AĞ SALDIRILARI

Sızma/İstismar İşlemi

Hedef alınan sunucuya birçok veri gönderilerek meşgul edilmesi, servisinin durdurulması ve hatta kapatılmaya zorlanmasını amaçlar. İkisi arasındaki temel fark ise DDOS saldırısının birden fazla odaktan yapılmasıdır.

Bir DDOS saldırısı profesyonel seviyede yapıldığında veri tabanı yanıt veremez ve çöker. DDOS saldırısı yüzlerce bilgisayar üzerinden gerçekleştirilebilir. Saldırının gerçekleştirilme şekli ise bir ana bilgisayar ile **zombi** olarak adlandırılan kurban bilgisayarlar üzerinden hedef siteye sürekli olarak giriş çıkış yapılmasıdır.

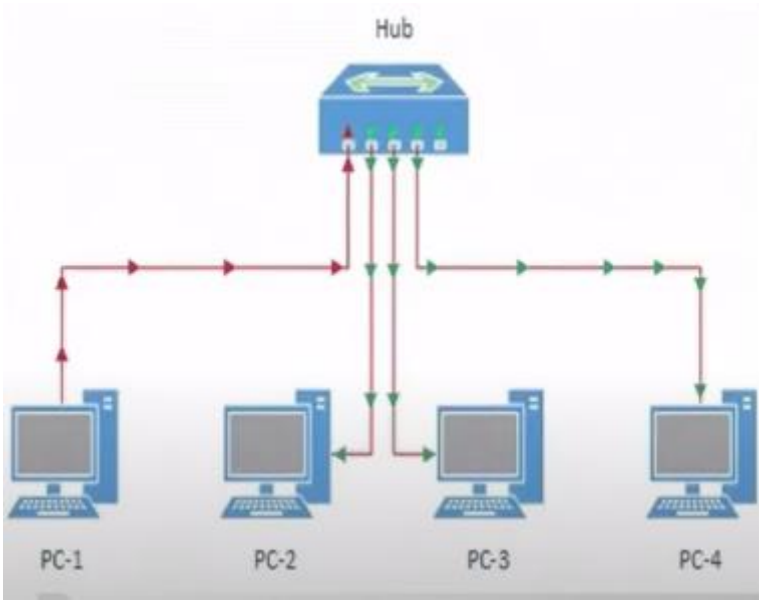
DDOS saldırılarını yüksek güvenliğe sahip güvenlik duvarı Firewall yazılımları sayesinde durdurabiliriz.

Ağ Trafiğini İzleme

Ağ trafiğini izlemek için trafiği yöneten cihazı yanıltmamız gerekir. Bunun için oldukça yaygın kullanılan Wireshark programını kullanacağız.

Wireshark programı bir ağ trafiğini dinlememize ve ağı manipüle ederek ağdaki diğer bilgisayarlardan değerli bilgiler toplamamızı sağlar.

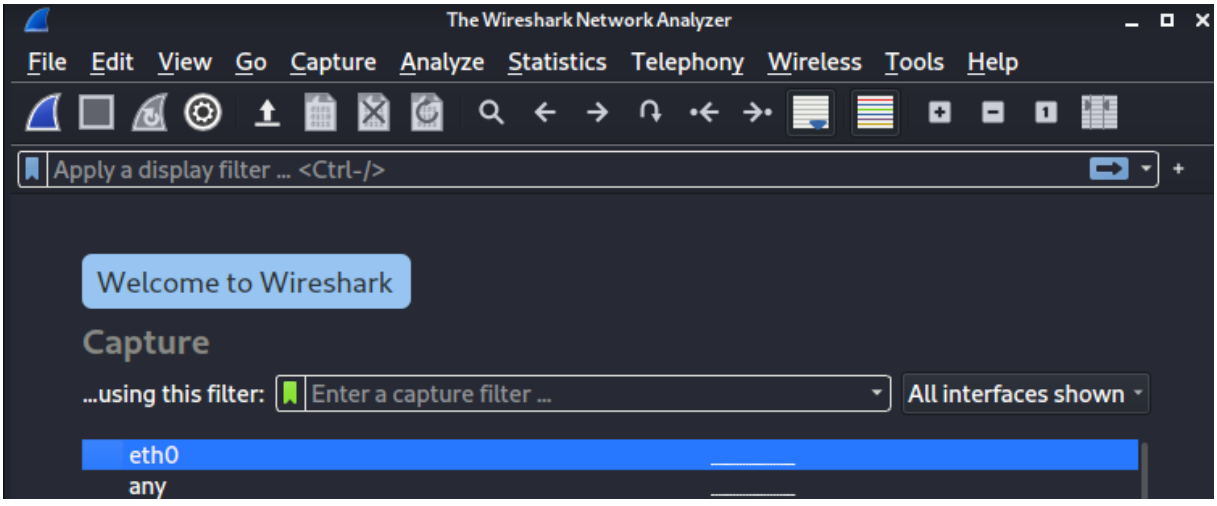
Yerel ağlarda eskiden hub adı verilen cihaz kullanılırdı. Bu cihaz ağ içinde iletişimi sağlamak için gönderilmesi gereken paketi alır. Bu paketi bütün ağlara yönlendirirdi. Gelen paketi alan cihazlar ise bilgileri paket ile uyuştuğu durumda paketi alır. Uyuşmadığı durumda gelen paketi silerdi.



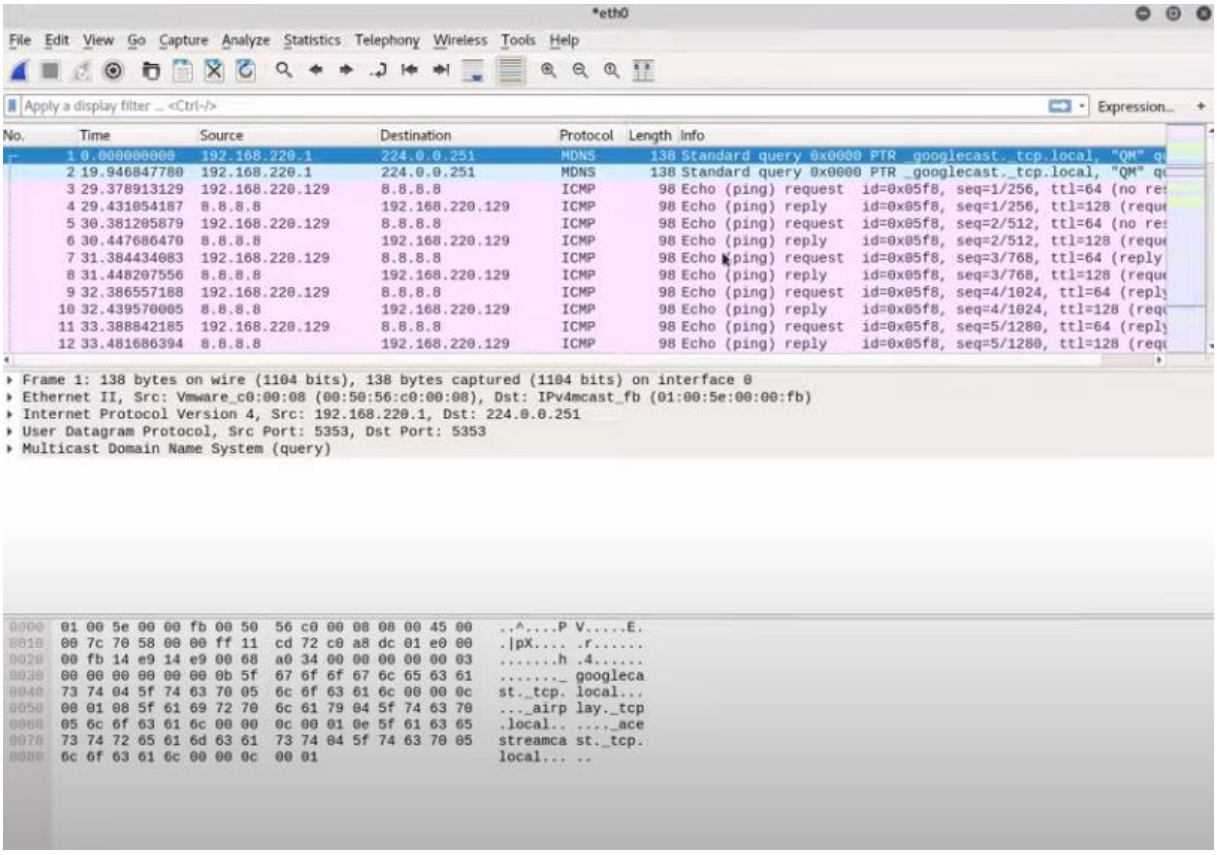
Switch, yani anahtarlayıcı. Cihazı kullanılan ağlarda gönderilen veri paketi sadece ilgili hedef makineye gönderilir. Bu veri iletimi yöntemi eskiden kullanılan hub cihazlarına kıyasla oldukça güvenlidir. Switch cihazı yerel ağda kendisine fiziksel olarak bağlı olan makinelerinin MAC adreslerini barındırdığı MAC tablosuna kaydeder. Bu tabloda ağdaki cihazların IP adresleri ile MAC adreslerini eşler ve ağ topolojisi her an bir değişiklik gösterebileceğinden bu tabloyu belirli aralıklarla günceller.

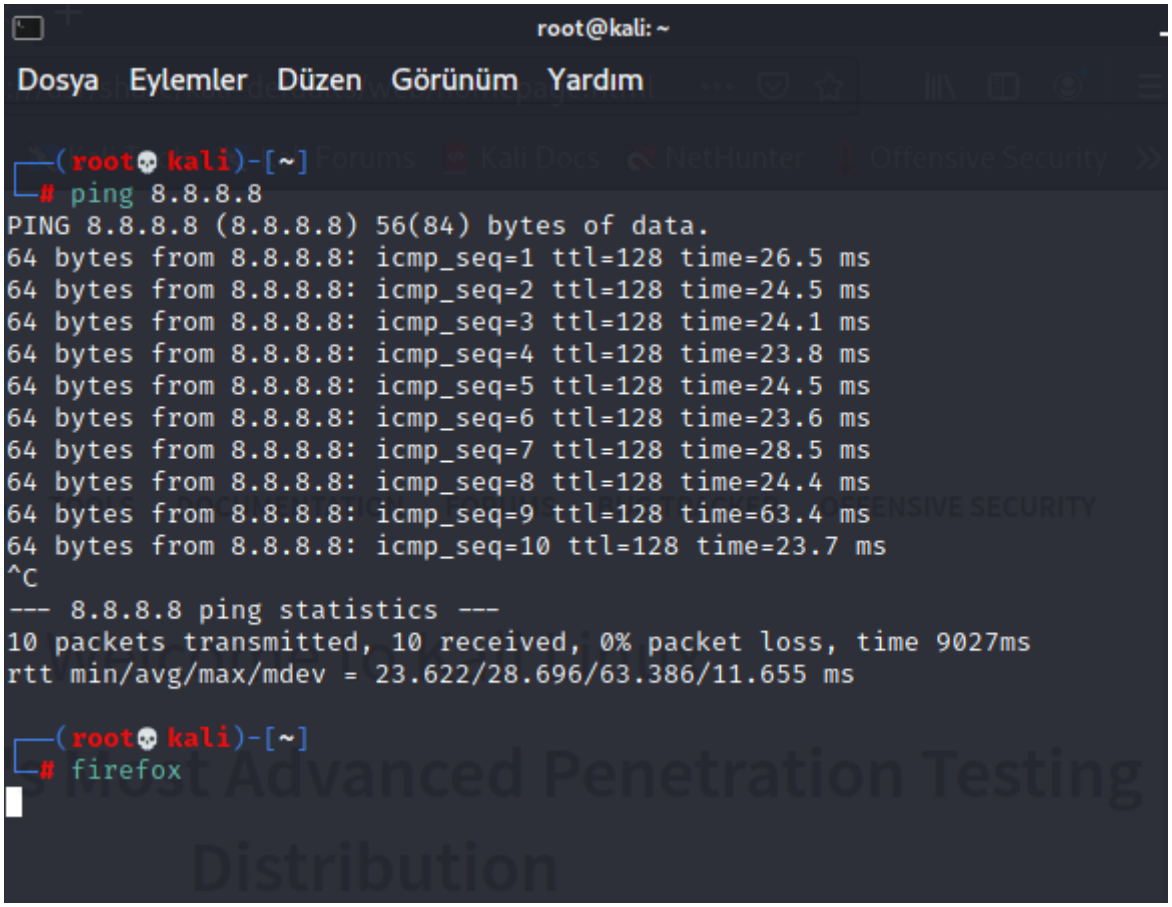
```
Switch#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000c.2928.5c6c    DYNAMIC     Fa0/1
   1    000c.29e2.03ba    DYNAMIC     Fa0/2
   1    000c.2944.0343    DYNAMIC     Fa0/3
```

Wireshark ile Ağ Trafiğini İzleme



Kalinin kullandığı ara birim eth0'dır.





ARP Zehirlemesi

Sızma testlerinde ARP zehirlemesiyle sisteme giriş yapan kullanıcı oturumlarını dinleyebiliriz. Bu oturum ile HTTP serverına erişim sağlayabilir, hatta sistemin farklı birçok yerinde oturum açabiliriz.

Ağı bilen bir switch cihazının bizimle ilgili olmayan paketleri hiçbir şekilde bize göndermeyeceğini biliyoruz.

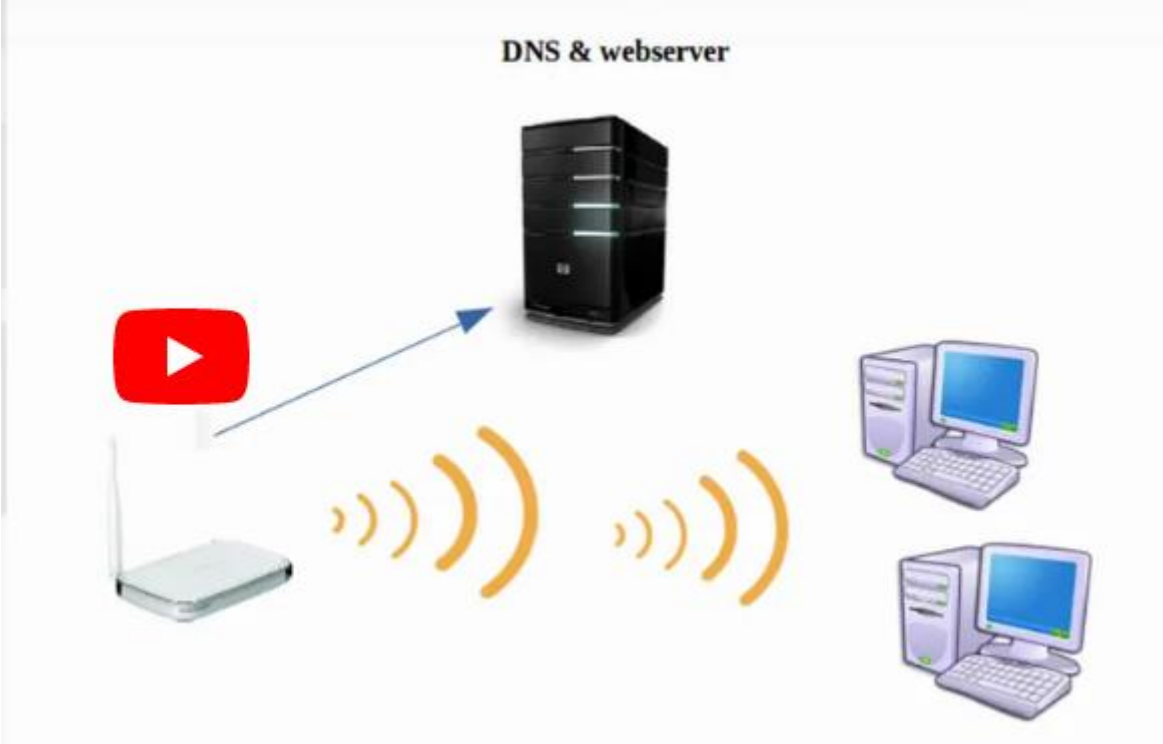
ARP (Adress Resolution Protocol) paketleri broadcast adresi olarak yönlendirilir. Gönderilen veri paketi, ağdaki bütün makinelere iletilir. Gönderici, alıcı ile iletişim kurmak istediğinde ARP tablosunu kontrol eder.

Hedef makineye benim switch cihazı olduğuma inandırırsam, hedef makineye veri iletmek için önce bana gönderecektir. Bende bu paketi gerçek switch cihazına yönlendirir ve bana gerçek switch cihazından geri dönen paketi hedef makineme geri gönderirim. Bu sayede hedefim hiçbir şey fark etmeden ben onun gönderdiği ve ona geri dönen paketleri dinlemiş olurum. Bu saldırı ortadaki adam (man in the middle) saldırısıdır ve ARP zehirlemesi olarak bilinir.

route -n : Gateway öğrenme.

ettercap -G : ARP zehirlemesi yapmak için grafik ara yüzü açmak.

DNS Zehirlemesi



DNS zehirlemesi ile de bir ağ trafiği dinleyebiliriz. ARP, IP ile MAC adreslerini eşliyorsa, DNS de IP adresleriyle alan adlarını eşler. DNS zehirlemesinde hedef makinedeki DNS cache'i zehirleyerek istediği siteye ulaşması yerine bizim kontrolümüz altında bulunan siteye ulaşmasını sağlarız.

Bağlanmak istediğimiz alan adıyla IP adresi eşleyen servis DNS servisidir. DNS, IP adresini alan adıyla kaydeder ve bize onlarca IP adresinin kime ait olduğunu hatırlama zorluğundan kurtarır.

KAYNAKÇA

Bilgeiş "Sızma Testine Giriş" eğitimi.