DOS -DDOS -1-

DOS SALDIRISI NEDİR?

DoS (Denial of Service-Servis Hizmet Reddi) bir hedef cihazın hizmet almasını veya vermesini engellemeye yönelik yapılan bir saldırı türüdür. Sistemler ağın bir parçası olurken aynı zamanda ağ üzerinde iletişim sağlayabilecekleri sınırlı bir ağ trafik hacmi ve hizmet verebilecekleri sınırlı istek sayısı vardır. DoS saldırısı hedef sistemin sahip olduğu kaynaklara aşırı yüklenebilmek için hedef sistemin karşılık veremeyeceği kadar gereksiz paketler göndermeyi amaçlar. DoS saldırısı sonucunda sistemin hizmet verememesine, kullanıcıların sisteme erişiminin yavaşlatılmasına, engellenmesine veya sistemin çökmesine neden olabilir.

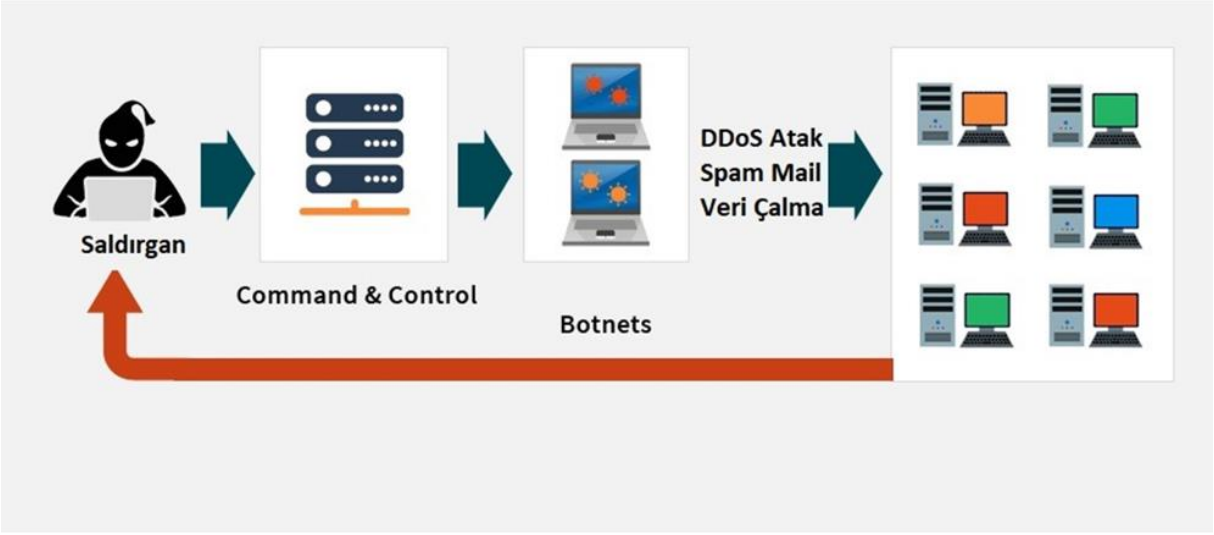
DDOS (Distributed Denial of Service) saldırısı ise DoS saldırısının etkisini arttırmak amacıyla saldırıyı zombi kaynaklardan yararlanılarak tek bir hedefe yönelik yapılan saldırılardır. Anlık gönderilen paket sayısı zombi kaynağı ile doğru orantılıdır. Saldırıyı yapan kaynak tespit edilemez. DDOS için bazı terimler ve açıklamaları aşağıdaki gibidir.

- Bot, “robot” ’un kısaltmasıdır ve komut üzerine görevler gerçekleştiren ve saldırganın etkilenen bir bilgisayardaki tüm kontrolü ele geçirmesini sağlayan bir tür yazılım uygulaması veya komut dosyasıdır. Güvenliği ihlal edilmiş bilgisayarlarada “zombi” denir.

- Zombi bilgisayarlar, özetle bir bilgisayar korsanı tarafından açığı bulunarak ele geçirilmiş cihazlardır. Çoğu zombi bilgisayar sahibi, sisteminin kullanıldığının fark edemez. Genellikle zayıf olan sisteme yerleştirilirler ve belirli bir porttan (1524 tcp, 27665 tcp, 2744 udp, 31335 udp, 33270 tcp) gelecek olan DDoS isteklerini gerçekleştirirler. Zombi bilgisayarların oluşturduğu ağa ise “botnet” (robot network) deniyor.

Zombi bilgisayarlar, dünyanın farklı konumlarında ve farklı ağlar içerisinde bulunan bilgisayarlardır. Bu bilgisayarların yönetilebilmesi için bir “botmaster” söz konusudur ve botmaster da tek başına yönetmediği için “kumanda ve kontrol sunucuları” (C&C) yardımıyla botnetlerin kontrolleri sağlanabilmektedir.

Özet bir DDOS saldırısı için kurulan topoloji aşağıdaki gibi olacaktır.



İsterseniz şimdi de bu saldırıların çeşitlerini inceleyelim;

1->Ping-of-Death Attack (Ölüm Pingi saldırısı)

İzin verilen maksimum boyuttan daha büyük boyutlu ICMP paketlerini direk hedefe gönderir. IP protokolünün izin verdiği 65536 byte boyutunda daha büyük bir paket gönderilmesi ile oluşur. Paketin büyüklüğüne göre hedef cihazın donamsına veya çökmesine neden olabilen bir DoS saldırı türüdür. Saldırıyı gerçekleştirebilmek için saldırganın hedef cihazın ip adresi bilmesi yeterlidir. Bu saldırı türü günümüzde pek kullanılmamaktadır.

2->TearDrop Attack (Gözyaşı Saldırısı)

Gözyaşı saldırısı , TCP/IP protokolünün güvenlik açığıdır. Bir bilgisayara gönderilen paketler bilgisayarda parçalar halinde aktarılır. Parça ofset (Fragment Offset) alanı, hedef cihaz tarafından paketteki tüm verilere yeniden birleştirilirken alınan bir parçanın yerleştirilmesi gereken yeri belirtmek için kullanılır ve bu ofset bilgilerinin çakışmaması gerekir. Saldırgan bu saldırı türü içi paketlere ofsetleri üst üste gelecek (çakışacak) şekilde düzenler. Paketleri alan cihaz gelen paketleri yeniden işleyemez. Bu durum zamanla cihazın çökmesine neden olur. Genelde Windows 3.1x , Windows NT , Windows 95 gibi eski işletim sistemlerinde olur.

3->SYN Flood Attack ()

SYN flood saldırısını açıklamadan önce saldırının daha iyi anlaşılması için “Three-way-handshake” yani üç yollu el sıkışmadan bahsetmeliyiz. TCP/IP ağında iletişime geçecek cihazlar arasında bir bağlantı kurmak için kullanılan bir işlemdir.

Bu işlem için ilk adımda bağlantı bağlatmak isteyen taraf hedef cihaza işletim sisteminin oluşturduğu rastgele bir sıra numarası ile SYN (synchronize) paketi yollar. İkinci adımda ise gönderilen SYN paketi alan hedef cihaz, kaynak cihaza SYN-ACK sinyali bitleriyle cevap verir. Burada gönderdiği SYN paketinin gönderdiği ACK paketiyle de aldığı paketin bilgisini bildirir. Ayrıca gönderdiği SYN paketinin sıra numarasını bir arttırır ve hangi sıra numarası ile başlayacağını belirtir. Üçüncü adımda kaynak hedef cihaza ACK paketi gönderir ve her iki cihaz da veri aktarımını başlatacağı bir bağlantıyı kurmuş olur.

SYN flood saldırısında ise TCP ‘nin üç yollu el sıkışmasını kullanarak uygulanır. Kaynak (saldırgan) SYN paketini hedefe gönderir. Böylece üç yollu el sıkışmanın ilk adımı tamamlanır. Hedef cihaz ise ikinci adımda yapılması gereken SYN+ACK olarak cevabını kaynak cihaza gönderir. Kaynak ise üçüncü adımda yapması gereken ACK mesajını göndererek bağlantıyı kurmak yerine yeni bir bağlantı istek paketi gönderir ve hedef cihaz belirli bir süre cevap bekler durumda kalır. Bu durumda cihaz yeni bağlantı oluşturamaz duruma gelir ve devre dışı kalır. Bu saldırıda dikkat edilmesi gereken nokta hedef cihazın cevap paketini beklediği belirli bir süre vardır. Bu süre içerisinde cevap paketini alamaz ise bağlantıyı sonlandırır. Bu nedenle hedefin bu bağlantıyı sonlandırmadan önce alabileceği bağlantı miktarından fazla bağlantıyı yarıda bırakarak hedefi hizmet dışı bırakmaya çalışılır.

4-Land Attack ()

Bu saldırı türünde saldırgan hedef ana bilgisayarın ip adresini içeren sahte bir TCP SYN (bağlantı başlatmak için gönderilir) paketinin hem kaynak kem de hedef adresi kısmını hedef adresin ip adresi

olarak ayarlar. Ayarladığı paketi hedef adrese gönderdiğinde hedef makinanın kendisine sürekli yanıt vermesine neden olur. Bu durum zamanla cihazın hedef makinanın CPU ‘su savunmasız makineyi süresiz olarak dondurur ve kitlenmesine veya çökmesine neden olur.

5-Smurf Attack()

Bu saldırıyı anlatmadan önce ICMP paketinden kısaca bahsedecek olursak, ICMP paketleri hata mesajları ve uzak sistem hakkında bilgi toplamak için kullanılır. Sorgu mesajları ve Kata mesajları olmak üzere iki tip ICMP mesajı vardır. Saldırgan smurf saldırısı için saldırgan ICMP paketindeki kaynak ip adresini hedef cihazın ip adresi ile değiştirir. ICMP echo istek paketlerini zombi (internete bağlı bir bilgisayar tarafından ele geçirilmiş olan internete bağlı cihaz) bilgisayarlara gönderir. Zombi bilgisayarlar ICMP yanıtlarını kaynak ip adresine gönderdiklerinde hedef bilgisayar kendisinin göndermediği cevap paketlerini alarak şişer ve bir süre sonra çalışamaz hale gelir. Bu saldırı bir DDoS (Distributed Denial Of Service) saldırı tipidir.

6-Slow Read Attack

Yavaş okuma saldırısı, anladığım kadarıyla TCP protokolünün veriyi eksiksiz iletebilmek için karşı tarafın birim zamanda alabileceği veri miktarına bağlı olarak gönderebileceği veri miktarı olarak tanımlayabiliriz. “Windows size” olarak adlandırılan bu durum hakkında buradan daha detaylı bilgi alabilirsiniz (https://accedian.com/blog/tcp-receive-window-everything-need-know/). Bu saldırıda da gönderilen verinin alındı bilgisi gelmeden yeni verinin gönderilememesinden kaynaklanmaktadır. Saldırıda özetle parçalar halinde gönderilen bir web sayfasının istemci tarafında parçaların yavaş okunmasıyla sunucunun portları işgal ediliyor. Veri aktarımı tamamlanmadığı için sunucu ve istemci arasındaki bağlantı kesilemeyecektir. Bu saldırı hedef sunucuya eş zamanlı saldırılar yapıldığında ise sunucunun farklı istemcilere hizmet vermesi engellenmiş olacaktır.

7-Icmp flood Attack

ICMP flood attack, asıl amaçlarından olan hedef cihaz ile bağlantı kontrolü, hedefin durumunu belirlemek için kullandığımız ICMP paketleri kullanılarak gerçekleştiriliyor. Saldırı hedefe ICMP yankı istek paketleri göndererek hedef cihazın hizmet vermesini engellemeye yönelik yapılıyor. Bu saldırı eş zamanlı olarak farklı cihazlardan yapılarak etkisi arttırılabilmektedir.

8-Challenge Collapsar (CC) Attack

Challenge Collapsar (CC) Attack, Web siteleri sayfa yüklemelerinde birçok farklı işlem gerçekleştirdiği gibi bu işlemler için ayrıca (CPU kaynağı) kaynak tüketmektedir. Bu kaynakları tüketebilmek adına hedef siteye yüksek miktarda HTTP isteği göndererek hedef sitenin İşlem gücünün %100 kullanılmasını sağlamaktır. Burada erişilen sayfalar çok fazla kaynak tüketmektedir. Bu durumda site yeni isteklere ayıracak kaynak bulamayacağı için hizmet veremeyecek durumda kalacaktır.

Daha fazla DOS – DDOS saldırısına buradan ulaşabilirsiniz. Ayrıca bu saldırıların uygulaması ve analizi ile ilgili yazıma buradan ulaşabilirsiniz.

9-ICMP NUKE Attack

Bilindiği gibi ICMP paketleri genel anlamda bilgisayarlar arasında bağlantıyı kontrol etmek için kullanılan bir protokoldür. ICMP NUKE Attack ise sahte adresler kullanılarak iki cihaz arasındaki düzgün işetişimi “time exceed” (type 11) veya “Destination uncreachable” (type 3) mesajlarını her iki cihaza da göndererek iki cihaz arasında sanki hata varmış gibi gösterebilir, bozabilir. Eski bir DOS saldırısıdır. Örnek bir saldırıyı buradan (https://www.youtube.com/watch?v=1eY-DqSm324) izleyebilirsiniz.

KAYNAK:

https://en.wikipedia.org/wiki/Denial-of-service_attack

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/slow-read-dos-attack-(yava%C5%9F-okutarak-hizmet-engelleme-sald%C4%B1r%C4%B1s%C4%B1)

https://www.netscout.com/what-is-ddos/slow-read-attacks#:~:text=A%20slow%20read%20DDoS%20attack%20involves%20an%20attacker%20sending%20an,slow%20speed%2C%20if%20at%20all.&text=Since%20the%20attacker%20sends%20a,therefore%20keeps%20the%20connection%20open.

https://blog.qualys.com/vulnerabilities-research/2012/01/05/slow-read

https://www.netscout.com/what-is-ddos/icmp-flood#:~:text=An%20Internet%20Control%20Message%20Protocol,echo%2Drequests%20(pings).

https://www.mlytics.com/blog/how-we-mitigated-one-of-the-largest-cc-ddos-attacks/

https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server#:~:text=A%20command%2Dand%2Dcontrol%20%5B,data%20from%20a%20target%20network.&text=Establishing%20C%26C%20communications%20is%20a,move%20laterally%20inside%20a%20network.

https://www.onespan.com/blog/what-bots-botnets-zombies

ICMP TYPE CODE LİNK

https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml