YILDIZ TECHNICAL UNIVERSITY

FACULTY OF ELECTRICAL AND ELECTRONICS

SECURITY OF COMPUTER SYSTEMS (BLM4011)

LAB 1 – ARP POISONING

20011701 – Muhammet Ali ŞEN
20011045 – Muhammed Ali LALE

ali.sen@std.yildiz.edu.tr
ali.lale@std.yildiz.edu.tr

DEPARTMENT OF COMPUTER ENGINEERING

1. GİRİŞ

ARP (Adres çözümleme protokolü), IP adresini ile yerel ağda tanınan fiziksel makine adresine (MAC) eşlemek için kullanılan bir protokoldür. IP adresleri, yerel veya genel ağlarda başka makinelerle iletişim kurabilmek için kullanılırlar. MAC adresleri ise ağ bağlantılı her makineye fiziksel olarak atanmış *unique* adreslerdir. Aynı ağda bulunan makineler arası iletişimi sağlamak için data link layer'da kullanılırlar.

Yerel bir ağda alıcının bilinen IP adresi kullanılarak bir veri paketi gönderildiğinde, gönderici, alıcının MAC adresini bulabilmek için aynı ağdaki tüm cihazlara bir mesaj yayınlar. MAC adresi bulunduğunda gönderici ARP tablosu denilen bir tabloda adresi saklar. Bu şekilde her request göndermek istenildiğinde MAC adresinin yeniden aranıp bulunmasına gerek kalmadan önce tabloyu kontrol eder.

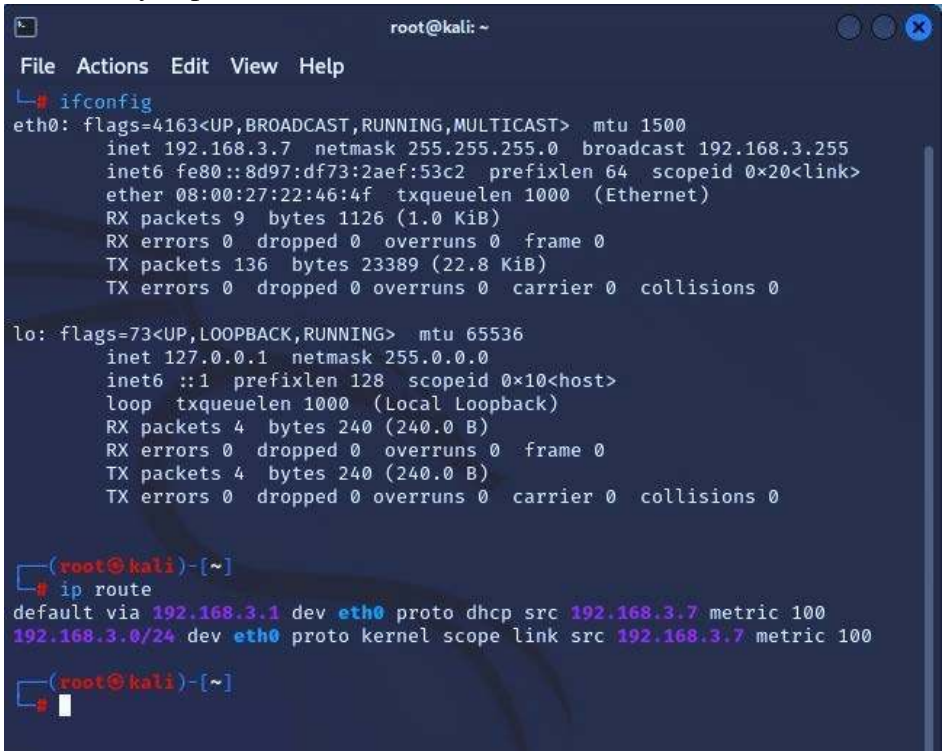
ARP'te kimlik doğrulamadaki bu güvenlik eksikliği nedeniyle yerel ağda bulunan her cihaz ARP isteklerine yanıt verebilir. Bir makine alıcı makineyi bulmak istediğinde yerel ağda herkesin yanıtlayabileceği bir ARP isteği gönderir. Bu güvenlik açığı sayesinde sahte ARP cevapları gönderilerek hedefin ARP tablosu sahte bilgilerle doldurulabilir. Saldırganlar "man-in-the-middle (ortadaki adam)" saldırısıyla kendilerini alıcı kimliğiyle gizleyerek hedef makinin paketlerine erişim kazanabilirler. Bu tür bir saldırı için saldırgan, göndericinin ARP tablosunda bulunan alıcı IP adresini ve alıcının ARP tablosunda bulunan gönderici IP adresini kendi MAC adresiyle eşlemek üzere *zehirlemelidir*. Bir DoS saldırısı tüm veri paketlerini tek bir MAC adresine göndererek de yapılabilir.

ARP poisoning'in doğası gereği bir saldırı, saldırıdan önce ve sonra hedefin ARP tablosu kontrol edilerek anlaşılabilir. Saldırının en büyük göstergesi bir makinenin MAC adresinin orijinalinden farklı olması ya da aynı MAC adresine sahip birden fazla makine olmasıdır. Bu durum her verinin elle girilmesinin gerektiği yerlerde statik bir ARP tablosu kullanılarak kolayca önlenebilir. Ancak bu yöntem IP adreslerinin ağ içinde sürekli olarak değişmesinden dolayı genel ağlarda uygulanabilir değildir. Saldırıları önlemede en yaygın yöntem şifrelemedir. HTTPS veya başka şifreleme protokollerinin kullanımında saldırgan hala paketleri görebilir ancak içeriğini okuyamaz.

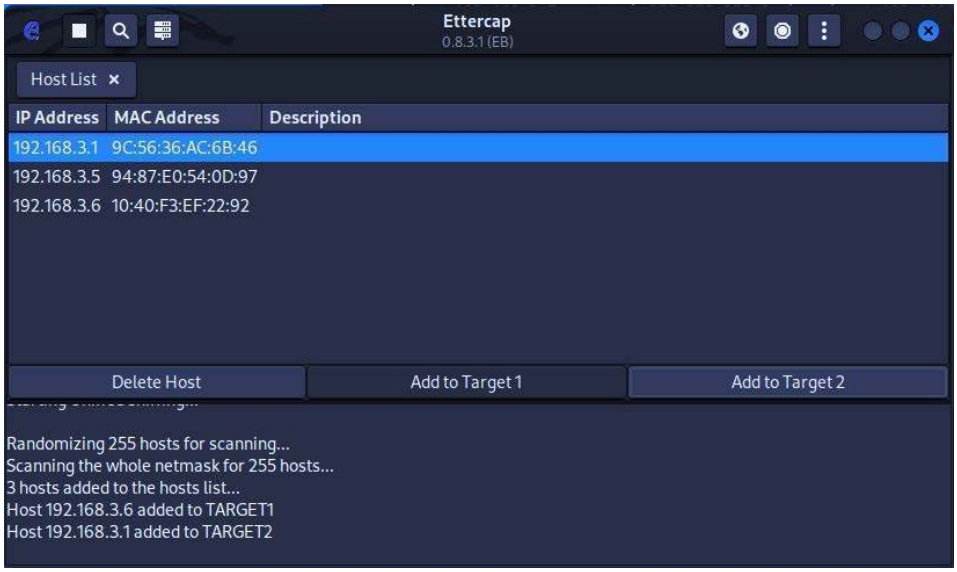
2. METOT

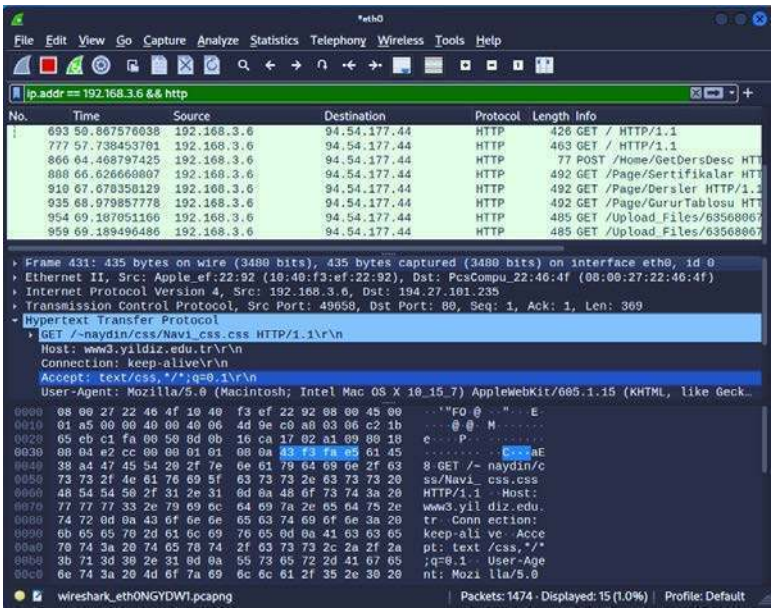
Bu saldırı için öncelikle saldırgan ve hedefi aynı yerel ağda olmalıdır.

- Router IP'yi 'ip route' komutu ile bulabiliriz.

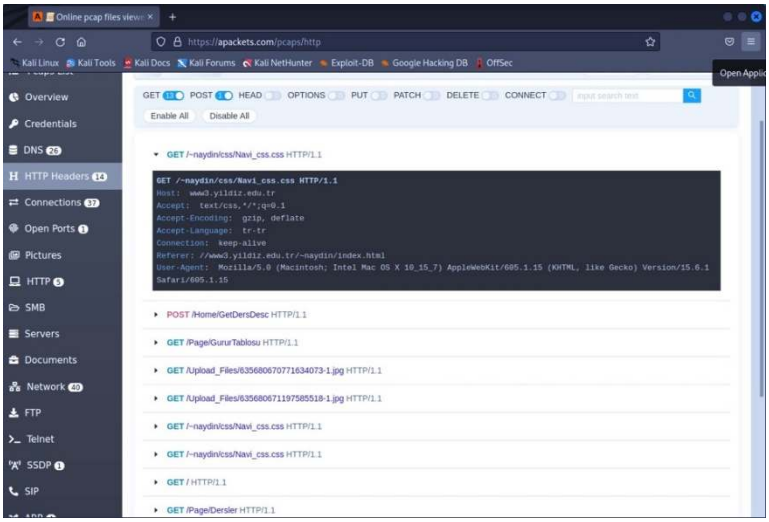


- Ağı sahte girişlerle doldurmak için Ettercap gibi bir tool kullanmalıyız.
- Ettercapte ağı tarayarak *availible hosts* bulunur.
- Bu host listesinden router ve hedef seçilir. Target 1'e hedefi, Target 2'ye de routerı seçeriz.
- Saldırıyı başlattıktan sonra hedefin ARP tablosundaki router MAC adresi bizim MAC adresimiz ile güncellenir. Bu şekilde veri paketleri artık routerdan önce bize gelecekler.





- Paketleri aldıktan sonra bu paketlerin içeriğini görebilmek için Wireshark gibi bir program kullanabiliriz. Burada elde edilen sonuçlar "ip.addr == <hedef_ip> && http" ile sadece hedeften gelen paketleri gösterecek şekilde filtrelenebilir.



- Apackets.com gibi siteler üzerinden gerekli analizler yapılarak data paketleri incelenebilir.

3. SONUÇLAR

Arp poisoning diğer bir deyişle ‘man in the middle’ saldırıları aynı ağda bulunan hedeflerin ip adreslerinin tespit edilmesi ve hedef ile router arasına girerek (kendisini router gibi göstererek) data paketlerinin yakalanmasına dayanır. Saldırgan MAC adresi Router MAC adresini zehirleyerek kendi MAC adresini Router MAC adresine kopyalar ve bu sayede çıkan data paketlerini hexadecimal olarak yakalar. Yakalanan data paketleri, http protokolü gibi güvenli olmayan protokollerle iletişim sağlamışsa kolayca içi açılıp incelenebilir. Bu tip saldırılara maruz kalmamak için https olan secure protokollerle iletişim kurulmalıdır. Ayrıca poisoning işlemi sonrası router MAC adresi saldırganın MAC adresi olmuştur. Bu şekilde kurban kendi terminali üzerinden ‘arp -a’ komutu ile MAC adreslerini de kontrol ederek poisoning (zehirleme) yapılıp yapılmadığını anlayabilir. OSI layer 2 katmanında (kısmen 3 de denilebilir) gerçekleşen arp zehirlemesi saldırısı tehlikeli bir saldırı türü olmakta ve tespiti için çok dikkatli olunması gerekmektedir. Arp zehirlemesine karşı kurulan güvenlik sistemleri ağlarda kullanılmalıdır.