DDoS El Kitabı

Ulusal Siber Olaylara Müdahale Merkezi (USOM -TRCERT)
Bilgi Teknolojileri ve İletişim Kurumu
Telekomünikasyon İletişim Başkanlığı
Tel: (0312) 586 53 05
Web: www.usom.gov.tr
E-posta: iletisim@usom.gov.tr

Eylül 2014
UR.RHB.004

İÇİNDEKİLER

1. GİRİŞ

Günümüzde en yaygın olarak görülen siber saldırılardan biri dağıtık hizmet dışı bırakma (DDoS) saldırısıdır. DDoS saldırısı çevrimiçi bir uygulama veya hizmetin çalışmasını engellemek amacıyla yapılan ve bant genişliğinin tamamını kullanarak sistemin cevap vermesini engellemeyi hedefleyen siber saldırı türü olarak tanımlanabilmektedir. Bu dokümanda OSI katmanlarına göre DDoS saldırıları, öneklerle açıklanarak, saldırılara karşı yapılabilecek işlemler anlatılmaktadır. Ayrıca DDoS trafik tiplerine ilişkin bilgiler verilmektedir.

2. OSI KATMANLARINA GÖRE DDOS SALDIRILARI

2.1. FİZİKSEL KATMAN

Verilerin fiziksel cihazlar üzerinden sinyal olarak gönderilmesini ve alınması bu katmanda sağlanır. Kablo, bağlantı, hub vb. elemanlar içerir. Fiziksel katman aynı zamanda 1. Katman olarak da adlandırılmaktadır. Bu katmanda protokol veri birimi "bittir (bits)".

Protokoller: 100Base – T & 1000 Base – X protokolleri kullanılır.

Saldırı Örnekleri: Fiziksel saldırılar.

Muhtemel Etkileri: Fiziksel varlıklar kullanılamaz, yeniden ayarlanamaz hale getirilebilir.

Yapılabilecek İşlemler: Fiziksel önlemler, erişim kontrolleri, denetim ve bakım kuralları tanımlanıp uygulanabilir.

2.2. VERİ BAĞLANTI KATMANI

Fiziksel katman üzerinden transferin kurulması, sürdürülmesi ve nasıl gerçekleştirileceğine karar verilmesi bu katmanda yapılır. Veri bağlantı katmanı 2. Katman olarak da adlandırılmaktadır. Bu katmanda protokol veri birimi "çerçevedir frame)".

Protokoller: 802.3 & 802.5 protokolleri kullanılır.

Saldırı Örnekleri: MAC flood saldırısı.

Muhtemel Etkileri: Kullanıcı kaynağından hedefine giden veri akışını bozar.

Yapılabilecek İşlemler: MAC sınırlaması, MAC yetkilendirmesi, kimlik doğrulama ve hesap verilebilme hizmetlerini sunabilen ileri seviyeli anahtarlama cihazları (switch) kullanılabilir.

2.3. AĞ KATMANI

Bu katman farklı ağlar asındaki paketlerin yönlendirme ve anahtarlama süreçlerini sağlar. Ağ katmanı aynı zamanda 3. Katman olarak da adlandırılmaktadır. Bu katmanda protokol veri birimi "pakettir (packet)".

Protokoller: IP, ICMP, ARP & RIP protokolleri kullanılır.

Saldırı Örnekleri: ICMP flooding saldırısı.

Muhtemel Etkileri: Ağ bant genişliği sınırını etkiler ve güvenlik duvarına ekstra yük getirir.

Yapılabilecek İşlemler: ICMP trafiği için hız sınırı konularak, bant genişliği ve güvenlik duvarının performansını etkileyebilecek saldırılara karşı önlemler alınabilir.

2.4. TAŞIMA KATMANI

Bu katman istemciler arasında hatasız iletişimi sağlar. 1. ve 3. katman arasında mesajların taşınması yönetilir. Taşıma katmanı aynı zamanda 4. Katman olarak da adlandırılmaktadır. Bu katmanda protokol veri birimi "bölümdür (segment)".

Protokoller: TCP ve UDP protokolleri kullanılır.

Saldırı Örnekleri: SYN flood, Smurf saldırısı

Muhtemel Etkileri: İstemci veya ağ ekipmanının bant genişliği veya bağlantı sınırına erişilmesi.

Yapılabilecek İşlemler: Internet servis sağlayıcılar (ISS) tarafından sunulan DDoS güvenlik hizmeti kullanılabilir. Bu hizmette genellikle literatürde "karadelik oluşturma (blackholing)" adı verilen yöntem kullanılarak abonelerin düşük hızlı bağlantı ya da hizmet aksaması problemleri yaşamaları önlenebilmektedir.

2.5. OTURUM KATMANI

Bu katmanda ağdaki işletim sistemleri içerisinde oturumun kurulmasını, sonlandırılması ve senkronizasyonu sağlanır. Oturum katmanı aynı zamanda 5. Katman olarak da adlandırılmaktadır. Bu katmanda protokol veri birimi "veridir (data)".

Protokoller: Oturum açma veya kapatma protokolleri kullanılır.

Saldırı Örnekleri: Telnet servis durdurma.

Muhtemel Etkileri: Sistem yöneticisinin anahtar yönetim fonksiyonlarını yerine getirmesini engelleyebilir.

Yapılabilecek İşlemler: Donanım sağlayıcının donanımlar ile ilgili yama ya da güncelleme yapıp yapmadığı ile ilgili kontroller yapılabilir.

2.6. SUNUM KATMANI

Gönderici ve alıcı arasında veri formatının dönüştürülmesi (TIFF, JPEG ve MPEG dönüşümleri), veri sıkıştırma, şifreleme/çözme işlemleri sunum katmanında sağlanmaktadır. Sunum katmanı aynı zamanda 6. Katman olarak da adlandırılmaktadır. Bu katmanda protokol veri birimi "veridir (data)".

Protokoller: Sıkıştırma & Şifreleme protokolleri kullanılır.

Saldırı Örnekleri: Kötü niyetle biçimlendirilmiş SSL İstekleri (Saldırgan sunucuyu hedef almak için http ataklarını SSL ile tüneller)

Muhtemel Etkileri: Etkilenen sistem SSL bağlantısı yapamayabilir ya da otomatik olarak yeniden başlatılır.

Yapılabilecek İşlemler: Bu katmandaki saldırıları en aza indirgemek için, SSL yük devri ayarlanması ve uygulamanın trafik akışındaki olası atakların ya da Uygulama Dağıtım Platformundaki güvenlik ihlallerinin tespit edilmesi için çalışmaların yapılması önerilir.

2.7. UYGULAMA KATMANI

Kullanıcı ya da gruplar tarafından kullanılan/koşturulan uygulamalar bu katmanda çalışmaktadır. Uygulama katmanı 7. Katman olarak da adlandırılmaktadır. Uygulama katmanında protokol veri birimi "veridir (data)".

Protokoller: Veritabanı erişimi, FTP, SMTP,POP3, HTTP, Telnet ve RAS gibi son kullanıcı protokolleri kullanılır.

Saldırı Örnekleri: PDF GET istekleri, HTTP GET, HTTP POST, İnternet Sitesi Formları (login, video ya da resim yükleme).

Muhtemel Etkileri: Kaynakların kullanım sınırlarına erişmesi dolayısıyla sistemin çalışması için gerekli kaynaklarda kıtlığının yaşanması.

Yapılabilecek İşlemler: Yazılım uygulamalarını belirli bir algoritma, teknoloji ve yaklaşımlar bütünü halinde izleyerek sıfırıncı gün açıklığı ve uygulama katmanı açıklıkları tespit edilmelidir. Bu tür kaynaklardan gelen saldırıların tespit edildikten sonra durdurulması ve saldırı kaynaklarına kadar izlenmesi diğer tür DDoS saldırıların durdurulmasından daha kolaydır.

3. DDOS TRAFİK TİPLERİ

DDoS saldırılarında görülmesi muhtemel trafik tiplerine ilişkin açıklamalar aşağıda verilmiştir.

Http Başlığı (Http Header): Http başlık içeriği URL, JPG veya GIF gibi hangi internet kaynaklarının talep edildiği bilgilerinin yanı sıra hangi internet tarayıcısının kullanıldığına ilişkin bilgileri kapsar. GET, POST, ACCEPT, LABGUAGE ve USER_AGENT çoğunlukla kullanılan Genel HTTP başlıklarıdır. DDoS saldırganları

bu başlıklar içerisindeki bilgileri değiştirerek saldırı kaynağının tespit edilmesini zorlaştırmaktadırlar. Ayrıca HTTP başlıkları ön belleğe alma (caching) ve proxy sunucu servislerini manipüle etmek için de kullanılabilmektedir.

Http Post Flood: Sunucunun cevap verebileceğinin üzerinde Http Post talebinin yapıldığı bir DDoS saldırısı türüdür. Sistem kaynaklarının yüksek hacimli kullanımı neticesinde sunucunun çökmesi ile sonuçlanabilir.

Http Post Request: Http Post Request form verilerinin yazılmış olduğu başlıktır. Örneğin Post request verilerini form'dan alır, çözümleme/kodlama yapar ve son olarak form içeriğini sunucuya gönderirler.

Https Post Flood: Http Post Flood'un SSL oturumu üzerinden gönderilmesidir. SSL kullanımı nedeniyle bu taleplerin incelenmesi için şifresinin çözülmesi gerekir.

Https Post Request: Https Post Request şifrelenmiş bir Http Post Request versiyonudur. Veriler şifrelenmiş biçimde transfer edilir.

Https Get Flood: Http Get Flood'un SSL oturumu üzerinden gönderilmesidir. SSL kullanımı nedeniyle bu taleplerin incelenmesi için şifresinin çözülmesi gerekir.

Https Get Request: Https Get Request şifrelenmiş bir Http Get Request versiyonudur. SSL kullanılmasından dolayı taleplerin incelenmesi için şifrelerinin açılması gerekmektedir.

Http Get Flood: Bu atak tipi Uygulama katmanı DDOS saldırı yöntemlerindendir. Saldırganlar yüksek hacimde talep göndererek kaynakların tükenmesine neden olmaktadır.

Http Get Request: HTTP GET Request sunucudan bilgi talebi yapmaktadır. GET sunucuya görüntü, script ya da farklı bir dosya için talep yapar. Talep sonucunu aldıktan sonra ise tarayıcıda gösterir.

SYN Flood (TCP / SYN): SYN Flood herhangi bir noda yarı-açık bağlantı kurarak çalışır. Hedef sistem SYN paketini açık olan porttan aldığı zaman, SYN-ACK ile cevap vererek bağlantı kurmaya çalışır. Bununla birlikte, SYN Flood sırasında,

istemci hiçbir zaman SYN-ACK paketine cevap vermez. Sonuç olarak hedeflenen bağlantı, zaman aşımı süresi bitene kadar, yarı-açık durumunda kalır.

UDP Flood: UDP'nin bağlantısız olması ve farklı diller ile kolaylıkla protokol 17 (UDP) mesajlarının oluşturulabilmesi nedeniyle UDP Flood genellikle büyük bant genişliğine sahip DDoS saldırıları için kullanılmaktadır.

ICMP Flood: ICMP (Internet Control Message Protocol) öncelikli olarak hata mesajlarında kullanılmakta ve sistemler arası veri değişimi yapmamaktadır. ICMP paketleri sunuculara bağlantı yapıldığı sırada TCP paketlerine eşlik edebilmektedir. ICMP taşması 3. Katman altyapılarına yönelik bir DDoS saldırısıdır. ICMP paketleri gönderilerek hedeflenen ağın bant genişliğine aşırı yükleme yapılmasını amaçlamaktadır.

MAC Flood: Çok nadir görülen bir saldırıdır. Saldırgan hedefe değişik MAC adreslerinden Ethernet frame'leri gönderir. Ağ anahtarlama cihazları MAC adreslerini ayrı ayrı ele alır dolayısıyla her bir talep için belirli bir kaynak ayırır. Anahtarlama cihazındaki tüm hafıza kullanılınca cihaz kapanır veya cevap veremez hale gelir. Bazı yönlendirici tiplerinde MAC Flood tüm yönlendirme işlemlerinin iptaline dolayısıyla yönlendiricinin alanında yer alan tüm ağın etkilenmesine neden olabilmektedir.

4. KAYNAKLAR

[1] Bhaiji, Y. 2009. *Understanding, Preventing, and Defending Against Layer 2 Attacks.* Cisco Expo.

https://www.cisco.com/web/ME/exposaudi2009/assets/docs/layer2_attacks_and_mitigation_t.pdf

[2] CERT Coordination Center. 2004. *Microsoft Windows Secure Sockets Layer (SSL) library vulnerable to DoS.* Carnegie Mellon University Software Engineering Institute.

https://www.kb.cert.org/CERT_WEB/services/vul-notes-cert.nsf/b38c0892d481f5d385256d4b005d34ea/e0bf4978a23a358385257179006cb1d8?OpenDocument

[3] Elis, J. 2012. *SSL DDoS attacks - a growing trend.* CSO Online.

http://www.cso.com.au/article/443802/ssl_ddos_attacks_-_growing_trend/

[4] Hasan, I. 2014. *Understanding MAC Address Flooding*.

http://www.ibrahimhasan.com/content/understanding-and-protecting-against-mac-address-flooding

[5] Juniper Networks. 2008. *Protecting the Network from Denial of Service Floods*. WordPress.

http://jncie.files.wordpress.com/2008/09/801003_protecting-the-network-from-denial-of-service-floods.pdf

[6] Onn Chee, W. & Brennan, T. 2010. *Http Post.* The Owasp Foundaition.

https://www.owasp.org/images/4/43/Layer_7_DDOS.pdf

[7] Phatak, P. 2011. *Cyber Attacks Explained: DoS and DDoS.* OpenSourceForU.

http://www.linuxforu.com/2011/11/cyber-attacks-explained-dos-and-ddos/

[8] Prolexic. 2014. DoS and DDoS Glossary of Terms. Knowledge Center.

http://www.prolexic.com/knowledge-center-dos-and-ddos-glossary.html

[9] Quizlet. 2014. *Lesson 2: Defining Networks With The OSI Model.* Microsoft Official Academic Course Networking Fundamentals Flashcards.

http://quizlet.com/14023507/lesson-2-defining-networks-with-the-osi-model-flash-cards/

[10] Rani, D.D. 2014. *Software Requirements Specification For TCP SYN Flooding Attacks.* QIS College of Engıneerıng & Technology.

http://learnfromtheleader.com/Downloads/SRS/TSFADP.pdf

[11] Smith, P. 2013. *DoS & DDoS Attack – Denial of Service & Distributed Denial of Service.* WebCyber.

http://webcyber.co.uk/?p=128

[12] US-CERT. 2014. *DDoS Quick Guide.* Publications.

http://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf