TCP/IP Zafiyetleri (TCP/IP Vulnerabilities)

Bknz: OSI

Ip Spoofing

IP Spoofing, gönderenin kimliğini gizlemek, başka bir bilgisayar sisteminin kimliğine bürünmek veya her ikisini birden yapmak için değiştirilmiş bir kaynak adresine sahip İnternet Protokolü (IP) paketlerinin oluşturulmasıdır. Genellikle kötü aktörler tarafından bir hedef cihaza veya çevresindeki altyapıya DDoS saldırıları başlatmak için kullanılan bir tekniktir.

TCP Session Hijacking - SKEY Bypass

Cleartext üzerinden işlem yapmakta olan protokoller, güvenlik yapısı olarak zayıflardır. Bu gibi iletişimlerin güvenli hale getirilebilmesi için, genellikle ağ dahilindeki yetkilendirilmeler düzenlenir ve one-time-password yapıları kullanılır.

ARP Protokolü - Spoofing

Kötü niyetli kişi, haberleşen cihazlara sahte kimlik bilgileri göndererek, kendini ağdaki başka bir cihaz gibi tanıtbilir ve bu sayede haberleşmenin kendi üzerinden gerçekleşmesini sağlayabilir.

IP Fragmentation / DoS & WAF Bypass

Bu saldırılar, hedef ağın elemanı olan cihazların işleyebileceğinden (MTU - Maximum Transmission Unit) daha büyük boyutlarda olan sahte UDP veya ICMP paketlerinin üretilmesi ve gönderilmesi ile gerçekleştirilir.

Gelen 4500 lük paket, 1500 1500 1500 parçalanır, okunur. Daha sonra birleştirilir. Bu sırada büyük paketler ekstra bir bayt için tükenir. Küçük bir bayt yorar. RAM yorulur. İncelemeden geçen baytlar olur. (sql inj temper örn)

ICMP Smurfing

Bu saldırıda, saldırgan bir ping paketi oluşturur ve bu pakete cevap verilecek IP adresini kurban makinenin ip adresi ile değiştirir. Sonrasında ise bu ping istekleri, ip bloğunun broadcast adresine flood şekline gönderilir.

İşlem sonucunda istekleri alan her elemen bu isteklere cevap verir. Cevap adresi daha önceden değiştirildiğinden ve kurban makineyi hedef aldığında tüm cevaplar kurban ip adresine gönderilir.

Bu iletişim akışı bir süre sonra hedef makinenin bu paketlere cevap veremez ve iletişime geçemez hale gelmesine sebep olur.

Ping özelliği kapatılır.

DNS Amplification

DNS Servisleri, hızlı olmak ve bir çok istemciye kısa sürede cevap verebilmek adına hem TCP hem de UDP türünde çalışırlar.

DNS istek yapılarının belirli kalıplara sahip olması durumu ile de birlikte, 512 byte ve daha küçük boyutta olan trafiklerin hepsi UDP olarak işlenir. Bundan daha büyük boyutlara sahip olan paketler ise, TCP alarak işlenirler.

Amplification saldırısı, saldırganların DNS paket boyutlarını büyütmeleri sonucunda sunucunun bunları TCP olarak işlemesi zorunluluğu ortaya çıkar.

Boyutu şişirilmiş olan bu paketler ile, sunucu artık üzerinde yapılabilecek TCP bazlı saldırılara yatkın olabilir.

TCP SYN Flood Attack
(SYN ACK FIN RST PSH URG)

TCP Slow HTTP Attack
(Layer 7)