Yapılan sorgu paketlerinin boyutu küçük olmasına rağmen cevap olarak dönen paketlerin boyutu büyüktür. Böylece kurbanın bant genişliği dolar.
- Fast-Flux DNS: Saldırgan DNS isteklerini yeniden yönlendirmek ve algılamayı önlemek amacıyla bu saldırıyı gerçekleştirir. Birden fazla IP adresini tek bir alan adına denk gelecek şekilde DNS kayıtları değiştirilerek gerçekleştirilir. Bu IP adresleri hızla değiştirilir. Bazen yüzlerce binlerce IP adresi kullanılır.

1.1.2. DNS Saldırı Önlemleri

DNS saldırılarının başarılı bir gerçekleşme olasılığını azaltmak için sunucu yöneticilerinin ilk olarak DNS yazılımlarının güncel tutmaları gerekmektedir. Yazılım güncel olduğunda eski sürümlerdeki bilinen hataları düzeltilmiş olur. Daha sonra trafiğin sürekli izlenmesi gerekmektedir. Örneğin DNS amplification saldırısında kurban herhangi bir sorgu yapamamasına rağmen sürekli olarak bir DNS sunucusundan gelen DNS paketleri trafikte görülebilir. Son olarak da sunucuların yapılandırılması gerekmektedir. Sunucuların işlevleri ayıracak ve yalıtacak şekilde yapılandırılması saldırı oranının azaltılmasını sağlar. [2]

1.2. TCP (Transmission Control Protocol)

Bilgisayarlar arsında gönderilen paketlerin taşınması için TCP protokolü kullanılır. TCP protokolünü amacı paketler arasında kayıp yaşanmamasıdır. Yolda kaybolan paketlerin tekrar istenmesi ile kayıp paket sorununun önüne geçilir. Paketler farklı yollardan geçerek sırası karışmış olarak hedefe ulaştığında TCP protokolü sayesinde bu paketler sıraya koyulur.

1.2.1. TCP Saldırıları

- **SYN Flood:** TCP protokolünde 3-Way Handshake denilen bir işlem gerçekleşir. Burada istemci ve sunucu arasında bir oturum başlatılır. İstemci-sunucu arasında bir oturum başlatılması için ilk olarak istemcinin sunucuya bir SYN paketi göndermesi gerekmektedir. Daha sonra sunucu da istemci ile senkronize olmak için SYN - ACK paketi gönderir. İstemci de ACK paketi gönderdiğinde 3-Way Handshake gerçekleşmiş olur. Bu sistemi saldırganlar bir DoS saldırısı için kullanabilir. Saldırgan farklı IP adresleri ile durmadan SYN paketi gönderdiğinde sunucu durmadan farklı IP adreslerine paket göndermeye başlar. Çok fazla paket ile sunucu baş edemez ve limitleri dolar. Bu şekilde sunucu gerçek bir kullanıcıya yanıt veremez duruma gelir. [3]
- **TCP Reset Saldırısı:** TCP reset saldırısında kurbanlar arasında geçen iletişimin kopması sağlanır. Sahte bir TCP reset paketi gönderilerek İnternet bağlantısı kurcalanır veya sonlandırılır. Bu teknik kötü kişilerin elinde kötüye kullanılabildiği gibi bir güvenlik duvarı tarafından da kullanılabilir. [4]
- **Session Hijacking:** İki farklı bilgisayar arasında kurulan TCP oturumunu başkasının ele geçirmesine denir. TCP protokolünde doğrulama işlemi en başta yapıldığından daha sonradan gelen saldırgan kurulmuş olan TCP oturumunu ele geçirebilir. Saldırgan yetkili kullanıcının oturum kimliğine erişmeye çalışır. Oturum kimliğine eriştiğinde ise yetkili kullanıcı gibi davranabilir. [5]

1.2.2. TCP Saldırısı Önlemleri

- **SYN Flood:** Bu saldırının amacına ulaşmasını önlenmek için ilk olarak sunucunun bellek kapasitesini arttırma işlemi yapılabilir. Bu durumda saldırgan farklı IP adresleri ile saldırsa bile hala sunucu kapasiteye sahip olduğundan gerçek bir kullanıcı saldırı sırasında bile sunucudan hizmet alabilir. Sunucuyu rahatlatmak için yapılabilecek bir diğer işlem ise uzun süre beklenen ACK paketlerinin isteklerinin sonlandırılmasıdır. 3-Way Handshake de sunucu SYN-ACK paketi göndermiş ve çok uzun süredir ACK paketi bekliyorsa bu isteği kapatabilir. Beklenen süre için bir zamanlayıcı belirlenir ve bu zaman dolduğunda istek silinir. [6]
- **Session Hijacking:** Oturum ele geçirme saldırılarını önlemek için yapılması gereken en önemli şey güvenli bir iletim kanalı oluşturmaktır. Bunun için SSH kullanılabilir. Benzer şekilde VPN kullanmak da güvenli iletişim sağlar. Saldırganın bir şekilde bir oturum için kullanıcı adı ve şifreni bilmesi durumunda diğer hesapların da tehlikeye girmemesi için her bir hesap için farklı kullanıcı adı ve parola kullanılması gerekmektedir. Bunların dışında otomatik koruma için IPS ve IDS teknolojilerinden de yararlanılabilir. [5]

1.3. Internet Protokolü (IP)

İnternet protokolü bilgisayarlar arası temel iletişim için gerekli olan bir protokoldür. Paketlerin içerisinde bir başlık ve bir data bölümü vardır. Data bölümünde taşınması gereken bilgiler yer alırken başlık kısmında ise IP adresleri ve TTL gibi gerekli olan başka bölümler yer alır. İletişim esnasında paketin içerisindeki hedef IP hiç değişmez. Bu şekilde yönlendiriciler IP adreslerine bakarak paketi gideceği yere gönderir. IP protokolü best-afford olarak adlandırılan protokollerdendir. Paketin hedefe ulaşıp ulaşmadığı ile ilgilenmez.

1.3.1. IP Spoofing

IP Spoofing, sahte kaynak IP adresi ile paketlerin gönderilmesine denir. Saldırganlar genel olarak bu işlemi kimliklerini gizlemek, gönderenin kim olduğunun anlaşılamaması için yaparlar. Bu işlem genel olarak tek başına zararsızdır. Fakat farklı IP adresleri ile DoS ve DDoS saldırıları gerçekleştirilebilir. [7]

1.3.2. IP Spoofing Önlemleri

IP Spoofing işlemini tam olarak önlenemese de Bazı filtreleme işlemleri ile bu işleme karşı bir savunma yapılabilir. Gelen IP paketleri incelenir ve herhangi bir anormallik görüldüğünde bu paketler atılır. Ek olarak bazı ağlar da giden paketler için filtreleme işlemi yapar. Ağlar IP Spoofing önlemek için filtreleme ile sadece meşru IP adreslerinin geçişine izin verir. [7]

1.4. ICMP (Internet Control Message Protocol)

ICMP protokolü sorunları iletişim halinde olan bilgisayarlara bildirir. Hata raporlama, hata düzeltme ya da durum bildirme gibi işlemlere IP protokolü sahip değildir. Bu yüzden bir geri besleme mekanizması olarak ICMP protokolü yer alır [8]. ICMP protokolünün geri bildirim vermesi gereken bazı durumlar şu şekilde sıralanabilir: yok edilen paket olduğunda, hata oluştuğunda, TTL süresi dolduğu zaman, paket başka bir yoldan gideceği zaman…

1.4.1. ICMP Saldırıları

- **ICMP Smurf Saldırıları:** Saldırgan IP spoofing yaparak kaynak adresi kurbanın adresi olarak değiştirir. Daha sonra bir sürü ping paketi gönderilir. Böylece kurbanının bant genişliği tıkanır. Ping istekleri directed broadcast olarak da ağ içerisinde yollanabilir. Bu şekilde ağ içerisindeki bilgisayarlar da saldırıya dahil olmuş olur. Bu ping paketlerinin cevabı da kurbana gönderilir. Bu şekilde saldırgan hem kimliğini saklamış hem de saldırısını gerçekleştirmiş olur. [8]
- **ICMP Flood Saldırısı:** ICMP ping paketlerinin boyutu değiştirilebilir. Saldırgan kurbana arka arkaya büyük boyutlarda ping paketi gönderdiğinde kurban paketleri karşılayamaz ve bağlantısı kopar. [8]
- **Ping of Death:** ICMP Echo request'lerin data kısmı 216 ile 65,536 byte arasında olmak zorundadır. Saldırgan olması gerekenden daha büyük bir paketi parçalanmış olarak gönderir. Alıcı cihaz bu paketleri alıp birleştirdiğinde olması gerekenden büyük olduğu için cihaz arabellek taşmasına ve cihazın çökmesine sebep olur. Eski cihazlar bu saldırılar karşısında savunmasız kalsa da yeni cihazlara bu saldırılara karşı savunmalar eklenmiştir. [9]

1.4.2. ICMP Saldırıları Önlemleri

ICMP saldırılarına karşı alınabilecek önlemler arasında ilk olarak dışarıdan, internetten, gelen ICMP trafiği engellenmelidir. Bu şekilde saldırılardan kaçınılabilir. Daha sonra ICMP paketlerinin denetimi yapılmalıdır ve ICMP paketlerinin sayısında bir kısılama getirilmelidir.

Basit bir şekilde ICMP trafiğini engelleyen güvenlik duvarı yapılandırması gerçekleştirilebilir. Son olarak ICMP hata mesajlarının dışarı çıkmasına izin verilmemelidir. Bu ağ içerisinde oluşan hataların dışarı saldırganlara gittiğini gösterir. [8]

1.5. FTP

Veri paylaşmak için en sık kullanılan yöntemlerden biri olarak FTP (File Transfer Protocol) protokolü verilebilir. İnternete bağlı iki farklı bilgisayar arasında dosya paylaşımı hizmeti sağlayan bir protokoldür. En eski protokollerden biri olan FTP güvenlik açısından bazı eksiklikler taşımaktadır. [10]

1.5.1. FTP Saldırıları

- **Anonymous Authentication:** Anonim kimlik doğrulama, FTP protokolünde kullanıcılar kullanıcı adı ile veya anonim olarak oturum açma izni bulunmaktadır. Bu bir güvenlik açığıdır. Kullanıcılar oturum açarken kullanıcı adı ve parola girerler ve oturum açma işlemi gerçekleşmiş olur. Güvenli bir kullanım için normalde kullanıcı adı ve parola bilgilerinin şifrelenmiş olarak gönderilmesi gerekmektedir. Ancak FTP protokolünde kullanılan komutlar ve kullanıcı adı – parola şifrelenmemiştir ve erişime açıktır. Aynı şekilde anonim olarak gönderilen dosyalar da korunmasız olarak bırakılır.[11]
- **Bounce Saldırısı:** Bounce saldırısında saldırganın kimliğinin bulunmasını zorlaştırmak saldırının en önemli özelliğidir. Saldırı temelde FTP sunucusunun Proxy olarak kullanılmasına dayanır. Saldırganlar FTP sunucusunu Proxy gibi kullanarak normal taramada görünmeyen bağlantı noktaları tarayabilirler. Ek olarak bu yöntemle temel paket süzgeçlerinden geçmek de mümkündür. Anonim bir FTP sunucusu gibi güvenlik duvarı aşılıp iç sunuculara ulaşabilir. [12]

1.5.2. FTP Saldırı Önlemleri

FTP protokolüne karşı yapılan saldırılardan korunmak için ilk yapılabilecek şey FTP protokolü kullanmayı bırakmak olabilir. Çünkü FTP protokolü çok eski bir protokoldür ve modern dünyanın gereksinimlerini karşılayamaz duruma gelmiştir. Bir diğer yöntem ise güçlü şifreler kullanmaktır. Çok fazla sayı ve karakterden oluşan güçlü şifre kullanmanın yanı sıra kullanılan şifrelerin de yaklaşık 3 ayda bir değiştirilmesi saldırganların şifreyi ele geçirmesini zorlaştırır.[13]

1.6. Rootkit

Rootkit, genellikle bilgisayara uzaktan erişmek ve kontrol etmek için kullanılan kötü amaçlı bir yazılım türüdür. İşletim sistemleri ve yazılımları etkiler. Rootkit, genellikle hedef cihaz üzerinde yönetici düzeyinde kontrol sağlar. Bir rootkit'in hedef bilgisayar üzerine yüklenmesi için en sık kullanılan yöntem sosyal mühendislik saldırılarıdır. Bir diğer yöntem ise işletim sistemi güncel olmayan hedeflerde işletim sisteminin zafiyetlerinden yaralanarak hedef makineye sızmaktır. Bunların dışında korsan olarak indirilen dosyalar ya da yazılımların içinde gömülü olarak cihaza rootkit yüklenebilir. [14]

Rootkit'ler işletim sisteminin içinde ya da yakınında çalışır. Bu sayede bilgisayar içinde komutlar çalıştırılabilir. Bu sebeple işletim sistemi olan her cihaz hedef olabilir. Yani, IoT geliştikçe sadece bilgisayarlar değil de buzdolapları, hatta kahve makineleri de rootkit tehdidi altında kalır.

Rootkit yazılımları bilgisayar üzerinde tam yetkiye sahip olduğu için çok tehlikelidir. Rootkit'lerin tehlikeli olmasının bazı nedenleri vardır. İlk olarak başarılı bir rootkit ile bilgisayarda kullanılan hesaplar ele geçirilebilir, bilgisayar üzerindeki dosyalara ve kredi kartı bilgilerine erişilebilir. Ayrıca korsanlar ele geçirilmiş olan bilgisayar ile başkalarına saldırılar düzenleyebilir. Bilgisayar bir botnet'in ya da bir DDoS saldırısının parçası olabilir. Başka bir neden ise güvenliği ihlal edilmiş bir bilgisayarda rootkit tespit edip temizlemek zordur. Rootkit'ler işletim sistemini derin bir şekilde bulaşmışsa kurtulmak için tek yol işletim sistemini yeniden yüklemektir. Hatta bazı durumlarda rootkit BIOS' bulaşır. Bu durumda BIOS onarılması gerekir, BIOS onarılamazsa yeni bir makine alınması gerekir. [15]

1.6.1 Rootkit Saldırısı Önlemleri

Rootkit yazılımları genellikle her kötü amaçlı yazılımda da olduğu gibi kullanıcıların kendi hataları ve güvenlik zafiyetleri sonucu başarılı olur. Rootkit engellemek için yapılabilecek en önemli şeylerden biri güncel kalmaktır. Kullanılan yazılımları, özellikle işletim sistemini güncel tutmak rootkit'lerden kaçınmanın önemli bir yoludur. Başka bir yol ise bilgisayara rootkit denetlemesi yapabilen bir yazılım kurmaktır. Ek olarak bilgisayara kurulacak uygulamaları ve indirilecek dosyaların güvenilir kaynaklardan emin olunması gerekir. Yasal olmayan crack, keygen veya actiator gibi yazılımlar kullanılmamalıdır. [14]

KAYNAKÇA

1. Karimkhani, R. (2018). DNS (DOMAIN NAME SYSTEM) NEDİR VE NASIL ÇALIŞIR? https://medium.com/@ramin_karimhani/dns-domain-name-system-nedi%CC%87r-ve-nasil-%C3%A7ali%C5%9Fir-465513138670
2. TechTarget Contributor. DNS attack. (2021). https://www.techtarget.com/searchsecurity/definition/DNS-attack
3. Wikipedia katılımcıları (2020). SYN saldırısı. *Vikipedi, Özgür Ansiklopedi*. https://tr.wikipedia.org/wiki/SYN_sald%C4%B1r%C4%B1s%C4%B1
4. Wikipedia contributors. (2022, February 23). TCP reset attack. In *Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/wiki/TCP_reset_attack
5. Şen, İ. (2018). Oturum Ele Geçirme (Session Hijacking) http://ismailsen.com.tr/oturum-ele-gecirme-session-hijacking/
6. Doğan, S. (2021). Syn Flood Nedir? Nasıl Önlenir? https://mertmekatronik.com/syn-flood-nedir#syn-nasil-onlenir
7. https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/
8. Yanmış, S. (2019). ICMP NEDİR? https://siberguvenligi.blogspot.com/2019/11/icmp-nedir.html
9. Lutkevich, B. (2021). ICMP (Internet Control Message Protocol). https://www.techtarget.com/searchnetworking/definition/ICMP
10. Hosting. (n.d.). FTP Nedir ve Nasıl Kullanılır? https://www.hosting.com.tr/bilgi-bankasi/ftp-nedir-ve-nasil-kullanilir/
11. Gloabalscape. (2018). Top 4 FTP Exploits Used by Hackers. https://www.globalscape.com/blog/top-4-ftp-exploits-used-hackers
12. İTÜ Bilgi İşlem Daire Başkanlığı. (2013). Bir FTP Sunucusuna Yapılabilecek Saldırı Türleri. https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/bir-ftp-sunucusuna-yap%C4%B1labilecek-sald%C4%B1r%C4%B1-t%C3%BCrleri
13. Helpsystems. (2017). 10 Essential Tips for Securing FTP and SFTP Servers. https://www.helpsystems.com/blog/10-essential-tips-securing-ftp-and-sftp-servers
14. https://wmaraci.com/nedir/rootkit
15. Kaspersky. (n.d.). What is Rootkit – Definition and Explanation https://www.kaspersky.com/resource-center/definitions/what-is-rootkit