|  |
| --- |
| ***Siber Saldırı Çeşitleri*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -DDOS Saldırıları  -Uygulama Bazlı Saldırılar  -Spear Phishing  -Phishing Saldırıları  -MITM |

**19.08.2021**

***DOS ve DDOS***

-DOS saldırısı tek bir aygıt üzerinden yapılırken,DDOS iki ve üzeri sayıda aygıt ile yapılan saldırılardır.Bu saldırı Botnetler aracılığı ile çok basit bir şekilde yapılmaktadır.

-Bu saldırı sırasında sunucuya sürekli “istek” gönderme işlemi yapılır ve sunucu artık geri dönüt veremeyerek devre dışı kalır.

-Büyük boyutlu saldırılara önlem almak gerçekten çok zordur.

-DDOS saldırılarının uygulanmasıyla ilgili bir doküman hazırlanmıştır.

***Uygulama Bazlı Saldırılar***

-Bu saldırılara Mobil ve Web uygulamalarını dahil edebiliriz.

-Bu tarz uygulamalara örnek vermek gerekirse;SQLİ,XSS,LFI verilebilir.

-Bu örneklerle ilgili kapsamlı uygulama dökümanı hazırlanmıştır.

-Bu saldırılar da genel olarak uygulamada ki input alanına sistemin beklemediği kodlar girerek hedef uygulamanın çalışma şeklini değiştirmek,veritabanından bilgileri sızdırmak veya yetkisiz erişimler sağlamak amaçlanmaktadır.

-Örneğin bir XSS saldırısında <script>alert(“XSS Alert”)</script> gibi payloadlar yerleştirilebilir.

***Phishing(Yemleme) Saldırıları***

-Yasa dışı yollarla bir kişinin şifresini veya kredi kartı detaylarını öğrenme saldırı olarak nitelendirilmektedir.

-Phishing saldırılarında saldırgan kişi bir “yem” hazırlar ve bu yeme kurbanların takılmasını amaçlar. Yem genelde maaş zammı, hediye, ücretsiz tatil, para ödülü şeklinde cezbedici senaryolardan oluşturulur.

-Bu saldırılar mail yoluyla gerçekleştirilmektedir.

***Spear Phishing***

-Hedef odaklı yapılan saldırılardır.Belirli bir hedefe yönelik yapılır.Başarı oranı en yüksek oltalama tekniğidir.

-Büyük kurumlara gelişmiş seviye zararlı yazılımların büyük çoğunluğu bu saldırı yöntemi ile bulaştırılmaktadır.

-Örneğin bir firma hakkında internet üzerinden şikayetçi olduk.Bunu görüntüleyen saldırgan sanki o firmadan arıyormuş gibi sizinle iletişime geçer.

-Daha sonrasında sizden kişisel bilgileri elde eder.

***Man In The Middle(MITM)***

-Ortadaki adam saldırısı olarak Türkçe’ye çevirebiliriz.

-Bu saldırı local ağ üzerinden gerçekleştirilmektedir..

-Klasik yöntemlerden biri şudur: ARP zehirlenmesi yaparak yönlendiricinin ARP tablosu taşırılır

-Yönlendirici gelen ARP isteklerini yanıtlayamaz hale gelir.

-Sonrasında ağda broadcast olarak ARP isteği yanıtı paketleri yollanır. Bu durumda ağda yönlendirici arayan bir bilgisayar olursa gerçek yönlendirici yerine saldırganın bilgisayarını yönlendirici olarak tanıyacaktır.

-Ağ üzerinde verilerini saldırganın bilgisayarı üzerinden gönderecektir. Şifrelenmemiş her veri paketi kolaylıkla açılabilir ve değiştirilebilir.