ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/arp-protokolu-ve-guvenlik-zafiyeti/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Arp%20Protokolu%20ve%20G%C3%BCvenlik%20Zafiyeti.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

• ARP protokolü yerel ağlarda iki hostun birbirleri ile anlaşabilmesi için kullanılan protokoldür.(RFC 826)

• İki host birbiri ile iletişime geçmeden önce birbirlerinin IP adreslerini bilmek zorundadır.

–IP adresini bilenlerin iletişime geçebilmesi için MAC adreslerini edinme zorunluluğu vardır.

• Ipv6 ‘da ARP yerine benzeri işlevi yerine getiren Neighbor Discovery Protocol(NDP) geliyor.

• ARP iki işlemli bir süreçtir.

–ARP Request

–ARP Reply

(Page 4)

2)

Arping

• Arping adından da anlaşılacağı gibi Layer 2 seviyesinde ping atmaya yarayan bir araçtır.

• Arping kullanarak Layer 2 seviyesinde bir makinenin açık olup olmadığı, ağdaki ip çakışmaları, bir ip adresinin ağda kullanılıp kullanılmadığı gibi bilgiler edinilebilir.

• Arping’in en basit kullanımı ağdaki bir ip adresine ARP Request paketi yollamak ve cevaben gelen ARP Response ile de MAC adresi öğrenmektir. Bunu aşağıdaki komutla gerçekleyebiliriz.

> arping -I eth1 -c 1 192.168.2.1

> tcpdump –i eth1 –tttnn arp

(Page 16)

3)

•Eğer ek güvenlik önlemleri alınmamışsa bir ağda ele geçirilen makine diğer tüm makinelerin güvenliğini tehdit eder!

(Page 19)

4)

•ARP cache poisoning yerel ağ saldırısı olarak gözükse de genellikle birçok saldırıda ara bileşen olarak kullanılır.

•Saldırgan web zaafiyetini kullanarak sunucunun barındığı yerel ağdaki bir makineyi ele geçirir.

(page 21)

5)

ARP Cache

•İşletim sistemleri erişmek istedikleri ip adreslerine her seferinde ARP sorgusu göndermek yerine aldıkları ARP cevaplarını bir müddet saklarlar.

•Bu saklanan bilgiye ARP kaydı denir.

•Arp kayıtlarını listeleme

> arp –a

Output:

```
Interface: 192.168.2.2 --- 0x5
  Internet Address      Physical Address      Type
  192.168.2.1           00-12-bf-54-3d-bd     dynamic
  192.168.2.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0x8
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

(Page 25)

6)

ARP Saldırı Araçları (Windows)

- Winarpspoof
- Ettercap
- Cain&Abel

ARP Saldırı Araçları (Linux)

- Arpspoof
- Ettercap
- Nemesis
- Scapy

(page 29)

7)

ARP Saldırılarından Korunma

• Statik ARP kaydı girilmesi

• Arpwatch gibi yazılımların kullanılması

> apt-get install arpwatch

(Page 65)

8)

Arp tablosuna statik IP–MAC kaydı koyularak router'ın kimliği değiştirilemez kılınabilir ve böylelikle yerel ağdaki saldırganın sahte arp paket yayını ile kendini router olarak göstermesinin önüne geçilmiş olur. Ancak router'ı tanımlayan statik IP-MAC kaydı yerel network'teki her bilgisayara koyulmalıdır. Anca bu sayede saldırgan hiçbir bilgisayarı ben router'ım diye kandıraz. Lakin büyük LAN'larda bu bir problemdir. Çünkü konfigure edilmesi gereken çok sayıda bilgisayar olacaktır.

http://www.youngzsoft.net/cc-get-mac-address/anti.htm