ARP POİSONİNG

Adress Resolution Protocol

ARP NEDİR?

- Açılımı: Adres Çözümleme Protokolü
- Network üzerindeki paketlerin gidiş gelişinde adresleme işlemlerini düzenler.
- Peki bu işleme neden gerek var?

ADRESLEME İŞLEMLERİ

- Yerel ağlarda ethernet kullanılarak haberleşilir.
- Ethernet 48 bitlik adresleme sistemi kullanır.
- TCP/IP kullanılan sistemlerde ise 32 bitlik adresleme kullanılır.
- Adresler arasındaki bu farklılıklar sonucu ARP geliştirilmiştir.
- Örnek IP : 255.255.255.255 4*8 = 32 bit
- Örnek MAC : 12:35:49:ac:de:f9 6*8 = 48 bit

- Burada ARP devreye girerek adresleme sorununu çözer. Ama nasıl?

PROTOKOLÜN ÇALIŞMASI

- Donanımların adresleri nasıl verilir ?
- Bir ana bilgisayarın adreslemede kullanılan iki verisi vardır;
  - IP
  - MAC
- Her bilgisayar için bu ikisinin eşleşmesinden oluşan bir adres sistemi vardır.
- MAC adresi eşsiz olmakla beraber IP dinamik veya statik olabilir.
- Adreslemenin içinde router cihazının da yeri vardır. Paketleri bu cihaz yönlendirir.
- Bu elemanlar Mac adreslerini önbelleklerinde de tutarlar. (ARP cache)

PROTOKOLÜN ÇALIŞMASI

- Paketi gönderecek bilgisayar karşıdaki cihazın IP adresine sahiptir. Yalnız bu yeterli olmamakta MAC adresinin de bilinmesi gerekmektedir.
- Mac adresi önce ARP Cache dediğimiz bellekte aranır. Burada varsa gönderilir. Yoksa;
- Paketi gönderecek bilgisayar ağ üzerinde broadcast bir yayın yapar ve elindeki IP nin sahibinin kendisine MAC adresini yollamasını ister.
- Yapılan yayındaki IP adresiyle eşleşen bir bilgisayar istekle gelen IP ve MAC adresini kullanarak kendi MAC adresini yollar.
- Paket yollamak isteyen ana makine bu bilgiyi kullanarak paketi yollar.
- İlgili makinede paketi alır.

ADRESS RESOLUTİON PROTOCOL

- Protokolün nasıl çalıştığını öğrendik. Konumuzla ilgili olarak şunu da ekleyebiliriz.

- Bu süreç doğal haliyle şifrelenmeden gerçekleşmektedir.
- Saldırıyı cazip kılan en önemli etkenlerdendir.

- Şimdi poisoning kısmını ele alalım.

ARP - POİSONİNG

- ARP Poisoning işlemi bir kaç adımla anlatılabilir.
- Öncelikle yöntemden bahsedelim.
- Bu işlem ARP Cache'teki MAC adresinin değiştirilmesiyle gerçekleştirilir. Bu manipülasyon yapılmadan önce saldırıyı gerçekleyecek kişi ağı dinleyip (yada koklayıp { sniff = koklamak }) kullanacağı IP ve MAC adreslerini belirler.
- Ağı dinlerken hiçbir saldırı yapmaz sadece giden gelen paketleri dinler.
- Buradan kendi Mapping tablosunu oluşturur diyebiliriz.
- Bu işlemde tamamlandıktan sonra zehirleme işlemine geçmek için hazır demektir.

ARP - POİSONİNG

- Burada önce ARP Cache alanındaki MAC adresleri değiştirilir.
- Sniffer bunu şu şekilde yapar. Kendi MAC adresini MAC spoofing denilen yöntemle rastgele bir şekilde seçer. ÖR: 00:11:22:33:44:55
- Önbellekteki MAC adresleri de bu Mac adresine eşitlenir.
- !!!!!! Asıl MAC adresleri değişmiyor sadece önbellekteki MAC adresleri değişiyor.
- Bu noktadan sonra iki bilgisayar arasına girerek karşılıklı gönderilen bütün paketler önce bize gelecektir.
- Bizde gelen paketi aldıktan sonra kendi map imizi kullanarak paketi tekrar ait olduğu yere göndeririz. Bunu yapmalıyız yoksa açığa çıkmış oluruz.
- Bu şekilde dosyalar mailler şifreler msn konuşmaları gibi bir çok bilgi ele geçebilmektedir.

ARP - POİSONİNG

- Burada hassas nokta paketler az bir gecikmeyle de olsa asıl sahibine ulaştığı için iki uç tarafında bir sorun olduğunu anlamamasıdır.

- Bu işlemden korunmak için bazı yollar vardır. Bunları şu şekilde sıralayabiliriz:

ARP – POİSONİNG KORUNMA YOLLARI

- Netrwork kartlarına fiziksel ulaşımı engelleyerek sniffer kurulmasını engellenmelidir.
- Statik IP adresleri kullanılmalı ve ARP kayıtlarını statik olarak eklenmelidir.
- Netwrork'te sniffer olup olmadığını denetleyecek birden fazla araç var bunlardan bazıları;
- Arp Watch
- Promiscan
- Antisniff
- Prodetect
- Network switchlerinde port güvenliğini sağlayacak özellikler aktif edilmelidir.
- Büyük işletmelerde farklı vlan'lar tanımlayın.
- Snifferlardan korunmanın en iyi yolu trafiği şifrelemektir. Bunun için networkte SSH veya Ipsec kullanılmalıdır. Bu snifferın çalışmasını engellemeyecek fakat yakaladığı verilen anlaşılması engelleyecek veya kırılması için gereken süreyi uzatacaktır.

ARP - POISONING

- Sonuç olarak bu saldırının çok kolay gerçekleştirilebildiğini görmüş oluyoruz.
- Kafe, hastane, pastane, internet kafe vs. her türlü ortak kullanım alanında bu saldırıya maruz kalabiliriz.
- Alınabilecek tedbirler olmakla birlikte bu saldırıların bitmeyeceğini aklımızda tutmalıyız.